servicenow

IT Operations Management Zürich

Zuletzt aktualisiert: 10.11.2025

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

product/event-management/files/K900249.PSM

product/event-management/files/R900249.PSM

IT Operations Management **5**

ITOM/OT SU-Lizenzierung Und -Abonnements 9

ITOM/OT SU-Lizenzierung erkunden 10

ITOM/OT SU-Lizenzierung konfigurieren 20

ITOM/OT SU-Lizenzierung verwenden 21

ITOM/OT SU-Lizenzierung – Referenz 26

ITOM Store-Upgrades 32

ITOM Cloud Accelerate 32

Cloud Account Management 34

Cloud-Services-Katalog 122

Bewertung der Cloud-Migration 194

Cloud Provisioning and Governance 194

Governance für Cloud-Konfigurationen 672

Bibliothek von Cloud-Aktionen 760

ITOM Cloud Accelerate-Referenz 791

ITOM-Optimierung 795

ITOM-Optimierung – Referenz 796

ITOM-Transparenz 797

Discovery 801

Firewall-Audits und Reporting 1415

Zertifikatsbestand-Management 1428

Service-Mapping 1507

Von ITOM-Transparenz verwendete Erkennungsmuster 1949

ITOM Content Service 2504

Tag-Governance 2513

Cloud Operations Workspace 2543

Cloud-Lizenzrechner 2555

ITOM-Transparenz-Referenz 2560

ITOM-Integrität 2901

ITOM-Integrität – Anwendungsfall 2903

Ereignismanagement 2904

Health Log Analytics 3479

Service Reliability Management 3800

Servicelevel-Zielmanagement 3885

Service-Observability 3909

Service Operations-Arbeitsbereich für ITOM 3966

Synthetische Überwachung 4192

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CSDM-Richtlinien auf ITOM-Integrität anwenden 4210
Agent Client Collector 4218
Agent Client Collector Framework 4220
Agent Client Collector-Überwachung 4373
Agent Client Collector Visibility – Inhalt 4731
Agent Client Collector Log Analytics 4766
Agent Client Collector Security Incident Response 4792
Live-CI-Daten mit Agent Client Collector anzeigen 4798
Metrikdaten 4801
Metrikdaten erkunden 4803
Metrikdaten konfigurieren 4826
Wird Optimiert Metrikdaten 4832
Metrikdaten – Referenz 4860
Now Assist für IT Operations Management (ITOM) 4861
Now Assist für IT Operations Management (ITOM) erkunden 4863
Konfigurieren von Now Assist für IT Operations Management (ITOM) 4864
Verwenden von Now Assist für IT Operations Management (ITOM) 4870
Mit agentischen Workflows in Now Assist für IT Operations Management (ITOM) 4877
Now Assist für IT Operations Management (ITOM) – Referenz 4889
Playbook für verbesserte Automatisierung von AIOps-Lernen (LEAP) 4890
Auf Cloud-Umgebungen für ITOM-Produkte zugreifen 4907
Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen 4907
Richten Sie einen Cloud-Service-Account ein 4913

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IT Operations Management

Mit ServiceNow® IT Operations Management erlangen Sie eine bessere Transparenz Ihrer Infrastruktur und Services, können Serviceausfälle verhindern und die operative Agilität Ihres Unternehmens erhöhen.

Mit IT Operations Management mehr sehen und mehr erreichen

Beschleunigen Sie Ihre Cloud-Strategie mit IT Operations Management. Optimieren Sie die Cloud-Nutzung in Ihrem Unternehmen, senken Sie Kosten, automatisieren Sie Anfragen, und helfen Sie bei Genehmigungen und beim Verwalten der Infrastruktur, mit der native Cloud-Umgebungen unterstützt werden.

Hier können Sie die vollständige Infokarte anzeigen oder herunterladen , die eine Übersicht der wichtigsten Funktionen von IT Operations Management bietet.

Transparenz Ihrer Infrastruktur und Services erlangen

Übernehmen Sie mithilfe einer zentralen Lösung das Kommando über Ihre Infrastruktur und Services. Verbessern Sie die Servicequalität, stärken Sie Change-Prozesse, reduzieren Sie Risiken, optimieren Sie Ihre Infrastrukturausgaben, und minimieren Sie Compliance-Probleme mit der Software.

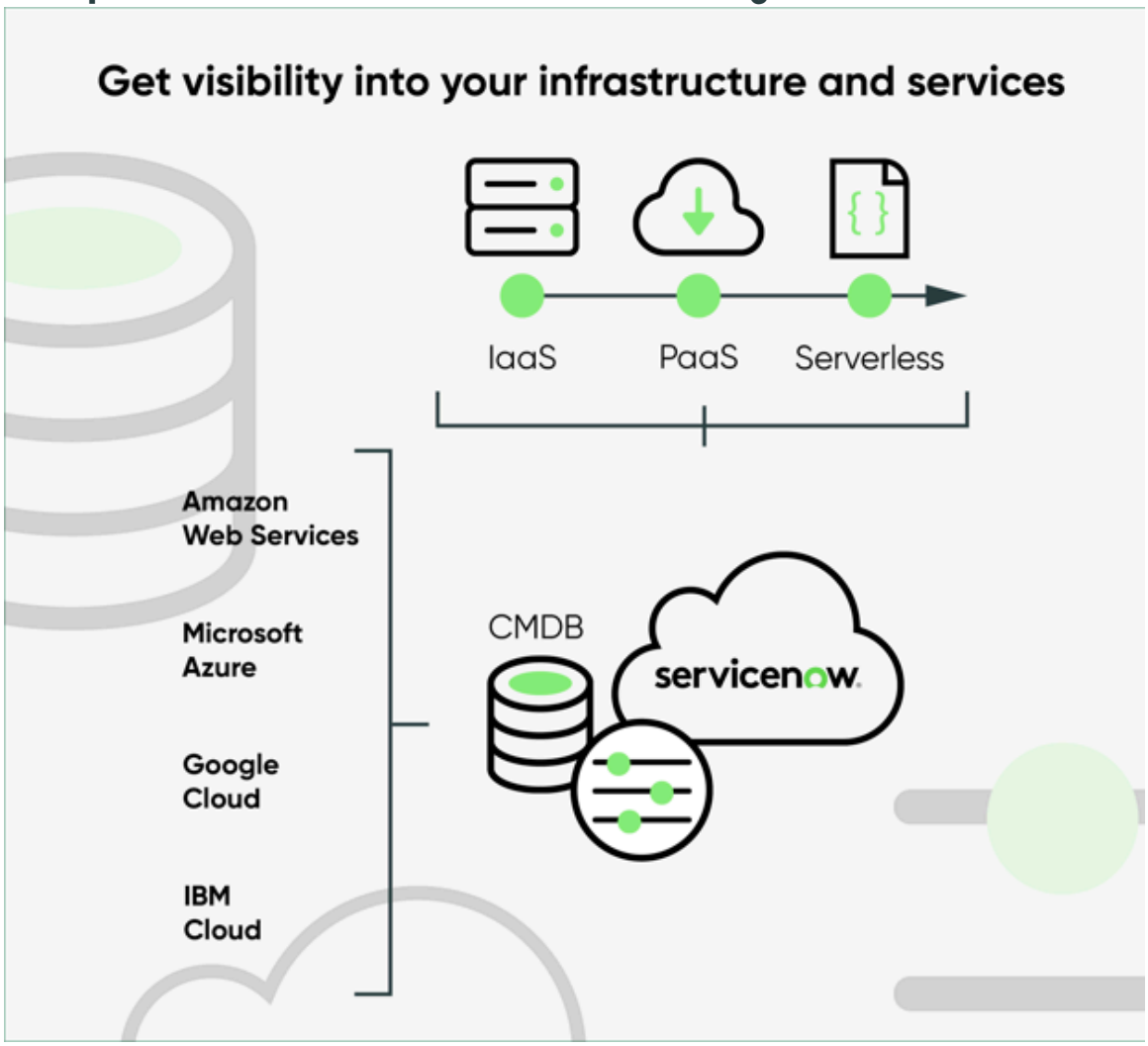
Serviceprobleme wirksam vermeiden und lösen

Entlasten Sie mit AIOps Ihre IT-Mitarbeiter von zeitaufwändigen, fehleranfälligen Aufgaben, und verringern Sie die Anzahl der Serviceausfälle. Beschleunigen Sie die Problemlösung mit relevanten und kontextbezogenen Change-, Problem- und Incident-Daten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

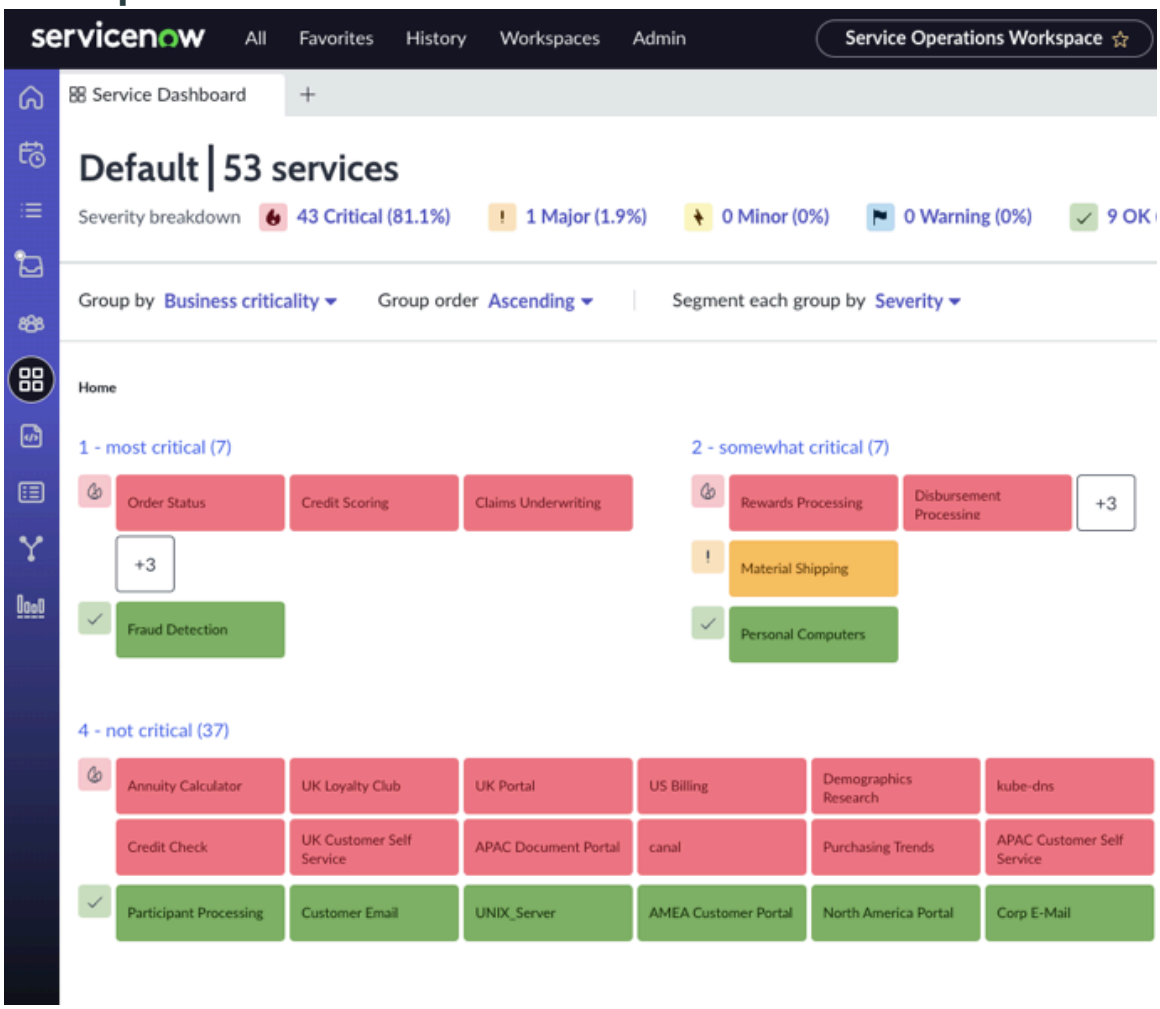
Transparenz Ihrer Infrastruktur und Services erlangen



Sie können sofort die Auswirkungen von Infrastrukturproblemen und Changes auf den Service sehen, die Ursachenanalyse vereinfachen und die durchschnittliche Zeit bis zur Reparatur (MTTR) reduzieren. End-to-End-Erkennung und -Servicezuordnung bieten Ihnen eine genaue, aktuelle CMDB-Ansicht der IT-Infrastruktur und -Services. Der resultierende vollständige und zuverlässige Datensatz wird von anderen ServiceNow-Anwendungen wie ITOM-Integrität, ITOM-Optimierung und Software Asset Management verwendet. Auf diese Weise verbessern Sie die Servicequalität, stärken Change-Prozesse, reduzieren Risiken, optimieren Infrastrukturausgaben und minimieren Compliance-Probleme mit der Software. Weitere Informationen finden Sie unter ITOM-Transparenz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serviceprobleme wirksam vermeiden und lösen



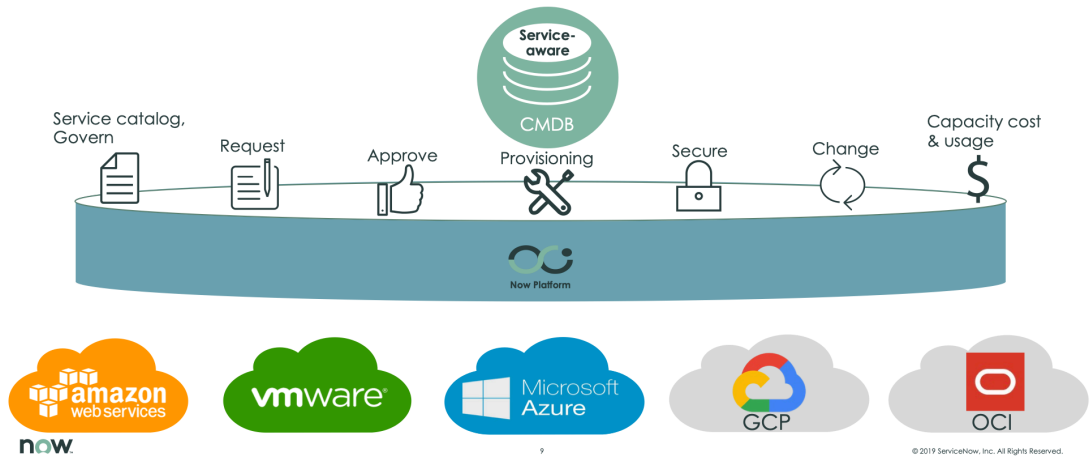
ITOM-Integrität nutzt die Möglichkeiten von AIOps, um Events in verwertbare Warnungen zu verwandeln. Erkennen Sie Serviceprobleme präzise, und identifizieren und beheben Sie die Ursachen im Handumdrehen. Im Gegensatz zu veralteten Event Management-Systemen, die statisch und regelbasiert sind, wendet ITOM-Integrität maschinelles Lernen und fortgeschrittene Analysen an, um Events zu korrelieren und sich automatisch an die sich schnell entwickelnden virtualisierten Umgebungen und Cloud-Umgebungen anzupassen. Weitere Informationen finden Sie unter ITOM Health .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Strategie beschleunigen und Kosten senken

Consistent cloud operating model on single platform



Mit ITOM-Optimierung können Sie den Lebenszyklus Ihrer Cloud-Ressourcen verwalten, von der Discovery über die Bereitstellung neuer Ressourcen, die Bearbeitung von täglichen Changes und Wartungen bis zur Aufhebung der Bereitstellung. Alle diese Funktionen basieren auf ServiceNow Gesteuerte Workflows, die Funktionen wie Change, Audit, Sicherheit und Genehmigung bieten.

Unabhängig davon, ob es sich um eine Cloud-Migrationsbewertung oder eine Konfigurationsprüfung von Cloud-Ressourcen handelt, bietet ITOM Governance Workflows, um den Prozess zu aktivieren und gleichzeitig Cloud-Tags und ungültige Konfigurationen zu korrigieren. Kombination der Stärken agiler und innovativer Fähigkeiten in der Cloud mit ITOM und etablierten ServiceNow Framework stellt einen erfolgreichen Übergang sicher.

IT Operations Management Produktlizenzierung

Für die ServiceNow AI Platform® wird eine Lizenzierungsmethode verwendet, bei der Ihrer Organisation die Nutzung folgender IT Operations Management-Produkte in Rechnung gestellt wird: ServiceNow® ITOM-Transparenz, ServiceNow® ITOM Discovery, ServiceNow® ITOM-Integrität, ServiceNow® Health Log Analytics, ServiceNow® ITOM-Optimierung und ServiceNow® ITOM Cloud Accelerate.

Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Erste Schritte

- Arbeiten Sie mit einem Implementierungsspezialisten zusammen, um Ihre gewünschten Geschäftsergebnisse zu erzielen. Weitere Informationen hierzu finden Sie im Customer Success Center .
- Wählen Sie im das Training aus, das für Sie am besten geeignet ist ServiceNow University Center .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehr erfahren

- Was ist AIOps?
- Was ist eine Configuration Management Database (CMDB)?
- Was ist IT Operations (ITOps)?
- Was ist ein Network Operations Center (NOC)?
- Was ist ein Common Service Data Model (CSDM)?
- Was ist Cloud-Computing?
- Was ist Cloud Orchestration?
- Was ist IT Operations Management (ITOM)?
- Was ist Netzwerk-Discovery?
- Was ist Erkennbarkeit?

Anwendungen und Funktionen

- ITOM-Lizenzierung und -Abonnements
- ITOM Cloud Accelerate
- ITOM-Transparenz
- Sichtbarkeit: Discovery
- Sichtbarkeit: Service-Mapping
- ITOM-Integrität
- Integrität: Ereignismanagement
- Integrität: Analytics Für Integritätsprotokolle
- Integrität: Agent Client Collector
- ITOM-Optimierung
- Optimierung: Cloud Provisioning and Governance

ITOM/OT SU-Lizenzierung Und -Abonnements

ServiceNow® IT Operations Management Bei der (ITOM)-Lizenzierung wird die Nutzung von ITOM-Abonnements basierend auf Abonnementeinheiten berechnet und angezeigt.

Einheitliche Statistiken für alle ITOM-Produkte

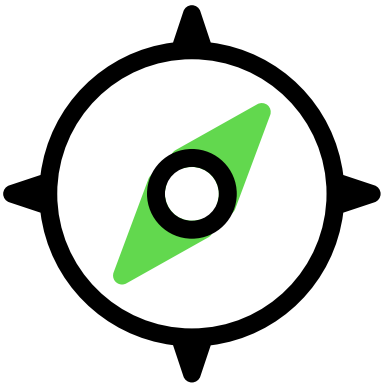
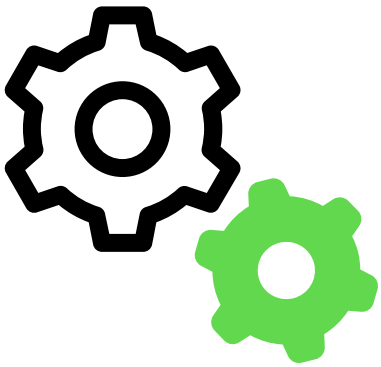
Verwenden Sie ITOM Lizenzierungsmodul zum Anzeigen von Abonnementinformationen für alle ITOM Produkte: ServiceNow® ITOM-Transparenz, ServiceNow® ITOM Discovery, ServiceNow® ITOM-Integrität, ServiceNow® Health Log Analytics, ServiceNow® ITOM-Optimierung, ServiceNow® ITOM Cloud Accelerate, ServiceNow® Digitale Endanwender-Experience(DEX), und ServiceNow® Service-Observability.

Die ServiceNow Die Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbrauchsniveau

Zeigen Sie einfach an, wie viele Abonnements für IT Operations Management-Anwendungen Ihr Unternehmen erworben und verbraucht hat.

Untersuchen	Installieren	Referenzen
		
Erkunden ITOM/ OT SU-Lizenzierung Und -Abonnements	Erfahren Sie, wie Sie installieren ITOM/ OT SU-Lizenzierung	Erfahren Sie mehr über geplante Aufgaben, Tabellen, Abonnementformular und Dashboard

Um mehr über zu erfahren Operational Technology-Management(OTM) Lizenzierung und Abonnements, siehe Abonnementformular für die OTM-Produkte .

ITOM/OT SU-Lizenzierung erkunden

Erfahren Sie mehr über ServiceNow® ITOM/OT SU-Lizenzierung, Der andere ITOM Abonnements, die darin enthalten sind, und ihr Vorteil.

ITOM/OT SU-Lizenzierung – Übersicht

Die ITOM/OT SU-Lizenzierung Die Anwendung berechnet und zeigt an, wie viele Abonnements für IT Operations Management(ITOM) Anwendungen, die Ihre Organisation kauft und verbraucht. Abonnements für Folgendes ITOM Anwendungen sind verfügbar: ServiceNow® ITOM-Transparenz, ServiceNow® ITOM Discovery, ServiceNow® ITOM-Integrität, ServiceNow® Health Log Analytics, ServiceNow® ITOM-Optimierung, ServiceNow® ITOM Cloud Accelerate, ServiceNow® Digitale Endanwender-Experience(DEX), und ServiceNow® Service Observability. Sie können Abonnements für jeden erwerben ITOM Anwendung separat (a la carte) oder zusammen (in einem Paket).

ITOM/OT SU-Lizenzierung – Vorteile

Vorteil	Funktion	Anwender
Die Nutzung von wird angezeigt ITOM Anwendungen, um fundierte Entscheidungen über zu treffen ITOM Abonnements. Sie können damit Ihre Erwartung des Lizenzverbrauchs bestätigen. Wenn die Messung höher als geplant ist, ändern Sie	Ressourcennutzung gegenüber den zugeteilten Abonnementeinheiten überprüfen	Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteil	Funktion	Anwender
entweder Ihre Nutzung von ITOM oder erhöhen Sie Ihr Abonnement.		
Die Analyse von Ressourcennutzung und -Status im Vergleich zu Ihren erworbenen Abonnements wird durch Dashboard-Berichte erleichtert. Diese Berichte zeigen sowohl die tägliche Nutzungsanzahl als auch den durchschnittlichen Verbrauch von Abonnementeinheiten über einen Zeitraum von 90 Tagen visuell an und zeigen Ihnen, welche Ressourcen für jede ITOM-Anwendung gezählt werden.	ITOM/OT SU-Lizenzierung-Dashboard	Administrator

Abonnements für IT Operations Management

Für die ServiceNow AI Platform® wird eine Lizenzierungsmethode verwendet, bei der Ihrer Organisation die Nutzung folgender IT Operations Management-Produkte in Rechnung gestellt wird: ServiceNow® ITOM-Transparenz, ServiceNow® ITOM Discovery, ServiceNow® ITOM-Integrität, ServiceNow® Health Log Analytics, ServiceNow® ITOM-Optimierung und ServiceNow® ITOM Cloud Accelerate.

Für Lizenzierungszwecke werden lizenzierbare Ressourcen CI-Kategorien zugewiesen. Die Lizenznutzung wird mithilfe von Abonnementeinheiten gemessen, die je nach CI-Kategorie der Ressource eine unterschiedliche Anzahl von Ressourcen abdecken können. Der Kundenvertrag für Ihr Unternehmen bestimmt die CI-Kategorien aus den verfügbaren Optionen und auch die Verhältnisse der CI-Zuweisung für die Abonnementeinheiten in jeder CI-Kategorie. Informationen aus dem Kundenvertrag werden mit der ServiceNow Platform synchronisiert. Die neueste Version von ServiceNow® ITOM/OT SU-Lizenzierung unterstützt die folgenden CI-Kategorien:

- Container
- PaaS
- FaaS
- Server
- Nicht gelöstes Überwachungsobjekt
- Nicht klassifizierte Kategorie
- Endanwendergeräte
- IoT
- Prem-Geräte des Kunden

Sie haben die Möglichkeit, Abonnements für einzelne ITOM-Produkte einzeln (à la carte) oder als Teil eines Pakets mit mehreren Produkten zu erwerben. Sie können auch beides erwerben – ein Paketabonnement, das die meisten erforderlichen Anwendungen abdeckt, und ein Abonnement à la carte für Anwendungen, die mehr Abonnementeinheiten verbrauchen. Weitere Informationen finden Sie unter ITOM/OT SU-Lizenzierung Abonnementtypen.

ServiceNow®-Gebühren für die folgenden IT Operations Management-Produkte:

ITOM-Transparenz

Das ProduktServiceNow® ITOM-Transparenz besteht aus ServiceNow® Discovery, ServiceNow® Service-Mapping, Zertifikatsbestand-Management, Service Graph Connectors, CMDB mit mehreren Quellen sowie Firewall-Audits und Reporting. Discovery und Service-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mapping vermitteln Ihnen zusammen eine einheitliche, verbundene Ansicht Ihres gesamten IT-Netzwerks und der von ihm unterstützten Services.

Darüber hinaus wird die CMDB mittels Service Graph-Connectors gefüllt, indem Daten aus Überwachungs- und Managementsystemen von Drittanbietern einbezogen werden. Mit CMDB mit mehreren Quellen können Sie nachverfolgen, welche verschiedenen Erkennungsquellen auf CI-Attributebene die CMDB enthält. Verwenden Sie Zertifikatsbestand-Management, um Serviceausfälle aufgrund abgelaufener TLS-Zertifikate zu vermeiden. Firewall-Audits und Reporting hilft Ihnen, Ihre Sicherheitsrichtlinien für die Firewall zu erkennen und zu verwalten, um das Sicherheitsbewusstsein für Firewall-Audits zu erhöhen.

Zu Lizenzierungszwecken gibt ITOM-Transparenz die Anzahl der erkannten CIs an, sowohl bei einer Horizontal- als auch bei einer Top Down-Discovery. Außerdem werden CIs gemeldet, mit denen die Service Graph-Connectors die CMDB füllen.

Sie können auch die eingeschränkte Tag-Governance-Funktionalität im Rahmen des ITOM-Transparenz-Abonnements verwenden. Sie können lokale Ressourcen identifizieren, die inkonsistent sind und nicht den Tag-Richtlinien Ihrer Organisation entsprechen.

ITOM Discovery

ServiceNow® ITOM Discovery ist ein alternatives Einstiegspaket, mit dem Kunden eine einwandfreie Datenplattform aufbauen können. Mit diesem Paket wird die Lizenznutzung für die Discovery-Funktion und für Servicediagramm-Connector ermittelt. Discovery ist eine Teilmenge von ITOM-Transparenz, die auch auf Abonnementeinheiten basiert. ITOM Discovery umfasst die folgenden grundlegenden Funktionen: ServiceNow® Discovery, Service Graph Connectors und CMDB mit mehreren Quellen. ServiceNow® Discovery sucht nach Anwendungen und Geräten in Ihrem Netzwerk und aktualisiert dann die CMDB. Service Graph-Connectors ergänzen die Auffüllung der CMDB, während die CMDB mit mehreren Quellen den vollständigen Verlauf der Erkennungsquellen und vorgeschlagenen Werte beibehält.

ITOM Discovery gibt die Anzahl der CIs an, die von ServiceNow® Discovery gefunden und von Service Graph-Connectors importiert wurden.

ITOM-Integrität

Das Produkt ServiceNow® ITOM-Integrität umfasst die Anwendungen ServiceNow® Ereignismanagement und ServiceNow® Metrikdaten, die Ihnen helfen, die Integrität von Services in Ihrer Organisation nachzuverfolgen und aufrechtzuerhalten.

ITOM-Integrität gibt die Anzahl der CIs an, für die Warnungen, Events und Metrikdaten erfasst werden. ITOM-Integrität meldet die CI-Anzahl für alle CI-Kategorien.

Health Log Analytics

Die Health Log Analytics-CI-Anzahl basiert auf Protokolldaten, die von lizenzierbaren Ressourcentypen empfangen wurden. Der Verbrauch wird in berücksichtigt ITOM-Integrität Sowie in Health Log Analytics. Aus diesem Grund benötigen Sie das ITOM-Integrität-Abonnement zusätzlich zum Health Log Analytics-Abonnement.

ITOM Cloud Accelerate

Die ITOM Cloud Accelerate Das Produkt besteht aus den folgenden Workflow-Anwendungen: Tag-Governance, Bewertung der Cloud-Migration, Governance für Cloud-Konfigurationen, Und Bibliothek von Cloud-Aktionen. In Tag-Governance können Sie CI-Tags in der Cloud-Umgebung aktualisieren, zusätzlich zur Aktualisierung in der CMDB.

Für Lizenzierungszwecke gibt die ITOM Cloud Accelerate-Lizenz die CI-Anzahl für CIs an, die von Bewertung der Cloud-Migration, Governance für Cloud-Konfigurationen oder Bibliothek

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von Cloud-Aktionen verwaltet und überwacht werden. Wenn von unterschiedlichen ITOM Cloud Accelerate-Funktionen dieselben CIs als ihre Ressourcen gemeldet werden, wird die CI-Anzahl so manipuliert, dass das Duplikat entfernt wird.

ITOM-Optimierung

Die ServiceNow® ITOM-Optimierung-Anwendung bietet Automatisierung für die Cloud-Workflows, die während ihres gesamten Lebenszyklus zur Verwaltung der Cloud-Ressourcen verwendet werden. Sie ermöglicht eine zertifizierte und unternehmenskonforme Cloud-Bereitstellung, Kostentransparenz und andere Cloud-Managementprozesse.

Service-Observability

Die ITOM Service Observability-Funktion erstellt umsetzbare Dashboards und Erkennbarkeitsregisterkarten, die Daten aus vorhandenen Überwachungstools von Drittanbietern zentralisieren. Sie ermöglicht es Ihnen, die Leistung geschäftskritischer Services nachzuverfolgen, eine schnellere Ursachenanalyse zu ermöglichen und die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR) zu verkürzen. Telemetrieinblicke in Anwendungen und Plattformen aus mehreren Erkennbarkeitstools werden zu einem zentralen Workflow kombiniert.

Zugehörige Informationen

Abonnement-Management

Datensammlung und -Zusammenfassung für den Lizenzierungsprozess

ITOM/OT SU-Lizenzierung Anwendung zählt CIs für ITOM Anwendungen und verwendet eine tägliche durchschnittliche Anzahl für die letzten 90 Tage, um Lizenzstatistiken für erworbene Abonnementeinheiten zu erstellen.

ServiceNow Gebühren für verschiedene ITOM Anwendungen, einschließlich ITOM-Transparenz, ITOM Discovery, ITOM-Integrität, Health Log Analytics, ITOM Cloud Accelerate, Und ITOM-Optimierung. Für spezifische Informationen zu den von abgedeckten Produkten und Funktionen ITOM Abonnements, siehe Abonnements für IT Operations Management.

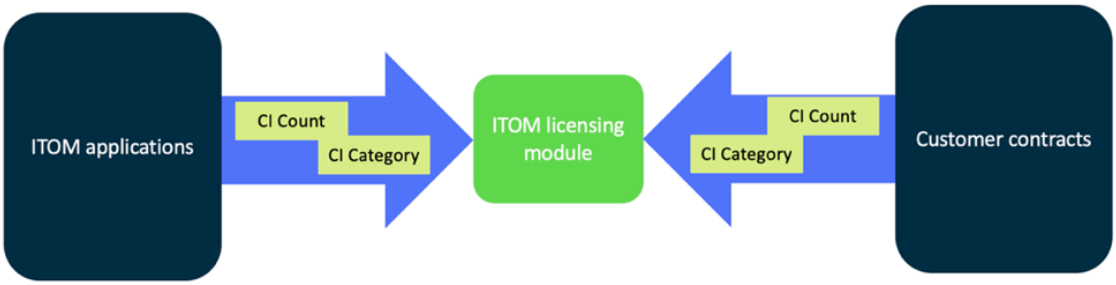
Das Sammeln und Zusammenfassen von Informationen zu Lizenzierungszwecken umfasst die folgenden Schritte:

1. Die ITOM Der Lizenzierungsmechanismus zählt die von jedem verwalteten Konfigurationselemente (Configuration Items, CIs) ITOM Produkt täglich und kategorisiert sie in lizenzierbare CI-Kategorien. Weitere Informationen finden Sie unter KB0748149: ITOM Subscription Unit license calculation logic (Lizenzberechnungslogik für ITOM-Abonnementeinheiten).
2. Wenn dieselben CIs von verschiedenen Funktionen innerhalb desselben verwaltet werden ITOM Produkte wird die CI-Anzahl angepasst, um die Duplizierung zu vermeiden. Beispiel: Beides Discovery Und Service-Mapping Erkennen Sie dieselben CIs. Diese CIs werden nur einmal in der CI-Anzahl angezeigt.
3. Das Lizenzierungsmodul fasst die CI-Anzahlen aus zusammen ITOM Anwendungen zur Bestimmung der durchschnittlichen täglichen CI-Anzahl für die letzten 90 Tage.
4. Das Lizenzierungsmodul vergleicht dann die täglichen durchschnittlichen CI-Anzahlen der letzten 90 Tage ab ITOM Anwendungen mit den Lizenzierungsinformationen im Kundenvertrag zum Generieren von Lizenzstatistiken.

Infolgedessen können Sie Statistiken darüber anzeigen, wie Ihr Unternehmen erworbene Abonnementeinheiten verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Anwendungslizenzflow



ITOM/OT SU-Lizenzierung Abonnementtypen

Erwerben Sie Lizenzierungsabonnements für ITOM Produkte einzeln (a la carte), bündeln mehrere Produkte, oder entscheiden Sie sich für Einzel- und gebündelte Abonnements.

Sie haben die Möglichkeit, Abonnements für einzelne ITOM-Produkte einzeln (à la carte) oder als Teil eines Pakets mit mehreren Produkten zu erwerben. Sie können auch beides erwerben – ein Paketabonnement, das die meisten erforderlichen Anwendungen abdeckt, und ein Abonnement à la carte für Anwendungen, die mehr Abonnementeinheiten verbrauchen.

Wenn Ihre Organisation mehr Abonnements als geschätzt verwendet, haben Sie die Möglichkeit, nach Bedarf zusätzliche Abonnementeinheiten zu kaufen. Diese Einheiten können entweder für ein Paket oder für einzelne Produkte (a la carte) erworben werden. Wenn Ihre Organisation jedoch verwendet ITOM Anwendungen in einem Paket auf verschiedenen Ebenen können Sie beide kaufen – ein Paket-Abonnement, das die meisten erforderlichen Anwendungen abdeckt, und ein A-la-Carte-Abonnement für diejenigen, die mehr Abonnementeinheiten benötigen.

Hinweis: ITOM-Pakete bieten zudem Berechtigungen für IntegrationHub zum Auswählen von Spokes und Protokollen. ITOM Cloud Accelerate erfordert die zusätzliche Berechtigung für das IntegrationHub Enterprise-Paket.

ITOM/OT SU-Lizenzierung Paket-Abonnement

Sie können Abonnements für mehrere erwerben ITOM Produkte zusammen als Teil eines Pakets.

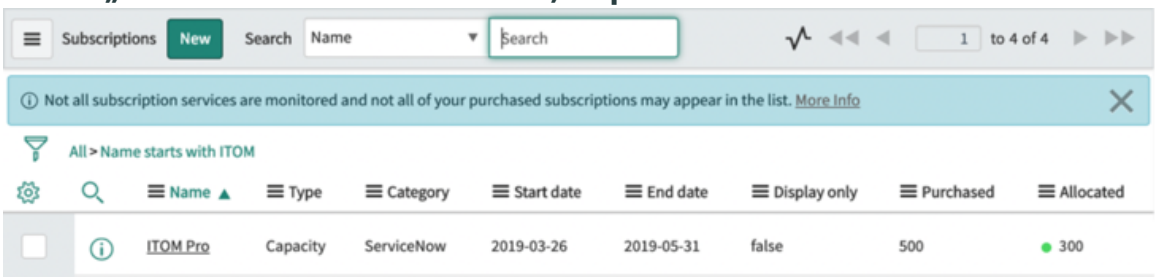
Die ITOM/OT SU-Lizenzierung Die Anwendung berechnet und zeigt den Abonnementverbrauch für Paketabonnements an. Wenn Ihre Organisation Abonnements in einem Paket kauft, erhalten Sie die gleiche Anzahl von Abonnementeinheiten für alle ITOM Vom Paket abgedeckte Anwendungen. Sie können Paketabonnements nicht für andere Anwendungen verwenden, auch wenn diese anderen Anwendungen Teil desselben Pakets sind. Die Verbrauchsstufe des Bündels wird durch die höchste Anzahl der Verbrauchsmengen durch eines der Produkte im Paket definiert.

Wenn Sie Abonnements in einem Paket erwerben, erhalten Sie dieselbe Anzahl von Abonnementeinheiten für alle ITOM-Anwendungen, die vom Paket abgedeckt werden. Wenn Sie beispielsweise ein Paket von 500 Einheiten für ITOM-Transparenz und ITOM-Integrität kaufen, erhält Ihr Unternehmen 500 Einheiten für jede Anwendung.

Hinweis: Sie können jeweils nur ein Paket kaufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

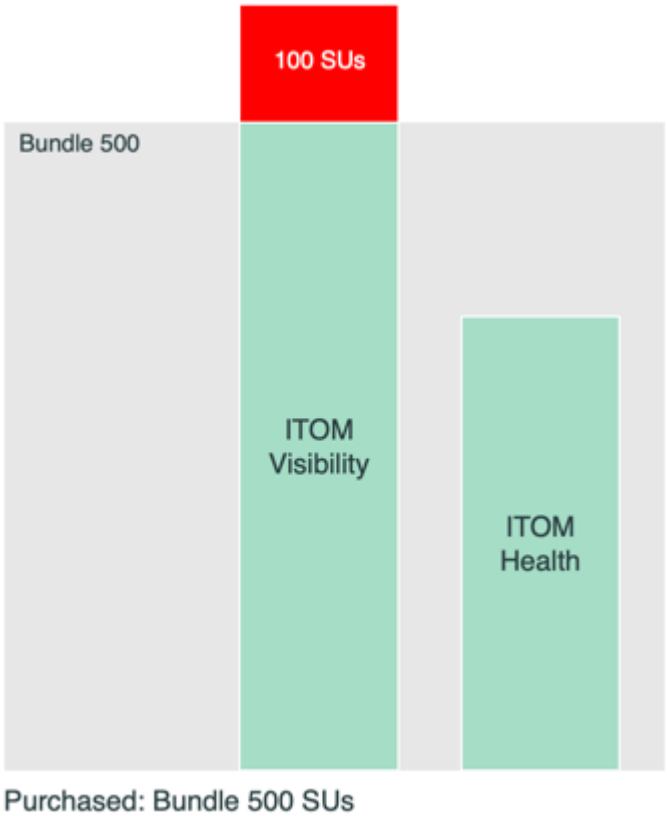
Fenster „Abonnements“ mit Abonnements, die paketweise erworben wurden



Paketabonnements sind spezifisch für bestimmte Anwendungen. Sie können Paketabonnements nicht für andere Anwendungen verwenden, auch wenn diese Anwendungen Teil desselben Pakets sind. Wenn Sie beispielsweise ein Paket von 500 Einheiten für ITOM-Transparenz und ITOM-Integrität erworben haben und alle 500 ITOM-Transparenz-Abonnementeinheiten verwendet haben, können Sie die verbleibenden ITOM-Integrität-Abonnementeinheiten nicht für ITOM-Transparenz verwenden.

Das Verbrauchsniveau des Pakets wird durch die höchste Nutzung der im Paket enthaltenen Produkte bestimmt.

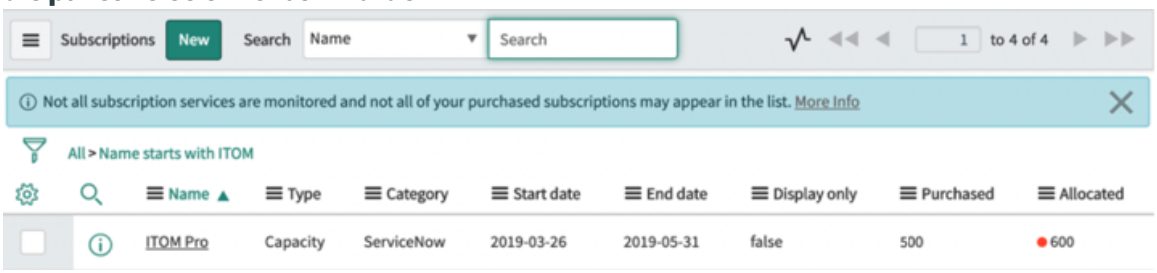
Automatische Anpassung des Pakets an den tatsächlichen Verbrauch



Das Fenster „Abonnements“ zeigt die tatsächliche Anzahl der verbrauchten Abonnements unter **Zugewiesen** an. Der rote Farbcode zeigt an, dass das Paket überzogen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fenster „Abonnements“, in dem die Überziehung an Abonnements dargestellt ist, die paketweise erworben wurden



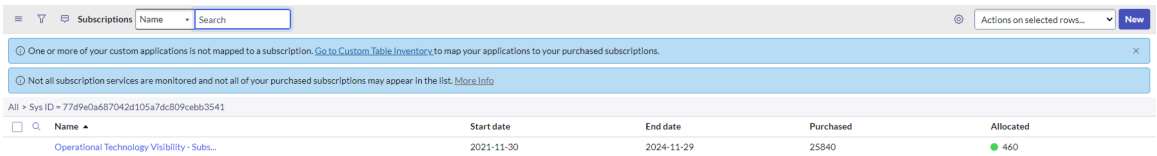
ITOM/OT SU-Lizenzierung Einzel-Abonnement (a la carte)

Sie können Abonnements für Einzelpersonen erwerben ITOM Anwendungen (Ala-Carte).

Die ITOM/OT SU-Lizenzierung Die Anwendung berechnet und zeigt den Abonnementverbrauch für an ITOM Anwendungen, die einzeln gekauft wurden (Ala-Carte). Wenn Ihr Unternehmen die Anzahl der Abonnementeinheiten überschreitet, wird im Fenster „Abonnements“ angezeigt, dass das relevante À-la-carte-Abonnement überzogen ist. Sie können nicht verbrauchte Abonnements nicht für überzogene Abonnements einer anderen Anwendung verwenden.

Im Fenster „Abonnements“ werden Informationen zu den erworbenen und zugeteilten Abonnements für angezeigt ITOM Anwendungen.

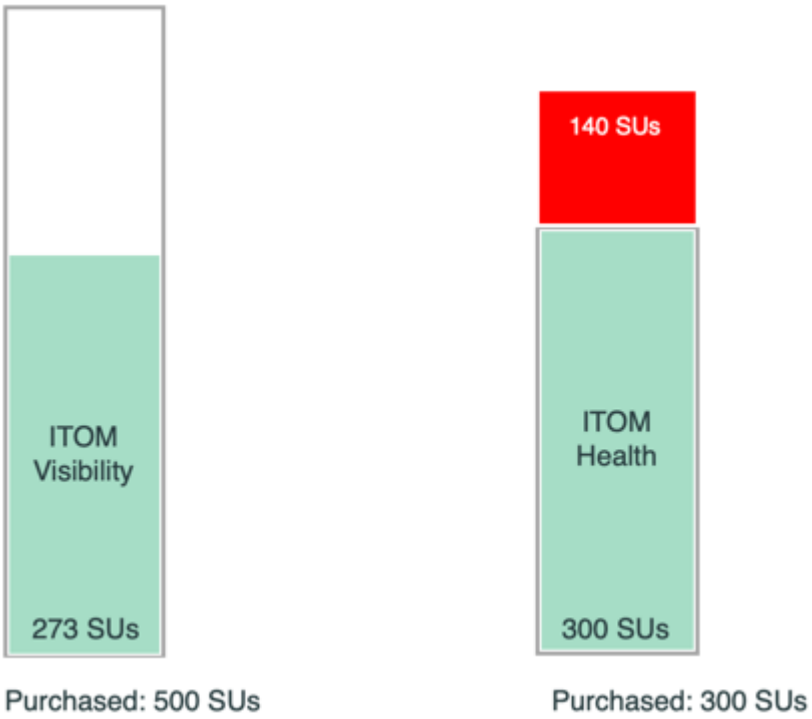
Fenster „Abonnements“, in dem à la carte erworbene Abonnements angezeigt werden



Wenn Ihre Organisation die Anzahl der erworbenen Abonnements für überschreitet ITOM Anwendung können Sie die verbleibenden Abonnements nicht für eine andere Anwendung verwenden.

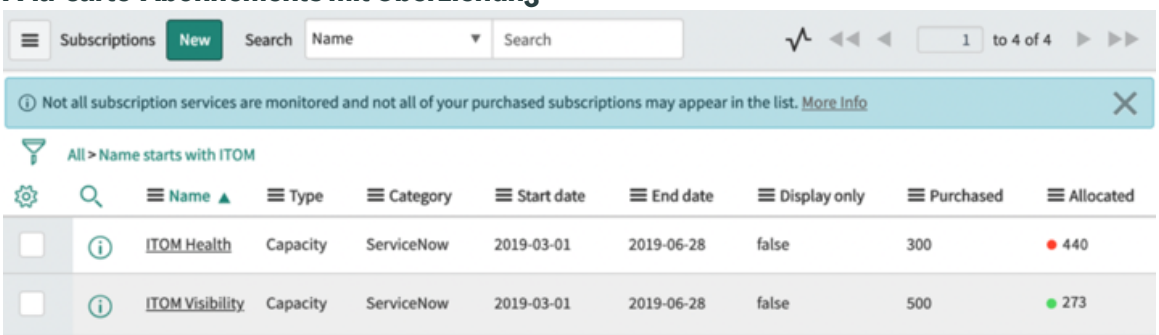
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechnung der à-la-carte-Abonnements



Wenn Ihre Organisation die Gesamtzahl der erworbenen Abonnementeinheiten überschreitet, wird im Fenster „Abonnements“ das relevante A-la-carte-Abonnement als überzogen angezeigt. In der folgenden Abbildung ITOM-Integrität Mehr Abonnements verbraucht als der dafür gekaufte Betrag.

À-la-carte-Abonnements mit Überziehung



ITOM/OT SU-Lizenzierung Paket- und Einzelabonnement (A A-Carte)

Sie können Abonnements für Einzelpersonen erwerben ITOM Anwendungen (a la carte) oder als Paket, das mehrere abdeckt ITOM Anwendungen.

Die ITOM/OT SU-Lizenzierung Die Anwendung berechnet und zeigt die Abonnementnutzung für an ITOM Produkte. Es wird angezeigt ITOM Produkte einzeln oder als Teil eines Pakets, basierend auf Ihrem Abonnement. In Fällen, in denen Ihre Organisation gekauft hat ITOM Abonnements sowohl als Paket als auch einzeln (a la carte) zieht das Lizenzierungsmodul die verbrauchten Abonnements zuerst vom Paket ab, bevor es von den einzeln gekauften Abonnements abgezogen wird.

Wenn Ihre Organisation die zugewiesene Anzahl der Abonnementeinheiten überschreitet, werden im Fenster „Abonnements“ die entsprechenden Abonnements als überzogen angezeigt. Wenn die kombinierte Anzahl der Abonnements aus den Optionen „Paket“ und „A la carte“ die Zuteilung überschreitet, identifiziert das Lizenzierungsmodul den Überschuss aus dem A la carte-Abonnement. Wenn außerdem die Gesamtzahl der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

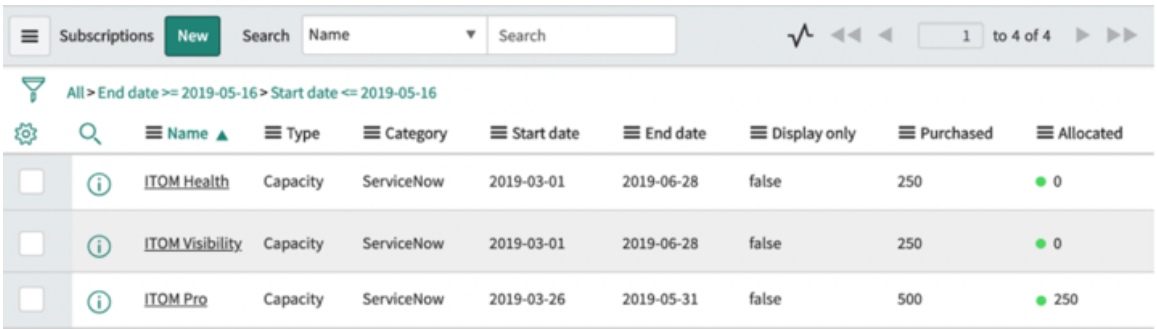
Abonnements für eine ausschließlich vom Paket abgedeckte Anwendung die Zuteilung übersteigt, wird das Paket im Fenster „Abonnements“ als überzogen angezeigt, ohne die einzelnen Anwendungen separat aufzulisten.

Abzugsprozess für Abonnements: Bündelnutzung und A-la-Carte-Szenario

Wenn Sie gekauft haben ITOM Abonnements als Paket und erworbene A-la-Carte-Abonnements für eine im Paket enthaltene Anwendung zieht das Lizenzierungsmodul die verbrauchten Abonnements vom Paket ab, bevor es von den separat erworbenen Abonnements abzieht.

Im folgenden Beispiel hat eine Organisation alle Abonnements verwendet, die vom zugewiesen wurden ITOM Pro-Paket für ITOM-Integrität. Anschließend wird das Lizenzierungsmodul von den A-la-Carte-Abonnements für abgezogen ITOM-Integrität.

Abonnementverbrauch nach Paketen



Name ▲	Type	Category	Start date	End date	Display only	Purchased	Allocated
ITOM Health	Capacity	ServiceNow	2019-03-01	2019-06-28	false	250	0
ITOM Visibility	Capacity	ServiceNow	2019-03-01	2019-06-28	false	250	0
ITOM Pro	Capacity	ServiceNow	2019-03-26	2019-05-31	false	500	250

Abonnementanzeige: Anwendung abgedeckt durch Paket- und A-la-Carte-Abonnements

Wenn Ihre Organisation die Gesamtzahl der Abonnements sowohl im Paket als auch im A-la-Carte-Abonnement überschreitet, betrachtet das Lizenzierungsmodul dies als überzogen für das A-la-Carte-Abonnement. Wenn Ihre Organisation jedoch die Abonnements speziell für eine Anwendung überschreitet, die ausschließlich vom Paket abgedeckt ist, gilt dies für das Paket als überzogen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Lizenzierungsmodul berechnet Paket- und A-la-Carte-Abonnements für dasselbe ITOM Anwendungen

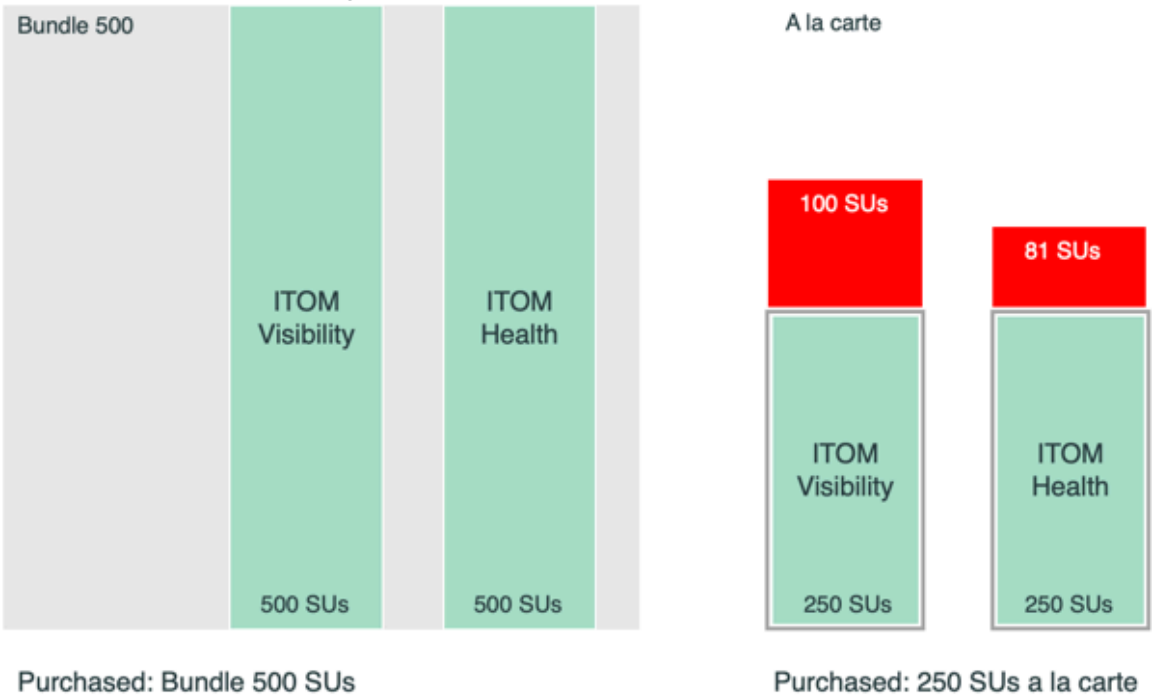
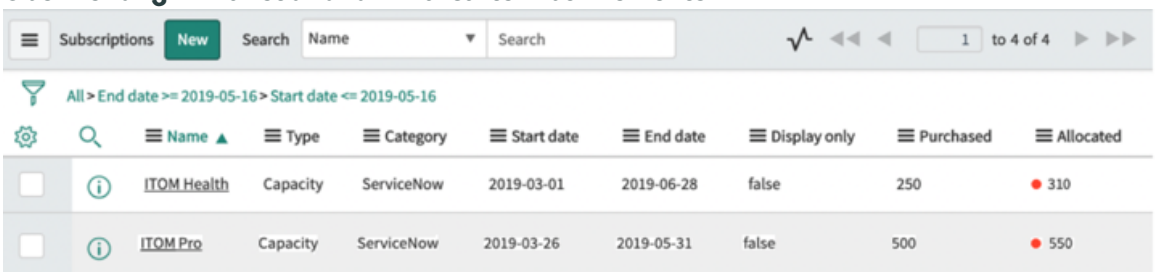


Abbildung der Abonnementberechnung: Bündel- und A-la-Carte-Zuteilung

Das Diagramm veranschaulicht, wie das Lizenzierungsmodul Abonnements über Paket- und A-la-carte-Methoden für bestimmte vom Paket abgedeckte Anwendungen berechnet.

Überziehung im Paket und für À-la-carte-Abonnements



In diesem Szenario zeigt das Fenster „Abonnements“ die A-la-Carte-Abonnements für diese Anwendung als überzogen an. Wenn Ihre Organisation die Gesamtzahl der Abonnements für eine Anwendung überschreitet, die ausschließlich vom Paket abgedeckt wird, wird das Paket im Fenster „Abonnements“ als überzogen angezeigt.

In der angegebenen Abbildung ITOM-Integrität Verbraucht 810 Abonnements, übertraf die vom Paket (500) und a la carte (250) bereitgestellten Abonnements. Daher wird im Fenster „Abonnements“ angezeigt ITOM-Integrität A-la-Carte-Abonnement als überzogen.

Für ITOM-Transparenz, Die 550 Abonnements verbraucht haben, und ohne erworbene A-la-Carte-Abonnements ITOM Pro-Paket-Abdeckung ITOM-Transparenz Wird als überzeichnet angezeigt.

Abonnements für Operational Technology-Management

Die ServiceNow Plattformverwendungen Operational Technology-Management(OTM) Zum Verwalten von Lizenzen für die Fertigungsindustrie. OTM enthält die Lizenzen, die in IT Operations Management enthalten sind, sowie spezifische Lizenzen für OTM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen OTM Lizenzen auf die gleiche Weise wie IT Operations Management Lizenzen. Die ServiceNow Instanz gibt OTM-Lizenztypen auf der an **Metadaten der ITOM-Lizenzierungskategorie** (**OTM-Lizenz** > **Lizenzen nach CI-Typen**) Seite, wobei **SKU-Typ** Spalte enthält einen Wert von **otm** . Standardmäßig ist der Lizenzfilter auf **SKU-Typ enthält otm** festgelegt.

Die gleichen Lizenzoptionen, die für IT Operations Management verfügbar sind, sind auch für OTM unter dem Menüpunkt **OTM License** (OTM-Lizenz) in einer ServiceNow-Instanz verfügbar.

Weitere Informationen zu Abonnements für OTM finden Sie unter Abonnements für IT Operations Management.

ITOM/OT SU-Lizenzierung konfigurieren

Erhalten Sie die Fähigkeit, effizient zu verwalten und zu optimieren ITOM Abonnements innerhalb von ServiceNow Framework für optimierte Vorgänge.

Konfiguration – Übersicht

Beginnen Sie mit der Installation ServiceNow® ITOM/OT SU-Lizenzierung, Legt die Grundlage für ein umfassendes Verständnis der Verwaltung fest ITOM Abonnements.

ServiceNow® ITOM/OT SU-Lizenzierung aktualisieren

Aktualisieren Sie ServiceNow® ITOM/OT SU-Lizenzierung[com.snc.itom.license] Anwendung, um sicherzustellen, dass Sie die neueste Lizenzierungsfunktion verwenden. Aktualisieren der zugehörigen Anwendungsinstallationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Stellen Sie sicher, dass Sie über einen verfügen ITOM Produkt, das auf Ihrem installiert ist ServiceNow Instanz für ITOM/OT SU-Lizenzierung Anwendung zu Arbeit. Installieren von ITOM/OT SU-Lizenzierung Anwendung ist nicht erforderlich, da das System die Anwendung automatisch zusammen mit installiert ITOM Produkt.
- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie ITOM/OT SU-LIZENZIERUNG Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie erhalten Benachrichtigungen, wenn Aktualisierungen für durchgeführt werden ITOM/OT SU-Lizenzierung Anwendung ist auf verfügbar ServiceNow Store.

Die folgenden Elemente werden mit ITOM/OT SU-Lizenzierung installiert:

- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter Mit ITOM/OT SU-Lizenzierung installierte Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach ServiceNow ITOM/OT SU-Lizenzierung Anwendung (sn_itom_Lizenzierung) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen.
3. In **Updates** Wählen Sie die Registerkarte aus ServiceNow ITOM/OT SU-Lizenzierung Anwendung.
4. Wählen Sie Aus **Fahren Sie mit der Aktualisierung fort** .

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die beim Aktualisieren der Anwendung installiert werden.
5. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
6. Wählen Sie die Version aus, auf die Sie ein Upgrade durchführen möchten, und wählen Sie sie aus **Installieren** .

ITOM/OT SU-Lizenzierung verwenden

Stellen Sie eine optimale Nutzung der Ihrer Organisation sicher ITOM Abonnements durch Analyse der Ressourcennutzung von ITOM Produkte.

Verwenden ITOM/OT SU-LizenzierungÜbersicht

Erkunden Sie, wie Sie Abonnements für anzeigen und nachverfolgen ITOM Anwendungen, die die Ressourcennutzung anhand zugeteilter Abonnementeinheiten analysieren, um eine optimale Nutzung sicherzustellen. Überprüfen Sie die Anzahl der Configuration Items (CIs), die für verwendet werden ITOM Abonnements und identifizieren Sie, welche CI-Typen speziell erfordern ITOM Abonnementeinheiten. Generieren Sie schließlich Listen, die die aktuell zählbaren CIs für jedes zeigen ITOM Anwendung, mit der Sie den Verbrauch von Abonnementeinheiten visualisieren können.

Abonnementstatistiken für ITOM anzeigen

Zeigen Sie an, wie viele Abonnements für IT Operations Management-Anwendungen Ihr Unternehmen erworben und verbraucht hat.

Vorbereitungen

Vergewissern Sie sich, dass Ihre Organisation ITOM-Abonnements erworben hat. Sie können die Informationen im **ITOM-Lizenz**-Modul nicht ohne Abonnements anzeigen.

Vergewissern Sie sich, dass Sie die neueste verfügbare Version der ITOM/OT SU-Lizenzierung von ServiceNow Store installiert haben.

Erforderliche Rolle: Usage_admin

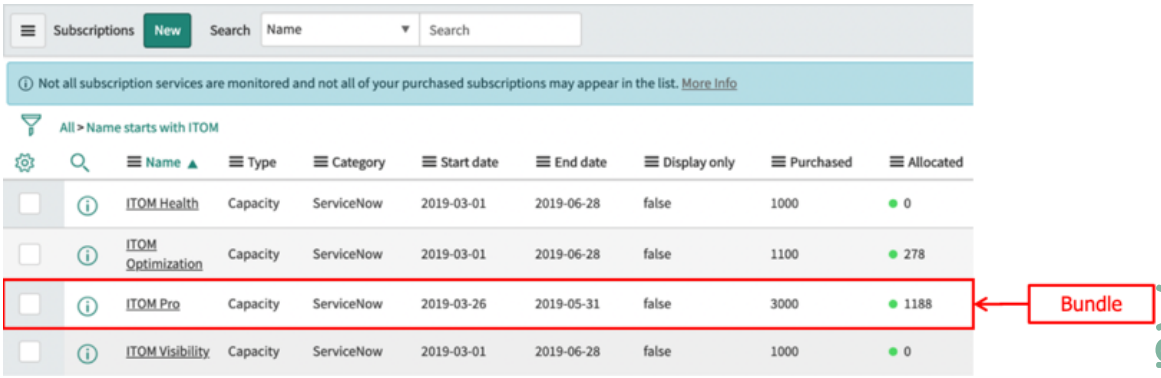
Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie die Zuordnung des Configuration Items (CI) und die Zuordnungsebene, um zu erfahren, wie Ihr Unternehmen IT Operations Management-Abonnements verwendet, und planen Sie den aufkommenden Abonnementbedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Dient zum Anzeigen von Abonnementinformationen für IT Operations Management Abonnements, die a la carte erworben wurden, navigieren Sie in Paketen zu **ITOM-Lizenz** > **Lizenzzusammenfassung**an. Verwenden Sie Abonnementnamen, um zwischen Abonnements, die in Paketen und à la carte erworben wurden, zu unterscheiden.



2. Überprüfen Sie die Informationen im Formular, wie unter Abonnementformular für die ITOM-Produkte beschrieben.

Zugehörige Informationen

KB0748149: ITOM Subscription Unit license calculation logic (Lizenzberechnungslogik für ITOM-Abonnementeinheiten)

Abonnements für IT Operations Management

Ressourcennutzung gegenüber den zugeteilten Abonnementeinheiten überprüfen

Überprüfen Sie die Statistiken für die Ressourcen, die von ITOM-Produkten verwaltet werden können. Vergleichen Sie diese Daten mit der durchschnittlichen Anzahl der zugeteilten Abonnementeinheiten.

Vorbereitungen

Erforderliche Rolle: Administrator

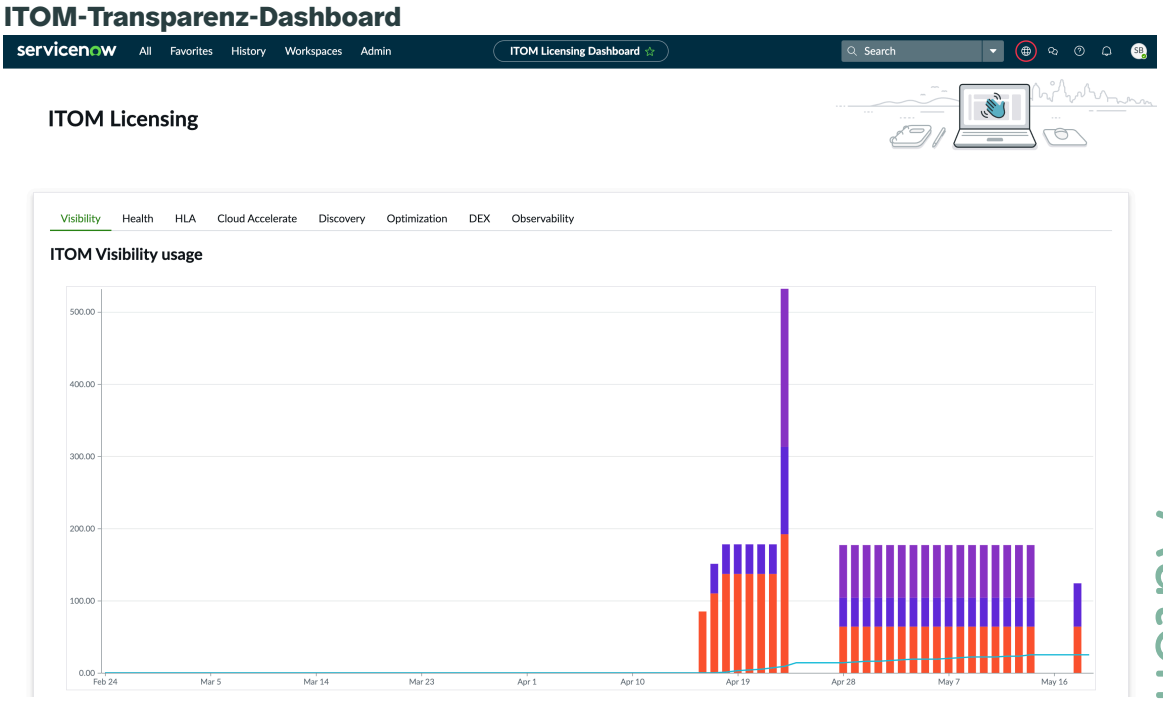
Siehe ITOM Detaillierte Lizenzierungsdaten im Zeitverlauf mit ITOM Lizenzierungsdashboard. Zeigen Sie die täglichen CI-Anzahlen oder den Durchschnitt der letzten 90 täglichen Anzahlen an. Mit domänenspezifischen Informationen und spezifischen CI-Listen für jede tägliche Anzahl können Sie die Ressourcennutzung überwachen und analysieren. Sie können eine Liste der derzeit zählbaren CIs für jedes der generieren ITOM Anwendungen wie in beschrieben ITOM-Abonnementeinheiten verbrauchende CIs anzeigen.

Prozedur

1. Navigieren zu **Alle** > **ITOM-Lizenz** > **ITOM-Lizenzierungsdashboard**an.
2. Wählen Sie die entsprechende Registerkarte aus, um das Dashboard für das ITOM-Produkt anzuzeigen. Wählen Sie beispielsweise aus **Sichtbarkeit** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Zeigen Sie auf einen Balken, um die Anzahl der CIs in jeder Kategorie anzuzeigen.
4. Wählen Sie den Balken aus, um eine Liste der gezählten CIs anzuzeigen.
5. Überprüfen Sie das unter ITOM/OT SU-Lizenzierung-Dashboard beschriebene Dashboard.

Für ITOM-Abonnements verwendete CI-Anzahl prüfen

Zeigen Sie die täglichen CI-Anzahlen oder den Durchschnitt der letzten 90 täglichen Anzahlen an.

Vorbereitungen

Vergewissern Sie sich, dass Ihre Organisation ITOM-Abonnements erworben hat. Sie können die Informationen im **ITOM-Lizenz**-Modul nicht ohne Abonnements anzeigen.

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

ITOM Anwendungen, z. B. ITOM-Transparenz, ITOM Discovery, ITOM-Integrität, Health Log Analytics, ITOM Cloud Accelerate und ITOM-Optimierung enthalten Informationen zu den von ihnen verwendeten Ressourcen. Diese Ressourcen, die als Konfigurationselemente (CIs) bezeichnet werden, werden von ITOM-Anwendungen in der CMDB gefunden, überwacht und gespeichert. Das ITOM/OT SU-Lizenzierung-Modul kombiniert diese CI-Daten mit den Abonnementinformationen Ihres Unternehmens, um Statistiken über Abonnementverbrauch und -nutzung der ITOM-Anwendungen zu erzeugen.Weitere Informationen zum Lizenzierungs-Workflow-Prozess finden Sie unter Datensammlung und -Zusammenfassung für den Lizenzierungsprozess.

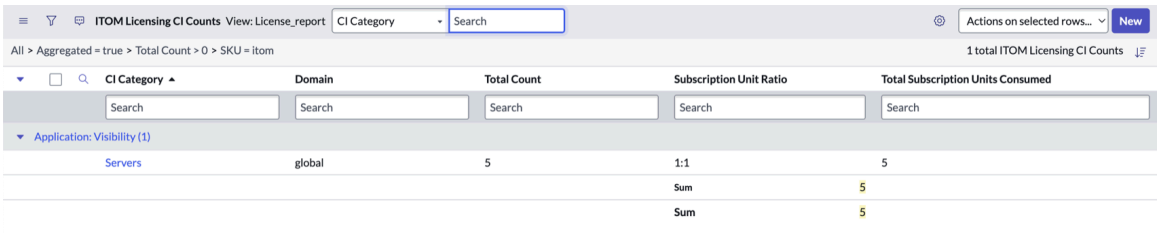
Diese Informationen enthalten keine Statistiken zu Abonnements, die in Paketen erworben wurden. Zeigen Sie für vollständige Informationen zu Abonnements die Abonnementstatistiken für IT Operations Management an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **ITOM-Lizenz** > **Lizenzbericht**an.



   Weitere Informationen zu den Feldern im Fenster „Lizenzbericht“ finden Sie unter Formular „Lizenzbericht“.

2. In **Gesamtanzahl** Spalte die durchschnittliche tägliche CI-Anzahl der letzten 90 Tage anzeigen.
3. Zeigen Sie die tägliche CI-Anzahl auf eine der folgenden Arten an.
   - Legen Sie fest **Aggregiert** Filterbedingung bis **[Aggregiert] [ist] [falsch]** Und wählen Sie aus **Ausführen** .
   - Navigieren zu **ITOM-Lizenz** > **Tägliche Lizenznutzungsanzahl**an.

Überprüfen, welche CI-Typen ein ITOM-Abonnement erfordern

Zeigen Sie die Liste der CI-Typen (Configuration Item) an, für die IT Operations Management-Abonnementeinheiten erforderlich sind.

Vorbereitungen

Vergewissern Sie sich, dass Ihre Organisation ITOM-Abonnements erworben hat. Sie können die Informationen im **ITOM-Lizenz**-Modul nicht ohne Abonnements anzeigen.

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

Für Lizenzierungszwecke werden lizenzierbare Ressourcen CI-Kategorien zugewiesen. Die Lizenznutzung wird mithilfe von Abonnementeinheiten gemessen, die je nach CI-Kategorie der Ressource eine unterschiedliche Anzahl von Ressourcen abdecken können. Der Kundenvertrag für Ihr Unternehmen bestimmt die CI-Kategorien aus den verfügbaren Optionen und auch die Verhältnisse der CI-Zuweisung für die Abonnementeinheiten in jeder CI-Kategorie. Informationen aus dem Kundenvertrag werden mit der ServiceNow Platform synchronisiert. Die neueste Version von ServiceNow® ITOM/OT SU-Lizenzierung unterstützt die folgenden CI-Kategorien:

- Container
- PaaS
- FaaS
- Server
- Nicht gelöstes Überwachungsobjekt
- Nicht klassifizierte Kategorie
- Endanwendergeräte
- IoT
- Prem-Geräte des Kunden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das System speichert Informationen zu CI-Kategorien und CI-Typen, die zu ihnen gehören, im ITOM Tabelle „Lizenzierungsmetadaten“ [itom_lu_metadata]. Diese Tabelle enthält nur Informationen zu übergeordneten CI-Typen. Alle CI-Typen, die durch Erweiterung dieser übergeordneten CI-Typen erstellt werden, sind standardmäßig enthalten. Beispielsweise ist der CI-Typ „Apache-Webserver“ in der CI-Anzahl enthalten, da es sich um eine Erweiterung des CI-Typs „Webserver“ handelt.

Prozedur

1. Überprüfen Sie, welche CI-Kategorie lizenzierbar ist:
   a. Navigieren zu **Alle** > **ITOM-Lizenz** > **Lizenzzusammenfassung**an.
   b. Wählen Sie das entsprechende aus ITOM Abonnement.
   Beispiel: **ITOM-Transparenz** .
   c. Scrollen Sie nach unten, und wählen Sie die Registerkarte **ITOM-CI – Abonnement-Einheiten-Verhältnis** aus.
   Auf der Registerkarte werden lizenzierbare CI-Kategorien aufgelistet, die aus dem Kundenvertrag generiert wurden. Dies sind die lizenzierbaren CI-Kategorien.
   d. Notieren Sie sich die dafür bereitgestellten lizenzierbaren CI-Kategorien ITOM Abonnement.
   e. **Wahlweise:** Kehren Sie zur Liste **Lizenzzusammenfassung** zurück, und prüfen Sie die für andere ITOM-Abonnements generierten CI-Kategorien.
2. Navigieren zu **Alle** > **ITOM-Lizenz** > **Lizenzen nach CI-Typ**an.

   Wichtig: Die Tabelle „ITOM-Lizenzierung – MetaData“ [itom_lu_metadata] enthält alle CI-Kategorien, einschließlich Kategorien von CIs, die keine ITOM-Abonnementeinheiten erfordern.
3. Prüfen Sie die Liste, um lizenzierbare CI-Kategorien zu identifizieren, die auf der Registerkarte **ITOM-CI – Abonnement-Einheiten-Verhältnis** der Liste **Lizenzzusammenfassung** angezeigt werden.
4. Wählen Sie den Pfeil neben der lizenzierbaren CI-Kategorie aus, um sie zu erweitern und auf die zugehörigen CI-Typen zuzugreifen.

   Die unter CI-Kategorien aufgeführten CI-Typen erfordern ITOM Abonnementeinheiten für den Zugriff.

ITOM-Abonnementeinheiten verbrauchende CIs anzeigen

Generieren Sie eine Liste der derzeit zählbaren CIs für jedes der CIs ITOM Anwendungen: ITOM-Transparenz, Discovery, ITOM-Integrität, Health Log Analytics, ITOM Cloud Accelerate, Und ITOM-Optimierung.

Vorbereitungen

Vergewissern Sie sich, dass Ihre Organisation ITOM-Abonnements erworben hat. Sie können die Informationen im **ITOM-Lizenz**-Modul nicht ohne Abonnements anzeigen.

Erforderliche Rolle: sn_itom_license.reader

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Die generierte CI-Liste korreliert eng mit der aktuellen täglichen CI-Anzahl. Gleichzeitig kann die Anzahl der CIs in der generierten CI-Liste geringfügig von der letzten täglichen CI-Anzahl abweichen, wenn seit der letzten täglichen Zählung Änderungen aufgetreten sind.

Prozedur

1. Navigieren zu **Alle** > **ITOM-Lizenz** > **ITOM-lizenzierbare CIs melden**an.
   Die Seite **ITOM-lizenzierbare CIs melden** wird angezeigt.
2. Wählen Sie die Anwendung aus, für die Sie lizenzierte CIs anzeigen möchten:
   - Discovery
   - Optimierung
   - Sichtbarkeit
   - HLA
   - Governance
   - Gesundheitswesen
3. Um einen Bericht für die ausgewählte Anwendung zu erstellen, wählen Sie aus **Füllen Sie lizenzierbare CIs aus** .
4. Wählen Sie aus, um die Bestätigungsnachricht zu akzeptieren und den Bericht zu generieren **Ja** .

   Im neuen Bericht werden die Daten aus dem zuvor generierten Bericht ersetzt. Sie können den Bericht abbrechen, indem Sie die Anwendung und dann **Auftrag abbrechen** auswählen.
5. Warten Sie einige Minuten, und aktualisieren Sie dann die Seite.
   Die **Status** Der Anwendung wird angezeigt **Abgeschlossen** Wenn der Bericht abgeschlossen ist.
6. Wählen Sie die Anwendung und dann **Lizenzierbare CIs anzeigen** aus.
   Die Seite „ITOM lizenzierbare CIs“ zeigt die Liste der CIs mit einer Lizenz an.

ITOM/OT SU-Lizenzierung – Referenz

Referenzthemen enthalten zusätzliche Informationen zu geplanten Aufgaben, Tabellen, Abonnementformular und Dashboard, die Sie zum Konfigurieren und Verwalten verwenden ITOM/OT SU-Lizenzierung.

Mit ITOM/OT SU-Lizenzierung installierte Komponenten

Bei der Aktivierung des ITOM/OT SU-Lizenzierung-Plugins werden mehrere Arten von Komponenten installiert, z. B. Tabellen und regelmäßige Aufgaben.

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
ITOM Ausschlusstabellen Aktualisieren Store	Aktualisiert die Ausschlussliste.
ITOM Lizenzierungsaggregator-Store	Berechnet die täglichen durchschnittlichen CI-Anzahlen der letzten 90 Tage.
ITOM Lizenzierung Cloud Accelerate CI Listing Store	Erstellt die Liste der lizenzierbaren CIs für ITOM Cloud Accelerate.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
ITOM Cloud Accelerate Lizenzierungsnutzungsanzahl Store	Berechnet die täglichen CI-Anzahlen für ITOM Cloud Accelerate.
Event Management – Speichern der Knotenanzahl	Berechnet die in Ereignismanagement verwendete Knotenanzahl.
ITOMHealthCIReporterWithOTOMCountITOMStore	Kompiliert die Liste von lizenzierbaren CIs für ITOM.
ITOMHealthCIReporterWithOTOMCountOTOMStore	Kompiliert die Liste von lizenzierbaren CIs für Operational Technology Management (OTM).
ITOM Speicher Für Nutzungsanzahl Der Integritätslizenzierung	Berechnet die tägliche CI-Anzahl für ITOM-Integrität.
ITOM Optimierungslizenzierung – Nutzungsanzahl – Store	Berechnet die tägliche CI-Anzahl für ITOM-Optimierung.
ITOM Listingstore für Listingoptimierung des CI	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Optimierung.
OTOM-Lizenzierung – Speichern der CI-Auflistung für ITOM Visibility	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Transparenz (OTM).
ITOM Lizenzierung von Discovery-CI – Listingstore	Kompiliert die Liste von lizenzierbaren CIs für Discovery.
ITOM Lizenzierungstransparenz CI-Listingstore	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Transparenz.
ITOM Speicher Für Nutzungsanzahl Der Sichtbarkeitslizenzierung	Berechnet die tägliche CI-Anzahl für ITOM-Transparenz.
OTOM-Lizenzierung – Speichern der CI-Auflistung für Discovery	Kompiliert die Liste von lizenzierbaren CIs für Discovery (OTM).
ITOM DEX Lizenzierungsnutzungsanzahl Store	Berechnet die täglichen CI-Anzahlen für ITOM DEX.
ITOM Lizenzierung DEX CI-Listenspeicher	Erstellt die Liste der lizenzierbaren CIs für ITOM DEX.
ITOM Lizenzierung Service-Observability CI-Listenspeicher	Erstellt die Liste der lizenzierbaren CIs für ITOMService-Observability.
ITOMService-Observability Lizenzierungsnutzungsanzahl Store	Berechnet die CI-Anzahlen für ITOMService-Observability.
ITOM Lizenzierungsverlaufstabelle – Aktualisierungsspeicher	Erstellt eine Tabelle, um alle lizenzierbaren CIs täglich zu speichern

Installierte Tabellen

Informationen dazu, wie lizenzierbare CIs für verschiedene ITOM-Produkte von ITOM/OT SU-Lizenzierung gezählt werden, finden Sie im KB-Artikel ITOM Subscription Unit license calculation logic (KB0748149) (Lizenzberechnungslogik für ITOM-Abonnementeinheiten).

Tabelle	Beschreibung
ITOM LU-Discovery-Quellzuordnung	Enthält die Liste der lizenzierbaren Discovery-Quellen für jede Kategorie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[itom_lu_Discovery_Source_Mapping]	
ITOM LU Governance-App-Zuordnung [itom_lu_Governance_App_Mapping]	Liste der Datensätze, die die Zuordnung von Governance-Anwendungen zu ihren jeweiligen lizenzierbaren CIs enthalten.
ITOM LU-Governance-CIs [itom_lu_Governance_ci]	Enthält die Liste der CIs, die unter der Governance-Lizenz gezählt werden.
ITOM Lizenzausschlussmetadaten [itom_license_Exclusion_metadata]	Enthält die Liste der Ausschlussregeln, die für verschiedene Lizenzen gelten.
Lizenzausschlüsse [License_Exclusion_list]	Enthält die Liste der CIs, die basierend auf der Ausschlussregel von der Lizenzanzahl ausgeschlossen werden müssen.
Sichtbarkeit LU Temporär [Sichtbarkeit_lu_temp]	Enthält die Liste der CIs, die unter der Discovery-Lizenz gezählt werden.
ITOM Metadaten der Lizenzierungskategorie [itom_lu_category_metadata]	Enthält Lizenzierungsmetadaten.
ITOM Discovery-Quellen Lizenzieren [itom_lu_Discovery_sources]	Enthält die Kategorien für alle Discovery-Quellen.
ITOM-LU DEX CIs [sn_itom_Lizenzierung_itom_lu_Dex_ci]	Enthält die Liste der CIs, die unter gezählt werden DEX Lizenz.
Historische lizenzierbare CIs [sn_itom_Lizenzierung_itom_lu_Historical_cis]	Enthält die Liste der historischen lizenzierbaren CIs.

Abonnementformular für die ITOM-Produkte

Beschreibung der Felder im Formular „Abonnements“ für ITOM Produkte.

ITOM Felder des Abonnementformulars für Produkte

Feld	Beschreibung
Name	Name des Abonnementpakets oder ITOM Anwendung, wenn Ihre Organisation Abonnements pro Anwendung separat erworben hat (a la carte).
Startdatum	Datum, an dem das Abonnement aktiviert wurde.
Enddatum	Datum, bis zu dem das Abonnement gültig ist.
Gekauft	Anzahl der erworbenen Abonnements pro Paket oder Anwendung (a la carte).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Felder des Abonnementformulars für Produkte (Fortsetzung)

Feld	Beschreibung
Zugeordnet	Anzahl der verbrauchten Abonnementeinheiten aus einem Paket oder einer Anwendung (a la carte). Für Pakete wird in diesem Feld die höchste Anzahl der verbrauchten Abonnementeinheiten nach Anwendungen angezeigt, die Teil des Pakets sind. Beispiel: Wenn ITOM-Transparenz 300 Abonnementeinheiten und ITOM-Integrität 200 Abonnementeinheiten verbraucht hat, wird in diesem Feld der Wert 300 für das Paket angezeigt, das diese Anwendungen abdeckt. Der Farbcode gibt den Prozentsatz der Abonnementeinheiten an, die Ihr Unternehmen verbraucht hat. Standardmäßig lautet der Schwellenwert für den Farbcode 90 %. • Grün: Ihre Organisation hat weniger als 10 % der erworbenen Abonnements verwendet. • Gelb: Ihre Organisation hat mehr als 90 %, aber weniger als 100 % der erworbenen Abonnements verwendet. • Rot: Ihre Organisation hat 100 % oder mehr verwendet und die Anzahl der erworbenen Abonnements überschritten. Die erworbenen Abonnements sind überzogen.

ITOM/OT SU-Lizenzierung-Dashboard

Verwenden Sie das ITOM Licensing Dashboard (ITOM-Lizenzierungsdashboard), um die Statistiken zum Ressourcenverbrauch und zum Status Ihrer erworbenen Abonnements zu überprüfen. Dieses Dashboard enthält Berichte für jede ITOM-Anwendung. Die Berichte bieten eine Visualisierung der täglichen Nutzungsanzahl und des durchschnittlichen Verbrauchs von Abonnementeinheiten für 90 Tage.

Die ITOM Das LizenzierungsDashboard ist Teil von ITOM Lizenzierungsanwendung. Siehe auch OTM LizenzierungsDashboard unter **Alle** > **OTM** > > **OTM-Lizenz** > **OTM-Lizenzierungsdashboard**an.

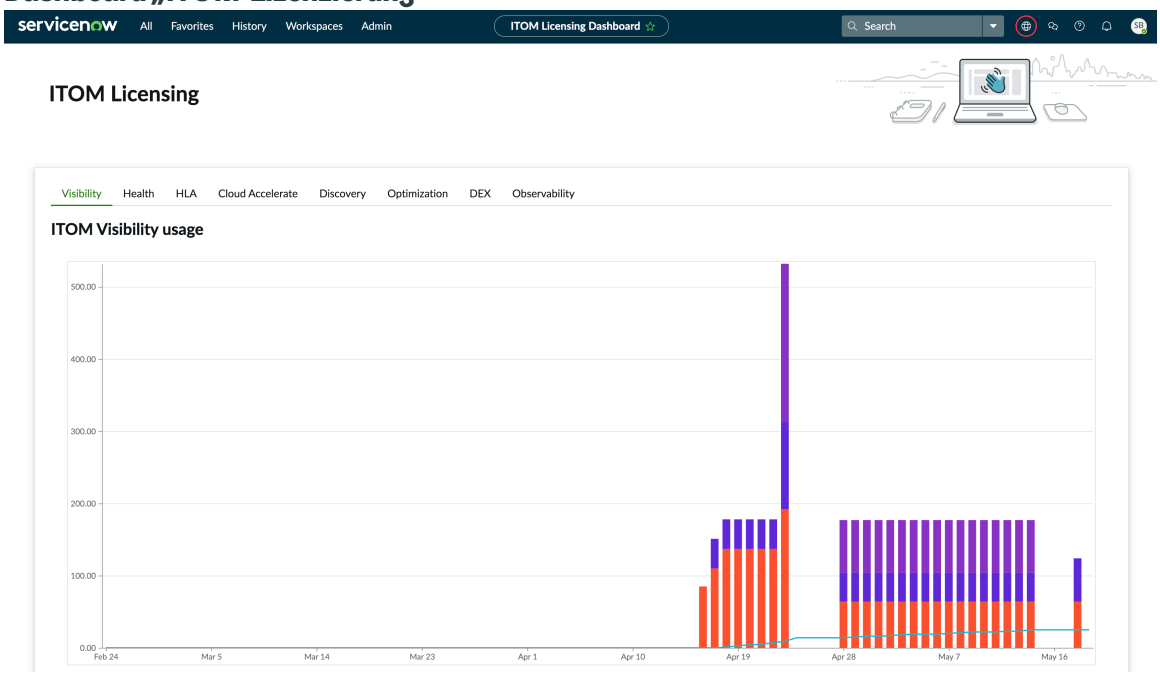
Erforderliche Rolle: Administrator

Bewertungs-Dashboard aufrufen

Stellen Sie sicher, dass Sie über eine Administratorrolle für den Zugriff auf verfügen ITOM LizenzierungsDashboard befindet sich in **Alle** > **ITOM-Lizenz** > **ITOM-Lizenzierungsdashboard**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „ITOM-Lizenzierung“



Anwendungsfälle

Beispiel dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie im folgenden Anwendungsfall.

Anwender	Dashboard-Verwendung
admin	Validieren Sie die Ressourcennutzung für verschiedene ITOM-Produkte. Melden Sie die Fälle, in denen die Organisation die Anzahl der erworbenen Abonnementeinheiten für bestimmte Ressourcen überschritten hat.

Hinweis: ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

Datenvisualisierung

Das Dashboard enthält die folgende Visualisierung:

Monatlich	Typ	Quelltabelle	Beschreibung
• ITOM-Transparenz • ITOM-Integrität • Health Log Analytics • ITOM Cloud Accelerate • ITOM Discovery • ITOM-Optimierung	§	ITOM-Lizenzierungs-CI-Anzahlen [itom_lu_ci_counts] und UsageAnalytics-Anzahlen für Tabellen [usageanalytics_count]	Zeigt Balken an, die die Anzahl der CIs verschiedener lizenzierbarer Kategorien für die letzten 120 Tage pro ITOM-Anwendung darstellen. Das Dashboard zeigt auch die Zeile an, die den durchschnittlichen Verbrauch von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Monatlich	Typ	Quelltabelle	Beschreibung
• ITOM Digitale Endanwender-Experience (DEX) • ITOM Service-Observability			Abonnementeinheiten für die letzten 90 Tage darstellt, wobei SU-Verhältnisse verwendet werden, bei denen ein Server, drei PaaS-Ressourcen, drei Container oder ein ungelöstes überwachtes Objekt 1 SU entspricht.

Formular „Lizenzbericht“

Beschreibung der Felder im Formular „Lizenzbericht“.

Formularfelder „Lizenzbericht“

Feld	Beschreibung
CI-Kategorie	Gruppierung von Konfigurationselementen (Configuration Items, CIs) in jeder Anwendung basierend auf gemeinsam genutzten Merkmalen oder Attributen.
Domäne	Domäne, zu der das CI gehört.
Gesamtanzahl	Durchschnitt von 90 täglichen Anzahlen von CIs, die nach CI-Typen kategorisiert sind, jeweils innerhalb ITOM Anwendung. **Hinweis:** Die Gesamtanzahl entspricht nur der obigen Definition, wenn der **Aggregiert** Die Bedingung im Filter ist auf festgelegt **Wahr** . Wenn **Aggregiert** Bedingung ist als festgelegt **Falsch** , Die Gesamtanzahl stellt die tägliche Anzahl für eine bestimmte Anwendung und Kategorie an diesem Tag dar.
Abonnement-Einheiten-Verhältnis	Anzahl der CIs in einer bestimmten Kategorie, die ein Abonnement benötigen.
Insgesamt verbrauchte Abonnementeinheiten	Gesamtzahl der Abonnementeinheiten, die von verbraucht werden ITOM Anwendungen innerhalb eines bestimmten Zeitrahmens. Das Lizenzierungsmodul berechnet diese Zahl anhand des Verhältnisses der Abonnementeinheiten mit der Anzahl der CIs in jeder CI-Kategorie.
Summe	Gesamtverbrauch der Abonnementeinheiten durch die Anwendung und alle ITOM Anwendungen. Wird unter verbrauchte Abonnementeinheiten insgesamt hervorgehoben angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Store-Upgrades

Um ITOM mit voller Kapazität nutzen zu können, können Sie die neuesten Out-of-Band-Upgrades aus dem ServiceNow Store bereitstellen. Erfahren Sie mehr über Funktionen und Erweiterungen, die out-of-Band verfügbar sind.

Was sind Store-Upgrades

Die ServiceNow Store Veröffentlicht regelmäßig neue Anwendungen und Updates für Anwendungen, die von erstellt wurden ServiceNow. Jede Anwendung besitzt möglicherweise einen anderen Release-Zeitplan und ist „out-of-Band“, was bedeutet, dass die Anwendung nicht ausdrücklich an einen Familien-Release gebunden ist. Wenn Sie schon eine bestimmte Store-Anwendung haben, können Sie die neueste Version herunterladen, um Ihre bestehende Erfahrung mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Features verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Liste der Store-Upgrades

- Agent Client Collector
- Certificate and Inventory Management
- Discovery-Muster
- Firewall Audit and Reporting
- CMDB CI Class Models
- Health Log Analytics
- Performance Analytics-Inhaltspaket für Cloud-Ressourcen
- Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich
- ITOM Cloud Accelerate

ITOM Cloud Accelerate

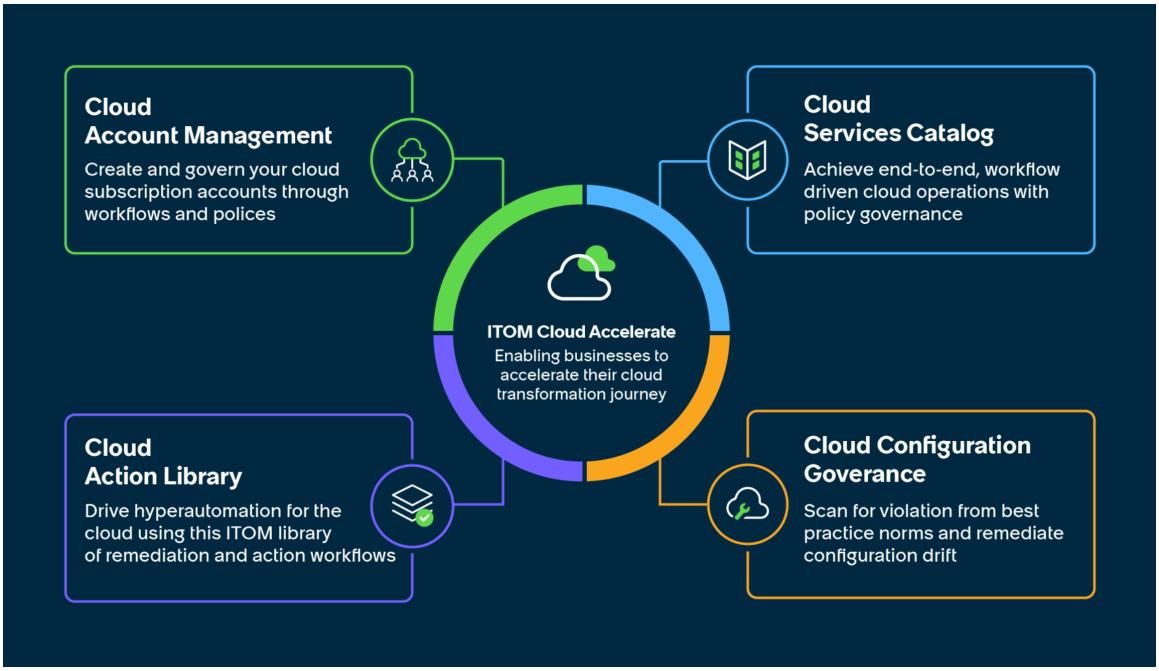
ITOM Cloud Accelerate Workflows optimieren die Cloud-Automatisierung über die gesamte Cloud-Adoption-Journey über Selfservice-Kataloge und kontrollierte Workflows. Sie beschleunigt die Anwendungsmigration, indem sie Bewertung, Planung und Nachverfolgung der Ressourcenmigration erleichtert.

Funktionen von ITOM Cloud Accelerate

ITOM Cloud Accelerate Ermöglicht Organisationen, ihre Cloud-Assets anhand vordefinierter Standards zu validieren und Abweichungen zu korrigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Cloud Accelerate



Diese automatisierten Prozesse ermöglichen es Unternehmen, ihren Weg zur Cloud-Transformation zu beschleunigen, indem sie Vorgänge an Tag 0, Tag 1 und Tag 2 automatisieren. Es bietet die folgenden Funktionen:

Cloud Account Management

ServiceNow® verwenden Cloud Account Management App für die effiziente Verwaltung und Bereitstellung von Cloud-Accounts . Mit der App können Sie entweder manuelle Genehmigungen für die Account-Erstellung einholen, um sicherzustellen, dass der Prozess von relevanten Stakeholdern genau überwacht und verifiziert wird, oder den Genehmigungsprozess basierend auf vordefinierten Regeln und Bedingungen automatisieren, was Zeit spart und manuelle Eingriffe reduziert.

Cloud-Services-Katalog

Verwenden Sie ServiceNow® Cloud-Services-Katalog App für eine vereinfachte, unterstützte und empfohlene Schnittstelle für den Zugriff auf Cloud-Ressourcen. Sie können Cloud-Angebote auch in einem Katalog veröffentlichen und die Nutzung und den Lebenszyklus dieser Ressourcen verwalten.

Bewertung der Cloud-Migration

Verwenden Sie die Anwendung ServiceNow® Bewertung der Cloud-Migration, um den Prozess der Verlagerung von IT-Ressourcen und Arbeitslasten Ihres Unternehmens auf Cloud-Plattformen zu planen, zu organisieren und nachzuverfolgen. Analysieren Sie die IT-Ressourcen mithilfe von Dashboards, in denen Informationen zu Ressourcen nach verschiedenen Kategorien visualisiert und zusammengefasst werden.

Governance für Cloud-Konfigurationen

Verwenden Sie die Anwendung ServiceNow® Governance für Cloud-Konfigurationen, um die Konfigurationseinstellungen von Cloud-Ressourcen in Ihrer Organisation anhand einer Reihe von Richtlinien zu überprüfen und so Verstöße zu identifizieren. Nachdem Sie den Verstoß identifiziert haben, verwenden Sie Fehlerkorrektur-Workflows, um ihn zu minimieren.

Bibliothek von Cloud-Aktionen

Verwenden Sie die einsatzbereiten Aktionen und Subflows der Anwendung ServiceNow® Bibliothek von Cloud-Aktionen, um mit den Cloud-Ressourcen der Organisation zu interagieren. Von ServiceNow® ITOM Cloud Accelerate-Funktionen wie Governance für Cloud-Konfigurationen werden diese Aktionen für den Betrieb verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Cloud Accelerate Lizenzierung

Bei der für ServiceNow AI Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM Cloud Accelerate. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

ITOM Cloud Accelerate bereitstellen

ITOM Cloud Accelerate-Funktionen sind im ServiceNow Store als separate Apps verfügbar.

Für Lizenzierungszwecke gibt die ITOM Cloud Accelerate-Lizenz die CI-Anzahl für CIs an, die von Bewertung der Cloud-Migration, Governance für Cloud-Konfigurationen oder Bibliothek von Cloud-Aktionen verwaltet und überwacht werden. Wenn von unterschiedlichen ITOM Cloud Accelerate-Funktionen dieselben CIs als ihre Ressourcen gemeldet werden, wird die CI-Anzahl so manipuliert, dass das Duplikat entfernt wird.

Guided Setup zum Implementieren von IT Operations Management-Anwendungen

Das IT Operations Management-Guided Setup mit Anleitung bietet eine Reihe an Aufgaben, die Sie beim Konfigurieren von IT Operations Management-Anwendungen auf Ihrer ServiceNow-Instanz unterstützen. Zum Öffnen IT Operations Management Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Cloud Account Management

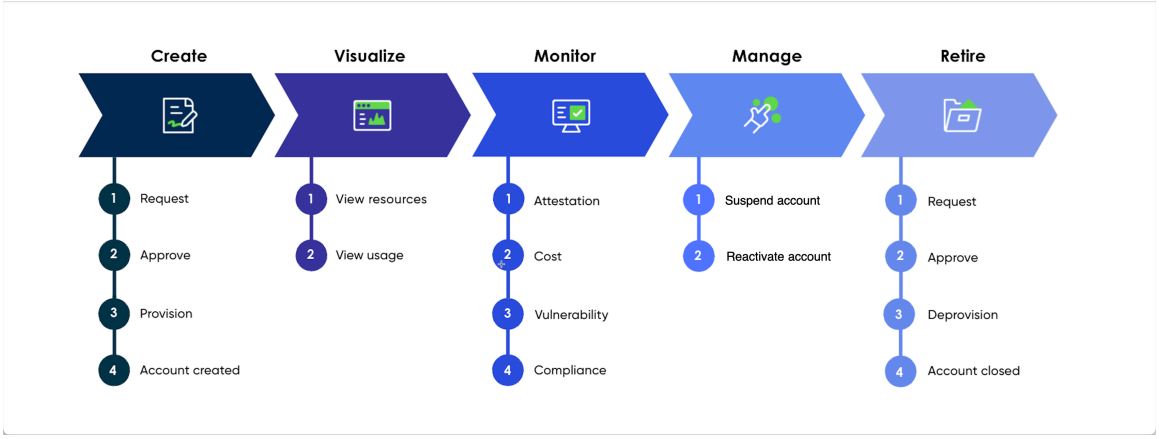
Cloud Account Management Vereinfacht die Account-Verwaltung, indem Aufgaben wie Erstellung und Bereitstellung automatisiert werden. Vordefinierte Richtlinien ermöglichen eine einfache Sperrung, Reaktivierung und Zertifizierung von Accounts. Reduzieren Sie die Bereitstellungszeiten potenziell von Wochen auf Minuten, indem Sie Anforderungen, Genehmigungen und Setups automatisieren.

Cloud Account Management Bringt zusammen ServiceNow Cloud-Lösungen in einer einheitlichen Experience als Teil von Cloud-Governance Suite.

Die Cloud Account Management Die Funktion automatisiert den Verwaltungsprozess für AWS Accounts und Azure Abonnementerstellung. Zu den wichtigsten Vorteilen gehören die Automatisierung des Account-Managements, die Optimierung von Genehmigungs-Workflows, die Reduzierung der Bereitstellungszeit und die Verbesserung der Sicherheit durch automatisierte Zertifizierungen.

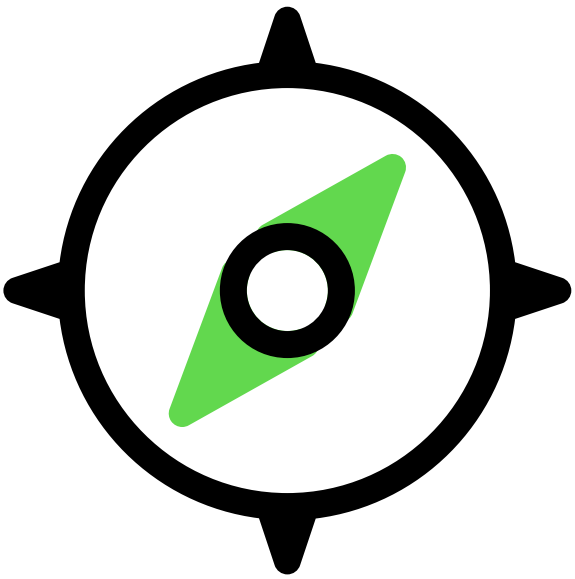
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management – Workflow



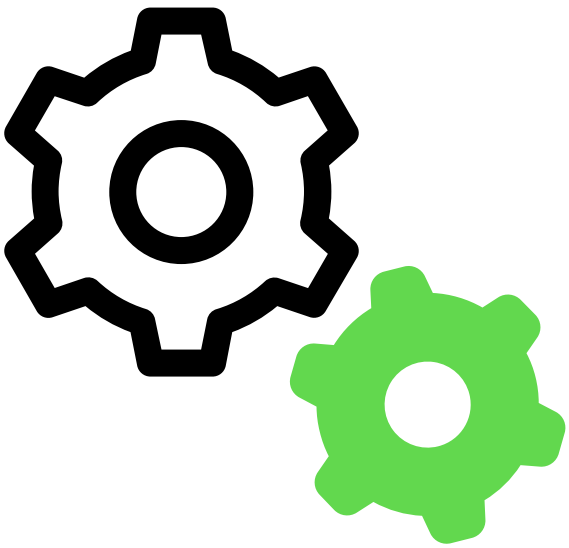
Erste Schritte

Untersuchen



Konzepte und Funktionen von Cloud Account Management kennenlernen.

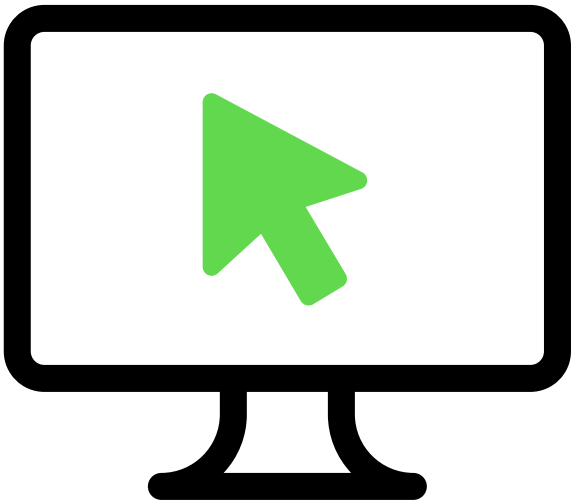
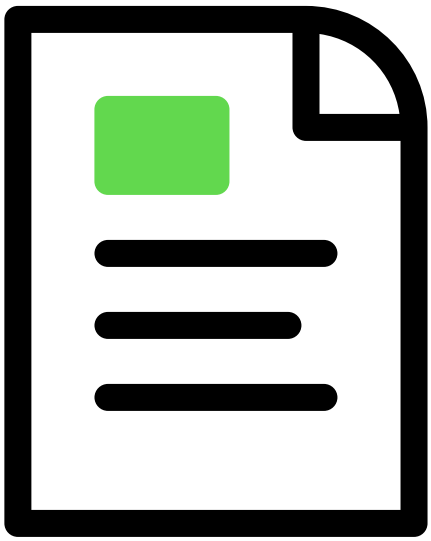
Konfigurieren



Konfigurieren Sie die Umgebung und den Anwenderzugriff.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
	
Machen Sie sich mit dem Workflow vertraut, um Cloud-Accounts zu erstellen und zu verwalten.	Rufen Sie Details zu Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Cloud Account Management erkunden

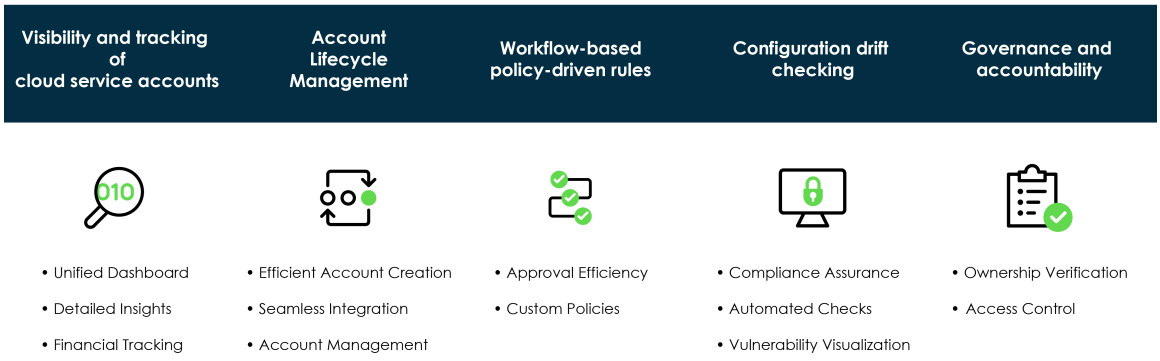
Die ServiceNow Cloud Account Management In Cloud-Arbeitsbereich Die Anwendung stellt ein Framework zur Optimierung des Prozesses zur Erstellung und Verwaltung von Cloud-Accounts bereit.

Cloud Account Management – Übersicht

Die Automatisierungsfähigkeiten von Cloud Account Management In Cloud-Arbeitsbereich Vereinfachen Sie administrative Aufgaben im Zusammenhang mit der Account-Verwaltung, z. B. Erstellung, Aussetzung, Reaktivierung und Zertifizierung. Die Datenzertifizierung bestätigt die Integrität und Sicherheit von Anwenderaccounts in der Cloud-Umgebung der Organisation.

Als Cloud Account Management administrator können Sie die Kontostatistiken anzeigen, die auf angezeigt werden **Startseite** Registerkarte, die Accounts mit Schweregrad „Kritisch“, Accounts mit hohem Schweregrad, ausgesetzte Accounts, Konten mit Zertifizierungen und Accounts mit nicht definierten Budgets umfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Über Cloud-Arbeitsbereich Berechtigungen

Cloud Account Management Passt die Ihnen verfügbaren Funktionen dynamisch basierend auf Ihren Berechtigungen an.

- Cloud Account Management Die Berechtigung wird mit verfügbar ITOM Cloud Accelerate Lizenz.
- Die Cloud-Governance Suite-Lizenz (CGS) ist eine Voraussetzung für die Verwendung Cloud-Arbeitsbereich. Die CGS-Lizenz bietet die folgenden Fähigkeiten:
  - Greifen Sie auf die Homepage zu
  - Greifen Sie auf den Asset-Explorer zu, der einen Überblick über Ihre Cloud-Assets und Asset-Details bietet
- Die Cloud-Governance Suite mit Cloud Account Management Berechtigungen (CGS + CAM) bieten die folgenden zusätzlichen Fähigkeiten:
  - Zeigen Sie eine Übersicht über Ihre Accounts und Account-Details an
  - Account-Anforderungen übermitteln, anzeigen oder genehmigen
  - Zertifizieren Sie einen Account
  - Zeigen Sie das Compliance-Dashboard an
  - Konfigurieren Cloud Account Management Oder zeigen Sie Konfigurationsdetails an
  - Erstellen Sie Anforderungsrichtlinien, um zu automatisieren Schließen Sie die Erstellung und Sperrung des Accounts ab Prozess

Compliance-Dashboard in Cloud-Arbeitsbereich

Das Compliance-Dashboard konsolidiert Daten aus ITOM-Transparenz, Cloud Account Management Bietet eine einheitliche Ansicht von Cloud-Daten und wichtigen Metriken, die für Sicherheits- und Compliance-Berichte wichtig sind.

Weitere Einzelheiten finden Sie unter Anzeigen des Compliance-Dashboards.

Cloud-Account-Terminologie

Cloud Account Management Verwendet den Begriff „Cloud-Account“, andere Cloud-Anbieter verwenden jedoch andere Begriffe für ähnliche Konzepte. Die Begriffe lauten wie folgt:

- Microsoft Azure Cloud(Azure) Bezieht sich auf Abonnements
- Amazon AWS Cloud(AWS) Bezieht sich auf Verwaltungs- und Mitgliedsaccounts
- Google Cloud Platform(GCP) Bezieht sich auf Projekte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Provider bieten zwei Hauptzugriffsmechanismen für die Ausführung von Vorgängen:

- Konsolenanwenderzugriff
- Programmgesteuerter Anwenderzugriff

Für Cloud Account Management, Diese Vorgänge werden als IAM-Service-Accounts bezeichnet. Andere Cloud-Anbieter verwenden jedoch eine andere Terminologie:

- AWS Bezieht sich auf den IAM-Anwender
- Azure Bezieht sich auf Service-Prinzipale
- GCP Bezieht sich auf Service-Accounts

Cloud Account Management Anwenderpersonas

In verwendete Personas Cloud Account Management

Anwender	Beschreibung
Anfordernde Person	Initiiert Anforderungen zur Erstellung von Cloud-Accounts und fordert die Sperrung oder erneute Aktivierung ihrer eigenen Accounts an.
Genehmigende Person	Überprüft Account-Anforderungen und genehmigt sie oder lehnt sie ab.
Administrator	Bestätigt, dass Cloud Account Management Konfigurationen stimmen mit Cloud-Konfigurationen überein. Passt die standardmäßige Datenzertifizierungsrichtlinie an. Onboarding von Accounts, die außerhalb von erstellt wurden Cloud Account Management Anwendung.
Zertifizierer	Genehmigt einen Account als zertifiziert oder fehlgeschlagen. Fungiert als Verifizierungsentität, indem die Richtigkeit und Integrität der Daten bestätigt wird.
Asset-Betrachter	Kann alle Konfigurationselemente (CIs) anzeigen Greifen Sie im Asset-Explorer auf das Compliance-Dashboard zu .

Weitere Informationen zu finden Cloud Account Management Gruppen und Verantwortlichkeiten, siehe Cloud Account Management ACL-Gruppen, Rollen und Zuständigkeiten.

Cloud Account Management Vorteile

Die Cloud Account Management Bietet mehrere Vorteile.

Cloud Account Management Vorteile

Leistung	Funktion	Anwender
Vereinfacht die Erstellung von Abonnementkonten, indem standardisierte Verfahren und Anwenderrollen und -Berechtigungen definiert werden, um die Konsistenz und Compliance mit Sicherheitsrichtlinien zu fördern.	Fordern Sie einen Cloud-Account an Brechen Sie eine Cloud-Account-Anforderung ab	Anfordernde Person
Ermöglicht das Aussetzen oder Reaktivieren von Accounts und das Hinzufügen nicht verwalteter Accounts.	Sperren Sie einen Cloud-Account	Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Vorteile (Fortsetzung)

Leistung	Funktion	Anwender
Bietet ein Visualisierungs-Dashboard zum Verwalten von Accounts und Anforderungsrichtlinien zur Automatisierung der Account-Erstellung, Genehmigungen und Budgetprüfungen.	Aktivieren Sie einen Cloud-Account erneut Fügen Sie einen nicht verwalteten Cloud-Account hinzu Konfigurationen werden erstellt Informationen zur Datenvisualisierung in Cloud Account Management Überprüfen Sie Anforderungsrichtlinien	
Optimiert die Durchführung von Verifizierungen, ob eine Person oder Entität aus Sicherheits-, Compliance- und regulatorischen Gründen legitim Eigentum oder Kontrolle über einen Account hat.	Zertifizieren Sie einen Account	Zertifizierer

Zugehörige Informationen

Über Amazon Web Services API-Berechtigungen

Mit Cloud Account Management installierte Komponenten

Informationen zu Bereitstellungsmodi in Cloud Account Management

Informationen zur Datenvisualisierung in Cloud Account Management

Die Cloud Account Management Das Übersichts-Dashboard bietet einen klaren Überblick über alle Cloud-Accounts und ihren Compliance-Status. Cloud Account Management Ruft Daten von ab Governance für Cloud-Konfigurationen Dient zum Erstellen einer einfachen, visuellen Übersicht über Compliance. Als Administrator können Sie die erforderlichen Aktionen für die gemeldeten Schwachstellen ergreifen.

Datenvisualisierungsprozess

Der Workflow zum Erstellen einer Scan-Konfiguration für die Datenvisualisierung.

1. Richtliniensätze auswählen:
   - Wählen Sie einen vordefinierten Richtliniensatz aus, oder passen Sie Richtlinien an, um anzugeben, was nach Account-Schwachstellen gescannt werden soll.
   - Cloud Account Management Stellt Standardrichtlinien für bereit AWS, Azure, Und GCP, Die Sie anpassen können, um bestimmte Compliance- oder Sicherheitsanforderungen zu erfüllen.
2. Accounts auswählen: Identifizieren Sie die zu scannenden Accounts, indem Sie entweder einen Verwaltungsaccount (der alle Mitgliedsaccounts enthält) oder einzelne Mitgliedsaccounts auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Definieren Sie einen Scan-Zeitplan, oder führen Sie einen Scan bei Bedarf aus: Richten Sie einen Scan-Zeitplan ein, oder führen Sie einen Scan bei Bedarf aus, um Schwachstellen basierend auf den ausgewählten Richtlinien für die angegebenen Accounts zu bewerten.

4. Tägliche Scans:
   - Führen Sie tägliche Scans durch, um Schwachstellen und Compliance-Probleme in Accounts zu identifizieren.
   - Diese Scans generieren Berichte zu Verstößen, Schweregradstufen und Account-Aliasse, die eine detaillierte Ansicht der Account-Compliance bieten.

5. Kosten nachverfolgen:
   - Cloud Account Management Ist in integriert Arbeitsbereich für Cloud-Kostenmanagement Dient zum Nachverfolgen von Budgets und Nutzung jedes Accounts.
   - Bestätigen Arbeitsbereich für Cloud-Kostenmanagement Version 8,1 oder höher ist installiert, und die Abrechnung ist konfiguriert.

Informationen zum Einrichten der Datenvisualisierung finden Sie unter Richten Sie die Scankonfiguration für die Datenvisualisierung ein.

Über Amazon Web Services API-Berechtigungen

Cloud Account Management Interagiert mit Amazon Web Services Dient zum Erstellen und Verwalten von Abonnementkonten.

Hinweis: Sie müssen einen einrichten AWS Service-Account für Cloud Account Management Das vom Account für getrennt ist Cloud-Discovery.

Die folgenden API-Berechtigungen sind erforderlich, um einen neuen Abonnementaccount in zu starten AWS:

- Budgets: CreateBudgetAction
- Budgets: DescribeBudgetAction
- Budgets: ModifyBudget
- Budgets: ViewBudget
- Organisationen: AttachPolicy
- Organisationen: CreateAccount
- Organisationen: CloseAccount
- Organisationen: DescribeAccount
- Organisationen: DescribePolicy
- Organisationen: DescribeOrganization
- Organisationen: DescribeOrganizationalUnit
- Organisationen: DescribeCreateAccountStatus
- Organisationen: ListRoots
- Organisationen: ListAccounts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Organisationen: ListTagsForResource
- Organisationen: ListAWSServiceAccessForOrganization“,
- Organisationen: ListAccounts
- Organisationen: ListParents
- Organisationen: ListOrganizationalUnitsForParent
- Organisationen: MoveAccount
- Organisationen: TagResource
- iam: GetAccountSummary
- sts: AssumeRole

Hinweis:

Weitere Details zu API-Berechtigungen finden Sie unter Cloud-Discovery REST API-Berechtigungstabelle So können Sie die für die Ausführung des Discovery-Prozesses erforderlichen Anwenderberechtigungen recherchieren und gewähren.

Informationen zu Bereitstellungsmodi in Cloud Account Management

Cloud Account Management Unterstützt beides Terraform Bereitstellungsmodi (Cloud und Enterprise) und der nativen Cloud-Schnittstelle.

Terraform -Unterstützung

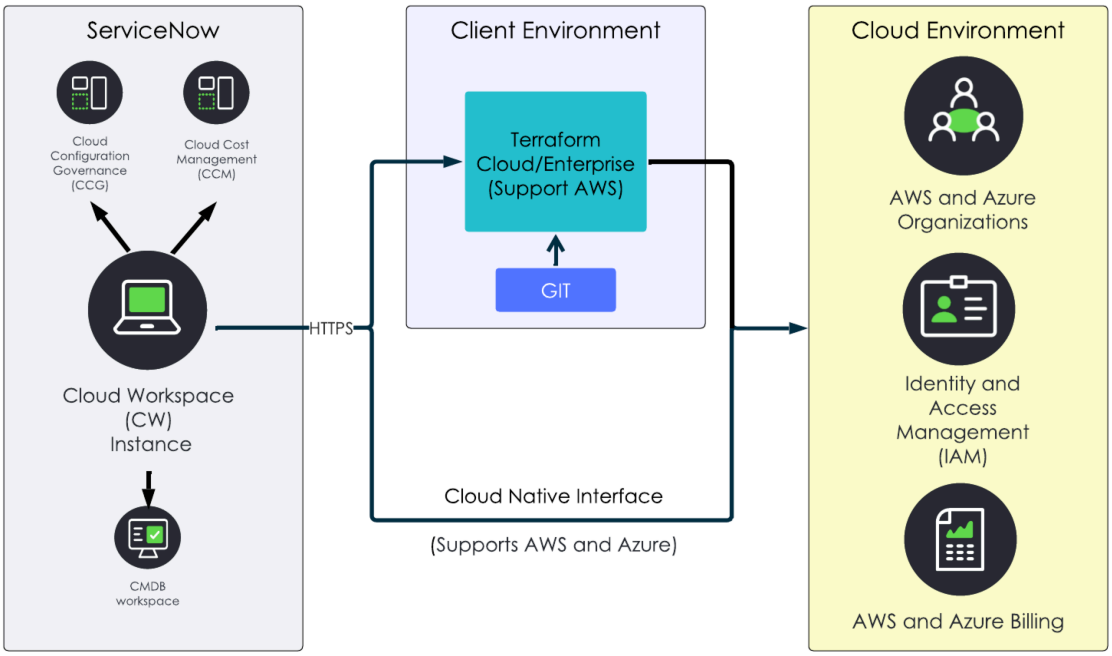
Terraform Vorlagen sind Konfigurationsdateien, die die Infrastrukturressourcen angeben, die für eine bestimmte Anwendung oder Umgebung mithilfe der Hashicorp Configuration Language (HCL) erforderlich sind. Cloud Account Management Ruft dynamisch ab Terraform Anmeldeinformationen und Vorlagen aus dem Git-Repository während der Terraform Account-Erstellungsprozess. Verwenden Sie die Terraform-Vorlage, die ServiceNow Die Instanz interagiert mit dem IAM (Identitäts- und Zugriffsmanagement) der Cloud-Organisation, um die Identität des Anwenders abzurufen.

Unterstützung der nativen Cloud-Schnittstelle

Ein AWS Oder Azure der administrator erstellt den IAM-Anwender mit den angegebenen Berechtigungen und Cloud Account Management der administrator gibt die Anmeldeinformationen des IAM-Anwenders in ein ServiceNow Instanz. Für Anwender sind keine zusätzlichen Schritte erforderlich, um auf die native Cloud-Schnittstelle zuzugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Bereitstellungsmodi



Über Richtlinien in Cloud Account Management

Cloud Account Management Stellt richtliniengesteuerte Regeln zur Automatisierung der Kontobereitstellung, Genehmigungen und Sicherheit bereit. Diese Richtlinien verbessern die Governance, kontrollieren die Kosten, verbessern die Sicherheit und fördern die Nachhaltigkeit im Cloud-Betrieb. Regelmäßige Überprüfungen fördern Konsistenz und Effizienz bei der Verwaltung der Cloud-Infrastruktur.

Cloud Account Management Stellt Richtlinien bereit, die Sie für die folgenden Zwecke verwenden können:

- Wird angehalten oder erneut aktiviert AWS Accounts. Weitere Einzelheiten finden Sie unter Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet.
- Auditing von Konten und Förderung der Compliance mit Sicherheits- und Governance-Standards. Weitere Einzelheiten finden Sie unter Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie.
- Automatisierung der allgemeinen Genehmigung, Budgetgenehmigung und Konfigurationszuweisungen durch die in der folgenden Tabelle aufgeführten Anforderungsrichtlinien.

Cloud Account Management Anforderungsrichtlinien

Richtlinie anfordern	Einzelheiten erfahren Sie von
Allgemeine Genehmigung der Erstellung eines Abonnement-Accounts	Automatisieren Sie den allgemeinen Genehmigungsrichtlinienprozess
Budgetgenehmigung der Erstellung eines Abonnement-Accounts	Automatisieren Sie den Richtlinienprozess für die Budgetgenehmigung
Konfigurationszuweisung der Erstellung eines Abonnement-Accounts	Automatisieren Sie den Richtlinienprozess für die Konfigurationszuweisung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile von Cloud Account Management Anforderungsrichtlinien

- Verbesserte Governance: Fördert konsistente Richtlinien für alle Cloud-Accounts.
- Kosteneinsparungen: Hilft, Überausgaben zu vermeiden, indem Accounts effizient verwaltet werden.
- Verbesserte Sicherheit: Enthält Sicherheitskontrollen als Teil der Leistung und Verfügbarkeit.

Sie können den Account-Genehmigungsprozess, den Budgetgenehmigungsprozess und den Konfigurationszuweisungsprozess automatisieren. Um die Konsistenz mit dem Cloud-Abonnement-Account-Erstellungsprozess zu fördern, überprüfen und aktualisieren Sie Ihre Richtlinien regelmäßig. Weitere Informationen finden Sie unter Überprüfen Sie Anforderungsrichtlinien.

Cloud Account Management konfigurieren

Konfigurieren von Cloud Account Management Die Anwendung umfasst eine Reihe erforderlicher Aufgaben, Integrationen und Setups, die abgeschlossen werden müssen, bevor die Erstellung und Bereitstellung eines Service-Accounts initiiert wird.

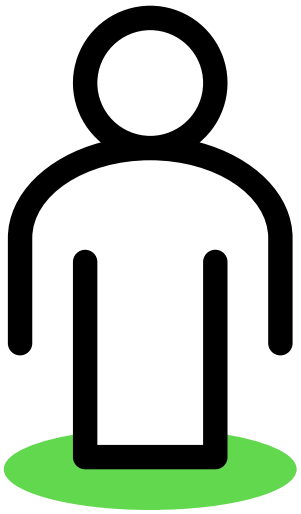
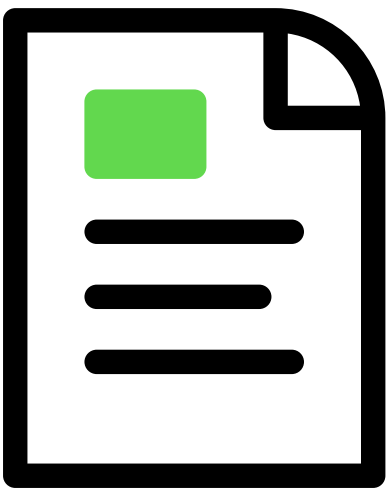
Die beteiligten Schritte unterscheiden sich für AWS Und Azure. Diese Konfigurationen sind in den folgenden Tabellen aufgeführt.

Konfigurationsschritte für AWS

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
1	Richten Sie die Stamm-E-Mail in ein, und überprüfen Sie sie AWS	E-Mail-Administrator	Erstellen Sie einen Account	Keine	E-Mail-Alias	Eine einzelne AD-E-Mail über mehrere hinweg AWS Accounts optimieren die Verwaltung, erhöhen die Sicherheit und fördern die Zusammenarbeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

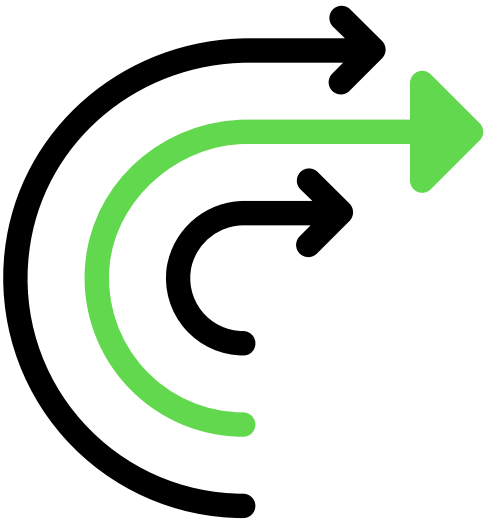
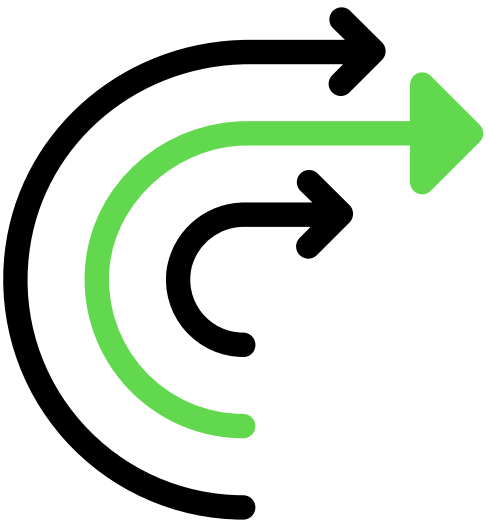
Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
2	 Richten Sie einen Identity Access Manager-Account für ein ein ServiceNow Anwender in AWS	AWS-Administrator	Alle Funktionen	Keine	AWS Zugriffsschlüssel AWS Geheimer Schlüssel	Ein zentralisierter IAM-Anwender im Verwaltungsaccount verwaltet effizient mehrere AWS Accounts über eine CloudFormation Vorlage.
3	 Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet	AWS-Administrator	Kontoaussetzung	Keine	SCP-Richtlinien-ID	Hinzufügen einer Kontonummer zu AWS Die Servicesteuerungsrichtlinie der Organisation blockiert die Erstellung neuer Ressourcen und hilft, Überausgaben zu vermeiden, während vorhandene Ressourcen nicht betroffen bleiben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

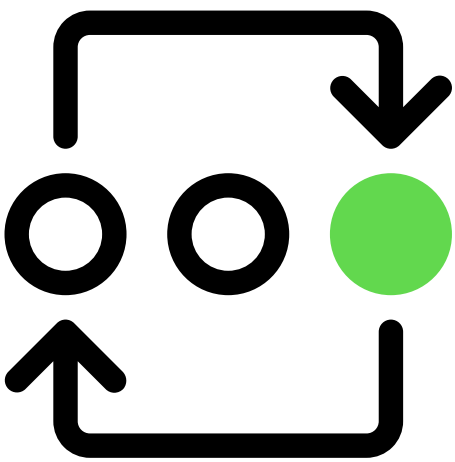
Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
4	 Wird eingerichtet Terraform Und GitHub **Hinweis:** Dieser Schritt ist nicht erforderlich, wenn die native Cloud-Schnittstelle für die Bereitstellung des Accounts verwendet wird.	Terraform-Administrator DevOps-Administrator	Erstellen Sie einen Account für AWS	AWS Zugriffsschlüssel AWS Geheimer Schlüssel Terraform OAuth-Token-ID Terraform Organisation VCS-Bezeichner Terraform-URL	Terraform API-Schlüssel-Token	GitHub-Vorlagen für bereitgestellt Terraform Cloud oder Enterprise optimieren Sie die Kontoerstellung und fördern Sie konsistente Konfigurationen
5	 Erstellen Sie eine Accountkonfiguration für die native Cloud-Schnittstelle **Hinweis:** Dieser Schritt ist nicht erforderlich, wenn Terraform Wird für die Bereitstellung des Accounts verwendet.	ServiceNow AI Platform-Administrator	Erstellen Sie einen Account für die native Cloud-Schnittstelle	Keine	Keine	Für die native Cloud-Schnittstelle ist kein zusätzliches Verfahren erforderlich. Sie können mit fortfahren Cloud-Arbeitsbereich installieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

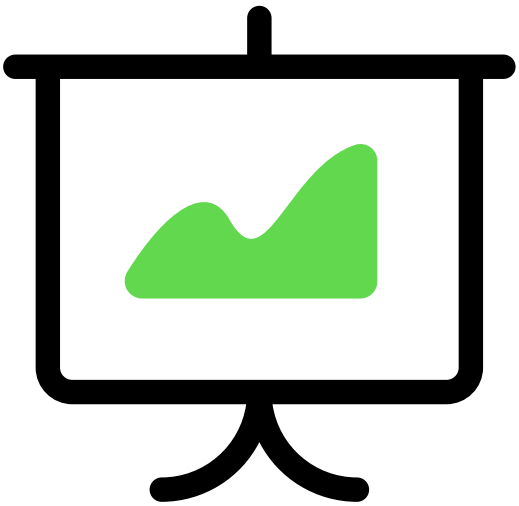
Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
6	 Füllen Sie Aus Cloud Account Management Abhängige Tabellen 1. Erstellen Sie einen Service-Account 2. Definieren Sie den Discovery-Zeitplan, und führen Sie ihn aus	ServiceNow AI Platform Administrator	Alle Funktionen	Discovery Anmeldeinformationen	Cloud-Organisation AWS Organisationseinheit Cloud-Serviceaccount	Cloud-Discovery oder Service Graph Connector für AWS Dient zum Importieren von Cloud-Organisationsstrukturen und zum Erstellen von Abonnementkonten.
7	 Bereitstellungsmodi für Cloud Account Management In Cloud-Arbeitsbereich • Einrichten Terraform API-Schlüssel in ServiceNow • Einrichten AWS API-Konfigurationsinformationen in ServiceNow	ServiceNow AI Platform Administrator	Erstellen Sie einen Account	E-Mail-Alias Terraform Cloud API-Schlüssel-Token Terraform Cloud OAuth-Token-ID Terraform Cloud Organisation VCS-Bezeichner	Keine	Optimieren Sie die Bereitstellung mit flexiblen Modi wie Terraform Und die native Cloud-Schnittstelle zentralisiert die Verwaltung, verbessert die Sicherheit, optimiert die Kosten und verbessert die Governance.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

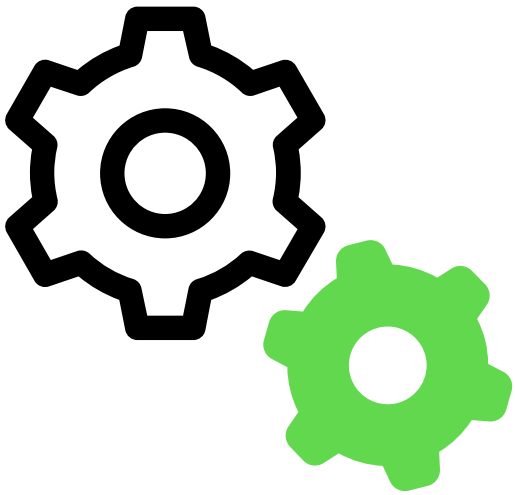
Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
8	 Richten Sie die Scankonfiguration für die Datenvisualisierung ein	ServiceNow AI Platform-Administrator	Visualisierung	Keine	Keine	Die Datenvisualisierung erfordert das Scannen aller Accountverstöße basierend auf dem Richtliniensatz.
9	 Fügen Sie der Gruppe Mitglieder hinzu	ServiceNow AI Platform-Administrator	Alle Funktionen	Keine	Keine	Bestätigen Sie, dass Mitglieder der richtigen Gruppe zugewiesen sind, damit sie den Account-Anforderungs-, Genehmigungs-, Bereitstellungs- und Zertifizierungsprozess ausführen können. Weisen Sie Mitglieder den richtigen Gruppen zu, um die richtigen Berechtigungen zu erhalten, um nicht autorisierten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
						Zugriff zu verhindern und die Sicherheit zu erhöhen.
10	 Konfigurationen werden erstellt	Cloud-Arbeitsbereich-Administrator	Alle Funktionen	Keine	Keine	Konfigurieren Sie die Konfiguration, bevor Sie Accounts erstellen, sperren oder scannen.
11	Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie	Cloud-Arbeitsbereich-Administrator	Alle Funktionen	Keine	Keine	Zertifizieren alle Cloud-Service-Accounts, die nach der Discovery erstellt oder integriert wurden, können zertifiziert werden. Der Administrator kann auch die Standardrichtlinie anpassen oder eine Richtlinie erstellen. Die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

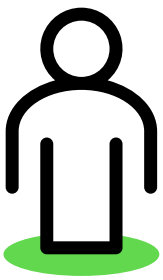
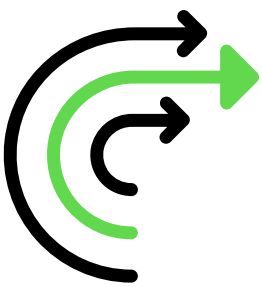
Konfigurationsschritte für AWS (Fortsetzung)

Nei	Aufgabe	Aufgaben	Betroffene Funktion	Eingabe	Ausgabe	Zweck
						Standardrichtlinie hilft, alle verfügbaren Cloud-Service-Accounts einmal alle 90 Tage zu zertifizieren.
12	Überprüfen Sie Anforderungsrichtlinien	Cloud-Arbeitsbereich-Administrator	Alle Funktionen	Keine	Keine	Anforderungsrichtlinien sind Regeln, die das Verhalten von Anforderungs-Workflows steuern, indem Datenprüfungen und -Bedingungen angewendet werden. Durch die regelmäßige Überprüfung und Aktualisierung dieser Richtlinien wird sichergestellt, dass Ihr Cloud-Account-Anforderungsprozess mit dem Verfahren zum Erstellen von Cloud-Abonnement-Accounts konsistent bleibt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschritte für Azure

Nein	Name	Aufgabenverantwortlicher	Betroffene Funktion	Eingabe	Ausgabe	Zweck
1	Konfigurieren Sie die Kontosperrung in Azure	Azure-Administrator	Kontoaussetzung	Keine	OAuth-Client-ID OAuth-Client-Geheimnis Mandanten-ID	Konfigurieren Sie die Berechtigung, und weisen Sie die Berechtigung einem Anwender zu, der den Account aussetzt oder reaktiviert.
2	 Einrichten Azure Service-Prinzipal-Anmeldeinformationen	ServiceNow AI Platform-Administrator	Alle Funktionen	OAuth-Client-ID OAuth-Client-Geheimnis Mandanten-ID	Keine	Geben Sie an Azure Anmeldeinformationen von erhalten Azure Administrator. Diese Anmeldeinformationen werden verwendet, um ein Aussetzungsprofil zu erstellen, und ermöglichen es Ihnen, vorübergehend auszusetzen oder zu beenden Azure Accounts nach Bedarf.
3	 Erstellen Sie eine Accountkonfiguration für die native Cloud-Schnittstelle	ServiceNow AI Platform-Administrator	Erstellen Sie einen Account für die native Cloud-Schnittstelle	Keine	Keine	Für die native Cloud-Schnittstelle ist kein zusätzliches Verfahren erforderlich. Sie können mit fortfahren Cloud-Arbeitsbereich installieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

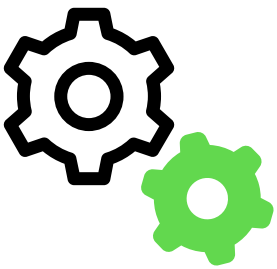
Konfigurationsschritte für Azure (Fortsetzung)

Nein	Name	Aufgabenverantwortlich	Betroffene Funktion	Eingabe	Ausgabe	Zweck
	Hinweis: Dieser Schritt ist nicht erforderlich, wenn Terraform Wird für die Bereitstellung des Accounts verwendet.					
4	Füllen Sie Aus Cloud Account Management Abhängige Tabellen 1. Erstellen Sie einen Service-Account 2. Definieren Sie den Discovery-Zeitplan, und führen Sie ihn aus	ServiceNow AI Platform-Administrator	Alle Funktionen	Discovery Anmeldeinformationen	Cloud-Organisation Azure Verwaltungsgruppe Cloud-Serviceaccount	Cloud-Discovery importieren Sie Cloud-Organisationsstrukturen und erstellen Sie Abonnementkonten.
5	Richten Sie die Scankonfiguration für die Datenvisualisierung ein	ServiceNow AI Platform-Administrator	Visualisierung	Keine	Keine	Die Datenvisualisierung erfordert das Scannen aller Accountverstöße basierend auf dem Richtliniensatz.
6		ServiceNow AI Platform-Administrator	Alle Funktionen	Keine	Keine	Bestätigen Sie, dass Mitglieder der richtigen Gruppe zugewiesen sind, damit sie den Account-Anforderungs-,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschritte für Azure (Fortsetzung)

Nein	Name	Aufgabenverantwortlich	Betroffe Funktion	Eingabe	Ausgabe	Zweck
	Fügen Sie der Gruppe Mitglieder hinzu					Genehmigungs-, Bereitstellungs- und Zertifizierungsprozess ausführen können. Weisen Sie Mitglieder den richtigen Gruppen zu, um die richtigen Berechtigungen zu erhalten, um nicht autorisierten Zugriff zu verhindern und die Sicherheit zu erhöhen.
7	 Konfigurationen werden erstellt	Cloud-Arbeitsbereich-Administrator	Alle Funktionen	Keine	Keine	Konfigurieren Sie die Konfiguration, bevor Sie Accounts erstellen, sperren oder scannen.
8	Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie	Cloud-Arbeitsbereich-Administrator	Alle Funktionen	Keine	Keine	Zertifizieren alle Cloud-Service-Accounts, die nach der Discovery erstellt oder integriert wurden, können zertifiziert werden. Der Administrator kann auch die Standardrichtlinie anpassen oder eine Richtlinie erstellen. Die Standardrichtlinie hilft, alle verfügbaren Cloud-Service-Accounts einmal

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschritte für Azure (Fortsetzung)

Nei	Name	Aufgabenverantwortlich	Betroffe Funktio	Eingabe	Ausgabe	Zweck
						alle 90 Tage zu zertifizieren.

Cloud-Provider werden konfiguriert

Die Themen in diesem Abschnitt behandeln verschiedene Cloud-Konfigurationen, die für die Einrichtung und die Arbeit mit erforderlich sind Cloud Account Management In Cloud-Arbeitsbereich.

Wird eingerichtet AWS Cloud

Dieser Abschnitt behandelt alle Themen, die zum Einrichten erforderlich sind AWS Cloud. Die Themen werden basierend auf der Konfigurationspriorität angeordnet.

Einrichten einer Stamm-E-Mail

Die App erstellt Accounts mit einer eindeutigen Anforderungs-ID und einer Stamm-E-Mail, wodurch eindeutige E-Mails für jeden Account heraufgestuft werden und die Verwaltung vereinfacht wird.

Vorteile des freigegebenen Stamm-E-Mail-Accounts:

- Reduziert den Verwaltungsaufwand: Es sind keine einzelnen E-Mail-Adressen für erforderlich AWS Accounts.
- Zentralisiert Benachrichtigungen: Alle Benachrichtigungen aus dem AWS Account an ein einzelnes Postfach geliefert.
- Verbessert die Zusammenarbeit: Der freigegebene E-Mail-Zugriff ermöglicht es dem DevOps-Team, Aufgaben anzuzeigen und daran zusammenzuarbeiten.

Hinweis: Beachten Sie bei der Bereitstellung eines neuen Abonnementaccounts Folgendes:

1. Die App hängt dynamisch eine Anforderungs-ID (z. B. CWSAREQ0000002) an eine vordefinierte Stamm-E-Mail-Adresse an (`aws-ccoe@mycompany.com`). Dieser Prozess erstellt eine eindeutige E-Mail-Adresse für jeden Account in einem strukturierten Format (`aws-ccoe+CWSAREQ0000002@mycompany.com`).
2. Nachdem der Account bereitgestellt wurde, AWS Sendet E-Mails in diesem Format, die in einem zentralen E-Mail-Account empfangen werden `aws-ccoe@mycompany.com` .

Richten Sie die Stamm-E-Mail in ein, und überprüfen Sie sie AWS

Erstellen Sie eine eindeutige E-Mail-Adresse, um mehrere Accounts zu verwalten. Mehrere Accounts und E-Mails zu haben, kann für eine eine erhebliche Herausforderung darstellen AWS administrator. Eine einzelne AD-E-Mail für mehrere AWS Accounts vereinfachen die Verwaltung.

Vorbereitungen
Erforderliche Rolle: E-Mail/AD-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Erstellen Sie eine E-Mail-Adresse ähnlich wie aws-ccoe@mycompany.com .
2. Senden Sie eine Test-E-Mail von Ihrer E-Mail an aws-ccoe+test@mycompany.com .
3. Bestätigen Sie, dass die Test-E-Mail im empfangen wurde aws-ccoe+test@mycompany.com Postfach.

Nächste Maßnahme

Geben Sie die bestätigte E-Mail-Adresse für den Bereitsteller oder frei ServiceNow AI Platform administrator für Konfigurationszwecke.

Sobald Sie am eine Bestätigungs-E-Mail zur Kontoerstellung erhalten haben aws-ccoe@mycompany.com , Legen Sie die Stamm-Anmeldeinformationen manuell basierend auf den Sicherheitsstandards Ihres Unternehmens fest.

Richten Sie einen Identity Access Manager-Account für ein ein ServiceNow Anwender in AWS

Erstellen Sie einen AWS CloudFormation Identity Access Manager (IAM)-Anwender im Verwaltungsaccount mit der CloudFormation-Vorlage (CFT), damit Sie mehrere verwalten können AWS Accounts mit einem zentralisierten IAM-Anwender.

Vorbereitungen

- Erforderliche Rolle: AWS Administrator
- Die ServiceNow IAM-Anwenderaccount erfordert spezifische AWS IAM-Berechtigungen zum Ausführen grundlegender Vorgänge. Weitere Informationen zu den Berechtigungen finden Sie unter Über Amazon Web Services API-Berechtigungen.

Prozedur

1. Melden Sie sich bei an AWS Verwaltungskonsole und Eingabetaste CloudFormation Wählen Sie es in der Suchleiste aus, und wählen Sie es aus.
2. Wählen Sie in der CloudFormation-Konsole aus **Stapel Erstellen** .

   Ein Stapel ist eine Sammlung von AWS Ressourcen, die Sie als einzelne Einheit verwalten können.

3. Kopieren Sie den CloudFormation-Vorlagencode (CFT) in eine Datei, und speichern Sie die Datei.

   Die Dateierweiterung muss sein .Yml . Beispiel: Erstellt ServiceNowUser.yml .

```
AWSTemplateFormatVersion: '2010-09-09'
Description: This script is executed in Management Account where the  ServiceNow user is
 created.

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: User Credentials
        Parameters:
          - SNUserName
    ParameterLabels:
      SNUserName:
        default: User Name
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Parameters:
  SNUserName:
    Type: String
    Description: User name for CW Service Account user
    MinLength: '6'
    MaxLength: '15'
    ConstraintDescription: The username must be between 6 and 15 characters

Resources:
  SnowCWMemberAccountAccessGroup:
    Type: 'AWS::IAM::Group'
    Properties:
      GroupName: SnowCWMemberAccountAccessGroup

  SnowCWAccountAccessPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: SnowCWAccountAccessPolicy
      PolicyDocument:
        Statement:
          - Sid: ServiceNowCWUserAccess
            Effect: Allow
            Action:
              - 'organizations:ListRoots'
              - 'organizations:ListTagsForResource'
              - 'organizations:DescribeAccount'
              - 'organizations:CreateAccount'
              - 'organizations:ListAWSServiceAccessForOrganization'
              - 'organizations:TagResource'
              - 'organizations:ListAccounts'
              - 'organizations:ListRoots'
              - 'organizations:ListTagsForResource'
              - 'organizations:DescribeAccount'
              - 'organizations:CreateAccount'
              - 'organizations:ListAWSServiceAccessForOrganization'
              - 'organizations:TagResource'
              - 'organizations:ListAccounts'
              - 'organizations:CloseAccount'
              - 'organizations:DescribeOrganization'
              - 'organizations:DescribeOrganizationalUnit'
              - 'organizations:ListParents'
              - 'organizations:ListOrganizationalUnitsForParent'
              - 'organizations:MoveAccount'
              - 'organizations:DescribeCreateAccountStatus'
              - 'organizations:AttachPolicy'
              - 'organizations:DescribePolicy'
              - 'organizations:ListAccounts'
              - 'budgets:CreateBudgetAction'
              - 'budgets:ModifyBudget'
              - 'budgets:ViewBudget'
              - 'budgets:ListTagsForResource'
              - 'iam:GetAccountSummary'
              - 'iam:GetAccountPasswordPolicy'
              - 'budgets:DescribeBudgetAction'
              - 'iam:ListAccountAliases'
              - 'sts:AssumeRole'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            - 'iam:GetRole'
            - 'iam:ListAccountAliases'
            - 'iam:GetAccountPasswordPolicy'
            - 'organizations:DetachPolicy'
            - 'iam:GetAccountAuthorizationDetails'
          Resource: '*'
      Groups:
       - !Ref SnowCWMemberAccountAccessGroup

  CreateServicenowUser:
    Type: 'AWS::IAM::User'
    Properties:
      Path: /
      UserName: !Ref SNUserName
  AddSnowUserToSnowCWMemberAccountAccessGroup:
    Type: 'AWS::IAM::UserToGroupAddition'
    Properties:
      GroupName: SnowCWMemberAccountAccessGroup
      Users:
        - !Ref SNUserName
    DependsOn: CreateServicenowUser

Outputs:
  ServiceNowUserARN:
    Description: ARN of ServiceNow user
    Value: !GetAtt
      - CreateServicenowUser
      - Arn

  ServiceNowUser:
    Description: ServiceNow user
    Value: !Ref SNUserName
```

4. Auf der **Stapel Erstellen** Seite auswählen **Wählen Sie eine vorhandene Vorlage aus** > **Laden Sie eine Vorlagendatei hoch** > **Datei wählen** Um eine Vorlagendatei von Ihrem lokalen Computer auszuwählen.
5. Wählen Sie Aus **Als Nächstes** Um fortzufahren und die Vorlage zu validieren.
6. Auf der **Geben Sie Stapeldetails an** Seite, geben Sie ein `CloudFormation-Stapelname` In **Stapelname** Feld.

   Der Stapelname ist ein Bezeichner, der Ihnen hilft, einen bestimmten Stapel aus einer Liste von Stapeln zu finden. Ein Stapelname darf nur alphanumerische Zeichen (Groß-/Kleinschreibung beachten) und Bindestriche enthalten. Er muss mit einem Buchstaben beginnen und darf nicht länger als 128 Zeichen sein.

7. In **Anwendername** Geben Sie ein Cloud Account Management Anwendername des Service-Accounts.
8. Wählen Sie Aus **Als Nächstes** Um fortzufahren.
9. Auf der **Konfigurieren Sie Stapeloptionen** Wählen Sie Seite aus **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen mit anwenderdefinierten Namen erstellen kann** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Als Nächstes** .
10. Auf der **Überprüfen und erstellen** Seite auswählen **Übermitteln** Um Ihren Stapel zu starten.
    Der IAM-Account wird erstellt.
11. So fügen Sie Sicherheitsanmeldeinformationen hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie Aus **Ressourcen** .

b. Wählen Sie den Anwendernamen-Link aus.

c. Wählen Sie im Abschnitt Zugriffsschlüssel die Option aus **Erstellen Sie einen Zugriffsschlüssel** .

d. Auf der **Greifen Sie auf wichtige Best Practices und Alternativen zu** Seite wählen Sie aus **Drittpartei-Service** Option.

Sie planen, diesen Zugriffsschlüssel zu verwenden, um den Zugriff für eine Drittpartei-Anwendung oder einen Drittpartei-Service zu ermöglichen, die bzw. den überwacht oder verwaltet AWS Ressourcen.

e. Wählen Sie aus **Ich verstehe die obige Empfehlung und möchte mit der Erstellung eines Zugriffsschlüssels fortfahren** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Als Nächstes** .

f. Wählen Sie Aus **Erstellen Sie einen Zugriffsschlüssel** .

g. In **Überprüfen Sie die Zugriffsschlüssel** Seite, laden Sie die Zugriffsschlüsseldatei herunter, und wählen Sie aus **Fertig** .

Hinweis: Geben Sie den Zugriffsschlüssel und den geheimen Schlüssel für den frei Terraform administrator und ServiceNow AI Platform administrator.

Nächste Maßnahme

Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet

Konfigurieren der Servicesteuerungsrichtlinie in AWS

Die AWS der administrator konfiguriert eine Service Control Policy (SCP) und gibt ihre ID für den frei ServiceNow AI Platform administrator für Cloud Account Management Setup. Cloud Account Management Erzwingt den SCP über API-Aufrufe, um die Ressourcenerstellung im Account zu blockieren.

Der Prozess, der zum Erstellen und Verwenden einer Servicesteuerrichtlinie gehört:

1. Die AWS der administrator richtet eine Service Control Policy (SCP) im Verwaltungsaccount ein, indem er eine Liste von Ressourcen aus dem CFT-Skript verwendet. Der Administrator kann diese Liste anpassen, indem er weitere Ressourcentypen hinzufügt.
2. Die AWS der administrator gibt die SCP-ID für den frei ServiceNow administrator, der es während der Registrierung verwendet Cloud Account Management Konfigurationsprozess.
3. Die Cloud Account Management Die App sendet eine Aussetzungsanforderung, die einen API-Aufruf an auslöst AWS Organisationen – API „Richtlinie anhängen“. Diese API erzwingt das SCP, um Anwender daran zu hindern, Ressourcen in diesem Account zu erstellen.

Kopieren Sie den folgenden Inhalt in eine Datei, und speichern Sie die Datei als CloudFormation-Vorlage (Erweiterung als *.cft):

```
AWSTemplateFormatVersion: 2010-09-09
Description: SCP policy for ServiceNow Cloud Workspace to restrict creation of new resources.
Resources:
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
PolicyTestTemplate:
  Type: AWS::Organizations::Policy
  Properties:
    Type: SERVICE_CONTROL_POLICY
    Name: CAM_SCP_SuspendAccount_Policy
    Content:
      Version: 2012-10-17
      Statement:
        - Sid: CAMSCPSuspendAccountPolicy
          Effect: Deny
          Action:
            - 'ec2:RunInstances'
            - 'ec2:CreateVolume'
            - 'ec2:CreateSnapshot'
            - 'ec2:CreateImage'
            - 's3:CreateBucket'
            - 'iam:CreateUser'
            - 'iam:CreateRole'
            - 'iam:CreatePolicy'
            - 'dynamodb:CreateTable'
            - 'sqs:CreateQueue'
            - 'sns:CreateTopic'
            - 'lambda:CreateFunction'
            - 'ec2:CreateVpc'
            - 'ec2:CreateSubnet'
            - 'ec2:CreateInternetGateway'
            - 'ec2:CreateRoute'
            - 'rds:CreateDBInstance'
            - 'redshift:CreateCluster'
          Resource: '*'
```

Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet

Richten Sie eine Einschränkung für die Erstellung von Cloud-Accounts ein. Beispiel: Wenn sich der Accountbesitzer nicht in der Organisation befindet oder Budgetbeschränkungen bestehen. Verwenden Cloud Account Management, Der Administrator fügt die Kontonummer zu hinzu AWS Servicesteuerrichtlinie der Organisation, die vorhandene Accounts heraufstufen, damit sie weiterhin normal funktionieren, während die Erstellung neuer Accounts blockiert wird.

Vorbereitungen

Stellen Sie sicher, dass Sie die CloudFormation-Vorlage gespeichert haben. Weitere Einzelheiten finden Sie unter Konfigurieren der Servicesteuerungsrichtlinie in AWS.

Erforderliche Rolle: AWS Administrator

Prozedur

1. Melden Sie sich bei an AWS Verwaltungskonsole.
2. Geben Sie Ein CloudFormation Wählen Sie es in der Suchleiste aus, und wählen Sie es aus.
3. Wählen Sie in der CloudFormation-Konsole aus **Stapel Erstellen** .
4. Auf der **Stapel Erstellen** Seite auswählen **Wählen Sie eine vorhandene Vorlage aus** > **Laden Sie eine Vorlagendatei hoch** > **Datei wählen** Um eine Vorlagendatei von Ihrem lokalen Computer auszuwählen.
5. Wählen Sie Aus **Als Nächstes** Um fortzufahren und die Vorlage zu validieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Auf der **Geben Sie Stapeldetails an** Seite, geben Sie ein CloudFormation-Stapelname In **Stapelname** Feld.

   Der Stapelname ist ein Bezeichner, der Ihnen hilft, einen bestimmten Stapel aus einer Liste von Stapeln zu finden. Ein Stapelname darf nur alphanumerische Zeichen (Groß-/Kleinschreibung beachten) und Bindestriche enthalten. Er muss mit einem Buchstaben beginnen und darf nicht länger als 128 Zeichen sein.

7. Wählen Sie Aus **Als Nächstes** Und wählen Sie dann aus **Übermitteln** .

Ergebnis

Sobald die CloudFormation-Vorlage (CFT) die Richtlinie erstellt hat, wird ein Amazon-Ressourcenname (ARN) zugewiesen. Ein ARN folgt normalerweise dem folgenden Format:

```
arn:aws:organizations::1234567890:policy/o-99t3h155el/service_control_policy/p-328wg3yb
```

Um den ARN anzuzeigen, wechseln Sie zu **AWS-Organisation** > **Richtlinien** > **Servicekontrollrichtlinien** > **CAM_SCP_SupsendAccount_Policy**an.

Das Schlüsselelement, das Sie für bereitstellen müssen ServiceNow AI Platform administrator ist das Richtlinienelement, das in diesem Beispiel lautet: p-328wg3yb.

Nächste Maßnahme

Bereitstellungsmodi für Cloud Account Management In Cloud-Arbeitsbereich

Bereitstellungsmodi für Cloud Account Management In Cloud-Arbeitsbereich

Cloud Account Management In Cloud-Arbeitsbereich Bietet flexible Bereitstellungsmodi wie Terraform Und native Cloud-Schnittstellen bei gleichzeitiger Zentralisierung der Verwaltung, Verbesserung der Sicherheit, Kostenoptimierung und Verbesserung der Governance.

Übersicht über Bereitstellungsmodi

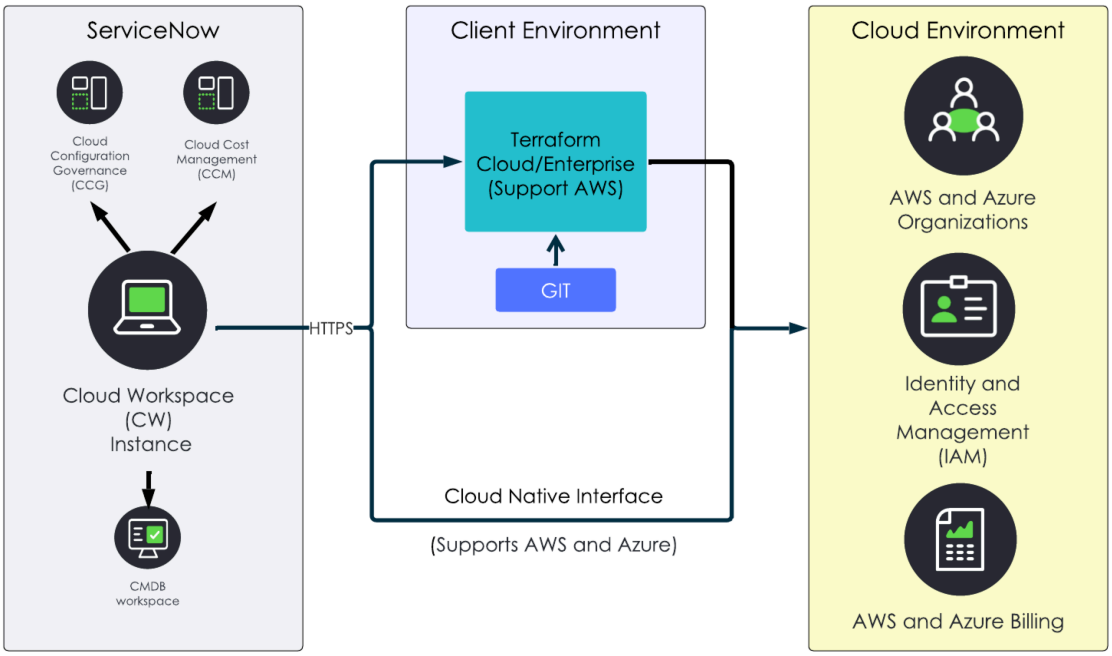
Bereitstellungsmodi zum Erstellen AWS Accounts sind:

- Terraform– Wird eingerichtet Terraform Und GitHub.
- Native Cloud-Schnittstelle: Für die native Cloud-Schnittstelle ist kein zusätzliches Verfahren erforderlich. Sie können mit fortfahren Cloud-Arbeitsbereich installieren.

  Hinweis: Weitere Informationen zu API-Berechtigungen finden Sie unter Über Amazon Web Services API-Berechtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Bereitstellungsmodi



Wird eingerichtet Terraform Und GitHub

Vereinfachen Sie die Cloud-Account-Bereitstellung mit Terraform. Der Workflow bietet die grundlegenden Schritte für die Einrichtung Terraform Und GitHub.

Veröffentlichen Terraform Vorlagen

Veröffentlichen Sie Terraform Von der Anwendung in definierte Vorlage GitHub Zum Aktivieren der Versionssteuerung, Zusammenarbeit und zentralisierten Speicher.

Vorbereitungen

Erforderliche Rolle: Terraform Administrator

Prozedur

1. Erstellen Sie einen GitHub Repository, das für Ihren bestimmt ist Terraform Vorlagen.
2. Speichern Sie die folgenden Codes in einer separaten Datei.
   - Dateiname: Awsaccount.tf

```
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = "~>5.0"
    }
  }
}

provider "aws" {
  region = var.region
}

resource "aws_organizations_account" "account" {
  email = var.root_email
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  name = var.account_name
  tags = var.tags
  parent_id = var.parent_id
  close_on_deletion=var.close_delete
  create_govcloud=var.gov_cloud
}

resource "aws_budgets_budget" "cost" {
  name  = join("-", ["SN-CAM-Monthly-Budget", aws_organizations_account.account.id])
  count = var.monthly_budget > 0 ? 1 : 0
  budget_type  = "COST"
  limit_amount = var.monthly_budget
  limit_unit   = "USD"
  time_unit    = "MONTHLY"

  cost_filter {
    name = "LinkedAccount"
    values = [
      aws_organizations_account.account.id
    ]
  }

  notification {
    comparison_operator       = "GREATER_THAN"
    threshold                 = 100
    threshold_type            = "PERCENTAGE"
    notification_type         = "FORECASTED"
    subscriber_email_addresses = [var.root_email, var.notification_email]
  }

  notification {
    comparison_operator       = "GREATER_THAN"
    threshold                 = 85
    threshold_type            = "PERCENTAGE"
    notification_type         = "ACTUAL"
    subscriber_email_addresses = [var.root_email, var.notification_email]
  }

  notification {
    comparison_operator       = "GREATER_THAN"
    threshold                 = 100
    threshold_type            = "PERCENTAGE"
    notification_type         = "ACTUAL"
    subscriber_email_addresses = [var.root_email, var.notification_email]
  }
}
```

- Dateiname: Variables.tf

```
variable "region" {
  type = string
  default = "us-east-1"
}

variable "account_name" {
  type = string
  description = "(Required) Account Name"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}

variable "root_email" {
  type = string
  description = "(Required) Account Email"
}

variable tags{
  type = map(string)
  description = "(Required) Tags for the resource"
}

variable "close_delete" {
  type = bool
  description = "Close Account on deletion"
  default = true
}

variable "gov_cloud" {
  type = bool
  description = "Gov Cloud Account"
  default = false
}

variable "parent_id" {
  type = string
  description = "(Required) Account Parent Organizational Unit"
}

variable monthly_budget {
  type = number
  default = 0
}

variable notification_email {
  type = string
  description = "Additional email where Budget Notifications are to be sent"
}
```

3. Drücken Sie Terraform Dateien im Remote-Repository.
4. Notieren Sie sich den Standort oder die URL, nachdem die Vorlage in gespeichert wurde GitHub.

Diese Vorlage wird dann in referenziert Terraform Cloud Und ServiceNow Instanz zur Automatisierung der Erstellung eines Abonnementaccounts.

Wichtig:

Ändern Sie die Vorlage nicht, da die Variablen eng mit der Anwendung verbunden sind.

Erstellen Sie einen Terraform Organisation für Cloud Account Management In Cloud-Arbeitsbereich

Integrieren Sie mit Terraform Cloud/ Terraform Enterprise Um Accounts zu organisieren, definieren Sie Workflows, erzwingen Sie die Sicherheit, verbessern Sie die Zusammenarbeit und verbessern Sie die Skalierbarkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Terraform Administrator

Für dieses Setup erforderliche Attribute:

- AWS Zugriffsschlüssel
- AWS Geheimer Schlüssel

Stellen Sie sicher, dass Sie Zugriff auf haben Terraform Cloud Oder Terraform Enterprise Um das folgende Verfahren auszuführen.

Prozedur

1. Melden Sie sich an, und navigieren Sie zu Terraform Cloud (`https://app.terraform.io/session`) Oder Terraform Enterprise-Portal (`https://<tfe_server_url>/api/v1`).
2. Wählen Sie den Anwendernamen oder Organisationsnamen aus.
3. Geben Sie im modalen Fenster einen eindeutigen Organisationsnamen und andere Details ein.
4. Wählen Sie Aus **Erstellen Sie Eine Organisation** .

   Hinweis:

   - Nachdem eine neue Organisation erstellt wurde, erhalten Sie eine Bestätigung innerhalb der Plattform. Sie können Ihre Organisationseinstellungen verwalten, Mitglieder hinzufügen und Arbeitsbereiche in Ihrer neu erstellten Organisation konfigurieren.
   - Um den Beamten anzuzeigen Terraform Dokumentation:
     - Terraform Cloud: https://developer.hashicorp.com/terraform/cloud-docs/users-teams-organizations/organizations
     - Terraform Unternehmen: https://developer.hashicorp.com/terraform/cloud-docs/users-teams-organizations/organizations
5. In Terraform Organisation, navigieren Sie zu **Einstellungen** > **Variablensatz** > **Erstellen Sie einen Variablensatz**an.

   Ein Variablensatz ist eine Sammlung von Variablen, die in mehreren Arbeitsbereichen gemeinsam genutzt werden können.
6. Geben Sie einen beschreibenden Namen wie an AWS Anmeldeinformationen.
7. Wählen Sie den entsprechenden Bereich (Organisation oder Arbeitsbereich) aus.
8. Erstellen Sie zwei Variablensätze in **Variablen** Abschnitt wie folgt:
   - Schlüssel: AWS_ACCESS_KEY_ID und Wert: <AWS Access key>
   - Schlüssel: AWS_SECRET_ACCESS_KEY und Wert: <geheimer AWS-Schlüssel>

     Hinweis: Wählen Sie als aus **Vertraulich** Um die Sichtbarkeit von Anmeldeinformationen auf nicht autorisiertes Personal mit zu beschränken Terraform Zugriff.

   Weitere Informationen zu Variablensätzen finden Sie unter https://developer.hashicorp.com/terraform/tutorials/cloud-get-started/cloud-create-variable-set# .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terraform Cloud mit GitHub integrieren

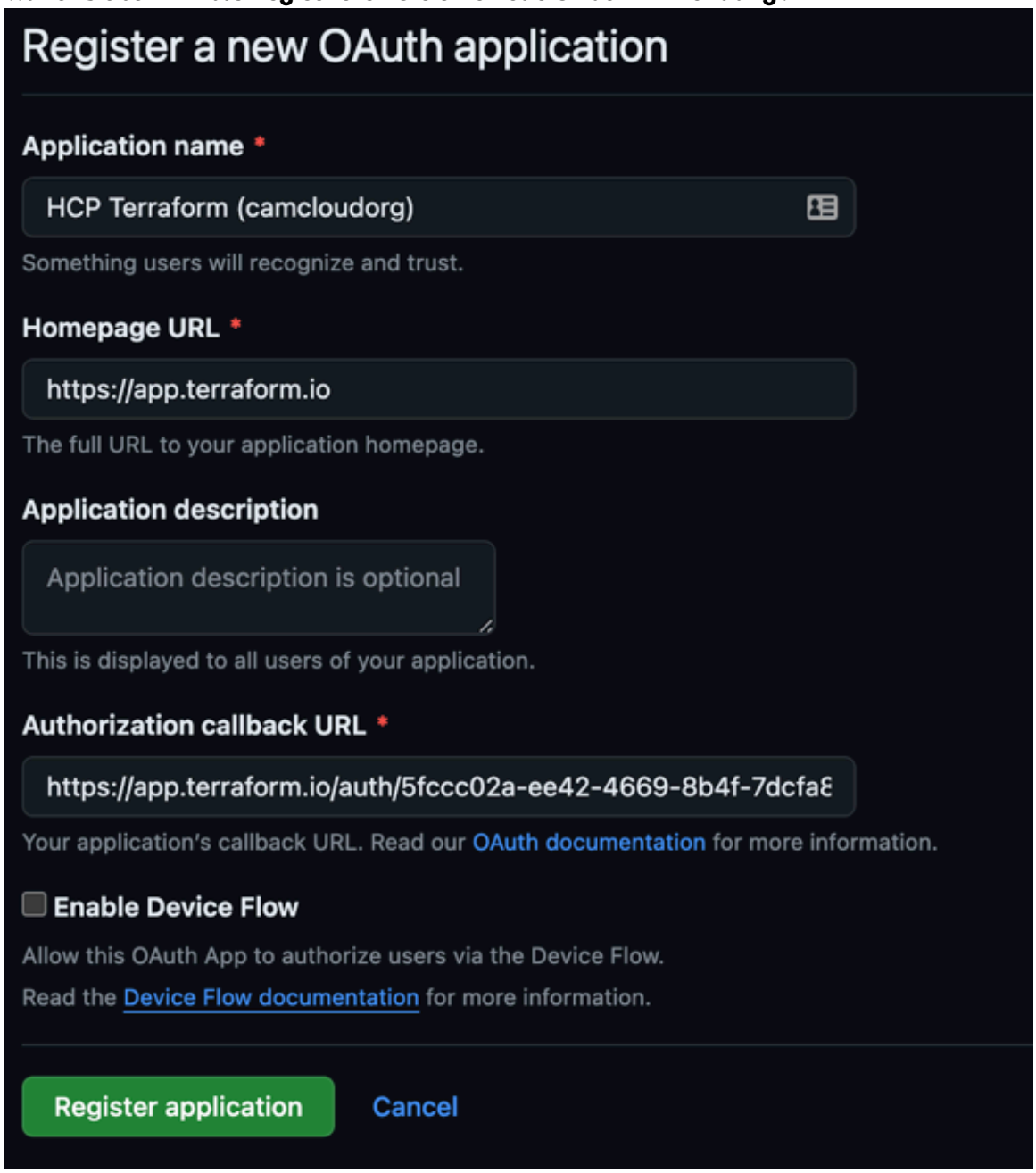
Integrieren GitHub Mit Terraform Dient zum Verknüpfen von Arbeitsbereichen mit Repositorys, um Versionssteuerung, Change-Nachverfolgung und Rollbacks zu aktivieren.

Vorbereitungen

Erforderliche Rolle: Terraform administrator oder DevOps-Teammitglied

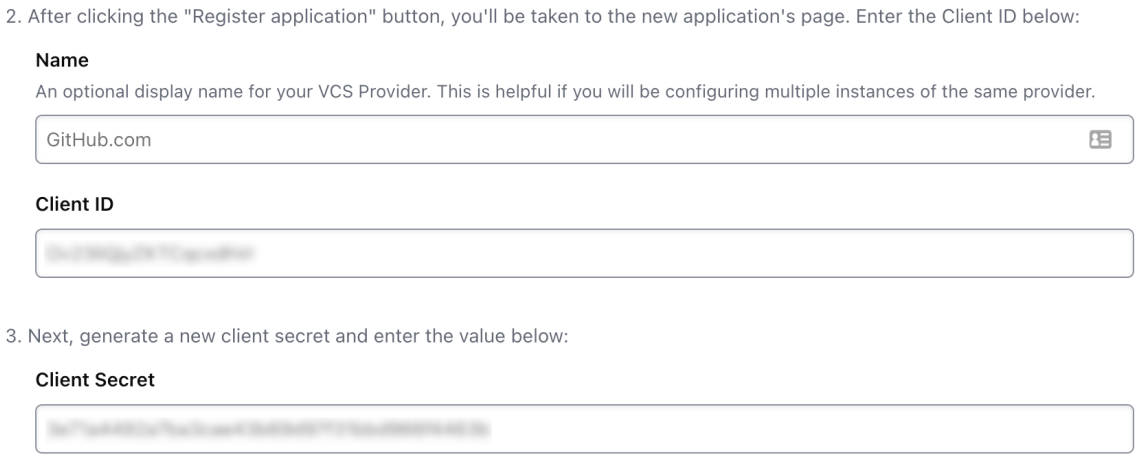
Prozedur

1. Wechseln Sie zu Terraform Organisation, die für diese Anwendung erstellt wurde.
2. Navigieren zu **Einstellungen** > **Anbieter**an.
3. Wählen Sie Aus **Fügen Sie einen VCS-Anbieter hinzu** .
4. Von GitHub Dropdown-Liste wählen Sie eine aus **GitHub.com (anwenderdefiniert)** .
5. Wählen Sie den Link aus **Registrieren Sie eine neue OAuth-Anwendung** .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie Aus **Anwendung registrieren** .
7. Kopieren Sie die Client-ID.
8. Wählen Sie Aus **Generieren Sie ein neues geheimes Clientgeheimnis** Und kopieren Sie das generierte Client-Geheimnis.
9. Kehren Sie zurück zu Terraform Konsole, in der **Fügen Sie einen VCS-Anbieter hinzu** Die Seite ist geöffnet, und fügen Sie sowohl die Client-ID als auch das geheime Client-Geheimnis ein.



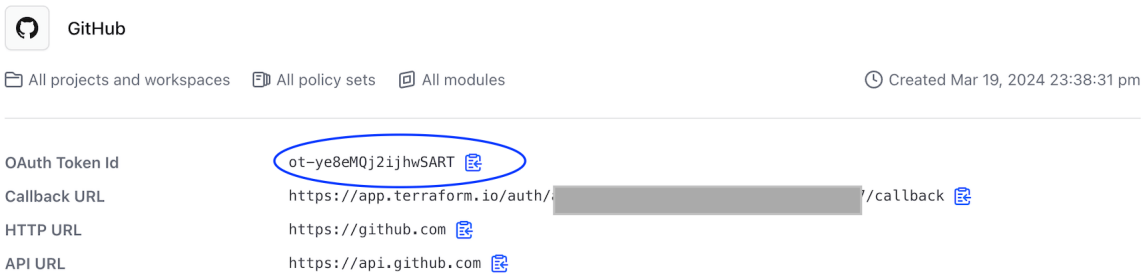
10. Wählen Sie Aus **Verbinden und fortfahren** .
11. Wählen Sie Aus **Autorisieren** .

> **Hinweis:** Befolgen Sie die plattformspezifischen Anweisungen, um zu autorisieren Terraform Cloud Um auf zuzugreifen GitHub Repository.
>
> Weitere Informationen finden Sie in der offiziellen Dokumentation: https://developer.hashicorp.com/terraform/cloud-docs/vcs/Github-enterprise .

12. Auf der **Erweiterte Einstellungen** Seite auswählen **Überspringen und beenden** .

Nächste Maßnahme

Notieren Sie sich die OAuth-Token-ID, und geben Sie sie für den frei ServiceNow administrator.



Erstellen Terraform API-Token

Das Generieren von API-Token mit eingeschränkten Berechtigungen erhöht die Sicherheit, ermöglicht eine feingranulierte Steuerung, erleichtert die Automatisierung und bietet temporären Zugriff in Ihrem Terraform Organisation.

Vorbereitungen

Erforderliche Rolle: Terraform Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei an Terraform Konsole.
2. Wählen Sie Aus **Account-Einstellungen** Aus dem Anwenderprofil.
3. Wählen Sie Aus **Token** Und wählen Sie dann aus **Erstellen Sie ein API-Token** .
4. Geben Sie Ein **Beschreibung** .
5. Legen Sie fest **Ablauf** Datum.

   Hinweis: Das Ablaufdatum sollte den Sicherheitsstandards Ihres Unternehmens entsprechen.

6. Wählen Sie Aus **Token generieren** .
7. Geben Sie die folgenden Details für den frei ServiceNow administrator, der in registriert werden soll ServiceNow Instanz:
   - VCS-Bezeichner oder GitHub Repository-Speicherort, in dem Sie gespeichert haben Terraform Vorlage, z. B.: `https://github.com/<your_repository>/Cam-create-aws-Account` .
   - Terraform Organisationsname
   - Terraform OAuth-Token-ID
   - Terraform API-Schlüssel-Token
   - Terraform-URL

Nächste Maßnahme

Cloud Account Management in Cloud-Arbeitsbereich einrichten

Fügen Sie der Gruppe Mitglieder hinzu

Einrichten Terraform API-Schlüssel in ServiceNow.

Richten Sie die Scankonfiguration für die Datenvisualisierung ein.

Wird eingerichtet Azure Cloud

Dieser Abschnitt behandelt alle Themen, die zum Einrichten erforderlich sind Azure Cloud. Die Themen sind in der Reihenfolge der Konfigurationspriorität angeordnet.

Konfigurieren Sie die Kontosperrung in Azure

Verwalten Sie einen Azure Abonnement mit der Berechtigung und durch Zuweisung der Rolle an einen Anwender. Die Rolle muss über die Berechtigung zum Ausführen der APIs zum Anhalten und erneuten Aktivieren von verfügen Azure Account.

Vorbereitungen

Erforderliche Rolle: Azure Administrator

Prozedur

1. Melden Sie sich bei an Azure Organisation.
2. Suchen und auswählen **Verwaltungsgruppen** .
3. Wählen Sie Aus **Mandanten-Stammgruppe** .
4. Auswahlvorgang **Zugriffssteuerung** > **Rollen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie Aus **Hinzufügen** Und wählen Sie dann aus **Fügen Sie eine anwenderdefinierte Rolle hinzu** .
6. In **Name der anwenderdefinierten Rolle** Feld einen Namen für die anwenderdefinierte Rolle angeben. Der Name muss für das Microsoft Entra-Verzeichnis eindeutig sein.
7. Wählen Sie **Weiter**.
8. Auf der **Berechtigungen** Wählen Sie die Registerkarte aus **Als Nächstes** .
9. Auf der **Zuweisbare Bereiche** Auf der Registerkarte geben Sie an, wo Ihre anwenderdefinierte Rolle für die Zuweisung verfügbar ist, z. B. Verwaltungsgruppe, Abonnements oder Ressourcengruppen.
10. Wählen Sie Zuweisbare Bereiche hinzufügen, um den Bereich Zuweisbare Bereiche hinzufügen zu öffnen.
11. Auf der **JSON** Fügen Sie den folgenden Code ein:

```
{
   "properties": {
      "roleName": "Policy Lock/Unlock Manager",
      "description": "Allows locking and unlocking Azure Policy assignments at management
 group level",
      "assignableScopes": [
         "/providers/Microsoft.Management/managementGroups/<ManagementGroupId>"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.Authorization/policyAssignments/write",
               "Microsoft.Authorization/policyAssignments/delete",
               "Microsoft.Authorization/policyAssignments/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
         }
      ]
   }
}
```

12. Wählen Sie Aus **Als Nächstes** Und wählen Sie dann aus **Erstellen** .

Nächste Maßnahme

Sie müssen die Berechtigung einer Rolle zuweisen. Weitere Informationen finden Sie unter https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal .

Konfigurieren Sie eine Sperr-/Entsperrungsrichtlinie. Weitere Informationen finden Sie unter Richten Sie die Aussetzung eines Abonnements mit ein Azure Richtlinie.

Einrichten Azure Service-Prinzipal-Anmeldeinformationen

Geben Sie an Azure Anmeldeinformationen von erhalten Azure Administrator. Diese Anmeldeinformationen werden verwendet, um ein Aussetzungsprofil zu erstellen, und ermöglichen es Ihnen, vorübergehend auszusetzen oder zu beenden Azure Accounts nach Bedarf.

Vorbereitungen

Überprüfen Sie Berechtigungen erforderlich für Azure Service-Prinzipal Thema vor dem Erstellen von Azure Service-Prinzipal-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: ServiceNow AI Platform Administrator

Prozedur

1. Melden Sie sich bei an ServiceNow Instanz.
2. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
3. Wählen Sie in der Liste aus **Azure-Service-Prinzipal** .
4. In **Verbindungen Und Anmeldeinformationen** Formular: Geben Sie die folgenden Informationen an.

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: Azure service principal credentials.
Mandanten-ID	Azure Verzeichnis-ID-Wert aus der Textdatei.
Client-ID	Azure Anwendungs-ID-Wert aus der Textdatei.
Geheimer Schlüssel	Azure Anwendungsschlüsselwert aus der Textdatei.
Anmeldeinformationsalias	Der Anmeldeinformationsalias, den Sie mit den OAuth 2,0-Anmeldeinformationen verknüpfen möchten. Verwenden Sie standardmäßig den vordefinierten Aliasnamen: sn_itom_Cam.CAM_Azure_Connection

5. In **API-Schlüssel** Geben Sie den vom Administrator erhaltenen Schlüssel ein.
6. Um den Prozess abzuschließen, wählen Sie aus **Übermitteln** .

Richten Sie die Aussetzung eines Abonnements mit ein Azure Richtlinie

Erstellen Sie die Richtlinie auf Stammebene, um eine zu sperren oder zu entsperren Azure Account. Als Azure Administrator, sperren Sie einen Azure Abonnement, Ressourcengruppe oder Ressource, um versehentliche Löschungen und Änderungen zu vermeiden.

Vorbereitungen

Stellen Sie sicher, dass Sie die Berechtigung bereits konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren Sie die Kontosperrung in Azure.

Erforderliche Rolle: Azure Administrator

Prozedur

1. Melden Sie sich bei an Azure Organisation.
2. Suchen und wählen Sie aus **Anwender** .
3. Wählen Sie in der Liste Anwendername einen Anwender aus.
4. Wählen Sie im Navigationsbereich aus **Zugewiesene Rollen** .
5. Fügen Sie unter Administrative Rollen die hinzu **Globaler Administrator** Rolle durch Auswahl **Fügen Sie Zuweisungen Hinzu** .
6. Geben Sie Ein Microsoft Entra-ID Wählen Sie im Suchfeld aus **Microsoft Entra ID** > **Eigenschaften**an.
7. Unter **Zugriffsmanagement für Azure-Ressourcen** , Legen Sie den Umschalter auf fest **Ja** .
   Mit dieser Option können Sie den Zugriff auf alle verwalten Azure Abonnements und Verwaltungsgruppen in diesem Mandanten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Suchen und wählen Sie aus **Richtlinie** .
9. Wählen Sie Aus **+ Richtliniendefinition** .
10. Geben Sie Folgendes ein:
    a. Wählen Sie die Mandantenstammgruppe mithilfe der Ellipsen in aus **Definitionsspeicherort** .

       Sie können entweder eine Verwaltungsgruppe oder ein Abonnement auswählen. Wenn Sie die Mandantenstammgruppe auswählen, können auch alle untergeordneten Abonnements verwaltet werden.

    b. Geben Sie den Namen der Richtliniendefinition ein. Beispiel: LockAccount_Policy.
    c. Die Beschreibung, was die Richtliniendefinition tun soll.
    d. Kopieren Sie unter RICHTLINIENREGEL den folgenden JSON-Code:

```
{
  "properties": {
    "displayName": "CAM_LockAccount_Policy",
    "policyType": "Custom",
    "mode": "All",
    "description": "Blocks the creation of resources and configurations that fall under
Azure Policy enforcement.",
    "parameters": {
      "allowedResourceTypes": {
        "type": "Array",
        "metadata": {
          "displayName": "Allowed Resource Types",
          "description": "List of resource types that are allowed for creation. Any
resource type not listed here will be blocked.",
          "strongType": "resourceTypes"
        },
        "defaultValue": []
      },
      "allowedLocations": {
        "type": "Array",
        "metadata": {
          "displayName": "Allowed Locations",
          "description": "List of allowed Azure regions for resource creation."
        },
        "defaultValue": []
      },
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "The effect determines what happens when the policy rule is
evaluated to match"
        },
        "allowedValues": [
          "Audit",
          "Deny",
          "Disabled"
        ],
        "defaultValue": "Deny"
      }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    },
    "policyRule": {
      "if": {
        "anyOf": [
          {
            "not": {
              "field": "type",
              "in": "[parameters('allowedResourceTypes')]"
            }
          },
          {
            "not": {
              "field": "location",
              "in": "[parameters('allowedLocations')]"
            }
          }
        ]
      },
      "then": {
        "effect": "[parameters('effect')]"
      }
    }
  }
}
```

e. Wählen Sie **Speichern**.

Hinweis: Um zu überprüfen, ob die Richtlinie erstellt wurde, wechseln Sie zu PolicyDefinitions. Ändern Sie den Filterbereich und den Richtlinientyp, um die Richtlinie zu finden.

f. Wählen Sie den Richtliniennamen aus, und kopieren Sie **Definitions-ID** .

Hinweis: Diese Definitions-ID ist erforderlich, wenn Sie Erstellen Sie eine Konfiguration zum Sperren des Accounts.

Nächste Maßnahme

Cloud Account Management in Cloud-Arbeitsbereich einrichten

Fügen Sie der Gruppe Mitglieder hinzu

Einrichten Azure Verbindung

Richten Sie die Scankonfiguration für die Datenvisualisierung ein

Cloud Account Management in Cloud-Arbeitsbereich einrichten

In diesem Abschnitt werden alle allgemeinen Themen behandelt, die für die Einrichtung erforderlich sind Cloud Account Management. Die Themen sind in der Reihenfolge der Konfigurationspriorität angeordnet.

Cloud-Arbeitsbereich installieren

Sie können installieren Cloud-Arbeitsbereich Anwendung (sn_itom_Cam), wenn Sie die Administratorrolle innehaben. Die Anwendung enthält Demodaten und installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie Cloud-Account-Management Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Rollen Werden mit installiert Cloud-Arbeitsbereich.

Weitere Informationen finden Sie unter In Cloud-Account-Management installierte Plugins .

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Cloud-Arbeitsbereich Anwendung (sn_itom_Cam) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben **Installieren** Schaltfläche, werden die verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind die Beispieldatensätze, die Anwendungsfunktionen für allgemeine Anwendungsfälle beschreiben. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.
6. Wählen Sie **Installieren** aus.

Füllen Sie Aus Cloud Account Management Abhängige Tabellen

Geben Sie die erforderlichen Informationen für die Erstellung und Bereitstellung von Cloud-Accounts an.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fügen Sie Umgebungselemente hinzu, um Cloud-Accounts basierend auf mehreren Umgebungen zu kategorisieren.

   a. Navigieren Sie zu **Alle** Und suchen Sie nach `sys_choice.LIST` .

   b. Wählen Sie auf der Auswahlseite aus **Element** Geben Sie aus der Dropdown-Liste ein `Umgebung` Im Suchfeld.

   c. Wenn Umgebungselemente, die Sie verwenden möchten, nicht vorhanden sind, erstellen Sie sie.

      i. Wählen Sie **Neu**.

      ii. Füllen Sie im Formular die erforderlichen Felder aus.

      Auswahlformular „neuer Datensatz“

Feld	Wert
Tabelle	Auswahltabelle [sys_choice]
Element	`Umgebung` (Groß-/Kleinschreibung beachten)
Bezeichnung	Der Name für die Umgebung, die auf der Anforderungsseite des Cloud-Accounts angezeigt werden soll, z. B. Produktion.
Wert	Derselbe Wert wie die Bezeichnung.

      iii. Wählen Sie **Absenden**.

2. Füllen Sie die verbleibenden Tabellen aus.

   a. Navigieren Sie zu **Alle** Und suchen Sie nach dem Tabellennamen.

   b. Fügen Sie die relevanten Informationen hinzu.

Tabellenname	Beschreibung
Umgebung (sys_choice)	Enthält übersetzten Text für Optionen, die in Listen angezeigt werden.
Kostenstelle (cmn_Cost_Center)	Enthält häufig verwendete Referenz zwischen Finanzsystemen und IT. Kostenstellendatensätze stellen Geschäftsentitäten dar und verfügen über eine zugehörige Liste von CI-Kostenstellen-Beziehungen, die den Verbrauch von Business-Services durch die Kostenstelle messen.
Geschäftsbereich (Business_unit)	Enthält Informationen zu den Geschäftsbereichen in Ihrer Organisation, einschließlich Funktionen wie Finanzen, HR oder IT.
Abteilung (cmn_Department)	Enthält die Namen der Abteilungen in Ihrer Organisation.
Systemanwender (sys_user)	Enthält Anwenderinformationen für die ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Service-Account

Erstellen Sie in einen Service-Account CAM. Ein Service-Account enthält die Anmeldeinformationen und Accountinformationen, die Sie in Ihrem Provider-Account erstellt haben. Discovery verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen und dann Informationen zu jedem logischen Rechenzentrum zu erhalten, das dem Account zugeordnet ist.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Service-Konten**an.
2. Füllen Sie die Felder aus.
   Weitere Informationen finden Sie unter Formular für Cloud-Servicekonto.
3. Wählen Sie **Absenden**.

Definieren Sie den Discovery-Zeitplan, und führen Sie ihn aus

Der Discovery-Zeitplan ist der Kontrollpunkt für die Ausführung von Erkennungen. Der Zeitplan steuert, wann die Discovery ausgeführt wird, definiert den zu verwendenden MID-Server, den Typ der Discovery, die ausgeführt werden soll, und die abzufragenden IP-Adressen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.

   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Discovery-Zeitpläne**an.
3. Wählen Sie Aus **Fügen Sie Einen Neuen Zeitplan Hinzu** .
4. Geben Sie die Details ein (indem Sie den Anbieter auswählen).

   Weitere Informationen zu den Felddetails finden Sie unter Erstellen Sie einen neuen Discovery-Zeitplan-Formularreferenz.

   Wenn das System keinen entsprechenden MID-Server erkennen kann, werden Sie aufgefordert, einen MID-Server zu konfigurieren.
5. Wählen Sie **Weiter**.

   Nachdem der Zeitplan ausgeführt wurde, erkennt das System Ressourcen aus den Organisations- und Organisationseinheiten, die mit dem AWS-Account oder den Azure-Mandanten und Verwaltungsgruppen verknüpft sind. Die Details werden in den folgenden Tabellen ausgefüllt:

   - cmdb_ci_Cloud_org_list.do
   - Für AWS: cmdb_ci_aws_org_unit_list.do
   - Für Azure: cmdb_ci_Azure_Management_Group

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Anwendungsservice für Cloud Account Management

Erstellen Sie einen Anwendungsservice, um die Organisation, Wartung und Überwachung von Services in Ihrer Organisation zu standardisieren.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Anwendungsservices**an.
2. Wählen Sie **Neu**.
3. In **Grundlegende Details** Geben Sie einen ein Name .
   Dieser Name wird im Account-Anforderungsformular angezeigt, sobald Sie die Umgebung ausgewählt haben.
4. Wählen Sie Aus **Umgebung** Aus der Dropdown-Liste.
   Die ausgewählte Umgebung wird dem Anwendungsservice zugeordnet.
5. Wählen Sie **Weiter**.
6. Auswahlvorgang **Weiter** > **Fertig**an.
   Ein Anwendungsservice wurde erfolgreich erstellt.

Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie

Überprüfen Sie die standardmäßige Zertifizierungsrichtlinie, die in bereitgestellt wird Cloud Account Management Dient zur Validierung von Daten anhand des Richtliniensatzes. Diese Standardrichtlinie zertifiziert alle 90 Tage alle verfügbaren Cloud-Service-Accounts. Administratoren können die Standardrichtlinie anpassen oder nach Bedarf eine erstellen.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Account-Zertifizierung**an.

   Das Richtlinien-Dashboard wird in geöffnet CMDB Arbeitsbereich, der vorhandene Richtlinien unter anzeigt **Veröffentlichte Richtlinien** Abschnitt.

2. Auswahlvorgang **CW-Zertifizierungsrichtlinie** > **Richtlinie anzeigen** Dient zum Überprüfen der Richtliniendetails.
3. Informationen zum Erstellen oder Anpassen einer Richtlinie finden Sie unter Erstellen Sie eine CMDB-Datenmanager-Richtlinie .

Hinweis:

- Wählen Sie aus, um die Datenvalidierung anzuhalten oder eine Richtlinie zu bearbeiten **Deaktivieren Sie Die Richtlinie** .
- Nachdem die Richtlinie ausgeführt wurde, zeigen Sie Aufgaben an, indem Sie auswählen **Meine Arbeit** Registerkarte.
- Sobald die Aufgaben dem zugewiesen wurden Cloud Account Management Zertifizierungsgruppe, ermöglicht es Zertifizierern, schreibgeschützte Felder zu überprüfen und die Felder zu ändern, die sie bearbeiten dürfen.
- Informationen zum Zertifizieren eines Accounts finden Sie unter Zertifizieren Sie einen Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Überprüfen Sie Anforderungsrichtlinien

Konfigurieren Sie einen anwenderdefinierten Namen für Cloud Account Management

Konfigurieren Sie einen anwenderdefinierten Namen für Cloud Account Management. Sie können optional ein neues Branding für durchführen Cloud Account Management Mit Ihrem Unternehmen oder einem beliebigen anwenderdefinierten Namen. Die Namensänderung gilt nur für Cloud Account Management Homepage und Navigation.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Now-Experience-Framework** > **Erfahrungen**an.
2. Suchen Sie in der Liste der Titel nach Cloud Account Management Und doppelklicken Sie auf den Namen, um die Änderung vorzunehmen.
3. Geben Sie einen anwenderdefinierten Namen ein, und wählen Sie die Prüfung aus Markieren.
4. Melden Sie sich erneut an, um die Änderung anzuzeigen.

Erstellen Sie einen Variablensatz für den Cloud-Account-Katalog anfordern

Passen Sie den Cloud-Account-Katalog anfordern an, indem Sie Variablensätze erstellen oder bearbeiten. Ein Variablensatz gruppiert zugehörige Variablen in einer einzelnen, wiederverwendbaren Sammlung. Wählen Sie nur die erforderlichen Variablen für bestimmte Cloud-Account-Anforderungen aus, um einen optimierten und einheitlichen Prozess sicherzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich**an.
2. Geben Sie Ein `sc_Cat_item.LIST` Im Navigationsfilter.
3. Suchen Sie in der Tabelle „sc_Cat_item.LIST“ nach , und klicken Sie auf `Request Cloud Account`Eigenschaft.
4. Klicken Sie auf **Variablensätze** Registerkarte und klicken Sie auf **Neu** .
   Der Bildschirm „Variablensatz“ wird angezeigt.
5. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Titel	Eindeutiger Name für den Variablensatz.
Interner Name	(Eindeutiger) Name des Variablensatzes für die interne Verwendung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn dieses Feld leer ist, wird sein Wert basierend auf dem Feld **Titel** für alle Variablentypen mit Ausnahme von Bruch, Containeraufteilung und Container-Ende automatisch ausgefüllt.
Layout	Für das Layout werden folgende Auswahlmöglichkeiten angezeigt: **1 Spalte breit**, **2 Spalten breit, wechselnde Seiten** oder **2 Spalten breit, eine Seite, dann die andere**.
Reihenfolge	Reihenfolgennummer für den Variablensatz.
Beschreibung	Beschreibung des Variablensatzes.

6. Klicken Sie auf **Absenden**.
   Der neue Variablensatz wird erstellt und auf der Registerkarte **Variablensätze** angezeigt. Öffnen Sie den neuen Variablensatz, und klicken Sie auf der Registerkarte **Cloud-Variablen** auf **Neu**, um Variablen für den Satz zu erstellen.

Bearbeiten Sie eine Variable für den Cloud-Account-Katalog anfordern

Passen Sie den Cloud-Account-Anforderungsprozess an, indem Sie eine Variable erstellen oder bearbeiten, um wichtige Informationen während der Cloud-Account-Anforderung zu erfassen.

Vorbereitungen
Vermeiden Sie das Entfernen der vorhandenen Cloud-Account-Variablen für Anforderungen, da diese Variablen für die Erstellung einer gültigen CAM-Anforderung wichtig sind.

Erforderliche Rolle: sn_itom_Cam.cw_admin

Warum und wann dieser Vorgang ausgeführt wird
Ändern Sie das Formular „Cloud-Account anfordern“, indem Sie Variablen im Katalog erstellen oder bearbeiten. Sie können eine Variable bearbeiten, um ihre Reihenfolge zu ändern, die Variable aktiv oder inaktiv zu machen und ihre Berechtigungs- und Verfügbarkeitseinstellungen zu ändern.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich**an.
2. Geben Sie Ein `sc_Cat_item.LIST` Im Navigationsfilter.
3. Suchen Sie in der Tabelle „sc_Cat_item.LIST“ nach , und klicken Sie auf *`Request Cloud Account`*Eigenschaft.
4. Klicken Sie auf **Variablensätze** Unterregisterkarte und klicken Sie auf den Variablensatz.
5. Wählen Sie die Variable aus, die Sie bearbeiten möchten, oder klicken Sie auf, um eine Variable zu erstellen **Neu** .
6. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Cloud-Variable“

Feld	Beschreibung
Typ	Zu erstellender Variablentyp. Wenn Sie **Auswahlfeld für die Suche**auswählen, werden auf der Unterregisterkarte **Typspezifikationen** diese Felder angezeigt: ○ **Poolfilter verwenden**: Aktivieren Sie dieses Kontrollkästchen, um dem Feld einen Poolfilter hinzuzufügen. ○ **Pool**: Wählen Sie einen Pool aus, um dem Benutzer des Cloud-Service eine Liste von Werten aus einer vorhandenen Tabelle im Katalogbestellformular anzubieten. Beispielsweise können Sie „CloudAccountPool“ auswählen, um eine Liste aller Cloud-Konten zu erhalten. ○ **Poolfilter**: Wählen Sie einen Filter aus, um die Auswahlmöglichkeiten im Pool weiter einzugrenzen.
Variablensatz	Der Variablensatz, zu dem die Variable gehört.
Obligatorisch	Option, um die Variable als Teil des Bestellvorgangs obligatorisch zu machen.
Aktiv	Option, um die Variable zur Verwendung verfügbar zu machen.
Reihenfolge	Ordnen Sie an, dass die Variable auf der Seite für das Katalogelement platziert wird. Die Variablen sind von oben nach unten vom kleinsten zum größten Reihenfolgenwert organisiert. Zum Beispiel wird eine Variable mit einem Ordnungswert von 1 über anderen Variablen mit Werten höherer Ordnung platziert.

Fragen

Feld	Beschreibung
Frage	Frage an Benutzer, die den Katalogartikel bestellen. **Hinweis:** Wenn Sie im Feld **Typ** die Option **Auswahlfeld** auswählen, wird am Ende des Bildschirms eine Unterregisterkarte **Fragenauswahl** angezeigt. Sie können eine bestimmte Auswahlliste für die Frage eingeben.
Name	Ein Name zur Identifizierung der Frage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn dieses Feld leer ist, wird sein Wert basierend auf dem Feld Frage für alle Variablentypen mit Ausnahme von break, container split, container end, HTML, container start, label, UI page und duration automatisch ausgefüllt.
Tooltip	Tooltip-Text, der angezeigt wird, wenn Benutzer auf die Variable zeigen. Geben Sie eine kurze Notiz ein, um den Zweck der Frage zu beschreiben.
Beispieltext	Hinweis, der im Fragefeld angezeigt wird, bevor ein Benutzer einen Wert eingibt. Anwendbar für folgende Variablen: ○ IP-Adresse ○ E-Mail ○ URL ○ Einzeiliger Text ○ Mehrzeiliger Text ○ Datum ○ Datum/Uhrzeit

Anmerkung

Feld	Beschreibung
Hilfe anzeigen	Wenn diese Option ausgewählt ist, wird der Hilfetext für die Variable angezeigt.
Immer erweitert	Diese Option wird nur angezeigt, wenn das Kontrollkästchen **Hilfe anzeigen** aktiviert ist. Wenn diese Option ausgewählt ist, wird der Wert des Felds **Hilfetext** standardmäßig erweitert, wenn die Katalogelementseite geladen wird.
Hilfe-Tag	Wenn das Kontrollkästchen **Immer erweitert** deaktiviert ist, klicken Sie auf den in diesem Feld angegebenen Wert, um den Wert des Feldes **Hilfetext** anzuzeigen.
Hilfetext	Hilfeinformationen für eine Service Catalog-Variable
Anweisungen	Informationen, die Rich-Text-Formatierung erfordern oder Bilder hinzufügen, um Hilfeinformationen zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Verwenden Sie für HTML-Tabellen Größen, die innerhalb der Breite der Variablen liegen.

Typspezifikationen (Die Felder in diesem Abschnitt variieren für jeden Variablentyp)

Feld	Beschreibung
Variablenbreite	Breite für die Variable auf der Katalogelementseite, um anzugeben, wie viel Prozent der Bildschirmgröße sie umfassen darf. Dieses Feld wird für alle Variablentypen mit Ausnahme der Zeilenumbrüche, des Containerendes, des Containerstarts, der Containeraufteilung, des Containerlayouts und der Beschriftungsvariablen angezeigt.
Regulärer Ausdruck zur Validierung	Regulärer Ausdruck, der die Benutzereingabe für die Eigenschaft validiert.
Validierungsfehler für regulären Ausdruck	Wenn der Ausdruck nicht gültig ist, wird ein Fehler angezeigt.

Standardwert

Feld	Beschreibung
Standardwert	Standardwert für die Variable
Variablenattribute	Attribute für diese Variable.

Berechtigungen

Feld	Beschreibung
Leserollen	Rollen, die die Variable vor oder nach dem Anfordern des Katalogelements oder Datensatzerstellers anzeigen können. Nur ein Benutzer mit den in diesem Feld angegebenen Rollen kann die Variable anzeigen.
Schreibrollen	Rollen, die die Variable im Variableneditor bearbeiten können, nachdem sie das Katalogelement oder den Datensatzersteller angefordert haben. Wenn ein Benutzer die in diesem Feld angegebenen Rollen nicht besitzt, ist die Variable im Variableneditor schreibgeschützt.
Erstellenrollen	Rollen, die Werte für die Variable erstellen können, bevor sie das Katalogelement oder den Datensatzersteller anfordern. Wenn ein Benutzer die angegebene Rolle nicht besitzt, ist die Variable schreibgeschützt, bevor das Katalogelement oder der Datensatzersteller angefordert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbarkeitsdiagramm

Sichtbar	Wenn diese Option ausgewählt ist, ist die Variable im Elementformular vor der Bestellung des Elements, im Variableneditor nach der Bestellung des Elements und in der Warenkorbansicht des Elements sichtbar.
Schreibgeschützt	Wenn ausgewählt, ist die Variable im Cloud-Benutzerportal schreibgeschützt und kann nicht bearbeitet werden.

7. Klicken Sie Auf **Aktualisieren** Sobald Sie alle Änderungen an der Variable vorgenommen haben.

Konfigurieren Sie eine anwenderdefinierte Katalog-ID in Cloud Account Management Account-Anforderung

Konfigurieren Sie die für verwendete Katalog-ID Cloud Account Management Anforderung zum Zuordnen des anwenderdefinierten Servicekatalogs und zur Optimierung der Accountbereitstellung.

Vorbereitungen

Verifiziert, ob der Katalog ein gültiger Servicekatalog ist, der auf verschiedenen Portalen wie dem Mitarbeiter-Center getestet wurde.

Erforderliche Rolle: sn_itom_Cam.cw_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Katalog-ID identifiziert den für verwendeten Katalog eindeutig Cloud Account Management. Um Ihren anwenderdefinierten Cloud-Account-Anforderungskatalog zuzuordnen, aktualisieren Sie den standardmäßigen sys_ID-Wert mit dem anwenderdefinierten sys_ID-Wert des Katalogs.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich**an.
2. Eingeben von `sys_properties.list` im Navigationsfilter.
3. Suchen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] nach , und klicken Sie auf `sn_itom_cam.cam_catalog_id` Datensatz.
4. In **Wert** Geben Sie die eindeutige sys_ID des anwenderdefinierten Katalogs ein.

   Hinweis: Sie können nur eine sys_ID in hinzufügen **Wert** Feld.

5. Klicken Sie auf **Aktualisieren**.

Fügen Sie der Gruppe Mitglieder hinzu

Stellen Sie sicher, dass Mitglieder ihren jeweiligen Gruppen genau zugewiesen werden, um Account-Anforderungen, Genehmigungen, Bereitstellung und Zertifizierung zu optimieren. Gewähren Sie erforderliche Berechtigungen durch die richtige Gruppenzuweisung, um nicht autorisierten Zugriff zu verhindern und die Sicherheit zu gewährleisten.

Vorbereitungen

Erforderliche Rolle: ServiceNow AI Platform Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anwender und Gruppen** > **Gruppen**an.
2. Suchen Sie nach *ITOM Im Suchfeld.
3. Weisen Sie jedem ein Mitglied zu ITOM Gruppieren Sie, indem Sie einen Eintrag auswählen.
   Um mehr über zu erfahren ITOM Cloud Account Management Anwenderrollen, siehe Mit Cloud Account Management installierte Komponenten.
4. Unter **Rollen** Abschnitt auswählen **Bearbeiten** .
5. Suchen Sie den Anwender, und wechseln Sie zur Liste der Gruppenmitglieder.
6. Wählen Sie **Speichern**.

Einrichten AWS API-Konfigurationsinformationen in ServiceNow

Die von bereitgestellten Anmeldeinformationen AWS In diesem Verfahren werden Administratoren verwendet, um ein Aussetzungsprofil zu erstellen, mit dem Sie vorübergehend anhalten oder beenden können AWS Accounts nach Bedarf.

Vorbereitungen

Das folgende Verfahren ist nur erforderlich, wenn Sie verwalten AWS Accounts auf Cloud Account Management.

Erforderliche Rolle: ServiceNow AI Platform Administrator

Prozedur

1. Melden Sie sich bei an ServiceNow Instanz.
2. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
3. Wählen Sie **Neu**.
4. In **Name** Geben Sie den Aliasnamen ein.
   Das Format muss „Name-key der Cloud-Organisation“ sein (z. B. org1-tfkey).
5. Von **Typ** Dropdown-Liste auswählen **Anmeldeinformationen** .
6. Wählen Sie **Absenden**.
7. Wählen Sie den Aliasnamen aus der Liste aus, die Sie zuvor eingegeben haben.
8. Unter **Anmeldeinformationen** Wählen Sie die Registerkarte aus **Neu** .
9. Wählen Sie in der Liste aus **AWS-Anmeldeinformationen** Als Anmeldeinformationstyp.
10. In **Name** Geben Sie den Aliasnamen ein.
11. In **API-Schlüssel** Und **Geheimer Zugriffsschlüssel** Geben Sie die vom Administrator erhaltenen Schlüssel ein.
12. Wählen Sie **Absenden**.

Einrichten Terraform API-Schlüssel in ServiceNow

Fügen Sie hinzu Terraform API-Schlüssel für ServiceNow Instanz, um eine konsistente und fehlerfreie Infrastrukturbereitstellung sicherzustellen.

Vorbereitungen

Das folgende Verfahren ist nur erforderlich, wenn Sie eine Integration durchführen Terraform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: ServiceNow AI Platform Administrator

Prozedur

1. Melden Sie sich bei an ServiceNow Instanz.
2. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
3. Wählen Sie in der Liste aus **API-Schlüssel-Anmeldeinformationen** .
4. In **Name** Geben Sie den Namen ein.
5. In **API-Schlüssel** Geben Sie den aus dem erhaltenen Schlüssel ein Terraform administrator.
6. Um den Prozess abzuschließen, wählen Sie aus **Übermitteln** .

Einrichten Azure Verbindung

Fügen Sie ein hinzu, und konfigurieren Sie es Azure Verbindung mit herstellen Azure Portal. Verwenden Sie die Anmeldeinformationen für die Verbindung, die Cloud Account Management Anwendungserstellungen Azure Abonnements. Dies ist ein einmaliger Konfigurationsschritt.

Vorbereitungen

Das folgende Verfahren ist nur erforderlich, wenn Sie erstellen Azure Abonnements.

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Flow Designer**an.
2. Auswahlvorgang **Integrationen** > **Verbindungen** > **Ausgehend**an.
3. Suchen und auswählen **Azure-Verbindung (sn_itom_Cam)** .
4. Wählen Sie **Details anzeigen**.
5. Wählen Sie **Konfigurieren**.
6. In **Konfigurieren Sie Die Verbindung** Geben Sie die folgenden Informationen an.

Verbindung konfigurieren

Feld	Beschreibung
Verbindungsname	Eindeutiger Name für Azure OAuth-Verbindung.
Verbindungs-URL	Die Standard-URL wird automatisch ausgefüllt. Bei Bedarf können Sie die URL ändern.
OAuth-Client-ID	Die Client-ID der Anwendung, die in registriert ist Azure OAuth-Server.
OAuth-Client-Geheimnis	Das geheime Clientgeheimnis der Anwendung, die in registriert ist Azure OAuth-Server.
OAuth-Token-URL	Die URL , die den Endpunkt angibt, um das Zugriffstoken vom OAuth- Server abzurufen. Die Standard-URL wird automatisch ausgefüllt. Bei Bedarf können Sie die URL ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie Aus **OAuth-Token konfigurieren und abrufen** .
8. **Wahlweise:** Um den Verbindungsalias anzuzeigen, wählen Sie aus **Zeigen Sie den Verbindungsalias an** .

Richten Sie die Scankonfiguration für die Datenvisualisierung ein

Visualisieren Sie alle Accountverstöße, indem Sie sie mithilfe des ausgewählten Richtliniensatzes scannen. Zeigen Sie den Schweregrad aller Verstöße im Administrator-Dashboard an, um entsprechende Aktionen zu ergreifen.

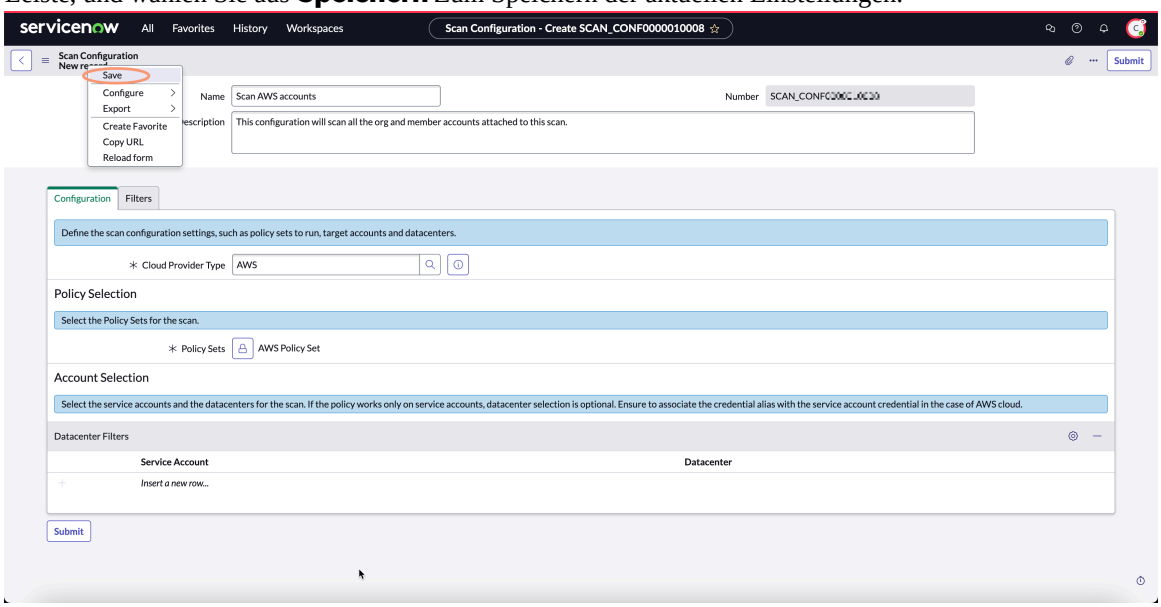
Vorbereitungen

Stellen Sie sicher, dass Sie sich auf die Standardrichtlinien (Richtlinienliste zum Scannen von Cloud-Accounts). Informationen zum Erstellen eines anwenderdefinierten Richtliniensatzes finden Sie unter Richtliniensatz erstellen.

Erforderliche Rolle: sn_itom_Cam.cw_admin oder sn_itom_ccg.Scheduling_admin

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Scan-Konfigurationen**an.
2. Erstellen Sie eine Scankonfiguration, indem Sie auswählen **Neu** .
3. Identifizieren Sie die Konfiguration, indem Sie eingeben Name Und Beschreibung .
4. Unter **Konfiguration** Wählen Sie eine Registerkarte aus **Cloud-Provider-Typ** Aus der Suche.
5. Wählen Sie aus **Richtliniensätze Entsperren** Symbol ( ) Und wählen Sie einen Richtliniensatz aus der Liste aus.
6. Wählen Sie aus **Sperren Sie Richtliniensätze** Symbol ( ).
7. Wählen Sie Symbol „zusätzliche Aktionen“ ( ) Oder klicken Sie mit der rechten Maustaste auf die obere Leiste, und wählen Sie aus **Speichern** Zum Speichern der aktuellen Einstellungen.

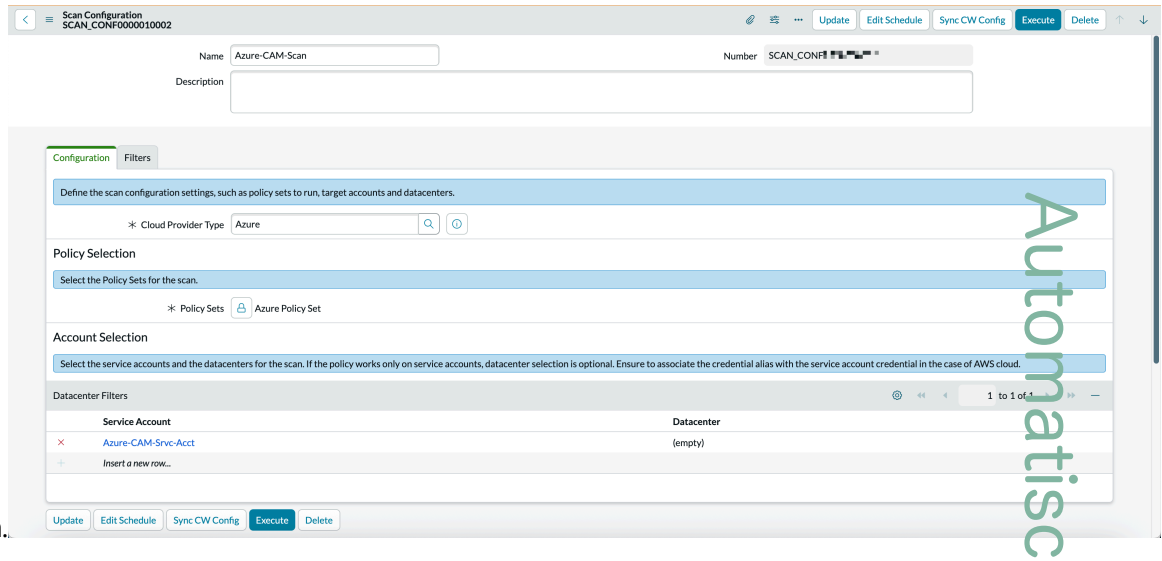


8. Unter **Service-Account** Spalte alle Verwaltungs-Accounts und Mitgliedsaccounts aus der Suche auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen Verwaltungsaccount auswählen, werden alle aktuellen und zukünftigen Mitgliedsaccounts automatisch überprüft. Die Auswahl einzelner Mitgliedsaccounts erfordert eine manuelle Auswahl für jeden Scan.

9. Wählen Sie Aus **Zeitplan Einrichten** Und legen Sie den Zeitplan nach Bedarf fest.
10. Wählen Sie **Aktualisieren**.
11. Synchronisieren Sie die Konfiguration mit Cloud Account Management App durch Auswählen **CAM-Konfiguration synchronisieren**.



Hinweis:

- Um die synchronisierte Konfiguration anzuzeigen, navigieren Sie zu **Alle** > **Cloud-Arbeitsbereich** > **Konfiguration**an.
- Wenn Sie die Konfiguration synchronisiert haben, müssen Sie keine in erwähnte Scan-Account-Konfiguration erstellen Erstellen Sie eine Scan-Account-Konfiguration.

12. **Wahlweise:** Wählen Sie aus, um einen Scan bei Bedarf auszuführen **Ausführen** .

Hinweis: Sie können unbegrenzte Konfigurationen für jeden Account erstellen. Ein Account kann mehrere Scan-Konfigurationen haben, wobei Verstöße und Bewertungen auf allen basieren.

Konfigurationen werden erstellt

Einrichten von Cloud Account Management App ist eine erforderliche Aufgabe, bevor Sie mit dem Erstellen, Aussetzen oder Scannen eines Service-Accounts fortfahren. Durch Konfigurieren Cloud Account Management, Sie können sicherstellen, dass die Anwendung bereit ist, Account-Verwaltungsaufgaben effektiv auszuführen und die gewünschten Ergebnisse zu liefern.

Erstellen Sie einen Terraform Account-Konfiguration

Konfigurieren Sie Cloud Account Management App als grundlegender Schritt vor der Erstellung eines Service-Accounts mit Terraform. Richtig Cloud Account Management Das Setup stellt sicher, dass die Anwendung optimal auf die Verarbeitung von Account-Management-Funktionen und das Erreichen der gewünschten Ergebnisse vorbereitet ist.Definieren und richten Sie Terraform-basierte Konfigurationen ein, um die Cloud-Account-Bereitstellung zu automatisieren, einschließlich erforderlicher Anmeldeinformationen und Infrastrukturvorlagen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Konfiguration**an.
2. Wählen Sie **Neu**.
3. Geben Sie die Details in ein **Neue Konfiguration** Formular.

   Informationen zum Ausfüllen der Formularfelder finden Sie unter Terraform Account-Konfigurationsfelder.
4. Wählen Sie **Absenden**.

Nächste Maßnahme
Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie

Erstellen Sie eine Accountkonfiguration für die native Cloud-Schnittstelle

Konfigurieren Sie Cloud-Accounts mithilfe der nativen Schnittstelle unterstützter Cloud-Anbieter wie AWS AWS Oder Azure Ermöglicht die nahtlose Bereitstellung und Integration.

Vorbereitungen
Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Konfiguration**an.
2. Wählen Sie **Neu**.
3. Geben Sie die Details in ein **Neue Konfiguration** Formular.

   Informationen zum Ausfüllen der Formularfelder finden Sie unter Konfigurationskontofelder der Cloud-nativen Schnittstelle.
4. Wählen Sie **Absenden**.

Nächste Maßnahme
Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie

Erstellen Sie eine Konfiguration zum Sperren des Accounts

Richten Sie ein Aussetzungsprofil ein, das die vorübergehende Sperrung oder Beendigung von Cloud-Accounts ermöglicht, um die Kostenkontrolle oder Richtliniendurchsetzung zu unterstützen.

Vorbereitungen
Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Konfiguration**an.
2. Wählen Sie **Neu**.
3. Geben Sie die Details in ein **Neue Konfiguration** Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Ausfüllen der Formularfelder finden Sie unter Konfigurationsfelder für Account sperren.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie

Erstellen Sie eine Scan-Account-Konfiguration

Konfigurieren Sie Cloud Account Management App, bevor ein Service-Account gescannt wird, um zu bestätigen, dass es für eine effektive Account-Verwaltung bereit ist.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Konfiguration**an.
2. Wählen Sie **Neu**.
3. In **Neue Konfiguration** Formular: Geben Sie die folgenden Informationen an.

Konfigurationstyp: Accounts scannen

Feldname	Beschreibung
Cloud-Anbieter	Name der Cloud-Anbieterplattform, z. B. AWS, Azure, Oder GCP.
Name	Name für die Konfiguration.
Service-Accounts	Der Service-Account und seine Mitgliedsaccounts. **Hinweis:** Wenn Sie einen Verwaltungsaccount auswählen, werden automatisch alle aktuellen und zukünftigen Mitgliedsaccounts durchsucht. Wenn Sie jedoch einzelne Mitgliedsaccounts auswählen, muss jeder manuell zum Scannen ausgewählt werden.
CCG-Scankonfiguration	CloudConfiguration Governance (CCG)-Scankonfiguration, die zum Abrufen der Verstöße für alle Accounts in der ausgewählten Cloud-Organisation verwendet wird.
Beschreibung	Informationen, die in Arbeitsnotizen aufgezeichnet werden können.

4. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie

Überprüfen Sie Anforderungsrichtlinien

Überprüfen und aktualisieren Sie Anforderungsrichtlinien, um sicherzustellen, dass sie mit Ihrem Cloud-Account-Anforderungsprozess übereinstimmen. Diese Richtlinien erzwingen Datenprüfungen und -Bedingungen und fördern die Konsistenz bei der Erstellung von Cloud-Abonnementkonten.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Bestimmte Schritte in der Anforderungsverarbeitung erfordern häufig manuelle Eingriffe. Diese Maßnahmen umfassen allgemeine Genehmigungen, Finanzgenehmigungen und die Zuweisung von Konfigurationen und AWS Organisationseinheit. Diese Schritte können jedoch automatisiert werden, wenn bestimmte Kriterien erfüllt sind. Cloud Account Management Ist in das PACE-Plugin integriert, um diese Kriterien als Richtlinien zu definieren und zu verwalten.

Für jeden Schritt wird ein Eintrag in erstellt *sn_itom_cam_automation_activity*Tabelle und die zugehörigen Richtlinien werden unter angezeigt **Anforderungsrichtlinien** Registerkarte in Cloud-Arbeitsbereich. Jede Richtlinie ist über eine Aktivität verknüpft **Zuordnungen** Registerkarte innerhalb der Richtlinie, obwohl gemäß der Automatisierungsaktivität nur eine Richtlinie unterstützt wird.

Hinweis: Derzeit Azure Account-Erstellung kann nicht automatisiert werden.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Anforderungsrichtlinien**an.
   Die vorhandenen Richtlinien werden unter angezeigt **Alle Richtlinien** Abschnitt und werden weiter als aktive Richtlinien und inaktive Richtlinien klassifiziert.
2. Zeigen Sie eine vorhandene Richtlinie an, oder passen Sie sie an, indem Sie den Richtliniennamen auswählen.
3. Unter **Richtliniengenerator** Registerkarte überprüfen Sie die Richtlinienbedingungen.
4. **Wahlweise:** Wählen Sie aus, um eine vorhandene Richtlinie zu ändern **Kopie erstellen** .
5. **Wahlweise:** Um eine Bedingung hinzuzufügen, wählen Sie aus **Neuer Bedingungssatz** .
6. **Wahlweise:** Um eine Bedingung zu entfernen, wählen Sie das Löschsymbol .

Hinweis: Weitere Informationen zum Verwalten von Richtlinien finden Sie unter Verwalten PaCE Richtlinien .

Nächste Maßnahme

In diesen Abschnitten wird erläutert, wie die Automatisierungsrichtlinie geändert, getestet und veröffentlicht wird.

- Automatisieren Sie den allgemeinen Genehmigungsrichtlinienprozess
- Automatisieren Sie den Richtlinienprozess für die Budgetgenehmigung
- Automatisieren Sie den Richtlinienprozess für die Konfigurationszuweisung

Automatisieren Sie den allgemeinen Genehmigungsrichtlinienprozess

Automatisieren Sie die allgemeine Genehmigung oder Ablehnung von Anforderungen basierend auf vordefinierten Bedingungen. Anforderungen werden automatisch genehmigt, wenn die Kriterien erfüllt sind. Andernfalls wartet das System auf die manuelle Genehmigung. Sie können die Standardrichtlinie ändern, um nach Bedarf zusätzliche Bedingungen einzubeziehen.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Warum und wann dieser Vorgang ausgeführt wird

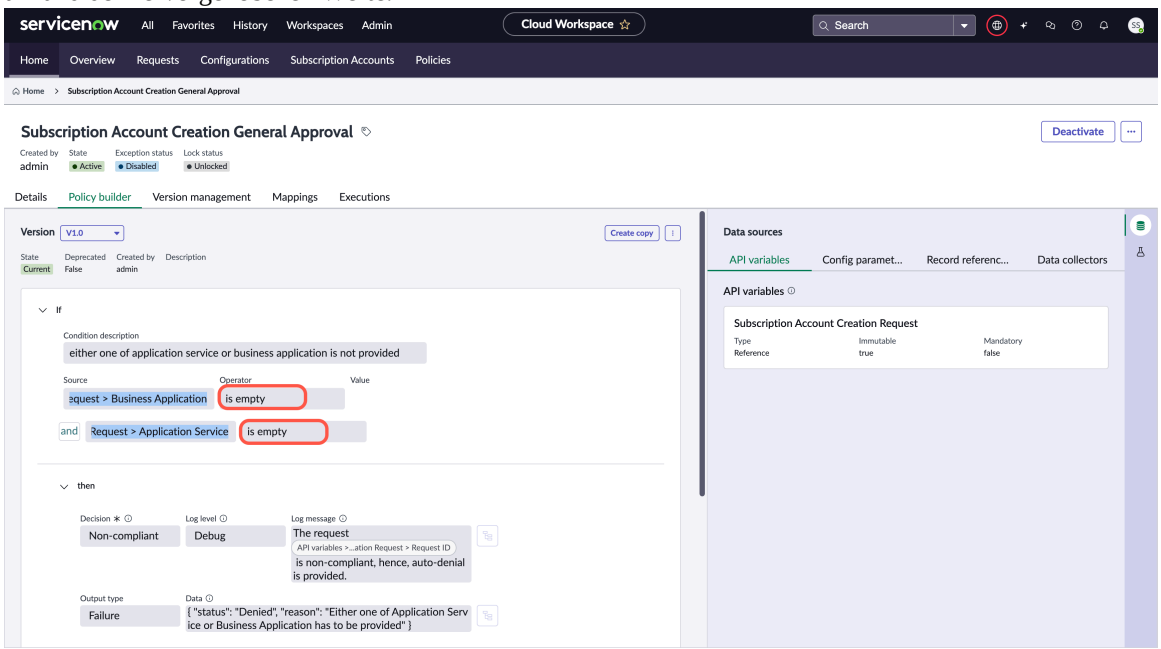
Dieses Verfahren demonstriert, wie ein Account mithilfe der allgemeinen Richtlinie zur Kontogenehmigung genehmigt oder abgelehnt wird. Wenn eine Account-Anforderung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beispielsweise eine vordefinierte Genehmigungsrichtlinie enthält, erklärt dieser Prozess, wie die Anforderung automatisch genehmigt oder abgelehnt wird.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Anforderungsrichtlinien**an.
2. Wählen Sie Aus **Allgemeine Genehmigung Zur Erstellung Eines Abonnement-Accounts** .
3. Passen Sie die Richtlinie an, indem Sie auswählen **Kopie erstellen** .
4. Unter **Richtliniengenerator** Registerkarte im **Wenn** Bedingungsblock, notieren Sie sich die Quellfelder anhand der hervorgehobenen Werte.



Hinweis: In diesem Abschnitt validieren Sie zwei Bedingungen:

a. Geschäftsanwendung = leer

b. Anwendungsservice = leer

5. Wählen Sie Aus **Zuordnungen** .
6. Überprüfen Sie, ob das Dokument zugewiesen ist **Automatisierungsaktivität: Allgemeine automatische Genehmigung für die Erstellung eines Abonnementaccounts** .

Hinweis:

- Wenn kein Dokument verknüpft ist, wählen Sie aus **Hinzufügen** Und wählen Sie aus **Allgemeine automatische Genehmigung für die Erstellung eines Abonnementaccounts** Dokument.
- Ordnen Sie nur eine Richtlinie gemäß der Automatisierung zu.
- Zeigen Sie Dokumente in an, oder erstellen Sie sie sn_itom_Cam_Automation_activity.list Tabelle.

7. **Wahlweise:** Um die automatische Genehmigung zu entfernen, wechseln Sie zu **Zuordnungen** Registerkarte und löschen Sie das zugeordnete Dokument.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Informationen zum Testen der Richtlinie finden Sie unter Testen Sie Updates für einen PaCE Richtlinienversion .

Informationen zum Veröffentlichen der Richtlinie finden Sie unter Veröffentlichen Sie eine PaCE Richtlinienversion .

Informationen zum Hinzufügen eines neuen Genehmigungsschritts im Flow Designer finden Sie unter Mit Workflow-Studio .

Automatisieren Sie den Richtlinienprozess für die Budgetgenehmigung

Finanzgenehmigungen für automatisieren Cloud Account Management Anforderungen basierend auf vordefinierten Bedingungen. Genehmigen Sie Anforderungen automatisch, wenn die Kriterien erfüllt sind. Andernfalls warten Sie auf die manuelle Genehmigung. Ändern Sie die Standardrichtlinie, um nach Bedarf zusätzliche Bedingungen einzubeziehen.

Vorbereitungen

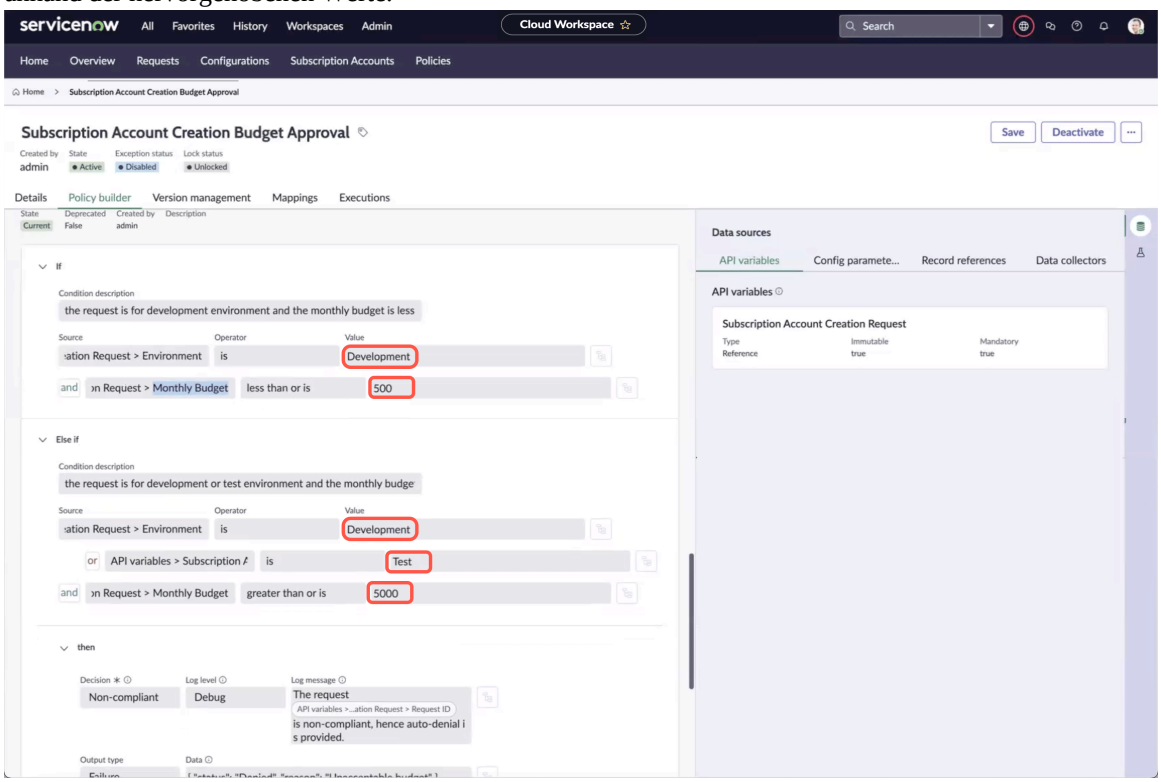
Erforderliche Rolle: sn_itom_Cam.cw_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren demonstriert, wie ein Budget mithilfe der Richtlinie zur Genehmigung des Account-Budgets genehmigt oder abgelehnt wird. Wenn eine Account-Anforderung beispielsweise eine vordefinierte Genehmigungsrichtlinie enthält, erklärt dieser Prozess, wie die Budgetanforderung automatisch genehmigt oder abgelehnt wird.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Anforderungsrichtlinien**an.
2. Wählen Sie Aus **Budgetgenehmigung Für Erstellung Eines Abonnement-Accounts** .
3. Passen Sie die Richtlinie an, indem Sie auswählen **Kopie erstellen** .
4. Unter **Richtliniengenerator** Registerkarte im **Wenn** Bedingungsblock, notieren Sie sich die Quellfelder anhand der hervorgehobenen Werte.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In diesem Abschnitt validieren Sie zwei Bedingungen:

a. Umgebung = Entwicklung

b. Monatliches Budget <= 500

a. Umgebung = Entwicklung oder Test

b. Monatliches Budget = > 5000

5. Wählen Sie Aus **Zuordnungen** .
6. Überprüfen Sie, ob das Dokument zugewiesen ist **Automatisierungsaktivität: Automatische Genehmigung der Finanzen für die Erstellung eines Abonnementaccounts** .

Hinweis:

- Wenn kein Dokument verknüpft ist, wählen Sie aus **Hinzufügen** Und wählen Sie aus **Automatische Finanzgenehmigung für die Erstellung eines Abonnementaccounts** Dokument.
- Ordnen Sie nur eine Richtlinie gemäß der Automatisierung zu.
- Zeigen Sie Dokumente in an, oder erstellen Sie sie sn_itom_Cam_Automation_activity.list Tabelle.

7. **Wahlweise:** Um die automatische Genehmigung zu entfernen, wechseln Sie zu **Zuordnungen** Registerkarte und löschen Sie das zugeordnete Dokument.

Nächste Maßnahme

Informationen zum Testen der Richtlinie finden Sie unter Testen Sie Updates für einen PaCE Richtlinienversion .

Informationen zum Veröffentlichen der Richtlinie finden Sie unter Veröffentlichen Sie eine PaCE Richtlinienversion .

Informationen zum Hinzufügen eines neuen Genehmigungsschritts im Flow Designer finden Sie unter Mit Workflow-Studio .

Automatisieren Sie den Richtlinienprozess für die Konfigurationszuweisung

Automatisieren Sie die Zuweisung von Konfigurationen und AWS Organisationseinheiten in Anforderungen basierend auf angegebenen Bedingungen. Wenn die Bedingungen erfüllt sind und Genehmigungen abgeschlossen sind, werden Anforderungen ohne Administratoreingabe weitergeleitet. Aktualisieren Sie die Standardrichtlinie, um bestimmte Bedingungen und Werte für die Konfiguration und einzubeziehen AWS Organisationseinheit.

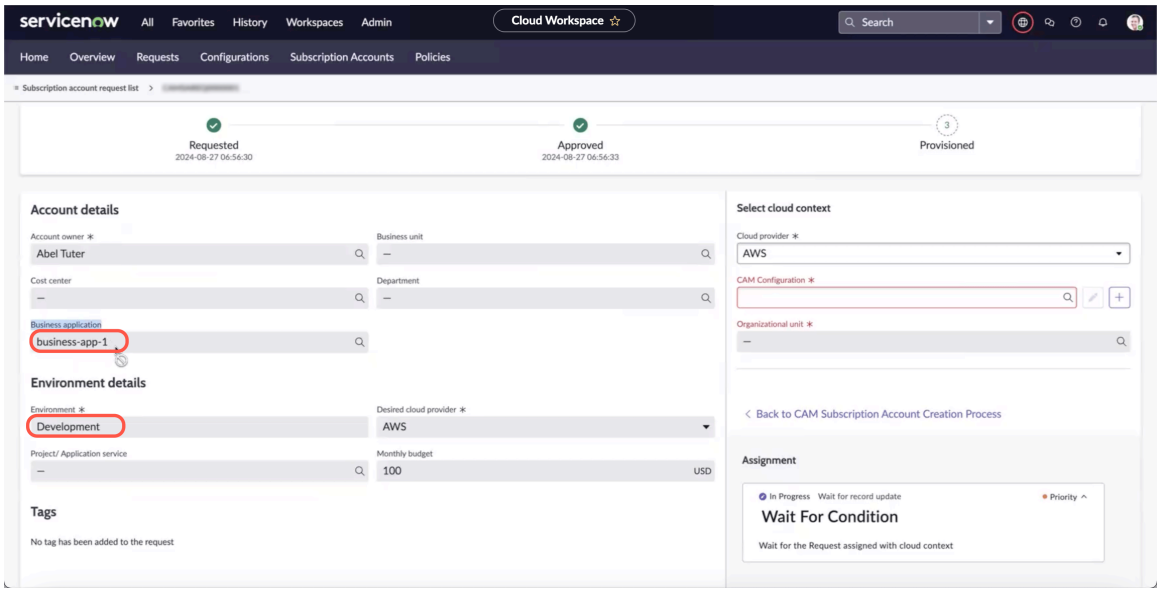
Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Warum und wann dieser Vorgang ausgeführt wird

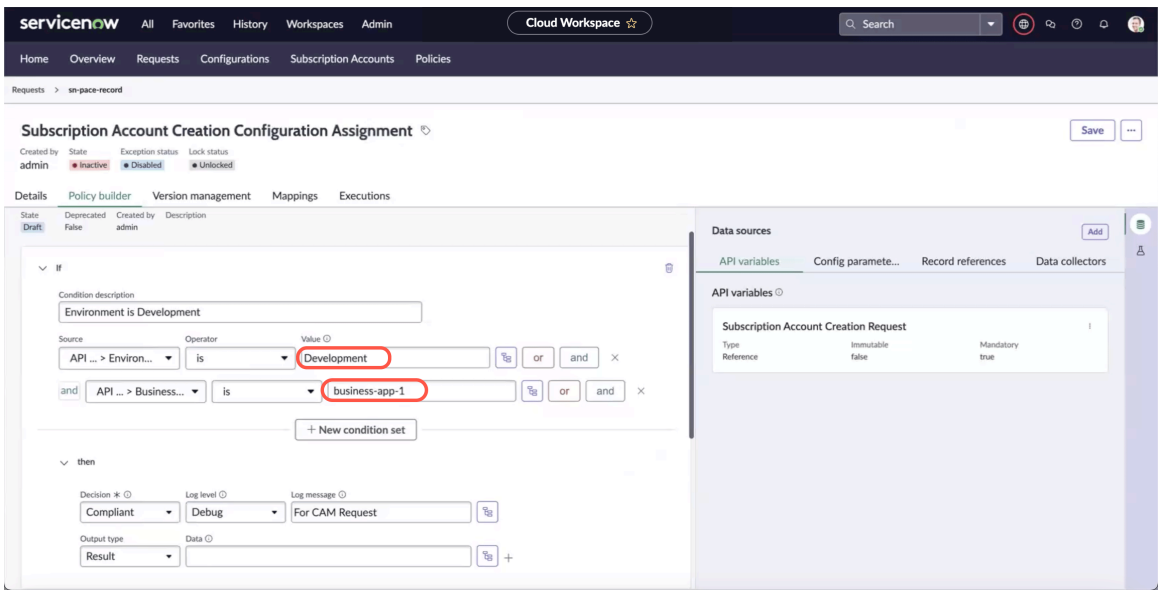
Dieses Verfahren demonstriert, wie die Accountkonfiguration mithilfe der Zuweisungsrichtlinie zugewiesen wird. Wenn beispielsweise die Anforderung zur Account-Erstellung genehmigt wird und auf die Konfigurationsinformationen der Bereitstellung wartet, wird diese Automatisierung ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Anforderungsrichtlinien**an.
2. Wählen Sie Aus **Zuweisung Der Konfiguration Für Die Erstellung Eines Abonnement-Accounts** .
3. Passen Sie die Richtlinie an, indem Sie auswählen **Kopie erstellen** .
4. Unter **Richtliniengenerator** Registerkarte im **Wenn** Bedingungsblock, notieren Sie sich die Werte, die Sie validieren.



Hinweis: In diesem Abschnitt validieren Sie:

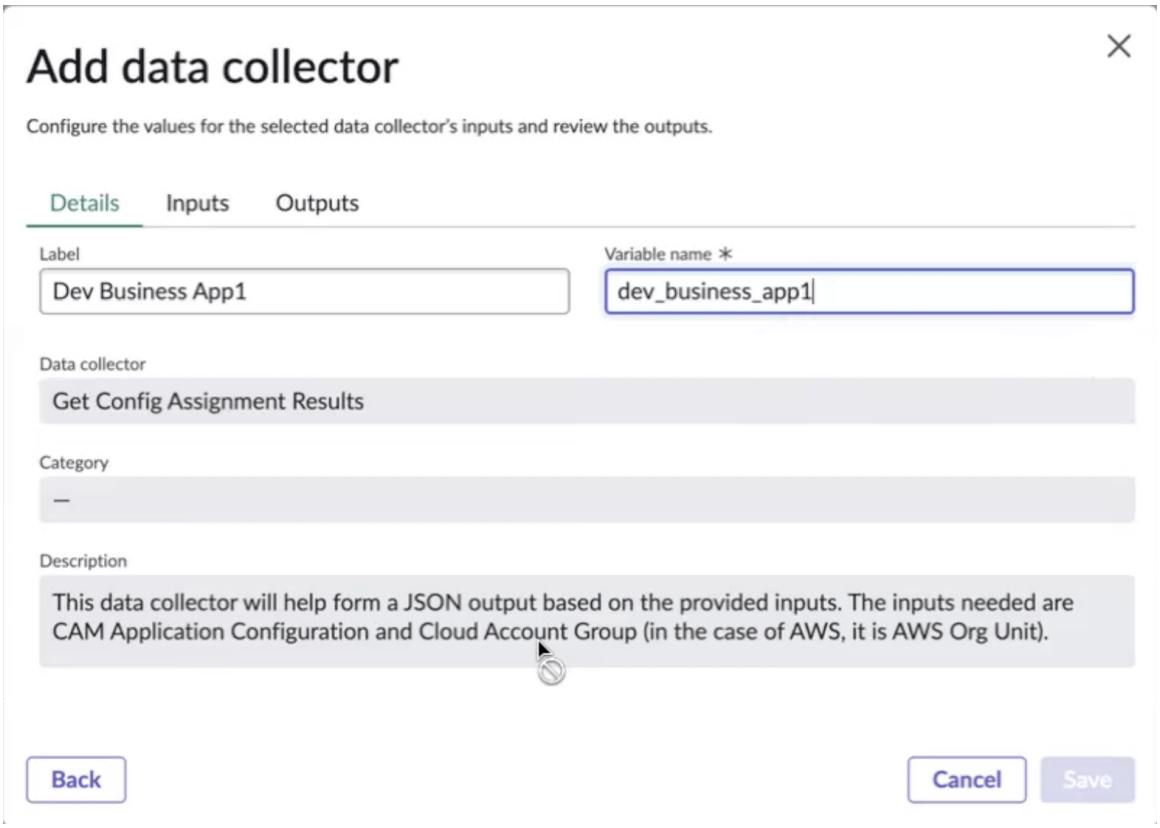
a. Umgebung = Entwicklung

b. Geschäftsbereich = Business-App-1

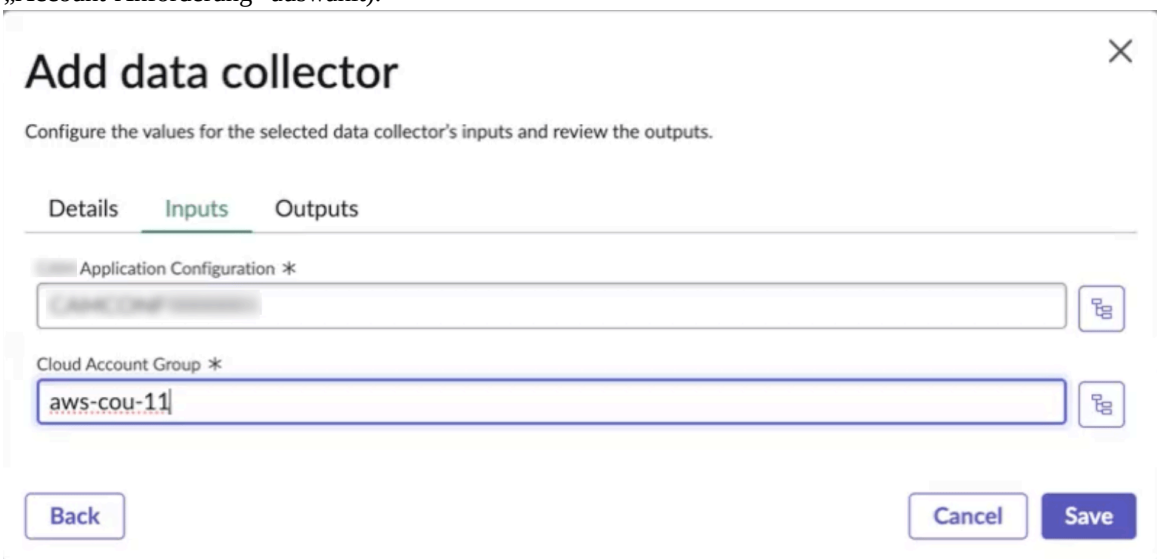
5. Um die Konfiguration und auszuwählen AWS Organisationseinheitsausgabe, wählen Sie aus **Datenerfasser** Im Abschnitt „Datenquellen“.
6. Wählen Sie **Hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie Aus **Rufen Sie Die Ergebnisse Der Konfigurationszuweisung Ab** .
8. In **Fügen Sie den Datenerfasser hinzu** Popup, Eingabetaste Bezeichnung Und Variablenname . Diese Feldwerte werden nur verwendet, um den Datenerfasser zu identifizieren.



9. Unter **Eingaben** Wählen Sie die Registerkarte aus **CW-Anwendungskonfiguration** Und **CW-Account-Gruppe** (Identisch mit AWS Organisationseinheit, die ein Administrator auf dem Bildschirm „Account-Anforderung“ auswählt).



Hinweis: Der ausgewählte AWS Organisationseinheit im Datensammler muss Teil derselben Cloud-Organisation sein, die in der Konfiguration bereitgestellt wird.

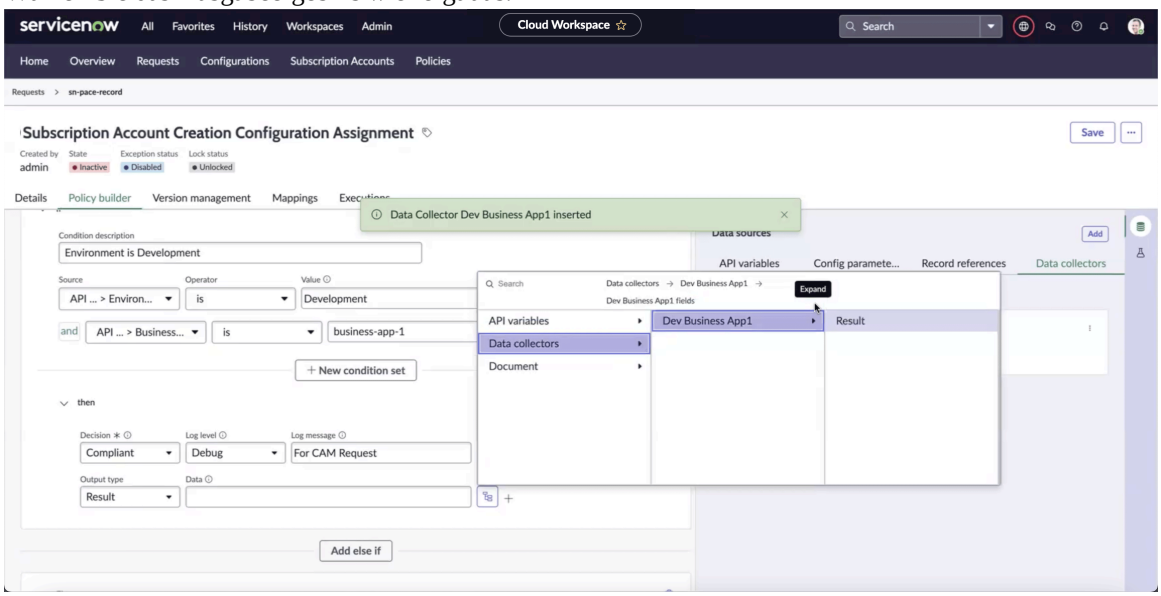
10. Wählen Sie **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der neue Datensammlereintrag wird gespeichert. Nur wenn **Wenn** Bedingung ist erfüllt, die **Dann** Bedingung wird ausgeführt.

11. Wählen Sie das Ausgabeergebnis wie folgt aus.



12. Um die Richtlinie zu speichern, wählen Sie aus **Speichern** .

Hinweis:

- Bei Bedarf können Sie die Protokollnachricht für das Ergebnis verbessern. Einige Beispiele finden Sie in den standardmäßig veröffentlichten Richtlinien.
- Ordnen Sie nur eine Richtlinie gemäß der Automatisierung zu.
- Diese Konfigurationsgenehmigungsrichtlinie ist standardmäßig inaktiv. Sie können deaktivieren, um die Automatisierung zu stoppen.

Nächste Maßnahme

Informationen zum Testen der Richtlinie finden Sie unter Testen Sie Updates für einen PaCE Richtlinienversion .

Informationen zum Veröffentlichen der Richtlinie finden Sie unter Veröffentlichen Sie eine PaCE Richtlinienversion .

Informationen zum Hinzufügen eines neuen Genehmigungsschritts im Flow Designer finden Sie unter Mit Workflow-Studio .

Konfigurieren Sie die Cloud-Asset-Sammlungstabelle

Konfigurieren Sie die Tabelle „Cloud-Asset-Sammlungskonfigurationen“, um Cloud-Assets zu erfassen oder den CI-Einträgen Kommentare hinzuzufügen.

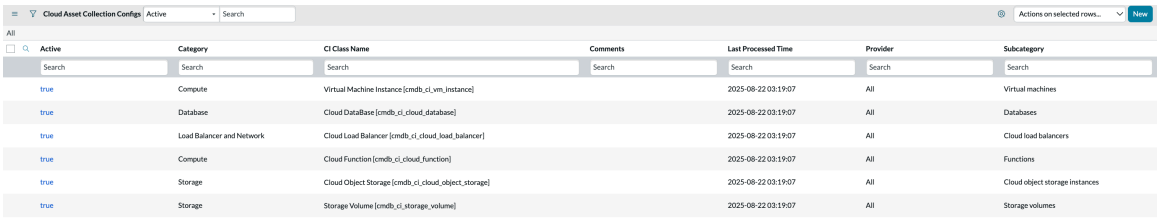
Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich**an.
2. Entfernen Sie die URL nach *service-now.com/, und geben Sie den Tabellennamen ein `sn_itom_Cam_Asset_Collection_config_list.do` .
   Die Tabelleneinträge lauten wie folgt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Doppelklicken Sie auf einen Eintrag, um die Spalte aktiv oder Kommentare zu aktualisieren, und wählen Sie dann das Symbol Speichern aus .

Hinweis: Sie können die Erfassung von Cloud-Assets beenden, indem Sie die Spalte aktiv auf falsch setzen.

Cloud Account Management in Cloud-Arbeitsbereich verwenden

Die Cloud Account Management Die App bietet die Möglichkeit, Ihre Cloud-Accounts zu verwalten.

Wird Angezeigt Cloud Account Management Dashboards

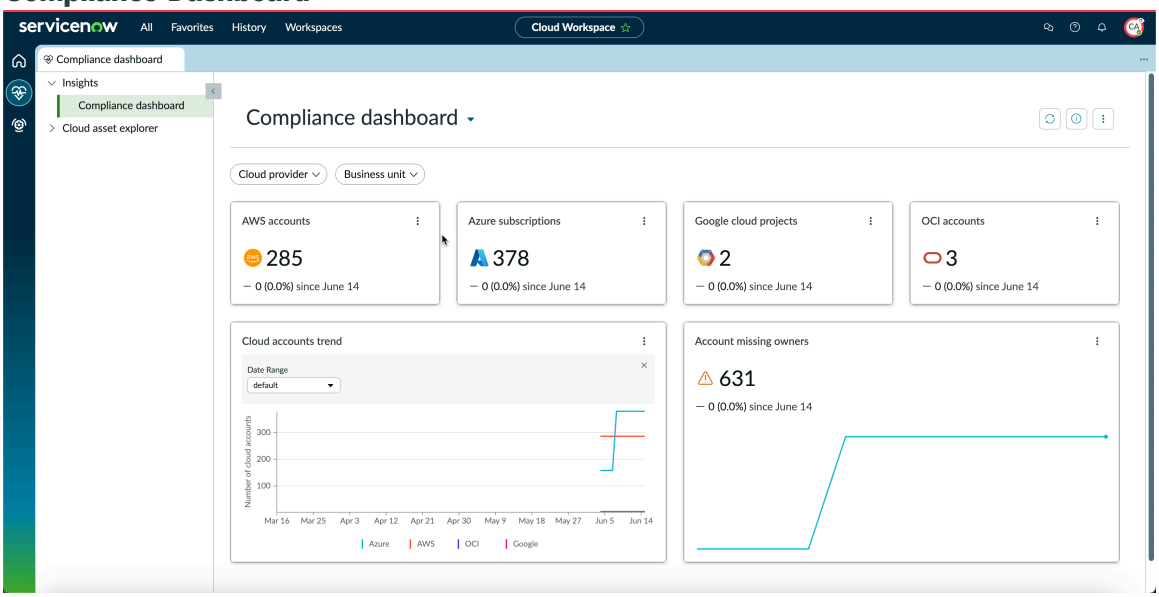
Cloud Account Management Hat Zwei Arten von Dashboards: Eines für Anfordernde Person S Und ein weiterer für Administrator S . Abhängig vom protokollierten – Im Anwender wird ein entsprechendes Dashboard angezeigt .

Anzeigen des Compliance-Dashboards

Die Cloud-Arbeitsbereich Compliance Das Dashboard bietet Einblicke, die der Sicherheit helfen Team S Identifizieren Sie Cloud-Ressourcen ohne Besitzinformationen, und kennzeichnen Sie angreifbare oder gefährdete Ressourcen. Dies Informationen helfen Teammitgliedern Führen Sie Sicherheits-Audits durch, und bestätigen Sie die Compliance mit Branchenvorschriften in Cloud-Umgebungen.

Als Administrator können Sie auf das Dashboard zugreifen Indem Sie zu navigieren **Alle** > **Cloud-Arbeitsbereich** > **Überwachen und nachverfolgen**an.

Compliance-Dashboard



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

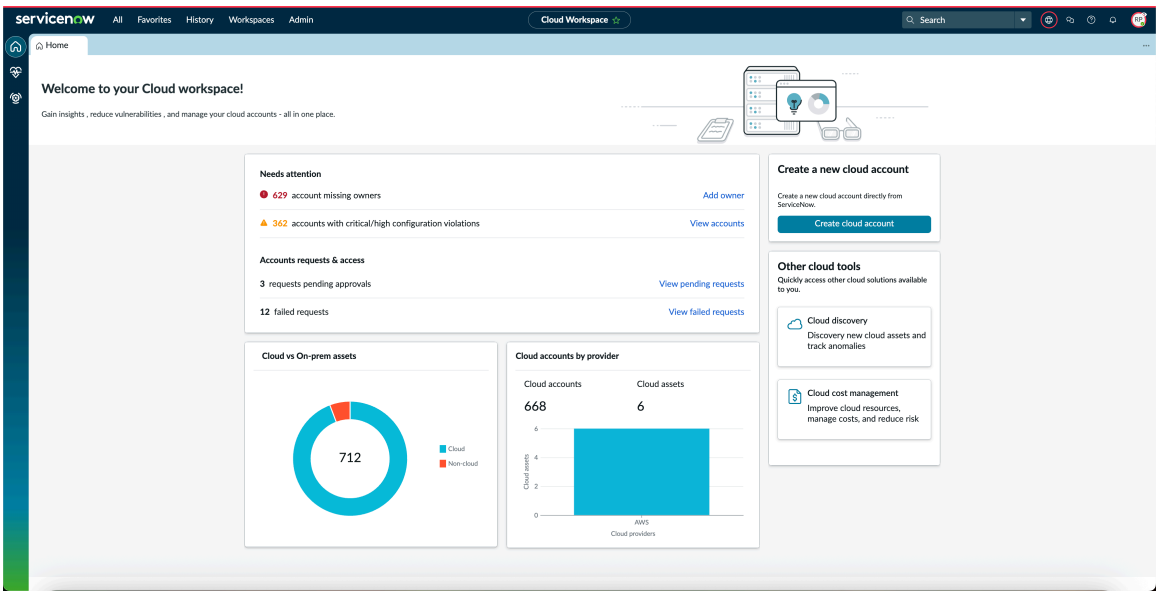
- Im Compliance-Dashboard werden nur die in Ihrer Instanz erkannten Accounts angezeigt.
- Im Compliance-Dashboard wird die Anbieterkarte ausgeblendet, wenn keine Accounts bereitgestellt werden.

Anzeigen von Administrator Homepage

Zeigen Sie Accountstatus und -Verstöße, umsetzbare Einblicke und administrative Steuerungen im an Administrator Homepage.

Als Administrator Oder Asset-Betrachter , Sie können auf die Homepage zugreifen, indem Sie zu navigieren **Alle** > **Cloud-Arbeitsbereich**an.

Administrator Oder Asset-Betrachter Dashboard



Hinweis:

- Das Widget „Handlungsbedarf“ wird nur für Administratoren mit angezeigt Cloud Account Management Berechtigung.
- Das Widget „andere Cloud-Tools“ zeigt die auf Ihrer Instanz installierten Anwendungen an. Cloud-Discovery ist eine Voraussetzung für die Installation Cloud Account Management.

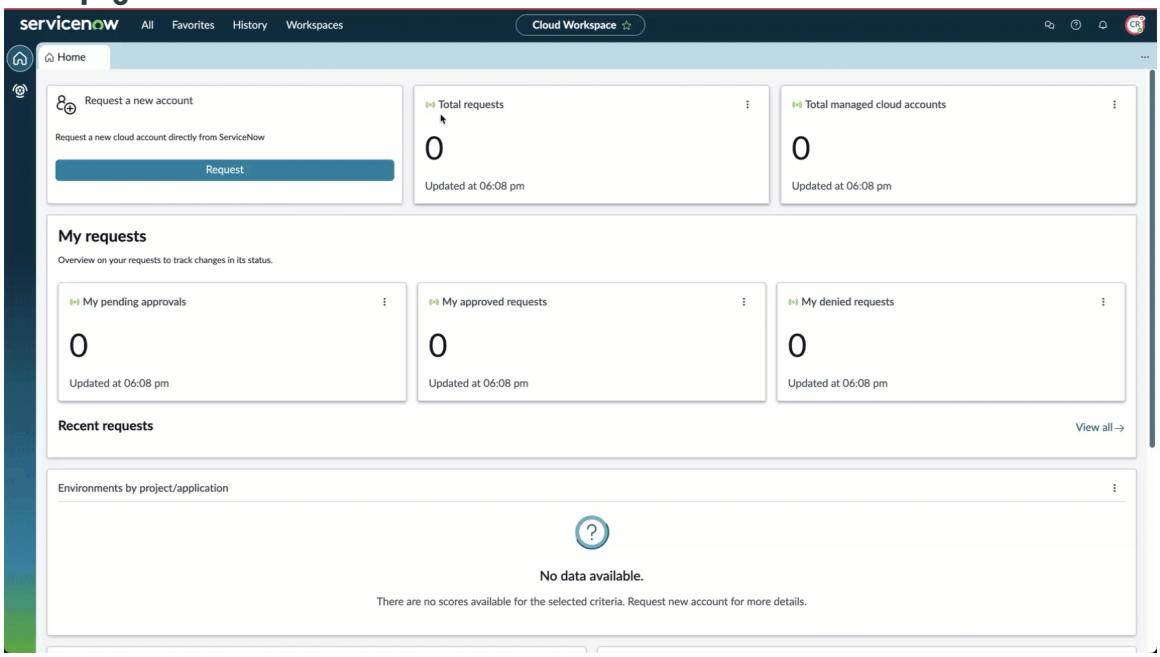
Homepage der anfordernden Person wird angezeigt

Zeigen Sie Cloud-Account-Anforderungen auf der Seite „anfordernde Person“ an, und verwalten Sie sie. Die Homepage bietet eine Ansicht der angeforderten, genehmigten, abgelehnten, ausstehenden und aktiven Accounts.

Anfordernde Personen können über n auf die Homepage der anfordernden Person zugreifen Navigieren ING Bis **Alle** > **Cloud-Arbeitsbereich**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage der anfordernden Person

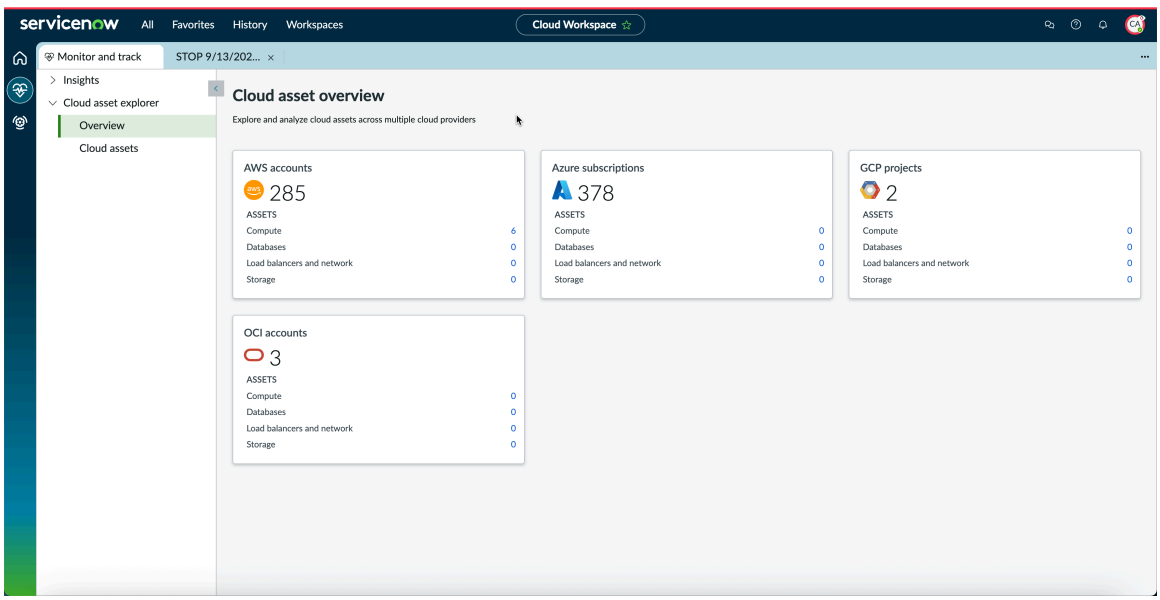


Anzeigen von C Lautes Asset Übersichtsseite

Die Cloud-Asset-Übersichtsseite Hilft Cloud-Governance- und Betriebsteams, Compliance- und Asset-Details effizienter zu überwachen, nachzuverfolgen und zu bearbeiten. Als Asset-Betrachter können Sie alle Assets anzeigen und Drilldown durchführen, um detaillierte Informationen zu jedem Konfigurationselement (CI) anzuzeigen.

Kann auf die Übersichtsseite für Cloud-Assets zugreifen, indem Sie zu navigieren **Alle** > **Cloud-Arbeitsbereich** Und dann in **Überwachen und nachverfolgen** Wählen Sie die Registerkarte aus **Cloud-Asset-Explorer** > **Übersicht**an.

Cloud-Asset Übersichtsseite



Hinweis: Sie können die Konfiguration der Asset-Sammlung aktivieren oder deaktivieren, um die CIs aufzulisten. Weitere Informationen finden Sie unter Konfigurieren Sie die Cloud-Asset-Sammlungstabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

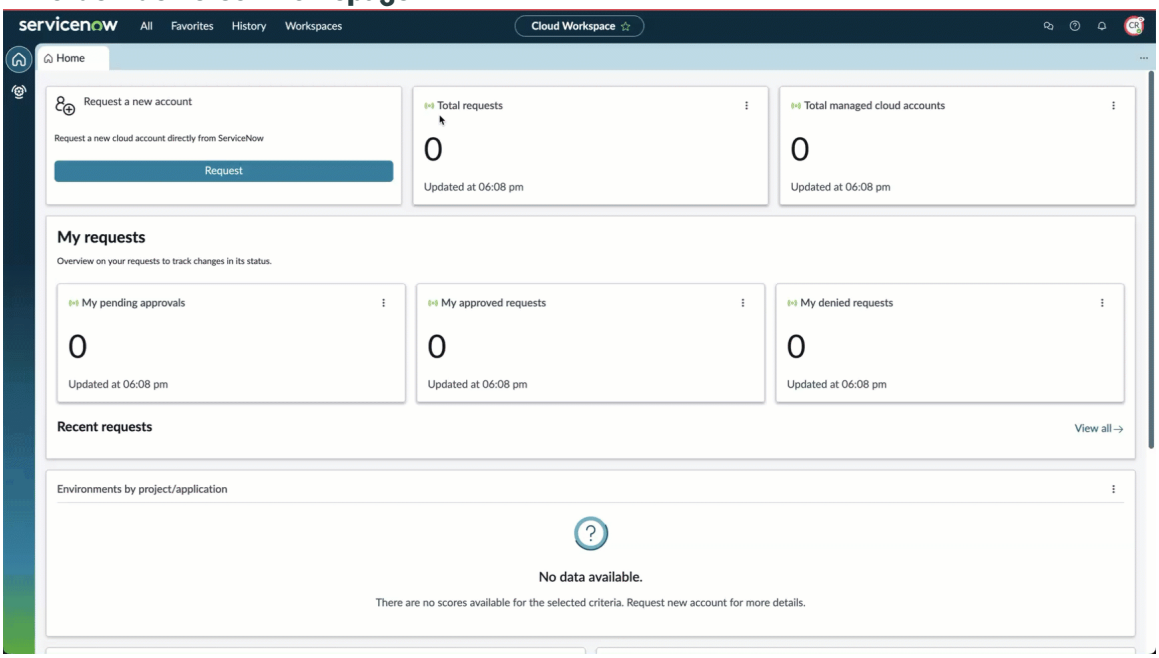
Die anfordernde Person wird angezeigt Startseite Seite

Zeigen Sie Cloud-Account-Anforderungen für die anfordernde Person an, und verwalten Sie sie Seite . Die Homepage Bietet eine Ansicht der angeforderten, genehmigten, abgelehnten, ausstehenden und aktiven Accounts.

Sie können auf zugreifen Homepage Auf eine der beiden Arten.

- Navigieren zu **Alle** > **Cloud-Arbeitsbereich**
- Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich**

Anfordernde Person Homepage



Anzeigen von Homepage

Zeigen Sie Accountstatus und -Verstöße, umsetzbare Einblicke und administrative Steuerungen im an Homepage .

Greifen Sie auf zu Homepage

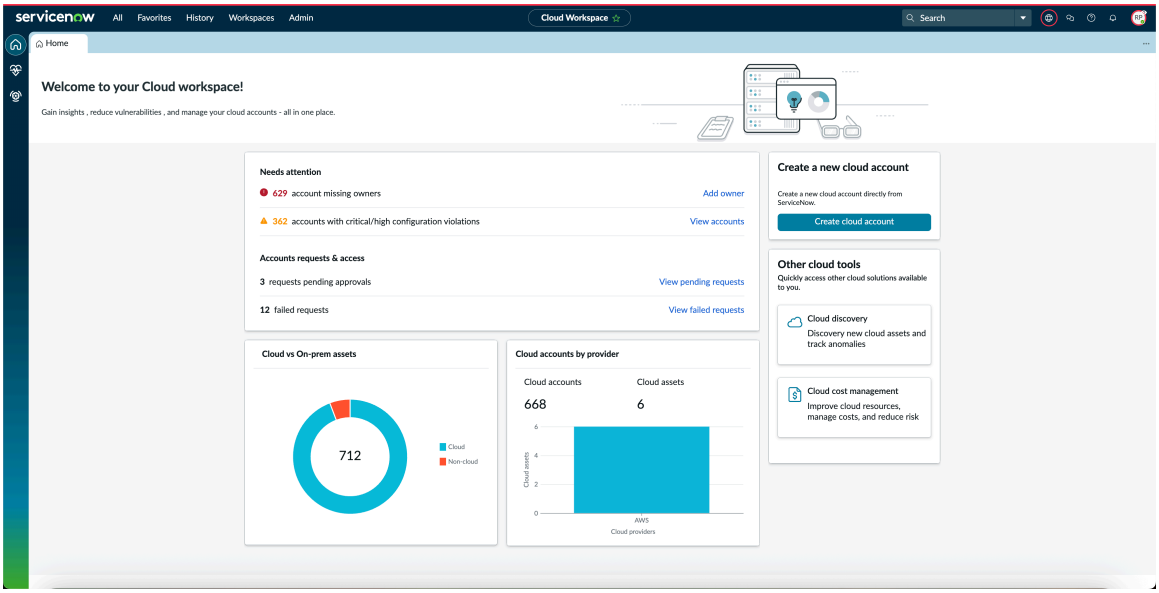
Als Administrator Oder Asset-Betrachter , Sie können auf zugreifen Homepage Auf eine der beiden Arten.

- Navigieren zu **Alle** > **Cloud-Arbeitsbereich**
- Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administrator-Dashboard



Hinweis:

- Das Widget „Handlungsbedarf“ wird nur für Administratoren mit angezeigt Cloud Account Management Berechtigung.
- Das Widget „andere Cloud-Tools“ zeigt die auf Ihrer Instanz installierten Anwendungen an. Cloud-Discovery ist eine Voraussetzung für die Installation Cloud Account Management.

Anzeigen des Compliance-Dashboards

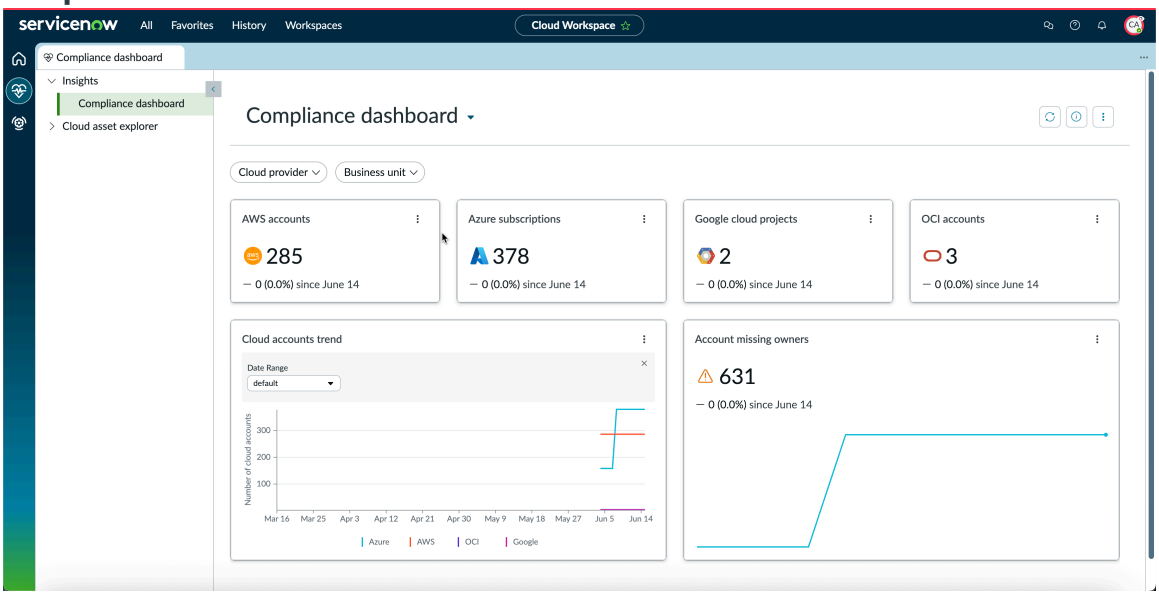
Die Cloud-Arbeitsbereich Compliance Das Dashboard bietet Einblicke, die der Sicherheit helfen Team S Identifizieren Sie Cloud-Ressourcen ohne Besitzinformationen, und kennzeichnen Sie angreifbare oder gefährdete Ressourcen. Dies Informationen helfen Teammitgliedern Führen Sie Sicherheits-Audits durch, und bestätigen Sie die Compliance mit Branchenvorschriften in Cloud-Umgebungen.

Greifen Sie auf das Compliance-Dashboard zu

Als Administrator können Sie auf das Dashboard zugreifen Indem Sie zu navigieren **Alle** > **Cloud-Arbeitsbereich** > **Überwachen und nachverfolgen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compliance-Dashboard



Hinweis:

- Im Compliance-Dashboard werden nur die in Ihrer Instanz erkannten Accounts angezeigt.
- Im Compliance-Dashboard wird die Anbieterkarte ausgeblendet, wenn keine Accounts bereitgestellt werden.

Cloud-Asset-Explorer anzeigen

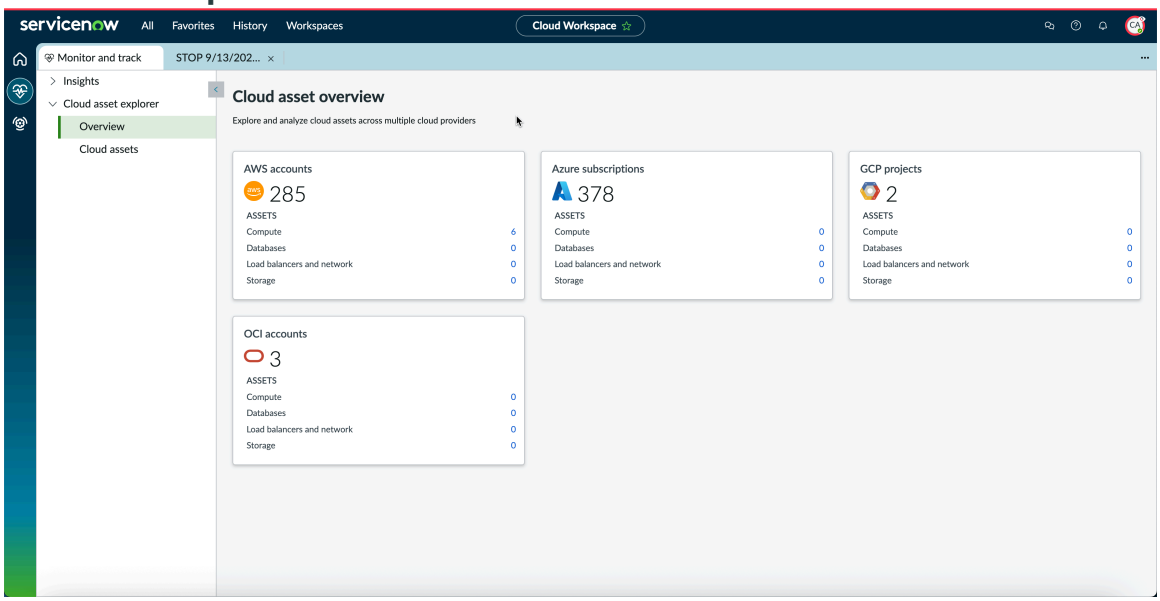
Das Dashboard hilft Cloud-Governance- und Betriebsteams, Compliance- und Asset-Details effizienter zu überwachen, nachzuverfolgen und zu bearbeiten. Als Asset-Betrachter können Sie alle Assets anzeigen und Drilldown durchführen, um detaillierte Informationen zu jedem Konfigurationselement (CI) anzuzeigen.

Sie können auf zwei Arten auf das Dashboard zugreifen.

- Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Cloud-Asset-Explorer**
- Navigieren zu **Arbeitsbereiche** > **Cloud-Arbeitsbereich** > **Cloud-Asset-Explorer**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Asset-Explorer-Dashboard



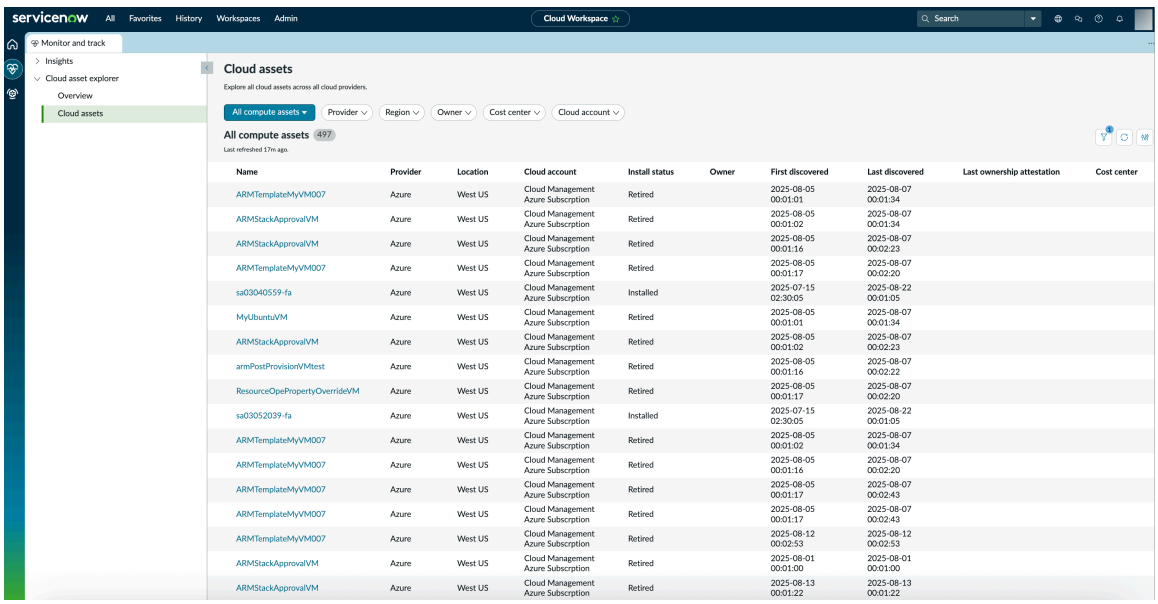
Hinweis: Sie können die Konfiguration der Asset-Sammlung aktivieren oder deaktivieren, um die CIs aufzulisten. Weitere Informationen finden Sie unter Konfigurieren Sie die Cloud-Asset-Sammlungstabelle.

Cloud-Assets werden angezeigt

Auf dieser Seite wird die Ansicht „Cloud-Assets“ angezeigt. Listet alle Computing-Assets über verbundene Cloud-Anbieter wie AWS, Azure, GCP und OCI zusammen mit Standort, Cloud-Account, Installationsstatus, Besitzer, Erkennungsdaten auf. Besitznachweis und Kostenstelle.

Als Administrator können Sie auf das Dashboard zugreifen, indem Sie zu navigieren **Alle** > **Cloud-Arbeitsbereich** > **Überwachen und nachverfolgen**

Cloud-Assets

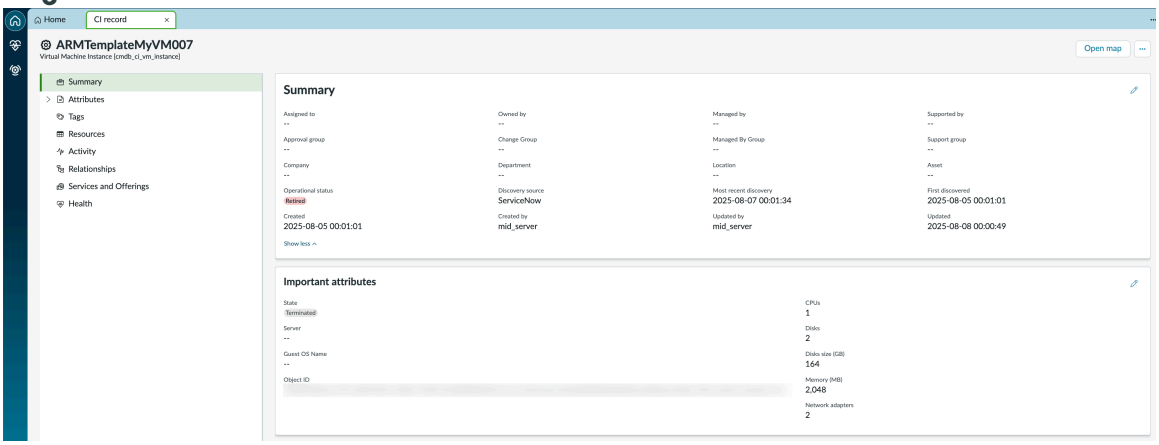


Klicken Sie auf den entsprechenden Namen, um die Details anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Cloud-Asset-Details an



Im Asset-Explorer bleiben stillgelegte Konfigurationselemente (Configuration Items, CIs) auch nach der Stilllegung in der Asset-Tabelle, solange sie in der CMDB vorhanden sind. Um dies zu verwalten, können Anwender einen anwenderdefinierten Aufbewahrungszeitraum (in Sekunden) konfigurieren, der stillgelegte CIs nach der definierten Dauer automatisch aus der Asset-Tabelle entfernt. Wenn Sie die Eigenschaft beispielsweise auf 86.400 Sekunden (1 Tag) festlegen, wird sichergestellt, dass ein stillgelegtes CI einen Tag nach der Stilllegung aus der Asset-Tabelle entfernt wird, auch wenn es in der CMDB weiterhin vorhanden sein kann. Dies trägt zur Verbesserung der Leistung in Umgebungen mit hohem Volumen bei, indem sichergestellt wird, dass nur aktive CIs in der Asset-Tabelle verbleiben.

Weitere Informationen zu den verschiedenen Abschnitten finden Sie unter Verwalten der Asset-Details des Cloud-Arbeitsbereichs.

Erstellen eines Cloud-Accounts

Das Erstellen eines Cloud-Accounts umfasst die Übermittlung einer Account-Anforderung durch die anfordernde Person, die Genehmigung oder Ablehnung der Anforderung durch einen Genehmiger und die Bereitstellung des Accounts durch den Administrator.

Fordern Sie einen Cloud-Account an

Fordern Sie einen Cloud-Account als anfordernde Person an. Eine Benachrichtigungs-E-Mail wird gesendet, wenn die anfordernde Person eine Account-Anforderung erstellt.

Vorbereitungen

Die ServiceNow der administrator muss die Daten für den Account-Besitzer, die Kostenstelle, den Geschäftsbereich, die Abteilung und die Geschäftsanwendung ausgefüllt haben.

Erforderliche Rolle: sn_itom_Cam.cw_Requester

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich**an.
2. Von Startseite Seite , Wählen Sie aus **Anforderung** .
3. Auf der Fordern Sie einen neuen Cloud-Account an Füllen Sie die Felder aus.

   Eine Beschreibung der Feldwerte finden Sie unter Anforderungsfelder für neue Cloud-Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zum Erstellen Ihres anwenderdefinierten Katalogs finden Sie unter Konfigurieren Sie eine anwenderdefinierte Katalog-ID in Cloud Account Management Account-Anforderung.

4. Wählen Sie **Absenden**.

Genehmigen Sie eine Cloud-Account-Anforderung

Genehmigen oder verweigern Sie eine Cloud-Account-Anforderung als Genehmiger. Eine Benachrichtigungs-E-Mail wird empfangen, wenn die anfordernde Person eine Account-Anforderung erstellt. Wenn ein Cloud-Account angefordert wird, erfasst die Tabelle die Details der Anforderung und ruft sie ab. Sobald Cloud Account Management Anforderung wird genehmigt und einem Bereitsteller zugewiesen, z. B. CCOE, DevOps oder SRE.

Vorbereitungen
Erforderliche Rolle: sn_itom_Cam.cw_Approver

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Accounts anzeigen**an.
2. Auswahlvorgang **Anforderungen** > **Ausstehende Genehmigungen**an.
3. Überprüfen Sie die Anforderung, und wählen Sie aus **Genehmigen** Oder **Ablehnen** .
4. Bestätigen Sie Ihre Entscheidung.

Stellen Sie einen Cloud-Account bereit

Stellen Sie einen Cloud-Account als Administrator über bereit Cloud-Arbeitsbereich.

Vorbereitungen
Bestätigen Sie, dass der Cloud-Kontext konfiguriert wurde. Weitere Informationen finden Sie unter Konfigurationen werden erstellt.

Discovery muss im Cloud-Administratorportal durchgeführt worden sein.

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Anforderungen**an.
2. Wählen Sie auf der Seite „Account-Anforderungen“ die Option aus **Genehmigte Anforderungen** Kachel.
3. Wählen Sie den bereitzustellenden Account aus.
4. In **Wählen Sie Cloud-Kontext aus** Füllen Sie die Felder aus.

Feld	Beschreibung
Cloud-Provider	Dieses Feld wird in der Anforderung automatisch auf die Cloud-Anbieterplattform festgelegt.
CAM konfigurieren	Konfigurationsname der Cloud-Organisation.
Organisationseinheit (wird für angezeigt AWS)	Organisationseinheit (OU) ist die Liste der Einheiten, die nach der Ausführung der Discovery automatisch ausgefüllt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verwaltungsgruppe (wird für angezeigt Azure)	Verwaltungsgruppen helfen Ihnen, mehrere Abonnements zu verwalten, indem sie Governance-Einstellungen anwenden, die automatisch für alle Abonnements in ihnen gelten. Dieses Feld wird automatisch auf die Verwaltungsgruppe festgelegt, die nach der Discovery gefunden wurde.

5. Wenn Sie eine bereitstellen Azure Account festlegen, ob ein vorhandenes Abrechnungskonto verwendet oder ein neues Abrechnungskonto erstellt und hinzugefügt werden soll.

Option	Aktion
Fügen Sie ein vorhandenes Abrechnungs-konto hinzu	Wählen Sie einen vorhandenen Account aus der Dropdown-Liste aus.
Erstellen und fügen Sie einen neuen einzelnen Account hinzu	**a.** Wählen Sie das Symbol Neues Abrechnungskonto erstellen (+). **b.** Wählen Sie Aus **Einzelner Account** . **c.** In **Account-Name** Geben Sie den Account-Namen ein. **d.** In **Anzeigename** Feld den Anzeigenamen eingeben. **e.** Wählen Sie **Hinzufügen**.
Erstellen und fügen Sie neue Massenkonten hinzu	**a.** Wählen Sie das Symbol Neues Abrechnungskonto erstellen (+). **b.** Wählen Sie Aus **Massenupload** . **c.** Suchen Sie nach dem Mandantennamen, und wählen Sie ihn aus. **d.** Unter **Geben Sie die API-Antwort ein** Wählen Sie den Link aus Azure-Playground . **e.** Melden Sie sich bei an Azure Portal. **f.** Kopieren Sie im Azure-Portal die Beispiel-JSON-Antwort, die unter angezeigt wird **RegistrierungAccountsListByBillingAccount** Abschnitt. **g.** In Cloud Account Management Anwendung, fügen Sie die Beispiel-JSON-Antwort in ein **Geben Sie die API-Antwort ein** Feld. **h.** Wählen Sie **Hinzufügen**.

6. Wenn Sie eine bereitstellen Azure Account festlegen, ob ein vorhandenes Registrierungskonto verwendet oder ein neues Registrierungskonto erstellt und hinzugefügt werden soll.

   Ein Registrierungs-Account ist eine Verwaltungseinheit innerhalb eines Abrechnungsaccounts für Organisationen mit einem Enterprise Agreement (EA), das zum Organisieren und Steuern verwendet wird Azure Abonnements und Ressourcen.

Option	Aktion
Registrie-rungsaccount	Wählen Sie einen vorhandenen Account aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Erstellen und fügen Sie einen neuen einzelnen Account hinzu	**a.** Wählen Sie das Symbol Neues Registrierungskonto erstellen (+). **b.** Wählen Sie Aus **Einzelner Account** . **c.** In **Account-Name** Geben Sie den Account-Namen ein. **d.** In **Anzeigename** Feld den Anzeigenamen eingeben. **e.** Suchen Sie nach dem Mandantennamen, und wählen Sie ihn aus. **f.** Wählen Sie **Hinzufügen**.
Erstellen und fügen Sie neue Massenkonten hinzu	**a.** Wählen Sie das Symbol Neues Registrierungskonto erstellen (+). **b.** Wählen Sie Aus **Massenupload** . **c.** Suchen Sie nach dem Mandantennamen, und wählen Sie ihn aus. **d.** Unter **Geben Sie die API-Antwort ein** Wählen Sie den Link aus Azure-Playground . **e.** Melden Sie sich bei an Azure Portal. **f.** Kopieren Sie im Azure-Portal die Beispiel-JSON-Antwort, die unter angezeigt wird **RegistrierungAccountsListByBillingAccount** Abschnitt. **g.** In Cloud Account Management Anwendung, fügen Sie die Beispiel-JSON-Antwort in ein **Geben Sie die API-Antwort ein** Feld. **h.** Wählen Sie **Hinzufügen**.

7. **Wahlweise:** Geben Sie einen Kommentar an.
   a. In **Arbeitsnotizen** Geben Sie im Abschnitt Ihre Kommentare ein **Kommentare** Textfeld.
   b. Wählen Sie Aus **Kommentar Veröffentlichen** .
8. Wählen Sie in der oberen rechten Ecke des Bildschirms aus **Bereitstellung** .
9. Bestätigen Sie im Dialogfeld die Bereitstellungsanforderung, indem Sie auswählen **Ja** .

Ergebnis

Basierend auf dem definierten Kontext Cloud Account Management Erstellt einen Abonnement-Account innerhalb der angegebenen Cloud-Organisation und AWS Organisationseinheit oder Azure Verwaltungsgruppe.

Cloud-Accounts verwalten

Mit der Verwaltung eines Cloud-Accounts können Sie eine Reihe von Aufgaben ausführen, z. B. das Abbrechen, Aussetzen oder Reaktivieren von Cloud-Accounts und das Hinzufügen nicht verwalteter Accounts.

Account-Management-Aktivitäten

Aktivität	Beschreibung
Brechen Sie eine Cloud-Account-Anforderung ab	Anfordernde Personen können ihre eigenen Account-Anforderungen stornieren.
Sperren Sie einen Cloud-Account	Gesperrte Accounts können weiterhin zusammen mit ihren Ressourcen verwendet werden, aber es können keine neuen Ressourcen dafür

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Account-Management-Aktivitäten (Fortsetzung)

Aktivität	Beschreibung
	erstellt werden. Bevor Sie die Kontosperrung anfordern ServiceNow der administrator muss bereits eine Aussetzungskonfiguration eingerichtet haben.
Aktivieren Sie einen Cloud-Account erneut	Gesperrte Accounts können erneut aktiviert werden.
Fügen Sie einen nicht verwalteten Cloud-Account hinzu	Sie können Cloud-Accounts importieren, um sie zu verwalten.

Brechen Sie eine Cloud-Account-Anforderung ab

Brechen Sie eine Account-Anforderung ab, die Sie übermittelt haben.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_Requester

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Startseite**an.
2. Wählen Sie aus **Anforderungen** Registerkarte.
3. Wählen Sie einen Account unter aus **Angefordert** Bereich.
4. Wählen Sie Aus **Anforderung Abbrechen** .
5. Wählen Sie Aus **Ja** Zur Bestätigung.

Sperren Sie einen Cloud-Account

Sperren Sie einen Account, wenn eine Budgetbeschränkung vorliegt oder der Accountbesitzer in der Organisation nicht verfügbar ist. Nur Administratoren und Accountbesitzer können die gesperrten Accounts anzeigen.

Vorbereitungen

Für einen Account muss ein Aussetzungsprofil ausgesetzt werden. Weitere Informationen finden Sie unter Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet.

Erforderliche Rolle: sn_itom_Cam.cw_admin oder sn_itom_Cam.cw_requestor

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Startseite**an.
2. Wählen Sie Aus **Abonnement-Accounts** .
3. Unter **Verwaltete Accounts** Abschnitt auswählen **Aktiv** .
4. Aktivieren Sie ein Account-Kontrollkästchen, und wählen Sie aus **Anhalten** .
5. Geben Sie im Bestätigungsdialogfeld den Grund für die Aussetzung ein, und wählen Sie aus **Ja** .
   - Sobald Sie eine Aussetzungsanforderung erstellt haben, wird die Anforderung zur Genehmigung an den Administrator gesendet.
   - Gesperrte Accounts werden unter aufgeführt **Verwaltete Accounts** > **Angehalten** Abschnitt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie einen Cloud-Account erneut

Aktivieren Sie einen Account, der zuvor ausgesetzt wurde, erneut, wenn der Account abgerufen werden muss. Nach der erneuten Aktivierung eines Accounts ändert sich der Accountstatus von „ausgesetzt“ in „aktiv“. Nur Cloud Account Management Verwaltete Accounts können erneut aktiviert werden.

Warum und wann dieser Vorgang ausgeführt wird

Nur ein Administrator oder Account-Besitzer kann den erneut aktivierten Account anzeigen.

Vorbereitungen

Ein Aussetzungsprofil muss vorhanden sein, damit ein Account erneut aktiviert werden kann. Weitere Einzelheiten finden Sie unter Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet.

Erforderliche Rolle: sn_itom_Cam.cw_admin oder sn_itom_Cam.cw_requestor

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Startseite**an.
2. Wählen Sie Aus **Abonnement-Accounts** .
3. In **Verwaltete Accounts** Abschnitt auswählen **Angehalten** .
4. Wählen Sie einen Eintrag in der Liste der gesperrten Accounts aus, und wählen Sie aus **Erneut Aktivieren** .
5. Geben Sie einen Grund für die erneute Aktivierung in ein **Grund** Feld und wählen Sie aus **Ja** .
   Die Reaktivierungsanforderung wird zur Genehmigung gesendet. Reaktivierte Accounts werden in aufgeführt **Verwaltete Accounts** Abschnitt.

Fügen Sie einen nicht verwalteten Cloud-Account hinzu

Die Verwaltung eines Cloud-Accounts umfasst die Nachverfolgung von Budgets, die Überprüfung auf Konfigurationsverstöße und die Validierung von Zertifikaten. Das Verfahren hilft Ihnen beim Onboarding eines nicht verwalteten Cloud-Accounts.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Abonnement-Accounts**an.
2. In **Nicht Verwaltete Accounts** Abschnitt auswählen **Alle Accounts** .
3. Wählen Sie einen Account aus, und wählen Sie aus **Account Verwalten** .

   Hinweis: Derzeit nur AWS Accounts werden unterstützt.

4. Füllen Sie im Anforderungsformular die Felder Kostenstelle, Abteilung, Account-Besitzer und Geschäftsbereich aus.

   Eine Beschreibung der Feldwerte finden Sie unter Anforderungsfelder für neue Cloud-Accounts.

5. Wählen Sie Aus **Account-Details Aktualisieren Und Verwalten** .
   Eine Bestätigungsnachricht wird angezeigt, dass Ihr Account integriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisieren Sie die Cloud-Account-Details

Halten Sie die Account-Details auf dem neuesten Stand, damit Sie Richtlinienverstöße effektiv identifizieren und beheben können.

Vorbereitungen

Erforderliche Rolle: sn_itom_Cam.cw_admin

Prozedur

1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Accounts anzeigen**an.
2. Unter **Alle Cloud-Accounts** , Wählen Sie einen Account aus.
   Die **Übersicht** Auf der Registerkarte werden allgemeine Details, Besitzdetails und Zertifizierungsdetails angezeigt.
3. Wenn die Details des Account-Besitzers nicht festgelegt sind, wählen Sie aus **Account verwalten** Und aktualisieren Sie die Besitzerdetails.
   Dieser Name des Account-Besitzers wird automatisch täglich an neu erstellte CIs weitergegeben.
4. **Wahlweise:** Aktualisieren Sie bei Bedarf die Accountinformationen.

   a. Wählen Sie das Bearbeitungssymbol ( ).

   b. Aktualisieren Sie die Informationen.

Felder	Beschreibung
Kostenstelle	Name der Kostenstelle, die diesem Account zugeordnet werden soll.
Geschäftsbereich	Name des Geschäftsbereichs, der diesem Account zugeordnet werden soll.
Anwendungsservice	Das Projekt oder die Anwendung, das bzw. die diesem Account zugeordnet werden soll.
Abteilung	Abteilungsname, der diesem Account zugeordnet werden soll.

5. **Wahlweise:** Aktualisieren Sie bei Bedarf den Account-Besitzer.

   a. Wählen Sie das Bearbeitungssymbol ( ).

   b. Wählen Sie aus **Account-Besitzer** Aus der Dropdown-Liste.

6. **Wahlweise:** Propagieren Sie die Namensänderung an zugeordnete CIs, oder stoppen Sie die Verbreitung.
   - Um den Besitzernamen zu propagieren, ändern Sie die Änderung an den Cloud-Account und alle zugehörigen CIs, die direkt mit dem Cloud-Account verknüpft sind, indem Sie vorhandene Besitzernamen überschreiben, indem Sie auswählen **Übertragen Sie das Eigentum an CIs** .

     Zugeordnete CIs enthalten Elemente wie S3-Bucket oder VM. CIs, die nicht direkt mit dem Cloud-Account verknüpft sind, umfassen Dinge wie Azure Availability Zones.
   - Um die zukünftige Verbreitung des Besitzernamen zu entfernen, löschen Sie **Übertragen Sie das Eigentum an CIs** Option.

     Der Besitzername ist nicht mehr neu zugeordneten CIs zugewiesen, wird jedoch für die vorhandenen CIs beibehalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie eine große Anzahl von CIs haben, kann die Verbreitung einige Zeit in Anspruch nehmen, und Änderungen werden möglicherweise nicht sofort berücksichtigt. Sie können den Fortschritt überprüfen, indem Sie auf die Tabelle „sn_itom_Cam_Subscription_Account_Batch_Job_list“ zugreifen und den Status der in aufgeführten Aufträge „owner_Name“ überprüfen **Parameter** Spalte.

7. Wählen Sie das Symbol Speichern ( ).

Zertifizieren Sie einen Account

Eine Zertifizierungsaufgabe stellt die Arbeit der Verifizierung und Zertifizierung der Daten dar, die einem Datensatz zugeordnet sind. Der Zertifizierer überprüft Aufgaben, die nach der Datenvalidierung erstellt wurden, anhand der veröffentlichten Richtlinie. Die Accountzertifizierung hilft bei der Lösung von Problemen wie veraltetem Besitz, inaktiven Anwenderprofilen und falschen Berechtigungen in Cloud-Accounts.

Vorbereitungen

Stellen Sie sicher, dass der Administrator überprüft hat Cloud Account Management Standardrichtlinie. Optional kann der Administrator basierend auf den Organisationsanforderungen Richtlinien anpassen oder neue hinzufügen. Weitere Informationen finden Sie unter Überprüfen – Standard Cloud Account Management Zertifizierungsrichtlinie. Das ITOM Cloud Account Management Zertifizierungsgruppe muss mindestens einen Anwender enthalten.

Hinweis: Cloud Account Management der administrator kann Anwender zu hinzufügen Cloud Account Management Zertifizierungsgruppe, indem Sie zu navigieren **Alle** > **Account-Zertifizierung** > **ITOM-CAM-Zertifizierungsgruppe** > **Gruppenmitglieder**an.

Erforderliche Rolle: sn_itom_Cam.cw_Certifier

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

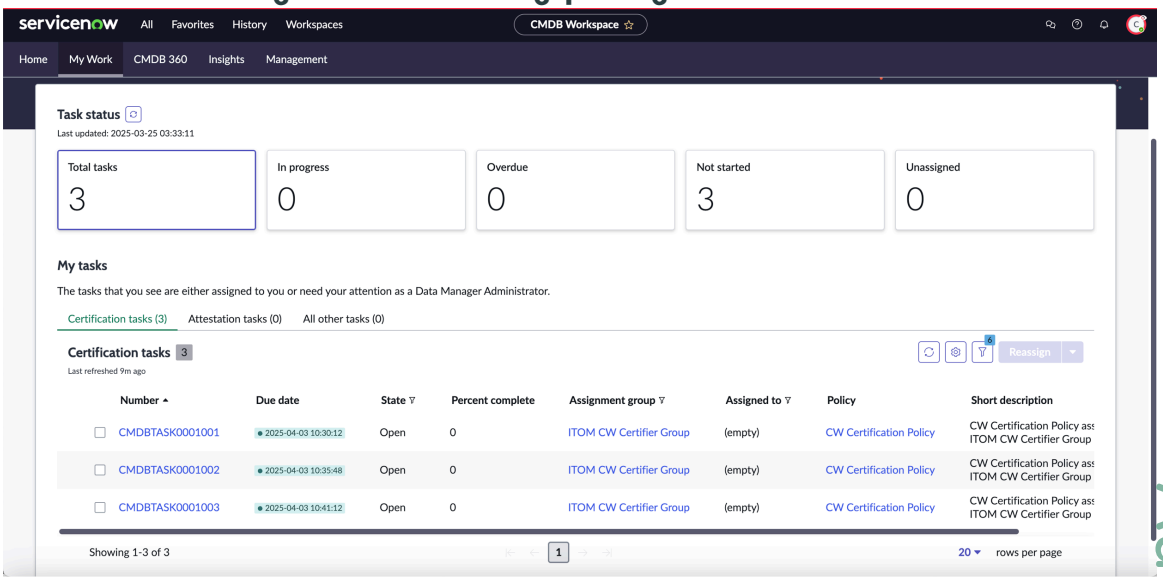
1. Navigieren zu **Alle** > **Cloud-Arbeitsbereich** > **Account-Zertifizierungsaufgaben**an.

   Die Liste unter Zertifizierungsaufgaben zeigt ausstehende Zertifizierungsaufgaben an.

2. Wählen Sie auf der Registerkarte Zertifizierungsaufgaben die Zertifizierungsaufgabe aus, die Sie überprüfen möchten.
3. Überprüfen Sie die Details der Zertifizierungsaufgabe, und wählen Sie dann aus **Überprüfen Sie die zu zertifizierenden Datensätze** .
4. Wählen Sie auf der Registerkarte Überprüfung nicht abgeschlossen die Datensätze aus, für die Sie die Überprüfung abschließen möchten, und wählen Sie dann aus **Zertifizieren** Oder **Fehlgeschlagen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Zertifizierungsprüfung



Hinweis: Wenn Sie auswählen **Fehlgeschlagen** , Die Aufgabe wird in die Registrierung und verschoben Cloud Account Management der administrator führt die nächste Aktion aus. Sie können auch den Besitz einer Aufgabe neu zuweisen.

5. Wählen Sie die Datensätze aus, die Sie im Detail überprüfen möchten, und wählen Sie dann aus **Überprüfen Sie Datensätze** .
6. Wählen Sie Aus **Übermitteln** Wenn alle Datensätze überprüft wurden.
   Die **Übermitteln** Die Schaltfläche ist erst verfügbar, wenn alle Datensätze in der Aufgabe überprüft wurden und die Aufgabe abgeschlossen ist.
7. **Wahlweise:** Weisen Sie Besitzer zu (wenn sie leer sind), indem Sie sie auswählen und gedrückt halten (oder mit der rechten Maustaste klicken) **Im Besitz Von** Eingabe und Auswahl des Namens aus der Suche.

Hinweis:

Der Accountzertifizierungsstatus ändert sich in Ausstehend, wenn er die Richtlinienbedingungen des Administrators für die erneute Zertifizierung erfüllt.

Weitere Informationen zum Zertifizieren einer Aufgabe finden Sie unter Überprüfen Sie Zertifizierungsaufgaben im CMDB-Arbeitsbereich .

Cloud Account Management – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von Cloud Account Management In Cloud-Arbeitsbereich Anwendung.

Mit Cloud Account Management installierte Komponenten

Mit werden mehrere Anwenderrollen installiert Cloud Account Management App.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rolle	Beschreibung	Gruppe, die die Rolle bereitstellt
Anfordernde Person [sn_itom_Cam.cw_anfordernde Person]	Teamleiter oder Vertreter der Anwendung. • Initiiert Anforderungen zur Erstellung eines Cloud-Accounts. • Erstellen Sie Anforderungen für die Aussetzung oder erneute Aktivierung ihrer eigenen Accounts.	ITOM CAM Gruppe Der Anfordernden Person
Genehmigende Person [sn_itom_Cam.cw_Approver]	Vorgesetzter, Manager oder Finanzgenehmiger. Überprüft Anforderungen und genehmigt sie oder lehnt sie ab.	ITOM CAM Genehmigergruppe
Administrator [sn_itom_Cam.cw_admin]	Mitglied des Cloud Center of Excellence (CCOE) oder Sites Reliability Engineer (SRE). • Bestätigt das Cloud Account Management Konfigurationen richten sich an der Cloud und aus Terraform Konfigurationen. • Passt die Datenzertifizierungsrichtlinie an. • Erstellt Accounts, die sich außerhalb von befinden Cloud Account Management Anwendung.	ITOM CAM Administratorgruppe
Zertifizierer [sn_itom_Cam.cw_Certifier]	Markiert einen Account als zertifiziert oder fehlgeschlagen.	ITOM CAM Zertifizierungsgruppe

Informationen zur Rückkehr zum Hauptthema finden Sie unter Cloud Account Management erkunden.

Terraform Account-Konfigurationsfelder

Terraform Kontokonfigurationsformular und Beschreibungen der zugehörigen Listenfelder.

Konfigurationstyp: Account erstellen

Feld	Beschreibung
Bereitstellungsmodus	Name des Bereitstellungsmodus. Hier sollte es sein Terraform.
Cloud-Anbieter	Der Name der Cloud-Provider-Plattform. Derzeit nur AWS Wird unterstützt.
Cloud-Organisation	Die Cloud-Organisation, in der der Abonnementaccount erstellt wird. Weitere Einzelheiten finden Sie unter Füllen Sie Aus Cloud Account Management Abhängige Tabellen.
Name	Ein Name zur Identifizierung der Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationstyp: Account erstellen (Fortsetzung)

Feld	Beschreibung
Stamm-E-Mail	Cloud Account Management Verwendet eine E-Mail-Adresse, um die Stamm-E-Mail-ID für den neu erstellten Account zu generieren. Wenn Ihre Stamm-E-Mail-ID beispielsweise myawsaccount@example.com lautet, wird die Cloud Account Management Die Anwendung hängt eine Anforderungs-ID an, um myawsaccount-CWSAREQ0000001@example.com zu generieren. **Hinweis:** Informationen zum Erstellen einer Stamm-E-Mail finden Sie unter Richten Sie die Stamm-E-Mail in ein, und überprüfen Sie sie AWS.
Terraform-URL	Eine Standard-URL wird angezeigt. Sie können die URL anpassen, indem Sie auf das Bearbeitungssymbol klicken .
Terraform OAuth-Token-ID	Die OAuth-Token-ID, die angegeben wurde, wenn Sie den VCS-Provider in konfiguriert haben Terraform.
Terraform-Anmeldeinformationen	Die Terraform Anmeldeinformationen, die Sie konfiguriert haben. Die Einträge werden aus dem ausgefüllt CMDB Datensätze.
Terraform Organisation	Die Terraform Organisationsname, der als Arbeitsbereich zum Erstellen eines Abonnements verwendet wird.
VCS-Bezeichner	GitHub(Oder Versionssteuerungssystem (VCS)) Standort von Terraform Vorlage.
Beschreibung	Option zum Bereitstellen einer Beschreibung für Terraform Account.

Informationen zur Rückkehr zum Verfahren finden Sie unter Erstellen Sie einen Terraform Account-Konfiguration.

Konfigurationskontofelder der Cloud-nativen Schnittstelle

Beschreibungen des Kontos für die Konfiguration der nativen Cloud-Schnittstelle und der zugehörigen Listenfelder.

Konfigurationstyp: Account erstellen

Feld	Beschreibung
Bereitstellungsmodus	Name des Bereitstellungsmodus. Hier sollte es sich um eine native Cloud-Schnittstelle handeln.
Cloud-Anbieter	Name der Cloud-Provider-Plattform. Unterstützt derzeit AWS Und Azure Plattformen.
Cloud-Organisation	Die Cloud-Organisation, in der der Abonnementaccount erstellt werden soll.
Name	Ein Name zur Identifizierung der Konfiguration.
Stamm-E-Mail (AWS)	Cloud Account Management Verwendet eine E-Mail-Adresse, um die Stamm-E-Mail-ID für den neu erstellten Account zu generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationstyp: Account erstellen (Fortsetzung)

Feld	Beschreibung
	Wenn Ihre Stamm-E-Mail-ID beispielsweise myawsaccount@example.com lautet, wird die Cloud Account Management Die Anwendung hängt eine Anforderungs-ID an, um myawsaccount-CWSAREQ0000001@example.com zu generieren. **Hinweis:** Informationen zum Erstellen einer Stamm-E-Mail finden Sie unter Richten Sie die Stamm-E-Mail in ein, und überprüfen Sie sie AWS.
Cloud-Anmeldeinformationsalias	Alias für den Zugriff auf alle Cloud-APIs erstellt. Die Einträge werden aus dem ausgefüllt CMDB Datensätze. **Hinweis:** Nur Cloud Account Management der administrator kann den Cloud-Anmeldeinformationsalias konfigurieren. Informationen zum Konfigurieren des Cloud-Anmeldeinformationsalias finden Sie unter Einrichten AWS API-Konfigurationsinformationen in ServiceNow.
Beschreibung	Informationen, die in Arbeitsnotizen aufgezeichnet werden können.

Informationen zur Rückkehr zum Verfahren finden Sie unter Erstellen Sie eine Accountkonfiguration für die native Cloud-Schnittstelle.

Anforderungsfelder für neue Cloud-Accounts

Beschreibungen des neuen Cloud-Account-Anforderungsformulars und der zugehörigen Listenfelder.

Fordern Sie einen Cloud-Account an

Felder	Beschreibung
Umgebung	Name der Umgebung .
Gewünschter Cloud-Provider	Name der Cloud-Anbieterplattform, z. B. AWS Oder Azure.
Monatliches Budgetlimit	Monatliches Budget für diesen Account. **Hinweis:** Wenn der Budgetschwellenwert erreicht ist, wird eine E-Mail-Warnung an den Stammanwender von gesendet AWS Organisationsaccount und Besitzer des neu erstellten Accounts. Selbst wenn der Schwellenwert überschritten wird, gibt es keine Einschränkungen beim Zugriff auf den Account, Sie können jedoch keine Ressourcen für den gesperrten Account erstellen.
Projekt-/Anwendungsservice	Das Projekt oder die Anwendung, das bzw. die diesem Account zugeordnet werden soll.
Account-Besitzer	Besitzer dieses Accounts.
Kostenstelle	Kostenstelle, die diesem Account zugeordnet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fordern Sie einen Cloud-Account an (Fortsetzung)

Felder	Beschreibung
Geschäftsbereich	Geschäftsbereich, der diesem Account zugeordnet werden soll.
Abteilung	Abteilung, die diesem Account zugeordnet werden soll.
Geschäftsanwendung	Geschäftsanwendung, die diesem Account zugeordnet werden soll.
Cloud-Account – Namenssuffix	Suffix für einen Namen zur einfacheren Nachverfolgung.
Cloud-Account – Name	Automatisch ausgefüllter Cloud-Account-Name.
Tags	Schlüssel-Wert-Informationen, um den Account zu kategorisieren. Zum Beispiel nach Region, Land, Organisation oder Zweigstelle.

Informationen zur Rückkehr zum Verfahren finden Sie unter Fordern Sie einen Cloud-Account an.

Konfigurationsfelder für Account sperren

Sperren Sie das Kontokonfigurationsformular und die zugehörigen Listenfeldbeschreibungen.

Konfigurationstyp: Account sperren

Feld	Beschreibung
Cloud-Anbieter	Name der Cloud-Provider-Plattform. Die Einträge werden aus abgerufen CMDB Datensätze.
Cloud-Organisation	Die Cloud-Organisation, die den Abonnementaccount erstellt.
Name	Ein Name zur Identifizierung der Konfiguration.
Cloud-Anmeldeinformationsalias	Der von Ihnen konfigurierte Cloud-Anmeldeinformationsalias. Die Einträge werden aus dem ausgefüllt CMDB Datensätze.
ID der SCP-Richtlinie für Aussetzung (gilt nur für AWS)	Die AWS ID der Aussetzungsrichtlinie. Diese Richtlinien-ID wird verwendet, um anzuhalten AWS Account. Servicesteuerungsrichtlinien beschränken die Ressourcen, Services und API-Vorgänge. Zum Konfigurieren AWS Richtlinie aussetzen, siehe Richten Sie die Aussetzung von ein AWS Account, der die Servicesteuerrichtlinie verwendet.
ID der Azure-Aussetzungsrichtlinie (gilt nur für Azure)	Die Azure ID der Aussetzungsrichtlinie. Diese Richtlinien-ID wird verwendet, um anzuhalten Azure Account. Servicesteuerungsrichtlinien beschränken die Ressourcen, Services und API-Vorgänge. Zum Konfigurieren Azure Richtlinie aussetzen, siehe Richten Sie die Aussetzung eines Abonnements mit ein Azure Richtlinie.
Beschreibung	Informationen, die in Arbeitsnotizen aufgezeichnet werden können.

Informationen zur Rückkehr zum Verfahren finden Sie unter Sperren Sie einen Cloud-Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienliste zum Scannen von Cloud-Accounts

Eine Liste der Standardrichtlinien, die zum Scannen der Cloud-Accounts bereitgestellt werden.

Standardrichtlinien für Scan-Accounts

Richtlinienname	Beschreibung
Überprüfen AWS Discovery-Zeitplan	Überprüft, ob ein AWS Dem Account ist ein Discovery-Zeitplan angehängt. Die regelmäßige Ausführung von Discovery erleichtert die Identifizierung und Verwaltung potenzieller Sicherheitsrisiken.
Überprüfen AWS Account-Alias	Verifiziert einen AWS Account hat einen eindeutigen Alias, um die Account-Verwaltung zu verbessern, Fehler zu reduzieren und die Klarheit und Nachverfolgbarkeit in Ihrer AWS-Infrastruktur zu fördern. **Hinweis:** Stellen Sie sicher, dass Sie über API-Berechtigung für verfügen `iam: ListAccountAliasse` .
Überprüfen AWS Tag Des Account-Besitzers	Überprüft, ob ein AWS Der Account verfügt über einen bestimmten Besitzer, der die Verantwortlichkeit verbessert, die Reaktion auf Incidents optimiert und die Kommunikation innerhalb von erleichtert AWS Umgebung.
Überprüfen AWS Anwenderdefinierte Passwortrichtlinie	Überprüft, ob für jeden eine anwenderdefinierte Passwortrichtlinie festgelegt ist AWS Account. Eine robuste Passwortanforderung für alle IAM-Anwender erhöht die Schwierigkeit für Angreifer, Passwörter durch Brute-Force-Angriffe oder Versuche zum Diebstahl von Anmeldeinformationen zu knacken, was letztendlich die allgemeine Sicherheit von verbessert AWS Infrastruktur. **Hinweis:** Stellen Sie sicher, dass Sie über API-Berechtigung für verfügen `iam: GetAccountPasswordPolicy` .
Überprüfen AWS Zertifizierung Fehlgeschlagen	Verifiziert AWS Account-Zertifizierungsstatus. Fehlgeschlagene Zertifizierungen weisen auf potenzielle Sicherheitsschwachstellen hin, da gefährdete Anmeldeinformationen möglicherweise nicht umgehend deaktiviert werden, und bieten Angreifern ein Fenster mit Möglichkeiten, diese Schwachstellen auszunutzen.
Überprüfen AWS Ausstehende Zertifizierung	Überprüft, ob ein AWS Die Account-Zertifizierung befindet sich im Status „Ausstehend“, um die prompte Lösung ausstehender Zertifizierungen zu ermöglichen und potenzielle Sicherheitsschwachstellen zu vermeiden.
Überprüfen AWS Strenge Passwortrichtlinie	Überprüft, ob ein AWS Account hält sich an eine Richtlinie für sichere Passwörter, um die Sicherheit zu erhöhen. Diese Richtlinie erfordert robuste Anforderungen an die Passwortkomplexität, wodurch Ihr erheblich unterstützt wird AWS Schutz der Umgebung vor nicht autorisiertem Zugriff. **Hinweis:** Stellen Sie sicher, dass Sie über API-Berechtigung für verfügen `iam: GetAccountPasswordPolicy` .
Überprüfen Azure Discovery-Zeitplan	Überprüft, ob Azure Dem Account ist ein Discovery-Zeitplan angehängt. Diese Richtlinie hilft bei der sicheren und aktuellen Ressourcenlandschaft, um die Identifizierung und das Management potenzieller Sicherheitsrisiken zu erleichtern.
Überprüfen Azure Tag Des Account-Besitzers	Überprüft, ob Azure Account hat ein festgelegtes Besitzer-Tag, um die Verantwortlichkeit zu verbessern und die Kommunikation innerhalb Ihres zu erleichtern Azure Umgebung. Diese Richtlinie identifiziert leicht die verantwortliche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienname	Beschreibung
	Partei für jeden Account, wodurch eine Unternehmenskultur und eine optimierte Reaktion auf Incidents gefördert werden.
Überprüfen Azure Zertifizierung Fehlgeschlagen	Verifiziert Azure Account-Zertifizierungsstatus für Fehler beim Heraufstufen einer starken Zugriffssteuerung durch proaktive Überwachung für jeden Service-Account mit einem fehlgeschlagenen Zertifizierungsstatus. Fehlgeschlagene Zertifizierungen weisen auf potenzielle Sicherheitsschwachstellen hin, da gefährdete Anmeldeinformationen möglicherweise nicht umgehend deaktiviert werden. Diese Richtlinie minimiert das Zeitfenster, in dem Angreifer diese Schwachstellen ausnutzen können.
Überprüfen Azure Ausstehende Zertifizierung	Überprüft, ob Azure Die Service-Account-Zertifizierung befindet sich im Status „Ausstehend“. Diese Überwachung ermöglicht eine schnelle Lösung ausstehender Zertifizierungen und vermeidet potenzielle Sicherheitsschwachstellen.
Überprüfen GCP Discovery-Zeitplan	Überprüft, ob GCP Dem Account ist ein Discovery-Zeitplan angehängt. Diese Richtlinie hilft bei der sicheren und aktuellen Ressourcenlandschaft, um die Identifizierung und das Management potenzieller Sicherheitsrisiken zu erleichtern.
Überprüfen GCP Tag Des Account-Besitzers	Überprüft, ob GCP Account hat ein festgelegtes Besitzer-Tag, um die Verantwortlichkeit zu verbessern und die Kommunikation innerhalb Ihres zu erleichtern GCP Umgebung. Diese Richtlinie identifiziert leicht die verantwortliche Partei für jeden Account, wodurch eine Unternehmenskultur und eine optimierte Reaktion auf Incidents gefördert werden.
Überprüfen GCP Zertifizierung Fehlgeschlagen	Verifiziert GCP Account-Zertifizierungsstatus für Fehler beim Heraufstufen einer starken Zugriffssteuerung durch proaktive Überwachung für jeden Service-Account mit einem fehlgeschlagenen Zertifizierungsstatus. Fehlgeschlagene Zertifizierungen weisen auf potenzielle Sicherheitsschwachstellen hin, da gefährdete Anmeldeinformationen möglicherweise nicht umgehend deaktiviert werden. Diese Richtlinie minimiert das Zeitfenster, in dem Angreifer diese Schwachstellen ausnutzen können.
Überprüfen GCP Ausstehende Zertifizierung	Überprüft, ob GCP Account-Zertifizierung befindet sich im Status „Ausstehend“. Diese Überwachung ermöglicht eine schnelle Lösung ausstehender Zertifizierungen und vermeidet potenzielle Sicherheitsschwachstellen.

Informationen zur Rückkehr zum Verfahren finden Sie unter Richten Sie die Scankonfiguration für die Datenvisualisierung ein.

Cloud Account Management ACL-Gruppen, Rollen und Zuständigkeiten

Zugriffssteuerungslisten (ACLs), Gruppen und Rollen in Cloud Account Management Steuern Sie, wie Zugriffsberechtigungen in einer Cloud-Umgebung organisiert und verwaltet werden.

Gruppen und Rollen in Cloud Account Management

Cloud Account Management Gruppen und Verantwortlichkeiten

Gruppe	Rolle	Verantwortlichkeiten
ITOM Cloud Account Management Gruppe der anfordernden Person	sn_itom_Cam.cw_anfordernde Person	• Initiiert Cloud-Account-Anforderungen: Löst den Prozess zum Erstellen von Cloud-Accounts aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Gruppen und Verantwortlichkeiten (Fortsetzung)

Gruppe	Rolle	Verantwortlichkeiten
		• Begründet die Account-Erstellung: Gibt klare und überzeugende Gründe dafür an, warum jeder Cloud-Account benötigt wird. • Erfasst und übermittelt Account-Informationen: Erfasst und übermittelt alle erforderlichen Details, die für die erfolgreiche Erstellung eines Cloud-Accounts erforderlich sind. • Verwaltet den Account-Status: Fordern Sie bei Bedarf die Sperrung oder erneute Aktivierung von Cloud-Accounts an.
ITOM Cloud Account Management Genehmigergruppe	sn_itom_Cam.cw_Approver	• Bewertet und genehmigt Account-Anforderungen: Überprüfen Sie Accounterstellungsanforderungen, bewerten Sie ihre Gültigkeit sorgfältig, und richten Sie sie an Budgetbeschränkungen aus. Nach dieser Auswertung erteilt der Administrator die Genehmigung oder Ablehnung der Anforderung. • Überprüft die Budget-Compliance: Bestätigt, dass der angeforderte Cloud-Account an den verfügbaren Budgetressourcen ausgerichtet ist, bevor die Genehmigung erteilt wird. • Kommuniziert Entscheidungen mit klarer Begründung: Kommuniziert die Entscheidung über Genehmigung oder Ablehnung eindeutig an die anfordernde Person, indem der Anforderung selbst ein Kommentar hinzugefügt wird. Dieser Kommentar sollte eine kurze und informative Erklärung für die Entscheidung bieten.
ITOM Cloud Account Management Administratorgruppe	sn_itom_Cam.cw_admin	• Verifiziert die Konfigurationsausrichtung: Verifiziert das Cloud Account Management Konfigurationen sind konsistent und an Cloud-Provider-Konfigurationen und Terraform-Konfigurationen ausgerichtet. Dieser Prozess fördert sichere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Gruppen und Verantwortlichkeiten (Fortsetzung)

Gruppe	Rolle	Verantwortlichkeiten
		Zugriffsverwaltungspraktiken in allen Umgebungen. • Stellt Cloud-Accounts bereit: Konfiguriert den Cloud-Kontext, um neue Cloud-Accounts bereitzustellen, wodurch der Account-Erstellungsprozess optimiert wird. • Behebung von Bereitstellungsproblemen: Diagnostiziert und löst Probleme, die während der Cloud-Account-Bereitstellung auftreten, wodurch die erfolgreiche Account-Erstellung gefördert wird. • Passt die Datenzertifizierungsrichtlinie an: Passt die an Cloud Account Management Standardmäßige Datenzertifizierungsrichtlinie, um bestimmte organisatorische Anforderungen zu erfüllen und entsprechende Datenverarbeitungsverfahren zu fördern. • Verwaltet alle Accounts: Überwacht alle Cloud-Accounts, einschließlich CW-verwalteter Accounts und Onboarding-Accounts, wodurch eine zentrale Kontrolle und Transparenz gewährleistet wird.
ITOM Cloud Account Management Zertifizierungsgruppe	sn_itom_Cam.cw_Certifier	• Zertifiziert erkannte Accounts: Überprüft erkannte Accounts, die auf der Registerkarte Abonnementkonten aufgeführt sind, und bezeichnet sie als zertifiziert, wenn sie Compliance-Standards erfüllen oder fehlgeschlagen sind, wenn sie nicht Dieser Prozess verifiziert die ordnungsgemäße Überprüfung und laufende Überwachung von Cloud-Accounts. • Verwaltet Verifizierungsaufgaben: Greift auf Verifizierungsaufgaben zu, die Cloud-Accounts zugeordnet sind, und überprüft sie. Nach der Überprüfung kann der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Gruppen und Verantwortlichkeiten (Fortsetzung)

Gruppe	Rolle	Verantwortlichkeiten
		Administrator Aufgaben zertifizieren, um ihren erfolgreichen Abschluss anzuzeigen.

Wie sie zusammenarbeiten

Cloud Account Management Gruppen und Verantwortlichkeiten

Gruppe	Rolle	Verantwortlichkeiten
ITOM Cloud Account Management Gruppe der anfordernden Person	sn_itom_Cam.cw_anfordernde Person	• Initiiert Cloud-Account-Anforderungen: Löst den Prozess zum Erstellen von Cloud-Accounts aus und stellt die Informationen zum Erstellen des Accounts bereit. • Verwaltet den Account-Status: Fordert die Aussetzung oder erneute Aktivierung von Cloud-Accounts an.
ITOM Cloud Account Management Genehmigergruppe	sn_itom_Cam.cw_Approver	• Wertet Account-Anforderungen aus und genehmigt sie. • Überprüft die Budget-Compliance der angeforderten Cloud-Accounts und die Ausrichtung mit verfügbaren Budgetressourcen.
ITOM Cloud Account Management Zertifizierungsgruppe	sn_itom_Cam.cw_Certifier	• Zertifiziert erkannte Accounts. • Greift auf und überprüft Verifizierungsaufgaben zu, die Cloud-Accounts zugeordnet sind.
ITOM Cloud Account Management Administratorgruppe	sn_itom_Cam.cw_admin	• Verifiziert das Cloud Account Management Konfigurationen sind konsistent und an Cloud-Provider-Konfigurationen und ausgerichtet Terraform Konfigurationen. • Stellt Cloud-Accounts bereit. • Behebung von Bereitstellungsproblemen: Diagnostiziert und löst alle Probleme, die während der Cloud-Account-Bereitstellung auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Account Management Gruppen und Verantwortlichkeiten (Fortsetzung)

Gruppe	Rolle	Verantwortlichkeiten
		• Passt Datenzertifizierungsrichtlinien an bestimmte organisatorische Anforderungen an. • Überwacht alle Cloud-Accounts, einschließlich CW-verwalteter und integrierter Accounts, und gewährleistet eine zentrale Kontrolle und Transparenz.

Informationen zur Rückkehr zum Hauptthema finden Sie unter Cloud Account Management erkunden.

Berechtigungen erforderlich für Azure Service-Prinzipal

Diese Tabelle bietet die Berechtigungen, die zum Erstellen, Schließen oder Abbrechen von erforderlich sind Azure Abonnement, Abrechnungsdetails herunterladen und Abonnements kennzeichnen.

Für erforderliche Rollen Azure Service-Prinzipal

Rolle	Aktion	Rollendefinitions-ID
RegistrierungReader	Registrierungsleser können Daten in den Bereichen Registrierung, Abteilung und Account anzeigen. Diese Daten enthalten Gebühren für alle Abonnements in diesen Bereichen, auch für Mandanten hinweg, und zeigen den Saldo von AzurePrepayment (zuvor als monetäre Zusage bezeichnet) an, der der Registrierung zugeordnet ist.	24f8edb6-1668-4659-b5e2-40bb5f3a7d7e
DepartmentReader	Laden Sie die Nutzungsdetails für die von Ihnen verwaltete Abteilung herunter. Sie können auch die Nutzung und die Gebühren anzeigen, die Ihrer Abteilung zugeordnet sind.	Db609904-a47f-4794-9be8-9bd86fbffd8a
Microsoft.Abrechnung/Abrechnungskonten/Lesen	Lesen Sie die Liste der Abrechnungskonten.	
Microsoft.Management/ManagementGroups/Subscriptions/write Microsoft.Management/ManagementGroups/write	Verschieben Sie das Abonnement nach der Erstellung an den entsprechenden Standort	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für erforderliche Rollen Azure Service-Prinzipal (Fortsetzung)

Rolle	Aktion	Rollendefinitions-ID
Microsoft.resources/Tags/write	Fügen Sie dem Abonnement Tags hinzu.	
Microsoft.Billing/BillingAccounts/BillingSubscriptions/Cancel/write	Schließen oder stornieren Sie ein Abonnement.	

Verwalten der Asset-Details des Cloud-Arbeitsbereichs

Auf dieser Seite kann der Anwender einen umfassenden Satz von Details eines Cloud-Assets anzeigen, bearbeiten und verwalten, z. B. seine Attribute, seine Integrität und seine Datensätze.

Die Cloud-Asset-Seite ist ein zentralisierter, hoch organisierter und umfassender Satz von Abschnitten mit Cloud-Asset-Details. Diese Seite wird verwendet, um Cloud-Asset-Attribute, -Beziehungen, -Tags, -Services und -Angebote, die Kontointegrität und Daten zu untersuchen und zu bearbeiten, die dem Cloud-Asset, Ressourcen, Aktivitäten und zugehörigen Services zugeordnet sind.

In den folgenden Abschnitten werden die verschiedenen Abschnitte der Cloud-Asset-Seite beschrieben.

Zusammenfassung

Der Abschnitt „Zusammenfassung“ bietet eine konsolidierte Ansicht wichtiger Informationen für das ausgewählte Konfigurationselement (CI). Diese Seite hilft Ihnen, schnell auf Metadaten, Besitzerdetails, Betriebsstatus, Discovery-Zeitstempel und kritische Attribute zuzugreifen, die für die Überwachung und Entscheidungsfindung erforderlich sind.

Attribute

Im Abschnitt Attribute werden alle UI-Abschnitte angezeigt, die in der CI-Ansicht „Erkunden“ für die CI-Klasse konfiguriert sind. Wählen Sie Attribute aus, um auf die verfügbaren Unterabschnitte zuzugreifen. Standardmäßig sind die Unterabschnitte „Discovery“ und „operativ“ an den entsprechenden Abschnitten in der Ansicht „CI erkunden“ ausgerichtet. Im Unterabschnitt alle werden alle CI-Attribute aufgelistet. Obligatorische Attribute sind mit einem Sternchen (*) markiert und müssen einen Wert haben.

Tags

In diesem Abschnitt werden Tags aufgelistet, die als Schlüssel-Wert-Paare in der Tabelle „Schlüsselwerte“ [cmdb_key_value] gespeichert sind. Diese Cloud-Tags werden normalerweise CIs und Ressourcen von Anbietern wie AWS und Google Cloud Platform zugeordnet. Cloud-Tags werden in ITOM-Anwendungen wie Tag Governance verwendet und sind der Schlüssel für die Tag-basierte Discovery in Service-Mapping. Sie werden automatisch von Discovery und Service Graph Connectors ausgefüllt und können nach Bedarf innerhalb Ihrer Organisation gruppiert und verwaltet werden.

Ressourcen

In diesem Abschnitt „Ressourcen“ werden die mit dem CI verknüpften Ressourcen angezeigt und entsprechen den zugehörigen Listen, die in der Ansicht „CI erkunden“ definiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivität

In diesem Abschnitt werden zugehörige Elemente wie offene Incidents und der Aktivitätenstrom für das CI auf den folgenden Registerkarten angezeigt:

Zugehörige Elemente

Kreisdiagramme, die standardmäßig offene Incidents (Incidents-Tabelle), offene Changes (Change-Anforderungstabelle) und offene Probleme (Problemtabelle) enthalten, aufgeschlüsselt nach Priorität oder Status.

CI-Verlauf

Verlauf der Aktivitäten im Zusammenhang mit dem CI, z. B. Wertänderungen in den CI-Attributen, die in chronologischer Reihenfolge aufgeführt sind.

Beziehungen

In diesem Abschnitt werden die CI-Beziehungen angezeigt, zu denen Folgendes gehört:

- Beziehungen insgesamt: Gesamtzahl der Beziehungen für dieses CI
- Doppelte Beziehungen: Gesamtzahl der doppelten Beziehungen für dieses CI
- Veraltete Beziehungen: Gesamtanzahl der veralteten Beziehungen für dieses CI

Services und Angebote

In diesem Abschnitt werden Karten mit der Anzahl der folgenden Services und Angebote angezeigt, die dem CI zugeordnet sind:

- Serviceinstanz: Beliebiges CI, das sich auf die Tabelle „Serviceinstanz“ [cmdb_ci_Service_Auto] bezieht, in der die Serviceklassifizierung „Anwendungsservice“ ist.
- Business-Service-Angebot: Jede Serviceinstanz, die eine Beziehung zu Service_offering hat, wobei die Serviceklassifizierung Business-Service ist.
- Technologiemanagement-Angebot: Jede Serviceinstanz, die eine Beziehung zu Service_offering hat, wobei die Serviceklassifizierung technischer Service ist oder das CI einer dynamischen CI-Gruppe zugeordnet ist, die Teil eines technischen Serviceangebots ist.
- Technologiemanagement-Service: Übergeordnetes Element eines Technologiemanagement-Angebots.

Gesundheitswesen

In diesem Abschnitt werden Zusammenfassungen aus den neuesten CMDB-Integritätstestergebnissen für die KPIs Vollständigkeit, Richtigkeit, Compliance und Beziehung sowie den aggregierten Status des Nachweises angezeigt. Farbcodes werden verwendet, um die Punktzahlen für Bestanden/Fehlgeschlagen anzugeben.

Hinweis: Weitere Informationen zu den einzelnen Abschnitten finden Sie unter Verwalten Sie CI-Details im CI-Formular .

Tabelle „Cloud-Asset-Sammlung“

Speichert Metadaten von Cloud-Assets, die von Anbietern für IT-Vorgänge erfasst wurden.

Eine Cloud-Asset-Sammlungstabelle ist ein strukturiertes Repository in IT Operations Management, das Metadaten von Cloud-Ressourcen speichert und verwaltet, die von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mehreren Cloud-Service Providern erfasst wurden. In der Tabelle werden alle erkannten oder synchronisierten Cloud-Assets wie virtuelle Computer, Speicher-Buckets und Datenbanken nach der Erfassung aus Cloud-Umgebungen gespeichert.

Konfigurationsfelder der Cloud-Asset-Sammlung

Feld	Beschreibung
Aktiv	Gibt an, ob diese spezifische Konfiguration der Cloud-Asset-Sammlung aktiviert oder deaktiviert ist. • Wahr: Die Konfiguration ist für das ausgewählte CI aktiv. Sie wurde verarbeitet und in der flachen Tabelle ausgefüllt, und Assets werden gemäß dem definierten Zeitplan erfasst. • Falsch: Die Konfiguration ist inaktiv, und es werden keine Assets erfasst.
Kategorie	Allgemeine Klassifizierung der gesammelten Cloud-Assets, z. B. Compute, Storage, Networking, Datenbank, oder Sicherheit.
Unterkategorie	Granulare Klassifizierung unter der Hauptkategorie. Beispiele sind virtuelle Computer, Container und Funktionen unter „Compute“; Blockspeicher, Objektspeicher und Dateispeicher unter „Speicher“.
CI-Klassenname	CMDB-Klasse, in der gesammelte Assets gespeichert werden, z. B. `cmdb_ci_vm_instance` Für virtuelle Computer.
Anbieter	Cloud-Service Provider, von dem Assets erfasst werden.
Letzte Verarbeitungszeit	Zeitstempel der letzten erfolgreichen Asset-Sammlungsausführung. Nützlich für: • Nachverfolgung der Aktualität von Daten • Fehlerbehebung bei Verzögerungen oder Fehlern
Kommentare	Freitextfeld für Notizen oder Kontext zur Konfiguration.

Cloud-Services-Katalog

Mit ServiceNow® Cloud-Services-Katalog Anwendung können Sie eine vereinfachte Schnittstelle verwenden, um auf Cloud-Ressourcen zuzugreifen. Sie können Cloud-Angebote in einem Katalog veröffentlichen und die Nutzung und den Lebenszyklus dieser Ressourcen verwalten.

Integriert in Cloud-Anbieter, einschließlich Amazon Web Services, Microsoft Azure, Und Google Cloud Platform, Cloud-Services-Katalog(CSK) Ermöglicht Ihnen die Verwendung von Azure DevOps- und CI-CD-Pipeline-Integration . Sie können Integrieren Sie Ansible Mit Cloud-Services-Katalog Als Tag 1-Aktivität zur Bereitstellung einer Ansible-Auftragsvorlage über ein ServiceNow-Katalogelement. Verwenden Die Multi-Repository-Unterstützung mit Terraform Connector IAC-Erkennungsfähigkeiten, um die hierarchische Struktur mehrerer Repositorys zu verbessern.

Hinweis: Cloud-Services-Katalog Unterstützt eine selbst gehostete Umgebung. Stellen Sie sicher, dass MID-Server Hat Internetzugang. Weitere Informationen finden Sie unter Bereitstellungsleitfaden für die selbst gehostete Umgebung [KB0563731] artikel in der Now Support Knowledge Base.

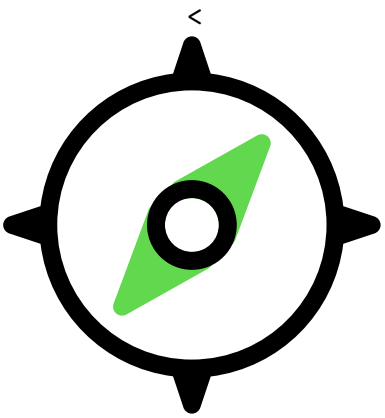
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS, Azure und Google Cloud Platform – sofort einsatzbereite Kataloge Sind mit diesem Release von verfügbar Cloud-Services-Katalog. Sie können entweder eines der Katalogelemente bestellen, wie in diesem Video gezeigt, oder eines erstellen.

Bestellen Sie ein Katalogelement.

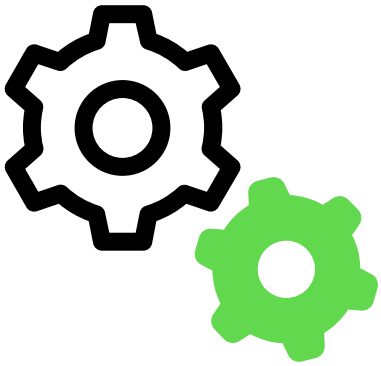
Erste Schritte

Erkunden



Erkunden Sie, und erfahren Sie, wie Cloud-Services-Katalog Die Anwendung bietet den zentralen Ort, an dem Sie Cloud-Management-Tools automatisieren können.

Konfigurieren

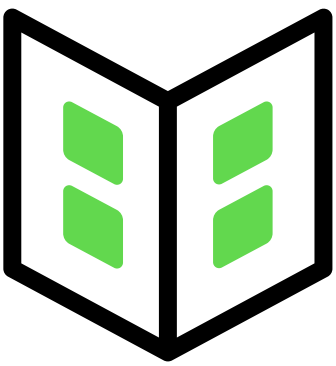


Konfigurieren Sie Ihren Cloud-Services-Katalog Und integrieren Sie sie in andere Anwendungen.

Verwenden Sie Den Cloud-Servicekatalog

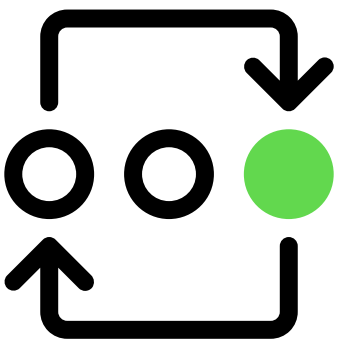
Verwenden Sie Cloud-Services-Katalog Anwendung zum Suchen und anfordern von Cloud-Services, zum Arbeiten mit Ihren Stapeln und Ressourcen usw.

Meine Stapel Erkunden



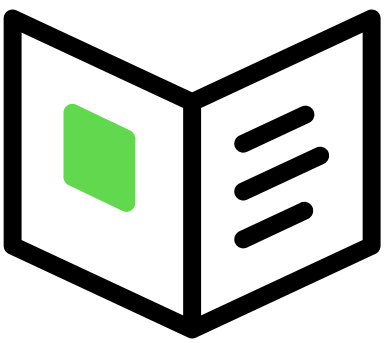
Meine Ressourcen Erkunden

Bestellen Sie einen Katalog



Verwenden Sie Cloud-Services-Katalog Anwendung zum Bestellen aus einer Vielzahl von sofort einsatzbereiten

Referenz



Rufen Sie weitere Details zu den Berechtigungen und Problemumgehungen ab.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelementen, Aktionen und Richtlinien.

Cloud-Services-Katalog erkunden

Die Cloud-Services-Katalog Die Anwendung ist der zentrale Ort, an den Sie zur Automatisierung von Cloud-Management-Tools wechseln müssen. Es ersetzt und verbessert die Fähigkeiten, die von angeboten wurden Cloud Provisioning and Governance Anwender- und Administratorportale.

Cloud-Services-Katalog – Übersicht

Die Cloud-Services-Katalog Seite anfordern auf Mitarbeiter-Center Ermöglicht Ihnen das anfordern von Cloud-Management-Aktionen. Sie können beispielsweise die Bereitstellung (Tag 1), Patch- und Wartungsaktionen (Tag 2) oder Lebenszyklusvorgänge wie Starten, Stoppen oder Aufheben der Bereitstellung anfordern.

Cloud-Services-Katalog – Vorteile

Die folgende Tabelle listet die Vorteile von auf Cloud-Services-Katalog.

Vorteile der Verwendung Cloud-Services-Katalog

Leistung	Funktion
Unterstützung für Anwender	Geführtes Setup
Sofort einsatzbereiter Inhalt für Amazon AWS Cloud Anforderung und Automatisierung	AWS – sofort einsatzbereite Kataloge
Sofort einsatzbereiter Inhalt für Microsoft Azure Microsoft Azure Cloud-Services-Anforderung und -Automatisierung	Sofort Einsatzbereite Azure-Kataloge
Sofort einsatzbereiter Inhalt für Google Cloud Platform Anforderung	Sofort einsatzbereite Kataloge mit Cloud-Services-Katalog
Anforderungen für Prozess und Seiten für die Bestellung von Cloud-Services	Cloud-Services-Anforderungsprozess
Seite „Verwaltung meiner Stapel“ zum Anzeigen und Arbeiten an Stapeln	Stapelverwaltung
Seite „meine Ressourcenverwaltung“ zum Anzeigen und Bearbeiten von Ressourcen	Ressourcenverwaltung
Azure DevOps Pipeline-Integration für kontinuierliche Bereitstellung (Continuous Integration Continuous Deployment, CICD)	Azure DevOps- und CI-CD-Pipeline-Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteile der Verwendung Cloud-Services-Katalog (Fortsetzung)

Leistung	Funktion
Integration von Ansible Mit Cloud-Services	Integrieren Sie Ansible
Microsoft Azure Und Amazon AWS Cloud Setup	Cloud-Setup
Multi-Repository-Unterstützung mit Terraform Connector App	Cloud Provisioning and Governance: Terraform Connector erkunden

Nächste Schritte

Siehe Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate Um die Liste der Plugins zu finden, die Sie mit aktivieren Cloud-Services-Katalog.

Cloud-Services-Katalog konfigurieren

Sie können konfigurieren Cloud-Services-Katalog Anwendung, damit Sie mit der Automatisierung der Cloud-Management-Tools beginnen können.

Konfiguration – Übersicht

Die Konfiguration erfolgt in einer sequenziellen Reihenfolge, in der Sie zuerst die Voraussetzungen erstellen und einrichten und dann die Anmeldeinformationen in Ihr Cloud-Account-Profil integrieren. Diese Setup-Schritte werden als Aufgaben „Tag 1“ und „Tag 2“ identifiziert.

Die Cloud-Services-Katalog Die Konfiguration von Tag 1 umfasst Aufgaben wie das Erstellen MID Servers, Einrichten Ihrer Cloud-Provider, Amazon Web Services, Oder Microsoft Azure Cloud. Sie können es auch Ihrem Cloud-Account zuordnen und das Rechenzentrum planen Discovery .

Eine Übersicht über den Setup-Prozess für Tag 1 finden Sie hier:

1. Fordern Sie an Cloud-Services-Katalog Anwendung, falls erforderlich.
2. Weisen Sie Ihren Cloud-Anwendern die entsprechenden Rollen zu.
3. Richten Sie ein MID Servers Die die sichere Kommunikation mit den Provider-API-Endpunkten verarbeiten.
4. Erfassen Sie im Anbieterportal Ihre Accounteinstellungen und die Anmeldeinformationen, die für angegeben sind Discovery Prozessverwendungen (über einen MID-Server), um auf Ihre Provider-Accounts zuzugreifen.
5. Ordnen Sie die Accounteinstellungen und -Anmeldeinformationen sicher einem Service-Account in zu Cloud-Services-Katalog.
6. Richten Sie einen Cloud-Account ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie einen Service-Account ein, der mit einem Ihrer Provider-Accounts kompatibel ist.
7. Geben Sie die Rechenzentren im Service-Account an, die in den Cloud-Account aufgenommen werden sollen.

An Tag 2 können Sie die zusätzlichen Cloud-Accounts und Service-Accounts desselben oder anderer Anbieter einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Verwenden Sie Configuration Management Database (CMDB) Daten, mit denen Sie Cloud-Ressourcen anfordern und verwalten und Ihre Cloud-Infrastruktur verwalten können.
2. Führen Sie manuell aus Discovery Verarbeiten Sie in jedem Rechenzentrum im Service-Account, um auszufüllen CMDB Mit den Ressourcendaten für alle Rechenzentren.
3. Konfigurieren Discovery Wird in einem regelmäßigen Zeitplan ausgeführt, um sicherzustellen, dass die Daten aktualisiert bleiben.

Verwenden Geführtes Setup Zu implementieren Cloud-Services-Katalog

Geführtes Setup Stellt eine Sequenz von Aufgaben bereit, die Ihnen bei der Konfiguration helfen CSK Auf Ihrem ServiceNow Instanz. Zum Öffnen Geführtes Setup Für Cloud-Services-Katalog, Navigieren Sie zu **Alle** > **Cloud-Servicekatalog: Geführtes Setup** In Ihrer Instanz.

Weitere Informationen finden Sie unter Geführtes Setup .

Cloud-Services-Katalog installieren

Sie können installieren Cloud-Services-Katalog Anwendung, die über erworben wurde ServiceNow® Store, Um es in Ihrer Instanz verfügbar zu machen.Die Anwendung enthält auch Demodaten und Installationen im Zusammenhang mit ServiceNow Anwendungen und Plugins, wenn Sie sie nicht bereits installiert haben.

Vorbereitungen

- Cloud-Services-Katalog Anwendung aus dem ServiceNow® Store.
- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow® Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Siehe Ruft die Berechtigung für ein ServiceNow-Produkt oder eine ServiceNow-Anwendung ab .

Erforderliche Rolle: admin, sn_appclient.App_Client_Company_Installer (kann nur Anwendungen installieren, die dem Instanzunternehmen entsprechen) oder sn_appclient.App_Client_user

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Cloud-Services-Katalog installiert:

- Plugins
- Sofort Einsatzbereiter Katalog
- Rollen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:

Wenn Sie ein vorhandener Anwender von sind Cloud-Services-Katalog Oder CSK Innovationslabore:

- Ein Upgrade von der vorherigen Version wird derzeit nicht unterstützt. Um ein Upgrade einer vorhandenen Instanz mit durchzuführen Cloud-Services-Katalog Oder CSK Apps: Führen Sie die folgenden Aktionen aus:

- ○ Deinstallieren Sie die zuvor installierte CSK Apps mit Tabellenbereinigungen (CSK Inhaltspaket und CSK In Ordnung).
  - ○ Installieren Sie neu CSK Apps (CSK Und CSK Inhaltspaket in derselben Reihenfolge).
  - ○ Da Sie das geführte Setup nur einmal in einer Instanz ausführen können, platzieren Sie neue Terraform-Vorlagen manuell in das Feld Terraform, aktualisieren Sie den sofort einsatzbereiten Terraform-Konfigurationsanbieter entsprechend, und führen Sie die Ausführung aus Discovery .

Weitere Informationen finden Sie unter den Komponentenlinks.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendung** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach der Anwendung anhand ihres Namens oder ihrer ID.
   Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über anfordern ServiceNow® Store. CSK Ist als separates Abonnement verfügbar und erfordert Cloud Provisioning and Governance Plugin (com.snc.Cloud.mgmt).
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.
   Im angezeigten Dialogfeld Installieren werden alle mit Ihrer Anwendung installierten Abhängigkeiten aufgelistet.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow® Store Um zusätzliche Berechtigungen für Abhängigkeiten abzurufen.
5. Wählen Sie **Installieren** aus.

Cloud-Services-Katalog Setup für die Tag-1-Konfigurationsaufgabe

Sie sind bereit, die Tag-1-Konfigurationsaufgabe zum Einrichten von auszuführen Cloud-Services-Katalog Anwendung zum ersten Mal. Sie können das optionale Setup für Tag 2 durchführen und Verfahren nach Bedarf in beliebiger Reihenfolge konfigurieren.

Sie müssen tun Cloud-Services-Katalog Setup-Schritte in der Reihenfolge. An Tag 1 richten Sie den Cloud-Service für Zugriffs-, Sicherheits- und Abrechnungszwecke für ein Amazon Web Services Und Microsoft Azure Cloud.

Bevor Sie diese Aufgaben ausführen können, müssen Sie integrieren Cloud-Services-Katalog Mit Amazon Web Services Oder Microsoft Azure Cloud- und Fortschritt bis Tag 2-Konfigurationsaufgaben.

Wenn Sie alle Aufgaben „Tag 1“ und „Tag 2“ abgeschlossen haben, finden Sie unter Administrationsleitfaden für Cloud-Services-Katalog Weitere Informationen zur Verwendung von Cloud-Services-Katalog Anwendung in Ihrer Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einrichten Amazon Web Services Ein Cloud-Services-Katalog

Integrieren Cloud-Services-Katalog Mit Amazon Web Services Account als Teil der Tag-1-Konfigurationsaufgabe zum ersten Mal einrichten der Anwendung.

Vorbereitungen

Erfassen Sie Ihre Accounteinstellungen und -Anmeldeinformationen aus dem Anbieterportal. Diese Einstellungen und Anmeldeinformationen helfen Ihnen, die Ressourcen in einem Account von einem anderen Account zu unterscheiden und sich bei anzumelden oder zu authentifizieren AWS. Berechtigungsrichtlinien geben Ihre Genehmigungen innerhalb der Ressourcen im Account an.

Erforderliche Rolle:

- Administrator für Vorgang in AWS Oder AWS Verwaltungskonsole
- Rolle „sn_CMP.Cloud_admin“ für Vorgänge in Cloud-Services-Katalog

Prozedur

1. Weisen Sie Rollen zu zu zu AWS Anwender von Cloud-Services-Katalog Und einzelnen Anwendern nach ihren Aktivitäten und Verantwortlichkeiten.
   Weitere Informationen finden Sie unter Weisen Sie AWS-Anwendern von Rollen zu Cloud-Services-Katalogan.
2. Installieren und konfigurieren MID Servers Für Cloud-Discovery Und Cloud Provisioning and Governance.

   Um eine sichere und zuverlässige Kommunikation zu gewährleisten Discovery Process kommuniziert mit Ihren Cloud-Provider-Accounts und Cloud-Ressourcen über einen oder mehrere MID Servers. Weitere Informationen finden Sie unter Installieren und konfigurieren MID Servers Für Cloud-Discovery und Cloud-Bereitstellung und -Governancean.
3. Richten Sie ein MID-Server In Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke und konfigurieren Sie es für Cloud-Services-Katalog Dient zur Verwendung eines Proxy-Servers.
   Die Verwendung eines Proxy-Servers unterstützt alle cloudbasierten Aktivitäten, z. B. die Ausführung Discovery, Abrechnungsdownloads, Bereitstellung virtueller Computer und Ausführung von Lebenszyklusvorgängen auf virtuellen Computern.
4. Konfigurieren Sie mindestens einen MID Servers Für jedes Rechenzentrum für hohe Leistung und Sicherheit. Daten werden mit verschlüsselt MID-Server Und zwischen MID-Server Und der API-Endpunkt.
5. Konfigurieren Sie MID-Server Auch wenn Sie bereits andere konfiguriert haben MID Servers Während der Einrichtung Cloud-Services-Katalog Für einen anderen Cloud-Anbieter.
6. Konfigurieren Sie den Zugriff auf AWS Accounts mit permanenter Verwendung AWS Anmeldeinformationen.

   - Um sicher auf Daten in Ihrem Provider-Account zuzugreifen, die Discovery Der Prozess muss die entsprechenden Anmeldeinformationen aufweisen.
   - Um die Anmeldeinformationen für verfügbar zu machen Discovery Und Cloud-Services-Katalog, Erstellen Sie zuerst einen Anwender mit programmgesteuertem Zugriff auf AWS Verwaltungskonsole.
   - Sie können die Anmeldeinformationen sicher in einem Service-Account auf der speichern ServiceNow AI Platform®.
   - Weitere Informationen finden Sie unter Konfigurieren Sie den Zugriff auf die AWS-Accounts mit permanenten AWS-Anmeldeinformationen .
7. Richten Sie einen Cloud-Account und einen Service-Account für ein AWS.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Service-Account ist ein sicherer Datensatz in Ihrer Instanz, der die Anmeldeinformationen und Zugriffsinformationen für Ihren Provider-Account speichert. Discovery Verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen, um die Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud-Services-Katalog. Ein Cloud-Account kann mehrere Service-Accounts enthalten, einschließlich der Service-Accounts verschiedener Anbieter.
Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen. Weitere Informationen finden Sie unter Richten Sie einen Cloud-Account und einen Service-Account für AWS ein .

Google Cloud Platform im Cloud-Servicekatalog einrichten

Integrieren Cloud-Services-Katalog Mit Google Cloud Platform Account als Teil der Tag-1-Konfigurationsaufgabe für die Einrichtung CSK Zum ersten Mal.

Vorbereitungen

Erfassen Sie Ihre Accounteinstellungen und -Anmeldeinformationen aus dem Anbieterportal. Diese Einstellungen und Anmeldeinformationen helfen Ihnen, die Ressourcen in einem Account von einem anderen Account zu unterscheiden und sich bei Google Cloud anzumelden oder zu authentifizieren. Berechtigungsrichtlinien geben Ihre Genehmigungen innerhalb der Ressourcen im Account an.

Erforderliche Rolle:

- Administrator für den Betrieb in Google Cloud oder Google Cloud Management Console
- Rolle „sn_CMP.Cloud_admin“ für Vorgänge in CSK

Um mehr über die Einrichtung zu erfahren Google Cloud Mit CSK Terraform Connector App zum ersten Mal finden Sie unter Setup-Leitfaden für Tag 1 für Google Cloud Bis Cloud-Services-Katalog Terraform Connector.

Prozedur

1. Weisen Sie Google Cloud-Anwendern von Rollen zu CSK Und einzelnen Anwendern nach ihren Aktivitäten und Verantwortlichkeiten.

   Weitere Informationen finden Sie unter Rollen an Google Cloud Platform-Benutzer zuweisen.

2. Installieren und konfigurieren Sie MID-Server für Cloud-Discovery und Cloud Provisioning and Governance. Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Server statt. Weitere Informationen finden Sie unter Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.

3. Richten Sie den MID-Server in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke ein, und konfigurieren Sie ihn für CSK Dient zur Verwendung eines Proxy-Servers.
   Die Verwendung eines Proxy-Servers unterstützt alle cloudbasierten Aktivitäten, z. B. die Ausführung von Discovery, die Abrechnung von Downloads, die Bereitstellung virtueller Computer und die Ausführung von Lebenszyklusvorgängen auf virtuellen Computern.

4. Konfigurieren Sie einen oder mehrere MID-Server für jedes Rechenzentrum für hohe Leistung und Sicherheit.
   Daten werden auf dem MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt.

5. Konfigurieren Sie den MID-Server, auch wenn Sie bereits andere MID-Server konfiguriert haben, während Sie die Einrichtung vorgenommen haben Cloud-Services-Katalog Für einen anderen Cloud-Anbieter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Erstellen Sie einen Service-Account und die Schlüssel (Anmeldeinformationen) in Google Cloud, wenn Sie ihn nicht haben.
   Sie können die Anmeldeinformationen sicher in einem Service-Account speichern. Sie benötigen die IAM-Rolle „Service-Account-Schlüsseladministrator“ (Rollen/iam.serviceAccountKeyAdmin) für das Projekt oder den Service-Account, dessen Schlüssel Sie verwalten möchten. Diese Berechtigungen können vom Administrator bereitgestellt werden. Um sicher auf Daten in Ihrem Provider-Account zuzugreifen, muss der Discovery-Prozess die entsprechenden Anmeldeinformationen enthalten.

   Weitere Informationen finden Sie unter Richten Sie Google Cloud Platform-Service-Accounts ein.

7. Richten Sie einen Cloud-Account und einen Service-Account für ein Google Cloud Platform.

   - Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert werden. Discovery verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen, um die Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.
   - Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud-Services-Katalog. Ein Cloud-Account kann mehrere Service-Accounts enthalten, einschließlich der Service-Accounts verschiedener Anbieter. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

   Weitere Informationen finden Sie unter Richten Sie ein Cloud-KontoUnd ServicekontoFür Google Cloud Platform.

Einrichten Microsoft Azure Cloud auf Cloud-Services-Katalog

Integrieren Cloud-Services-Katalog Mit Microsoft Azure Account als Teil der Tag-1-Konfigurationsaufgabe für die Einrichtung CSK Zum ersten Mal.

Vorbereitungen

Erfassen Sie Ihre Accounteinstellungen und -Anmeldeinformationen aus dem Anbieterportal. Diese Einstellungen und Anmeldeinformationen helfen Ihnen, die Ressourcen in einem Account von einem anderen Account zu unterscheiden und sich bei anzumelden oder zu authentifizieren Microsoft Azure. Berechtigungsrichtlinien geben Ihre Genehmigungen innerhalb der Ressourcen im Account an.

Erforderliche Rollen:

- Microsoft Azure Oder Microsoft Azure AD-Administrator (Active Directory)
- Anwendungsadministrator
- Anwendungsentwickler
- Cloud-Anwendungsadministrator und die Rolle „Beitragender der Ressourcenrichtlinie“ zum Erstellen oder Ändern der Ressourcenrichtlinien.
- Rolle „sn_CMP.Cloud_admin“ für Vorgänge in Cloud-Services-Katalog

Prozedur

1. Weisen Sie Rollen zu zu zu AzureAnwender von Cloud Provisioning and Governance.

   Sie weisen zu Cloud Provisioning and Governance Rollen für die Anwendergruppen und einzelnen Anwender basierend auf den Anwenderaktivitäten und -Verantwortlichkeiten. Weitere Informationen finden Sie unter Weisen Sie Azure-Anwendern von Cloud Provisioning and Governance Rollen zu .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Installieren und konfigurieren MID Servers Für Cloud-Discovery Und Cloud Provisioning and Governance.

   Um eine sichere und zuverlässige Kommunikation zu gewährleisten Discovery Process kommuniziert mit Ihren Cloud-Provider-Accounts und Cloud-Ressourcen über einen oder mehrere MID Servers. Weitere Informationen finden Sie unter Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.

3. Richten Sie ein MID Servers In Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke.
   Daten werden mit verschlüsselt MID-Server Und zwischen MID-Server Und der API-Endpunkt.

4. Konfigurieren Sie mindestens einen MID Servers Für jedes verwaltete Rechenzentrum für hohe Leistung und Sicherheit.
   Konfigurieren Sie MID-Server Auch wenn Sie bereits andere konfiguriert haben MID Servers Beim Einrichten Cloud-Services-Katalog Für einen anderen Cloud-Anbieter.

5. Erstellen Sie einen Microsoft Azure Service-Prinzipal.

   Um sicher auf die Ressourcen und Abrechnungsdaten in zuzugreifen Microsoft Azure Account, die Discovery Der Prozess muss angemessen sein Microsoft Azure Account-Anmeldeinformationen. Sie erstellen einen speziellen programmgesteuerten Account – ein Microsoft Azure Serviceprinzipal: Zum Generieren der erforderlichen Anmeldeinformationen. Weitere Informationen finden Sie unter Erstellen Sie einen Microsoft Azure-Service-Prinzipal .

6. Speichern Sie AzureService-Prinzipal-Anmeldeinformationen in der Instanz.

   Um sicher auf die Daten in Ihrem Provider-Account zuzugreifen, die Discovery Der Prozess muss die entsprechenden Anmeldeinformationen aufweisen. Um die Anmeldeinformationen für verfügbar zu machen Discovery, Erstellen Sie zuerst Microsoft Azure Service-Prinzipal-Anmeldeinformationen in AzurePortal. Sie können die Anmeldeinformationen dann sicher in einem Service-Account in Ihrer Instanz speichern. Weitere Informationen finden Sie unter Speichern Sie die Anmeldeinformationen des Azure-Serviceprinzips in der Instanz .

7. Fügen Sie einen hinzu AzureService-Account. Fügen Sie einen Azure-Service-Account hinzu

   Ein Service-Account ist ein sicherer Datensatz in Ihrer Instanz, der die Anmeldeinformationen und Zugriffsinformationen für Ihren Provider-Account speichert. Discovery Verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen, um Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Weitere Informationen finden Sie unter Fügen Sie einen Azure-Service-Account hinzu .

8. Erkennen Sie alle Rechenzentren in einem Service-Account.

   Discovery Verwendet die Informationen im Service-Account, um alle logischen Rechenzentren zu identifizieren, die dem Provider-Account zugeordnet sind.

9. Richten Sie einen Cloud-Account für ein Azure.

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud-Services-Katalog. Ein Cloud-Account kann mehrere Service-Accounts enthalten, einschließlich der Service-Accounts verschiedener Anbieter. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen. Weitere Informationen finden Sie unter Richten Sie einen Cloud-Account für Azure ein .

10. Legen Sie die Kapazitätsgrenzen für Anwenderanforderungen für Ressourcen fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kapazitätsgrenzen setzen Einschränkungen für die Attribute der Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder Aggregatspeicher ein. Sie können die Grenzwerte für die Ressourcen für jedes logische Rechenzentrum in einem Cloud-Account separat festlegen.

Integration Azure DevOps Und die Pipeline kontinuierliche Integration – kontinuierliche Bereitstellung

Sie können die Release-Anforderung über verarbeiten Cloud-Services-Katalog Workflow mit Azure DevOps Für die End-to-End-Automatisierung des Entwicklungsprozesses, einschließlich Bereitstellung der Ressourcen und Bereitstellung und Überwachung der Anwendungen.

Die Azure DevOps Und die Pipeline-Integration für kontinuierliche Integration – kontinuierliche Bereitstellung (CI-CD-Tool) ist ein Release-Bereitstellungsprozess. Sie können verwenden Cloud-Services-Katalog Und das CI-CD-Tool zum Verwalten der bereitgestellten Ressourcen in Configuration Management Database (CMDB), Direkt über Flows und Aktionen.

Vorteile von Azure DevOps Pipelines mit Cloud-Services-Katalog

Mithilfe von Azure DevOps Pipelines mit Cloud-Services-Katalog, Erhält Ihre Organisation die folgenden Vorteile:

- Fähigkeit, mit CI-CD-Pipelines unabhängig von den zugrunde liegenden Sprachen zu arbeiten, die in den Pipelines verwendet werden (JavaScript, Java, Node.js oder Python).
- Unterstützung für alle Hauptversionskontrollsysteme wie GitHub, GitLab, Azure DevOps, Atlassian Bitbucket oder Team Foundation Version Control (TFVC).
- Support für Amazon Web Services Und Microsoft Azure Cloud-Services.
- Fähigkeit, die Anwendung überall (Cloud oder lokal, Container oder virtuelle Computer) oder in einer beliebigen Umgebung bereitzustellen. Weitere Informationen finden Sie unter ADO und Release- und Lebenszyklusmanagement .
- Fähigkeit, Kubernetes, Platform as a Service (PaaS) usw. ohne Entwicklungsänderungsanforderungen bereitzustellen.
- Automatische Updates von CMDBÜber die erforderlichen Tags.
- Genehmigungen und Governance-Schritte, die in den Workflow integriert sind.

Wichtige Schritte bei der Integration von Azure DevOps und CI-CD-Pipeline

1. Verwenden Sie die Release-Pipelines und Azure DevOps Bis Cloud-Services-Katalog.
2. Richten Sie ein Microsoft Azure DevOps Konsole.
3. Ausführen Discovery Ein Azure DevOps Konfigurations-Provider.
4. Bestellen Sie A Microsoft Azure DevOps Katalogelement.

Release-Pipelines und Azure DevOps Bis Cloud-Services-Katalog

Azure DevOps Verfügt über Release-Pipelines, z. B. die CI-CD-Pipelines (Continuous Integration – Continuous Deployment), die einen Build-, Test- und Bereitstellungsansatz bieten. Sie können diese vollständig automatisierten Prozesse verwenden, um Build-Anforderungen schnell in der Produktionsumgebung bereitzustellen.

Cloud-Services-Katalog Bietet an Azure DevOps Release-Pipeline als CI-CD-Tool, mit dem Sie Anwendungen für den gesamten Entwicklungslebenszyklus auf verschiedenen Plattformen und Cloud-Anbietern erstellen, testen und bereitstellen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure DevOps Innerhalb von Cloud-Services-Katalog Bietet zusätzliche Funktionen für die Verwaltung von Arbeitselementen, Versionssteuerung, Projektmanagement und Berichterstellung. Ressourcenanforderungen über Azure DevOps Pipelines werden durch Genehmigung über den Governance- und Konformations-Workflow verarbeitet.

Richten Sie ein Microsoft Azure DevOps Konsole

Richten Sie ein Microsoft Azure DevOps Konsole als erster Schritt vor der Ausführung Discovery Und bestellen Sie ein Katalogelement im Cloud-Services-Katalog Anwendung.

Vorbereitungen

1. Fügen Sie eine bereitstellungs-ID-Variable zu hinzu Microsoft Azure DevOps Pipelines in Ihrer Organisation. Die Microsoft Azure DevOps Die Integration erkennt nur Pipelines mit einer Bereitstellungs-ID-Variable.
2. Kennzeichnen Sie alle bereitgestellten Ressourcen mit einem Deployment-ID-Schlüssel in der Pipeline, damit Sie die Ressourcen nach der Bereitstellung erkennen können.

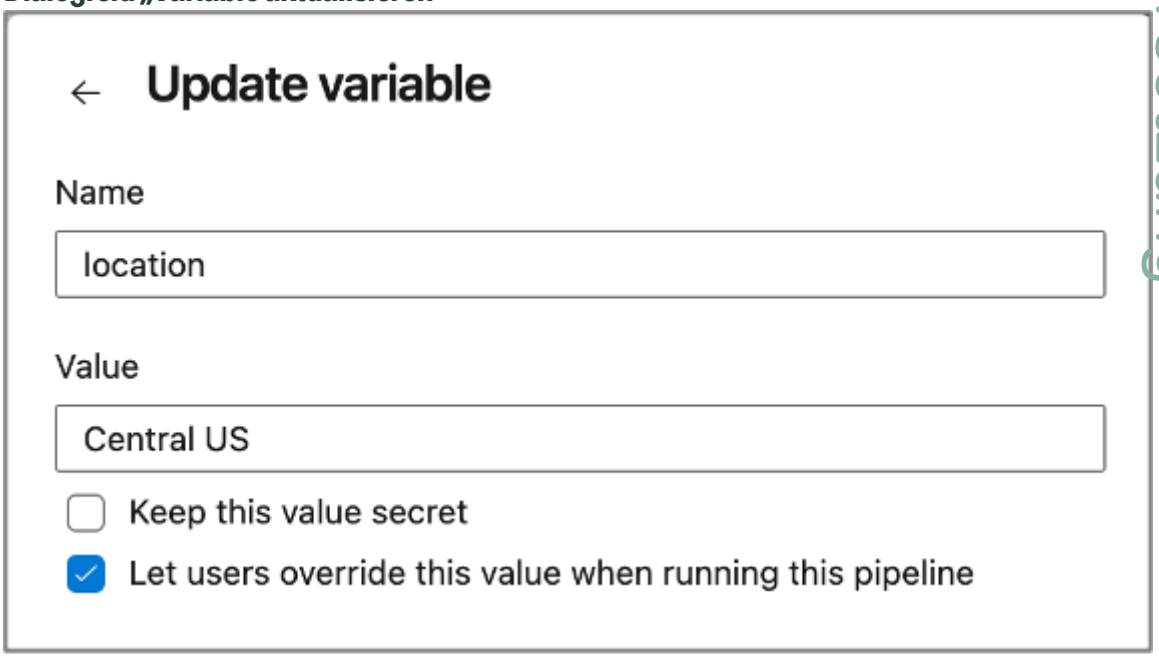
Die SubscriptionID ist für nicht erforderlich Azure DevOps Und Ansible Vorlagen.

Erforderliche Rolle: keine

Prozedur

1. Benennen Sie eine Bereitstellungs-ID der Pipeline-Variable, die Sie für Point verwenden können Discovery Um die Ressourcen in zu aktualisieren CMDB.
2. Erstellen Sie eine PAT-Anmeldeinformation (Personal Access Token), die Sie in verwenden können Azure DevOps Discovery.
3. In **Aktualisieren Sie die Variable** Überschreiben Sie die Pipeline-Variablen, indem Sie auswählen **Zulassen, dass Anwender diesen Wert überschreiben, wenn diese Pipeline ausgeführt wird** Kontrollkästchen.

Dialogfeld „Variable aktualisieren“



Die Pipeline funktioniert mit CSK DevOps-Integrationskatalogelement. Die Microsoft Azure DevOps Die Integration erkennt Pipelines mit der Variable „Bereitstellungs-ID“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführen Discovery Ein Azure DevOps Konfigurations-Provider

Fügen Sie hinzu Azure DevOps Konfigurieren Sie den Provider, und führen Sie ihn aus Discovery Um alle Projekte, Pipelines und Pipeline-Variablen in einer Organisation mithilfe von zu erkennen Cloud-Services-Katalog Anwendung.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

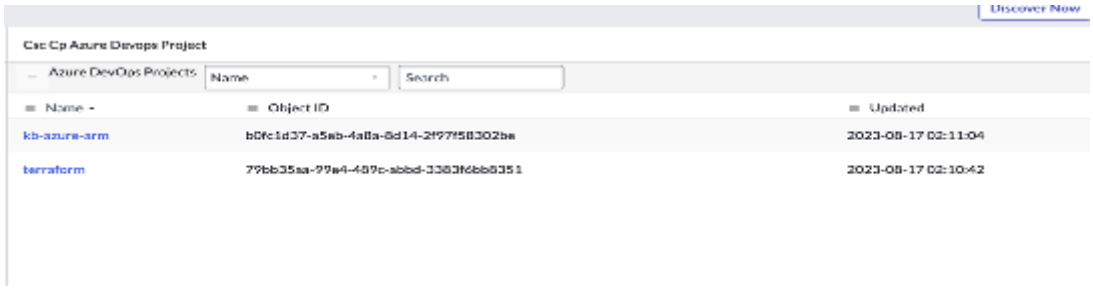
1. Navigieren Sie zu **Administrator** Portal und wählen Sie aus **VerwaltenAnmeldeinformationen** .
2. Fügen Sie hinzu **API-Schlüssel** Anmeldeinformationen, die Sie mit den PAT-Anmeldeinformationen (Personal Access Token) erstellt haben.
3. Setzen Sie den PAT-Anmeldeinformationen (Personal Access Token) gerade Anführungszeichen („:“) voran, und codieren Sie sie im Base64-Format.
4. Stellen Sie der codierten Formatzeichenfolge eine Standardzeichenfolge vor.
   Beispiel: Basic-codierte Basis 64(:PAT).
5. Fügen Sie einen erforderlichen Alias hinzu.
6. Navigieren zu **Verwalten** > **Konfigurationsverwaltung** Und fügen Sie einen Konfigurationsanbieter hinzu.

Wichtig:

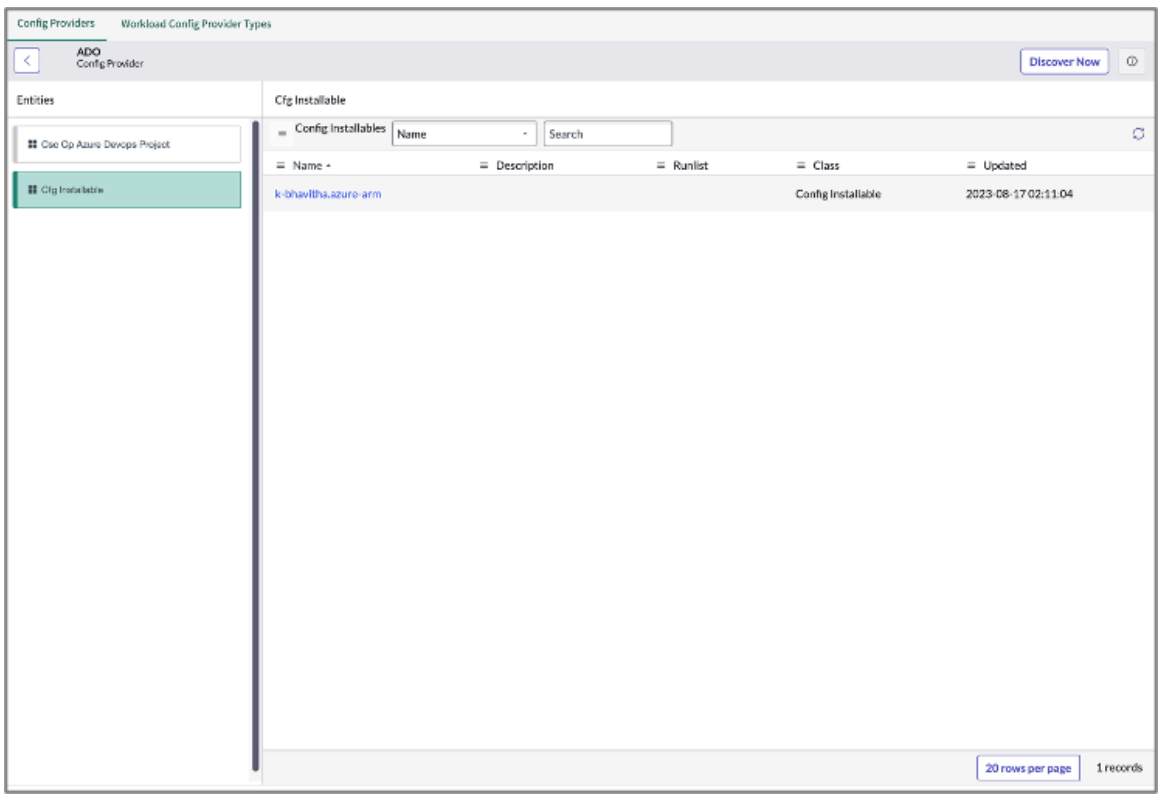
Infrastruktur als Code (IAC) Discovery Wird unterstützt. Sie können erkennen Azure DevOps Pipeline Ansible Auftragsvorlagen durch Einrichten einer geplanten Discovery.

7. Erkennen Sie alle Projekte, Pipelines und Pipeline-Variablen in einer Organisation, indem Sie ausführen Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Suchen Sie die installierbaren Konfigurationsdateien unter dem ausgewählten Azure DevOps Projekt.



Ergebnis

Sie können jetzt bestellen Azure DevOps Katalogelement aus dem Azure DevOps Katalogbestellungsformular auf Mitarbeiter-Center.

Bestellen Sie A Microsoft Azure DevOps Katalogelement

Stellen Sie bereit Microsoft Azure DevOps Kataloge mithilfe von Microsoft Azure DevOps Formular „Katalogbestellung“ in Cloud-Services-Katalog Anwendung.

Vorbereitungen

Zu verwenden Microsoft Azure DevOps Für Cloud-Services-Katalog, Zuweisen Azure DevOps Und Cloud-Management-Fähigkeiten für den MID-Server. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Server-Fähigkeiten .

Legen Sie die Bereitstellungs-ID als Variablen in fest AWS Pipelines, die Sie erkennen möchten. Die SubscriptionID ist für nicht erforderlich Microsoft Azure Pipelines.

Kennzeichnen Sie alle Ressourcen mit dem Schlüssel „Bereitstellungs-ID“.

Erforderliche Rolle: keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

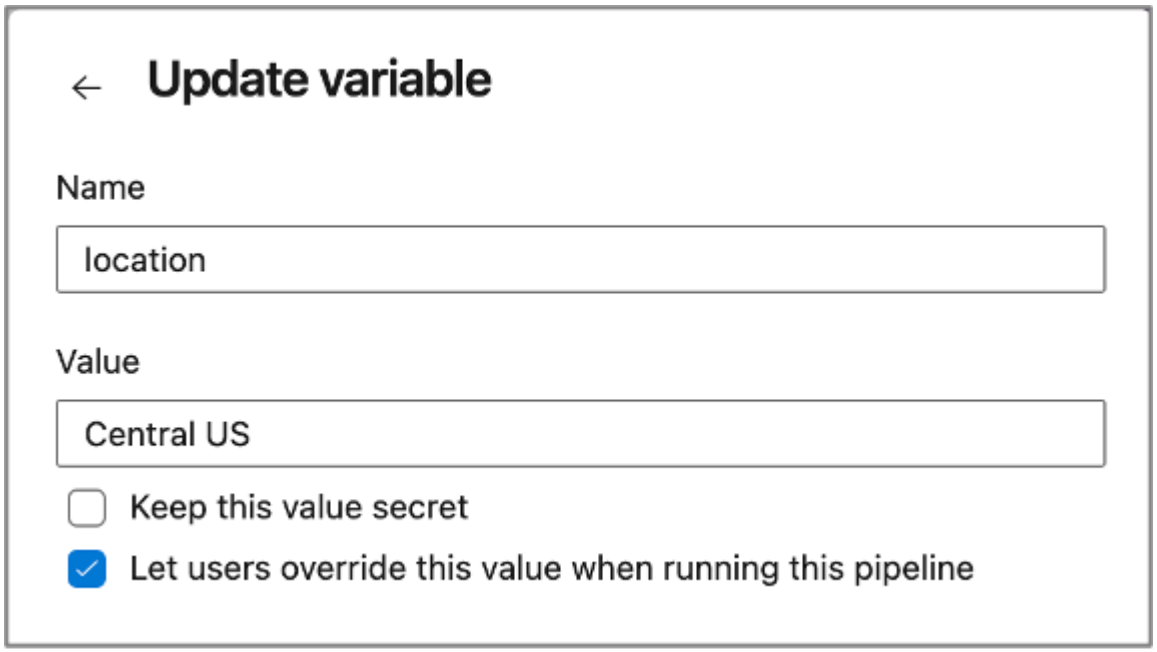
Warum und wann dieser Vorgang ausgeführt wird

https://players.brightcove.net/6274575390001/nUx4EKfUz_default/index.html?videoId=6351050870112

Folgen Sie diesem kurzen Video, um zu erfahren, wie Sie ein Azure DevOps-Katalogelement bestellen.

Prozedur

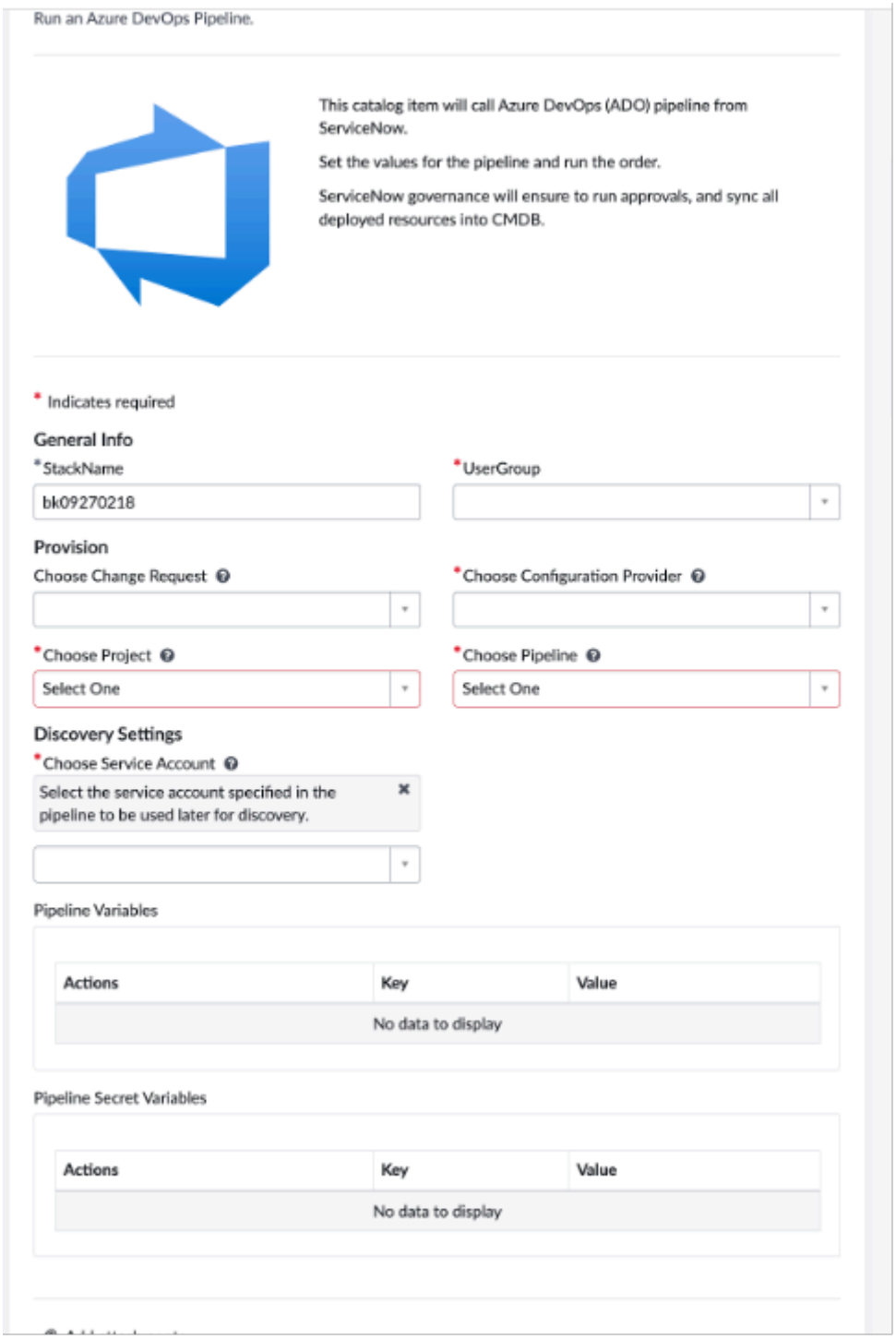
1. In **Aktualisieren Sie die Variable** Überschreiben Sie die Pipeline-Variablen, indem Sie auswählen **Zulassen, dass Anwender diesen Wert überschreiben, wenn diese Pipeline ausgeführt wird** Kontrollkästchen.



2. Navigieren zu **Mitarbeiter-Center** > **Cloudservices** > **Integrationen** > **CSC DevOps-Integration**an.

   Verwenden Sie dies Azure DevOps Bestellformular für Katalogelemente zum Aufrufen einer ADO-Pipeline.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Füllen Sie im Formular aus **Anwendergruppe** Und **Change-Anforderung** Felder.
4. Wählen Sie in der Liste Konfigurationsanbieter auswählen den Konfigurationsanbieter aus, der dem zugeordnet ist Azure DevOps Organisation.
5. Wählen Sie das Projekt und die zugehörige Pipeline in der Organisation aus.

   Die Pipeline-Variablen werden automatisch ausgefüllt. Sie können die Variablen ändern. Wenn beispielsweise die geheimen Pipeline-Variablen maskiert sind, können Sie diese Werte ändern.
6. Wählen Sie aus **Service-Account** , Dies ist die gleiche Option, die Sie als Serviceverbindung in ausgewählt haben Azure DevOps Pipeline.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Amazon Web Services, Eine Standortliste wird angezeigt, wenn Sie auswählen **Service-Account** .
- Sie können einen Standort oder eine Region einer Pipeline-Variable angeben und sie in einer Pipeline für die Bereitstellung verwenden. Diese Pipeline-Variable wird durch den Wert überschrieben, den Sie in der Standortliste ausgewählt haben, um die Bereitstellung und sicherzustellen Discovery Befinden sich am selben Standort.
- Für ist ein Standort erforderlich Discovery In Microsoft Azure, Daher wird keine Liste angezeigt, wenn Sie auswählen **Service-Account** . Diese Einstellungen stellen sicher, dass die richtigen Ressourcen, die sich auf den Stapel beziehen, in ausgefüllt werden CMDB. Sie können ausführen Discovery Basierend auf diesen Einstellungen.

7. Wenn der Standort für vorab ausgefüllt ist AWS Pipeline: Wählen Sie denselben Standort im Katalog für aus Discovery.
8. Richten Sie die Identifizierungs-Tags für die bereitgestellten Ressourcen ein.
   Das Feld Bereitstellungs-ID ist schreibgeschützt und wird für den Auftrag automatisch generiert. Die Bereitstellungs-ID wird allen bereitgestellten Ressourcen als Tag zugewiesen, wenn Sie sie als Tag in hinzugefügt haben Azure DevOps Pipeline-Vorlage der Stapel in der Cloud. Die Bereitstellungs-ID wird dem Stapel auch als Tag zugewiesen. Wenn die Pipeline eine dieser drei Variablen enthält (Anwendung, BusinessService oder CostCenter), werden sie in den allgemeinen Informationen in angezeigt Azure DevOps UI.
9. Wählen Sie in der Liste die Feldwerte aus, die in den Pipeline-Variablen aktualisiert werden sollen.

   Diese Einträge werden nur für den aktuellen Auftrag berücksichtigt.

   Hinweis: Sie können diese schreibgeschützten Variablen nicht im Abschnitt „Pipeline-Variable“ ändern. Diese Variablen werden dem Stapel in der Cloud als Tags hinzugefügt und in eingefügt CMDB Auch Schlüsselwerttabelle. Sie können nur Aktionen auf Ressourcenebene für einen bereitgestellten Stapel ausführen, da die Aktion auf Stapelebene deaktiviert ist. Der vorherige Stapel wird als veraltet markiert, wenn Sie die Pipeline erneut ausführen, obwohl die Ressourcen in der Cloud verbleiben.

Nächste Maßnahme

Überprüfen Sie, ob eine Blueprint-Genehmigungsrichtlinie (CSKInhaltsgenehmigungsrichtlinie ADO Integration) wird auf angewendet Microsoft Azure DevOps Katalog. Diese Richtlinie schreibt vor, dass eine Genehmigung von der Change-Management-Gruppe eingeholt werden muss, bevor eine Bereitstellung erfolgen kann.

Ansible mit Cloud-Services-Katalog integrieren

Integrieren Ansible Mit Cloud-Services-Katalog Als Tag 1-Aktivität. Mit dieser Aktivität können Sie einen bereitstellen Ansible Auftragsvorlage über ein ServiceNow Katalogelement.

Als Cloud_Service_user können Sie auf den Konfigurationsanbieter und die Auftragsvorlagen zugreifen und eine Auftragsvorlage über ein Katalogelement bereitstellen.

Support für Tag 0	Tag 1-Support	Tag 2-Support
1. Rufen Sie die Ressourcen aus der Cloud ab, und aktualisieren Sie CMDB 2. Stellen Sie sicher, dass keine Fehler vorhanden sind. Wenn Fehler angezeigt werden, wird	1. Bestellen Sie einen Ansible Auftragsvorlage von Servicekatalog 2. Referenzieren Sie die erkannte Microsoft Azure	1. Korrigieren Sie die Zuordnung von sofort einsatzbereiten über Cloud-Services-Katalog Inhalt 2. Aktualisieren Sie die Dokumentation zur Beschränkung der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support für Tag 0	Tag 1-Support	Tag 2-Support
die angezeigt Discovery Oder die Bereitstellung der Auftragsvorlage ist fehlgeschlagen	Pipelines, die spezifisch für sind Ansible 3. Wählen Sie Eingaben aus, die für die Release-Bereitstellungs-Pipeline erforderlich sind 4. Übermitteln Sie einen Katalog 5. Veröffentlichen Sie ein sofort einsatzbereites Katalogelement als Cloud-Services-Katalog Inhalt 6. Wählen Sie die Auftragsvorlagen aus, auf die Sie Zugriff haben, und stellen Sie sie bereit	Auftragsvorlage auf die Ausführung auf einem bestimmten Host 3. Testen und dokumentieren Sie, wie die Bereitstellung der Auftragsvorlage auf nicht verwalteten Knoten unterstützt wird 4. Beginnen Sie Ihren Support für Tag 2 für Ansible AWX
Speichern Sie in CMDB Als referenzierbare Objekte.	1. Warten Sie auf die Auftragsgenehmigung 2. Verfolgen Sie den Fortschritt Ihrer Vorlagenbestellung 3. Aktualisieren CMDB Mit den bereitgestellten Ressourcen	1. Stellen Sie sicher, dass alle Support-Aktionen für Tag 2 erfolgreich ausgeführt werden 2. Wechseln Sie zwischen der blauen (aktuelle Anwendung) und grünen (neue Anwendung) Umgebung

Einrichten Ansible Als Aufgabe von Tag 1

Richten Sie ein Ansible Konsole als Tag 1-Aufgabe, bevor Sie ausführen Discovery Und stellen Sie eine Auftragsvorlage über einen bereit ServiceNow Katalogelement mithilfe von Cloud-Services-Katalog Anwendung.

Vorbereitungen

Legen Sie die Bereitstellungs-ID für die zusätzlichen Variablen für fest Ansible Auftragsvorlagen.

Wählen Sie aus **Aufforderung beim Start** Option neben dem Variablenabschnitt in der Vorlage. Wenn Sie diese Aktion nicht ausführen, können Sie die standardmäßigen extra_vars, die mit den Werten aus dem Katalogauftragsformular definiert sind, während Sie die Vorlage starten, nicht aktualisieren oder überschreiben.

Markieren Sie alle Ressourcen mit dem Schlüssel „Deployment-ID“, um sie zu aktivieren Discovery Nach der Bereitstellung.

Erforderliche Rolle: Administrator

Prozedur

1. Speichern Sie die zusätzlichen Variablen lokal im JSON-Format, um sie zu erkennen und zu aktualisieren Configuration Management Database (CMDB).
2. Erstellen Ansible tower-Anmeldeinformationen, die in verwendet werden sollen Ansible Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Ansible Tower-Benutzernamen und -Passwort konfigurieren.

3. Zulassen, dass die zusätzlichen Variablen und Auftragsvorlagen überschrieben werden.
   Der Standard Ansible Auftragsvorlage muss überschrieben werden, damit die Pipeline mit funktioniert Cloud-Services-Katalog Ansible Automatisierungskatalogelement.

Ausführen Discovery Auf der Ansible Konfigurations-Provider

Fügen Sie hinzu Ansible Konfigurieren Sie den Provider, und führen Sie ihn aus Discovery Um zu erkennen, was sich im Bestand befindet, die Hostgruppe und die verfügbaren Auftragsvorlagen.

Vorbereitungen

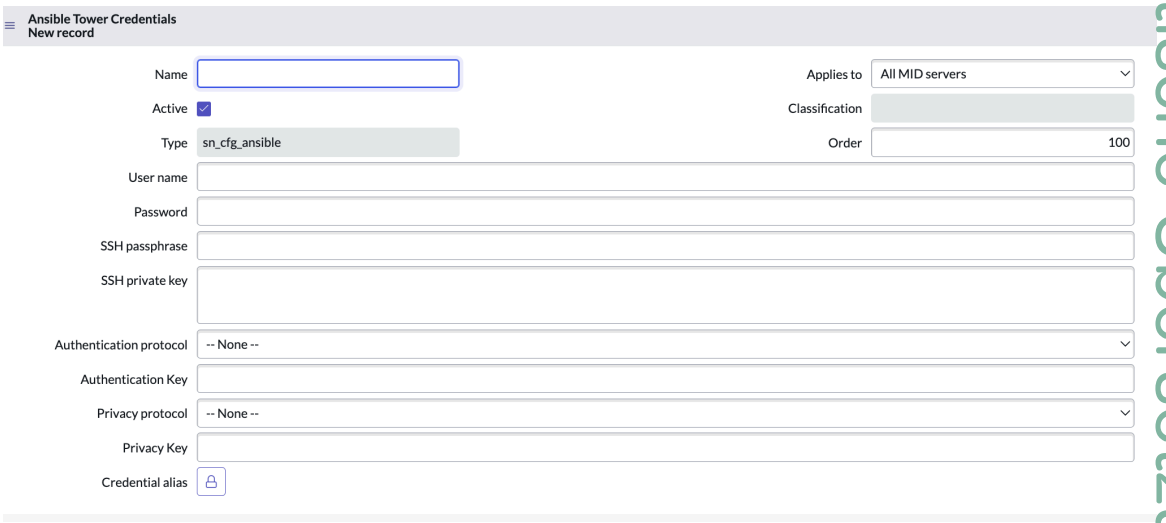
Führen Sie dieses Verfahren nur aus, wenn Sie haben Ansible Tower-Anmeldeinformationen.

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Anmeldeinformationen** > **Neu** > **Ansible Tower-Anmeldeinformationen**an.
2. Füllen Sie die Felder im Formular gemäß den Informationen aus, die Sie von erhalten haben Ansible Tower.

Ansible Tower-Anmeldeinformationen

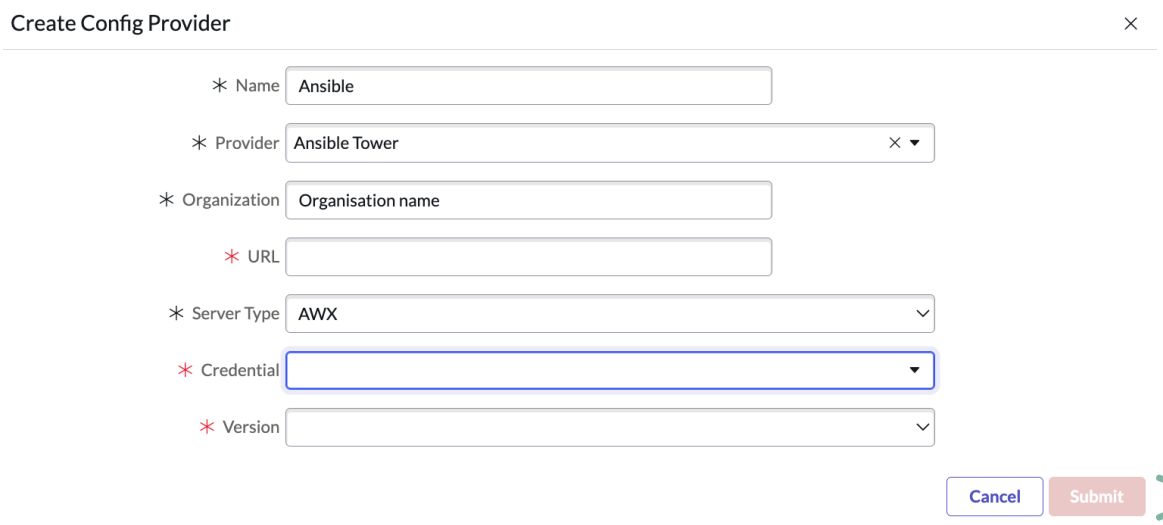


3. Wählen Sie **Absenden**.
4. Erstellen Sie einen Konfigurationsanbieter, indem Sie auswählen **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Konfigurationsprovider erstellen

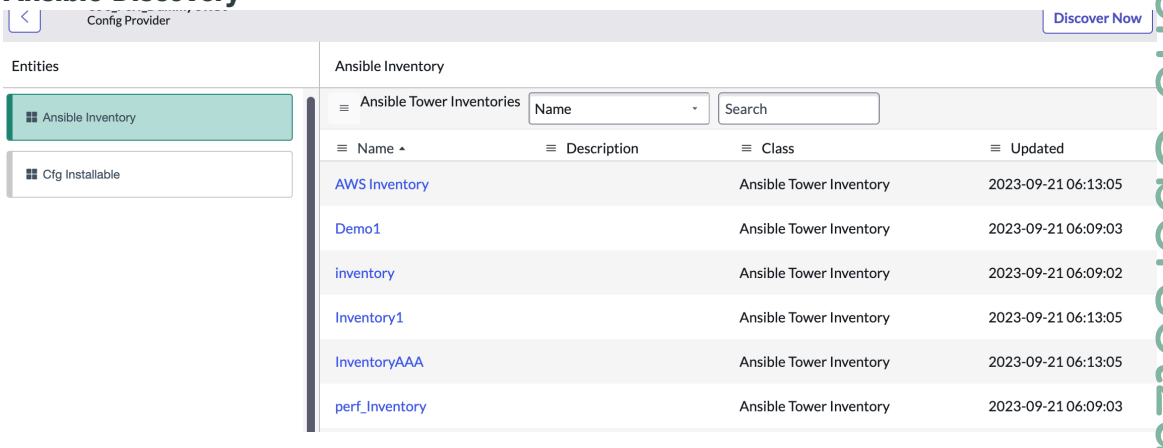


Wichtig:

Infrastruktur als Code (IAC) Discovery Wird unterstützt. Sie können Auftragsvorlagen, Bestand und Gruppen erkennen.

5. Führen Sie aus Discovery Um alle Projekte und zusätzlichen Variablen in einer Organisation zu erkennen.

Ansible-Discovery



Ergebnis

Sie sind bereit, die nächsten Schritte auszuführen, um einen zu bestellen Ansible Element.

Bestellen Sie einen Ansible Auftragsvorlage

Verwenden Cloud-Services-Katalog Zum Bestellen eines Ansible Auftragsvorlage, die aus dem Katalogelement aufgerufen wird.

Vorbereitungen

Erforderliche Rolle: Cloud_Service_user

Warum und wann dieser Vorgang ausgeführt wird

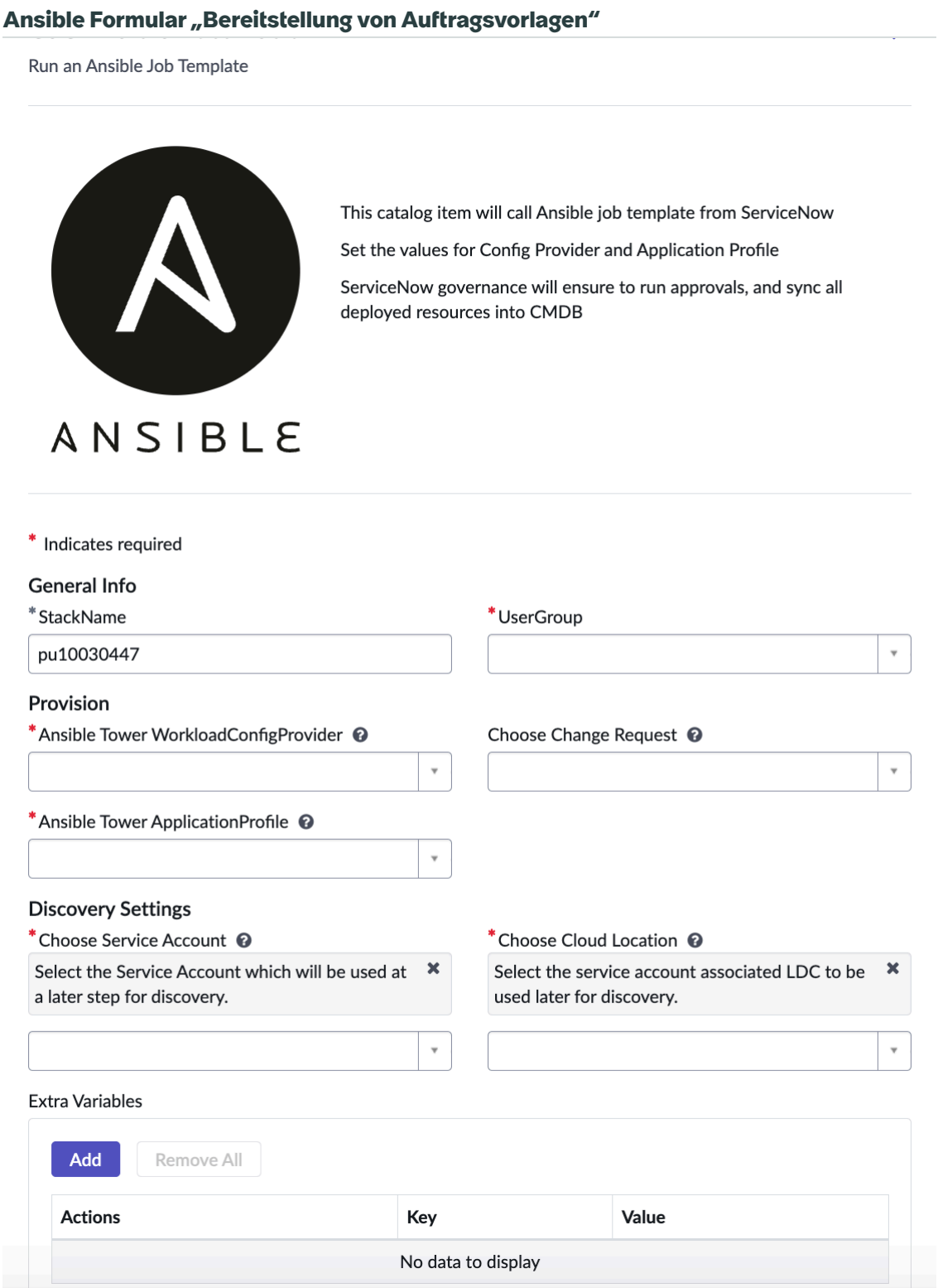
Sie können verwenden Ansible Formular für die Bereitstellung von Auftragsvorlagen zum Aufrufen von Ansible Auftragsvorlage und führen Sie sie über ein aus ServiceNow Katalogelement für die Bereitstellung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Mitarbeiter-Center** > **Cloudservices** > **Integrationen** > **CSC Ansible-Automatisierung**an.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansible Vorlagenformularfelder

Felder	Beschreibung
UserGroup	Anwendergruppe, die dem Anwender zugewiesen ist.
Bereitstellung	Bereitstellungsdetails. Wählen Sie den Anbieter der Arbeitsauslastungskonfiguration und das Anwendungsprofil aus Ansible Tower.
Service-Account wählen	Pipeline. Für Amazon Web Services, Die Liste Standort wird angezeigt, wenn Sie auswählen **Service-Account** . Der Standort ist für nicht erforderlich Discovery In Microsoft Azure. **Tipp:** Sie können eine zusätzliche Variable angeben, die im JSON-Format gespeichert wurde Ansible tower-Standort oder -Region, und verwenden Sie ihn in der Vorlage für die Bereitstellung. Diese zusätzliche Variable wird durch den Wert überschrieben, den Sie in der Liste Standort ausgewählt haben. Durch die Verwendung dieser zusätzlichen Variable stellen Sie sicher, dass die Bereitstellung und Discovery Befinden sich am selben Standort. Diese Einstellungen stellen sicher, dass die richtigen Ressourcen, die sich auf den Stapel beziehen, in ausgefüllt werden CMDB. Sie können ausführen Discovery Basierend auf diesen Einstellungen.
Cloud-Standort wählen	Serviceaccount, der dem Discovery zugeordnet ist.
Zusätzliche Variablen	Zusätzliche Variablen, die Sie ändern können, auch wenn die Werte automatisch ausgefüllt und maskiert werden.

2. Richten Sie die Identifizierungs-Tags ein.
   Das Feld Bereitstellungs-ID ist schreibgeschützt und wird für den Auftrag automatisch generiert. Die Bereitstellungs-ID wird allen bereitgestellten Ressourcen als Tag zugewiesen, wenn Sie sie als Tag in hinzugefügt haben Azure DevOps Pipeline-Vorlage der Stapel in der Cloud. Die Bereitstellungs-ID wird dem Stapel auch als Tag zugewiesen. Wenn die Pipeline eine dieser drei Variablen enthält (Anwendung, BusinessService oder CostCenter), werden sie in den allgemeinen Informationen in angezeigt Ansible Formular-UI für Auftragsvorlage.
3. Wählen Sie die Feldwerte aus der Liste aus, die in den Pipeline-Variablen aktualisiert werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Einträge werden nur für den aktuellen Auftrag berücksichtigt.

Hinweis: Sie können nur Aktionen auf Ressourcenebene für einen bereitgestellten Stapel ausführen, da die Aktion auf Stapelebene deaktiviert ist. Der vorherige Stapel wird als veraltet markiert, wenn Sie die Pipeline erneut ausführen, obwohl die Ressourcen in der Cloud verbleiben.

Nächste Maßnahme
Überprüfen Sie, ob eine Blueprint-Genehmigungsrichtlinie (CSKInhaltsgenehmigungsrichtlinie Ansible) Wird angewendet. Diese Richtlinie schreibt vor, dass die Genehmigung von der Change-Management-Gruppe eingeholt werden muss, bevor eine Bereitstellung erfolgen kann.

Cloud-Services-Katalog-Administrationsleitfaden

Nachdem Sie eingerichtet haben Cloud-Services-Katalog Anwendung müssen Sie einige zusätzliche Elemente einrichten, damit Ihre Anwender Cloud-Ressourcen anfordern und verwalten können.

Governance wird konfiguriert

Sie können Governance-Tools verwenden, um die Bereitstellung von Cloud-Ressourcen wie Quoten und Richtlinien einzuschränken. Sie können beispielsweise den Genehmigungs-Workflow konfigurieren, der verwendet wird, nachdem ein Anwender eine Cloud-Ressource angefordert hat, ob eine E-Mail gesendet wird, nachdem eine Cloud-Ressource gestoppt wurde, und welches Rechenzentrum automatisch ausgewählt wird, wenn ein Anwender eine Ressource von einem Cloud-Anbieter auswählt. Weitere Informationen zu Quoten, Richtlinien und anderen Governance-Typen finden Sie unter Cloud-Governance.

Wird ausgefüllt Cloud-Services-Katalog

Nachdem Sie die Governance-Quoten und -Richtlinien angewendet haben, müssen Sie erstellen Cloud-Services-Katalog Elemente. Sie haben folgende Möglichkeiten, um ein Katalogelement zu erstellen:

1. Importieren Sie eine Vorlage aus Amazon Web Services, Microsoft Azure Oder Google Cloud Platform.
2. Verwenden oder ändern Sie einen Sofort einsatzbereit Katalogelement.
3. Verwenden Sie einen Terraform-Vorlage .

Informationen zur Domänentrennung, Unterstützung für mehrere Repositorys mit Terraform App, Cloud-Accounts, das Cloud-Administratorportal oder die Cloud-API finden Sie in den folgenden Themen:

- Verwenden Sie die Struktur mehrerer Repositorys mit Terraform Connector App
- Domain Separation und Cloud-Services-Katalog: Ruft zusätzliche Informationen zur Domänentrennung ab.
- Cloud-Accounts: Erfahren Sie mehr über die logische Darstellung Ihrer gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance.
- Cloud-Adminportal: Verwalten, entwerfen, steuern, betreiben und analysieren Sie alle Ihre Cloud-Ressourcen über dieses Portal.
- Cloud-API (CAPI): Integrieren Sie Cloud Provisioning and Governance mit Cloud-Anbietern mithilfe VON REST APIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Services-Katalog Und Terraform-Connector

Verwenden Sie Cloud-Services-Katalog App mit Terraform Connector-Unterstützung mit allen Funktionen, die bei der Bereitstellung und Verwaltung von Cloud-Ressourcen in verschiedenen öffentlichen und privaten Clouds helfen.

Wichtige Funktionen von Terraform Connector:

- Verwenden Sie Terraform als Konfigurationsanbieter, um Ressourcen in den folgenden Clouds bereitzustellen:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud-Anbieter
- Erkennen Sie die IAC-Vorlagen (Infrastructure as Code), um die IAC zu erkennen (Terraform) Vorlagen aus dem Terraform Umgebung.
- Generieren Sie Katalogelemente mit Terraform Vorlagen, die sie zur Bereitstellung von Ressourcen in verschiedenen Cloud-Umgebungen verwenden.
- Verwenden Sie die Unterstützung der Struktur mehrerer Repositorys mit Terraform App. Siehe Verwenden Sie die Struktur mehrerer Repositorys mit Terraform Connector App Um mehr zu erfahren.

Weitere Informationen zu finden Terraform Connector, Konfigurieren der erweiterten Funktionen und ihrer Verwendung finden Sie unter Cloud Provisioning and Governance: Terraform Connector erkunden.

Berechtigungsverwaltung für Cloud-Services-Katalog

Berechtigungen sind Ihre Zugriffsrechte auf Gruppenebene für Funktionen und Aktionen in Cloud-Services-Katalog.

Die Berechtigungsrichtlinien in Cloud Provisioning and Governance Anwenderportal steuert die Aktionen, die für Anwender basierend auf der Anwendergruppe zulässig oder beschränkt sind. Siehe Berechtigungsverwaltung Für Berechtigungstypen und Ideen.

Derzeit gilt dies nicht für die Katalogbereitstellung in Cloud-Services-Katalog. Für CSK, Alle Anwender mit Rollenberechtigung können standardmäßig auf die Kataloge zugreifen, sie anzeigen und bereitstellen.

Richtlinien und Berechtigungsstufen für Services

Konfigurieren Sie Richtlinien mit den erforderlichen Berechtigungen, um Zugriff auf AWS, Azure, ADO zu gewähren. Ansible Und Google Cloud-Services.

- Cloud-Services-Katalog AWS – Standardkatalogberechtigungen
  - Amazon Web Services EC2 Linux Out-of-Box-Berechtigungen
  - AWS EC2 Windows OOB-Berechtigungen
  - AWS Dynamo DB-Berechtigungen
  - AWS S3-Bucket
- Azure OOB-Katalogberechtigungen
- Ansible-Berechtigungen
- ADO-Berechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cloud-Services-Katalog Google Cloud Platform – Out-of-Box-Katalogberechtigungen
  - Google Cloud Platform (GCP) Große sofort einsatzbereite Berechtigungen für Abfrage
  - Google Cloud Platform Cloud-SQL-Out-of-Box-Berechtigungen
  - Google Cloud Platform Standardmäßige Linux-Berechtigungen
  - Google Cloud Platform Standardberechtigungen für Lastenausgleichsmodul
  - CSK GCP Windows OOB-Berechtigungen

Cloud-Services-Katalog verwenden

Die Cloud-Services-Katalog Die Anwendung ist ein dynamisches Portal für alle Ihre täglichen Cloud-Aktivitäten. Mit dieser Option können Sie Stapel verwalten, mit Anforderungen arbeiten und auf die sofort einsatzbereiten Katalogelemente und andere beliebte Themen zugreifen.

Sie können Cloud-Services erkunden, indem Sie eine Suche in durchführen ServiceNow AI Platform® Plattform. Sie können auch zugehörige Links finden, z. B. **Durchsuchen Sie Den Cloud-Katalog** Und **Geführtes Setup für CSC** .

Cloud-Services sind auch so konzipiert, dass sie im angezeigt werden Mitarbeiter-Center Symbolleiste als neue Registerkarte. Suchen Sie nach den bereitgestellten Optionen, oder navigieren Sie zu **Durchsuchen Sie Cloud-Services** Zu Experience Cloud-Services-Katalog.

Die Cloud-Services-Katalog Anwendung zeigt die Funktionen in der folgenden Tabelle an.

Cloud-Services-Funktionen

Funktion	Beschreibung
Meine Stapel	Listet alle Stapel auf, die Ihnen zugewiesen sind. Wählen Sie ein Katalogelement aus, um die vom Element gestarteten Stapel anzeigen zu lassen. Wählen Sie einen Stapel aus, um die Details anzuzeigen, z. B. alle Ressourcen, Ressourceneigenschaften, Aktivitäten und Lebenszyklusvorgänge.
Cloud-Services-Themen	Stellt die Quick-Links zu beliebten und relevanten Themen bereit.
Durchsuchen Sie Cloud-Services	Stellt die Suchfunktion bereit, die von unterstützt wird KI-Suche. Es gibt relevante Cloud-Services zurück, stellt Filter bereit und sortiert Ergebnisse, mit denen Sie den gewünschten Cloud-Service vergrößern können. Diese Funktion ist von der globalen Suche getrennt, die auf der angezeigt wird Mitarbeiter-Center Zielseite. 1. Verwenden Sie Filtern nach und Sortieren nach, um Ihre Suche einzugrenzen. 2. Sie können auch die Karten- oder Listenansicht nach Bedarf verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Services-Funktionen (Fortsetzung)

Funktion	Beschreibung
	3. Wählen Sie eine der Quellen aus, um die Suchergebnisse zu filtern. **4.** Verwenden Sie einen Themenfilter, um die Ergebnisse einzugrenzen.
Letzte Stapel	Listet alle Stapel mit den letzten Aktivitäten auf, die für sie ausgeführt wurden.
Meine Ressourcen	Beobachtet die erkannten Ressourcen und interagiert mit ihnen.

Cloud-Services Werden Angefordert

Senden Sie eine Anforderung für eines der verfügbaren Servicekatalogelemente in Cloud-Services. Sie finden die Kataloge unter **Durchsuchen Sie Cloud-Services** .

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Navigieren Sie zu **Durchsuchen Sie Cloud-Services** Unter **Cloud-Services** Auf der Seite „Mitarbeiterzentralportal“ in Cloud-Services-Katalog.
2. Suchen Sie in den angezeigten Optionen nach einem geeigneten Katalogelement.
3. Wählen Sie Aus **Anforderung** .
   Dadurch wird das Anforderungsformular mit Informationen und Anhängen geöffnet, die angegeben werden sollen.
4. Geben Sie die Details in die Formularfelder ein, um sie zu bestellen.
   Wenn Sie eine Anforderung für ein Element an den Servicekatalog übermitteln, stellt das System den Stapel in der Regel sofort bereit. Manchmal muss die Anforderung zuerst genehmigt werden.

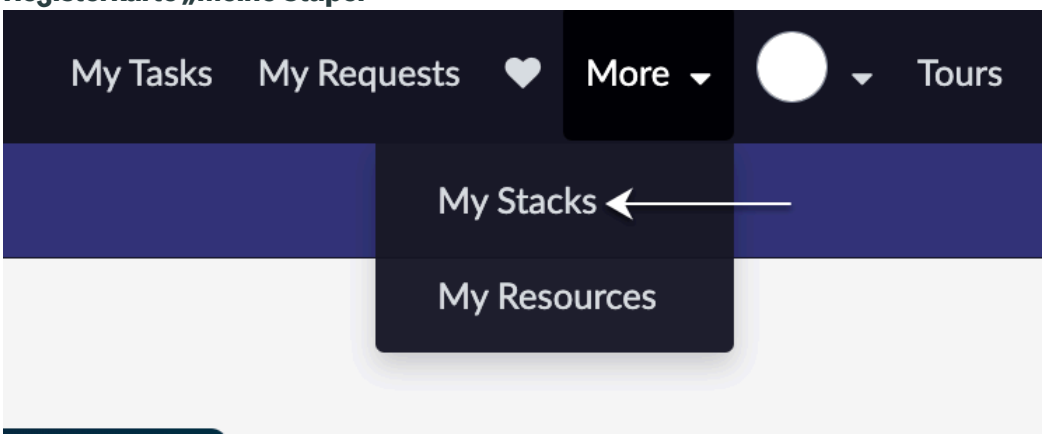
Erkunden Sie die Registerkarte meine Stapel

Sortieren, anzeigen oder verwalten Sie Ihren Stapel von Cloud-Ressourcen und -Services als Teil der Aktivitäten von Tag 2 mithilfe von **Meine Stapel** Registerkarte im Mitarbeiter-Center Symbolleiste in Cloud-Services-Katalog.

Die **Meine Stapel** Die Registerkarte verfügt über mehrere Optionen, mit denen Sie Ihre Stapel mit einem anderen verwalteten Status kategorisieren, sortieren oder anzeigen können. Das folgende Beispiel zeigt, was der ist **Meine Stapel** Registerkarte sieht wie auf aus Mitarbeiter-Center.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „meine Stapel“



Auf der **Meine Stapel** Registerkarte können Sie die folgenden Status anzeigen:

- Verwaltete Stapel: Alle Stapel in allen Servicekategorien.
- Stapel nach Katalogelementen: Stapel, die nach dem Katalogelement aufgelistet werden.
- Stapel mit Problemen: Stapel, die aufgrund unvollständiger oder nicht genehmigter Elemente Fehler aufweisen.
- Stapel mit Folgeaktionen: Stapel mit ausstehender Aktion, die verfolgt werden soll.
- Erkannte Stapel (nicht verwaltet): Stapel, denen kein Katalog zugeordnet ist.

Suchen Sie nach **Ansicht „meine Stapel“** Registerkarte am Ende des Menübands „meine Stapel“, um auf eine der folgenden Ansichten zuzugreifen:

- Stapel, die ich besitze: Von Ihnen erstellte Stapel.
- Stapel im Besitz von Gruppen, denen ich angehöre: Stapel, die von Ihnen und allen Gruppen erstellt werden, denen Sie zugeordnet sind.
- Stapel im Besitz einer beliebigen Person: Alle Stapel in der Instanz.

Meine Stapel Verwalten

Verwenden Sie **Meine Stapel** Registerkarte, um auf alle Stapeleigenschaften zuzugreifen, z. B. die Details zum Erstellen, Aktualisieren und Löschen.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Rufen Sie die Seite „Stapel“ auf, indem Sie zur Symbolleiste oder Homepage wechseln.

   - Wählen Sie in der Symbolleiste die aus **Meine Stapel** Registerkarte.
   - Wählen Sie auf der Homepage meine Stapel die aus **Letzte Stapel** Registerkarte.

     Standardmäßig werden alle Stapel in allen Servicekategorien mit Ausnahme des Status „Veraltet“ aufgelistet.

2. Verwenden Sie im Navigationsbereich eine Filterkategorie, um die übereinstimmenden Stapel anzuzeigen. Die Filter werden als bearbeitbare Bedingungen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Die Stapel werden mit den Eigenschaften angezeigt, die sich in der folgenden Tabelle befinden.

Stapeleigenschaften

Eigenschaftsname	Beschreibung
Name	Name, den Sie bei der Anforderung des Stapels angegeben haben.
Servicekatalogelement	Service, der bei der Bestellung des Katalogs erstellt wurde, der zu diesem Stapel geführt hat.
Stapelstatus	Status des Stapels: • Wird initialisiert • Aktiv (bereitgestellte Stapel) • Fehler • Wird verarbeitet (Stapel werden verarbeitet) • Wird beendet • Beendet (bereitgestellte Stapel) • Nicht verwaltet (erfasste Stapel) • Fehler wird behoben (Stapel mit Fehlern) • Nachverfolgung erforderlich • Veraltet
Eigentum von	Benutzername der anfordernden Person.
Besitzergruppe	Gruppenname, dem der Stapel zugewiesen ist.
Serviceanforderungselement	Datensatz, der in der Tabelle „Anforderungselement“ erstellt wurde, als Sie den Katalog bestellt haben, der zu diesem Stapel geführt hat.
Anforderung	Anforderungsnummer, die dem Anforderungselement zugeordnet ist.
Erstellt	Datum und Uhrzeit der Anforderung des Stapels.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Stapeldetails.

Arbeiten Sie mit Stapeln

Starten Sie Ihre Day 2-Vorgänge, indem Sie Ihre Stapel starten, stoppen, die Bereitstellung aufheben oder ändern.

Vorbereitungen
Erforderliche Rolle: sn_CMP.Cloud_Service_user.root_admin, admin oder sn_CMP.Cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

festgelegt, dass der Change entweder automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss. Weitere Informationen finden Sie unter .

Prozedur

1. Im Navigationsbereich in **Name** Feld einen Stapel und dann auswählen **Vorgänge Nachverfolgen** .
2. Zeigen Sie den Anforderungsstatus und den Status der Stapel an, indem Sie auswählen **Status** .
3. Zeigen Sie die Eigenschaften und Anforderungsparameter an, indem Sie auswählen **Anforderungsdetails** .
   Sie können die Stapeldetails auch in einem Popup-Fenster anzeigen, indem Sie auswählen **Vollständige Details Anzeigen** .
4. Suchen und sortieren Sie alle Vorgänge, die Sie durch Auswahl von ausgeführt haben **Stapelvorgänge** .

Zeigen Sie die Stapelabhängigkeit an

Erkunden Sie die Details der Konfigurationselemente, Services und anderer Aufgaben, die den Stapeln und Ressourcen zugeordnet sind, mithilfe von Abhängigkeit anzeigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

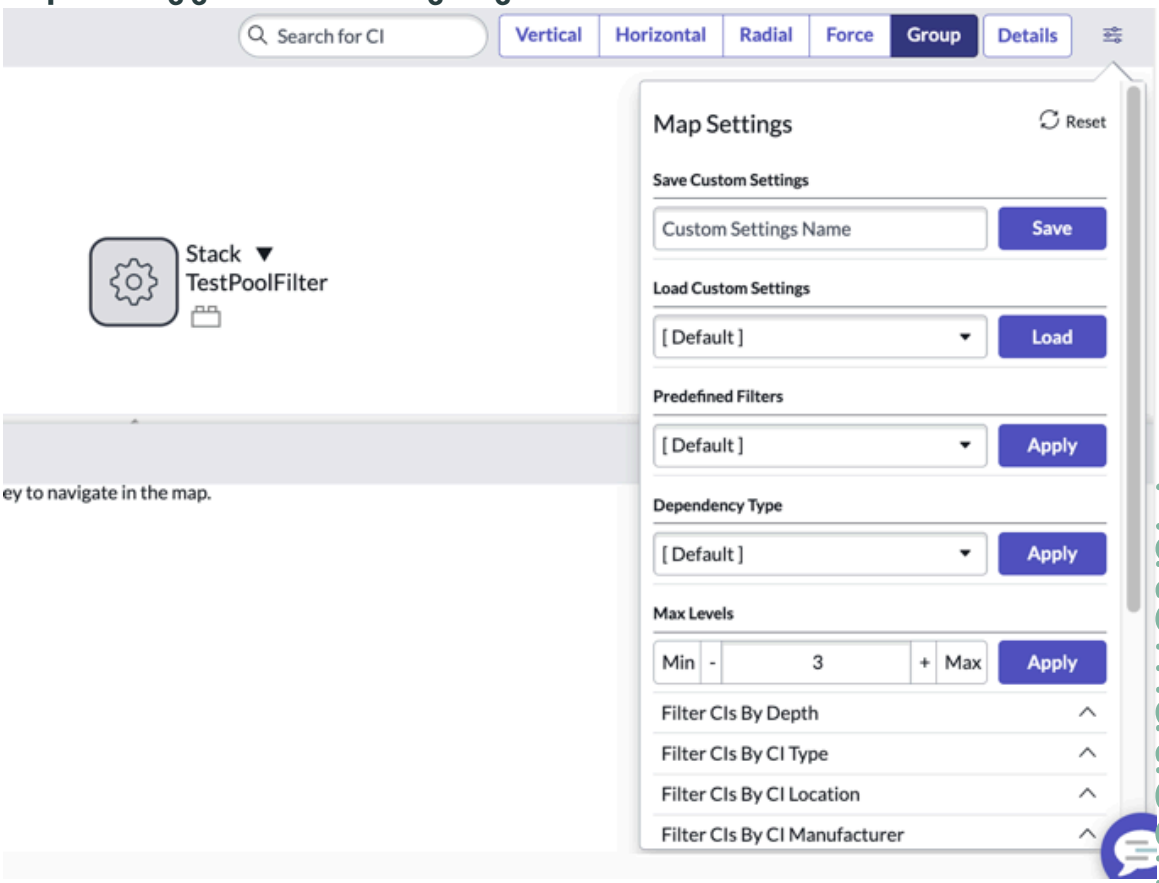
Ein Stapel kann von mehreren Stapeln abhängig sein, und mehrere Stapel können von einem einzelnen Stapel abhängen. Stapel, die mehrere Konfigurationselemente (Configuration Items, CIs) und Services enthalten, bilden die Stapelabhängigkeiten in der Cloud-Services-Katalog Anwendung. Die Abhängigkeitszuordnung bietet eine einfache und detaillierte grafische Darstellung dieser komplexen Einstellungen. Sie können durch die Verweise navigieren, um die Auswirkungen des Ereignisses zu verstehen, die eine Verzweigung auf eine andere hat.

Prozedur

1. Wählen Sie auf der Seite „verwaltete Stapel“ einen Stapel aus, um die Seite „Stapelvorgänge“ zu öffnen.
2. Wählen Sie im Menüband „vollständige Details anzeigen“ die Option aus **Abhängigkeit anzeigen** .
3. In **Suchen Sie nach CI** , Geben Sie ein CI ein, um die Abhängigkeitszuordnung anzuzeigen.
4. Füllen Sie im Formular die Felder aus.
   Das folgende Beispiel zeigt die Einstellungen zum Anzeigen der Stapelabhängigkeiten. Zu den Einstellungen gehören „Anwenderdefinierte Einstellungen speichern“, „Anwenderdefinierte Einstellungen laden“, „Vordefinierte Filter“, „Abhängigkeitstyp“ und „Max. Ebenen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stapelabhängigkeiten werden angezeigt



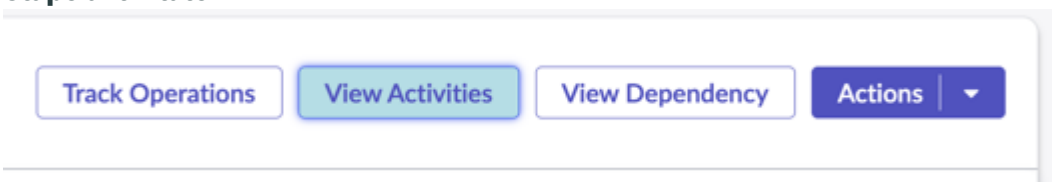
5. Machen Sie alle CI-Filterauswahlen rückgängig, und setzen Sie die Zuordnungseinstellung zurück, indem Sie auswählen **Zurücksetzen** .

Ansicht „Stapelaktivitäten“

Zeigen Sie die Cloud-Aktionen für Ihre Stapel und Ressourcen mit an **Zeigen Sie Aktivitäten An** Registerkarte.

Sie können im Stapellebenszyklus mehrere Aktionen ausführen, z. B. Vorgänge nachverfolgen, Aktivitäten anzeigen, Abhängigkeit anzeigen und Aktionen ausführen. Das folgende Beispiel zeigt die Stapelaktivitäten, die Sie ausführen können, und die folgende Tabelle beschreibt die Aktivitäten.

Stapelaktivitäten



Stapelt Aktivitäten

Aktivität	Beschreibung
Change-Anforderungen	Change-Anforderungen, die für Stapel oder Ressourcen eingereicht wurden, die Ihnen zugewiesen sind. Das System generiert Change-Anforderungen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

StapeIt Aktivitäten (Fortsetzung)

Aktivität	Beschreibung
	wenn Sie Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen.
Incidents	Incidents für Stapel und die zugehörigen Ressourcen, die Ihnen zugewiesen sind.
Aufgaben	Katalogaufgaben, die erstellt werden, wenn eine Anforderung für einen Stapel nicht bereitgestellt werden kann.
Geplante Vorgänge	Liste der geplanten Vorgänge, die Stapeln zugeordnet sind und als folgende Funktionen angezeigt werden: • Betriebszeit • Zielvorgabe • Vorgang • Status

Aktionen für Stapel

Greifen Sie auf einen bestimmten Stapel zu, um einen Tag 2- oder Lebenszyklusvorgang auszuführen, z. B. „Stoppen“, „Start“, „Deprovisionierung“, „ModifyLease“ oder „ModifySchedule“.

Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. Eine Genehmigungsrichtlinie gibt an, dass der Change automatisch genehmigt wird oder dass ein Anwender in der Genehmigerliste den Change genehmigen muss.

Die Stapel und Ressourcen durchlaufen Lebenszyklusvorgänge ab dem Zeitpunkt, zu dem sie gestartet, bereitgestellt, debereitgestellt und dann beendet werden. Manchmal müssen Sie den Zeitplan einer bestimmten Ressource für Konfigurationsprobleme aktualisieren oder stoppen. Sie können einen Stapel oder eine Ressource auswählen, um diese Vorgänge auszuführen. Die Aktionen enthalten nur die entsprechenden Vorgänge für die ausgewählte Ressource oder den ausgewählten Stapel. Nicht alle Vorgänge werden standardmäßig für alle Anbieter oder für alle Servicekategorien (Ressourcentypen) unterstützt.

Das folgende Beispiel zeigt die Aktionen, die Cloud-Services-Katalog Anwendungsunterstützung auf Stapeln. Die Aktionen sind „Stoppen“, „Start“, „Deprovisionierung“, „ModifyLease“ oder „ModifySchedule“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen für Stapel

In der folgenden Tabelle sind die Vorgänge aufgeführt, die die Cloud-Services-Katalog Anwendungsunterstützung als Aktionen auf Stapeln.

Aktion	Funktion
Stoppen	Stoppt die ausgewählte virtuelle Maschine (VM). Der Ressourcenstatus ändert sich in aus. Keine Einstellung ist erforderlich.
Start	Startet die von Ihnen ausgewählte VM. Der Ressourcenstatus ändert sich in ein. Keine Einstellung ist erforderlich.
Aufheben der Bereitstellung	Beendet den ausgewählten Stapel und sendet eine Benachrichtigung an den Stapelbesitzer. Keine Einstellung erforderlich.
ModifyLease	Ändert das Mietenddatum.
ModifySchedule	Ändert das Zeitplanprofil und die Zeitzone des Zeitplans.

Weiterleitung zu „meine Stapel“

Sie können Umleitung zu verwenden **Meine Stapel** Registerkarte als alternative, aber vereinfachte Methode zum Auffinden eines Stapels aus dem **Meine Anforderungen** Registerkarte. Sie können beispielsweise Umleitung verwenden, während Sie nach einem Stapel suchen, der kürzlich bereitgestellt wurde.

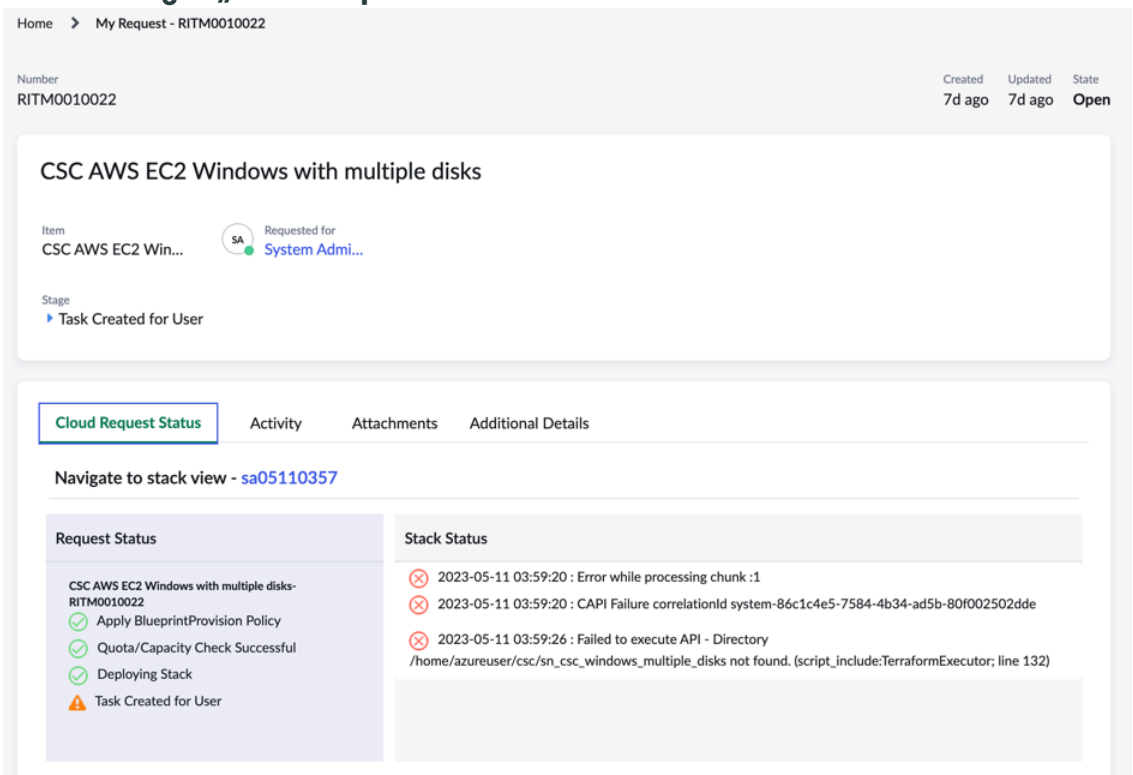
Sie können alle Ihre Stapel mit jedem relevanten Status anzeigen, die angezeigte Liste kann jedoch lang sein.

Umleitung zu Stapeldetails über **Meine Anforderungen** Registerkarte in Mitarbeiter-Center Ermöglicht Ihnen, den angeforderten Stapel durch das angeforderte Element (Requested Item, RITM) zu finden. Verwenden Sie **Cloud-Anforderungsstatus** Registerkarte im Cloud-Services-Katalog Anwendung zum Anzeigen der Anforderungsdetails und des Status der Stapel.

Das folgende Beispiel zeigt, wie Sie zu umleiten können **Meine Stapel** Registerkarte von **Meine Anforderungen** Registerkarte, anstatt sich eine umfassende Liste von Stapeln auf der Stapel-Homepage anzusehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weiterleitung zu „meine Stapel“



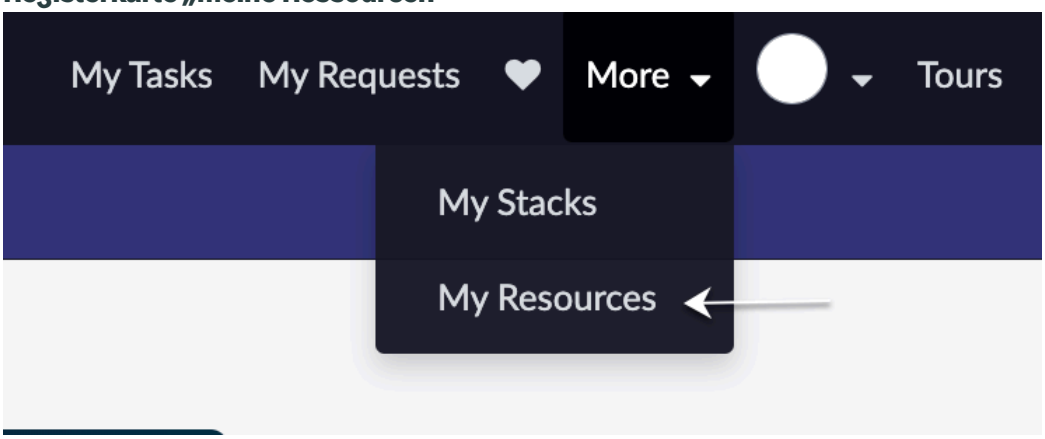
Meine Ressourcen Erkunden

Beobachten und interagieren Sie mit erkannten Ressourcen, indem Sie verwenden **Meine Ressourcen** Option Unter **Mehr** Registerkarte Auf der Mitarbeiter-Center Symbolleiste.

Sie können die Operatoren oder Besitzer für die identifizierten Ressourcen festlegen, damit sie diese Ressourcen mit standardmäßigen Tag 2-Vorgängen verarbeiten können. Indem Sie diese Aktionen über ausführen ServiceNow AI Platform Von Cloud-Services-Katalog Anwendung können Sie die Workflows für das richtige Change-Management, Audit-Trails und die allgemeine Governance nutzen.

Das folgende Beispiel zeigt **Meine Ressourcen** Registerkarte.

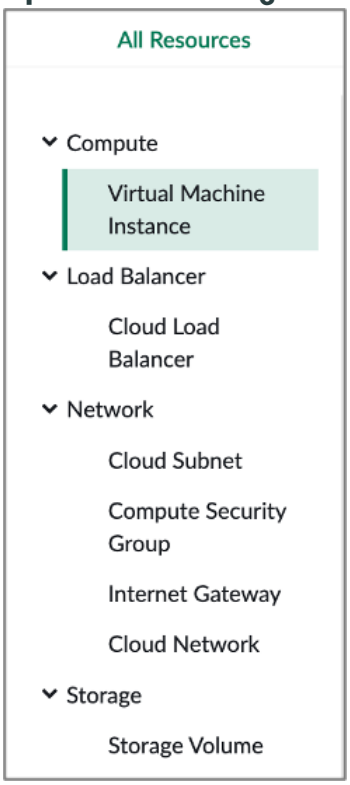
Registerkarte „meine Ressourcen“



Das folgende Beispiel zeigt eine Liste der Ressourcenkategorien und Filter, mit denen Sie auf die relevante Ressource zugreifen und andere Funktionen ausführen können, z. B. Speichern und Exportieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen auf der Registerkarte alle Ressourcen



Die Cloud-Ressourcen werden wie oben beschrieben kategorisiert. Sie können auf eine der Kategorien zugreifen, um sie zu verwalten.

Verwalten Sie meine Ressourcen und Ressourcenfilter

Greifen Sie mit dem Ressourcenfilter auf die Ressourcen zu, die Sie besitzen, Ressourcen, die einer Gruppe gehören, oder auf die Ressourcen eines beliebigen Benutzers. Sie können dann die benötigten Informationen mithilfe von Sortierfunktionen, Bedingungen, Kategorien und Stichwörtern finden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

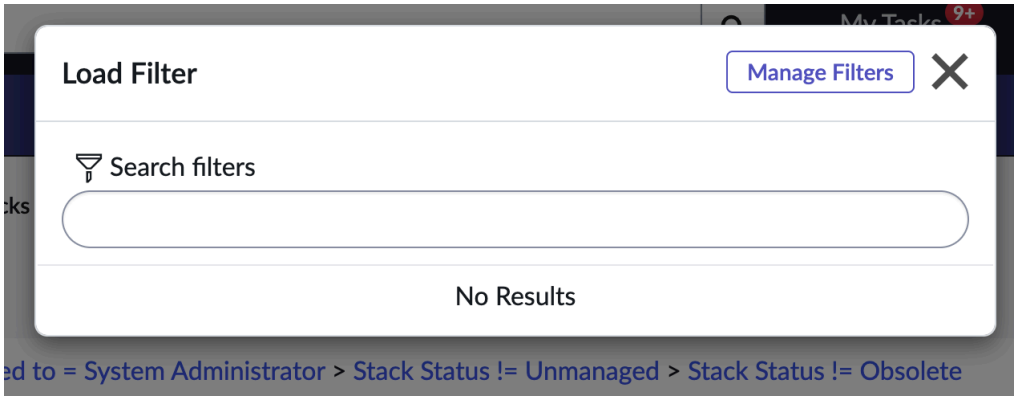
1. Wählen Sie im Navigationsbereich die Ressourcenkategorie aus, wenden Sie einen Filter an (vorab hinzugefügt oder neu), und wählen Sie aus **Ausführen** Dient zum Anzeigen und Exportieren einer Reihe von Ressourcen.
2. Sortieren Sie, zeigen Sie die Details an, und exportieren Sie sie nach Bedarf.

Ressourcenfilteroptionen

Automatische Übersetzung

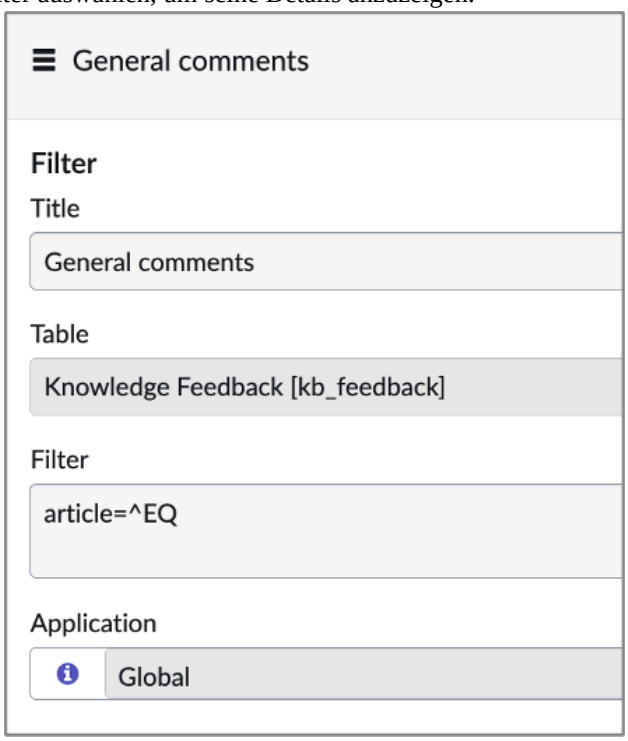
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenden Sie einen vorhandenen oder einen gespeicherten Filter an, indem Sie auswählen **Filter Laden** .
4. Wählen Sie im Fenster Filter laden die Option aus **Filter Verwalten** Um die Liste der zuvor hinzugefügten Filter zu finden.



5. Wählen Sie die Menüoption entlang aus **Filter** Zum Anzeigen der verschiedenen Optionen zum Exportieren der gefilterten Ressourcen.

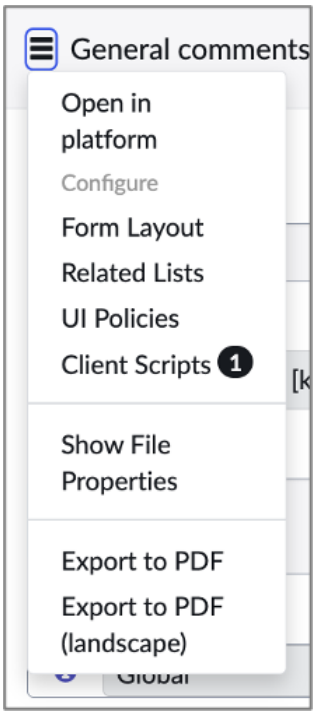
6. Sie können auch einen Filter auswählen, um seine Details anzuzeigen.



7. Zeigen Sie weitere Optionen und Details zum ausgewählten Filter an, indem Sie die Menüoption neben Allgemeine Kommentare auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Stichwortsuche verwenden, um einen Filter direkt mithilfe von Stichwörtern zu finden. Sie können Exportoptionen wie PDF, Excel oder CSV auswählen.

8. Erstellen und fügen Sie einen oder mehrere Sätze von Bedingungen hinzu, indem Sie zu navigieren **Neues Kriterium** > **Einen weiteren Satz Bedingungen erstellen**an.
9. Speichern Sie den erstellten Filter, indem Sie auswählen **Filter Speichern** .
10. Weisen Sie in den Feldern Name, Abfrage und Sichtbarkeit den Namen, die Abfrage, und Sichtbarkeit. Sie können auch Sortieroptionen hinzufügen, indem Sie auswählen **Sortierung Hinzufügen** .
11. Weisen Sie eine Sortierreihenfolge aus der Liste zu, und wählen Sie dann aus **Speichern** .
12. Wählen Sie unter Ansichtsoptionen eine der folgenden Optionen aus:
    - Ressourcen, die ich besitze: Diese Option ist standardmäßig ausgewählt
    - Ressourcen im Besitz von Gruppen, denen ich angehöre: Diese Option zeigt alle Gruppen an, denen Sie angehören.
    - Ressourcen im Besitz eines beliebigen Benutzers: Diese Option zeigt alle Ressourcen in der ausgewählten Kategorie in an Configuration Management Database (CMDB), Und zugewiesen.

Sofort einsatzbereite Kataloge mit Cloud-Services-Katalog

Cloud-Services-Katalog Enthält sofort einsatzbereite Katalogelemente, Aktionen und Richtlinien, die Sie nach Bedarf rendern können.

Gebrauchsfertige Katalogelemente für Azure verwenden, GCP Und Amazon Web Services Cloud-Serviceanforderungen und -Automatisierungen. Sie können entweder eines der Katalogelemente bestellen, Flow Designer-basierte Aktionen oder Bereitstellungsrichtlinien verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie die Katalogelemente unverändert, und ändern oder aktualisieren Sie sie nicht. Durch Änderungen oder Anpassungen wird das Standardverhalten des Katalogs geändert und es werden nicht die erwarteten Ergebnisse erzielt. Dies wirkt sich auch auf deren Upgrades aus. Sie können eine Kopie der Vorlagen erstellen und Ihre Katalogelemente unter Berücksichtigung des sofort einsatzbereiten Inhalts neu erstellen.

Bestellen Sie von diesen Cloud-Services-Katalog Sofort Einsatzbereite Katalogelemente:

Amazon Web Services EC2 Linux – sofort einsatzbereite Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzliche Datenträger auf EC2 oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Linux-Instanz eines beliebigen Instanztyps von Amazon EC2 anzufordern.

Bestellen Sie eine AWS EC2 Linux-VM Das Video zeigt, wie Sie einen bestellen Amazon Web Services Virtuelle EC2 Linux-Maschine.

Linux-VM-Aufträge und -Funktionen:

Reihenfolge	Features
Bestellen Sie eine virtuelle Linux-Maschine auf EC2, die die Installation von Agent Client Collector ermöglicht. ACC ist für Produktionsinstanzen obligatorisch. Andere VM-Größen als t2.nano, t2.Micro erfordern eine Genehmigung. Der Cloud-Konfigurationsscan wird zur Compliance-Prüfung ausgeführt.	Für andere Instanztypen als t2.nano und t2.micro ist eine Genehmigung durch den Administrator erforderlich, je nach Richtlinie. Das Katalogelement verfügt über integrierte Clientregeln, um eine ACC-Installation (Agent Client Collector) zu steuern, wenn die Bereitstellungsumgebung für die Produktion markiert ist. Um den Anmeldeinformationsalias-Schlüssel für die ACC-Bereitstellung aus MID auszuwählen, müssen dem Anwender die entsprechenden ACC-Administratorrollenberechtigungen gewährt werden. Die Voraussetzungen finden Sie unter „ACC-* nach der Bereitstellung bereitstellen“ unten. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel mit dem Status „Nachverfolgung erforderlich“ festgelegt, um zu benachrichtigen, dass die Stapelbereitstellung nicht den Normen entspricht.
Bestellen Sie eine virtuelle Linux-Maschine auf EC2, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich. Holen Sie für alles darüber hinaus eine Genehmigung ein.	Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, bitten Sie den Administrator nach Richtlinie um Genehmigung.
Bestellen Sie einen sicheren virtuellen Linux-Computer mit	Dieses Katalogelementformular ermöglicht die Zuweisung einer Netzwerksicherheitsgruppe zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
erhöhter Sicherheit, indem Sie eine Netzwerk-Sicherheitsgruppe zuweisen, um die höchste Sicherheitsstufe zu gewährleisten.	Recheninstanz, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Amazon Web Services EC2 Linux Out-of-Box-Berechtigungen

Amazon Web Services Berechtigungen für EC2 Linux OOB-Katalogelemente

Katalogelement	Services	Berechtigungen
CSK AWS EC2 Linux-VM	AWS EC2-Bereitstellung	1. DescribeVolumes 2. DescribeImages 3. DescribeInstances 4. DescribeVolumes 5. DescribeInstanceCreditSpecifications 6. DescribeInstanceAttribute 7. DescribeInstances 8. DescribeTags 9. DescribeInstanceTypes 10. DescribeInstances 11. DescribeVpcs 12. Ausführungsinstanzen 13. DescribeImages 14. GetCallerIdentity
	AWS EC2-Instanz: Stoppen	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2-Instanz – Start	1. DescribeImages 2. DescribeInstances 3. Startinstanzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
	AWS EC2-Instanz: Bereitstellung der vm aufheben **Hinweis:** Auch dieses Speichervolume wird von der Bereitstellung aufgehoben.	1. DescribeAddresses 2. Beendigungsinstanzen
	AWS EC2-Instanz: Stack zur Aufhebung der Bereitstellung **Hinweis:** Beendet alles, einschließlich nic.	1. GetCallerIdentity 2. DescribeInstances 3. DescribeImages
CSK AWS EC2 Linux mit mehreren Datenträgern	AWS EC2 Linux – Bereitstellung mehrerer Datenträger	1. DescribeVolumes 2. DescribeImages 3. DescribeInstances 4. AttachVolume 5. DescribeInstances 6. Erstellen Sie ein Volume 7. DescribeInstanceCreditSpecifications 8. DescribeInstanceAttribute DescribeVpcs 9. DescribeInstanceTypes 10. DescribeTags RunInstances 11. GetCallerIdentity
	AWS EC2 Linux – mehrere Datenträger werden angehalten	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2 Linux – mehrere Datenträger starten	1. DescribeImages 2. DescribeInstances 3. Startinstanzen
	AWS EC2 Linux-Stapeldeprovisionierung für mehrere Datenträger: Beendet alle Ressourcen	1. DescribeInstances 2. Beendigungsinstanzen 3. ModifyInstanceAttribute 4. DescribeVolumes 5. Löschen Sie Volume 6. GetCallerIdentity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		7. DetachVolume 8. DescribeInstanceCreditSpecifications 9. DescribeVpcs 10. DescribeInstanceTypes 11. DescribeTags 12. DescribeImages
CSK AWS EC2 Linux mit Sicherheitsgruppen	AWS EC2 Linux mit Sicherheitsgruppen – Bereitstellung	1. DescribeVolumes 2. DescribeImages 3. DescribeInstances 4. DescribeInstanceCreditSpecifications 5. DescribeInstanceAttribute 6. DescribeVolumes 7. DescribeTags 8. DescribeVpcs 9. DescribeInstanceTypes 10. Ausführungsinstanzen 11. GetCallerIdentity
	AWS EC2 Linux mit Sicherheitsgruppen stoppen	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2 Linux mit Sicherheitsgruppen starten	1. DescribeInstances 2. DescribeImages 3. Startinstanzen
	AWS EC2 Linux mit Sicherheitsgruppen – Stapeldebereitstellung: Beenden Sie alle Ressourcen	1. DescribeInstances 2. Beendigungsinstanzen 3. ModifyInstanceAttribute 4. GetCallerIdentity 5. DescribeInstanceCreditSpecifications 6. DescribeInstanceAttribute 7. DescribeVolumes 8. DescribeTags 9. DescribeInstanceTypes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		10. DescribeVpcs **11.** DescribeImages

Amazon Web Services EC2 Microsoft Windows – sofort einsatzbereite Katalogelemente

Cloud-Services-Katalog Windows-VM, bis zu 10 zusätzliche Datenträger auf EC2 oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Instanztyps von Amazon EC2 anzufordern. Diese obligatorischen Schritte sind für die Bereitstellung erforderlich:

1. In Terraform Fügen Sie die Pem-Datei des privaten Schlüssels hinzu, die für die Bereitstellung verwendet wird.
2. Kopieren Sie den Pfad der PEM-Datei aus Terraform Aktivieren und aktualisieren Sie diesen Pfad im Standardwert der Variablen „Verwaltungsschlüssel“.

Reihenfolge	Features
Bestellen Sie einen virtuellen Microsoft Windows-Computer auf EC2. Der Cloud-Konfigurationsscan wird zur Compliance-Prüfung ausgeführt.	Für andere Instanztypen als t2.nano und t2.micro ist eine Genehmigung durch den Administrator erforderlich, je nach Richtlinie. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM.
Bestellen Sie eine virtuelle Windows-Maschine auf EC2, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich, aber für alles darüber hinaus ist eine Genehmigung erforderlich.	Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, bitten Sie den Administrator nach Richtlinie um Genehmigung.
Bestellen Sie einen sicheren virtuellen Windows-Computer auf EC2, und weisen Sie Sicherheitsgruppen zu. Wählen Sie so viele aus, die für die höchste Sicherheitsstufe erforderlich sind.	Dieses Katalogelementformular ermöglicht die Zuweisung einer oder mehrerer Sicherheitsgruppen (Firewall-Port-Regeln) zur Recheninstanz, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Der Bereitstellungs-Workflow benachrichtigt die anfordernde Person per E-Mail über das Windows-Administratorpasswort. Es kann mindestens vier Minuten dauern, bis das Windows-Administratorpasswort von abgerufen wird Amazon Web Services.

Amazon Web Services EC2 Windows-Standardberechtigungen

Amazon Web Services Berechtigungen für EC2 Windows OOB-Katalogelemente

Katalogelement	Services	Berechtigungen
CSK AWS EC2 Microsoft Windows-VM	AWS EC2-Bereitstellung	1. PasswordData abrufen 2. DescribeInstanceCreditSpecifications 3. DescribeInstanceAttribute 4. DescribeInstances 5. DescribeTags 6. DescribeInstanceTypes 7. DescribeVolumes 8. DescribeVpcs 9. Ausführungsinstanzen 10. GetCallerIdentity 11. DescribeImages
	AWS EC2-Instanz: Stoppen	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2-Instanz – Start	1. DescribeImages 2. DescribeInstances 3. Startinstanzen
	AWS EC2-Instanz: Bereitstellung aufheben	1. DescribeInstances 2. GetCallerIdentity 3. ModifyInstanceAttribute 4. Beendigungsinstanzen 5. PasswordData abrufen 6. DescribeInstanceAttribute 7. DescribeInstanceCreditSpecifications

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		8. DescribeImages 9. DescribeTags 10. DescribeVolumes 11. DescribeInstanceTypes 12. DescribeVpcs
CSK CSC AWS EC2 Windows mit mehreren Datenträgern	AWS EC2 Windows-Bereitstellung mit mehreren Datenträgern	1. DescribeVolumes 2. DescribeVolumes 3. AttachVolume 4. DescribeInstances 5. PasswordData abrufen 6. Erstellen Sie ein Volume 7. DescribeInstanceAttribute 8. DescribeInstanceCreditSpecifications 9. DescribeTags 10. DescribeVpcs 11. DescribeInstanceTypes 12. Ausführungsinstanzen 13. DescribeImages 14. GetCallerIdentity
	Amazon Web Services EC2 Windows – mehrere Datenträger werden angehalten	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2 Windows – mehrere Datenträger werden gestartet	1. DescribeImages 2. DescribeInstances 3. Startinstanzen
	AWS EC2 Windows-Bereitstellung mehrerer Datenträger aufheben	1. DescribeInstances 2. Beendigungsinstanzen 3. ModifyInstanceAttribute 4. DescribeVolumes 5. Löschen Sie Volume 6. DetachVolume 7. GetCallerIdentity 8. DescribeVpcs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		9. DescribeInstanceAttribute 10. DescribeInstanceTypes 11. DescribeTags 12. DescribeInstanceCreditSpecifications 13. PasswordData abrufen 14. DescribeImages
CSK AWS EC2-Windows mit Sicherheitsgruppen	AWS EC2-Windows mit Sicherheitsgruppen – Bereitstellung	1. PasswordData abrufen 2. DescribeVolumes 3. DescribeInstanceAttribute 4. DescribeInstance 5. DescribeInstanceTypes 6. DescribeVpcs 7. DescribeTags 8. DescribeInstanceCreditSpecifications 9. Ausführungsinstanzen 10. GetCallerIdentity 11. DescribeImages
	AWS EC2-Windows mit Sicherheitsgruppen stoppen	1. DescribeInstances 2. Stoppinstanzen
	AWS EC2-Windows mit Sicherheitsgruppen starten	1. DescribeInstances 2. DescribeImages 3. Startinstanzen
	AWS EC2-Windows mit Sicherheitsgruppen-Deprovisionierung	1. DescribeInstances 2. TerminateInstances ModifyInstanceAttribute 3. GetCallerIdentity 4. DescribeInstanceAttribute 5. DescribeInstanceCreditSpecifications 6. DescribeVpcs 7. DescribeVolumes 8. DescribeTags 9. PasswordData abrufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		10. DescribeImages 11. DescribeInstanceTypes

Amazon Web Services Vordefinierte DynamoDB-Katalogelemente

Cloud-Services-Katalog AWS DynamoDB-Tabelle für hoch skalierbare NoSQL-Datenbank.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Dynamo DB-Tabelle zu bestellen – eine Name-Wert-Datenbanktabelle für Amazon Web Services Oder AWS Cloud. Die Standardeingaben, die bereitgestellt werden sollen, sind der Tabellenname und der Partitionsschlüssel sowie Sortierschlüsselnamen. Die Details der Dynamo-DB werden in den zurückgegebenen Stapeldetails angezeigt.

Bestellen Sie eine AWS DynamoDB-Tabelle, bei der es sich um einen Schlüssel-Wert-Speicher handelt, mit primären Schlüsseln und sekundären Indizes. Dies ist nützlich für Entwickler, die eine hoch skalierbare und vollständig verwaltete NoSQL-Datenbank benötigen.

Amazon Web Services Vordefinierte DynamoDB-Berechtigungen

Amazon Web Services Berechtigungen für DynamoDB-OOB-Katalogelemente. DynamoDB unterstützt nur die Bereitstellung und Aufhebung der Bereitstellung.

Katalogelement	Services	Berechtigungen
Cloud-Services-Katalog AWS DynamoDB	AWS DynamoDB-Bereitstellung	1. DescribeTimeToLive 2. DescribeTable 3. DescribeContinuousBackups 4. ListTagsOfRessource 5. UpdateTimeToLive 6. UpdateContinuousBackups 7. GetCallerIdentity 8. Tabelle erstellen 9. GetCallerIdentity
	AWS DynamoDB-Deprovisionierung	1. DescribeTable 2. DeleteTable 3. GetCallerIdentit 4. ListTagsOfRessource 5. DescribeContinuousBackups 6. DescribeTimeToLive 7. DescribeTable

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Web Services Sofort einsatzbereite S3-Bucket-Katalogelemente

Cloud-Services-Katalog AWS S3-Bucket mit sicherem Zugriff und Verschlüsselung.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um einen Objektspeicher-Bucket aus dem S3-Service von Amazon Cloud zu bestellen. Für den Bucket-Namen wird eine Validierung durchgeführt, um sicherzustellen, dass die s3-Benennungsrichtlinie eingehalten wird. Die zugrunde liegende Terraform-Vorlage wird verwendet, um den öffentlichen Zugriff auf den Bucket zu verhindern und die Standardverschlüsselung für Daten einzurichten.

Bestellen Sie einen AWS S3-Speicher-Bucket, der Sicherheitsmaßnahmen wie die Verhinderung des öffentlichen Zugriffs und die serverseitige Verschlüsselung enthält, die von Amazon S3 verwaltete Schlüssel (SSE-S3) verwendet. Diese Sicherheitsfunktionen stellen sicher, dass die im Bucket gespeicherten Daten geschützt und sicher sind.

Amazon Web Services Standardmäßige S3-Bucket-Berechtigungen

AWS Berechtigungen für S3-Bucket-OOB-Katalogelemente. S3-Bucket unterstützt nur die Bereitstellung und Aufhebung der Bereitstellung.

Katalogelement	Services	Berechtigungen
CSK AWS S3-Bucket	AWS S3-Bucket-Bereitstellung	**1.** GetBucketPolicy **2.** PutBucketPublicAccessBlock **3.** GetBucketLifecycle **4.** GetBucketReplication **5.** GetBucketTagging **6.** Bucket erstellen **7.** GetBucketLogging **8.** GetBucketPublicAccessBlock **9.** GetBucketRequestPayment **10.** GetBucketAcl **11.** GetBucketWebsite **12.** GetAccelerateConfiguration **13.** GetBucketVersioning **14.** GetBucketEncryption **15.** GetBucketCors **16.** GetBucketObjectLockConfiguration **17.** PutBucketEncryption **18.** GetCallerIdentity
	AWS S3-Bucket-Aufhebung	**1.** Löschen Sie BucketEncryption **2.** DeleteBucketPublicAccessBlock **3.** DeleteBucket

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Katalogelement	Services	Berechtigungen
		4. GetBucketObjectLockConfiguration **5.** GetBucketLifecycle **6.** GetBucketEncryption **7.** GetBucketReplication DescribeTable

Google Cloud Platform (GCP) Große Abfrage

Cloud-Services-Katalog Mit Google Cloud Platform BigQuery serverloses Data Warehouse.

BigQuery Serverless Data Warehouse ist ein voll funktionsfähiges Beispielkatalogelement, das den Prozess der Bestellung einer Data Warehouse-Lösung optimiert, die auf BigQuery vom Google Cloud Provider basiert.

Reihenfolge	Features
Bestellen Sie ein serverloses, kosteneffektives Multi-Cloud-Data Warehouse mit BigQuery für das Echtzeit-Streaming von Daten mit integriertem maschinellen Lernen, und geben Sie Analytics mit nur wenigen Klicks frei.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das den Prozess der Bestellung einer serverlosen, kosteneffektiven Multi-Cloud-Data Warehouse-Lösung optimiert, die auf BigQuery rom des Google Cloud-Anbieters basiert. Mit wenigen Klicks können Sie Daten-Streaming und Analytics-Freigabe in Echtzeit einrichten. Die serverlose Architektur von BigQuery ermöglicht eine SQL-basierte Datenanalyse und bietet Anpassungsoptionen für Skalierbarkeit.

Google Cloud Platform (GCP) Große sofort einsatzbereite Berechtigungen für Abfrage

Berechtigungen für Standardkatalogelemente für große GCP-Abfrage

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP BigQuery	Bereitstellung	• bigquery.Datasets.create • bigquery.Tabellen.erstellen • Speicher.Objekte.Abrufen
	Point-Discovery	• bigquery.Tabellen.Liste • bigquery.Datasets.Get
	Aufheben der Bereitstellung	• bigquery.tables.delete • bigquery.datasets.delete

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• bigquery.routines.delete • bigquery.models.delete

Google Cloud Platform Cloud SQL

Cloud-Services-Katalog Mit GCP Cloud SQL Database.

Die Cloud SQL-Datenbank ist ein Beispielkatalogelement, mit dem Sie eine Cloud SQL-Datenbanklösung bestellen können.

Reihenfolge	Features
Bestellen Sie eine Cloud SQL-Datenbanklösung, die in Google Cloud-Services integriert wird.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Cloud SQL-Datenbanklösung zu bestellen, die in Google Cloud-Services integriert ist, um innerhalb von Minuten Ihre erste skalierbare Datenbank zu erstellen und eine Verbindung mit ihr herzustellen. Nach Abschluss werden umfassende Details zur Cloud SQL-Konfiguration in den Stapeldetails bereitgestellt. Es automatisiert wichtige Funktionen wie Sicherungen, Replikation, Patching, Verschlüsselung und Anpassung der Speicherkapazität, um sicherzustellen, dass Anwendungen von verbesserten Zuverlässigkeits-, Skalierbarkeits- und Sicherheitsmaßnahmen profitieren.

Google Cloud Platform Cloud-SQL-Out-of-Box-Berechtigungen

Google Cloud Platform Cloud SQL Out-of-Box-Katalogelementberechtigungen

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Cloud-SQL	Bereitstellung	• cloudsql.instances.create • cloudsql.instances.get • cloudsql.users.delete
	Point-Discovery	• cloudsql.databases.list • cloudsql.instances.list

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• cloudsql.users.list • compute.regions.list • Compute.Zones.list
	Aufheben der Bereitstellung	cloudsql.instances.delete

Google Cloud Platform Sofort einsatzbereite Linux-Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzlichen Datenträgern oder sicherer Linux-Bereitstellung.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Linux-Instanz eines beliebigen Instanztyps von Google Cloud Platform anzufordern.

Linux-VM-Aufträge und -Funktionen:

Reihenfolge	Features
CSK GCP Linux-VM: Bestellen Sie eine virtuelle Linux-Maschine, die die Installation von Agent Client Collector ermöglicht. ACC ist für Produktionsinstanzen obligatorisch. Andere VM-Größen als e2-Micro und e2-small erfordern eine Genehmigung.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Linux-Instanz eines beliebigen Instanztyps von Google Cloud Provider anzufordern. Für andere Instanztypen als e2-micro und e2-small ist eine Genehmigung durch den Administrator nach Richtlinie erforderlich. Das Katalogelement verfügt über integrierte Clientregeln zum Vorantreiben einer ACC-Installation (Agent Client Collector), wenn die Bereitstellungsumgebung für die Produktion markiert ist. Um den Anmeldeinformationsaliasschlüssel für die ACC-Bereitstellung aus MID auszuwählen, müssen dem Anwender die entsprechenden ACC-Administratorrollenberechtigungen bereitgestellt werden.
CSK GCP Linux mehrere Datenträger: Bestellen Sie eine virtuelle Linux-Maschine, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich, aber für alles darüber hinaus ist eine Genehmigung erforderlich.	Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, bitten Sie den Administrator nach Richtlinie um Genehmigung.
CSK GCP Linux Cloud Firewall: Bestellen Sie eine sichere virtuelle Linux-Maschine mit verbesserter	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Linux-Instanz eines beliebigen Instanztyps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
Sicherheit, um Datenverkehr zu und von Ihren VM-Instanzen basierend auf Ihrer angegebenen Konfiguration zu ermöglichen oder zu verweigern, um die höchste Sicherheitsstufe zu gewährleisten.	von Google Cloud Provider anzufordern. Dieses Katalogelementformular ermöglicht die Zuweisung einer oder mehrerer Sicherheitsgruppen (Firewall-Port-Regeln) zur Recheninstanz, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Google Cloud Platform Standardmäßige Linux-Berechtigungen

Google Cloud Platform Berechtigungen für vordefinierte Linux-Katalogelemente

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Linux-VM	Bereitstellung	• Berechnen.Datenträger.Erstellen • compute.disks.get • compute.instances.create • compute.instances.get • compute.instances.setMetadata • compute.networks.get • Compute.Subnetzwerke.Get • compute.subnetworks.use • compute.subnetworks.useExternalIp • Berechnen.Zonen.Abrufen
	Point-Discovery	• compute.disks.list • Berechnen.Bilder.Liste • compute.instanceTemplates.list • compute.instances.list • Compute.machineTypes.list • Berechnen.Snapshots.Liste • Compute.Zones.list • compute.regions.list

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Tag 2 VM: Virtueller Server – Stoppknoten	• compute.instances.stop • Berechnen.Regionen.Abrufen • Compute.machineTypes.Get
	Virtueller Server: StartNode	compute.instances.start
	Virtueller Server – Größe Ändern	• compute.instances.stop • Compute.machineTypes.Get • Berechnen.Regionen.Abrufen • compute.instances.setMachineType • compute.instances.start
	Virtueller Server: Deprovison	• compute.instances.delete • Berechnen.Regionen.Abrufen
	Stapelbereitstellung Aufheben	• compute.instances.delete • compute.disks.delete **Hinweis:** Datenträgerberechtigungen für Tag 2 sind ebenfalls erforderlich. Diese sind identisch mit mehreren Linux-Datenträgern.
CSK GCP Linux – Mehrere Datenträger	Bereitstellung	• Berechnen.Datenträger.Erstellen • compute.disks.get • compute.disks.use • compute.instances.create • compute.instances.get • compute.instances.setMetadata • compute.networks.get • Compute.Subnetzwerke.Get • compute.subnetworks.use • compute.subnetworks.useExternalIp • Berechnen.Zonen.Abrufen • Compute.zoneVorgänge.Abrufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Point-Discovery	• compute.disks.list • Berechnen.Bilder.Liste • compute.instanceTemplates.list • compute.instances.list • Compute.machineTypes.list • Berechnen.Snapshots.Liste • Compute.Zones.list • compute.regions.list
	Tag 2 Datenträgerspeicher: Trennen	compute.instances.detachDisk
	Speicherbereitstellung Aufheben	compute.disks.delete
	Speicher – Datenträger anhängen	compute.instances.attachDisk
	Stapelbereitstellung Aufheben	• compute.instances.delete • compute.disks.delete **Hinweis:** VM-Berechtigungen für Tag 2 sind ebenfalls erforderlich. Diese sind identisch mit einer standardmäßigen Linux-VM.
CSK GCP Sichere Linux-Bereitstellung	Bereitstellung	• Berechnen.Datenträger.Erstellen • compute.disks.get • compute.instances.create • compute.instances.get • compute.instances.setMetadata • compute.instances.setTags • Berechnen.Firewalls.Erstellen • Berechnen.Firewalls.Abrufen • compute.networks.get • compute.networks.updatePolicy • Compute.Subnetzwerke.Get • compute.subnetworks.use

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• compute.subnetworks.useExternalIp • Berechnen.Zonen.Abrufen
	Point-Discovery	• compute.disks.list • Berechnen.Bilder.Liste • compute.instanceTemplates.list • compute.instances.list • Compute.machineTypes.list • Berechnen.Snapshots.Liste • Compute.Zones.list • compute.regions.list • compute.networks.list • Compute.Firewalls.list
	Stapelbereitstellung Aufheben	• compute.firewalls.delete • compute.networks.updatePolicy • compute.instances.delete • compute.disks.delete **Hinweis:** VM-Datenträgerberechtigungen für Tag 2 sind ebenfalls erforderlich.

Google Cloud Platform Lastenausgleichsmodul

Cloud-Services-Katalog Mit Google Cloud Platform HTTP Load Balancer für hohe Verfügbarkeit.

Dies ist ein Beispielkatalogelement, das entwickelt wurde, um den Prozess der Bereitstellung eines HTTP-Lastenausgleichsmoduls vom Google Cloud Provider zu optimieren. Ihr primäres Ziel besteht darin, Leistungsprobleme zu mindern und die Anwender-Experience zu verbessern, indem eingehender Datenverkehr effizient verwaltet wird.

Reihenfolge	Features
Bestellen Sie ein HTTP-Lastenausgleichsmodul, um den Anwenderdatenverkehr auf mehrere Instanzen der Anwendungen zu verteilen und so das Risiko von Leistungsproblemen zu verringern.	Dieses voll funktionsfähige Katalogelement erstellt einen klassischen Anwendungslastenausgleichsmodul – Global. Nur externe Lastenausgleichsmodule sind als globale Lastenausgleichsmodule verfügbar. Wählen Sie einen globalen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
	Lastenausgleichsmodul aus, wenn der Lastenausgleichsmodul global verteilt werden soll. Jeder globale Lastenausgleichsmodul ist auf alle Regionen verteilt. Sie ist von zonalen und regionalen Ausfällen nicht betroffen.

Google Cloud Platform Standardberechtigungen für Lastenausgleichsmodul

Google Cloud Platform Vordefinierte Berechtigungen für HTTP-Lastenausgleichsmodul

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP HTTP-Lastenausgleichsmodul	Bereitstellung	• Berechnen.BackendServices.Erstellen • Compute.BackendServices.Get • compute.backendServices.use • Compute.globalAddresses.create • Compute.globalAddresses.Get • compute.globalAddresses.use • Compute.globalForwardingRules.create • Compute.globalForwardingRules.Get • Berechnen.Integritätsprüfungen.Erstellen • Berechnen.Integritätsprüfungen.Abrufen • compute.healthChecks.useReadOnly • compute.instanceGroups.create • compute.instanceGroups.get • compute.instanceGroups.update • compute.instanceGroups.use • compute.instances.use • Compute.targetHttpProxys.create • Compute.targetHttpProxys.GET • compute.targetHttpProxies.use • Berechnen.urlZuordnungen.Erstellen • Berechnen.urlZuordnungen.Abrufen • compute.urlMaps.use • compute.networks.get
	Point-Discovery	• Compute.BackendServices.list • Compute.ForwardingRules.list

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• Berechnen.Integritätsprüfungen.Liste • Compute.httpHealthChecks.list • Compute.httpsHealthChecks.list • compute.instanceGroupManagers.list • compute.instanceGroups.list • compute.instances.list • Compute.targetHttpProxys.list • Compute.targetHttpsProxys.list • Compute.targetSslProxys.list • Compute.targetTcpProxys.list • Berechnen.urlZuordnungen.Liste • compute.regions.list • Compute.Zones.list
	LB: Aufhebung der Bereitstellung	• compute.globalForwardingRules.delete • compute.targetHttpProxies.delete • compute.urlMaps.delete
	Stapel: Bereitstellung Aufheben	• compute.globalAddresses.delete • compute.backendServices.delete • compute.healthChecks.delete • compute.instanceGroups.delete • compute.globalForwardingRules.delete • compute.targetHttpProxies.delete • compute.urlMaps.delete

Google Cloud Platform Sofort einsatzbereite Windows-Katalogelemente

Cloud-Services-Katalog Windows VM, bis zu 10 zusätzliche Datenträger auf Google Cloud Platform Oder mit Cloud-Firewall.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Typs von anzufordern Google Cloud Platform.

Linux-VM-Aufträge und -Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
CSK GCP Windows VM: Bestellen Sie eine virtuelle Windows-Maschine, die die Installation von Agent Client Collector ermöglicht. Andere VM-Größen als e2-Micro und e2-small erfordern eine Genehmigung.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Instanztyps von Google Cloud Provider anzufordern. Für andere Instanztypen als e2-micro und e2-small ist eine Genehmigung durch den Administrator nach Richtlinie erforderlich. Die Windows-Anmeldeinformationen werden vom Anwender im Katalogbestellformular bereitgestellt. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version. Die Workflow-Automatisierung führt einen CCG-Scan auf der bereitgestellten Windows-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel mit dem Status „Nachverfolgung erforderlich“ festgelegt, um zu benachrichtigen, dass die Stapelbereitstellung nicht den Normen entspricht.
CSK GCP Mehrere Windows-Datenträger: Bestellen Sie eine virtuelle Windows-Maschine, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich, aber für alles darüber hinaus ist eine Genehmigung erforderlich.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Instanztyps von Google Cloud Provider anzufordern. Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Die Windows-Anmeldeinformationen werden vom Anwender im Katalogbestellformular bereitgestellt. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version.
CSK GCP Windows Cloud-Firewall: Bestellen Sie eine sichere virtuelle Windows-Maschine mit verbesserter Sicherheit, um Datenverkehr zu und von Ihren VM-Instanzen basierend auf Ihrer angegebenen Konfiguration zuzulassen oder zu verweigern, um die höchste Sicherheitsstufe zu gewährleisten.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Instanztyps von Google Cloud Provider anzufordern. Dieses Katalogelementformular ermöglicht die Zuweisung einer oder mehrerer Sicherheitsgruppen (Firewall-Port-Regeln) zur Recheninstanz, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
	Die Windows-Anmeldeinformationen werden vom Anwender im Katalogbestellformular bereitgestellt. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

CSK GCP Windows OOB-Berechtigungen

Google Cloud Platform Standardmäßige Windows-Berechtigungen

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Windows-VM	Bereitstellung	• Berechnen.Datenträger.Erstellen • compute.disks.get • compute.instances.create • compute.instances.get • compute.instances.setMetadata • compute.networks.get • Compute.Subnetzwerke.Get • compute.subnetworks.use • compute.subnetworks.useExternalIp • Berechnen.Zonen.Abrufen
	Point-Discovery	• compute.disks.list • Berechnen.Bilder.Liste • compute.instanceTemplates.list • compute.instances.list • Compute.machineTypes.list • Berechnen.Snapshots.Liste • Compute.Zones.list • compute.regions.list

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Tag 2 VM: Virtueller Server – Stoppknoten	• compute.instances.stop • Berechnen.Regionen.Abrufen • Compute.machineTypes.Get
	Virtueller Server: StartNode	compute.instances.start
	Virtueller Server – Größe Ändern	• compute.instances.stop • Compute.machineTypes.Get • Berechnen.Regionen.Abrufen • compute.instances.setMachineType • compute.instances.start
	Virtueller Server: Deprovison	• compute.instances.delete • Berechnen.Regionen.Abrufen
	Stapelbereitstellung Aufheben	• compute.instances.delete • compute.disks.delete **Hinweis:** Datenträgerberechtigungen für Tag 2 sind ebenfalls erforderlich. Diese sind identisch mit mehreren Windows-Datenträgern.
CSK GCP Windows Mehrere Datenträger	Bereitstellung	• Berechnen.Datenträger.Erstellen • compute.disks.get • compute.disks.use • compute.instances.create • compute.instances.get • compute.instances.setMetadata • compute.networks.get • Compute.Subnetzwerke.Get • compute.subnetworks.use • compute.subnetworks.useExternalIp • Berechnen.Zonen.Abrufen • Compute.zoneVorgänge.Abrufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Point-Discovery	• compute.disks.list • Berechnen.Bilder.Liste • compute.instanceTemplates.list • compute.instances.list • Compute.machineTypes.list • Berechnen.Snapshots.Liste • Compute.Zones.list • compute.regions.list
	Tag 2 Datenträgerspeicher: Trennen	compute.instances.detachDisk
	Speicherbereitstellung Aufheben	compute.disks.delete
	Speicher – Datenträger anhängen	compute.instances.attachDisk
	Stapelbereitstellung Aufheben	• compute.instances.delete • compute.disks.delete **Hinweis:** VM-Berechtigungen für Tag 2 sind ebenfalls erforderlich. Diese sind identisch mit der Standard-Windows-VM.
CSK GCP Sichere Windows-Bereitstellung	Stapelbereitstellung Aufheben	• compute.firewalls.delete • compute.networks.updatePolicy • compute.instances.delete • compute.disks.delete **Hinweis:** VM-Datenträgerberechtigungen für Tag 2 sind ebenfalls erforderlich.

Microsoft Azure Sofort einsatzbereite Linux-Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzlichen Datenträgern, Sicherheitsgruppen oder mit skalierbaren Webservern oder Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Linux-Instanz eines beliebigen Instanztyps von anzufordern Microsoft Azure.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
Bestellen Sie einen virtuellen Linux-Computer auf Microsoft Azure, Der die Installation von Agent Client Collector ermöglicht. ACC ist für Produktionsinstanzen obligatorisch. Andere VM-Größen als Standard_A1_v2 und Standard_A2_v2 erfordern eine Genehmigung. Der Cloud-Konfigurationsscan wird zur Compliance-Prüfung ausgeführt.	Für andere Instanztypen als Standard_A1_v2 und Standard_A2_v2 ist eine Genehmigung durch den Administrator nach Richtlinie erforderlich. Das Katalogelement verfügt über integrierte Clientregeln, um eine ACC-Installation (Agent Client Collector) zu steuern, wenn die Bereitstellungsumgebung für die Produktion markiert ist. Um den Anmeldeinformationsalias-Schlüssel für die ACC-Bereitstellung aus MID auszuwählen, müssen dem Anwender die entsprechenden ACC-Administratorrollenberechtigungen gewährt werden. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel mit dem Status „Nachverfolgung erforderlich“ festgelegt, um zu benachrichtigen, dass die Stapelbereitstellung nicht den Normen entspricht.
Bestellen Sie einen virtuellen Linux-Computer, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich. Holen Sie für alles darüber hinaus eine Genehmigung ein.	Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, bitten Sie den Administrator nach Richtlinie um Genehmigung.
Bestellen Sie einen sicheren virtuellen Linux-Computer, und weisen Sie Sicherheitsgruppen zu. Wählen Sie so viele aus, wie Sie benötigen, um die höchste Sicherheitsstufe zu erhalten.	Dieses Katalogelementformular ermöglicht die Zuweisung einer oder mehrerer Sicherheitsgruppen (Firewall-Port-Regeln) zur Recheninstanz, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.
Bestellen Sie einen Skalierungssatz für virtuelle Linux-Maschinen, um identische virtuelle Computer bereitzustellen, die eine automatisierte Skalierung ermöglichen und eine hohe Verfügbarkeit gewährleisten.	Dieses Katalogelement bietet die Möglichkeit, identische virtuelle Computer mithilfe eines Skalierungssatzes für virtuelle Linux-Maschinen bereitzustellen, der automatisierte Skalierung für eine verbesserte Verfügbarkeit unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
	E-Mail-URL wird als Vorgang nach der Bereitstellung hinzugefügt, der die Endpunkt-URL der bereitgestellten Anwendung per E-Mail an die anfordernde Person sendet.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Microsoft Azure Sofort einsatzbereite Windows-Katalogelemente

Cloud-Services-Katalog Windows VM, bis zu 10 zusätzliche Datenträger auf Microsoft Azure Oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das verwendet werden kann, um eine Windows-Instanz eines beliebigen Instanztyps von anzufordern Microsoft Azure.

Reihenfolge	Features
Bestellen Sie eine Microsoft Windows-VM, die die Installation von Agent Client Collector ermöglicht. Andere VM-Größen als Standard_A1_v2 und Standard_A2_v2 erfordern eine Genehmigung. Der Cloud-Konfigurationsscan wird zur Compliance-Prüfung ausgeführt.	Für andere Instanztypen als „Standard_A1_v2“ und „Standard_A2_v2“ ist eine Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM.
Bestellen Sie einen virtuellen Windows-Computer auf Microsoft Azure Und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich, aber für alles darüber hinaus ist eine Genehmigung erforderlich.	Dieses Katalogelementformular ermöglicht die Bestellung von bis zu 10 zusätzlichen Datenträgern (Volumes), die an die VM mit unterschiedlichen Größen und Typen angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, bitten Sie den Administrator nach Richtlinie um Genehmigung. Das Windows-Administratorpasswort wird von abgerufen Microsoft Azure Zum Zeitpunkt der Erstellung.
Bestellen Sie einen sicheren virtuellen Windows-Computer auf Microsoft Azure, Weisen Sie Sicherheitsgruppen zu. Wählen	Dieses Katalogelementformular ermöglicht die Zuweisung einer oder mehrerer Sicherheitsgruppen (Firewall-Port-Regeln) zur Recheninstanz, sodass der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reihenfolge	Features
Sie so viele aus, die für die höchste Sicherheitsstufe erforderlich sind.	Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und Subnetze aufgelistet.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Key-value wird derzeit nur in der Tabelle „cmdb_key_value“ aktualisiert, nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Microsoft Azure Standardberechtigungen

Cloud-Services-Katalog Microsoft Azure Standardberechtigungen für Katalogelemente.

Services	Ressourcen
Microsoft.Compute	1. VirtualMachines/* 2. Datenträger/* 3. Verfügbarkeitssätze/* 4. Bilder/* 5. VirtualMachineScaleSets/* 6. Standorte/* 7. VmSize/* 8. Registrieren/Aktion/* 9. Registrierung aufheben/Aktion/* 10. KapaziteReservierungGruppen/* 11. CloudServices/* 12. DiskAccesses/privateEndpointConnectionsApproval/* 13. DiskEncryptionSets/* 14. Galerien/* 15. HostGroups/* 16. ProximityPlacementGroups/* 17. RestorePointCollections/* 18. SshPublicKeys/* 19. SharedVMExtensions/* 20. SharedVMImages/* 21. skus/Lese-Snapshots/*
Microsoft.Network	1. Registrieren/Aktion/* 2. Registrierung aufheben/Aktion/*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Services	Ressourcen
	3. CheckTrafficManagerNameAvailability/action/* 4. InternalNotify/action/* 5. GetDnsResourceReference/action/* 6. CheckFrontDoorNameAvailability/action/* 7. PrivateDnsZonesInternal/action/* 8. ApplicationGateways/* 9. ExpresRouteCircuits/* 10. LoadBalancers/* 11. NetworkInterfaces/* 12. Netzwerksicherheitsgruppen/* 13. PrivateDnsZones/* 14. PublicIPAddresses/* 15. Standorte/* 16. VirtualNetworks/* 17. Virtuelle Netzwerke/Subnetze 18. VirtualNetworks/virtualNetworkPeerings/* 19. NatGateways/* 20. Localnetworkgateways/* 21. Verbindungen/* 22. RouteTables/* 23. Subnetze/*
Microsoft.Storage	1. Registrieren/Aktion/* 2. Registrierung aufheben/Aktion/* 3. StorageAccounts/* 4. Blobs/*
Microsoft.Ressourcen	1. Tags/* 2. ResourceGroups/* 3. Abonnements/* 4. Ressourcen/* 5. Providerbereitstellungen/*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Services	Ressourcen
Microsoft.Sql	**1.** Server/* **2.** Server/Datenbanken/* **3.** Standorte/*/gelesen
Microsoft.ResourceHealth	Verfügbarkeitsstatus/*
Microsoft.ContainerService	**1.** VerwaltungCluster/* **2.** Flotten/*
Microsoft.Web	**1.** ServerFarms/* **2.** Sites/*
Microsoft.ResourceGraph	Ressourcen/*

Microsoft Azure Funktionen-App-Katalogelemente

Cloud-Services-Katalog Microsoft Azure Funktions-App mit Pay-as-you-go-Preisvorteil.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem Anwender eine Windows-Instanz eines beliebigen Instanztyps von anfordern können Microsoft Azure.

Reihenfolge	Features
Bestellen Sie eine Funktions-App, um kleine, ereignisgesteuerte Funktionen zu erstellen und bereitzustellen, ohne die Infrastruktur zu verwalten. Es bietet eine serverlose Computing-Experience mit Pay-as-you-go-Preisen.	Dieses Katalogelement stellt eine NodeJS-Basisanwendung „Hello World“ auf der bereitgestellten bereit Microsoft Azure Funktions-App. Die unterstützten Versionen von NodeJS sind mit den im Azure-Portal unterstützten Versionen identisch. Das Windows-Administratorpasswort wird von abgerufen Microsoft Azure Zum Zeitpunkt der Erstellung.

Hinweis:

Tag (Key-value) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Key-value wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der öffentlichen Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Sofort Einsatzbereite Aktionen

Die sofort einsatzbereiten Aktionen umfassen OOB-Bereitstellungs-, Tagging-, Abruf- und Nachbereitstellungsvorgänge. Alle diese Aktionen basieren auf Flow Designer und sind als Integration Hub-Subflows implementiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen	Flow Designer-Subflow-Name	Beschreibung
Stellen Sie ACC-* nach der Bereitstellung bereit	CSK Inhalt – nach der Bereitstellung – Bereitstellen von ACC in Stapel-VMs	ACC (Agent Client Collector) wird über eine Flow Designer-Aktion bereitgestellt. Dies wird als Schritt nach der Bereitstellung für das Katalogelement der Linux-Basis-VM-Bereitstellung bezeichnet. Voraussetzungen: **1.** ACC-Listener muss in jedem konfiguriert sein MID-Server. Dadurch werden ein MID-Webserver-Endpunkt und ein generiert MID-Server API-Schlüssel. **2.** In den Vorgangsparametern nach der Bereitstellung des Standardkatalogs für Linux-VM werden diese beiden Parameter verwendet: Webserverendpunkt (normalerweise im Format wss://<IP_Address>:3389/WS/Events) und MID-Server API-Schlüssel, müssen festgelegt werden. Standardmäßig haben diese Parameter leere Werte. **Hinweis:** Wenn die generierte WS-Endpunkt-URL die private IP von zurückgibt MID-Server, Dann muss diese private IP durch öffentliche IP des ersetzt werden MID-Server VM für die internetbasierte Konnektivität. **3.** Es muss eine Konnektivität über den SSH-Port von vorhanden sein MID-Server An die bereitgestellte VM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen	Flow Designer-Subflow-Name	Beschreibung
		Bei einem Fehler beim Installieren des Service Desk-Mitarbeiters auf der bereitgestellten VM wird eine Aufgabe erstellt, und der Stapel wird auf den Status „Nachverfolgung erforderlich“ gesetzt und wird automatisch aktiv, sobald alle Folgeaufgaben geschlossen wurden.
CCG-Scan nach der Bereitstellung	CSK Inhalt: Erstellen Sie einen CCG-Richtlinienscan für Stapelelemente	CCG-Scan mit der standardmäßigen OOB-Richtliniensatz in CCG wird mit der einfachen Windows- und Linux-Bereitstellung aufgerufen. Wenn ein CCG-Scan aufgrund eines Verstoßes fehlschlägt, wird der Stapel auf den Status „Nachverfolgung erforderlich“ gesetzt. Der Betreiber muss sicherstellen, dass der Verstoß behoben wird, und die Verstoßaufgabe schließen. Sobald alle Folgeaufgaben geschlossen sind, wechselt der Stapel automatisch in den Status „aktiv“ und kann von der anfordernden Person verwendet werden.
Tagging-Aktion	CSK Inhalt – nach der Bereitstellung – Schlüsselwerte in CMDB aktualisieren	Für alle Katalogelemente wird eine Tagging-Aktion ausgeführt, die als Schritt nach der Bereitstellung ausgeführt wird. Diese Aktion aktualisiert nur die Schlüssel-Wert-Einträge in CMDB, nicht in der Cloud. Die aktualisierten Standard-Tags sind StackName, Anwendung, CostCenter und BusinessService. Felder mit leeren Werten werden nicht als Schlüssel-Wert-Datensätze gespeichert.
Rufen Sie Das Windows-Passwort Ab	CSK Inhalt – Nach Der Bereitstellung – Windows-Passwort Abrufen	Alle Windows-Kataloge verfügen über eine Aktion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen	Flow Designer-Subflow-Name	Beschreibung
		zum Abrufen des Passworts, die dem Administrator das Passwort der bereitgestellten Windows-VM per E-Mail an die anfordernde Person sendet. Das Passwort wird von AWS abgerufen, nachdem die Bereitstellung abgeschlossen ist. Verwenden Sie dazu eine SSH-Schlüsseldatei („PEM“), um das Passwort zu entschlüsseln. Führen Sie die folgenden erforderlichen Schritte aus, um diese Pem-Datei auf dem Terraform Linux-Server einzurichten: **1.** Stellen Sie sicher, dass die Anmeldeinformationen des privaten SSH-Schlüssels für die VM mit installierter Terraform-CLI dem Anmeldeinformationsalias mit dem Namen „TFO-Server-Anmeldeinformationsalias“ zugeordnet sind. Dieser Alias wurde bereits mit der Installation von erstellt CSK Inhaltspaket. Dieser Alias wird verwendet, um SSH in den Terraform-Server zu übertragen, um das Windows-Passwort aus der Ausgabevariable abzurufen. **2.** Stellen Sie sicher, dass im Bereitstellungsvariablensatz des Katalogs für die Variable mit dem Namen „Schlüsselpfad“ der Standardwert auf den Pfad des Verwaltungsschlüssels (des Schlüssels, der das Passwort entschlüsseln kann) auf der Terraform-VM festgelegt ist. **3.** Stellen Sie sicher, dass die anfordernde Person die E-Mail eingerichtet hat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen	Flow Designer-Subflow-Name	Beschreibung
		Hinweis: Für anwenderdefinierte Kataloge ist dieser Vorgang nur zur Verwendung mit Terraform OpenSource- Linux-basierten Katalogelementen verfügbar.
E-Mail-URL für Microsoft Azure Skalierbare Webserveranwendung	CSK Inhalt: E-Mail-URL für Microsoft Azure Skalierbare Webserveranwendung	Diese Aktion wird als Vorgang nach der Bereitstellung in „“ hinzugefügt. CSK Microsoft Azure Linux mit dem Katalogelement des skalierbaren Webservers, das die Endpunkt-URL der bereitgestellten Anwendung per E-Mail an die anfordernde Person sendet. Die URL wird von abgerufen Microsoft Azure Nachdem die Bereitstellung abgeschlossen ist. Stellen Sie sicher, dass die anfordernde Person die E-Mail eingerichtet hat.
Abrufen Microsoft Azure Host-Name der Funktions-App	CSC-Inhalt – nach der Bereitstellung – Abrufen Microsoft Azure Host-Name der Funktions-App	Diese Aktion wird als Vorgang nach der Bereitstellung in „“ hinzugefügt. CSK Microsoft Azure Funktions-App-Katalogelement, das den Hostnamen der bereitgestellten Funktions-App an die anfordernde Person abruft.

Sofort Einsatzbereite Richtlinien

Die Cloud-Services-Katalog Sofort einsatzbereite Richtlinien umfassen Richtlinien für Genehmigung, Benennung, Leasing und Quotenbereitstellung.

Bereitstellungsrichtl	Beschreibung
Freigabe	ServiceNow-Genehmigungsaktion, die bei bestimmten Anlässen über den Richtlinienauslöser aufgerufen wird. Beispiel: Wenn eine anfordernde Person eine VM vom Typ t2.micro und t2.nano bestellt oder mehr als zwei zusätzliche Datenträger für bestimmte Katalogelemente angefordert werden.
Benennungsrichtlinie	Ein guter Ansatz für Ressourcen, die als Teil einer einzelnen Anforderung bereitgestellt werden, besteht darin, die Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereitstellungsrichtl	Beschreibung
	mit einem allgemeinen Namen zu versehen, z. B. mit dem Namen des Stapels. Wenn der Stapelname der Standardkonvention entspricht, ist dies zur einfachen Identifizierung des Besitzers und für das Alter nützlich. Die sofort einsatzbereite Benennungsrichtlinie ist für alle Cloud-Katalogelemente aktiviert. Wenn die Richtlinie aktiv ist, wird ein Stapelname in einem bestimmten Benennungsformat für das Feld Stapelname im Formular vorgeschlagen. Das Benennungsformat verwendet eine Kombination aus Anfangsbuchstaben des Namens der anfordernden Person, gefolgt vom aktuellen Datum und der aktuellen Uhrzeit im Format mm TT hh mm. Beispiel: Wenn der Name der anfordernden Person John Smith ist und das Datum/die Uhrzeit am 15. Mai 10:30 Uhr ist, wird der Stapelname als „js05151030“ generiert.
Mietrichtlinie	Mietrichtlinie wird verwendet, um die Debereitstellung nicht verwendeter/unerwünschter Stapel auszulösen, um Kosten in der Cloud zu sparen. Die Leasingrichtlinie hebt die Bereitstellung aktiver Stapel nach Ablauf des Leasingzeitraums auf. Eine Woche zuvor werden Erinnerungen an Stapelbesitzer gesendet, in denen erwähnt wird, dass der Stapel abläuft.
Kontingentrichtlinie	Die Quotenrichtlinie wird verwendet, um zu entscheiden, ob eine Anforderung, die ausgeführt wird, sobald die Quote überschritten wurde, zur Genehmigung übergehen oder abgebrochen werden soll. Siehe Steuerungen für Ressourcenbestellungen für vorlagenbasierte Cloud-Katalogelemente

CSC-Referenzen

Referenzthemen enthalten zusätzliche Informationen zu den Listen und Formularen, die Sie zum Konfigurieren, Verwalten und Verwenden verwenden Cloud-Services-Katalog.

Domain Separation und Cloud-Services-Katalog

Die Domänentrennung wird in Cloud-Services-Katalog unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Empfehlungen für die Domänentrennung in Cloud-Services-Katalog

Empfehlungen zur Domänentrennung in Cloud-Services-Katalog:

CSK Geführtes Setup

CSK Das geführte Setup sollte nur vom Systemadministrator innerhalb der globalen Domäne ausgeführt werden. Es ist wichtig zu beachten, dass die lokale Domäne nicht die geeignete Umgebung für diese Aufgabe ist.

Terraform OpenSource in globaler Domäne

Alle Kataloge und Konfigurationsanbieter werden mit der Installation von in der globalen Domäne installiert Cloud-Services-Katalog Plugin. Daher funktionieren die sofort einsatzbereiten Kataloge auch nur, wenn Sie die Terraform OpenSource(TFO)-Konfiguration und -Anmeldeinformationen in der globalen Domäne und nicht in einer bestimmten Domäne erstellen. Dadurch können Managed Service Provider (MSP)-Anwender einen einzelnen TFO-Server für mehrere Domänen verwenden.

Service Provider-Anmeldeinformationen

Service Provider (AWS, Microsoft Azure Und Google Cloud Platform Anmeldeinformationen müssen domänenspezifisch sein. Jedoch Azure DevOps) Und Ansible Installierbare Konfigurationselemente müssen sich für die Bereitstellung in der globalen Domäne befinden.

MID-Server in globaler Domäne

Legen Sie den MID-Server in der globalen Domäne als TFO fest, und die zugehörige Konfigurationsverwaltung wird auch im globalen Kontext festgelegt. Dies ermöglicht eine genaue globale Discovery.

MSP-Anwender können globale MID-Server festlegen und auch domänenspezifische MID für verschiedene Service Provider für Tag 1 verwenden.

Nächste Schritte

Um weitere Informationen zur Funktionsweise der Domänentrennung in zu erhalten Cloud Provisioning and Governance, Besuch Domain Separation und Cloud Provisioning and Governance.

Zugehörige Informationen

Domänentrennung für Service Provider

Azure DevOps Berechtigungen

Azure DevOps Discovery- und Bereitstellungsberechtigungen.

Berechtigungstyp	Beschreibung	PAT-Zugriff
Cloud-Services-Katalog Azure DevOps Discovery	Erkennt Projekte und Pipelines in Azure DevOps Organisation und fügt hinzu CMDB.	# Build (Lesen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungstyp	Beschreibung	PAT-Zugriff
Cloud-Services-Katalog Azure DevOps Bereitstellung	Stellen Sie über bereit Azure DevOps Pipeline ausgelöst von Cloud-Services-Katalog DevOps-Integrationskatalog.	# Build (Lesen Und Ausführen)
Cloud-Services-Katalog Azure DevOps Tag: Berechtigung „Ressourcen abrufen“	Erkennen AWSÜber bereitgestellte Ressourcen Azure DevOps Pipeline.	Nicht zutreffend

Ansible Berechtigungen

Ansible Konfigurationsberechtigungen für Provider, Ansible-Katalog und Vorgänge.

Ansible Berechtigungen für Tag 0, Tag 1 und Tag 2

Berechtigungstyp	Beschreibung
Ansible Konfigurations-Provider Discovery An Tag 0	1. Konfigurieren Ansible Referenz-Link für Anmeldeinformationen: https://docs.ansible.com/ansible-tower/latest/html/userguide/credentials.html 2. Ansible Tower-Anwender werden erstellt: https://docs.ansible.com/ansible-tower/3.2.5/html/userguide/users.html 3. Rollen/Berechtigungen können gewährt werden Ansible tower-Anwender pro Projekt/Bestand/Auftragsvorlage/ Anmeldeinformationen nach Bedarf. Weitere Details: https://docs.ansible.com/ansible-tower/latest/html/userguide/users.html#users-permissions 4. CAPI verwendet einen Token-basierten Mechanismus für die Standardauthentifizierung, der verwendet Ansible Anmeldeinformationen des tower-Anwenders. OAuth-Token werden basierend auf Anmeldeinformationen für die Standardauthentifizierung generiert. 5. Projekte, die die GitHub-Anmeldeinformationen des Playbooks enthalten (hier sind .yml-Dateien vorhanden), werden manuell in konfiguriert Ansible. Weitere Informationen: https://docs.ansible.com/ansible-tower/latest/html/userguide/credentials.html#source-control 6. Verwendet Ansible Anmeldeinformationen für Discovery Von „Bestand“, „Projekte“, „installierbar“ – Auftragsvorlagen (Playbooks und ihre zusätzlichen Variablen werden abgerufen) mithilfe von CAPI.
Ansible Katalogbereitstellung/ -Aufhebung der Bereitstellung an Tag 1	Verwendet Ansible tower-Anwenderanmeldeinformationen und Service-Account-Anmeldeinformationen von Amazon Web Services/Azure, angegeben in Ansible Auftragsvorlage.
Ansible Tag: Ressourcen für Discovery abrufen	Verwendet `tag:GetResources`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansible Berechtigungen für Tag 0, Tag 1 und Tag 2 (Fortsetzung)

Berechtigungstyp	Beschreibung
	Berechtigung zum Erkennen AWSÜber bereitgestellte Ressourcen Ansible Pipeline.
Ansible Tag 2-Vorgänge	Verwendet Ansible tower-Anwenderanmeldeinformationen, Service-Account-Anmeldeinformationen von Amazon Web Services/Azure und privates SSH-Schlüsselpaar oder Windows-Anwendername/Passwort, um eine Verbindung mit der bestimmten bereitgestellten Cloud-Ressource herzustellen.

Phasen von Azure DevOps In Release-Lebenszyklusmanagement

Die Komponenten und Phasen von Azure DevOps Die Pipeline ist umfassend und in hohem Maße anpassbar. Mit können Sie mehrere Phasen, Aufgaben und Integrationen basierend auf Ihren spezifischen Anforderungen und Technologiestapel definieren Cloud-Services-Katalog.

Support für Tag 0	Tag 1-Support	Tag 2-Support
1. Scannen Sie die Projekte und Pipelines 2. Erfassen Sie Pipeline-Variablen aus Azure DevOps	1. Bestellung aus Servicekatalog 2. Referenz von erkannt Azure DevOps Projekte und Pipelines 3. Wählen Sie Eingaben aus, die für die Release-Bereitstellungs-Pipeline erforderlich sind 4. Katalog übermitteln	1. SRE-Vorgänge – Patching, Sicherung usw. für Produktionsressourcen 2. Tägliche Wartung – Neustart, Neustart, Aussetzen usw. 3. Tagging von Ressourcen, Ausführung von Härtung usw.
Speichern Sie in CMDB Als referenzierbare Objekte	1. Auf Genehmigung warten 2. Verfolgen Sie den Fortschritt 3. Aktualisieren CMDB Mit bereitgestellten Ressourcen	1. Stellen Sie Resilienz in der Produktion sicher. 2. Wechseln Sie zwischen blauer und grüner Umgebung

Problemumgehung für bekannte Probleme

Die Workaround-Schritte für einige der bekannten Probleme werden in der Knowledge Base kompiliert und beschrieben.

Workaround	Verknüpfung
Cloud-Services-Katalog: Bekannte Probleme und Problemumgehungen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1362282

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1362282

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertung der Cloud-Migration

Diese Anwendung wird nicht mehr bereitgestellt, erweitert oder unterstützt.

Weitere Informationen finden Sie im Artikel Deprecation Process [KB0867184] (Ausgliederungsprozess) in der Knowledge Base des Now Support.

Cloud Provisioning and Governance

Die ServiceNow® Cloud Provisioning and Governance (CPG) dient als einheitliche Schnittstelle für den Zugriff auf Cloud-Ressourcen, die Bereitstellung von Cloud-Angeboten für einen Katalog und die Überwachung der Ressourcennutzung. Diese Anwendung wird in die Anwendung Cloud-Services-Katalog umgewandelt, die eine verfeinerte und optimierte Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen bietet.

Cloud Provisioning and Governance Ist sowohl in private als auch öffentliche Cloud-Anbieter integriert, z. B. Amazon Web Services, Microsoft Azure, Google Cloud Platform und VMware.

Hinweis:

Migration von Workflow zu Subflows:

- Wenn die Standard-Workflows nicht angepasst sind, werden die Flows zu Subflows migriert.
- Wenn die Standard-Workflows angepasst werden, verwenden die Flows weiterhin den vorhandenen Workflow.

Die Cloud Provisioning and Governance-Anwendung ist mit der veralteten Cloud-Management v1-Anwendung nicht kompatibel und kann nicht gleichzeitig mit dieser verwendet werden. Die Anwendung Cloud Provisioning and Governance (früher Cloud-Management) ist ab dem Jakarta-Release kompatibel.

Workflow-Migration

Während sich die Automatisierungs-Experience weiterentwickelt, werden Legacy-Workflows ab nicht mehr unterstützt Zurich Release. Sie können vorhandene anwenderdefinierte Workflows und veraltete Basissystem-Workflows nur verwenden, wenn sie bereits vorhanden sind, aber die neuen Basissystem-Flows für alle zukünftigen Anforderungen verwenden. Weitere Informationen finden Sie in den folgenden Artikeln in der Now Support Knowledge Base :

- So aktualisieren Sie DAS PAD FÜR die Cloud-Bereitstellung-Serviceanfrage oder DAS PAD für die Anforderung von Cloud-Ressourcenvorgängen [KB2265927]
- So migrieren Sie den Cloud-Servicekatalog zur Verwendung des Flows, falls einer der sofort einsatzbereiten Workflows geändert wurde [KB2262737]

Alle standardmäßigen vordefinierten Workflows wurden mit neu gestaltet Flow Designer.

Richtlinienregelaktionen können jetzt verwenden Flow Designer Subflows anstelle von Legacy-Workflows. Wenn Sie die Standard-Workflows nicht angepasst haben, werden die Legacy-Workflows automatisch zu Subflows migriert. Wenn Sie die Standard-Workflows angepasst haben, werden sie nicht migriert, und ihre Anwendungsfälle funktionieren weiterhin mit den vorhandenen Workflows.

Die folgenden Workflows wurden zu migriert Flow Designer Flows oder Subflow:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Change-Anforderung für Cloud-Vorgang
- Cloud-Aufgabenverarbeitung
- Cloud-Genehmigungs-Workflow
- Nachverarbeitungs-Workflow
- Workflow vorverarbeiten
- Anforderung für Cloud-Ressourcenvorgang
- Blueprint-Anforderung

Die folgenden Workflows sind veraltet:

- Rufen Sie Cloud-Abrechnungsdaten ab
- Cloud-Abrechnungsmonat abrufen
- Workflow-Startprogramm für Cloud-Vorgangsschritt

Erkunden	Einrichten	Verwalten
• Zurich • Domain Separation und Cloud Provisioning and Governance	• Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance • Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance • Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance	Cloud Provisioning and Governance-Administrationsleitfaden
Verwenden	**Entwickeln**	**Problembehandlung und Hilfe**
• Cloud-Adminportal • Cloud-Benutzerportal	• Entwicklerschulungen • Entwicklerdokumentation	• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Fragen in der ITOM-Community stellen oder beantworten • Kontakt Kundenservice und Support

Guided Setup zur Implementierung von Cloud Provisioning and Governance verwenden

Das Guided Setup für Cloud Provisioning and Governance stellt eine Reihe von Aufgaben bereit, die Sie bei der Konfiguration von Cloud Provisioning and Governance für Ihre Instanz unterstützen. Zum Öffnen Cloud Provisioning and Governance Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Die Anwendung Cloud Provisioning and Governance anfordern

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt).

Vorbereitungen

Erforderliche Rolle: Administrator

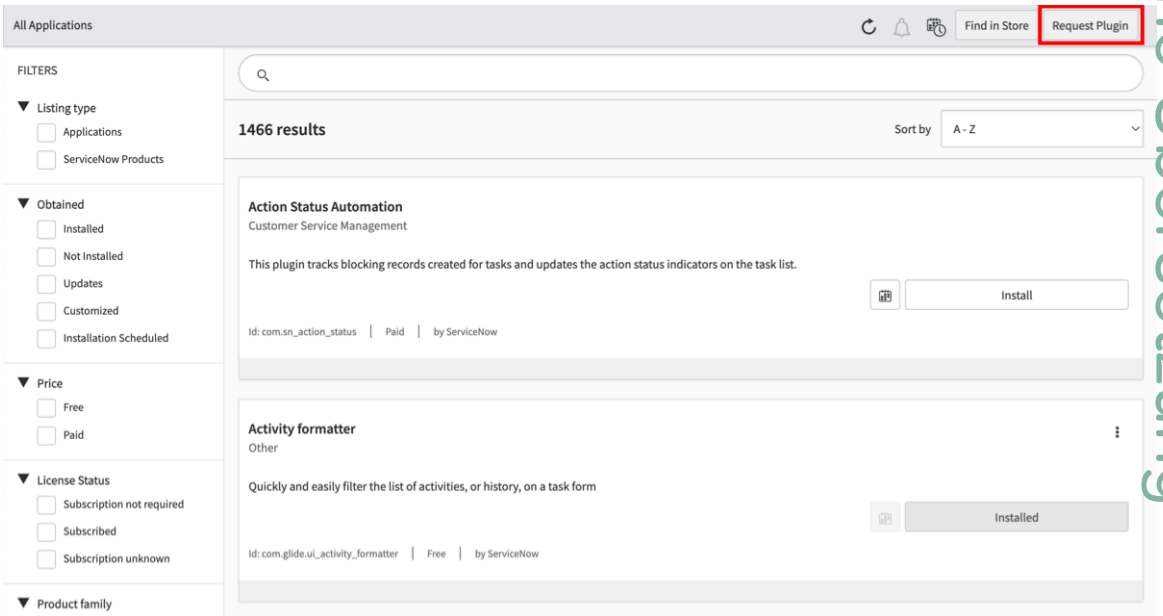
Warum und wann dieser Vorgang ausgeführt wird

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

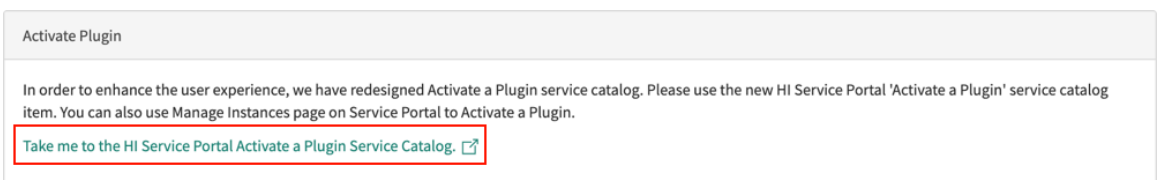
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

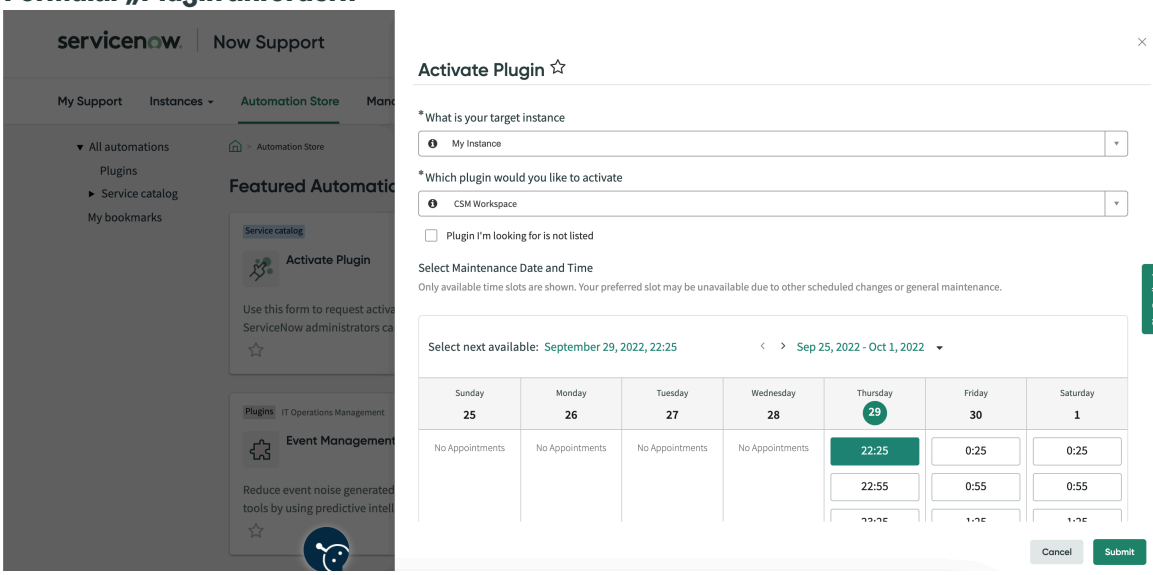
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Zugehörige Informationen

- Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance
- Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance
- Setup-Leitfaden für Tag 1 für Google Cloud Bis Cloud-Services-Katalog Terraform Connector
- Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

Produktnamensänderung

Beginnend mit Paris Release, die ServiceNow® Cloud-Management Anwendung wurde aufgerufen ServiceNow® Cloud Provisioning and Governance. Die Anwendung wird in umgewandelt Cloud-Services-Katalog Anwendung, die eine verbesserte und effiziente Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen bietet.

Das eigenständige Abonnement für Cloud Provisioning and Governance Wird eingestellt. Es wird neu strukturiert und in Cloud Accelerate integriert. Darüber hinaus wurde es in Cloud-Migrationsbewertung, Cloud-Account-Management, Cloud-Servicekatalog, Cloud-Konfiguration und -Governance und Cloud-Aktionsbibliothek segmentiert.

Obwohl Produktnamenreferenzen in der gesamten Produktdokumentation und der grafischen Benutzeroberfläche (GUI) aktualisiert werden, stoßen Sie möglicherweise je nach Kontext gelegentlich auf Verweise auf ihre alten Namen. Bei einigen Kernkomponenten bleibt der Produktname absichtlich unverändert, um die vorhandene Funktionalität beizubehalten.

Komponentennamensmatrix

Komponente	Vorheriger Name	Neuer Name
ITOM-Optimierung > Cloud Provisioning and Governance	Cloud-Management-Anwendung	Cloud Provisioning and Governance-Anwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponentennamensmatrix (Fortsetzung)

Komponente	Vorheriger Name	Neuer Name
com.snc.cloud.mgmt	Plugin Cloud-Management	Plugin Cloud Provisioning and Governance
com.snc.cloud.core	Cloud-Management Core-Plugin	Cloud Provisioning and Governance Core-Plugin
Anwendungskontext (**Einstellungen** > **Entwickler** > **Anwendung** > **Cloud Provisioning and Governance**)	Cloud-Management	Cloud Provisioning and Governance
com.sn_cmp_ibm	Cloud-Management: IBM Cloud Connector	Cloud Provisioning and Governance: IBM Cloud Connector
MID-Server-Fähigkeit > Cloud-Management	MID-Server-Fähigkeit > Cloud-Management	Cloud Provisioning and Governance
Unveränderte Komponentennamen		
MID-Server-Anwendung > Cloud-Management	MID-Server-Anwendung > Cloud-Management	Nicht geändert

Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie an Cloud Provisioning and Governance Anwendung

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Für Vorgänge in der AWS-Verwaltungskonsole ist die Administratorrolle erforderlich.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud Provisioning and Governance verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In AWS werden die bereichsspezifischen Container für virtuelle Ressourcen als *Regionen* bezeichnet. In Cloud Provisioning werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

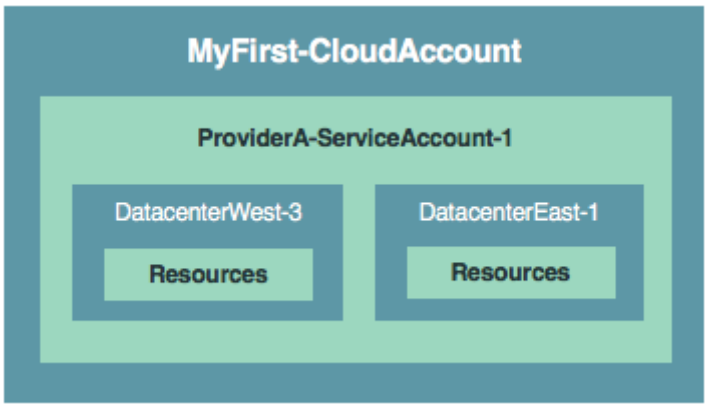
ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Schneller Überblick über den Setup-Prozess

Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration von Cloud Provisioning and Governance in Ihre AWS-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. **Weisen Sie Rollen zu zu zu AWSAnwender von Cloud Provisioning and Governance**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen

Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten. Sie können den MID-Server für Cloud Provisioning and Governance für die Verwendung eines Proxy-Servers konfigurieren. Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten wie Ausführen von Discovery, Abrechnungsdownloads, Bereitstellen virtueller Computer und Ausführen von Lebenszyklusvorgängen auf virtuellen Computern unterstützt.

Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

3. Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Damit die Anmeldeinformationen für Discovery und Cloud Provisioning and Governance verfügbar sind, müssen Sie in der AWS-Verwaltungskonsole zunächst einen Benutzer mit programmgesteuertem Zugriff erstellen. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in ServiceNow AI Platform.

4. Erstellen AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance

Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Eine AWS GovCloud (US)-Region ist eine isolierte AWS-Region, die die strengen Sicherheits- und Complianceanforderungen der US-Regierung zum Hosten sensibler Arbeitsauslastungen erfüllt. Cloud Provisioning and Governance bietet Unterstützung für alle AWS GovCloud (US)-Services.

5. Servicekonten für AWS GovCloud erstellen

Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

Wenn Ihre Organisation verwendet AWS GovCloud (US)Region, müssen Sie erstellen ServicekontoIn der Region, in der Sie die Ressourcen bereitstellen. Diese von Ihnen erstellten Anmeldeinformationen werden für Cloud-Discovery, Cloud Provisioning and Governance und Cloud-Einblicke verwendet.

6. Richten Sie ein Cloud-KontoUnd ServicekontoFür AWS

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. **Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren**

   Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Server s regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Weisen Sie Rollen zu zu AWSAnwender von Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Root-Administrator [sn_cmp.cmp_root_admin]	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator [sn_cmp.cloud_admin]	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle [sn_cmp.cloud_governor]	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation	Governance: • Richtlinien • Pools

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
	durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	• Kontingente • Berechtigungen
Service Designer [sn.cmp.cloud_service_designer]	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer [sn_cmp.cloud_service_user]	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Ihnen zugewiesenen Aufgabendatensätze zugreifen, wenn Sie die Rolle „Cloud-Service-Anwender“ innehaben.
Cloud-Betreiber [sn_cmp.cloud_operator]	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration [sn_cmp.cloud_event_integration] **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
		• AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator [sn_cmp.cloud_group_admin]	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Richten Sie ein Cloud-KontoUnd ServicekontoFür AWS

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

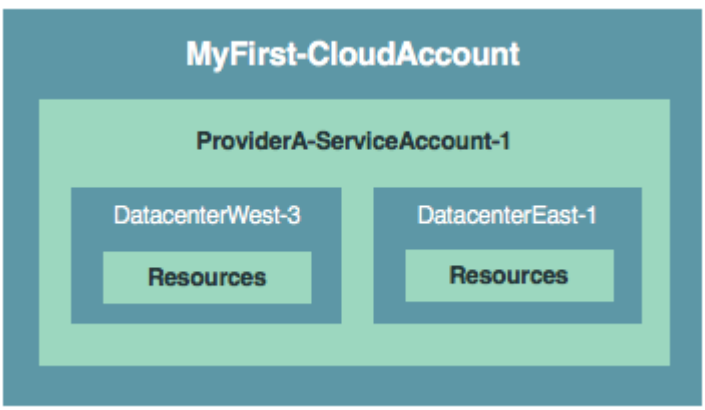
Erforderliche Rolle: keine

- Für Vorgänge in der AWS-Verwaltungskonsole ist die Administratorrolle erforderlich.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie das Setup für „Tag 1“ abgeschlossen haben, sieht Ihr Cloud-Konto möglicherweise so aus:

Struktur eines Cloud-Kontos an Tag 1

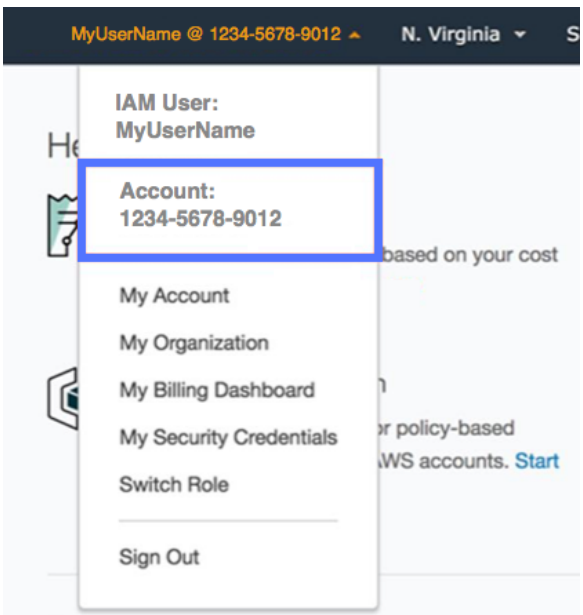


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.
2. Wählen Sie das Cloud-Konto aus, oder erstellen Sie es:
   - Wählen Sie ein vorhandenes Cloud-Konto aus:
     a. Klicken Sie auf der Seite des Cloud-Kontos auf **Konfigurieren**.
     b. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
   - Cloud-Konto erstellen:
     a. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Neu**, und geben Sie dann einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für das Cloud-Konto ein.
     b. Provider auswählen.
     c. Klicken Sie auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
3. Erstellen Sie auf der Seite „Rechenzentren“ ein Servicekonto: Klicken Sie neben dem Feld **Servicekonto** auf das **+**, und füllen Sie dann das Formular für Servicekonto aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer. **Nummer des IAM-Benutzerkontos** 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ○ Wenn Sie Konfigurierte AWS-Anmeldeinformationen unter ServiceNow AI Platform , Wählen Sie das Lupensymbol, und wählen Sie dann den Namen des entsprechenden aus AWS Anmeldeinformationen. ○ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für erforderlich AWS Region China und AWS GovCloud (USA)-Accounts. Zum Beispiel: ○ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ○ AWS GovCloud (USA): `https://ec2.us-gov-west-1.amazonaws.com`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie müssen die richtige Berechtigung in einrichten AWS Oder die Organisationsrolle für Standardanmeldeinformationen. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

4. Klicken Sie auf **Absenden**, um das Servicekonto zu erstellen.
5. Klicken Sie auf **Rechenzentren erkennen**
6. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

   Hinweis:
   - Wählen Sie nur die LDC/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
   - Um Ressourcen in Regionen/LDC zu erkennen, z. B. Nordamerika (US East, US West und Kanada Central), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik, stellen Sie mit eine Zugriffsanforderung für die erforderlichen Endpunkte GCP Support.

   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.
7. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:
   - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
   - **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
   - **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.

Nächste Maßnahme

- Konfigurieren Sie zusätzliche Berechtigungen zum Bereitstellen von Amazon AWS Cloud-Ressourcen mit Cloud Provisioning and Governance.
- Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Zusätzliches Cloud-Konto einrichten

Fügen Sie einen hinzu AWS ServicekontoZu Cloud-Konto

Benutzerdefinierte AWS-Mitgliedsrolle konfigurieren

Passen Sie die AWS-Rollen an, die ein MID Server annehmen kann, um temporäre Anmeldeinformationen für Mitgliedskonten zu erhalten. Sie können zusätzliche Parameter konfigurieren, um die Sicherheit zu verbessern und um anzupassen, wie die Rolle des Mitgliedskontos angenommen wird, wenn Cloud-Ressourcen erkannt werden.

Vorbereitungen

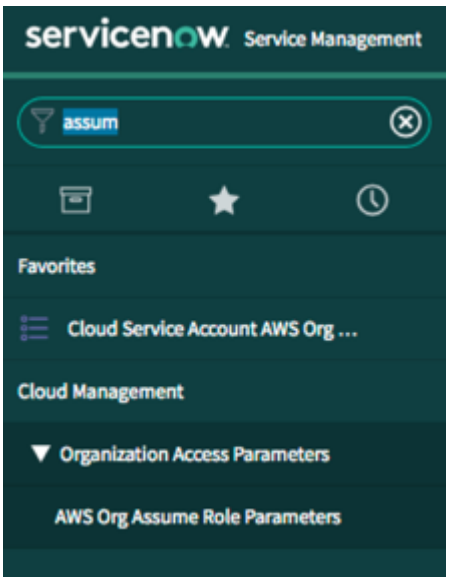
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Werte, die Sie in der Tabelle „Cloud-Servicekonto > AWS-Org. - Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] eingeben, werden als Parameter für das Konto des benannten Services an die AWS AssumeRole API weitergegeben.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS-Org. – Parameter für Rollenübernahme**an.



2. Klicken Sie auf **Neu**, und füllen Sie dann das Formular mit diesen Parametern aus:

Feld	Beschreibung
Zugriffsrollenname [access_role_name]	Name der AWS-Rolle im Mitgliedskonto, die vom Verwaltungskonto zum Abrufen temporärer Anmeldeinformationen verwendet wird. Standard: OrganizationAccountAccessRole
Rollensitzungsname [role_session_name]	Name für die Sitzung unter Verwendung der temporären Sicherheitsanmeldeinformationen, der dazu beitragen kann, die Verwendung einer Rolle nach einem Prinzipal oder Zweck zu unterscheiden. Dieser Sitzungsname ist in den AWS Cloud Trail-Protokollen sichtbar. Weitere

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Informationen finden Sie unter Cloud-API-Pfad und in der AWS-Dokumentation zu AWS Cloud Trail. Standard: Master_Account_ID_<Management Account ID number> ein Beispiel hierfür ist: Master_Account_ID__321003876149 .
Anmeldeinformations-TTL in Sekunden [credential_ttl_seconds]	Gültigkeitsdauer der temporären Sicherheitsanmeldeinformationen in Sekunden. Standard: Wird wie folgt berechnet: **a.** Rufen Sie den Wert in ab *mid.aws.sts.assume_role.credential_ttl_minutes* MID-Server-Eigenschaft . **b.** Beschränken Sie diesen Wert auf einen Wert zwischen 15 und 720 Minuten. Wenn die Einstellung in der Eigenschaft weniger als 15 Minuten beträgt, werden vom System 15 Minuten eingegeben. Wenn die Einstellung größer als 720 Minuten ist, werden vom System 720 Minuten eingegeben. **c.** Konvertieren Sie den resultierenden Wert in Sekunden.
Externe ID [external_id]	Ein eindeutiger Bezeichner, der für die Vertrauensrichtlinie der angenommenen Rolle erforderlich ist. Standard: ServiceNow_MID_Server
Sitzungsrichtlinie [session_policy]	IAM-Richtlinie im JSON-Format, die die Berechtigungen der temporären Sicherheitsanmeldeinformationen über die von der Rolle konfigurierte Richtlinie hinaus weiter einschränkt. (JSON in der AWS-Richtliniensprache.) Standard: leer
MFA [multifactor authentication]	Seriennummer des Multifaktor-Authentifizierungsgeräts (MFA) (Hardware oder virtuell), das zur Authentifizierung des Verwaltungs-Accounts verwendet wird. Standard: leer
MFA-Tokencode [mfa_token_code]	Vom MFA-Gerät (Hardware oder virtuell), das zur Authentifizierung des Verwaltungskontos verwendet wird, bereitgestellter Tokencode. Standard: leer
Cloud-Servicekonto [cloud_service_account]	Erforderlich. Servicekonto, der den Zugriffsparametern zugeordnet werden soll, die Sie an die AWS AssumeRole API übergeben. Geben Sie eine Konto-ID (entweder ein Verwaltungskonto oder ein Mitgliedskonto) aus der Tabelle „Servicekonten“ [cmdb_ci_cloud_service_account] ein.

Hinweis: Weitere Informationen zur Verwendung dieser Parameter und zu ihrer Bedeutung finden Sie in der AWS-Dokumentation zur AWS Security Token Service API für die Aktion „AssumeRole“.

Erstellen AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance

Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet. Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Eine AWS GovCloud (US)-Region ist eine isolierte AWS-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Region, die die strengen Sicherheits- und Complianceanforderungen der US-Regierung zum Hosten sensibler Arbeitsauslastungen erfüllt. Cloud Provisioning and Governance bietet Unterstützung für alle AWS GovCloud (US)-Services.

Vorbereitungen

Hinweis:

- ServiceNow® ITOM-Produkte werden für die Regionen Deutschland und China nicht offiziell zertifiziert oder unterstützt.
- Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

- Sie benötigen die AWS GovCloud (US)-Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel, den Sie auf der AWS-Verwaltungskonsole generiert haben.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud Provisioning and Governance Zugriffe GovCloudRegionen, die einen Satz von Anmeldeinformationen für jede Region verwenden. Zur Konfiguration von Cloud Provisioning and Governance zur Unterstützung einer GovCloud-Region erstellen Sie ein AWS-Standardkonto für jede Region (erforderlich für die Abrechnung), rufen die Anmeldeinformationen für das Konto ab und erstellen dann einen Servicekonto für die Region. Weitere Informationen zur Abrechnung finden Sie auf der Seite zur Abrechnung und Zahlung bei AWS GovCloud (US) in der AWS-Dokumentation .

Prozedur

1. Geben Sie in der AWS-Verwaltungskonsole im Suchfeld AWS-Services **IAM** ein, um den Identitäts- und Zugriffsverwaltungsservice (Identity and Access Management, IAM) zu öffnen.
2. Klicken Sie im IAM-Ressourcenportal auf **Benutzer**.
3. Erstellen Sie den Discovery-Benutzer, der über programmgesteuerten Zugriff auf Ihre AWS GovCloud (US)-Ressourcen und -Abrechnungsdaten verfügt.
4. Wählen Sie **Anwender hinzufügen** aus.
   Konfigurieren Sie auf der Seite „Details“ die Benutzereinstellungen, und klicken Sie dann auf **Weiter**.

Anwendername	Name für den Benutzer mit programmgesteuertem Zugriff, z. B. servicenowcloud.
Zugriffstyp	Wählen Sie **Programmatic access** (Programmgesteuerter Zugriff) aus.

5. Hängen Sie den Anwender auf der Seite Berechtigungen an eine Richtlinie an, indem Sie die folgenden Einstellungen konfigurieren, und klicken Sie dann auf **Als Nächstes** .

Berechtigungen für <Benutzername> festlegen	Wählen Sie **Attach existing policies directly** (Vorhandene Richtlinien direkt anhängen) aus.
Attach one or more policies … (Mindestens eine Richtlinie anhängen …)	Wählen Sie die entsprechende Richtlinie aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Richtlinie **AdministratorAccess** hat die umfassendste Berechtigungsstufe, einschließlich der Berechtigung zum Bereitstellen von Cloud-Ressourcen. Die Richtlinie ermöglicht den gleichen Zugriff, der der Instanz gewährt würde, wenn Sie nicht IAM, sondern die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres AWS-Kontos verwenden würden. Sie können stattdessen eine Richtlinie erstellen oder mehrere Richtlinien kombinieren, um die entsprechende Berechtigungsstufe zu gewähren. Weitere Detailinformationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.

6. Überprüfen Sie auf der Überprüfungsseite Ihre Auswahl, und klicken Sie dann auf **Create user** (Benutzer erstellen).
7. Führen Sie auf der Abschlussseite zwei Schritte aus:

   Hinweis: Verlassen Sie die Seite erst, wenn Sie beide Schritte abgeschlossen haben. Der Wert des **geheimen Zugriffsschlüssels** wird nicht erneut angezeigt. Fügen Sie die in diesen Schritten generierten Werte in ein Cloud Provisioning and Governance-Formular ein.

   a. Klicken Sie auf **Show** (Anzeigen), um den geheimen Zugriffsschlüssel anzuzeigen. Kopieren Sie den Wert.
   b. Klicken Sie auf **Download .csv** (.csv herunterladen), um die Datei, die den Benutzernamen, die Zugriffsschlüssel-ID und den Wert des geheimen Zugriffsschlüssels enthält, im CSV-Format zu speichern. Erstellen Sie die Datei als Sicherung für den Fall, dass Sie die Werte verlieren. Stellen Sie sicher, dass die Datei erstellt wurde, und speichern Sie sie dann sicher.
8. Navigieren Sie in Ihrer Instanz zu **Orchestration** > **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**an.
9. Klicken Sie auf **Neu**, wählen Sie **AWS-Anmeldeinformationen** aus, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein (z. B. AWS GovCloud Creds 01), und füllen Sie dann das Formular aus.

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

10. Klicken Sie auf **Absenden**.
    Die Instanz zeichnet die Anmeldeinformationen auf. Als Nächstes können Sie einen Servicekonten für AWS GovCloud erstellen.

Servicekonten für AWS GovCloud erstellen

Wenn Ihre Organisation verwendet AWS GovCloud (US)Region, müssen Sie erstellen ServicekontoIn der Region, in der Sie die Ressourcen bereitstellen. Diese von Ihnen erstellten Anmeldeinformationen werden für Cloud-Discovery, Cloud Provisioning and Governance und Cloud-Einblicke verwendet.

Vorbereitungen

Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

- Erforderliche Rolle: sn_cmp.cloud_admin
- AWS GovCloud (US)-Anmeldeinformationen für jede GovCloud-Region.
- AWS GovCloud (US)-Konto-ID (über die AWS-Verwaltungskonsole).

Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto enthält die Anmeldeinformationen und Kontoinformationen, die Sie in Ihrem Provider-Konto erstellt haben. Discovery verwendet die Informationen, um auf Ihren Provider-Konto zuzugreifen und dann Informationen zu jedem logischen Rechenzentrum abzurufen, das dem Konto zugeordnet ist.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal** > **Service-Konten**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen Namen für das Konto ein (z. B. AWS GovCloud SA O1), und füllen Sie dann das Formular „Cloud-Servicekonto“ aus.

Feld	Beschreibung
Konto-ID	Konto-ID, zu der die Anmeldeinformationen gehören.
Discovery-Anmeldeinformationen	Wählen Sie den Namen der Anmeldeinformationen aus, die Sie unter Erstellen AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance erstellt haben. Im Beispiel haben Sie den Namen AWS GovCloud Creds O1 verwendet.
Rechenzentrums-URL	URL des Rechenzentrums. Beispiel: https://ec2.us-gov-west-1.amazonaws.com
Rechenzentrumstyp	Wählen Sie die CMDB-Tabelle aus, die für den Typ des Rechenzentrums steht. Beispiel: Tabelle [cmdb_ci_aws_datacenter]
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Nächste Maßnahme

Wiederholen Sie den Vorgang, um nach Bedarf weitere Servicekonten zu erstellen. Führen Sie Discovery für jedes Rechenzentrum aus.

Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren

Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Server s regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Vorbereitungen

Wichtig:

Ab dem Vancouver-Release ist das Abrechnungs-Dashboard nicht mehr verfügbar, wenn Sie die ServiceNow Store Cloud Cost Management-App heruntergeladen und aktiviert haben. Die folgenden Änderungen treten auf:

- Sie werden standardmäßig zur Homepage des Cloud-Kostenmanagements weitergeleitet.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Das Widget „Ausgaben für aktuellen Monat“ und das Widget „Budget“ im Cloud-Anwenderportal zeigen keine Daten an, wenn Cloud-Kostenmanagement in der Instanz aktiviert ist.

Wenn Sie die Cloud-Kostenmanagement-App aktiviert haben, können Sie nur zum AbrechnungsDashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

- Richten Sie ein Bezahlkonto ein, der die Abrechnungsinformationen für alle verknüpften Konten empfängt.
- Erstellen Sie den Amazon S3-Bucket, der den Datenspeicherbereich für die täglichen detaillierten Abrechnungsdatensätze im AWS-Konto darstellt. Die Anmeldeinformationen, die für den Zugriff auf den Bericht verwendet werden, müssen über Berechtigungen für den S3-Bucket verfügen. Legen Sie den S3-Bucket basierend auf dem Auftragsstandort fest. Die AssumeRole-Richtlinien MÜSSEN eine S3-Zugriffsrichtlinie enthalten. Unter Umständen sind Sie der Meinung, dass von dem AWS-Konto, das Sie immer verwenden, ein S3-Bucket in der Region erstellt werden kann, in der die CloudFormation-Vorlage bereitgestellt wird. Wenn Sie STS-basierte Authentifizierung verwenden, kann der Bucket jedoch möglicherweise nicht vom AWS-Konto erstellt werden, da die Authentifizierung an die AssumeRole-Richtlinien gebunden ist. Weitere Informationen finden Sie in der AWS-Dokumentation auf der Seite zum Thema der Einrichtung des Amazon S3-Bucket für AWS-Kosten- und -Nutzungsberichte.
- Aktivieren Sie detaillierte Abrechnungsberichte in AWS. Weitere Informationen finden Sie in der AWS-Dokumentation .

  Hinweis: Die Funktion für detaillierte Abrechnungsberichte wird von Amazon AWS Cloud für neue Kunden zurückgezogen. Weitere Informationen und Migrationsdetails finden Sie in der AWS-Dokumentation zu detaillierten Abrechnungsberichten .

Erforderliche Rolle: sn_cmp.cloud_governor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren umfasst zwei Aufgaben:

1. Füllen Sie das Formular des AWS-Abrechnungszeitplans mit Informationen aus, die Sie aus dem AWS-Portal kopieren. Mit dieser Aktion können AWS-Abrechnungsdaten aus der Instanz heruntergeladen werden.
2. Geben Sie den Zeitplan zum Herunterladen von AWS-Rechnungsinformationen an.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Analysieren** > **Abrechnung**an.
2. Klicken Sie auf der Registerkarte **Abrechnungszeitpläne** auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** ein, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Anbieter	Wählen Sie **AWS** aus.
Servicekonto	Der AWS-Servicekonto, den Sie bei der Ersteinrichtung erstellt haben. (Das AWS-Konto, für das der Abrechnungsbericht ausgeführt werden soll.)
Bucket	Datenspeicherbereich für die täglichen Abrechnungsdatensätze im AWS-Konto. Führen Sie die folgenden Schritte aus, um den Wert zu erhalten: **a.** Melden Sie sich bei der AWS-Verwaltungskonsole an, und wählen Sie im Menü **My Billing Dashboard** (Mein Abrechnungsdashboard) aus. **b.** Wählen Sie im Dashboard **Billing Preferences** (Abrechnungseinstellungen) aus. **c.** Erweitern Sie im Abschnitt **Cost Management Preferences** (Kostenmanagementeinstellungen) die Option **Detailed Billing Reports [Legacy]** (Detaillierte Abrechnungsberichte [veraltet]) aus und stellen Sie sicher, dass das Kontrollkästchen **Turn on the legacy Detailed Billing Reports feature to receive ongoing reports of your AWS charges** (Alte Funktion „Detaillierte Abrechnungsberichte“ aktivieren, um fortlaufend Berichte Ihrer AWS-Gebühren zu erhalten) ausgewählt ist. **d.** Kopieren Sie den Wert aus dem Feld **Save the S3 bucket:** (S3-Bucket speichern:) in das Feld **Bucket** des Formulars. **Hinweis:** AWS wählt standardmäßig den S3-Bucket aus, der dem AWS-Konto zugeordnet ist, bei dem Sie derzeit angemeldet sind. Ein grünes Häkchen zeigt an, dass der Bucket ordnungsgemäß konfiguriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren Sie das Kontrollkästchen, um den Job zum Herunterladen zu aktivieren.
Ausführen	Frequenz, in der der Job zum Herunterladen ausgeführt werden soll.
Uhrzeit	Uhrzeit, zu der der Job zum Herunterladen ausgeführt werden soll.

3. Klicken Sie auf **Speichern**.
   Um den Job bei Bedarf auszuführen, klicken Sie auf **Jetzt ausführen**. Wählen Sie im Fenster **Abrechnungsdaten abrufen** einen Datumsbereich aus, und klicken Sie dann auf **Herunterladen**.

Nächste Maßnahme

Lassen Sie Cloud-Kosten auf dem Abrechnungsdashboard anzeigen.

Zugehörige Informationen

Cloud-Anmeldeinformationen

Downloadgröße von AWS-Abrechnungsdaten konfigurieren

Ein einzelner Satz Cloud Billing-Daten kann umfangreich sein. Vom MID-Server werden die Daten daher in verwaltbaren Blöcken an die ECC-Warteschlange gesendet. Optional können Sie eine Systemeigenschaft so konfigurieren, dass die Größe der einzelnen Blöcke begrenzt wird. So vermeiden Sie Leistungsprobleme, die durch die Übertragung großer Datenmengen verursacht werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“, indem Sie im Anwendungsfilter `sys_properties.list` eingeben.
2. Filtern Sie die Liste, um die Eigenschaft `sn_cmp.billing.page_size` zu öffnen.
   Der Standardwert ist 3 MB.
3. Modifizieren Sie den Wert nach Bedarf.
   Der Höchstwert beträgt 5 MB.
4. Speichern Sie die Eigenschaft.

Fügen Sie einen hinzu AWS ServicekontoZu Cloud-Konto

Im Rahmen des Tag-1-Setups von Cloud Provisioning and Governance haben Sie ein Servicekonto zum Cloud-Konto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

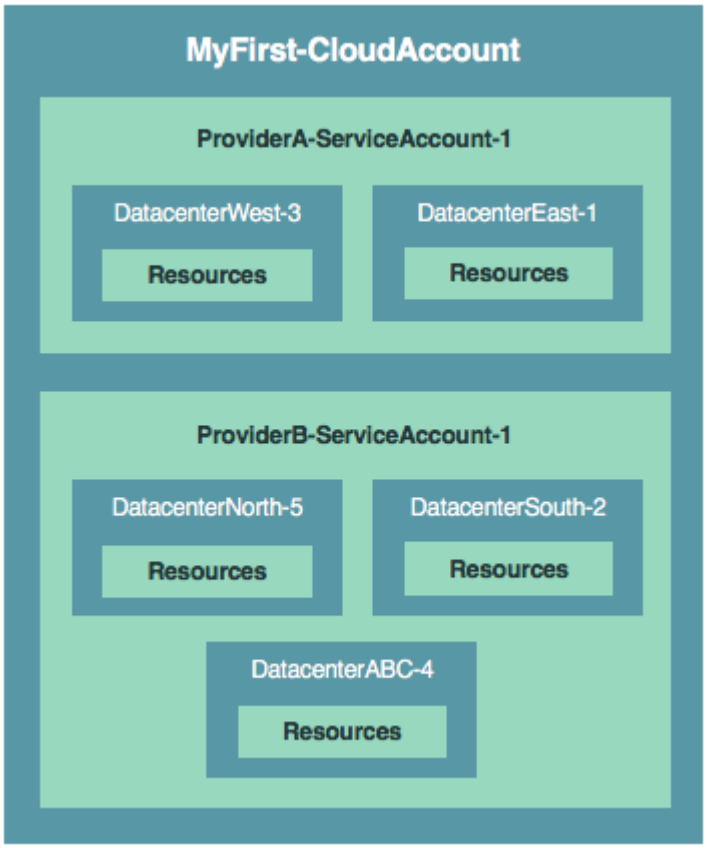
Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel haben Sie ein Servicekonto mit dem Namen **ProviderB-ServiceKonto-1** hinzugefügt und drei Rechenzentren zur Einbindung in das Cloud-Konto ausgewählt:

Servicekonto mit drei ausgewählten Rechenzentren



Wichtig: In einem Cloud-Konto können Sie kein bestimmtes Rechenzentrum in zwei verschiedenen Servicekonten auswählen.

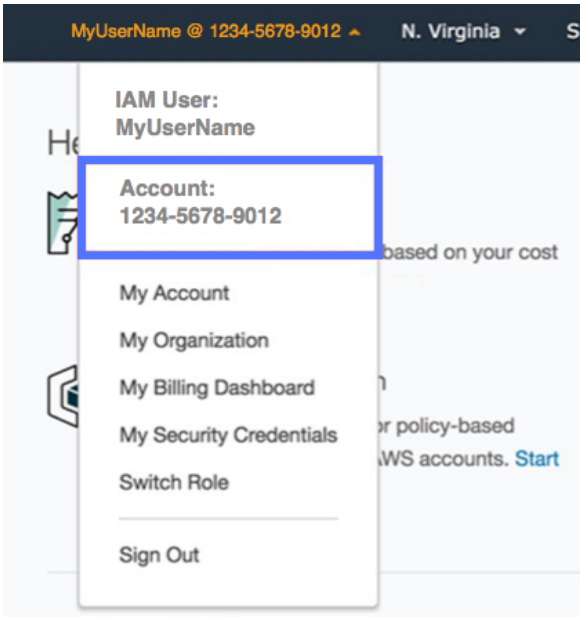
Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Service-Konten**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein, und füllen Sie dann das Formular aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nummer des IAM-Benutzerkontos 
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ○ Wenn Sie Konfigurierte AWS-Anmeldeinformationen unter ServiceNow AI Platform , Wählen Sie das Lupensymbol, und wählen Sie dann den Namen des entsprechenden aus AWS Anmeldeinformationen. ○ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für erforderlich AWS Region China und AWS GovCloud (USA)-Accounts. Zum Beispiel: ○ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ○ AWS GovCloud (USA): `https://ec2.us-gov-west-1.amazonaws.com`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen. **Hinweis:** Sie müssen die richtige Berechtigung in einrichten AWS Oder die Organisationsrolle für Standardanmeldeinformationen. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

3. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.
4. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie an Cloud Provisioning and Governance Anwendung

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Vorgänge im Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator
    und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud Provisioning and Governance verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In Azure werden die bereichsspezifischen Container für virtuelle Ressourcen als *Regionen* bezeichnet. In Cloud Provisioning and Governance werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

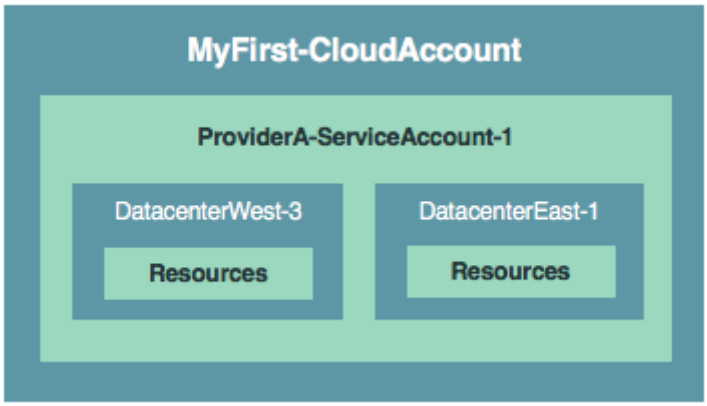
Schneller Überblick über den Setup-Prozess

Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration von Cloud Provisioning and Governance in Ihre Microsoft Azure-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. **Weisen Sie Rollen zu zu AzureAnwender von Cloud Provisioning and Governance**

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. **Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen**

   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten.

   Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

3. **Microsoft Azure-Dienstprinzipal erstellen**

   Für den sicheren Zugriff auf Ressourcen und Abrechnungsdaten in Ihrem Microsoft Azure-Konto muss der Discovery-Prozess entsprechende Anmeldeinformationen für das Microsoft Azure-Konto bereitstellen. Sie erstellen ein spezielles programmgesteuertes Konto – einen Microsoft Azure-Dienstprinzipal –, um die erforderlichen Anmeldeinformationen zu generieren.

4. **Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern**

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst die Anmeldeinformationen des Azure-Dienstprinzipals in der Azure-Portal. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

5. **Fügen Sie einen hinzu Azure Servicekonto**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

6. **Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen**

   Discovery nutzt die Informationen im Servicekonto dazu, alle dem Anbieter-Account zugeordneten logischen Rechenzentren zu identifizieren.

7. **Richten Sie ein Cloud-KontoFür Azure**

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

8. **Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen**

   Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

10. **Erstellen Microsoft Azure Anmeldeinformationen für Abrechnungsdownload**

    Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Server s regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Microsoft Azure Government Cloud auf Cloud Provisioning and Governance einrichten

Richten Sie Microsoft Azure Government Cloud zum ersten Mal auf Cloud Provisioning and Governance ein. Anschließend können Sie Microsoft Azure Government Cloud-Ressourcen mit Cloud Provisioning and Governance erkennen, bereitstellen und verwalten.

Vorbereitungen

Zum Einrichten von Microsoft Azure Government Cloud auf Cloud Provisioning and Governance müssen Sie folgende Schritte ausführen:

- Richten Sie im Azure Government-Portal einen Microsoft Azure-Dienstprinzipal ein, und registrieren Sie das Servicekonto in der Cloud Provisioning and Governance-Anwendung.
- Konfigurieren Sie einen MID-Server mit den erforderlichen Eigenschaften, damit Microsoft Azure Government und die ServiceNow-Instanz richtig kommunizieren können.
- Verwenden Sie die Anmeldeinformationen des Microsoft Azure-Dienstprinzipals, um zugehörige Servicekonten und Cloud-Ressourcen zu erkennen.
- Im Basissystem Terraform Vorlage, legen Sie fest *Umgebung* Variable zu `UsGovernment`. Informationen dazu, wo die zu ändernde Vorlage gefunden werden kann, finden Sie unter Erkennen Sie die IAC-Vorlagen (Infrastructure as Code).

```
provider "azurerm" {
    subscription_id = "<REPLACE_WITH_ACCOUNT_ID»"
    client_id = "<REPLACE_WITH_APP_ID»"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  client_secret = "<REPLACE_WITH_PASSWORD»"
  tenant_id = "<REPLACE_WITH_TENANT_ID»"
  environment = "usgovernment"
}
```

Erforderliche Rolle: Administrator

Hinweis: ServiceNow® ITOM Produkte werden nicht offiziell für die Regionen Deutschland und China zertifiziert oder unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für Tag 1 durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für Tag 2 je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Prozedur

1. Erstellen von Microsoft Azure Service-Prinzipal Auf der Microsoft Azure Behördenportal.

   Hinweis: Navigieren zu **App-Registrierungen** > **Registrieren Sie eine Anwendung** > **Unterstützte Account-Typen** Abschnitt. Wählen Sie dann die Option **Accounts in this organizational directory only (Single tenant)** (Konten nur in diesem Organisationsverzeichnis (Einzelner Mandant)), um sicherzustellen, dass das Active Directory, das für die Microsoft Azure Government Cloud konfiguriert ist, für die Authentifizierung verwendet wird.

   Weitere Informationen finden Sie unter Erstellen einer Azure AD-Anwendung und eines Dienstprinzipals mit Ressourcenzugriff über das Portal .

2. Konfigurieren MID Servers Um eine Verbindung herzustellen Cloud Provisioning and Governance Bis A Microsoft Azure Cloud-Account für Behörden.

   a. Navigieren zu **MID-Server verwenden** > **Fähigkeiten**an.

   b. Klicken Sie auf **Bearbeiten**, und fügen Sie die folgenden Optionen hinzu:

      - **Azure**
      - **Cloud Management**

   c. Klicken Sie auf **Speichern**.

   d. **Wahlweise:** Navigieren zu **MID-Server verwenden** > **Unterstützte Anwendungen**an. Überspringen Sie den nächsten Schritt, wenn **ALLE** Anwendungen ausgewählt sind.

   e. **Wahlweise:** Klicken Sie auf **Bearbeiten**, und fügen Sie die folgenden Anwendungen zur **Liste der unterstützten Anwendungen** hinzu:

      - **Discovery**
      - **Cloud Management**
      - **Orchestration**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen finden Sie unter:

- MID-Server-Auswahl
- MID-Server-Fähigkeiten

3. Navigieren zu **MID-Server verwenden** > **Eigenschaften**an.

a. Klicken Sie auf **Neu**, und fügen Sie für jedes der folgenden Name-Wert-Paare neue Datensätze hinzu: MID-Server -Eigenschaften

Name	Wert
mid.cmp.azure_api.base_endpoint	https://management.usgovcloudapi.net/${apiPath}
mid.cmp.azure_api.storage.containe	https://${accountName}.blob.core.usgovcloudapi.net/?comp=list
mid.property.azure_token_manage	https://login.microsoftonline.us/${tenantId}/oauth2/token
mid.property.azure_token_manage	grant_type=client_credentials&client_id=${clientId}&resource=https%3A%2F%2Fmanagement.usgovcloudapi.net%2F&client_secret=${clientSecret}
mid.cmp.azure_api.storage.blobpath	https://${accountName}.blob.core.usgovcloudapi.net/${containerName}?restype=container&include=snapshots&comp=list

b. Klicken Sie auf **Absenden**.

4. Speichern Sie die Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz.

5. In **Cloud-Administratorportal** , Navigieren Sie zu **Verwalten** > **Anmeldeinformationen**, Und wählen Sie den Azure Service Prinzipal-Datensatz aus.

6. Zum Erkennen von Servicekonten, die den Azure-Abonnements zugeordnet sind, die für diesen Dienstprinzipal verfügbar sind, klicken Sie auf den zugehörigen Link **Abonnements ermitteln**.

Ergebnis

In der zugehörige Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.

Nächste Maßnahme

Definieren Sie den Zeitplan für das Herunterladen Microsoft Azure Abrechnungsdatenan.

Weisen Sie Rollen zu zu AzureAnwender von Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Root-Administrator [sn_cmp.cmp_root_admin]	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator [sn_cmp.cloud_admin]	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle [sn_cmp.cloud_governor]	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer [sn.cmp.cloud_service_designer]	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer [sn_cmp.cloud_service_user]	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Ihnen zugewiesenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
		Aufgabendatensätze zugreifen, wenn Sie die Rolle „Cloud-Service-Anwender“ innehaben.
Cloud-Betreiber [sn_cmp.cloud_operator]	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration [sn_cmp.cloud_event_integration] **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator [sn_cmp.cloud_group_admin]	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Microsoft Azure-Dienstprinzipal erstellen

Für den sicheren Zugriff auf Ressourcen und Abrechnungsdaten in Ihrem Microsoft Azure-Konto muss der Discovery-Prozess entsprechende Anmeldeinformationen für das Microsoft Azure-Konto bereitstellen. Sie erstellen ein spezielles programmgesteuertes Konto – einen Microsoft Azure-Dienstprinzipal –, um die erforderlichen Anmeldeinformationen zu generieren.

Vorbereitungen

Erforderliche Rollen:

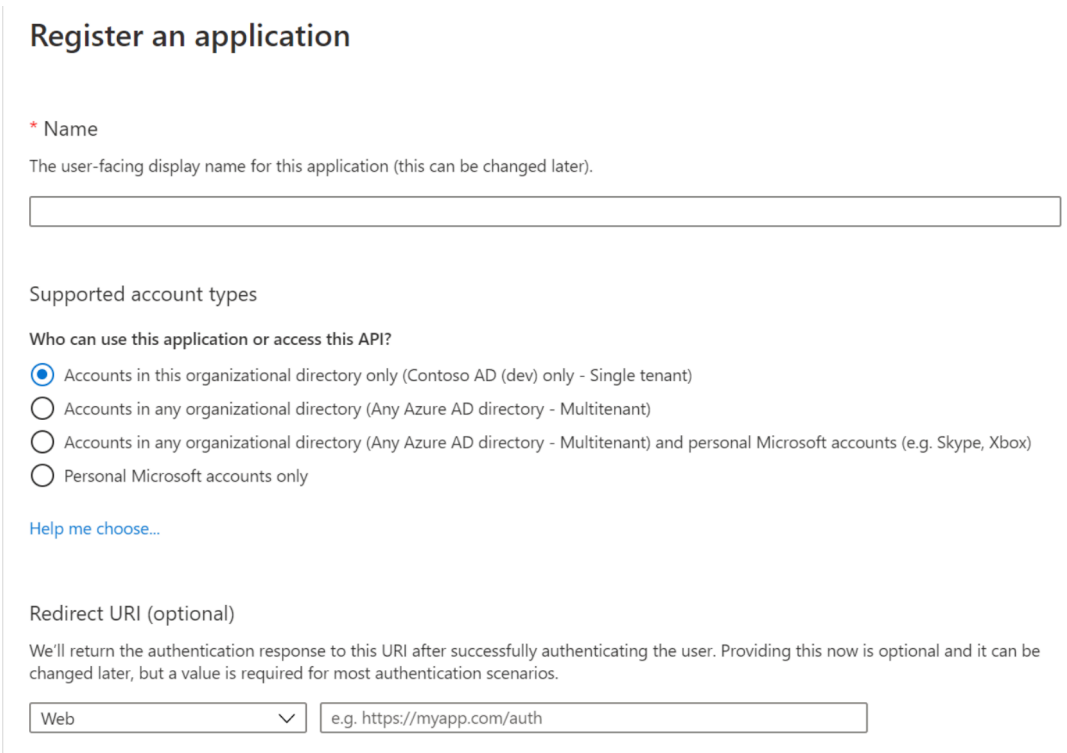
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rollen „Discovery_admin“, „Service_Mapping_admin“, „sn_CMP.Cloud_admin“ in Cloud Provisioning and Governance Oder Rolle sn_Cloud_OPS_WS.Cloud_OPS_admin in Cloud Operations Workspace.
- Vorgänge im Microsoft Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator
  und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Aktivieren Sie die interne Netzwerkverbindung zwischen den MID-Servern und den Azure Cloud API-Endpunkten:
  - Die US-GovCloud-URL ist `https://management.usgovcloudapi.net/` .
  - Die kommerzielle Azure Cloud-URL ist `management.azure.com` .

> **Hinweis:** Es ist nicht erforderlich, wenn Anmeldeinformationen hinzugefügt werden, wenn der hinzuzufügende Account bereits ein GovCloud-Account ist.

Prozedur

1. Melden Sie sich beim Azure-Portal an, und navigieren Sie zu **Azure Active Directory**.
2. Navigieren Sie zum Abschnitt **App registrations** (Appregistrierungen), und klicken Sie auf **New application registration** (Neue Anwendungsregistrierung).
   Geben Sie für Ihre Anwendung folgende Informationen ein:



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Eindeutiger Name für die Anwendung und ihre Integrationsanmeldeinformationen. Beispiel: ServiceNow Integration.
Unterstützte Account-Typen	Geben Sie an, wer die Anwendung verwenden kann.
Redirect URI (optional, Umleitungs-URI)	URL, die auf Azure zugreift. Normalerweise die URL der ServiceNow-Instanz

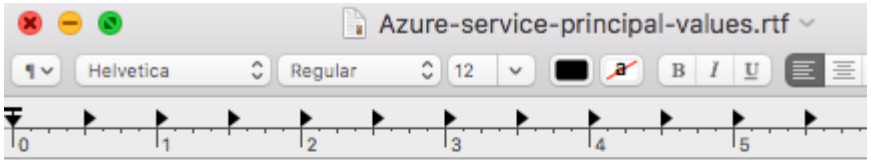
3. Wählen Sie **Register** aus, um die Registrierung der App abzuschließen.
4. Wenn die Registrierung abgeschlossen ist, kopieren Sie die Werte für die Anwendungs- (Client-) ID und Verzeichnis (Mandant) ID, und fügen Sie sie in den Texteditor ein.
5. Bezeichnen Sie die Werte **Anwendungs-ID** Und **Verzeichnis-ID** Entsprechend.
6. Navigieren Sie im Azure-Portal zum Abschnitt **Certificates & secrets** (Zertifikate und geheime Schlüssel), und geben Sie dann unter **New client secret** (Neuer Client-Geheimschlüssel) die folgenden Werte an:

Feld	Beschreibung
Schlüsselbeschreibung	Beschreibung für den Schlüssel
Dauer	Ablauf für den Schlüssel. **Hinweis:** Ihre Organisation kann Richtlinien anwenden, um die Gültigkeitsdauer des Schlüssels einzuschränken. Wählen Sie die entsprechende Dauer aus.

7. Klicken Sie auf **Hinzufügen**.
8. Kopieren Sie den Schlüsselwert, fügen Sie ihn in den Texteditor ein, und beschriften Sie den Wert als **Anwendungsschlüssel**.
9. Damit der Dienstprinzipal mit verschiedenen Azure-Abonnements arbeiten kann, navigieren Sie zu **Abonnements**.
   Zum Verwalten mehrerer Abonnements müssen Sie das folgende Verfahren für jedes Abonnement ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Fügen Sie die Abonnements-ID in den Texteditor ein, und beschriften Sie sie als **Abonnements-ID**.
Die Textdatei, die Sie während dieses Verfahrens generieren, sieht möglicherweise wie folgt aus:



Directory ID: 8bcdd120-9979-491e-8683-d9a4550bdd

Application ID: e6821ea9-e5c5-428a-b50c-7ea62993b2d

Application key: d348050-f893ccb7-hg84yg8-rg200hd

Subscription ID: 4803be48c3ee89-96d2-4fed-bedb-22e49013ee89

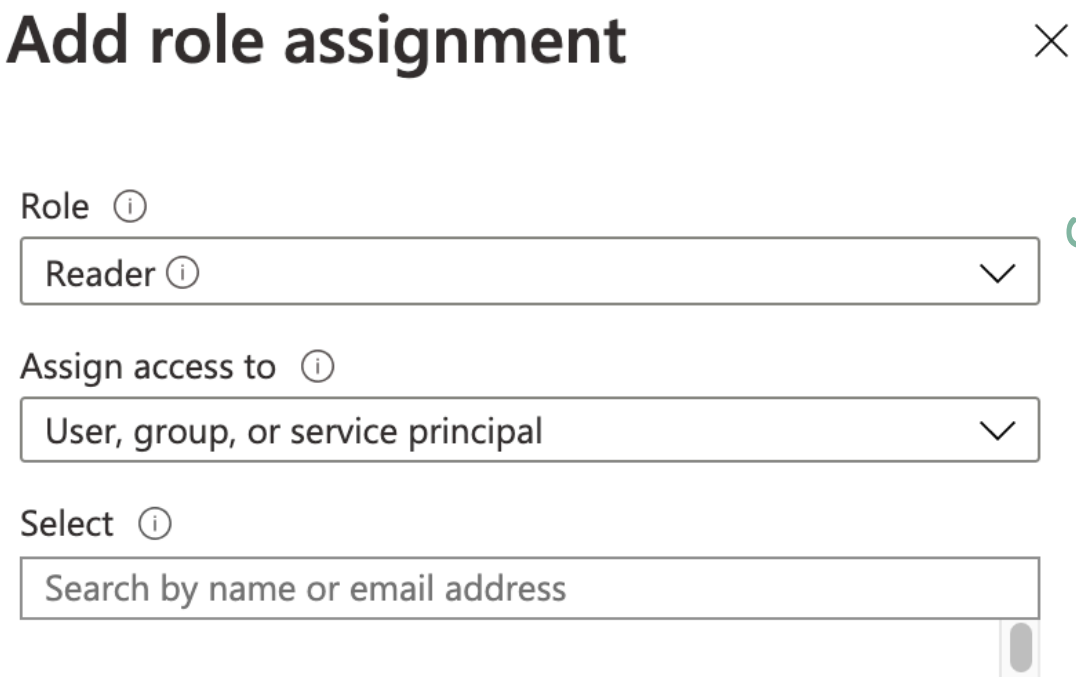
b. Navigieren Sie zum Abonnement, und wählen Sie im Menü die Option **Zugriffssteuerung (IAM)** aus.

c. Klicken Sie oben im Bildschirm auf **+ Hinzufügen** und dann auf **Add role assignment** (Rollenzuweisung hinzufügen).

d. Wählen Sie im Feld **Rolle** den Wert **Leser** aus.
Lassen Sie den Standardwert für **User, group, or service principal** (Benutzer, Gruppe oder Service-Prinzipal) für das Feld **Assign Access to** (Zugriff zuweisen an) unverändert.

> **Hinweis:** Die Rolle **Mitwirkender bei Ressourcenrichtlinien** ist nur für die Bereitstellung erforderlich.

e. Wählen Sie im Feld **Auswählen** den Namen aus, den Sie in Schritt 2 erstellt haben, und klicken Sie auf **Speichern**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Führen Sie die entsprechende Aktion aus.

- Wenn Sie Cloud-Discovery nicht über Cloud Operations Workspace verwenden, gehen Sie wie folgt vor:

  Klicken Sie im Discovery Manager auf das Plus-Symbol (**+**) Und dann auswählen **Azure-Service-Prinzipal** Aus der Liste.

- Wenn Sie Cloud-Discovery über Cloud Operations Workspace verwenden, gehen Sie wie folgt vor:

  a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

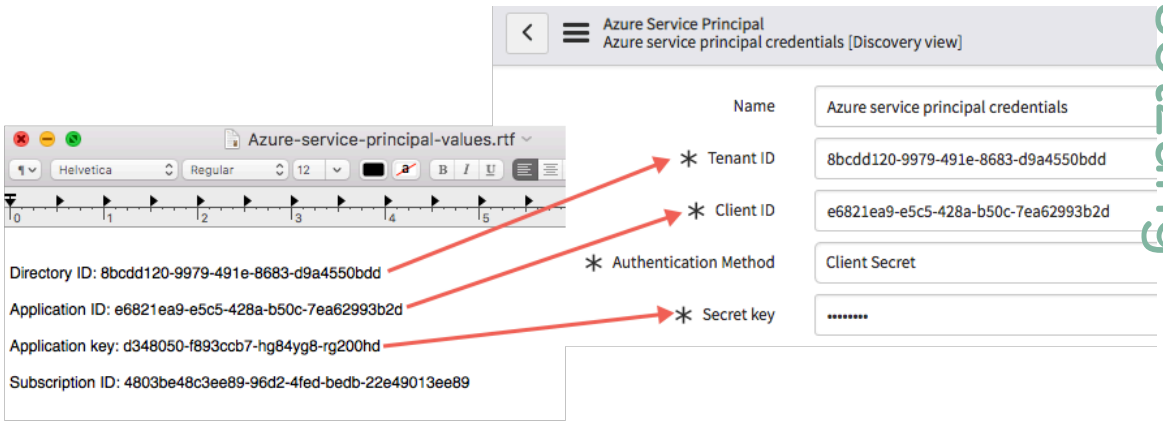
  b. Wählen Sie **Neu**.

  c. Wählen Sie **Azure-Service-Prinzipal** aus.

11. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: Azure service principal credentials.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

12. Kopieren Sie die Werte aus der temporären Textdatei, und fügen Sie sie in die verbleibenden Felder ein.



Formularfeld „Anmeldeinformationen“	Wert „Azure-Dienstprinzipal“
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei
Geheimer Key	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Klicken Sie auf **Speichern**, um den Azure-Dienstprinzipal zu erstellen.
14. Klicken Sie auf den zugehörigen Link **Abonnements erkennen**, um alle Abonnements für den Azure-Dienstprinzipal zu suchen.
    Die Instanz erstellt ein Servicekonto für jedes erkannte Abonnement. In der zugehörigen Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.
15. Klicken Sie auf ein Abonnement, um das für das Abonnement erstellte Servicekonto anzuzeigen.
16. Klicken Sie auf einen Discovery-Statuseintrag in der Liste **Berechtigung Discovery-Status**, um das Discovery-Protokoll anzuzeigen.
    Bei jedem Klicken auf **Discovery-Abonnement** generiert die Instanz einen neuen Discovery-Status und zeigt ihn in der Liste **Berechtigung Discovery-Status** an.

Nächste Maßnahme

Nur Cloud Provisioning and Governance: Erstellen Sie einen Datensatz der Anmeldeinformationen des Dienstprinzipals in der ServiceNow-Instanz, damit über Cloud Provisioning and Governance-Prozesse auf Microsoft Azure-Daten zugegriffen werden kann. Weitere Informationen finden Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern.

Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst die Anmeldeinformationen des Azure-Dienstprinzipals in der Azure-Portal. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

Vorbereitungen

Erforderliche Rolle:

- Azure-Portal Active Directory-Administrator (AD)
- Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin, discovery_admin

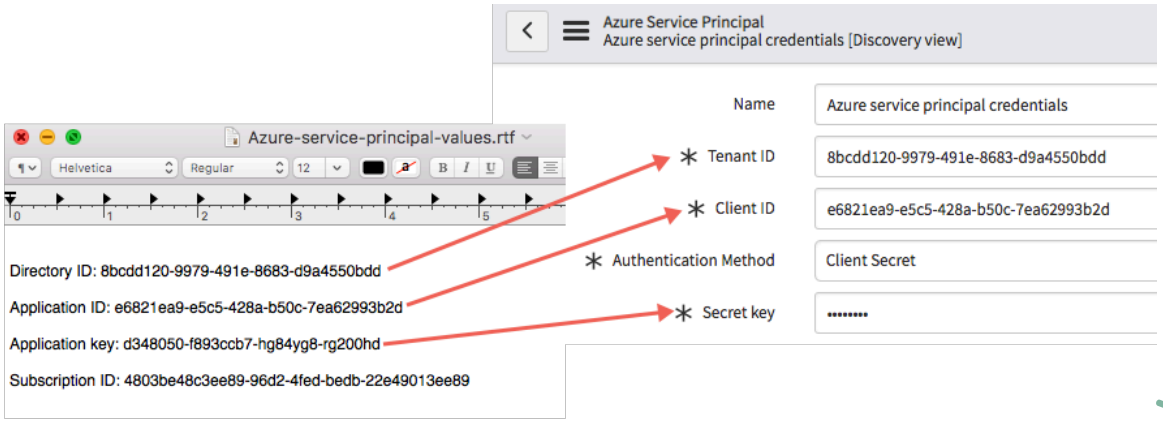
Prozedur

1. Microsoft Azure-Dienstprinzipal erstellen und öffnen Sie die Textdatei, die Sie während des Verfahrens erstellt haben.
2. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Anmeldeinformationen**an.
3. Klicken Sie auf **Neu**, und wählen Sie dann **Azure-Dienstprinzipal** aus.
4. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: Azure service principal credentials.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis** aus. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Kopieren Sie die Werte aus der Textdatei Azure-Credentials.txt, und fügen Sie sie in die verbleibenden Felder ein.



6. Wählen Sie die entsprechenden **EA-Anmeldeinformationen** aus der Liste aus, wählen Sie das Kontrollkästchen **Aktiv** aus, und klicken Sie dann auf **Speichern** , um den Datensatz zu erstellen.
7. Klicken Sie auf den zugehörigen Link **Abonnements ermitteln**, um alle Abonnements zu finden, die mit dem Azure-Dienstprinzipal verknüpft sind.
   Die Instanz erstellt für jedes ermittelte Abonnement einen Servicekonto.Die **Azure-Abonnements** Zugehörige Liste zeigt alle Abonnements an, die dem Azure-Serviceprinzip zugeordnet sind.
8. Klicken Sie auf ein Abonnement, um den Servicekonto zu sehen, der für dieses Abonnement erstellt wurde.
9. Klicken Sie in der Liste **Discovery-Status für Anmeldeinformationen** auf den Eintrag eines Discovery-Status, um das zugehörige Discovery-Protokoll aufzurufen.
   Jedes Mal, wenn Sie auf **Abonnements ermitteln** klicken, generiert die Instanz einen neuen Discovery-Status und führt den Status in der Liste **Discovery-Status für Anmeldeinformationen** auf.

Fügen Sie einen hinzu Azure Servicekonto

Im Rahmen des Setup-Leitfadens für Tag 1 für Cloud Provisioning haben Sie dem Cloud-Konto ein Servicekonto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

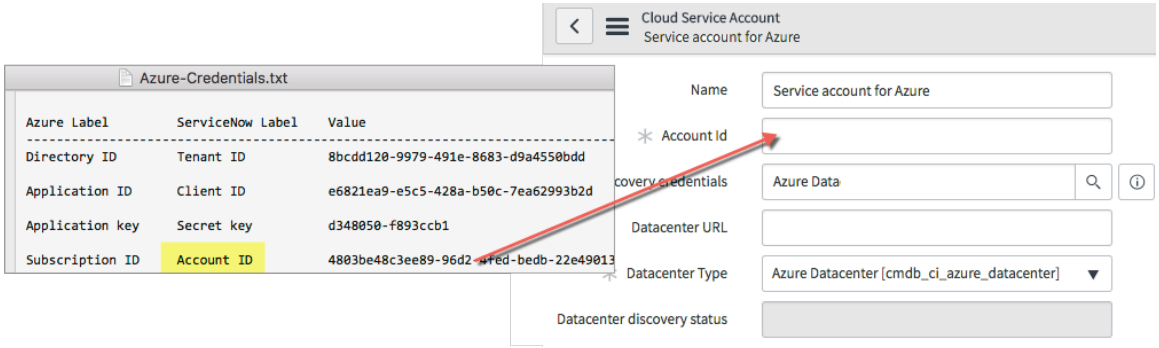
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Öffnen Sie die Textdatei Azure-Credentials.txt, die Sie während der Anleitung Microsoft Azure-Dienstprinzipal erstellen erstellt haben.
2. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Service-Konten**an.
3. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** ein, und füllen Sie dann das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Konto-ID	Der Wert der Azure-**Abonnement-ID**, den Sie aus der Azure-Portal in die Textdatei kopiert haben. Siehe Erkennung von Azure-Clouds Um Abonnement-IDs für Verwaltungsgruppen zu lernen.
Discovery-Anmeldeinformationen	Name der Anmeldeinformationen, die Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern erstellt haben. Im Beispiel haben Sie den Namen Azure service principal credentials verwendet.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist nur für Regierungs- und regionale Konten erforderlich. Muster für Discovery und Service-Mapping Unterstützt die USA, Deutschland und China Microsoft Azure Behörden-Clouds.
Rechenzentrumstyp	Wählen Sie **Azure-Rechenzentrum** aus.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Sollte Events abrufen	Option, um in der ServiceNow AI Platform® das Sammeln von Informationen über Ressourcen-Changes aus der Microsoft Azure-Cloud zu aktivieren. Die ServiceNow AI Platform® verwendet die Informationen über Ressourcen-Changes zur Aktualisierung der Configuration Management Database (CMDB). Weitere Informationen zu unterstützten finden Sie unter Azure Ressourcentypen, siehe Azure Change-Verarbeitung. Wenn Sie das Kontrollkästchen sollte Ereignisse abrufen für eine Verwaltungsgruppe aktivieren, wird die aktiviert ServiceNow AI Platform Aktiviert Azure Change-Verarbeitung für alle Abonnements in der Verwaltungsgruppe.

4. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Nächste Maßnahme

Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind.

Zugehörige Informationen

Erkennung von Azure-Clouds

Richten Sie ein Cloud-KontoFür Azure

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

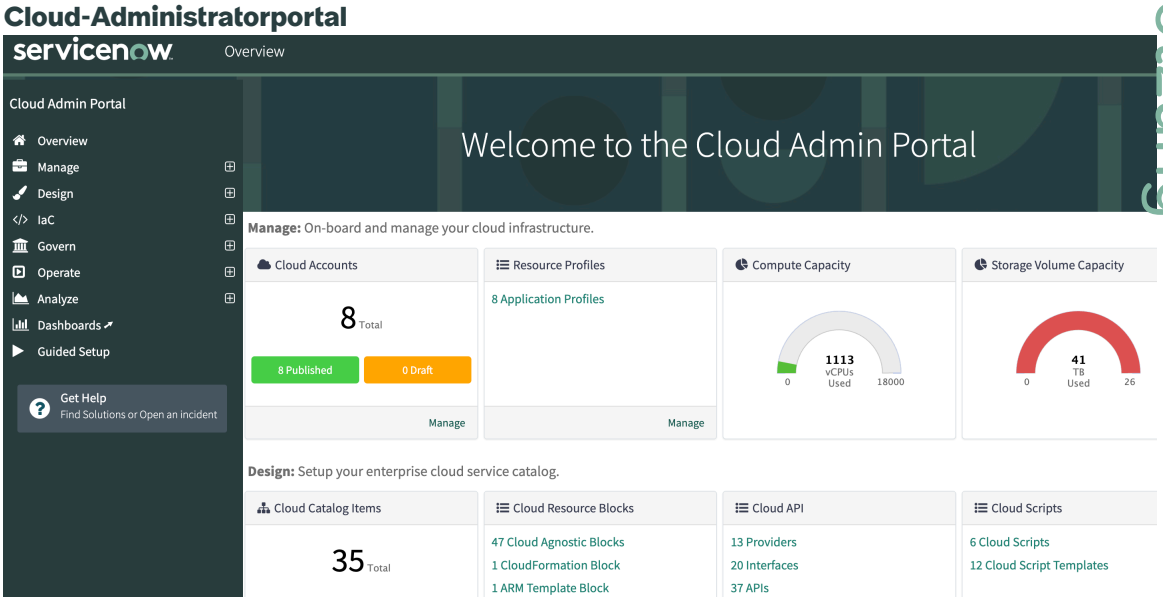
Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu Cloud-Accounts finden Sie unter Cloud-Accounts.

Hinweis: Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In Azure werden die bereichsspezifischen Container für virtuelle Ressourcen als *Regionen* bezeichnet. In Cloud Provisioning and Governance werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet. .

Prozedur

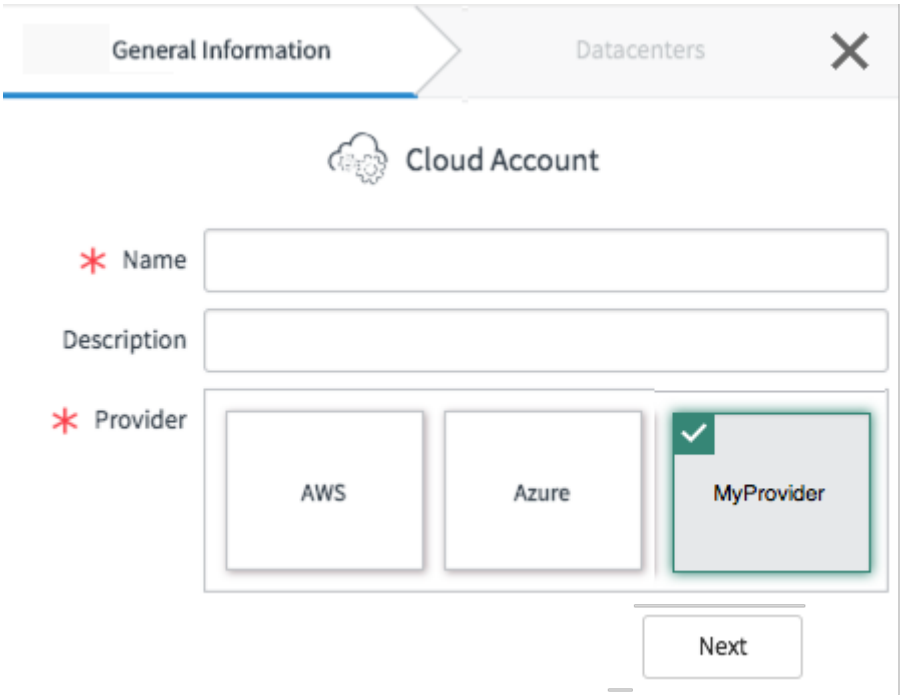
1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.



2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und wählen Sie dann den Cloud-**Provider** für das Konto aus (Azure).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Next** (Weiter).
   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt, und eine Liste der ermittelten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um sie zu suchen. Weitere Detailinformationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.

4. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

   Hinweis:

   - Wählen Sie nur die LDC/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
   - Um Ressourcen in Regionen/LDC zu erkennen, z. B. Nordamerika (US East, US West und Kanada Central), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik, stellen Sie mit eine Zugriffsanforderung für die erforderlichen Endpunkte GCP Support.

   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.

5. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
- **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.

6. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Erstellen Microsoft Azure Anmeldeinformationen für Abrechnungsdownload

Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Server s regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Vorbereitungen

Wichtig:

Beginnend mit Vancouver Release: Das AbrechnungsDashboard ist nicht mehr verfügbar, wenn Sie heruntergeladen und aktiviert haben ServiceNow Store Cloud-Einblicke Anwendung. Folgende Änderungen finden statt:

- Sie werden zu weitergeleitet Cloud-Einblicke Homepage standardmäßig.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Das Widget „Ausgaben für aktuellen Monat“ und das Widget „Budget“ im Cloud-Anwenderportal zeigen keine Daten an, wenn Cloud-Einblicke Ist auf der Instanz aktiviert.

Wenn Sie aktiviert haben Cloud-Einblicke Anwendung können Sie nur zum Abrechnungs-Dashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

Sie müssen über einen API-Zugriffsschlüssel-Anmeldeinformationen für eine Enterprise Agreement (EA) für alle verfügen Azure Accounts, für die Sie Abrechnungsinformationen benötigen.

Erforderliche Rolle: sn_cmp.cloud_governor

Warum und wann dieser Vorgang ausgeführt wird

Während des Abrechnungsdownloadvorgangs werden alle Ressourcen in das System abgerufen. Azure Datenbanken werden in der Tabelle „Datenbank“ [cmdb_ci_database] platziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie ein geheimes Client-Geheimnis, indem Sie zur Übersichtsseite der zuvor bereitgestellten Service Principal-Anwendung navigieren.

   a. Wählen Sie im linken Bereich aus **Zertifikate und Geheimnisse** .

   b. Wählen Sie im Abschnitt geheime Clientgeheimnisse die Option aus **Neues geheimes Clientgeheimnis** .

   c. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Beschreibung	Beschreibung des geheimen Clientschlüssels. Beispiel: Geheimer Clientschlüssel für MyServicePrincipal .
Läuft ab	Ablaufzeitraum, der Ihren Anforderungen entspricht. Beispiel: 6 Monate , 12 Monate , 24 Monate , Oder Nie .

   d. Wählen Sie **Hinzufügen**.

   Nach dem Hinzufügen des geheimen Clientschlüssels wird ein Wert generiert und angezeigt.

   Hinweis: Kopieren Sie diesen Wert sofort, da er nicht erneut angezeigt würde. Dies ist Ihr geheimer Client-Schlüssel (Zugriffsschlüssel).

2. Kopieren Sie die Anwendungs-(Client-)ID und Verzeichnis-ID (Mandant) zur späteren Verwendung.
3. Weisen Sie dem Service Prinzipal eine Rolle zu.
   a. Wählen Sie im linken Bereich aus **Azure Active Directory** .
   b. Wählen Sie Aus **Rollen und Administratoren** .
   c. Wählen Sie Aus **Alle Rollen** Und suchen Sie die Rolle, die Sie zuweisen möchten.
   d. Wählen Sie die Rolle und dann aus **Fügen Sie die Zuweisung hinzu** .
   e. Suchen Sie nach Ihrem Serviceprinzip, wählen Sie ihn anhand seines Namens aus, und wählen Sie dann aus **Hinzufügen** .
4. Rufen Sie eine Abonnement-ID ab, indem Sie auswählen **Abonnements** .
   a. Wählen Sie das Abonnement aus, das Sie verwenden möchten.
   b. Kopieren Sie die Abonnement-ID von der Seite „Abonnementübersicht“.

Downloadgröße von Microsoft Azure-Abrechnungsdaten konfigurieren

Ein einzelner Satz Cloud Billing-Daten kann umfangreich sein. Vom MID-Server werden die Daten daher in verwaltbaren Blöcken an die ECC-Warteschlange gesendet. Optional können Sie eine Systemeigenschaft so konfigurieren, dass die Größe der einzelnen Blöcke begrenzt wird. So vermeiden Sie Leistungsprobleme, die durch die Übertragung großer Datenmengen verursacht werden.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“, indem Sie im Anwendungsfilter sys_properties.list eingeben.
2. Filtern Sie die Liste, um die Eigenschaft sn_cmp.billing.page_size zu öffnen.
   Der Standardwert ist 3 MB.
3. Modifizieren Sie den Wert nach Bedarf.
   Der Höchstwert beträgt 5 MB.
4. Speichern Sie die Eigenschaft.

Setup-Leitfaden für Tag 1 für Google Cloud Bis Cloud-Services-Katalog Terraform Connector

Zum Einrichten Google Cloud Führen Sie zum ersten Mal die Schritte in diesem Setup-Leitfaden für Tag 1 in der Reihenfolge aus, in der sie angezeigt werden. Nach Abschluss des Setups für Tag 1 können Sie nach Bedarf mit den optionalen Konfigurationsschritten für Tag 2 in beliebiger Reihenfolge fortfahren. Detaillierte Anweisungen für jeden Schritt finden Sie in den folgenden Abschnitten.

Hinweis: Die ServiceNow® Cloud Provisioning and Governance: Google Cloud Connector Wird nicht mehr bereitgestellt, erweitert oder unterstützt. Weitere Informationen finden Sie im Artikel Deprecation Process [KB0867184] (Ausgliederungsprozess) in der Knowledge Base des Now Support.

Zum Einrichten von Google Cloud Platform erforderliche Rollen

- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud Provisioning and Governance verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. Bei der Google Cloud Platform werden die bereichsspezifischen Container für virtuelle Ressourcen als *Regionen* bezeichnet. Im ServiceNow-Clouddatenmodell werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Schneller Überblick über den Setup-Prozess

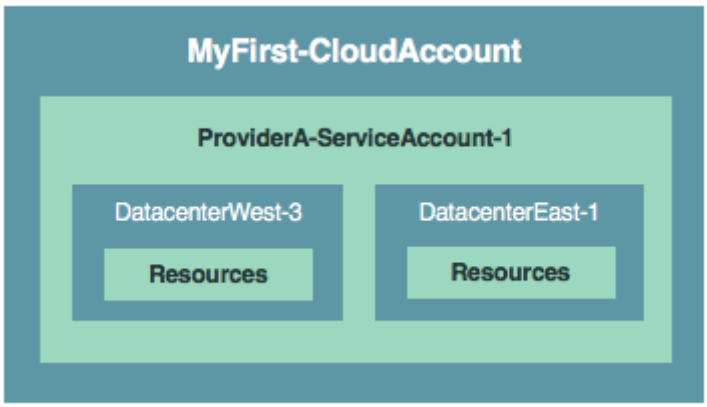
Ihr Setup-Prozess an „Tag 1“ umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Laden Sie die App Connector und unterstützende Store-Apps aus dem ServiceNow Store herunter, und aktivieren Sie die Store-Anwendungen.
- Weisen Sie Cloud-Administratoren und Endanwendern die entsprechenden Rollen zu.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration Ihrer Google Cloud Platform-Cloud-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. Rufen Sie ab CSK Terraform Connector App auf der ServiceNow Store
2. Rollen an Google Cloud Platform-Benutzer zuweisen

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

3. Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen

   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten.

   Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie die Anmeldeinformationen an CSK Terraform Connector Verwendet für den Zugriff Google Cloud PlatformDaten

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, öffnen Sie die Google Cloud Console, um das Google Cloud Platform-Projekt anzugeben, das über programmgesteuerten Zugriff auf Ihre Google Cloud Platform-Daten verfügt. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

5. Richten Sie ein Cloud-KontoUnd ServicekontoFür Google Cloud Platform

   Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Rollen an Google Cloud Platform-Benutzer zuweisen

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Root-Administrator [sn_cmp.cmp_root_admin]	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator [sn_cmp.cloud_admin]	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
		• Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle [sn_cmp.cloud_governor]	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer [sn.cmp.cloud_service_designer]	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer [sn_cmp.cloud_service_user]	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Ihnen zugewiesenen Aufgabendatensätze zugreifen, wenn Sie die Rolle „Cloud-Service-Anwender“ innehaben.
Cloud-Betreiber [sn_cmp.cloud_operator]	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration [sn_cmp.cloud_event_integration]	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten	Cloud-Infrastruktur:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Hinweis: Von IBM Cloud Connector nicht unterstützt	von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	• Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator [sn_cmp.cloud_group_admin]	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Geben Sie die Anmeldeinformationen an CSK Terraform Connector Verwendet für den Zugriff Google Cloud PlatformDaten

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, öffnen Sie die Google Cloud Console, um das Google Cloud Platform-Projekt anzugeben, das über programmgesteuerten Zugriff auf Ihre Google Cloud Platform-Daten verfügt. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

Vorbereitungen

Erforderliche Rollen:

- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Weil ServiceNow Die Anwendung unterstützt mehrere Cloud-Anbieter. Die App verwendet allgemeine Namen für die Einstellungen.

Prozedur

1. Wenn Sie die Anmeldeinformationen bereits generiert haben, die von verwendet werden Google Cloud, Springen Sie zum letzten Schritt.
   Andernfalls fahren Sie mit dem nächsten Schritt fort.
2. Wählen Sie im Google Cloud Console-Dashboard das Projekt aus.
3. Navigieren zu **APIs und Services** > **Anmeldeinformationen**an.

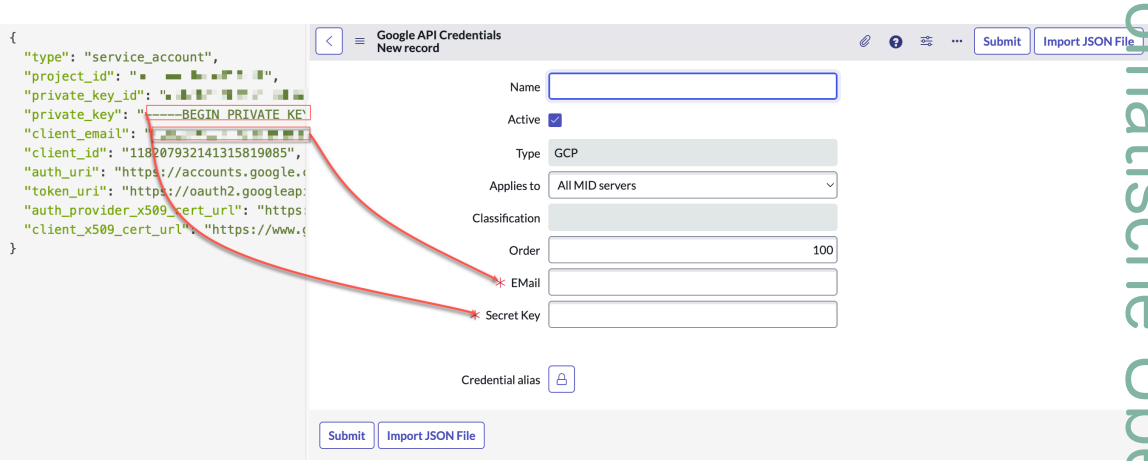
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Auf der **Anmeldeinformationen** Klicken Sie auf die Registerkarte **Anmeldeinformationen erstellen** > **Service-Account-Schlüssel**, Und erstellen Sie dann den Schlüssel.
   Geben Sie den **JSON-**-Schlüsseltyp an.
5. Identifizieren Sie die Anmeldeinformationen, die Google Cloud, Discovery, Und den Cloud-Servicekatalog (CSK) Terraform Connector Sollte in Ihrer -Instanz verwenden, um auf Daten von zuzugreifen Google Cloud Platform.

   a. Öffnen Sie die JSON-Datei in einem Texteditor.

   b. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Anmeldeinformationen**, Klicken Sie auf **Neu** Und wählen Sie dann aus **Google-Anmeldeinformationen** .

   c. Geben Sie den **Namen** der Anmeldeinformationen an, die bei der Instanz registriert werden sollen. Geben Sie beispielsweise `Google credentials-1` ein, und kopieren Sie dann die Werte aus der JSON-Schlüsseldatei in die Formularfelder. Fügen Sie den Wert von `private_key` in das Feld **Geheimer Schlüssel** und den Wert von `client_email` in das Feld **E-Mail** ein.



   d. Wählen Sie die Checkbox **Aktiv** aus, um die Anmeldeinformationen zu verwenden, und klicken Sie dann auf **Absenden**.

Richten Sie ein Cloud-KontoUnd ServicekontoFür Google Cloud Platform

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

Erforderliche Rolle: keine

- Laden Sie herunter, und aktivieren Sie CSK Terraform Connector Von ServiceNow® Store. Um auszuprobieren Sofort einsatzbereite Kataloge mit Cloud-Services-Katalog Installieren Sie für Google CSK Inhaltspaket.
- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

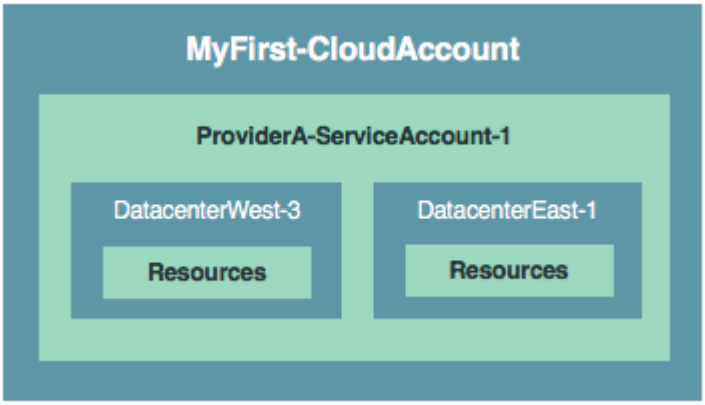
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie das Setup für „Tag 1“ abgeschlossen haben, sieht Ihr Cloud-Konto möglicherweise so aus:

Struktur eines Cloud-Kontos an Tag 1



Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.
2. Wählen Sie das Cloud-Konto aus, oder erstellen Sie es:
   - Wählen Sie ein vorhandenes Cloud-Konto aus:
     a. Klicken Sie auf der Seite des Cloud-Kontos auf **Konfigurieren**.
     b. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
   - Cloud-Konto erstellen:
     a. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Neu**, und geben Sie dann einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für das Cloud-Konto ein.
     b. Provider auswählen.
     c. Klicken Sie auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
3. Erstellen Sie auf der Seite „Rechenzentren“ ein Servicekonto: Klicken Sie neben dem Feld **Servicekonto** auf das **+**, und füllen Sie dann das Formular für Servicekonto aus.
4. Füllen Sie aus der JSON-Schlüsseldatei, die dem Service-Account zugeordnet ist, aus **Projekt_ID** Wert in **Account-ID** Feld.

   Hinweis: Sie können die Option JSON-Datei importieren zum Ausfüllen verwenden. Weitere Einzelheiten finden Sie unter Konfigurieren Sie Google API-Anmeldeinformationen für Cloud-Discovery.

5. Wählen Sie im Feld **Discovery-Anmeldeinformationen** die entsprechenden Anmeldeinformationen für das Servicekonto aus.
   Dies sind die Anmeldeinformationen, die Sie im Geben Sie die Anmeldeinformationen an CSK Terraform Connector Verwendet für den Zugriff Google Cloud PlatformDaten-Vorgang generiert haben.
6. Lassen Sie das Feld **Rechenzentrums-URL** leer.
7. Füllen Sie die restlichen Felder aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rechenzentrumstyp	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenzentrum) aus.
Status der Rechenzentrumserkennung	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenzentrum) aus.
Sollte Events abrufen	Aktiviert Cloud Provisioning and Governance zum Sammeln von Events von Ressourcentypen in Google-Projekt-LDCs in der `sn_cmp_cloud_event_list` .

8. Klicken Sie auf **Absenden**, um das Servicekonto zu erstellen.
9. Klicken Sie auf **Rechenzentren erkennen**
10. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

Hinweis:

- Wählen Sie nur die LDC/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
- Um Ressourcen in Regionen/LDC zu erkennen, z. B. Nordamerika (US East, US West und Kanada Central), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik, stellen Sie mit eine Zugriffsanforderung für die erforderlichen Endpunkte GCP Support.

Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.

11. Klicken Sie auf ein Rechenzentrum.
Die folgenden Listen werden angezeigt:
    - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
    - **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
    - **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.
12. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Nächste Maßnahme

Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Zusätzliches Cloud-Konto einrichten

(Optional) Fügen Sie ein hinzu Google Cloud Platform ServicekontoZu Cloud-Konto

Erkennung von Google Cloud Platform

(Optional) Fügen Sie ein hinzu Google Cloud Platform ServicekontoZu Cloud-Konto

Im Rahmen des Tag-1-Setups von Cloud Provisioning and Governance haben Sie ein Servicekonto zum Cloud-Konto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

Vorbereitungen

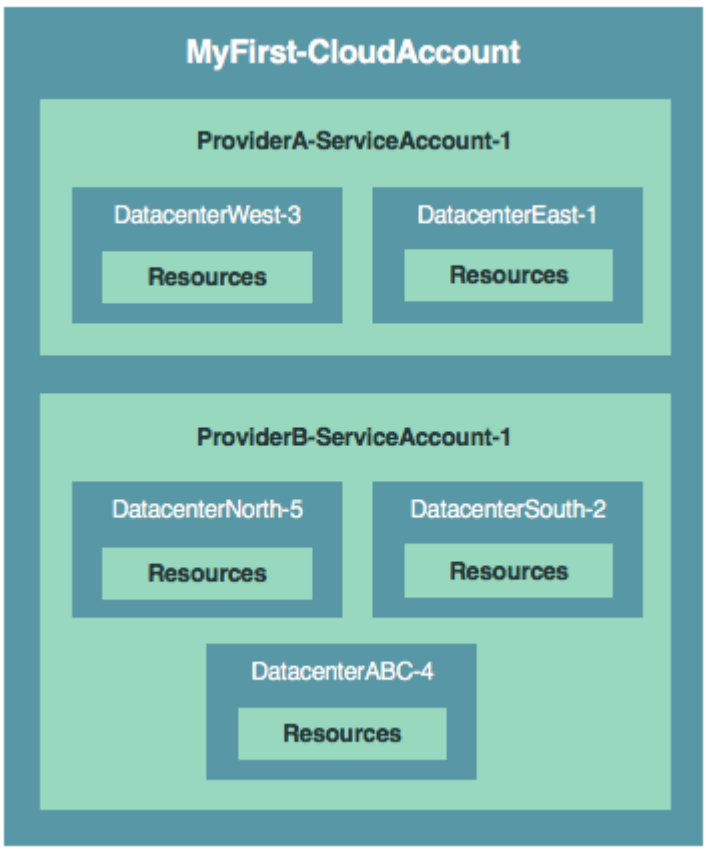
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

In diesem Beispiel haben Sie ein Servicekonto mit dem Namen **ProviderB-ServiceKonto-1** hinzugefügt und drei Rechenzentren zur Einbindung in das Cloud-Konto ausgewählt:

Servicekonto mit drei ausgewählten Rechenzentren

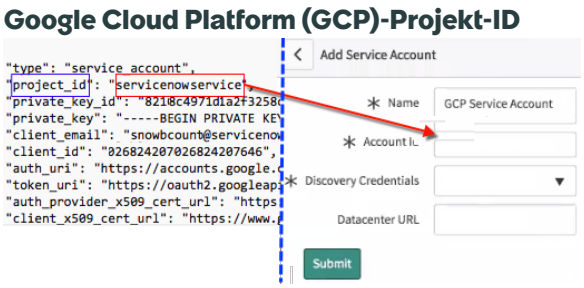


Wichtig: In einem Cloud-Konto können Sie kein bestimmtes Rechenzentrum in zwei verschiedenen Servicekonten auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Service-Konten**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein, und füllen Sie dann das Formular aus.
3. Füllen Sie die restlichen Felder aus:

Feld	Beschreibung
Konto-ID	Kopieren Sie aus der JSON-Schlüsseldatei, die Servicekonto zugeordnet ist, den Wert für **projec Konto-ID**. 
Discovery-Anmeldeinformationen	Wählen Sie die entsprechenden Anmeldeinformationen für das Servicekonto aus. Informationen z oder Abrufen der Anmeldeinformationen finden Sie unter Geben Sie die Anmeldeinformationen a Connector Verwendet für den Zugriff Google Cloud PlatformDaten.
Rechenzentrums-URL	Lassen Sie das Feld **Rechenzentrums-URL** leer.
Rechenzentrumstyp	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenzentrum) a
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im F

4. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.
5. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie an Cloud Provisioning and Governance Anwendung

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Vorgänge in der VMware-Konsole erfordern die Rolle „VMware-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Cloud-Management verwendete Begriffe

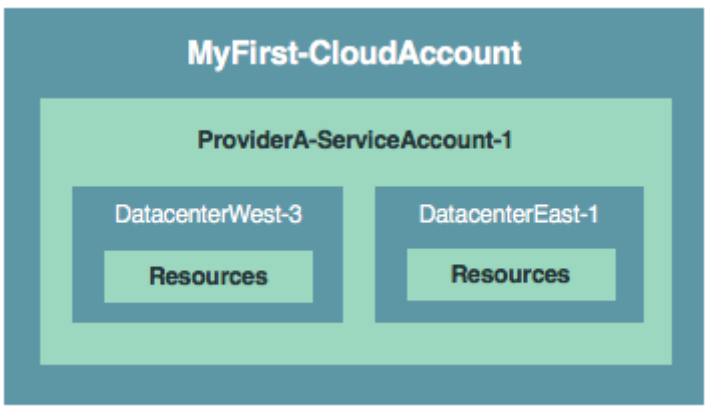
Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

Schneller Überblick über den Setup-Prozess

Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen zur Integration vom Cloud Provisioning and Governance in Ihre VMware Cloud-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. **Weisen Sie Rollen zu zu VMwareAnwender von Cloud Provisioning and Governance**

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. **Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift**

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst einen Account in der VMware-Konsole. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz. Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

3. **Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen**

   Discovery nutzt die Informationen im Servicekonto dazu, alle dem Anbieter-Account zugeordneten logischen Rechenzentren zu identifizieren.

4. **Einrichten Cloud-AccountsFür VMware**

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

5. **Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen**

   Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

vSphere

- Enterprise oder Enterprise Plus Edition 5.5 oder höher.
- Aktivieren Sie die vSphere-Umgebung für verteilte Ressourcenplanung (Distributed Resource Scheduling, DRS).
- Richten Sie Datenspeicher in Speicher-DRS (Storage DRS) ein.

Lesen und ändern Sie bei der Bereitstellung von virtuellen Computern unter Windows die genannten Anpassungsspezifikationen.

ESXi-Hosts

Wenn die IP-Adresse eines virtuellen Computers manuell mithilfe eines Skripts oder Post-Init-Skripts festgelegt wird, das auf der VM ausgeführt wird, müssen Sie HTTPS-Datenverkehr zwischen dem MID-Server und dem ESXi-Host für die VM zulassen.

Aktivieren Sie die NTP-Zeitsynchronisierung. Aktivieren Sie den NTP-Client für den Hypervisor auf dem vSphere-Webclient. Weitere Informationen finden Sie in der vSphere-Dokumentation .

vCenter Server-Anforderungen

vCenter 5.5 oder 6.0 Standard oder Foundation Edition.

vCenter-Zugriffsanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mindestberechtigungen für den Benutzer, der über die Instanz eine Verbindung zu vSphere herstellt:

- Datenspeicher: Alle
- Datenspeicher-Cluster: Alle
- Ordner: Erstellen, Löschen
- Global: Aufgabe abbrechen, Lizenz
- Host > Lokale Vorgänge: Virtuelle Computer erstellen/löschen/neu konfigurieren
- Profilgesteuerte Speicherung: Alle
- Netzwerk: Netzwerk zuweisen
- Ressource: Empfehlung anwenden; virtuelle Computer erstellen/ändern/zuweisen/entfernen
- Virtuelle Computer: Alle

vCenter-Anmeldeinformationen

- Anwendername
- Passwort
- URL oder IP-Adresse des vCenter-Servers, auf den von der Instanz über den MID-Server zugegriffen wird
- vCenter-Instanz-UUID. Unter Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift finden Sie Anweisungen zum Abrufen der UUID.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Weisen Sie Rollen zu zu VMwareAnwender von Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Root-Administrator [sn_cmp.cmp_root_admin]	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in Cloud Provisioning and Governance**
Cloud-Administrator [sn_cmp.cloud_admin]	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle [sn_cmp.cloud_governor]	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer [sn.cmp.cloud_service_designer]	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer [sn_cmp.cloud_service_user]	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Ihnen zugewiesenen Aufgabendatensätze zugreifen, wenn Sie die Rolle „Cloud-Service-Anwender“ innehaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Cloud-Betreiber [sn_cmp.cloud_operator]	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration [sn_cmp.cloud_event_integration] **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator [sn_cmp.cloud_group_admin]	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift

Für den sicheren Zugriff auf Daten in Ihrem Providerkonto muss der Discovery-Prozess entsprechende Anmeldeinformationen bereitstellen. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst ein Konto in der VMware-Konsole. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

Vorbereitungen

Erforderliche Rollen:

- VMware-Konsole Administrator
- Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Anmeldeinformationen**an.
2. Klicken Sie auf der Registerkarte **Anmeldeinformationen** auf **Neu**, wählen Sie **VMware-Anmeldeinformationen** aus, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Felder des Formulars für VMware-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und aussagekräftiger Name für die Anmeldeinformationen (z. B. Cloud Management VMware-Anmeldeinformationen)
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Anmeldeinformationen zu aktivieren.
Benutzername	Benutzername für den Zugriff auf Ihr vSphere-Konto.
Passwort	Passwort für den Zugriff auf das vSphere-Konto

3. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Service-Konten**, Klicken Sie auf **Neu** , Geben Sie eine eindeutige und aussagekräftige ein **Name** (Beispiel: Cloud Provisioning-Service-Account), und füllen Sie dann das Formular aus.

Neuer Service-Account für VMware

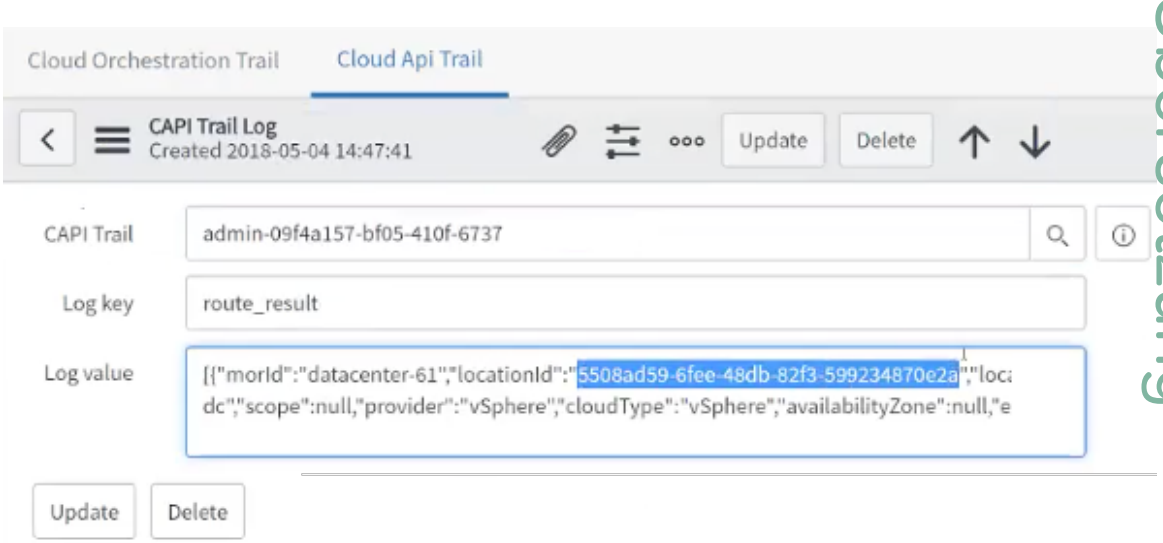
Account-ID	Es gibt zwei Methoden, den Wert festzulegen: ○ Wenn Sie Zugriff auf den Browser für verwaltete Objekte (Managed Object Browser, MOB) für das vCenter haben: Die Konto-ID ist die Instanz-UUID. Öffnen Sie die MOB, und klicken Sie dann auf **Inhalt** > **Über**an. Fügen Sie den Wert der Eigenschaft **instanceUuid** in das Feld **Konto-ID** ein. ○ Wenn Sie nicht auf den Managed Object Browser (MOB) zugreifen können, geben Sie in das Feld **Konto-ID** einen temporären alphanumerischen Text wie 5ca3033a-1290-4a02-8221-2c5f2f29be8b ein. In einem Schritt nach dieser Tabelle erstellen Sie den tatsächlichen Wert und kehren dann zu diesem Formular zurück, um den temporären Text durch den tatsächlichen Wert zu ersetzen.
Discovery-Anmeldeinformationen	Name der Anmeldeinformationen, die Sie im vorherigen Schritt erstellt haben. Im Beispiel: Cloud Provisioning VMware Credentials.
Rechenzentrums-URL	Vollständige URL des vCenters, z. B.: https://<IP-Adresse>/sdk.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datencenter-Typ	Wählen Sie **VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]** aus.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Sollte Events abrufen	Aktiviert Cloud Provisioning and Governance zum Sammeln von Events von Ressourcentypen im VMware vCenter-Rechenzentrum in der Liste `sn_cmp_cloud_event_list`.

4. Klicken Sie auf den zugehörigen Link **Rechenzentren erkennen**.
   Mit den Anmeldeinformationen greift Discovery auf das vCenter unter der angegebenen URL zu, um VMware-Rechenzentren zu erkennen.
5. Wenn Sie den UUID-Wert der Instanz im Feld **Konto-ID** verwendet haben, klicken Sie auf **Absenden** und überspringen Sie die verbleibenden Schritte in diesem Verfahren.
   Das System erstellt den Servicekonto und zeigt die Liste aller Servicekonten an.
6. Auf der Portal für Cloud-Admin., Navigieren Sie zu **Betreiben** > **Pfade**an.
7. Suchen Sie auf der Registerkarte **Cloud API-Pfad** den Eintrag mit dem Wert **ListDatacenters** für **Methodenname** und dem Wert **vmware-compute** für **Providername** (normalerweise der neueste Eintrag).
   Öffnen Sie den Eintrag.
8. Öffnen Sie in der zugehörigen Liste **CAPI-Pfadprotokolle** den Eintrag **route_result**.
9. Kopieren Sie im Textfeld **Protokollwert** den Wert für **locationId**.
   Dieser Wert ist die **Konto-ID**, die Sie im nächsten Schritt in das Formular einfügen.



10. Navigieren Sie in der -Instanz zu **Cloud-Adminportal** > **Verwalten** > **Service-Konten** Und klicken Sie dann auf ServicekontoDie Sie zuvor erstellt haben (`Cloud Provisioning-Service-Account` Im Beispiel).
11. Fügen Sie den Wert für **locationId** (den Sie aus dem Formular **CAPI-Pfadprotokoll** kopiert haben) in das Feld **Konto-ID** des Formulars ein, und klicken Sie dann auf **Aktualisieren**.
12. Klicken Sie auf **Absenden**.
    Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erkennung von VMware-Clouds

Einrichten Cloud-AccountsFür VMware

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

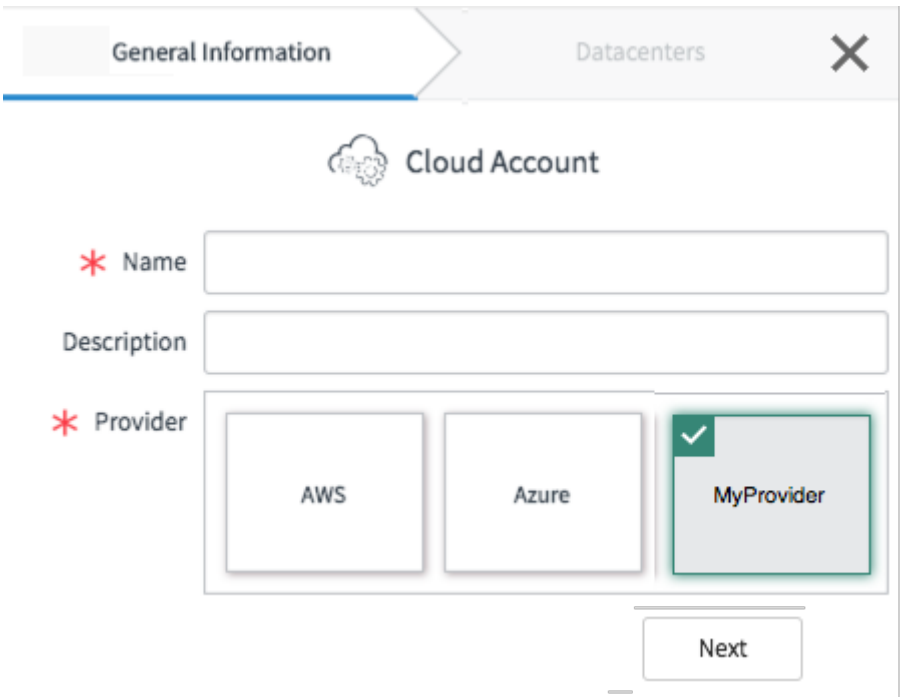
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Ausführliche Informationen finden Sie unter Cloud-Accounts.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und wählen Sie dann den Cloud-**Provider** für das Konto aus (VMware vCenter).



3. Klicken Sie auf **Next** (Weiter).
   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt, und eine Liste der ermittelten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um sie zu suchen. Weitere Detailinformationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
4. Wählen Sie ein oder mehrere Rechenzentren aus, die dem Cloud-Konto zugeordnet werden sollen, klicken Sie auf **Speichern**, und schließen Sie dann das Popup.
   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.
5. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Größe des Speichervolume und andere Services. Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen
- **Discovery-Protokoll**: Der Prozess erstellt einen Protokolldatensatz für jede Aktion in einem Rechenzentrum.

Hinweis:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind.

Nächste Maßnahme

Wiederholen Sie den Prozess, um zusätzliche zu erstellen Cloud-AccountsNach Bedarf. Führen Sie Discovery aus, und legen Sie Kapazitätsgrenzen für jedes Rechenzentrum fest.

Fügen Sie einem ein Rechenzentrum hinzu Cloud-Konto

Sie können der Cloud-Infrastruktur jederzeit ein logisches Rechenzentrum hinzufügen, das durch einen Cloud-Konto dargestellt wird.

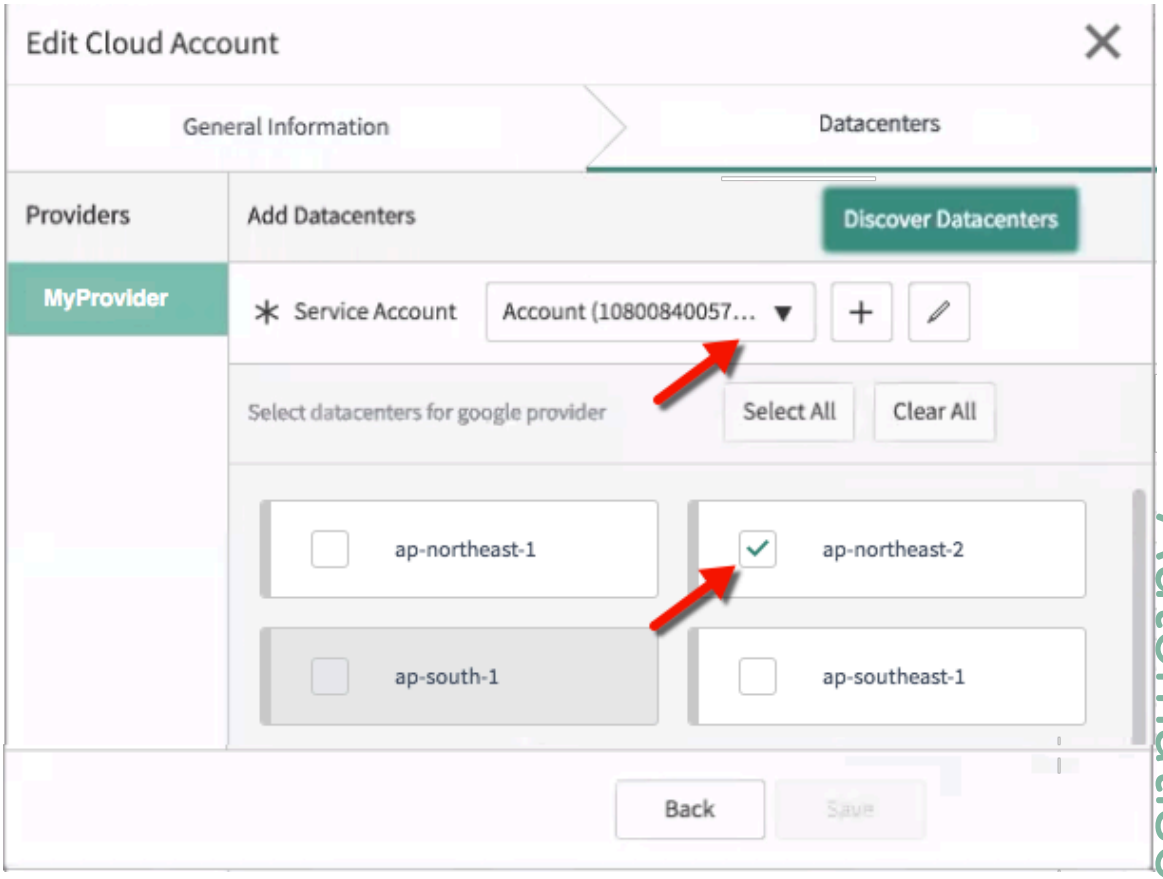
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.
2. Öffnen Sie einen Cloud-Konto, legen Sie den Status auf **Entwurf** fest, und klicken Sie dann im Formularheader auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Rechenzentren**, und wählen Sie dann das **Servicekonto** aus, der die Anmeldeinformationen enthält, die den Zugriff auf das Provider-Konto mit dem hinzuzufügenden Rechenzentrum ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie den Servicekonto auswählen, wird die Liste der erkannten Rechenzentren für den Servicekonto angezeigt.

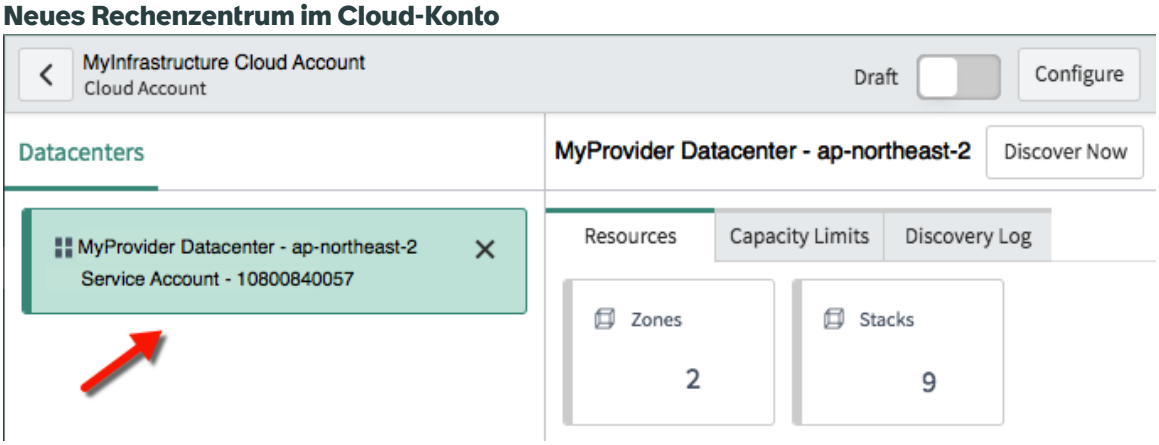
Hinweis: Wenn die erwarteten Rechenzentren nicht angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um die Liste zu aktualisieren. Discovery wird ausgeführt und zeigt alle mit dem Servicekonto verknüpften Rechenzentren an.

4. Wählen Sie die hinzuzufügenden Rechenzentren aus, und klicken Sie dann auf **Speichern**.
   Im Beispiel wählen Sie **ap-northeast-2** aus.

Ergebnis

Die Rechenzentren werden dem Cloud-Konto hinzugefügt und auf der Registerkarte **Rechenzentren** angezeigt. Wenn Discovery ausgeführt wird, werden die Ressourcen im Rechenzentrum auf der Registerkarte „Ressourcen“ angezeigt.

Neues Rechenzentrum im Cloud-Konto



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliches Setup von Cloud Provisioning and Governance an Tag 2

Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zusätzliche Setup- und Konfigurationsvorgänge

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zusätzliches Cloud-Konto einrichten

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Planen Sie die Discovery aller Ressourcen in einem Servicekonto

Fügen Sie einen anwenderdefinierten Zeitplan für hinzu Discovery Um alle Ressourcen in jedem Rechenzentrum in zu erkennen ServicekontoUnd aktualisieren Sie dann die CMDB mit den neuen Informationen.

Sie können die Discovery-Zeitpläne wie auf der Seite „Zeitplan für Cloud-Discovery“ angeboten verwenden.

Hinweis:

Ab dem Xanadu-Release führt jeder neue Anwender standardmäßig eine musterbasierte Discovery aus. In Szenarien, in denen die neueste Musteranwendung nicht installiert ist, schlägt die Discovery fehl, und der Systemadministrator wird aufgefordert, die CAPI-basierte Discovery zu installieren oder zu migrieren.

Wird Installiert Cloud Operations Workspace Löst die automatische Installation der neuesten Musteranwendung aus.

Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

Bei Bedarf alle Ressourcen in einem Rechenzentrum erkennen

Sie können jederzeit Discovery für ein Rechenzentrum ausführen, um die CMDB zu aktualisieren.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Zusätzliches Cloud-Konto einrichten

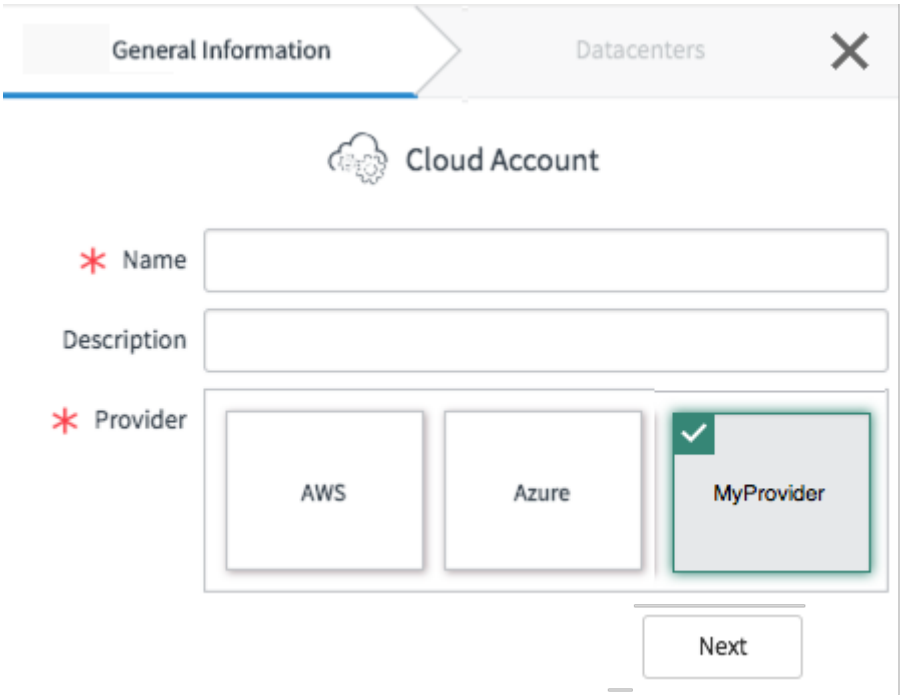
Während der Erstinstallation richten Sie einen Cloud-Konto ein. Zum Organisieren und Aufteilen Ihrer Infrastruktur können Sie zusätzliche Cloud-Accounts einrichten, um verschiedene Provider, Servicekonten oder Rechenzentren einzubeziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen. Ausführliche Informationen finden Sie unter Cloud-Accounts.

Prozedur
1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Cloud-Accounts**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, wählen Sie den Cloud-**Provider** für das Konto aus (im Beispiel **MyProvider**), und klicken Sie dann auf **Weiter**.

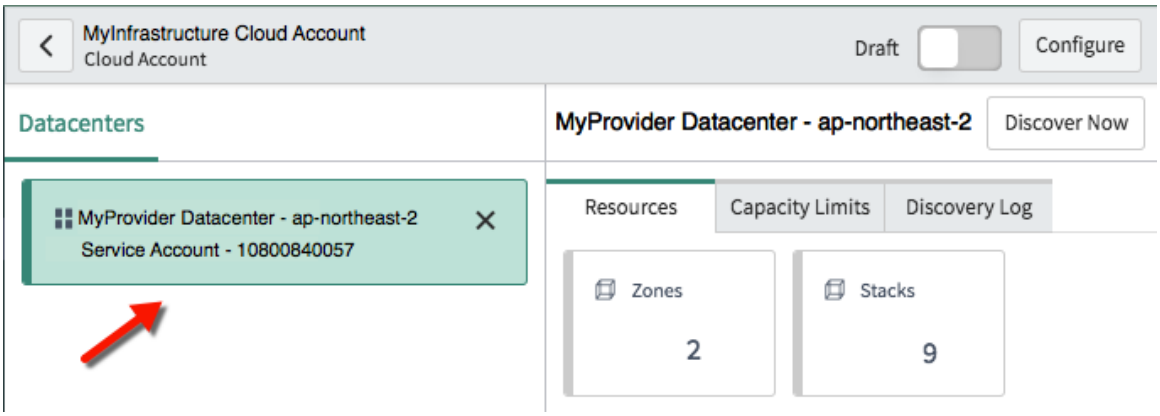


   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt.
3. Wählen Sie das entsprechende **Servicekonto** aus.
   Eine Liste der erkannten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Entdecken Sie Jetzt** . Details siehe Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
4. Wählen Sie alle Rechenzentren aus, die dem Cloud-Konto zugeordnet werden sollen, klicken Sie auf **Speichern**, und schließen Sie dann das Popup.

   Die Rechenzentren werden auf der Registerkarte **Rechenzentren** für den Cloud-Konto angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

Hinweis:

- Wählen Sie nur die LDC/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
- Um Ressourcen in Regionen/LDC zu erkennen, z. B. Nordamerika (US East, US West und Kanada Central), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik, stellen Sie mit eine Zugriffsanforderung für die erforderlichen Endpunkte GCP Support.

Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.

6. Klicken Sie auf ein Rechenzentrum.
Die folgenden Listen werden angezeigt:
   - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
   - **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
   - **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.
7. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Nächste Maßnahme

Wiederholen Sie den Prozess, um zusätzliche zu erstellen Cloud-AccountsNach Bedarf. Führen Sie Discovery aus, und legen Sie Kapazitätsgrenzen für jedes Rechenzentrum fest.

Erkennen Sie mithilfe von Cloud Operations-Arbeitsbereich und -Mustern

Sie können jetzt Discovery mit planen und durchführen Cloud Operations Workspace Und Muster für Discovery und Service-Mapping.

Vorbereitungen

Erforderliche Rolle: Systemadministrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Cloud Operations-Arbeitsbereich ist jetzt als bekannt Cloud Operations Workspace Oder CDW.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Überprüfen Sie, ob *Cloud Operations Workspace*(CDW) ist installiert.
2. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Discovery-Zeitpläne** > **ManageDiscovery-Zeitpläne**an.

   Befolgen Sie diese Szenarien für die nächsten Schritte.

Szenario	Nächste Schritte
Cloud-Discovery-Zeitpläne werden für die Systemadministratoranmeldung nicht angezeigt	○ *Cloud Operations Workspace* Ist nicht installiert. Die Seite, die darüber benachrichtigt *Cloud Operations Workspace*Muss installiert sein, wird angezeigt. ○ Die Seite fordert zu auf **Wechseln Sie zu Anwendungsmanager** Um die Installation zuzulassen
Cloud-Discovery-Zeitpläne werden für die Anmeldung mit sn_CMP Cloud Admin nicht angezeigt	○ *Cloud Operations Workspace* Ist nicht installiert. Die Seite, die darüber benachrichtigt *Cloud Operations Workspace*Muss installiert sein, wird angezeigt. ○ Die Seite fordert an, sich für an den Systemadministrator zu wenden *Cloud Operations Workspace*Installation.
Cloud-Discovery wird angezeigt	Cloud-Discovery-Zeitpläne werden auf einer neuen Registerkarte Ihres Browsers angezeigt.

3. Stellen Sie sicher, dass die Cloud-Administratorrolle sn_CMP die Rolle „sn_Cloud_OPS_WS.Cloud_OPS_admin“ enthält.
4. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Discovery-Zeitpläne**an.
5. Klicken Sie auf , und bestätigen Sie, wenn Discovery-Zeitpläne auf einer neuen Registerkarte geöffnet werden.
6. Stellen Sie sicher, dass der Cloud-Administrator sn_CMP standardmäßig die Seite „Discovery-Zeitpläne“ anzeigen kann.

Nächste Maßnahme

Installieren und verwenden Sie die neueste Muster für Discovery und Service-Mapping, Mindestens Version 1,15, als Standardmechanismus für die Ausführung Discovery.

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Nachdem Sie einen Service-Account eingerichtet haben, führen Sie aus Discovery Zum Ausfüllen der Rechenzentren im Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Cloud Operations Workspace, Und mindestens Version 1,15 von Muster für Discovery und Service-Mapping Von ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. Bei der Google Cloud Platform werden die bereichsspezifischen Container für virtuelle Ressourcen als *Regionen* bezeichnet. Im ServiceNow-Clouddatenmodell werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Sie können ausführen Discovery Bei Bedarf.

Wichtig: Verwenden Cloud Operations Workspace(CDW) zum Ausführen des Discovery-Zeitplans. Die UI-Aktion „Rechenzentrum erkennen“ ist veraltet, und der bevorzugte Ansatz besteht darin, Zeitpläne über CDW einzurichten.

Prozedur

1. Navigieren Sie zur Tabelle Cloud-Service-Accounts [cmdb_ci_Cloud_Service_Account_list].
   Weitere Informationen zum direkten Navigieren zu einer Tabelle finden Sie unter Navigieren Sie direkt zu einer Tabelle .
2. Wählen Sie den Service-Account aus, dessen LDCs Sie erkennen möchten.
3. Wählen Sie aus **Erstellen Sie Einen Discovery-Zeitplan** Zugehöriger Link.
4. Wählen Sie **Weiter**.
5. Wählen Sie Aus **Aktualisieren Sie Rechenzentren** .
6. Wählen Sie **Abbrechen**.
7. Wählen Sie den Service-Account aus, dessen LDCs Sie erkennen wollten.
   Bei erfolgreicher Rechenzentrums-Discovery wird das Feld Status der Rechenzentrums-Discovery auf festgelegt JJJJ-MM-TT HH:MM:SS: ABGESCHLOSSEN ⋯ Laden Sie dieses Formular neu, um eine aktualisierte Rechenzentrumsliste anzuzeigen .

Ergebnis

Die erkannten Rechenzentren werden in der zugehörigen Liste der logischen Rechenzentren angezeigt.

Zugehörige Informationen

Protokolle für horizontale Erkennung

Planen Sie die Discovery aller Ressourcen in einem Servicekonto

Fügen Sie einen anwenderdefinierten Zeitplan für hinzu Discovery Um alle Ressourcen in jedem Rechenzentrum in zu erkennen ServicekontoUnd aktualisieren Sie dann die CMDB mit den neuen Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Cloud Operations Workspace, Und mindestens Version 1,15 von Muster für Discovery und Service-Mapping Von ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

- Geplant Cloud-Discovery Erkennt nur Rechenzentren, die Teil von sind Servicekonto Wann der Zeitplan erstellt wird. Wenn seit der Erstellung des Zeitplans Rechenzentren hinzugefügt wurden, erkennt Discovery diese Rechenzentren nicht. Löschen Sie den alten Zeitplan und erstellen Sie jedes Mal einen Zeitplan, wenn sich die Rechenzentren in einem Servicekonto ändern.
- Discovery füllt die CMDB mit den erkannten Ressourcen und aktualisiert die entsprechenden Informationen auf der Registerkarte **Ressourcen**. Sie können sich die Discovery-Ergebnisse auf der Registerkarte **Discovery-Protokoll** ansehen.

Wichtig: Verwenden Sie Cloud Operations Workspace Zum Ausführen des Discovery-Zeitplans. Die UI-Aktion „Rechenzentrum erkennen“ ist veraltet, und der bevorzugte Ansatz besteht darin, Zeitpläne über CDW einzurichten.

Prozedur

1. In **Cloud-Administratorportal** Navigieren Sie zu **Verwalten** > **Discovery-Zeitpläne**an.
2. Wählen Sie **Cloud-Zeitplan hinzufügen** aus.
3. Wählen Sie auf der Seite „Konto hinzufügen“ den Cloud-**Provider** aus, und geben Sie einen eindeutigen, beschreibenden **Namen** für den Zeitplan ein.
4. In **Service-Account** Abschnitt auswählen **Wählen Sie Account Aus** Geben Sie den Service-Account an, und klicken Sie dann auf **Als Nächstes** .

   Hinweis: Wählen Sie aus, um einen Service-Account zu erstellen **Account Hinzufügen** Und füllen Sie dann das Formular aus. Weitere Informationen finden Sie im Setup-Leitfaden für Tag 1 unter den Prozess zum Einrichten eines Service-Accounts.

5. Geben Sie auf der Seite „Rechenzentren auswählen“ an, welche der Rechenzentren im Service-Account erkannt werden sollen, indem Sie die zu erkennenden Rechenzentren in verschieben **Ausgewählt** Liste oder durch Auswahl von **Erkennen Sie alle unten aufgeführten Rechenzentren** Um alle Rechenzentren in zu verschieben **Ausgewählt** Liste.
6. Klicken Sie auf **Next (Weiter)**.
7. Auf der Seite „Zeitplan“ erstellen geben Sie den Zeitpunkt und die Häufigkeit der Discovery an.

   Hinweis: Die Einstellung **Laufzeit** verwendet immer die Systemzeitzone.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Planausführungsoptionen

Häufigkeit	Beschreibung
Bei Bedarf	Wird nicht nach einem Zeitplan ausgeführt. Wählen Sie Aus **Entdecken Sie jetz** ist die Standardoption.
Täglich	Läuft jeden Tag. Verwenden Sie das Feld **Startzeit**, um die Uhrzeit anzugeben.
Wöchentlich	Läuft an einem bestimmten Wochentag. Verwenden Sie das Feld **Startzeit**, um die Uhrzeit an
Monatlich	Läuft an einem bestimmten Tag jedes Monats. Verwenden Sie das Feld **Tag**, um den Tag des M Feld **Startzeit**, um die Uhrzeit anzugeben. Wenn der festgelegte Tag nicht im Monat liegt, wir ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan nicht im Februar ausg
Regelmäßig	Wird jedes festgelegte Mal ausgeführt. Verwenden Sie **Wiederholungsinterval** in Tagen, Stunden, Minuten und Sekunden. Das erste Mal, wenn Discovery zu d Zeitpunkt ausgeführt wird. Die nachfolgenden Erkennungen werden nach Abla Zeitraums ausgeführt.
Einmal	Einmal ausführen, wie durch das Datum und die Uhrzeit festgelegt, die im festgelegt sind **Beg**
An Wochentagen	Läuft jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag. Verwenden Sie das Feld **Sta**
An Wochenenden	Läuft jeden Samstag und Sonntag. Verwenden Sie das Feld **Startzeit**, um die Uhrzeit auszuwä
Letzter Tag des Monats	Führen Sie den letzten Tag jedes Monats aus. Verwenden Sie das Feld **Startzeit**, um die Uhrz
Ende des Kalenderquartals	Läuft am 31. März, 30. Juni, 30. September und 31. Dezember. Verwenden Sie das Feld **Startz** Ändern Sie das Skript `DiscoveryScheduleRunType`, um das Datum zu ändern.
Nach Discovery	Ermöglicht die sequenzielle Staffelung des Zeitplans. Verwenden Sie diese Opt dem im Feld **Ausführen nach** bezeichneten Discovery auszuführen. Wählen Sie **Abbruch**, um anzugeben, dass diese Erkennung auch dann ausgeführt werden Discovery vor Abschluss abgebrochen wird. ◦ Diese Option ist nicht gültig, wenn Discovery Wird über DiscoverNow oder be erkennen“ gestartet. ◦ Sie können keinen inaktiven angeben Discovery Zeitplan. ◦ Sie können keine Schleife erstellen, indem Sie die Ausführung nach angeben Discovery. ◦ Dies Discovery Wird nicht ausgeführt, wenn **Ausführen nach** Discovery Wird n der Ausnahme, dass **Auch wenn abgebrochen** Das Kontrollkästchen ist aktiv abgebrochen.
Discovery abbrechen, wenn länger als	Zeitbegrenzung für die Ausführung der Discovery. Wenn die angegebene Zeit v verbleibenden Aufgaben für Discovery Werden abgebrochen, auch wenn Discov das Kontrollkästchen nicht aktiviert ist, wird Discovery Wird bis zum Abschluss beschränkt die Systemlast auf ein gewünschtes Zeitfenster.

8. Wählen Sie **Fertigstellen** und **Jetzt ausführen** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

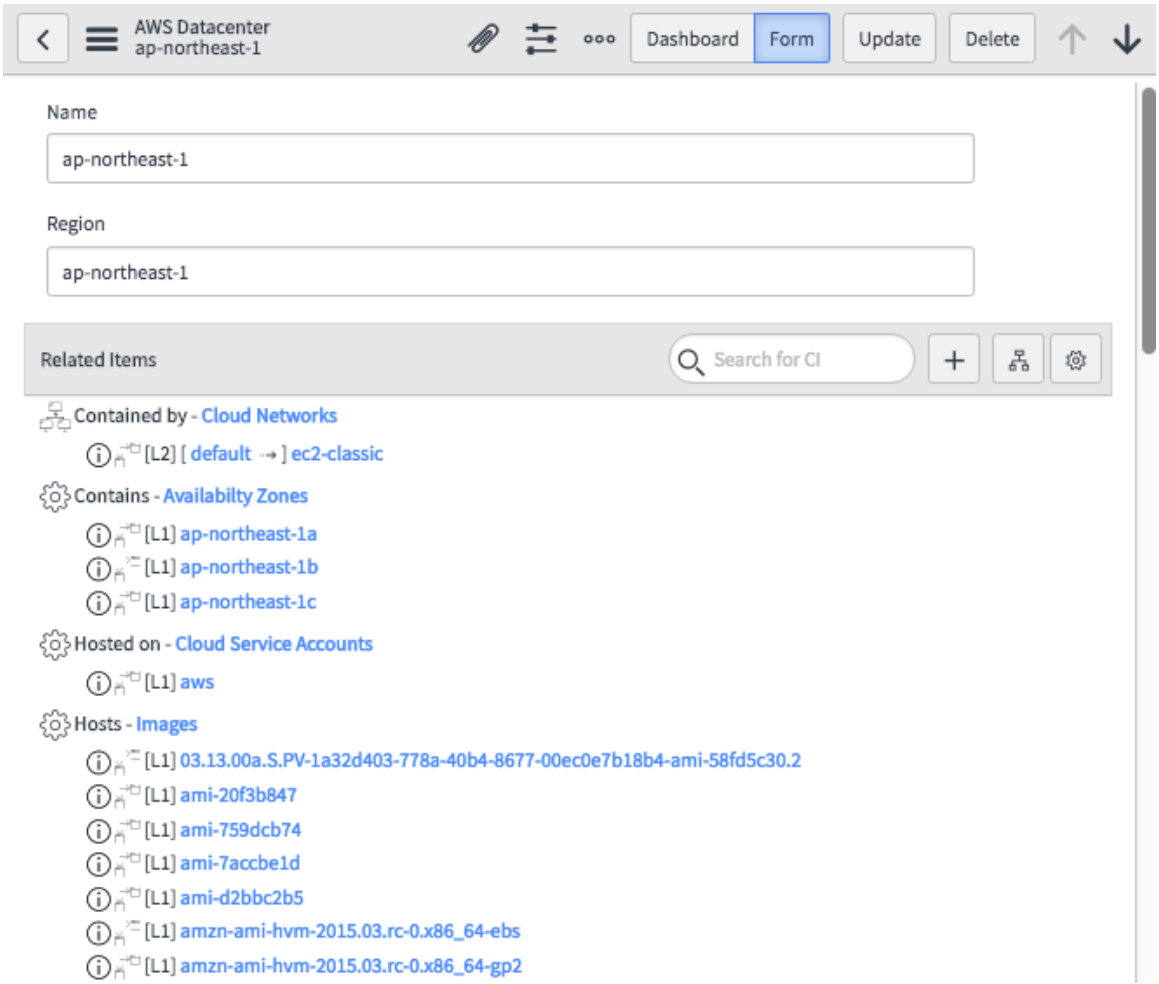
Ergebnis

Discovery wird sofort ausgeführt. Discovery wird zu den angegebenen Zeiten ausgeführt und fügt erkannte Rechenzentren der zugehörigen Liste „Logische Rechenzentren“ hinzu.

Wenn Sie einen Discovery-Zeitplan konfiguriert haben, wird dieser in der zugehörigen Liste „Discovery-Konfiguration – logische Rechenzentren“ angezeigt. Um Discovery für ein einzelnes Rechenzentrum auszuführen, fügen Sie das Rechenzentrum dem Discovery-Zeitplan in der zugehörigen Liste hinzu und führen Sie dann Discovery erneut aus.

Öffnen Sie einen Rechenzentrums-Datensatz, um die Beziehungen zwischen dem Rechenzentrum und den Ressourcen im Rechenzentrum anzuzeigen.

Ressourcen in einem AWS-Rechenzentrum



Hinweis: Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Wenn Sie in dieser Tabelle eine ungewöhnlich große Anzahl von Datensätzen feststellen, verwenden Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type], um die erkannten VM-Hardwaretypen zu speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren. Alle Funktionen von Cloud Provisioning and Governance wie Bereitstellung, Kontingente usw. funktionieren auch nach dem Wechsel zur Tabelle „Cloud-Hardwaretyp“ unverändert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Zum Anzeigen des Discovery-Status, der Discovery-Protokolle, der erkannten Geräte und der ECC-Warteschlange klicken Sie auf **Erweiterte Ansicht**.
- Wenn Discovery Schlägt fehl, überprüfen Sie die Cloud-Discovery-Ergebnisse auf der Discovery-Homepage.

Bei Bedarf alle Ressourcen in einem Rechenzentrum erkennen

Sie können jederzeit Discovery für ein Rechenzentrum ausführen, um die CMDB zu aktualisieren.

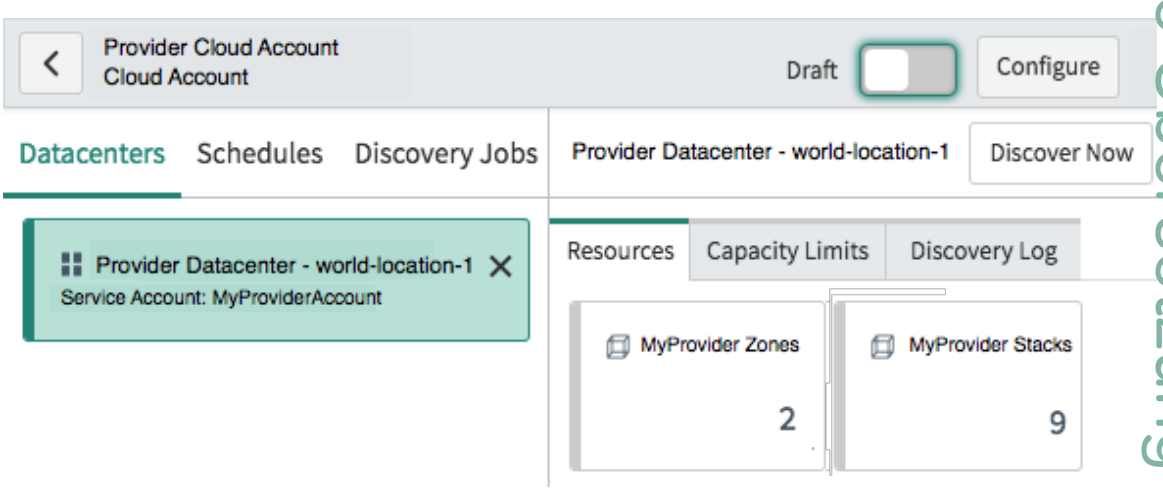
Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Cloud Operations Workspace, Und mindestens Version 1,15 von Muster für Discovery und Service-Mapping Von ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Cloud-Accounts**an.
2. Klicken Sie auf einen Cloud-Konto, und wählen Sie auf der Registerkarte **Rechenzentren** ein Rechenzentrum aus.
   Auf der Registerkarte **Ressourcen** werden die Ressourcen in der CMDB aufgeführt.



3. Ändern Sie den Status in **Entwurf**, und klicken Sie dann auf **Discovery starten**.
   Beachten Sie das **Entdecken Sie Jetzt** Ist deaktiviert, wenn weder CAPI noch Muster installiert sind. Befolgen Sie diese Szenarien, um fortzufahren.

> **Hinweis:** **Entdecken Sie jetzt** Wird auch mit einer Meldung deaktiviert, die Ihnen empfiehlt, die neueste zu installieren Muster für Discovery und Service-Mapping. Dies kann behoben werden, indem mindestens Version 1.15.1 installiert oder der manuelle Migrationsschritt ausgelöst wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Nächste Schritte
Entdecken Sie Jetzt Ist für die Systemadministratoranmeldung deaktiviert	○ Auf der Seite wird vorgeschlagen, dass Sie die neueste Musteranwendung installieren müssen, um fortzufahren. ○ Das Banner oben auf der Seite fordert Sie auf, zu besuchen **Wechseln Sie zu Anwendungsmanager** Zur Installation
Entdecken Sie Jetzt Ist für die Anmeldung bei sn_CMP Cloud Admin deaktiviert	○ Auf der Seite wird vorgeschlagen, dass Sie die neueste Musteranwendung installieren müssen, um fortzufahren. ○ Auf der Seite wird angefordert, den System–administrator für die Installation der Musteran–wendung zu kontaktieren.
Die Anwendung „neueste Muster“ ist installiert	„Jetzt erkennen“ ist aktiviert. **Hinweis:** Discovery verwendet jetzt Muster als Standardmechanismus.

4. Ausführen **Entdecken Sie Jetzt** Und warten Sie auf Discovery Zum Fertigstellen.
5. Ändern Sie den Status des Cloud-Kontos in **Veröffentlicht**.

Entdecken Sie jetzt Wird deaktiviert, wenn dieselbe Nachricht angezeigt wird. Dies kann behoben werden, indem die Version 1.15.1+ installiert oder der manuelle Migrationsschritt ausgelöst wird

Ergebnis

Discovery füllt die CMDB mit den erkannten Ressourcen aus und aktualisiert die Informationen auf der Registerkarte **Ressourcen**. Sie können sich die Discovery-Ergebnisse auf der Registerkarte **Discovery-Protokoll** ansehen.

Hinweis: Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Wenn Sie in dieser Tabelle eine ungewöhnlich große Anzahl von Datensätzen feststellen, verwenden Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type], um die erkannten VM-Hardwaretypen zu speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren. Alle Funktionen von Cloud Provisioning and Governance wie Bereitstellung, Kontingente usw. funktionieren auch nach dem Wechsel zur Tabelle „Cloud-Hardwaretyp“ unverändert.

Zugehörige Informationen

Discovery-Protokoll anzeigen

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Cloud Operations Workspace, Und mindestens Version 1,15 von Muster für Discovery und Service-Mapping Von ServiceNow Store.

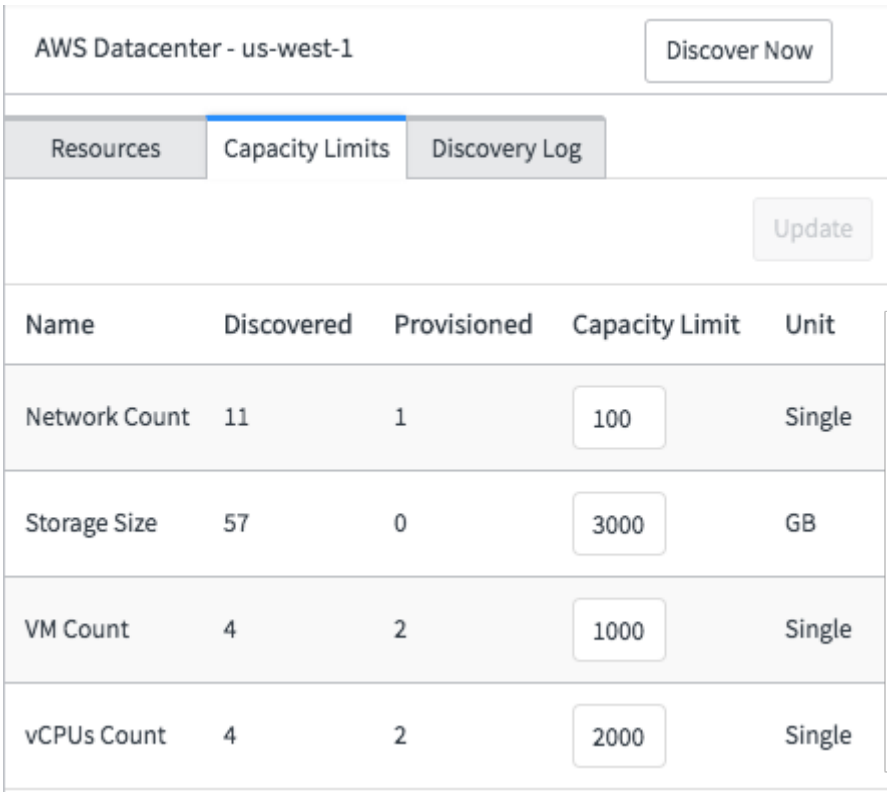
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Sie können auch Kontingente verwenden, um Beschränkungen pro Benutzer und eine Gesamtkapazität für Ressourcen festzulegen. Weitere Informationen finden Sie unter Kontingente und Steuerungen für Ressourcenbestellungen.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Verwalten** > **Cloud-Accounts**an.
2. Klicken Sie auf einen Cloud-Konto, und wählen Sie auf der Registerkarte **Rechenzentren** ein Rechenzentrum aus.
3. Legen Sie den Status auf **Entwurf** fest.
4. Legen Sie auf der Registerkarte **Kapazitätsgrenzen** die **Kapazitätsgrenzen** nach Bedarf fest.



Wert	Beschreibung
Erkannt	Vom Discovery-Prozess erkannter Gesamtwert für alle Ressourcen im ausgewählten Servicekonto.
Bereitgestellt	Gesamtwert, der für den ausgewählten Servicekonto bereitgestellt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Kapazitätsgrenze	Maximal zulässiger Wert, berechnet als Summe für alle Ressourcen im ausgewählten Servicekonto.
Einheit	Maßeinheit für den angegebenen Wert. Beispielsweise wird Speicher in GB gemessen.

5. Klicken Sie auf **Aktualisieren**.
6. Legen Sie den Status auf **Veröffentlicht** fest.

Nächste Maßnahme
Klicken Sie auf **Discover starten**, um Discovery für die logischen Rechenzentren auszuführen.

Verwenden Sie Besitzer- und Zuweisungsgruppen

Sie müssen die Anwendergruppen in einrichten und verwenden Cloud Provisioning and Governance Als Teil der Aufgabe „Tag 2“.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Besitzergruppe: Wird in der Quotenverwaltung verwendet. Während einer Stapelbereitstellung muss der Anwender die „Anwendergruppe“ im Bestellformular auswählen. Eine Kontingentprüfung wird basierend auf der im Formular ausgewählten Anwendergruppe durchgeführt, und diese Anwendergruppe wird später als Stapel „Besitzergruppe“ in der Tabelle „sn_CMP_Stack“ hinzugefügt. Quotenprüfungen können auf Anwendergruppenebene definiert werden. Weitere Einzelheiten finden Sie unter Kontingente und Steuerungen für Ressourcenbestellungen.

Hinweis: Wenn der Stapel gelöscht wird oder sich das Besitzergruppenfeld für den Stapel ändert, wird das Kontingent neu berechnet. Die Quote wird in der Geschäftsregel neu berechnet: Verbrauchte Quote bei Stapelaktualisierung neu berechnen.

Gruppe zuweisen: Die Discovery-Zeitplanausführungen bringen die aus anderen Instanzen erstellten Ressourcen in Ihre Instanz. Diese Ressourcen werden nicht verwaltet. In ähnlicher Weise erstellt die geplante Aufgabe „Tag-Zuweisungen ausfüllen“ nicht verwaltete Stapel. Um diese Stapel und Ressourcen zu verwalten, können Sie ihnen eine Change-Gruppe zuweisen.

Weisen Sie eine Change-Gruppe einem nicht verwalteten Stapel oder einer nicht verwalteten Ressource zu, um sie in sichtbar zu machen **Cloud-Anwenderportal** , Mit der Sie Tag 2-Vorgänge für diese Ressource ausführen können.

Prozedur

1. Navigieren Sie zu **Cloud-Anwenderportal** .
2. Klicken Sie Auf **Stapel Anzeigen** Und navigieren Sie zu **Erkannte Stapel** Für nicht verwaltete Stapel.
3. Klicken Sie Auf **Zeigen Sie Ressourcen An** Und navigieren Sie zu **Virtuelle Computer** Für nicht verwaltete Ressourcen.
4. Ändern Sie die Ansicht in **Meine Gruppen** .
5. Wählen Sie einen der virtuellen Computer aus, und führen Sie den Tag 2-Vorgang aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance-Administrationsleitfaden

Nachdem Sie die Anwendung Cloud Provisioning and Governance auf Ihrer Instanz eingerichtet haben, müssen Sie viele Elemente konfigurieren, bevor Ihre Benutzer Cloud-Ressourcen anfordern und verwalten können.

Anforderungen

Rolle, die zur Verwendung von erforderlich ist Cloud Provisioning and Governance Administrationsleitfaden ist „Cloud_admin“.

Bevor Sie beginnen

Cloud Provisioning and Governance einrichten

Weitere Informationen finden Sie im entsprechenden Setup-Leitfaden für Ihren Cloud-Provider:

- Cloud Provisioning and Governance Setup-Leitfaden für AWS
- Cloud Provisioning and Governance Setup-Leitfaden für Azure
- Cloud Provisioning and Governance Setup-Leitfaden für VMware

an.

Aktionen nach dem Setup

Erstellen Ressourcenprofile

Ressourcenprofile enthalten die Attribute, die eine Ressource haben kann. Benutzer wählen Werte für diese Attribute aus, wenn sie eine Cloud-Ressource bestellen. Sie können die folgenden Typen von Ressourcenprofilen konfigurieren: Computing (z. B. Größe einer VM), Betriebssystem (z. B. Typ und Version), Speicher (z. B. Sicherung) und Sicherheitsgruppen (z. B. Verwenden von HTTPS). Weitere Informationen finden Sie unter Ressourcenprofile.

Governance konfigurieren

Governance-Tools, mit denen Sie die Bereitstellung von Cloud-Ressourcen einschränken können, umfassen unter anderem Kontingente und Richtlinien. Beispiele für Dinge, die Sie konfigurieren können, sind der Genehmigungs-Subflow, der verwendet wird, nachdem ein Anwender eine Cloud-Ressource angefordert hat, ob eine E-Mail gesendet wird, nachdem eine Cloud-Ressource gestoppt wurde, und welches Rechenzentrum automatisch ausgewählt werden soll, wenn ein Anwender eine Ressource von einem bestimmten Cloud-Anbieter auswählt. Weitere Informationen finden Sie unter Cloud-Governance.

Cloud-Servicekatalog ausfüllen

Nachdem Sie Governance-Kontingente und -Richtlinien angewendet haben, erstellen Sie Servicekatalogelemente. Sie haben folgende Möglichkeiten, um ein Katalogelement zu erstellen:

- Vorlagen aus AWS oder Microsoft Azure importieren
- Basissystem-Katalogelement verwenden oder ändern
- Terraform-Vorlage verwenden

Domain Separation und Cloud Provisioning and Governance

Die Domänentrennung wird in Cloud Provisioning and Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Cloud Provisioning and Governance Domänentrennung – Übersicht

Alle Tabellen in Cloud Provisioning and Governance sind nicht domänengetrennt. Delegierte Domänentrennung wird nicht unterstützt.

Domänentrennung für Cloud Provisioning and Governance unterstützt:

Service Provider (SPs), die die Anwendung zur Bereitstellung von Datentrennung verwenden.

In diesem Szenario kann ein SP Datentrennung für mehrere Kunden anbieten, wobei Domänen erforderlich sind, um alle relevanten Kundendaten und -prozesse zu enthalten. Beispielsweise bietet ein SP Support für Kunden, die normalerweise Cloud Provisioning and Governance für die Verwaltung ihrer IT-Infrastruktur in der Cloud verwenden. SPs können ihren Kunden Kataloge, Vorlagenprofile, Ressourcenpools und -filter, Ressourcenprofile, Kontingente, Berechtigungen, IP-Adressenverwaltung (IPAM), Miet- und Geschäftszeitenplanung und Abrechnungsansicht als domänengetrennte Angebote bieten.

So funktioniert Domain Separation in Cloud Provisioning and Governance

Die Domänentrennung für Cloud Provisioning and Governance richtet ein oder mehrere Unternehmen an einer Domäne aus. Zur Verwendung der Domänentrennung in der Anwendung weisen Sie alle Benutzerkonten einem bestimmten Unternehmen zu, das dieser Domäne zugeordnet ist.

Alle mit dem Unternehmen verknüpften Entitäten, z. B. Cloud-Konten und Servicekonten, werden in derselben Domäne wie das Unternehmen erstellt. Wenn ein neues Unternehmen erstellt wird, erstellen Sie eine Domäne mit einem eindeutigen Namen und weisen Sie sie dem Unternehmen zu. Alle zugehörigen Entitäten für ein Konto, z. B. Kontakte und Fälle, müssen sich in derselben Domäne befinden. Wenn eine zugehörige Entität für ein domänengetrenntes Konto erstellt wird, wird die Entität der Unternehmensdomäne zugewiesen.

Mitglieder einer Domäne können nur die Daten aufrufen, die in ihrer Domäne oder in untergeordneten, in der Domänenhierarchie niedriger angesiedelten Domänen enthalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, sofern Sie sie nicht einer bestimmten Domäne zuweisen. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können nur Daten in ihrer eigenen oder einer untergeordneten Domäne anzeigen lassen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen lassen können. Delegieren Sie die Verwaltung nicht an Cloud-Administratorbenutzer der untergeordneten Domänen in Cloud Provisioning and Governance.

Domänentrennung für Cloud Provisioning and Governance einrichten

Aktivieren Sie die folgenden Plugins:

Plugin „Domain Support – Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer), um Domänentrennung in Cloud Provisioning and Governance zu ermöglichen.

Plugin „Service Catalog – Domänentrennung“ (glideapp.servicecatalog.domain_separation), um die Trennung von Katalogelementen in unterschiedlichen Domänen in Cloud Provisioning and Governance zu ermöglichen.

Änderungen an Cloud Provisioning and Governance-Tabellen

Die Domänentrennung für Cloud Provisioning and Governance fügt den Listenansichten die Felder **Domäne** und **Domänenpfad** hinzu. Diese Felder werden standardmäßig nicht verfügbar gemacht. Als Domänenadministrator können Sie Listen und Formulare anpassen, um diese Felder anzuzeigen. Nicht alle Tabellen in Cloud Provisioning and Governance sind domänengetrennt. Während einige Tabellen der obersten Ebene domänengetrennt sind, sind mehrere untergeordnete Tabellen nicht domänengetrennt. Dies hat jedoch keinen Einfluss darauf, wie die Anwendung Cloud Provisioning and Governance in einem domänengetrennten Kontext funktioniert.

Konto-Domänen und zugehörige Entitäten

Beim Erstellen zugehöriger Entitäten für ein Konto wird die Domäne für die zugehörigen Entitäten auf die Kontodomäne festgelegt.

Domänensichtbarkeit für Cloud-Administratoren und -Benutzer

Weisen Sie Benutzer mit den Rollen „Cloud-Benutzerportal“ (sn_cmp.cloud_service_user) und „Cloud-Adminportal“ (sn_cmp.cmp_root_admin) für jede Domäne manuell der Domäne **TOP/MSP/Standard/Unternehmen** oder der Blattdomäne zu. Domänenadministratoren und Benutzer in Cloud Provisioning and Governance können Daten nur in der Domäne anzeigen, in der sie erstellt wurden, bis sie der TOP-Domäne zugewiesen werden. Die Top-Domäne stellt eine einzige gemeinsame übergeordnete Domäne dar, die als einzelner übergeordneter Knoten für die Service Provider-Domänen fungiert.

Nächste Schritte

Weitere Informationen zum Erstellen, Implementieren und Verwalten der Domänentrennung für Cloud Provisioning and Governance-Services in der Instanz, die Sie für Ihre Kunden einrichten, finden Sie unter Domänentrennung in Cloud Provisioning and Governance– Überlegungen für Service Provider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Domänentrennung in Cloud Provisioning and Governance– Überlegungen für Service Provider

Berücksichtigen Sie die folgenden Überlegungen, um die Domänentrennung für Cloud Provisioning and Governance-Services in der Instanz, die Sie für Ihre Kunden einrichten, effektiv zu erstellen, zu implementieren und zu verwalten.

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

So funktioniert Domain Separation in Cloud Provisioning and Governance

Die Domänentrennung für Cloud Provisioning and Governance richtet ein oder mehrere Unternehmen an einer Domäne aus. Zur Verwendung der Domänentrennung in der Anwendung weisen Sie alle Benutzerkonten einem bestimmten Unternehmen zu, das dieser Domäne zugeordnet ist.

Alle mit dem Unternehmen verknüpften Entitäten, z. B. Cloud-Konten und Servicekonten, werden in derselben Domäne wie das Unternehmen erstellt. Wenn ein neues Unternehmen erstellt wird, erstellen Sie eine Domäne mit einem eindeutigen Namen und weisen Sie sie dem Unternehmen zu. Alle zugehörigen Entitäten für ein Konto, z. B. Kontakte und Fälle, müssen sich in derselben Domäne befinden. Wenn eine zugehörige Entität für ein domänengetrenntes Konto erstellt wird, wird die Entität der Unternehmensdomäne zugewiesen.

Mitglieder einer Domäne können nur die Daten aufrufen, die in ihrer Domäne oder in untergeordneten, in der Domänenhierarchie niedriger angesiedelten Domänen enthalten sind. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, sofern Sie sie nicht einer bestimmten Domäne zuweisen. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können nur Daten in ihrer eigenen oder einer untergeordneten Domäne anzeigen lassen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen lassen können. Delegieren Sie die Verwaltung nicht an Cloud-Administratorbenutzer der untergeordneten Domänen in Cloud Provisioning and Governance.

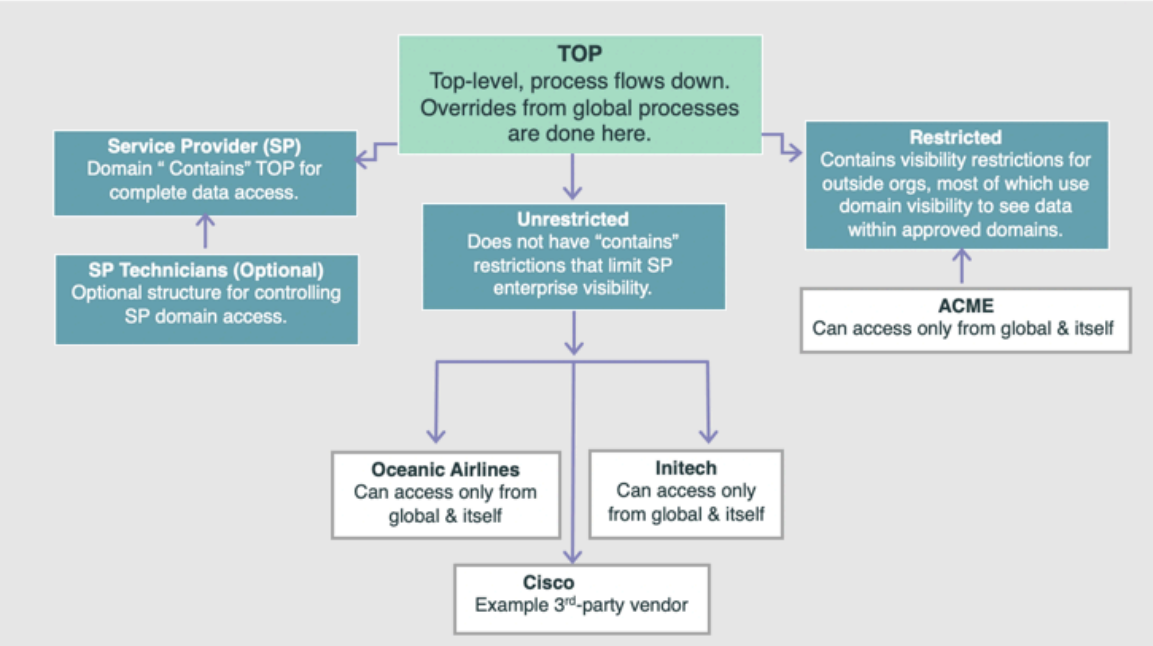
Poolfilter, Ressourcenprofil, Abrechnung, Kontingent, Berechtigungen, IPAM, Budget und Benachrichtigungen sind domänengetrennt. Nicht alle Tabellen in Cloud Provisioning and Governance sind domänengetrennt. Während die meisten Tabellen der obersten Ebene domänengetrennt sind, sind mehrere untergeordnete Tabellen nicht domänengetrennt. Die Tatsache, dass nicht alle Tabellen domänengetrennt sind, wirkt sich jedoch nicht auf das Funktionieren der Anwendung in einem domänengetrennten Kontext aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung: Ändern Sie die blaupausenbezogenen Tabellen nicht direkt in den Tabellendatensätzen.

Überlegungen zum Instanz-Setup für Service Provider

Die Domänentrennung bietet zwar Unterstützung für mehrere Mandanten, die Mehrmandantenfähigkeit ist jedoch auch weiterhin in einer einzelnen Instanz enthalten. Einige globale Eigenschaften, Daten und Prozesse werden über alle Domänen hinweg gemeinsam genutzt. Die folgende Abbildung zeigt die Hierarchie der Domänentrennung für uneingeschränkte und eingeschränkte Anwendungsfälle.



Führen Sie die folgenden Aufgaben aus, um Ihre domänengetrennte Instanz einzurichten:

- **Erstellen Sie eine Domäne.**

    - Sie können beliebig viele Domänen erstellen, stellen Sie jedoch sicher, dass Sie keine unnötigen Domänen auf der Instanz erstellen. Eine große Anzahl von Domänen auf der Instanz kann die Leistung beeinträchtigen. Bevor Sie neue Domänen erstellen, überprüfen Sie die Domänenhierarchie unter **Domänenadministrator** > **Domänenzuordnung**an. Überprüfen Sie, ob Sie tatsächlich eine neue Domäne erstellen müssen oder ob stattdessen eine vorhandene Domänenhierarchie verwendet werden kann.

      Wählen Sie eine primäre Domäne aus, um die Domäne der obersten Ebene in der Domänenzuordnung anzugeben. Die Top-Domäne stellt eine einzige gemeinsame übergeordnete Domäne dar, die als einzelner übergeordneter Knoten für die Service Provider-Domänen fungiert. Weitere Informationen finden Sie unter Wählen Sie eine primäre Domäne aus .

    - Erstellen Sie die SP-Domäne unter der Top-Domäne, und legen Sie die Domäne als Standard fest. Die Organisation Ihrer Domänen ist ein wichtiger Teil des Domänentrennungsprozesses. Stellen Sie sicher, dass Sie sich der Wichtigkeit bewusst sind, einen Standard festzulegen. Das System weist der Standarddomäne automatisch Aufgaben- und Benutzerdatensätze zu, die noch keiner Domäne zugewiesen sind. Weitere Informationen finden Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unter Legen Sie eine Domäne als Standard fest Für Anweisungen zum Erstellen einer Standarddomäne.

- Erstellen Sie eine Domänenhierarchie. Weitere Informationen finden Sie unter Erstellen Sie eine Domänenhierarchie .

  Erstellen Sie eine Domänenhierarchie, die Organisationsstrukturen widerspiegelt, um die Gruppierung unter der obersten Domäne zu übernehmen. Da Sie Discovery und Bereitstellung nur von der Blattdomäne aus ausführen können, richten Sie Blattdomänen in der Hierarchie ein, die konkrete Entitäten und Organisationen darstellen.

  Basierend auf der Domänenhierarchie haben Benutzer Zugriff auf Daten in ihrer Stammdomäne und allen untergeordneten Domänen. Der Prozess-Flow ist nach unten gerichtet, während der Daten-Flow nach oben gerichtet ist. Sie können Benutzerdatensätzen einen Domänenwert zuweisen, der die Stammdomäne des Benutzers darstellt. Benutzer haben zwar keinen Zugriff auf Daten in übergeordneten Domänen, Peer-Domänen oder Domänen in anderen Zweigen der Hierarchie. Ein Prozess, der in einer übergeordneten Domäne eingerichtet ist, gilt aber für alle untergeordneten Domänen. Weitere Informationen finden Sie unter

  - Referenzarchitektur des Service Providers
  - Architekturdaten der Domänentrennung

  Kundendaten sind basierend auf Domänenhierarchien betroffen:

  - Über-/untergeordnet: betroffener Prozess und betroffene Daten
    - Design, das auf einem Prozess-Flow basiert.
    - Denken Sie daran, dass die übergeordneten Domänen auf alle Daten in den untergeordneten Domänen zugreifen können.
  - Domäne „Enthält“: Nur Daten sind betroffen. Beispiel: Wenn SP im Diagramm „TOP“ enthält, werden Prozesse in SP nicht in der Domäne „TOP“ und abwärts ausgeführt.
    - Gewährt Personen in Gruppen Datenzugriffsrechte, die dedizierten Zugriff auf bestimmte Domänen erfordern.
    - Enthält Ursachen oder Bedingungen, die Datenbankabfragen hinzugefügt werden sollen, die Leistungsprobleme bei großen Domänen und Datensätzen verursachen können
  - Sichtbarkeit: Hierarchie, die für Benutzer immer sichtbar ist, sobald Sie Zugriff gewähren. Nur die Daten sind betroffen, nicht die Prozesse.
    - Gewährt einer anderen Domäne, die beim Erstellen der über- und untergeordneten Hierarchie keinen Zugriff hatte, Datenzugriff auf eine Domäne
    - Ermöglicht es Benutzern, alle Daten in den Domänen zu sehen, für die sie Sichtbarkeitszugriff haben, und zwar jederzeit, unabhängig von dem Datensatz, an dem sie gerade arbeiten

    Hinweis: Gehen Sie sparsam damit um, da mit „Sichtbarkeit“ vollständiger Zugriff gewähren werden kann, was Sie möglicherweise nicht beabsichtigen.

- Neues Unternehmen hinzufügen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Unternehmen hinzufügen, die Lieferanten, Hersteller oder Kunden repräsentieren, mit denen Sie Geschäfte tätigen. Diese Unternehmen bieten eine Möglichkeit, Benutzer, Gruppen und Assets zu kategorisieren.

Erstellen Sie Unternehmen und Blattdomänen für jeden Kunden, den Sie auf einer einzelnen Instanz unterstützen. Unternehmen helfen Ihnen, Benutzer mit der Domäne zu verknüpfen. Unternehmen und Domäne müssen entweder eine Eins-zu-Eins-Zuordnung oder eine Viele-zu-Eins-Zuordnung aufweisen. Dies macht das Zuweisen von Benutzern zu einer Domäne für SPs einfacher und überschaubarer.

Wichtig: Wenn Sie ein Unternehmen für jede Domäne erstellen, verwenden Sie ein Präfix mit einem eindeutigen Bezeichner, z. B. „COMPANY_“ oder „ORG_“.

Zum Anpassen der ServiceNow-Instanz für jedes Unternehmen können Sie Telefonnummern, Adressen und zusätzliche Hinweise eingeben. Sie können auch das Unternehmenslogo und den Bannertext anpassen, die Ihren Endbenutzern oben auf jeder Seite angezeigt werden. Weitere Informationen finden Sie unter Erstellen Sie ein neues Unternehmensprofil .

- Erstellen Sie Benutzergruppen, und weisen Sie den Benutzern jedes neuen Unternehmens Rollen und eine Domäne zu. Sie weisen Unternehmen Benutzer zu, um sie Domänen zuzuordnen. Ordnen Sie einem Unternehmen einen Benutzer zu, um den Benutzer einer Domäne zuzuordnen.

  1. Navigieren zu **Organisationen** > **Unternehmen,** Und klicken Sie auf **Neu** Um neue Anwender zu erstellen. Weitere Informationen zum Erstellen von Anwendern finden Sie unter . Erstellen Sie einen Anwender

     Hinweis: Verwenden Sie nicht die Option für manuell verwaltete Domänen, um die Domäne für Benutzer auszuwählen.

  2. Erstellen Sie Gruppen, und weisen Sie den Gruppen Rollen zu. Benutzer, die der Gruppe zugewiesen sind, erben die Rollen. Sie können Cloud-Benutzerportal-Benutzer für ein Unternehmen in der Blattdomäne erstellen. Weitere Informationen zum Erstellen von Gruppen finden Sie unter Erstellen Sie eine Anwendergruppe .
  3. Erstellen Sie diese Benutzer in jeder der Blattdomänen:
     - MID Server-Benutzer für jede Blattdomäne und jedes Unternehmen. Weisen Sie MID-Server-Benutzern die Rolle „mid_server“ zu.
     - Domänenadministrator für jede Blattdomäne und jedes Unternehmen. Weisen Sie Cloud-(Domänen-)Administratoren die Rolle „sn_cmp.cmp_root_admin“ zu.
     - Domänenbenutzer für jede Blattdomäne. Weisen Sie Cloud-Benutzern die Rolle „sn_cmp.cloud_service_user“ zu.
     - (Optional) Erstellen Sie Benutzer für zusätzliche Rollen in Blattdomänen (Rollen wie Designer, Kontrolle).

       Um bestimmten Benutzern eingeschränkte Sichtbarkeit für bestimmte Domänen bereitzustellen, fügen Sie sie über Gruppen hinzu. Weitere Informationen finden Sie unter Gewähren Sie einem einzelnen Anwender Sichtbarkeitsdomänen .
  4. Erstellen Sie eine Domänenbeziehung „Enthält“ zwischen der SP-Domäne und der TOP-Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Indem Sie eine Beziehung vom Typ „Enthält“ erstellen, ermöglichen Sie allen Administratoren in der Service Provider-Domäne Zugriff auf alle Domänendaten. Benutzer der globalen Domäne können keine Daten aus dem Kartenlayout sehen, da die Erweiterung des Domänenbereichs standardmäßig nicht zulässig ist.

Weitere Informationen dazu, wie Sie steuern können, was bestimmte Anwender und was eine ganze Anwenderdomäne anzeigen kann, finden Sie unter Sichtbarkeitsdomänen und enthält Domänen .

Nächste Schritte

Weitere Informationen zum Onboarding von Kunden oder Unternehmen in einer domänengetrennten Instanz für Cloud Provisioning and Governance Services, siehe Onboarding eines Unternehmens.

Zugehörige Informationen

Domain Separation

Domänentrennung verstehen

Onboarding eines Unternehmens

Prüfen Sie die folgenden Überlegungen zum Onboarding von Kunden oder Unternehmen in einer domänengetrennten Instanz für Cloud Provisioning and Governance-Services.

Domänentrennung für Cloud Provisioning and GovernanceÜbersicht

Die Domänentrennung für Cloud Provisioning and Governance soll Service Providern eine mehrmandantenfähige Instanzarchitektur bieten, die ihren Kunden Angebote effizient und sicher bereitstellt. Starke allgemeine Prozessstandards, datenbasiertes Prozessdesign, strikte Governance und zentralisierte Administration maximieren diese Vorteile.

Kundenonboarding durch Service Provider

- Erstellen Sie den MID-Server-Anwender, und gewähren Sie die Rolle .

Die Domänentrennung in Cloud Provisioning and Governance erfolgt durch die Installation und Konfiguration von mindestens einem dedizierten MID Servers für jedes Unternehmen/jede Domäne, die Sie in Ihrer Instanz verwalten. Durch Angabe eines MID-Server s für jede Domäne/jedes Unternehmen wird sichergestellt, dass Konfigurationselemente (Configuration Items, CIs) der gewünschten Domäne zugewiesen werden. Für jede Domäne ist mindestens ein MID Servers für Cloud Discovery, Bereitstellung und andere Orchestrierung eingerichtet.

Hinweis: Erstellen Sie in der globalen Domäne einen MID-Server, damit Sie Ziele in anderen Domänen untersuchen können. Weitere Informationen finden Sie unter Richten Sie die Domänentrennung für MID-Server ein

Der MID Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. Die MID-ServerAktiviert die Kommunikation und die Verschiebung von Daten zwischen ServiceNow®Instanz und externe Anwendungen, Datenquellen und Services.

Für die Kommunikation mit der Instanz benötigen MID Server eine Benutzer-ID und die entsprechende Rolle. Erstellen Sie die Benutzer-ID für einen MID Server, und geben Sie der ID die Rolle **mid_server**. Um ein Fehlschlagen der MID Server-Validierung zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verhindern, werden vom System Geschäftsregeln zur Überwachung der für MID Server-Benutzer ausgewählten Einstellungen ausgeführt.

- Einrichten von MID-Server an.

  Weitere Informationen zum Einrichten des MID-Server s finden Sie unter:

  - Installieren von MID-Server
  - Konfigurieren MID Servers

- Ressourcenblöcke in Cloud Provisioning and Governance

  Erstellen Sie Ressourcenblöcke in der globalen Domäne, da zwischen CI und Ressourcenblock eine 1:1-Beziehung besteht. Erstellen Sie keine Ressourcenblöcke in einer der untergeordneten Domänen oder Blattdomänen. Ressourcenblöcke fungieren als Prozessdatensatz, sodass jede Vorlage einer übergeordneten Domäne in der untergeordneten Domäne sichtbar ist und funktioniert.

  Ressourcenblöcke fungieren als eine Art Middleware-Komponente zwischen Katalogelementen, der Cloud-API (CAPI) und der CMDB.

  - Wenn die Blöcke im Basissystem nicht die erforderlichen Cloud-Ressourcen bereitstellen, können Sie einen benutzerdefinierten Ressourcenblock erstellen.
    - In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Katalogelementen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben. Weitere Informationen finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.
    - BS-Profil ein Skript zuordnen

      Um geskriptete Aktionen während der VM-Bereitstellung auszuführen, können Sie einem BS-Profil ein Skript zuordnen. Das Skript wird auf VMs ausgeführt, die basierend auf der Bildvorlage im BS-Profil erstellt werden.

  - Ressourcenprofile definieren

    Erstellen Sie Ressourcenprofildefinitionen in der globalen Domäne, und erstellen Sie Zuordnungen zu diesen Definitionen in den untergeordneten (Blatt-)Domänen. Löschen Sie keine Ressourcenprofile, ohne allen betroffenen Unternehmen zu überprüfen. Sie können domänenspezifische Ressourcenpools und Poolfilter für alle unterstützten Cloud-Provider erstellen. Als Domänenadministrator können Sie globale, Domänen- und benutzerdefinierte Ressourcenpools für Unterdomänen anzeigen lassen. Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen. Für domänengetrennte Ressourcenpools werden nur Datensätze der relevanten Domäne zurückgegeben.

    Ressourcen-Profile sind vom Cloud Provider unabhängige Definitionen, die die zulässigen Attributwerte für eine Ressource angeben. Ressourcen-Profile ermöglichen Ihnen die Steuerung der Auswahlmöglichkeiten, die dem Benutzer beim Anfordern einer Cloud-Ressource angezeigt werden. Daher müssen Sie nicht für jede Variation der Ressource eine eindeutige Blaupause definieren.

- Richten Sie Cloud Provisioning and Governance für Kontingent, Richtlinien, Pools, Berechtigungen ein und verwalten Sie diese. Governance bezieht sich auf die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen, die Sie für verfügbare Cloud-Ressourcen festlegen können. Als SP können Sie die Prozesstrennung in Cloud Provisioning and Governance-Richtlinien und Berechtigungen für jedes Unternehmen oder jede Domäne verwalten, die Sie in Ihrer Instanz verwalten. Es wird empfohlen, dass Richtlinien nur in der globalen Domäne eingerichtet werden. Prozesstrennung auf Domänenebene ist für Governance und Richtlinien durchführbar. Für eine benutzerdefinierte Richtlinienerzwingung verwenden Sie das Unternehmensfeld in der Richtlinienregelbedingung, um eine Richtlinie auf die bestimmte Domäne auszurichten.

Typ	Beschreibung
Kontingente	Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.
Richtlinien	Eine Cloud-Richtlinie kann einen von einem Anwender festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorab ausfüllen oder ausblenden, anwenderdefinierte Skripts ausführen und aufrufen Cloud-API, Oder starten oder brechen Sie Subflows ab. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.
Pools	Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.
Berechtigungen	Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Katalogelemente oder Cloud-Konten. Sie können auch grundlegende Governance-Richtlinien, Kontingente und Pools einrichten und dem Cloud-Administratorbenutzer gestatten, diese je nach Bedarf weiter anzupassen. Erstellen Sie eine Benutzergruppe, die die Domänenbenutzer darstellt, und ordnen Sie dieser Benutzergruppe Berechtigungen zu, um Berechtigungen auf Domänenebene einzurichten. Weitere Informationen zum Verwalten von Berechtigungen für Cloud Provisioning and Governance-Rollen finden Sie unter Cloud-Berechtigungen verwalten.

- Konfigurieren und verwalten Sie Richtlinien, und verwalten Sie die Miete für den bereitgestellten Stapel. Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

  Richten Sie Richtlinien in der globalen Domäne nur ein, wenn die Richtlinien für alle Domänen gelten sollen. Sie können Cloud Provisioning and Governance anpassen und spezifische Richtlinien für einen Kunden oder eine Domäne festlegen, wenn keine globalen Richtlinien auf eine Domäne angewendet werden sollen. Für eine benutzerdefinierte Richtlinienerzwingung verwenden Sie das Domänenfeld in der Richtlinienregelbedingung, um eine Richtlinie auf die bestimmte Domäne auszurichten. Wenn globale und Domänenrichtlinien gleichzeitig vorhanden sind, werden beide Richtlinien in der für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die einzelnen Richtlinien konfigurierten Reihenfolge ausgeführt. Wenn die in den Sortierungsspalten festgelegten Werte identisch sind, ist die Reihenfolge, in der die Richtlinien ausgeführt werden, nicht bestimmt. Stellen Sie sicher, dass Richtlinienaktionen nach Domänen getrennt sind, d. h. alle Aktionsregeln befinden sich innerhalb einer einzelnen Domäne und sind nicht von Regeln in anderen Domänen abhängig.

Weitere Informationen finden Sie unter:

- Richtlinien-Governance in Cloud Provisioning and Governance
- Cloud-Richtlinienregel konfigurieren
- Aktion für eine Richtlinie „Mietvertragsende“ erstellen
- Cloud-Richtlinienbeispiel

- Cloud-Katalogelement erstellen

  Erstellen Sie, basierend auf einer Vorlage, ein Cloud-Katalogelement für die Bereitstellung, und veröffentlichen Sie das Katalogelement, um einen Service bereitzustellen.

  Sie können allgemeine oder globale Katalogelemente basierend auf Vorlagen in der SP-Domäne erstellen, um sie für alle von Ihnen verwalteten Domänen verfügbar zu machen. Sie können auch benutzerdefinierte Katalogelemente für jede Domäne/jedes Unternehmen basierend auf Ihren Anforderungen erstellen. Ein Benutzer mit der Rolle Domänenadministrator oder Cloud-Designer kann Cloud-Skripts aktualisieren oder löschen. Cloud-Skriptvorlagen gehören zur Domäne und Unterdomänen. Sie können keine allgemeinen Kataloge mit unterschiedlichen Poolfiltern für jede Domäne verwenden. Erstellen Sie stattdessen einen benutzerdefinierten Katalog für jede Domäne.

  Bereitstellungs-, Nachbereitstellungs- und Tag-2-Vorgänge sind domänengetrennt. Beispiel: Wenn ein Cloud-Portalbenutzer eines bestimmten Unternehmens eine VM bestellt, werden der Stapel, die Anforderung, der virtuelle Computer und alle Komponenten im Stapel in ihrer jeweiligen Domäne gespeichert. Nachfolgende Vorgänge für eine Domäne werden ebenfalls auf dieselbe Weise behandelt. Sie können ein Katalogelement basierend auf der Terraform-Konfigurationsverwaltungsvorlage generieren oder Azure Resource Manager- und AWS CloudFormation-Vorlagen verwenden.

- Cloud-Vorlagen erstellen

  Fügen Sie dem Vorlageninhalt keine sensiblen und privaten Informationen wie CIDR-Werte, IP-Adressen, Anmeldeinformationen usw. hinzu, wenn Sie das Katalogelement als globales Katalogelement einrichten. Die sensiblen Informationen könnten anderen Cloud-Administratoren zugänglich gemacht werden.

  Erstellen Sie eine Cloud-Vorlage, und ordnen Sie die Vorlage einem Katalogelement zu. Sobald Sie eine Vorlage erstellt haben, können Sie die Vorlage erneut verwenden, um zusätzliche Katalogelemente für die Services zu erstellen, die Sie bereitstellen möchten.

- Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

  Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen ein, z. B. die Anzahl der virtuellen Computer und virtuellen CPUs oder den zusammengefassten Speicher. Sie können für jedes logische Rechenzentrum in einem Cloud-Konto separate Beschränkungen festlegen.

- Cloud-Kontingentdefinition erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können für jede Domäne, die Sie in einer Instanz verwalten, separate Kontingentdefinitionen einrichten.

Sie wenden Kontingente auf eine Ressource, z. B. einen virtuellen Server, ein Rechenzentrum oder eine generische Cloud-Ressource sowie auf Benutzer einer bestimmten Gruppe an. Sie können für die Ressource ein Limit pro Benutzer und ein Gesamtlimit für die Gruppe festlegen. In einer Cloud-Kontingentdefinition werden die Einschränkungen für einen Ressourcenblock angegeben. Sie können Vorlagen verwenden oder manuell verschiedene Konfigurationstypen für jede Kontingentdefinition erstellen.

- IPAM-Integration verwenden

  Die IP-Adressenverwaltung (IP Address Management, IPAM) in Cloud Provisioning and Governance unterstützt die Domänentrennung.

  Wenn Sie ein Tool zur IP-Adressverwaltung (IP Address Management, IPAM) wie Infoblox verwenden, können Sie Cloud-IP-Adressen, Netzwerke und Subnetze in Ihren Cloud-Katalogangeboten verwalten.

- Geschäftszeitplanung

  Richten Sie die Geschäftszeitenplanung auf allen virtuellen Computern in einem Stapel ein. Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden. Zeitpläne können dafür festgelegt werden, wann ein Stapel gestartet, gestoppt und/oder seine Bereitstellung aufgehoben werden soll, indem Parameter wie Geschäftszeiten, Feiertage oder lange Wochenenden definiert werden.

  Sie ordnen einem Instanzzeitplan ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll.

  Hinweis: Globale Geschäftszeitpläne gelten für alle Domänen. Sie können keine domänenspezifischen Zeitpläne einrichten, wenn ein aktiver globaler Zeitplan vorhanden ist.

- Zeitplanprofil erstellen

  Stellen Sie zum Einrichten domänenspezifischer Mietzeitpläne sicher, dass keine globalen Mietzeitpläne vorhanden sind. Sie können einen domänenspezifischen Mietvertrag oder Zeitplan nur erstellen, wenn keine aktiven globalen Richtlinien vorhanden sind. Sie können zwar mehrere Mietverträge oder Zeitpläne im Entwurfsstatus haben, es kann jedoch nur ein Mietvertrag oder Zeitplan aktiv sein.

Nächste Schritte

Weitere Informationen zur Bereitstellung von Cloud-Ressourcen und zur Bereitstellung von Cloud Provisioning and Governance-Lebenszyklusvorgängen für jede Domäne, die Sie in Ihrer Instanz verwalten, finden Sie unter Überlegungen zum Domänenadministrator.

Überlegungen zum Domänenadministrator

Bevor Sie die Domänentrennung für Kunden konfigurieren, sollten Sie vor der Bereitstellung von Cloud-Ressourcen für jede Domäne, die Sie in der Cloud Provisioning and Governance-Anwendung verwalten, die folgenden Überlegungen berücksichtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänenadministratoraktivitäten in der Organisation eines Service Providers

Im folgenden Abschnitt werden Aktivitäten aufgelistet, die der Administrator einer Domäne für das Unternehmen ausführt, das von einem Service Provider verwaltet wird. Richten Sie Servicekonten und Cloud-Konten über das Cloud-Adminportal ein. Erstellen Sie die Bereitstellung vorbereitende Vorgänge, die Sie für Cloud-Ressourcen konfigurieren können, bevor Ihre Benutzer sie bereitstellen oder Lebenszyklusvorgänge ausführen.

Starke allgemeine Prozessstandards, datenbasiertes Prozessdesign, strikte Governance und zentralisierte Administration maximieren die Vorteile der Domänentrennung in Cloud Provisioning and Governance in einer einzelnen Instanz. Die Domänenadministratorrolle muss streng auf Benutzer in der Organisation des Service Providers beschränkt sein und darf nicht den Cloud-Administratorbenutzern aus der Organisation des Kunden zugewiesen werden. Diese Einschränkung ermöglicht dem SP sicherzustellen, dass ein Kunde keinen vollständigen Zugriff auf die Daten einer anderen Domäne erhält. Da Daten häufig von mehreren Clients gemeinsam verwendet werden, machen Sie als Domänenadministratoren keine Berechtigungen verfügbar oder gewähren solche, die zu Datenlecks führen könnten.

Cloud-Ressourcen bereitstellen

- Stellen Sie sicher, dass Sie Cloud-Konten in jeder Domäne relevante Servicekonten zuordnen. Beispielsweise wird beim Erkennen eines primären Abonnements in der Azure-Cloud mindestens ein untergeordnetes Servicekonto in derselben Domäne erstellt. Dies bedeutet, dass alle Servicekonten in einem Master-Abonnement aus der Azure-Cloud zu einem einzigen Unternehmen und einer Domäne gehören müssen.

  Melden Sie sich als Benutzer mit Rolle „root_admin“ oder „cloud_admin“ an, wenn Sie Cloud- und Servicekonten einrichten und eine Erkennung für eine beliebige Domäne ausführen. Verwenden Sie die Domänenauswahl, wenn Sie Aktionen wie Discovery oder das Erstellen und Zuordnen von Cloud- und Servicekonten ausführen.

  Hinweis:

  - Cloud Provisioning and Governance unterstützt das Erweitern und Reduzieren des Domänenbereichs nicht.
  - Weitere Informationen dazu, was ein Anwender aufrufen kann und was er nicht kann, finden Sie unter Domänenbereich

  Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert werden. In Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dazu verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten enthalten – sogar Servicekonten verschiedener Provider. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

  Stellen Sie sicher, dass Verwaltungsschlüssel und Anmeldeinformationen von Servicekonten für jede Domäne eindeutig sind und nicht freigegeben werden. Führen Sie zum Einrichten von Cloud-Konten und Servicekonten für mehrere Cloud-Provider Aktionen für Tag 1 durch:

  - Setupleitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance
  - Setup-Leitfaden für Tag 1 für Azure am Cloud Provisioning and Governance

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Setup-Leitfaden für Tag 1 für Google Cloud Connector auf Cloud Provisioning and Governance
- Setupleitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

- Cloud API (CAPI) und Cloud-Skripts und Cloud-Skriptvorlagen

  CAPI ist nicht domänengetrennt, Domänentrennung wird in Cloud Provisioning and Governance unterstützt. Da CAPI in einer globalen Domäne eingerichtet und über Blattdomänen hinweg gemeinsam genutzt wird, stellen Sie sicher, dass Skripts keine hartcodierten vertraulichen Informationen wie Kontodetails, Anmeldeinformationen oder Namen enthalten, nicht einmal in Kommentaren oder Anmerkungen.

  CAPI ermöglicht mithilfe von REST APIs die Integration von Cloud Provisioning and Governance in Cloud-Provider. Cloud-Skripts sind einfache Java-Skripts, die Plattformfunktionen verwenden. In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Vorlagen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben. Cloud-Skriptvorlagen sind tatsächliche ausführbare Dateien, die zur Ausführung an einen virtuellen Computer übergeben werden. Erstellen Sie zuerst eine Cloud-Vorlage, und ordnen Sie sie dann einem Cloud-Skript zu.

- Cloudbasierter Discovery-Vorgang

  Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können Daten nur in ihrer eigenen oder einer untergeordneten Domäne anzeigen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen können. Obwohl die Unterstützung der Domänentrennung für Discovery als Ebene 2 angesehen wird, wird die Verwaltung in Cloud Provisioning and Governance nicht an untergeordnete Domänen delegiert. Die SPs müssen die administrative Kontrolle behalten. Als SP führen Sie Discovery immer von einer Blattdomäne aus, indem Sie sich als Domänenadministrator anmelden oder die Identität eines solchen annehmen, um Ihre Cloud-Ressourcen zu erkennen.

  Cloud Discovery enthält einen Assistenten, mit dem Sie Cloud-Zeitpläne in einer einzigen Benutzeroberfläche erstellen und ausführen können. Wenn Sie mit dem Discovery Manager einen Zeitplan erstellen, wählen Sie die zu erkennenden Konten, die Anmeldeinformationen für den Zugriff auf diese Konten und die MID Server zum Scannen der Ressourcen aus. Anschließend können Sie die Ergebnisse auf der Discovery-Homepage ansehen und eventuell aufgetretene Fehler nachverfolgen.

  Weitere Informationen finden Sie unter

  - Discovery-Manager
  - Erkennungen im Netzwerk ausführen
    - Microsoft Azure Cloud-Discovery
    - Erkennung von VMware-Clouds
    - Google Cloud Platform-Discovery
    - Erkennung von IBM-Clouds

- Richten Sie Event Management ein und konfigurieren Sie es, um externe Events zu empfangen und Warnungen basierend auf den Event- und Warnungsverwaltungsregeln zu generieren. Die Sichtbarkeit von Events hängt von der Domäne des zugeordneten Servicekontos ab. Nur Benutzer, die zu dieser Domäne gehören, können die Eventdetails

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für verarbeitete Events sehen. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

Überwachen Sie die Integrität der Business Services und der Infrastruktur mithilfe einer einzigen Managementkonsole, und reagieren Sie angemessen auf alle auftretenden Probleme. Event Management bietet intelligente Event- und Warnungsanalysen und stellt so die Kontinuität Ihrer Business Service-Leistung sicher. Von Event Management werden Events über den MID Server empfangen und verarbeitet.

Weitere Informationen finden Sie unter

- Ereignismanagement erkunden
- Ereignismanagement-Setup
  - Konfigurieren Sie AWS Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz
  - Konfigurieren Sie Microsoft Azure Warnungsservice zum automatischen Aktualisieren von CMDB
  - Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB
  - Konfigurieren Sie VMware-EventsService zum automatischen Aktualisieren von CMDB

- Die Cloud Provisioning and Governance-Anwendung unterstützt die Integration in Lösungen zur kontinuierlichen Bereitstellung (auch bekannt als Konfigurationsverwaltung). Erstellen Sie einen Provider für die Ansible- oder Terraform-Konfigurationsverwaltung, und führen Sie dann Discovery für den Provider aus, um seine Ressourcen zu finden. Weitere Informationen finden Sie unter Unterstützung für kontinuierliche Bereitstellung (Konfigurationsmanagement) Und Erstellen Sie einen Arbeitsauslastungsanbietertyp Für jeden neuen Konfigurationsverwaltungsanbieter. Diese Informationen werden im Bestellkatalogformular als Verwaltungsattribute angezeigt, die Ihre Benutzer auswählen können, wenn sie eine virtuelle Ressource über einen Konfigurationsverwaltungs-Provider bereitstellen.

- Wenn Sie Kataloge basierend auf Terraform-Vorlagen erstellen und den Katalog für mehrere Domänen freigeben. Führen Sie eine Modulauflistung (Konfigurationserkennung) in der globalen Domäne durch. Der MID-Server sollte in der globalen Domäne erstellt werden, und ihm sollte nur die Terraform-Fähigkeit für die Discovery zugewiesen werden. Dadurch können SPs Kataloge für mehrere Domänen freigeben.

  ⚠ Warnung:

  Erstellen Sie einen globalen MID-Server mit keiner anderen Funktionalität als der Konfigurationsverwaltung für Terraform.

  Gemeinsamen Terraform-Katalog erstellen und für mehrere Kunden freigeben:

  - Erstellen Sie als globaler Administrator einen MID-Server in der globalen Domäne.
  - Erstellen Sie einen Terraform Open Source-Konfigurationsanbieter .

    Hinweis: Fügen Sie nur „Terraform“ als Konfigurations-Provider hinzu.

  - Erstellen Sie ein Katalogelement basierend auf einer Terraform-Vorlage.

- Cloud Provisioning and Governance Unterstützt Verwendung von ServiceNow AI PlatformMit Subflows. Regeln sind Sammlungen von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das System die Aktionen aus. Wenn eine Bedingung als „false“ ausgewertet wird, führt das System die Aktionen nicht aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Erstellen von Regeln hilft Ihnen, Aktivitäten nachzuverfolgen und schneller auf Probleme zu reagieren und sie zu lösen. Nutzen Sie den Flow Designer-Subflow, um Ihre Day 2-Vorgänge zu automatisieren. Schreiben Sie schnell einen Subflow, der mit einer Cloud-API oder einer bestimmten Ressource kommuniziert. Verwenden Sie SSH, PowerShell oder ein ähnliches Tool, um auf die Subflow-Fähigkeiten zuzugreifen und sie dann zu erweitern. Weitere Informationen finden Sie unter Tag 2-Vorgänge mit Subflows .

- Budgetbasierte Benachrichtigung und Genehmigung

  Die Domänentrennung in Cloud Provisioning and Governance unterstützt die Datentrennung von Budgets. Sie können domänenspezifische Budgets zuweisen. Weisen Sie ein Budget für eine Gruppe und einen Benutzer innerhalb der Gruppe zu. Wenn der Benutzer oder die Gruppe den Schwellenwert für das Budgetlimit erreicht, werden sie darüber benachrichtigt. Weitere Informationen finden Sie unter Budgets konfigurieren

  - Tags für Cloud-Ressourcen erstellen

    Mithilfe von Tags werden Cloud-Ressourcen kategorisiert, um umfangreichere und detailliertere Nachverfolgungs- und Abrechnungsberichtsdaten bereitzustellen. Tag-Schlüssel sind nicht domänengetrennt und werden Benutzern anderer Domänen angezeigt. Die Tag-Sichtbarkeit hängt von der zugeordneten CI-Domäne oder der zugehörigen Domäne des Abrechnungsdatensatzes ab. Tags, die keinem CI oder Abrechnungsdatensatz zugeordnet sind, sind für alle Domänenadministratoren sichtbar. Wenn ein Tag erstellt wird, wird es in jedem neu erstellten Katalog angezeigt. Der Cloud-Administrator muss die gewünschten Tags für seinen Katalog auswählen.

  - Abrechnungsdaten können für jede Domäne separat angezeigt werden. Abrechnungsaufträge verwenden die Domäne des konfigurierten Servicekontos. Konfigurieren Sie die Abrechnungseinrichtung so, dass Cloud-Administratoren und Cloud-Benutzer Berichte wie Cloud-Abrechnungsdaten und Cloud Tag-Nutzung auf dem Abrechnungsdashboard anzeigen lassen können.

    Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zur Erstellung von Berichten verwendet.

    Weitere Informationen zum Einrichten von Abrechnungszeitplänen und zum Herunterladen von Abrechnungsberichten finden Sie unter:

    - Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren
    - Zeitplan für das Herunterladen von Azure-Abrechnungsdaten definieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Schritte

Wichtig:

Stellen Sie beim Erstellen benutzerdefinierter Vorgänge, die Workflows für Ressourcenblöcke aufrufen, sicher, dass Sie den Kontext in die entsprechende Domäne ändern.

Zum Ändern des Kontexts in die richtige Domäne bearbeiten Sie die **Workflow-Aktivität**, um das folgende Skript aus dem Workflow heraus aufzurufen. Stellen Sie sicher, dass ein entsprechender Benutzer vom Servicekontoersteller oder vom Auftragsbenutzer abgerufen wird. Durch Aufrufen dieses Identitätswechselskripts kann der Workflow im richtigen Kontext ausgeführt und der richtige MID-Server der zugehörigen Domäne ausgewählt werden.

```
//var orderContext = json.decode(workflow.inputs.ordercontext) ;
new CMPDomainSeparationUtil() .impersonateUser(current.request.requested_for);
```

Weitere Informationen zum Ausführen von Cloud Provisioning and Governance Lebenszyklusvorgänge, die für jede Domäne verfügbar sind, die Sie in Ihrer Instanz verwalten, siehe Cloud-Anwenderportal .

Zugehörige Informationen

Zusätzliches Setup von Cloud Provisioning and Governance an Tag 2

Von ITOM Visibility verwendete Erkennungsmuster

Cloud Provisioning and Governance Rezepte

Multi-Cloud-Rezepte bieten bereitstehende Inhalte für typische Cloud-Bereitstellungen und allgemeine Betriebsszenarien auf verschiedenen Cloud-Plattformen.

Rezepte für Enterprise-Workloads und Tag-2-Vorgänge

Cloud Provisioning and Governance-Rezepte sind gebrauchsfertige Katalogelemente, die aus CFT- und ARM-Beispielvorlagen erstellt wurden, um reale Anwendungsfälle von Cloud-Bereitstellungen zu unterstützen. Diese Rezepte können für den Proof-of-Concept und in Umgebungen außerhalb der Produktion verwendet werden. Stellen Sie in Produktionsumgebungen sicher, dass die Rezepte gut getestet und intern ausgewertet werden. Sie können die Rezepte als Update Sets zum Herunterladen von SHARE im Developer Program unter der Kategorie „Cloud Provisioning-Rezepte“ verwenden.

Liste der Update Sets

Name	Beschreibung
Katalogelemente für Amazon Web Service	
CFT Single Linux VM	Katalogelement für einen einzelnen virtuellen Linux-Computer über ein CFT.
CFT Single Windows VM	Katalogelement für einen einzelnen virtuellen Windows-Computer über ein CFT.
CFT Linux VM with Multiple NICs	Katalogelement für einen virtuellen Linux-Computer mit mehreren Netzwerkschnittstellen über ein CFT.
CFT Linux VM with LB and Storage	Katalogelement für einen virtuellen Linux-Computer mit Lastenausgleich und Speicher über ein CFT.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
CFT Linux VM with Multi VM Multi Disk	Cloud Formation-Vorlage für eine Linux-VM mit mehreren VMs und mehreren Schnittstellen für virtuelle Datenträger.
CFT Linux Install Apache	Katalogelement zur Installation eines Apache-Servers auf einer Linux-VM über ein CFT.
CFT Simple VM with Approval Policy	Katalogelement für eine einfache VM mit einer Genehmigungsrichtlinie über ein CFT.
CFT Windows VM Multi Disk and LB	Katalogelement für eine Windows-VM mit mehreren Schnittstellen für virtuelle Datenträger und mit Lastenausgleich über ein CFT.
Katalogelemente für Azure	
ARM Windows VM with Multi NICs	Katalogelement für eine Windows-VM mit mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Windows Single VM Multi Disk	Katalogelement für eine einzelne VM mit mehreren Schnittstellen für virtuelle Datenträger über eine ARM-Vorlage.
ARM Windows Stack Multi Disk	Katalogelement für einen Windows-Stapel mit mehreren Schnittstellen für virtuelle Datenträger über eine ARM-Vorlage.
ARM Windows Stack Multi NIC	Katalogelement für eine Windows-Stapel-VM mit mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Linux VM Multi NIC Multi Disk	Katalogelement für eine Linux-VM mit mehreren Schnittstellen für virtuelle Datenträger und mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Linux VM Install Apache	Katalogelement zur Installation eines Apache-Servers auf einer Linux-VM über eine ARM-Vorlage.
ARM Linux VM Install MySQL	Katalogelement zur Installation eines MySQL-Servers auf einer Linux-VM über eine ARM-Vorlage.
ARM WebApp MySQL	Katalogelement zum Erstellen einer Web-App mit Azure-Datenbank für MySQL über eine ARM-Vorlage.
ARM VNET Multi Subnet with Approval Policy	Katalogelement für Multi-Subnetz-VNET mit Genehmigungsrichtlinie über eine ARM-Vorlage.
ARM VNIC Multi Subnet with Naming Policy	Katalogelement für Multi-Subnetz-VNIC mit einer Benennungsrichtlinie über eine ARM-Vorlage.

Tag-2-Vorgänge für AWS-VM

Ein Update Set wird für einige der wichtigen Vorgänge von Tag 2 beim AWS Cloud-Provider bereitgestellt. Allgemein sind Tag-2-Vorgänge der Typ von Vorgängen, die für Workloads ausgeführt werden, nachdem sie bereitgestellt wurden. Tag-2-Vorgänge können komplexe Lebenszyklusprozesse oder einfache Dienstprogramme umfassen. In diesem Update Set haben Sie Zugriff auf die folgenden Vorgänge:

Name	Beschreibung
AttachVolume	Fügt der Instanz mit dem angegebenen Gerätenamen ein Amazon EBS-Volume (Elastic Block Store) an und macht es verfügbar.
CreateSnapshot	Erstellt einen Snapshot Ihres Amazon EBS-Volumes (Elastic Block Store).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
[Erkennungsvorgang auf AWS-Rechenzentrumsebene]	
DescribeSnapshots	Beschreibt die angegebenen für Sie verfügbaren Amazon EBS-Snapshots (Elastic Block Store) oder alle für Sie verfügbaren EBS-Snapshots.
DetachVolume	Trennt ein EBS-Volume von einer Instanz.
ModifyInstanceAttribute [Nur InstanceType]	Ändern Sie das angegebene Attribut der angegebenen Instanz.
ModifyVolume [Nur Größe]	Ändern Sie die Parameter eines vorhandenen Amazon EBS-Volumes (Elastic Block Store).
Day 2 Operations for AWS VM – Set 1	Katalogelement für Vorgänge am Tag 2 für eine AWS-VM, Satz 1.

Cloud-Accounts

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

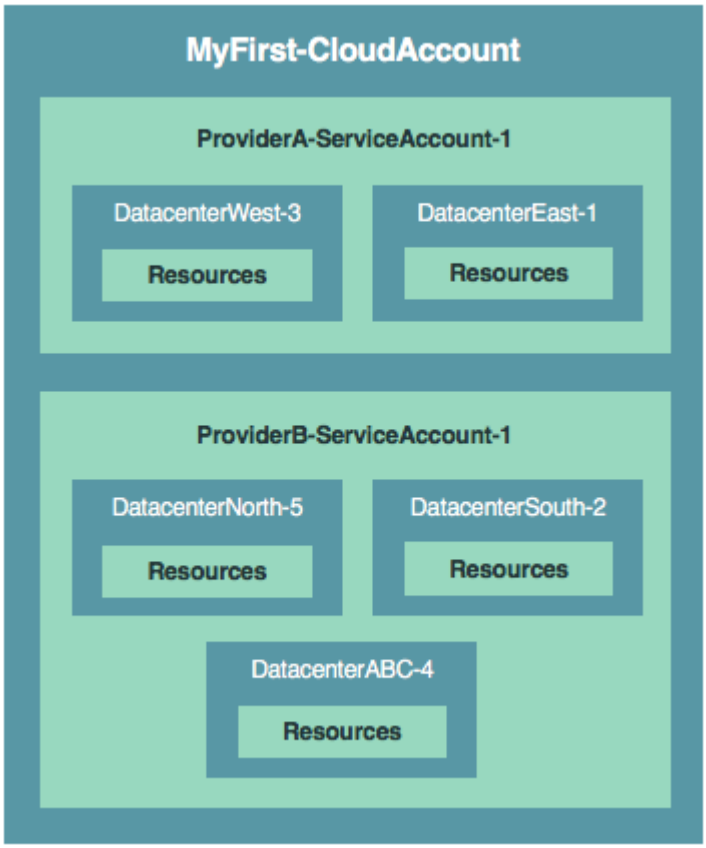
Mit einem Cloud-Konto können Sie:

- LZRs hinzufügen. Ein logisches Rechenzentrum (LZR) ist eine regionsspezifische virtuelle Cloud, die einem Servicekonto zugeordnet ist. Das Rechenzentrum hostet Ihre Cloud-Ressourcen.
- Discovery auf LZRs ausführen, um die CMDB mit Konfigurationsänderungen oder Lebenszyklusänderungen (Erstellen/Ändern/Beenden) für jede Ressource in jedem logischen Rechenzentrum zu aktualisieren, das dem Cloud-Konto zugeordnet ist.
- Kapazitätsgrenzen für Cloud-Services wie virtuelle Computer, virtuelle CPUs, virtuelle Netzwerke, Gesamtgröße des Speichervolume und andere Services festlegen. Legen Sie Grenzwerte fest, um sicherzustellen, dass Cloud-Ressourcen in angemessenem Umfang bereitgestellt werden. Grenzwerte sind besonders wichtig für kapazitätsbeschränkte Umgebungen wie private Clouds.
- Einen Cloud-Konto veröffentlichen, damit Geschäftsteams Stapel bereitstellen können.

Struktur eines Cloud-Accounts

Ein Vorteil von Cloud-Accounts ist, dass Sie angegebene Servicekonten nur mit den Regionen (Rechenzentren) gruppieren können, in denen Sie Cloud-Ressourcen zulassen möchten. Beispielsweise kann Ihr AWS-Konto global mehr als ein Dutzend Rechenzentren haben. Sie verwenden vielleicht jedoch nur eine oder zwei Regionen. Um Ihre Sicherheits- und Compliance-Regeln zu erfüllen, möchten Sie möglicherweise, dass keine Ressourcen für zusätzliche Regionen auf der ganzen Welt bereitgestellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein Cloud-Konto kann in den folgenden Szenarien beliebig viele Servicekonten enthalten:

Mögliche Cloud-Account-Strukturen

Struktur	Unterstützt	Nicht unterstützt
Fügen Sie dasselbe Servicekonto so oft wie erforderlich hinzu, sofern jeder Eintrag einem anderen LZR zugeordnet ist.	X	
Fügen Sie dasselbe LZR über verschiedene Servicekonten in einem Cloud-Konto hinzu.		X
Fügen Sie einem bestimmten Cloud-Konto verschiedene LZRs aus verschiedenen Servicekonten hinzu, sofern die Regionen nicht identisch sind. Beispiel: Sie haben „us-west-1“ in „serviceaccount1“ und „us-west-2“ in „serviceaccount2“. Beide können „cloudaccount1“ hinzugefügt werden. „us-west-1“ in „serviceaccount1“ und „us-west-1“ in „serviceaccount2“ können jedoch nicht zu „cloudaccount1“ hinzugefügt werden.	X	

Aktualisieren Sie einen Cloud-Account

Belassen Sie einen Cloud-Konto im Status **Entwurf**, bis Sie bereit sind, die Rechenzentren und Kapazitätsgrenzen verfügbar zu machen – z. B. in Blaupausen und dem Cloudbenutzerportal. Sie können den Status nach der Ausführung von Discovery in **Veröffentlicht** ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliches Cloud-Konto einrichten

Weitere Informationen finden Sie unter Zusätzliches Cloud-Konto einrichten.

Einem Cloud-Konto ein Rechenzentrum hinzufügen

Sie können der Cloud-Infrastruktur jederzeit ein logisches Rechenzentrum hinzufügen, das durch einen Cloud-Konto dargestellt wird. Siehe Fügen Sie einem ein Rechenzentrum hinzu Cloud-Konto.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

In AWS erkannte Servicekategorien

Der Discovery-Prozess erkennt AWS-Services.

In AWS erkannte Servicekategorien

Servicekategorie	Name	CI-Klasse	Muster	Produkt
Berechnen	AWS::CloudFormation::Stack	cmdb_ci_aws_cloudformation_stack		AWS CloudFor
Datenbank	AWS::Datacenter	cmdb_ci_aws_datacenter		
Sicherheit	AWS::DirectoryService			AWS Dire Service
Berechnen	AWS::EC2::EIP	cmdb_ci_cloud_ip_address		AWS Elas Compute
Berechnen	AWS::EC2::Image	cmdb_ci_os_template		AWS Elas Compute
Berechnen	AWS::EC2::Instance	cmdb_ci_vm_instance		AWS Elas Compute
Berechnen	AWS::EC2::InstanceType	cmdb_ci_compute_template		AWS Elas Compute
Sicherheit	AWS::EC2::Keypair	cmdb_ci_cloud_key_pair		AWS Key Managem Service
Netzwerk	AWS::EC2::NetworkInterface	cmdb_ci_nic		AWS Virt Private Cl
Berechnen	AWS::EC2::SecurityGroup	cmdb_ci_compute_security_group		AWS Elas Compute
Netzwerk	AWS::EC2::Subnet	cmdb_ci_cloud_subnet		AWS Virt Private Cl
Speicher	AWS::EC2::Volume	cmdb_ci_storage_volume		AWS Elas Storage

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekategorie	Name	CI-Klasse	Muster	Produkt
Netzwerk	AWS::EC2::VPC	cmdb_ci_network		AWS Virt Private Cl
Lastenausgleich	AWS::ElasticLoadBalancing::LoadBalancer	cmdb_ci_cloud_load_balancer	Amazon AWS Elastic Load Balancer Service	AWS Elas Balancer
Lastenausgleich	AWS::ElasticLoadBalancingV2::LoadBalancer	cmdb_ci_cloud_load_balancer	Amazon AWS Elastic Load Balancer Service	AWS Elas Balancer
Datenbank	AWS::RDS::DBEvent			Amazon A Relational Database
Datenbank	AWS::RDS::DBInstance	cmdb_ci_cloud_database	Amazon AWS Relational Database Service	Amazon A Relational Database
	Verfügbarkeitszone	cmdb_ci_availability_zone		AWS-Verfügbar

Hinweis: Die vollständige Liste der übereinstimmenden Klassen/Ressourcen finden Sie in der Tabelle „Cloud-Ressourcentypen“ [sn_CAPI_resource_type].

In Azure erkannte Servicekategorien

Der Discovery-Prozess erkennt Microsoft Azure-Services.

In erkannte Servicekategorien Azure

Hinweis:

Die CAPI-basierte Discovery-Methode ist veraltet. Folgen Migrieren Sie von CAPI zu Mustern Weitere Informationen finden Sie unter .

Servicekategorie	Name	CI-Klasse	Muster	Produkt
	Azure-Rechenzentrum	cmdb_ci_azure_datacenter		
	Azure-Abonnement	cmdb_ci_cloud_service_account		
	Cloud-Ressource	cmdb_ci_cmp_resource		
Applikationsservices	Microsoft (Unknown Resource Type)			Microsoft (Unknown Product)
Applikationsservices	Microsoft.ApiManagement/service			Microsoft.ApiManagement
Applikationsservices	Microsoft.Cache			Microsoft.Cache

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekategorie	Name	CI-Klasse	Muster	Produkt
Anwendungsservices	Microsoft.Web/ serverFarms			Microsoft.Web
Applikationsservices	Microsoft.Web/sites	cmdb_ci_cloud_webserver		Microsoft.Web
Berechnen	Microsoft.Compute/ availabilitySets	cmdb_ci_availability_zone		Microsoft.Compute
Berechnen	Microsoft.Compute/images	cmdb_ci_os_template		Microsoft.Compute
Berechnen	Microsoft.Compute/ virtualMachines	cmdb_ci_vm_instance		Microsoft.Compute
Berechnen	Microsoft.Compute/ virtualMachineScaleSets			Microsoft.Compute
Berechnen	Microsoft.ServiceFabric/ clusters			Microsoft.Compute
Berechnen	Microsoft.Compute/vmSize	cmdb_ci_compute_template		Microsoft.Compute
Berechnen	Microsoft.Resources/ deployments	cmdb_ci_azure_deployment		Microsoft.Compute
Berechnen	Microsoft.Resources/ resourceGroups	cmdb_ci_resource_group		Microsoft.Compute
Datenbank	Microsoft.DocumentDB			Microsoft.DocumentDB
Datenbank	Microsoft.Sql/servers	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.sql/ managedInstances	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.dbformysql	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.documentdb/ databaseAccounts	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.cache/redis	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.dbforpostgresql/ Servers	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	microsoft.dbformysql/ Server	cmdb_ci_cloud_database	Azure-Datenbank	Microsoft.Sql
Datenbank	Microsoft.Sql/servers/ databases	cmdb_ci_database	Azure-Datenbank	Microsoft.Sql
Load Balancer	Microsoft.Network/ loadBalancers	cmdb_ci_cloud_load_balancer		Microsoft.LoadBalancer
Netzwerk	Microsoft.Network/ applicationGateways			Microsoft.Network
Netzwerk	Microsoft.Network/ networkInterfaces	cmdb_ci_nic		Microsoft.Network
Netzwerk	Microsoft.Network/ networkSecurityGroups	cmdb_ci_compute_security_group		Microsoft.Network

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

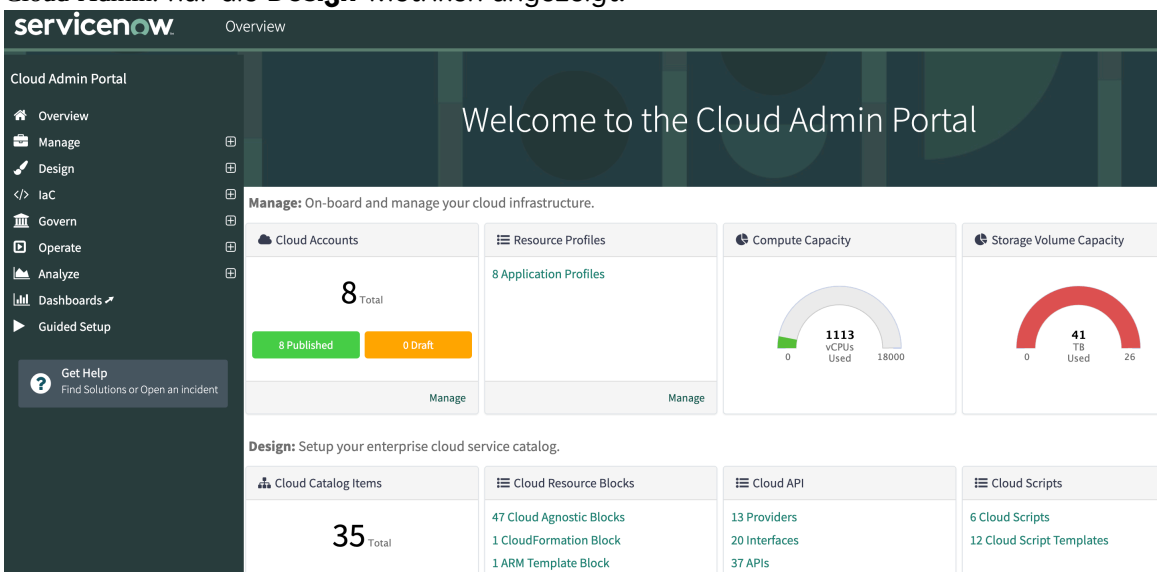
Servicekategorie	Name	CI-Klasse	Muster	Produkt
Netzwerk	Microsoft.Network/ publicIPAddresses	cmdb_ci_cloud_public_ipaddress		Microsoft.Network
Netzwerk	Microsoft.Network/ routeTables	cmdb_ci_route_table		Microsoft.Network
Netzwerk	Microsoft.Network/subnets	cmdb_ci_cloud_subnet		Microsoft.Network
Netzwerk	Microsoft.Network/ virtualNetworks	cmdb_ci_network		Microsoft.Network
Sicherheit	Microsoft.Security			Microsoft.Security
Speicher	Microsoft.Storage/blobs	cmdb_ci_storage_volume		Microsoft.Storage
Speicher	Microsoft.Storage/ storageAccounts	cmdb_ci_cloud_storage_account		Microsoft.Storage
Tools	Microsoft.Insights/ components			Microsoft.Insights
Tools	Microsoft.ServiceBus			Microsoft.ServiceBus

Automatische Übersetzung

Cloud-Adminportal

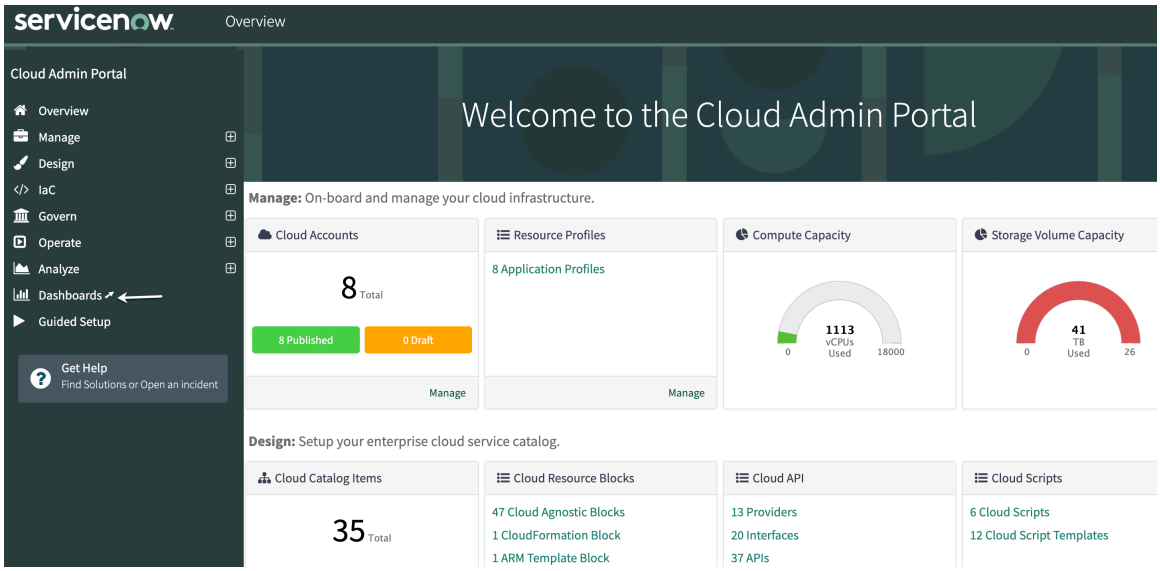
Das Portal für Cloud-Admin. ist ein rollenbasiertes Portal. Sie können alle Ihre Cloud-Ressourcen von einer einheitlichen Basis aus verwalten, entwerfen, steuern, betreiben und analysieren.

Je nachdem, mit welcher Rolle Sie angemeldet sind, zeigt das Portal für Cloud-Admin. unterschiedliche Metriken an. Wenn Sie beispielsweise bei der Cloud Provisioning and Governance-Anwendung als Cloud Service Designer angemeldet sind, werden im Portal für Cloud-Admin. nur die **Design**-Metriken angezeigt.



Ab diesem Release können Sie jetzt verwenden **Dashboards** Link im linken Navigationsbereich des Cloud-Administratorportals, um darauf zuzugreifen Next Experience Dashboard-Seiten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Suchen Sie den Link zu diesen Dashboards auf einer neuen Registerkarte basierend auf Ihrer Anwenderrolle:

- Cloud-Ursachenanalyse-Dashboard
- Dashboard für Cloud-Vorgänge
- Cloud-Tag-Werte-Dashboard

Folgen Die Anwendung Cloud Provisioning and Governance anfordern Um mehr über die Installation zu erfahren Cloud Provisioning and Governance Um auf die Administrator- und Anwenderseiten zuzugreifen. Melden Sie sich beim Portal mit den folgenden Cloud Provisioning and Governance-Rollen an, um die zugehörigen Metriken anzuzeigen oder zu verwalten:

Beschreibender Name und Rollenname	Zugriff auf die Metriken in Portal für Cloud-Admin.
Root-Administrator [sn_cmp.cmp_root_admin]	Alle Metriken. • Übersicht • Verwalten • Entwurf • LAC • Bedingungen • Betreiben • Analysieren • Geführtes Setup
Cloud-Administrator [sn_cmp.cloud_admin]	Verwalten Sie die Metriken. • Übersicht • Verwalten
Systemadministrator	Alle Metriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Zugriff auf die Metriken in Portal für Cloud-Admin.
[admin]	• Übersicht • Verwalten • Entwurf • LAC • Bedingungen • Betreiben • Analysieren • Geführtes Setup
Kontrolle [sn_cmp.cloud_governor] [sn_CAPI.Cloud_Developer]	• Bedingungen • Analysieren • Entwurf
Service Designer [sn.cmp.cloud_service_designer]	Design
Operator [sn_cmp.cloud_operator]	Betreiben

Nur die Rollen Root-Administrator, Cloud-Administrator und Systemadministrator können alle Metriken im Portal für Cloud-Admin. anzeigen und verwalten.

Klicken Sie auf **Guided Setup**, um die Cloud Provisioning and Governance-Anwendung auf Ihrer ServiceNow-Instanz zu konfigurieren. Sie werden durch das Abschließen verschiedener Konfigurationsaufgaben geleitet. Der Prozentsatz der Aufgaben, die Sie abgeschlossen haben, wird angezeigt, damit Sie Ihren Fortschritt überwachen können.

Klicken Sie auf **Hilfe**, um eine Frage zu stellen, einen Incident zu öffnen, zur Produktdokumentation oder zur Knowledge Base-Website zu wechseln.

Ressourcenprofile

Ressourcen-Profile sind vom Cloud Provider unabhängige Definitionen, die die zulässigen Attributwerte für eine Ressource angeben. Ressourcen-Profile ermöglichen Ihnen die Steuerung der Auswahlmöglichkeiten, die dem Benutzer beim Anfordern einer Cloud-Ressource angezeigt werden. Daher müssen Sie nicht für jede Variation der Ressource eine eindeutige Blaupause definieren.

Hinweis: Zusätzlich zu den Cloud-unabhängigen Profilen können Sie öffentliche Images von Providern zum Cloud Provisioning and Governance-Katalog hinzufügen. Siehe Öffentliches AWS-Image zu Cloud Provisioning and Governance hinzufügen und Öffentliches Azure-Image zu Cloud Provisioning and Governance hinzufügen.

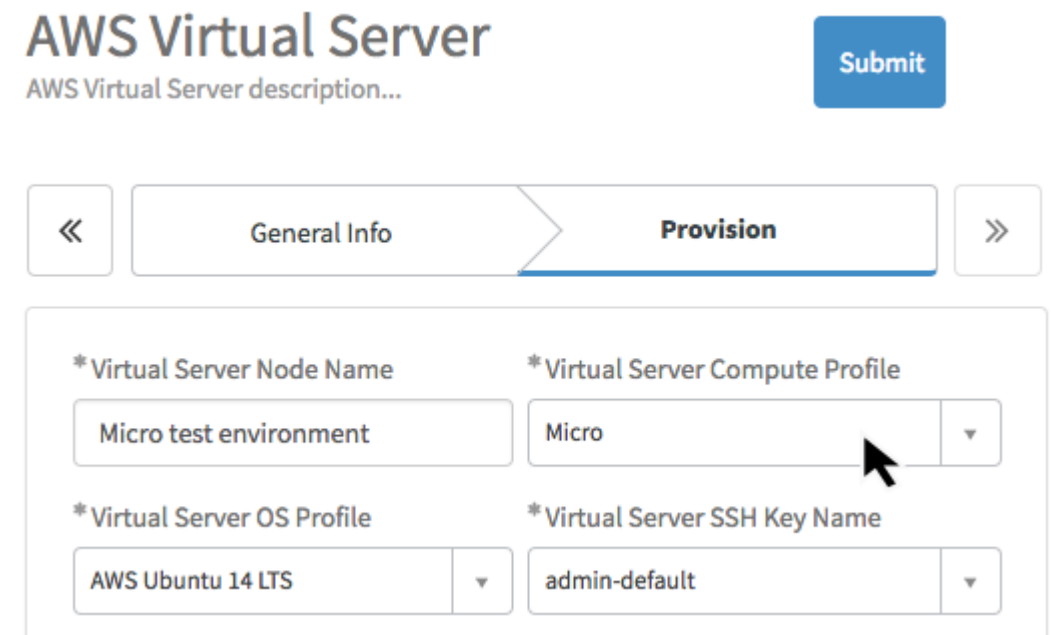
Beispiel: Computing-Profil

Sie können ein Computing-Profil mit dem Namen *Micro* erstellen und einem Hardwaretyp „micro“ mit angegebenen Werten für Arbeitsspeicher und CPU zuordnen. Später, wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein Benutzer beim Anfordern eines virtuellen Servers eine Computing-Ressource auswählt, wird **Micro** als Option in der Liste der verfügbaren Computing-Ressourcen angezeigt. Der Benutzer muss keine Werte für Arbeitsspeicher und CPU angeben – die Werte stammen aus dem Profil.

Computing-Profil im Anforderungsformular



Ressourcenprofilzuordnungen

Ressourcen-Profile erstellen Zuordnungen zwischen den folgenden Elementen:

- Cloud-Konto.
- Logisches Rechenzentrum im Cloud-Konto.
- Bestimmter Ressourcentyp in der CMDB, die die Attribute bereitstellt.
- Optional: Preiswert, der Benutzern angezeigt wird, wenn sie eine Ressource anfordern, die das Ressourcenprofil verwendet.

Standardmäßig ordnet Cloud Provisioning and Governance für AWS und Azure Profile nach der Ausführung von Discovery Vorlagen zu. Bei anderen Providern, z. B. Google Cloud, müssen Sie das Profil manuell der richtigen Vorlage und dem richtigen Rechenzentrum zuordnen.

Ressourcentypen

Jedem Ressourcenprofil sind Attribute zugeordnet. Die Attribute hängen von den Ressourcentypen ab, die nach der Ausführung von Discovery für ein Cloud-Konto ausgefüllt werden.

Ressourcen-Profil Typ	Beschreibung und Attribute	Ressourcentyp und Vorlage
Anwendungsprofil	Ein Anwendungsprofil gibt Anwendungssoftware an, die auf neu bereitgestellten Ressourcen installiert werden soll. Benutzer können Anwendungen auswählen, wenn sie einen Stapel anfordern. Verwenden Sie	Applikationsvorlage [sn_cmp_application_template]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen-Profil Typ	Beschreibung und Attribute	Ressourcentyp und Vorlage
	Anwendungsprofile bei der Integration in Konfigurationsverwaltung (kontinuierliche Bereitstellung) von Providern wie Ansible Playbooks. Attribute: Anwendungen, die auf virtuellen Computern ausgeführt werden.	
Computing-Profil	In einem Computing-Profil wird die Hardware für neu bereitgestellte virtuelle Computer angegeben. Attribute: Die Größe der Computing-Ressourcen, einschließlich virtueller CPUs, Arbeitsspeicher und lokalem Speicher.	Hardwaretyp [cmdb_ci_compute_template]
Computing-Sicherheitsgruppenprofil	Ein Computing-Sicherheitsgruppenprofil wendet bestimmte Sicherheitsregeln auf neu bereitgestellte Ressourcen an. Sie ordnen einem ein Berechtigungssicherheitsgruppenprofil zu Cloud-Konto, Ein Rechenzentrum, eine Vorlage für die Compute-Sicherheitsgruppe und Sicherheitsregeln für die Vorlage. Attribute: Firewallregeln, z. B. Aktivieren von HTTP und HTTPS.	Sicherheitsgruppenvorlage berechnen [cmdb_ci_security_grp_template]
BS-Profil	Mit einem BS-Profil wird ein bestimmtes Image auf einem neu bereitgestellten virtuellen Computer installiert. Sie ordnen ein BS-Profil einem Cloud-Konto, einem Standort (Rechenzentrum), einer Bildvorlage und einem Cloud-Skript zu. Attribute: Betriebssystem-Images, einschließlich BS-Typ und -Version, Root-Gerätetyp und Image-Quelle.	Bild [cmdb_ci_os_template]
Zeitplanprofil	Sie ordnen einem *Instanzzeitplan* ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll. Attribute: Zeitplanattribute, z. B. wann ein Stapel gestartet, gestoppt oder die Bereitstellung aufgehoben werden soll.	N/V

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Anwendungsprofil erstellen

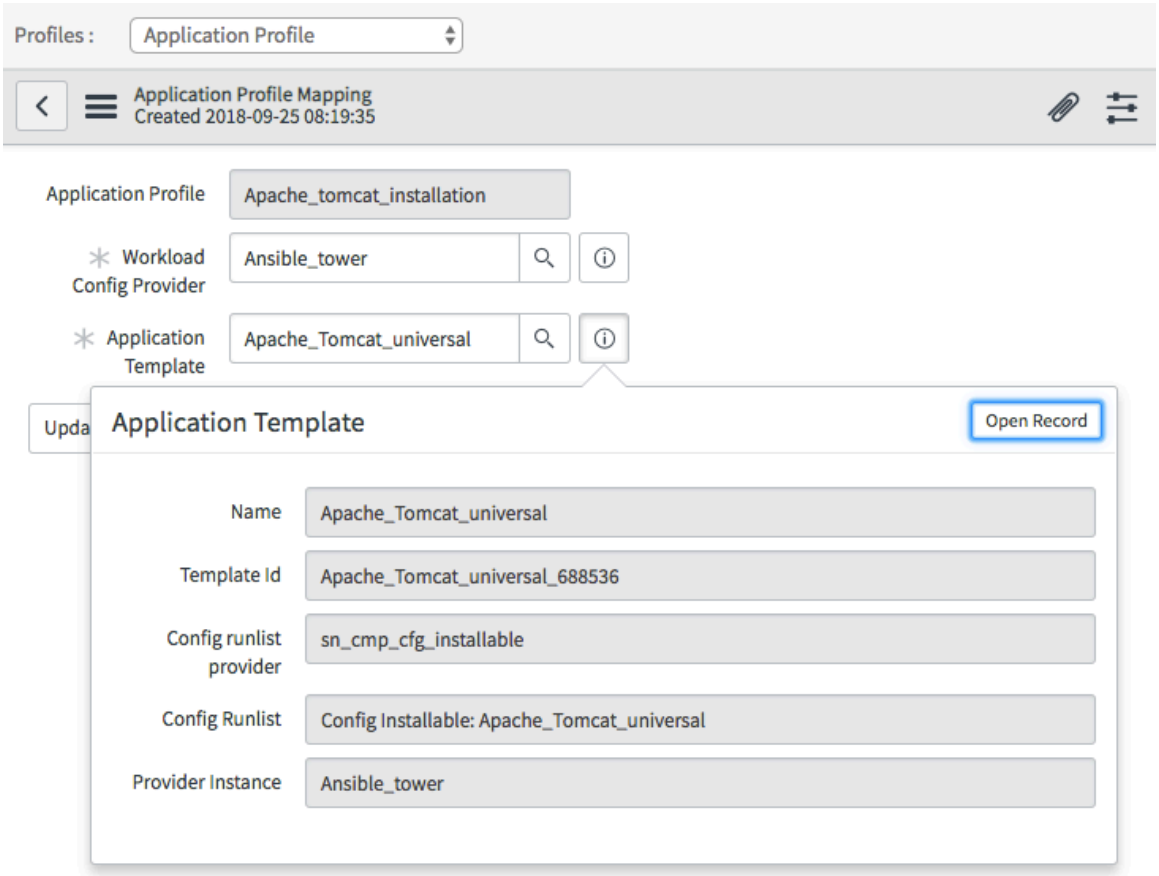
Ein Anwendungsprofil gibt Anwendungssoftware an, die auf neu bereitgestellten Ressourcen installiert werden soll. Benutzer können Anwendungen auswählen, wenn sie einen Stapel anfordern. Verwenden Sie Anwendungsprofile bei der Integration in Konfigurationsverwaltung (kontinuierliche Bereitstellung) von Providern wie Ansible Playbooks.

Vorbereitungen

- Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.
- Erforderliche Rolle: sn_cmp.cloud_admin

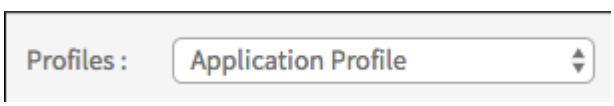
Warum und wann dieser Vorgang ausgeführt wird

Dieses Beispiel zeigt eine Anwendungsprofilzuordnung für einen Tomcat-Server in Ansible.



Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **Anwendungsprofil** aus, und klicken Sie dann auf **Neu**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.

   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.

   b. Klicken Sie in der zugehörigen Liste **Anwendungsprofilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Workload-Konfigurations-Provider	Wählen Sie einen Provider für Konfigurationsverwaltung aus, der dem Profil zugeordnet werden soll.
Applikationsvorlage [sn_cmp_application_template]	Wählen Sie eine Vorlage aus, der das Profil zugeordnet werden soll. Wenn Sie Discovery für den Konfigurations-Provider ausgeführt haben, sind die Vorlagen bereits ausgefüllt. Der einem Anwendungsprofil zugeordnete Ressourcentyp ist sn_cmp_application_template. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen. So erstellen Sie eine neue Vorlage: i. Klicken Sie auf das Referenzsymbol ( ), um die Liste der Anwendungsvorlagen zu öffnen. ii. Klicken Sie auf **Neu**, und füllen Sie das Formular der Anwendungsvorlage aus: ▪ **Name**: Geben Sie einen beschreibenden Namen für die Vorlage ein. ▪ **Vorlagen-ID**: Geben Sie eine ID für die Vorlage ein. ▪ **Provider der Konfig-Ausführungsliste**: Klicken Sie auf die Liste, wählen Sie eine Tabelle aus der Liste **Tabellenname** aus, und wählen Sie dann Datensätze für die Tabelle aus der Liste **Dokument** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ **Konfig-Ausführungsliste**: Geben Sie eine Konfigurations-Ausführungsliste an. ▪ **Provider-Instanz**: Wählen Sie eine Provider-Instanz aus.

5. Erstellen Sie so viele Zuordnungen wie nötig.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Computing-Profil erstellen

In einem Computing-Profil wird die Hardware für neu bereitgestellte virtuelle Computer angegeben. Ein Computing-Profil wird einem Cloud-Konto, einem Rechenzentrum und einer Hardwarevorlage zugeordnet.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

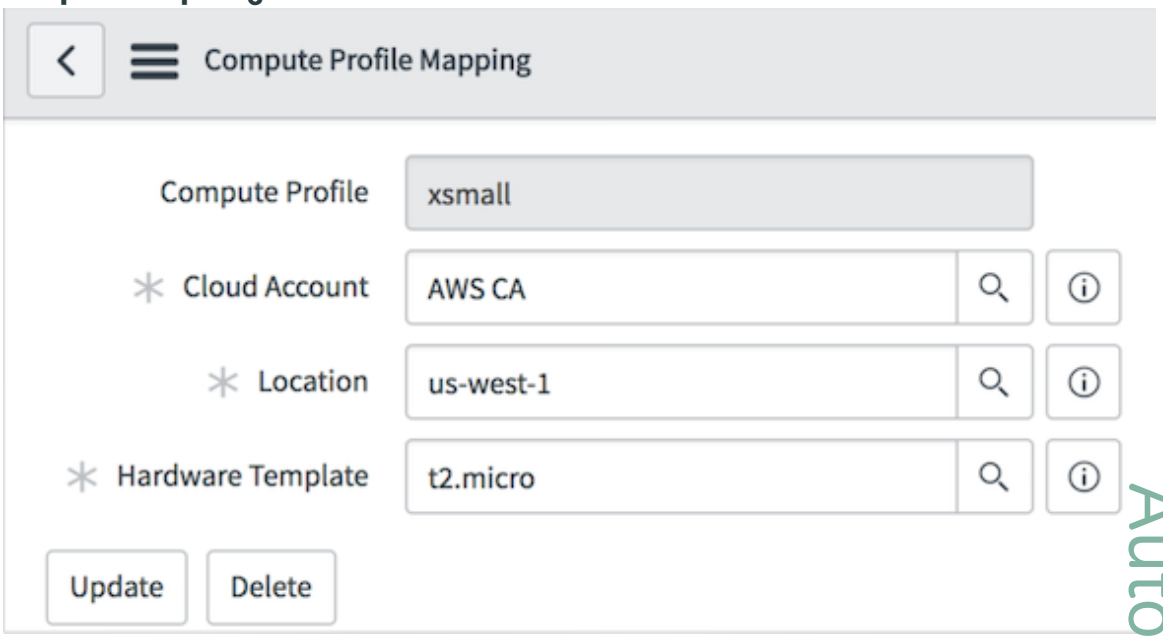
Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **Anwendungsprofil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Klicken Sie auf das von Ihnen erstellte Ressourcenprofil.
5. Ordnen Sie das Profil einer Vorlage zu.
   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.
   b. Klicken Sie in der zugehörigen Liste **Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Computing-Profil



Feld	Beschreibung
Cloud-Konto	Wählen Sie einen Cloud-Konto aus, für den das Profil gültig ist.
Standort	Wählen Sie das Rechenzentrum aus, für das das Profil gültig ist.
Hardwarevorlage [cmdb_ci_compute_template]	Wählen Sie einen Hardwaretyp aus, dem das Profil zugeordnet werden soll. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Computing-Sicherheitsgruppenprofil erstellen

Ein Computing-Sicherheitsgruppenprofil wendet bestimmte Sicherheitsregeln auf neu bereitgestellte Ressourcen an. Sie ordnen einem ein Berechtigungssicherheitsgruppenprofil zu Cloud-Konto, Ein Rechenzentrum, eine Vorlage für die Compute-Sicherheitsgruppe und Sicherheitsregeln für die Vorlage.

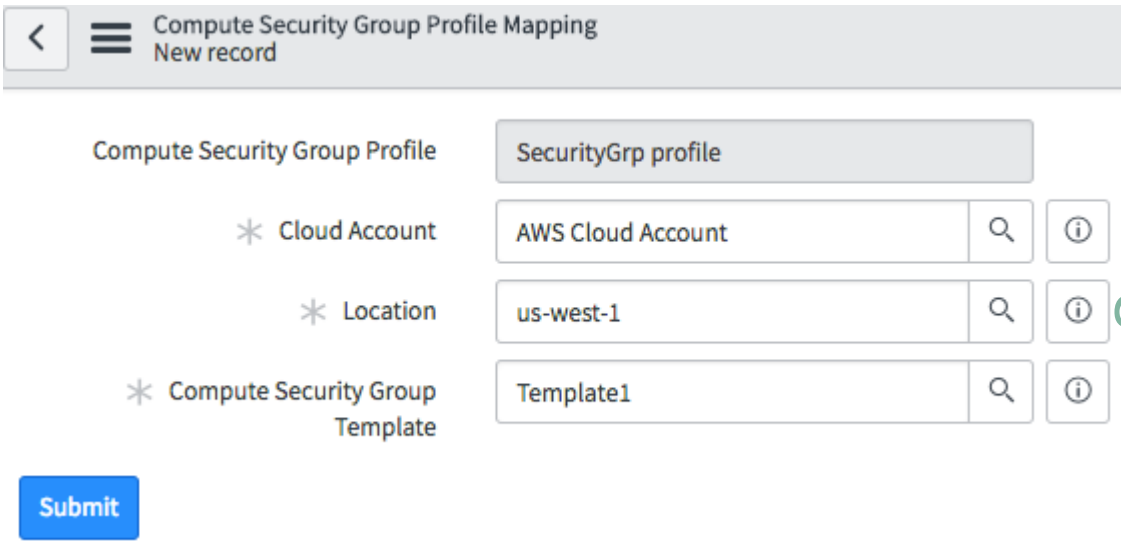
Vorbereitungen

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **Computing-Sicherheitsprofil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.
   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.
   b. Klicken Sie in der zugehörigen Liste **Computing-Sicherheitsgruppen-Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.



Feld	Beschreibung
Cloud-Konto	Wählen Sie einen Cloud-Konto für das Profil aus.
Standort	Wählen Sie das Rechenzentrum aus, das zum Cloud-Konto gehört.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sicherheitsgruppenvorlage berechnen [cmdb_ci_security_grp_template]	Wählen Sie eine Vorlage aus, der das Profil zugeordnet werden soll, oder erstellen Sie eine. Zum Erstellen einer neuen Vorlage klicken Sie auf das Listensymbol und dann auf **Neu**. Geben Sie einen Namen und eine Vorlagen-ID ein, und klicken Sie auf **Absenden**. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen.

5. Fügen Sie der Vorlage Regeln hinzu.
Sie können pro Vorlage mehrere Regeln erstellen.

a. Klicken Sie in der zugehörigen Liste **Sicherheitsgruppen-Profilzuordnungen** unter der Überschrift **Computing-Sicherheitsgruppenvorlage** auf den Vorlagennamen.

b. Klicken Sie in der zugehörigen Liste **Regelvorlage der Computing-Sicherheitsgruppen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
CIDR-Bereich	Geben Sie einen CIDR-Bereich an. Beispiel: 10.0.0.0/24
IP-Protokoll	Wählen Sie ein IP-Protokoll aus. In Azure werden die Protokolle TDP und UDP unterstützt. ICMP wird nicht unterstützt.
Von Port	Geben Sie die Quellportnummer an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ist ausgehend	Geben Sie 0 für eingehend und 1 für ausgehend ein.
Name	Geben Sie einen Namen für die Regel an.
Netzwerktyp	Wählen Sie den Typ des Netzwerks aus.
An Port	Geben Sie die Zielportnummer an.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

BS-Profil erstellen

Mit einem BS-Profil wird ein bestimmtes Image auf einem neu bereitgestellten virtuellen Computer installiert. Sie ordnen ein BS-Profil einem Cloud-Konto, einem Standort (Rechenzentrum), einer Bildvorlage und einem Cloud-Skript zu. BS-Profile sind anbieterunabhängig, und Sie können dasselbe Profil für mehrere Cloud-Accounts verwenden.

Vorbereitungen

- Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.
- Erforderliche Rolle: sn_cmp.cloud_admin

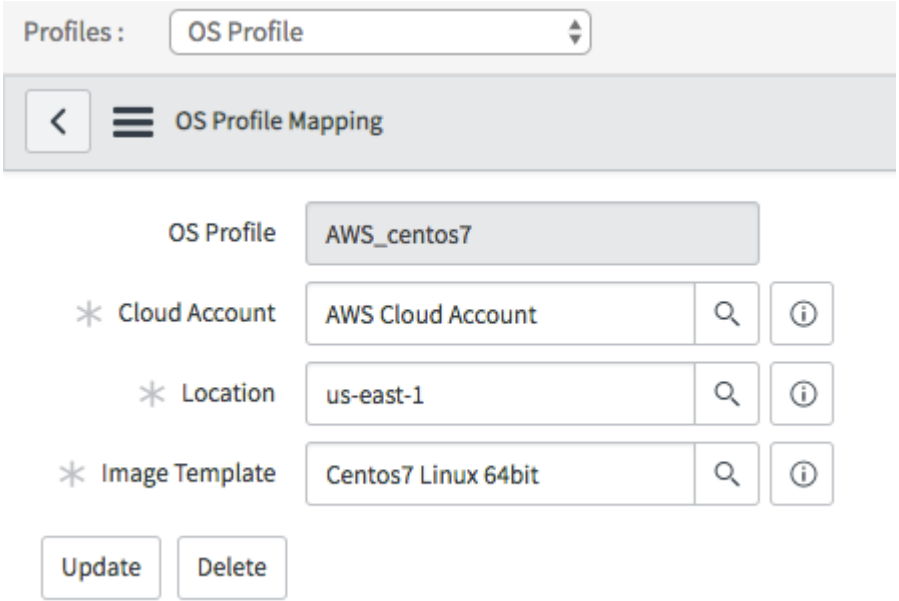
Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Profilzuordnungen, in denen mehr Details angegeben sind, werden zuerst ausgeführt. Beispielsweise hat eine Zuordnung, in der eine Blaupause, ein Betriebssystemprofil und ein Ressourcenalias angegeben sind, Vorrang vor einer Zuordnung, in der nur ein Betriebssystemprofil angegeben ist.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **BS-Profil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.
   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.
   b. Klicken Sie in der zugehörigen Liste **BS-Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Cloud-Konto	Wählen Sie den Cloud-Konto aus, dem das BS-Profil zugeordnet werden soll.
Standort	Wählen Sie ein Rechenzentrum im Cloud-Konto aus.
Bildvorlage [cmdb_ci_os_template]	Wählen Sie eine Bildvorlage aus, der das Profil zugeordnet werden soll. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen. **Wichtig:** Erstellen Sie keine neuen Bildvorlage. BildvorlagenMuss auf der Seite „Cloud-Accounts“ auf erkannt werden Portal für Cloud-Admin.(**Verwalten** > **Cloud-Accounts**) an. Wenn Sie einer Bildvorlage Anmeldeinformationen hinzufügen, werden die Anmeldeinformationen von allen VMs geerbt, die mithilfe der Vorlage bereitgestellt werden. Siehe Bildvorlagen Anmeldeinformationen hinzufügen.

5. Ordnen Sie das Profil einem Cloud-Skript zu. In diesem Verfahren geben Sie ein vorhandenes Skript an. Siehe Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der zugehörigen Liste „Cloud-Skript – BS-Profilzuordnungen“ auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Plan [Optional]	Wählen Sie eine Blaupause, um das Skript auf einen bestimmten, in der Blaupause verwendeten Ressourcenblock zu beschränken.
Cloud-Skript	Wählen Sie ein Cloud-Skript aus, dem das Betriebssystemprofil zugeordnet werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, wenn das Cloud-Skript nach der Bereitstellung des virtuellen Computers ausgeführt werden soll.
Applikation	Cloud Provisioning and Governance ist automatisch ausgewählt.
BS-Profil	Wenn Sie eine Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause bereitgestellt wird.
Ressourcen-Alias [Optional]	Wenn Sie einen Ressourcenalias für die Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause mit dem angegebenen Ressourcenalias bereitgestellt wird.

b. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
Das **Namensattribut** [scriptName] wird in der Liste „Überschreibungen der BS-Profilzuordnung“ aufgeführt.

c. Geben Sie in der Liste „Überschreibungen der BS-Profilzuordnung“ einen Attributnamen und einen Wert ein, die bei der Bereitstellung der Ressource verwendet werden.

Zeitplanprofil erstellen

Sie ordnen einem *Instanzzeitplan* ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **Zeitplanprofil** aus.
3. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitplan	Wählen Sie einen vorhandenen Zeitplan aus, oder definieren Sie einen benutzerdefinierten Zeitplan. Ein Zeitplan ist eine Regel, die bestimmte Zeiträume für Aktionen einschließt oder ausschließt. Verwenden Sie zum Definieren eines Zeitplans das **Systemzeitplaner**-Modul. Siehe Zeitplan definieren
Multiplikator	Automatisch ausgefüllter Wert zwischen 0 und 1: Der Bruchteil der Zeit, in dem erwartet wird, dass ein Stapel mit diesem Zeitplan eingeschaltet ist.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Bildvorlagen Anmeldeinformationen hinzufügen

Wenn Sie einer Bildvorlage Anmeldeinformationen hinzufügen, werden die Anmeldeinformationen von allen VMs geerbt, die mithilfe der Vorlage bereitgestellt werden.

Vorbereitungen

- Erforderliche Rolle: cloud_admin
- Eine Reihe von Anmeldeinformationen für die Standardauthentifizierung muss vorhanden sein.

Prozedur

1. Führen Sie eine der folgenden Aktionen aus:
   - Wenn der VM-Vorlage ein BS-Profil zugeordnet ist:
     a. Öffnen Sie das BS-Profil (**Verwalten** > **Ressourcenprofile**) an.
     b. Klicken Sie in der zugehörigen Liste „BS-Profilzuordnungen“ auf den **Namen** der Vorlage in der Spalte **Bildvorlage**.
   - Navigieren Sie für VMware-Vorlagen zu **Alle** > **Konfiguration** > **VMware** > **VM-Vorlagen**an.
2. Wählen Sie auf dem Formular „Image“ die **Anmeldeinformationen** der Standardauthentifizierung aus.
3. Klicken Sie auf **Aktualisieren**.

Öffentliches AWS-Image zu Cloud Provisioning and Governance hinzufügen

Sie können jedes AWS-Image in einem BS-Profil auswählbar machen.

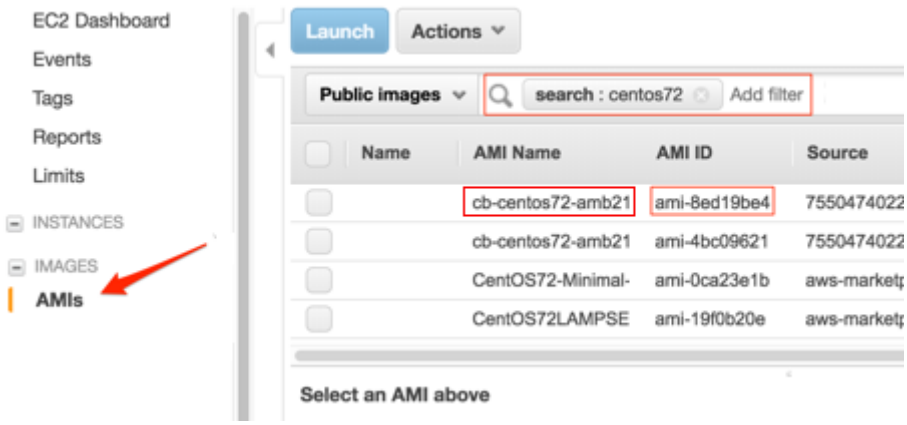
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie in der AWS-Konsole den EC2-Service aus, und klicken Sie dann auf **BILDER** > **AMIs**an.



2. Filtern Sie die Liste der Images, und notieren Sie sich die Werte für **AMI Name** und **AMI ID** für das gewünschte Image.
3. Geben Sie in der Instanz `cmdb_ci_os_template.list` in dem Textfeld **Filternavigator** zum Öffnen der Tabellen-Images [cmdb_ci_os_template] ein, und klicken Sie dann auf **Neu** .
4. Tragen Sie auf dem Formular **Image** die folgenden Werte ein:

Feld	Wert
Objekt-ID	**AMI ID**-Wert von AWS.
Name	Ein aussagekräftiger Name, der auf dem **AMI Name**-Wert von AWS basiert.
Gast-BS	Betriebssystem.

5. Im Feld **Berechtigungsnachweise** klicken Sie auf die Lupe und dann auf **Neu** auf der Berechtigungsnachweis-Seite.
6. Klicken Sie in der Liste auf **Grundlegende Berechtigungsnachweise**.
7. Geben Sie im Formular „Standard-Berechtigungsnachweise“ einen aussagekräftigen **Namen** für den Berechtigungsnachweis ein.
8. Geben Sie einen **Benutzernamen** ein, den Sie für Instanzen verwenden, die aus diesem Image bereitgestellt werden.

   In AWS werden SSH-Schlüssel verwendet, weswegen kein Passwort erforderlich ist.

   Hinweis: Wenn der Name `ec2-user` oder `root` nicht funktioniert, wenden Sie sich an Ihren AMI-Provider.

Richtlinien für Benutzernamen

Typ	Name
Amazon Linux	`ec2-user`
RHEL	`ec2-user` oder `root`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Name
Ubuntu	`ubuntu` oder `root`
Centos	`centos`
Fedora	`ec2-user`
SUSE	`ec2-user` oder `root`

9. Klicken Sie auf **Senden**, um das Formular „Basic Auth Credentials“ zu schließen.
10. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern**, um die aktuelle Konfiguration des neuen Image-Datensatzes zu speichern.
    In der Liste „zugehörige Elemente“ können Sie sehen, dass das Image dem angegebenen Datencenter zugeordnet ist.
11. Klicken Sie auf **Aktualisieren**, um das öffentliche Image in einem OS-Profil auswählbar zu machen.
    Dieser Schritt erstellt auch eine Beziehung zwischen dem öffentlichen Image und dem logischen Datencenter (LDC) in der CMDB.

Öffentliches Azure-Image zu Cloud Provisioning and Governance hinzufügen

Sie können jedes Azure-Image in einem BS-Profil auswählbar machen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Notieren Sie sich in der Azure-Befehlszeilenschnittstelle (CLI) die Werte für **Offer**, **Publisher**, **Sku** und **Version**.

   In der Befehlszeile können Sie nach „offer“ (Angebot) oder nach „publisher“ (Herausgeber) oder nach beidem suchen, wie im Beispiel gezeigt. Jeder Einzelposten ist ein Image einer bestimmten Version von CentOS von OpenLogic.

   Sie können den folgenden Beispielbefehl in der CLI verwenden, um die Werte abzurufen:
   `az vm image list -f Windows --output table`

```
:~ jsher.able$ az vm image list --offer CentOS --publisher OpenLogic --all --output table
Offer     Publisher   Sku   Urn                 Version
--------  ----------  ----  ------------------  -----------
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.201501
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.201503
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.201506
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.20150904
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.20160309
CentOS    OpenLogic   6.5   OpenLogic:CentOS  6.5.20170207
```

2. Geben Sie in der Instanz `cmdb_ci_os_template.list` in dem Textfeld **Filternavigator** zum Öffnen der Tabellen-Images [cmdb_ci_os_template] ein, und klicken Sie dann auf **Neu** .
3. Konfigurieren Sie das Formularlayout, um **Offer** (Angebot), **Serial number** (Seriennummer), **Version** und **Vendor** (Lieferant) anzuzeigen.
4. Tragen Sie auf dem Formular Image die folgenden Werte ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Objekt-ID	Geben Sie `/Herausgeber/Angebot/SKU/Version` ein. Sie können diese Werte von der Azure-Befehlszeilenschnittstelle abrufen. Beispiel: `/OpenLogic/CentOS/6.5/6.5.201501`.
Name	Aussagekräftiger Name, der die Version des Betriebssystems darstellt, `CentOS 6.5` im Beispiel.
Gast-BS	Betriebssystem.
Angebot	Wert **Offer** (Angebot) von Azure.
Seriennummer	Wert **Sku** von Azure.
Version	Wert **Version** von Azure.
Lieferant	**a.** Klicken Sie auf die Lupe und dann auf **Neu**. **b.** Geben Sie im Feld **Name** den Wert für **Publisher** (Herausgeber) von Azure ein. **c.** Klicken Sie auf **Absenden**.

5. Im Feld **Berechtigungsnachweise** klicken Sie auf die Lupe und dann auf **Neu** auf der Berechtigungsnachweis-Seite.
6. Klicken Sie in der Liste auf **Grundlegende Berechtigungsnachweise**.
7. Geben Sie im Formular „Standard-Berechtigungsnachweise“ einen aussagekräftigen **Namen** für den Berechtigungsnachweis ein.
8. Geben Sie einen **Benutzernamen** und ein **Passwort** zum Nutzen von Instanzen ein, die aus diesem Image bereitgestellt werden.
9. Klicken Sie auf **Senden**, um das Formular „Basic Auth Credentials“ zu schließen.
10. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern**, um die aktuelle Konfiguration des neuen Image-Datensatzes zu speichern.
    In der Liste „zugehörige Elemente“ können Sie sehen, dass das Image dem angegebenen Datencenter zugeordnet ist.
11. Klicken Sie auf **Aktualisieren**, um das öffentliche Image in einem OS-Profil auswählbar zu machen.
    Dieser Schritt erstellt auch eine Beziehung zwischen dem öffentlichen Image und dem logischen Datencenter (LDC) in der CMDB.

IPAM-Integration

Verwenden Sie ein IPAM-Tool (IP Address Management) wie Infoblox, um Cloud-IP-Adressen, Netzwerke und Subnetze in Ihren Cloud-Katalogangeboten zu verwalten. Es ist jedoch wichtig zu beachten, dass diese Funktionalität von unseren vorlagenbasierten Cloud-Katalogen nicht unterstützt wird.

Infoblox-Integration

Standardmäßig unterstützt Cloud Provisioning and Governance die Infoblox-Integration. Sie können Infoblox-Anmeldeinformationen erstellen und dann einen Infoblox-Instanzdatensatz einrichten. Siehe Infoblox-Server registrieren für Anweisungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die IPAM-Integration wird mit vorlagenbasierten Cloud-Katalogelementen nicht unterstützt.

Hinweis: Diese Integration wird nur mit Legacy-Blueprints unterstützt. Lesen Sie hierzu Knowledge Base artikel, um mehr zu erfahren.

Subnetze

Wenn Sie Subnetze in Ihren AWS- und Azure-Clouds haben, findet Cloud Provisioning and Governance diese, wenn Discovery für ein Servicekonto oder Cloud-Konto ausgeführt wird.

Hinweis: Wenn Sie Netzwerke und Subnetze in einer VMware vSphere-Plattform haben, erstellt Discovery keine Subnetzdatensätze in der CMDB und kann das Subnetz nicht dem entsprechenden Netzwerk zuordnen. Sie müssen die Datensätze manuell erstellen.

Infoblox-Server registrieren

Für die Integration von Infoblox müssen Sie einen Infoblox-Datensatz erstellen und ihn den entsprechenden Anmeldeinformationen zuordnen, um Ihren Infoblox-Server bei der Instanz zu registrieren.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_admin
- Erstellen Infoblox-Anmeldeinformationen .

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Netzwerke und IPAM** > **IPAM-Provider** > **Infoblox**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
URL	Geben Sie die URL des Infoblox-Servers ein.
Anmeldeinformationen	Wählen Sie die Infoblox-Anmeldeinformationen aus.

IP-Pool erstellen

Erstellen Sie einen IP-Pool, um ein Cloud-Subnetz einer IPAM-Provider-Instanz zuzuordnen.

Vorbereitungen

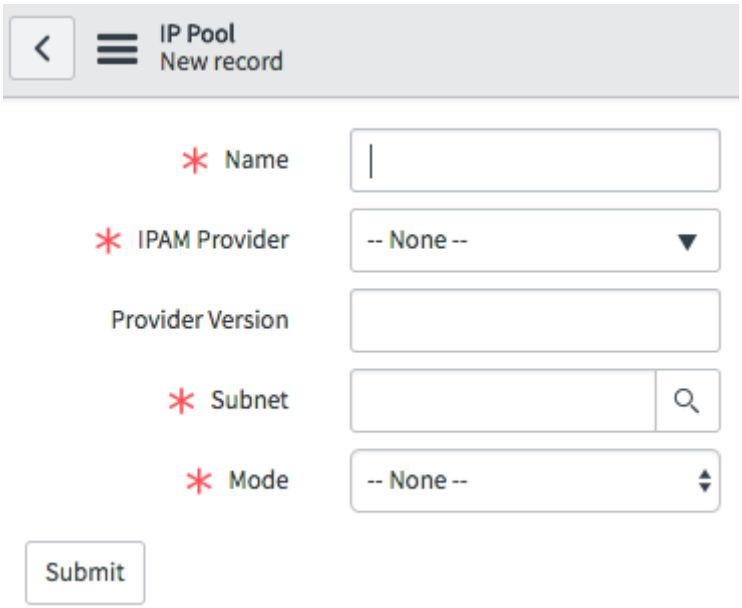
- Erforderliche Rolle: sn_cmp.cloud_admin
- Erstellen Infoblox-Anmeldeinformationen Und Registrieren Sie einen Infoblox-Server .
- Führen Sie Discovery für den Cloud-Konto aus, um Subnetze zu finden, oder erstellen Sie Cloud-Subnetze manuell.

Hinweis: Diese Funktionalität wird in unseren vorlagenbasierten Cloud-Katalogen nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Netzwerke und IPAM**an.
2. Klicken Sie auf der Registerkarte **IP-Pools** auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** ein, und füllen Sie dann das Formular aus.



Feld	Beschreibung
IPAM-Anbieter	Wählen Sie einen IPAM-Provider aus.
Provider-Instanz	Wählen Sie eine Instanz für den Provider aus.
Providerversion	Geben Sie eine Version für den Provider ein.
Subnetz	Wählen Sie ein Subnetz aus. Wählen Sie für AWS oder Azure ein erkanntes Subnetz aus, das in AWS oder Azure konfiguriert wurde. Für VMware kopieren Sie den CIDR-Bereich aus dem IPAM-Tool, und fügen Sie den CIDR-Bereich in dieses Feld ein. Weitere Informationen finden Sie unter Cloud-Subnetz erstellen.
Modus	Wählen Sie basierend auf dem Provider, für den Sie diesen IP-Pool erstellen, einen Modus aus. Der Modus hängt vom Provider ab.

3. Klicken Sie auf **Absenden**.

Ergebnis

Das zugehörige Subnetz wird in der zugehörigen Liste **Subnetz** am unteren Rand des Formulars angezeigt.

Cloud-Subnetz erstellen

Wenn Ihr VMware vSphere-Konto über Subnetze verfügt, erstellen Sie in der Instanz einen Cloud-Subnetz-Datensatz.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Netzwerke und IPAM**an.
2. Klicken Sie auf der Registerkarte **IP-Pools** auf **Neu**, um einen neuen Datensatz zu erstellen.
3. Klicken Sie im Feld **Subnetz** auf das Suchsymbol.
   Die Liste der Cloud-Subnetze wird angezeigt.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Status	Behalten Sie den Statuswert **Installiert** bei.
CIDR/ Gateway/ Subnetzmaske	Geben Sie die dem Subnetz zugeordnete CIDR, die IP-Adresse des Gateways und die Subnetzmaske ein. Für VMware sind die Felder „CIDR“, „Gateway“ und „Subnetzmaske“ obligatorisch.
Primäres und sekundäres DNS	Geben Sie die DNS-Werte ein. Für VMware, ist das Feld „Primäre DNS“ obligatorisch.

6. Klicken Sie auf **Absenden**.

Beziehung zwischen einem VMware-Netzwerk und einem Subnetz erstellen

Wenn Sie VMware-Netzwerke und Subnetze erkennen, müssen Sie manuell eine Beziehung zwischen beiden erstellen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn keine Beziehung vorhanden ist und ein Benutzer ein virtuelles Netzwerk und Subnetz im Cloudbenutzerportal auswählen muss, kann ein Fehler auftreten.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Service-Konten**an.
2. Öffnen Sie das Rechenzentrum, das das VMware-Cloud-Netzwerk enthält.

   Hinweis: VMware-Cloud-Netzwerke werden in der Tabelle „VMware vCenter-Netzwerk“ [cmdb_ci_vcenter_network] gespeichert. AWS- und Azure-Cloud-Netzwerke werden in der Tabelle „Cloud-Netzwerke“ [cmdb_ci_network] gespeichert.

3. Klicken Sie unter **Zugehörige Elemente** auf das Pluszeichen, um eine neue Beziehung hinzuzufügen.
4. Stellen Sie sicher, dass das Kontrollkästchen **Vorgeschlagene Beziehungen verwenden** aktiviert ist, und wählen Sie dann die Beziehung **Enthält (Übergeordnet)** aus.
5. Erstellen Sie unter **Filter** den erforderlichen Filter, um das Subnetz zu finden.
6. Aktivieren Sie unter **Konfigurationselemente** das Kontrollkästchen neben dem Subnetz.
7. Klicken Sie im Abschnitt **Beziehungen** auf das Pluszeichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Beziehung wird der Liste hinzugefügt.

8. Klicken Sie auf **Speichern und Beenden**.

IP-Adressen für VMware vSphere-VMs in InfoBlox reservieren

Erstellen Sie zum Zeitpunkt der Bereitstellung der virtuellen Computer eine Richtlinie zum Reservieren von IP-Adressen für VMware vSphere-VMs in Infoblox.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Richtlinie erstellen, die aufgerufen wird, wenn eine VMware-VM bereitgestellt wird, um eine IP-Adresse von Infoblox zu erhalten. Vor der Bereitstellung des virtuellen Computers ruft die Instanz Infoblox auf, das einen Hostdatensatz mit der IP-Adresse erstellt.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface provision** (Schnittstellenbereitstellung für virtuellen Server) aus.
Moment	Wählen Sie **Vor dem Vorgang** aus.

3. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
4. Erstellen Sie eine Richtlinienregel für die Richtlinie.
5. Geben Sie im Bedingungsgenerator eine Bedingung für die Suche nach der vSphere-VM an.
6. Auswahlvorgang **Anforderung von** > **beginnt mit** Und geben Sie ein `VSphere` .
7. Klicken Sie auf **Aktualisieren**.
8. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
9. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
10. Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse reservieren** aus.
11. Klicken Sie auf **Absenden**.
12. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen Ihres Netzwerks im Feld **DNSSuffix** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: corp.servicenow.com. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.

13. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

IP-Adressen für AWS- und Azure-VMs in Infoblox registrieren

Erstellen Sie eine Richtlinie zum Reservieren von IP-Adressen für AWS- und Azure-VMs in Infoblox, nachdem diese virtuellen Computer bereitgestellt wurden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn AWS- und Azure-VMs bereitgestellt werden, werden ihnen automatisch IP-Adressen zugewiesen. Sie können eine Richtlinie erstellen. Die Richtlinie wird aufgerufen, sobald diese virtuellen Computer bereitgestellt wurden, um ihre IP-Adressen abzurufen und diese IP-Adressen in Infoblox zu registrieren.

Hinweis: Diese Funktionalität wird in unseren vorlagenbasierten Cloud-Katalogen nicht unterstützt.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface provision** (Schnittstellenbereitstellung für virtuellen Server) aus.
Moment	Wählen Sie **Vor dem Vorgang** aus.

3. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
4. Erstellen Sie eine Richtlinienregel für die Richtlinie.
   Geben Sie im Bedingungsgenerator zwei Bedingungen für die Suche nach AWS- und Azure-VMs an. Auswahlvorgang **Anforderungsformular** > **beginnt mit** Und geben Sie ein AWS . Geben Sie eine andere Bedingung für Azure an.
5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
7. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
   Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse registrieren** aus.
8. Klicken Sie auf **Absenden**.
9. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen des Netzwerks Ihres Unternehmens im Feld **DNSSuffix** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: corp.servicenow.com. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.

10. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

Hostdatensatz in Infoblox löschen

Wenn die Bereitstellung eines virtuellen Computers aufgehoben wird, löschen Sie den Hostdatensatz aus Infoblox. Durch das Löschen des Hostdatensatzes kann diese IP-Adresse für andere virtuelle Computer verfügbar sein und verwendet werden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „Richtlinie“ aus (siehe Tabelle).

Feld	Wert
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface Deprovision** (Schnittstellenbereitstellung für virtuellen Server aufheben) aus.
Moment	Wählen Sie **Nach dem Vorgang** aus.

4. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
5. Erstellen Sie eine Richtlinienregel für die Richtlinie, und klicken Sie auf **Aktualisieren**.
6. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
7. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
   Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse freigeben** aus.
8. Klicken Sie auf **Absenden**.
9. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen des Netzwerks Ihres Unternehmens im Feld **DNSSuffix** ein.
   Beispiel: corp.servicenow.com. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.
10. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

Support für kontinuierliche Bereitstellung (Konfigurationsverwaltung)

Die Cloud Provisioning and Governance-Anwendung unterstützt die Integration in Lösungen zur kontinuierlichen Bereitstellung (auch bekannt als Konfigurationsverwaltung). Ansible wird als Standard-Provider für Konfigurationsverwaltung unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung Cloud Provisioning and Governance unterstützt Konfigurationsverwaltungs-Provider auf zwei Arten:

- **Ansatz auf Basis des Anwendungsprofils**: Erstellen Sie ein Anwendungsprofil für eine Entität, und wählen Sie im Bestellkatalogformular dieses Profil aus, um diese Entität bereitzustellen. Jedes Profil verfügt über eine installierbare Konfiguration. Sie können mehrere Anwendungsprofile erstellen, z. B. eines für PostgreSQL und eines für Apache. Jedes Profil kann einem Konfigurationsverwaltungs-Provider zugeordnet werden. Im Cloudbenutzerportal wird basierend auf dem von Ihnen ausgewählten Profil ein Konfigurationsraster mit Attributen und Werten für den jeweiligen Konfigurationsverwaltungs-Provider angezeigt. Sie können alle Werte im Bestellformular ändern und die Entität bereitstellen.
- **Ansatz auf Basis des Ressourcenblocks**: Verwenden Sie einen Ressourcenblock wie Apache2 in einer Blaupause, um eine Entität darzustellen, die von einem Konfigurationsverwaltung-Provider verwaltet wird. Derselbe Ressourcenblock kann zur Unterstützung von mehr als einer Entität derselben Art verwendet werden. Beispielsweise kann ein Apache2-Ressourcenblock zur Unterstützung mehrerer Apache2-Server verwendet werden. Wählen Sie im Bestellkatalogformular einen Provider-Typ aus, und wählen Sie dann einen Provider aus. Basierend auf dem spezifischen Provider werden Konfigurationsverwaltungsattribute und -werte angezeigt. Sobald Sie die Entität bereitgestellt haben, können Sie die Konfiguration des Ressourcenblocks speichern und in der CMDB für die zukünftige Verwendung ablegen.
- **Aktionen nach der Bereitstellung während der Katalogbereitstellung** : Anwender können den ansible-Auftrag als Schritt nach der Bereitstellung in jedem Katalog aufrufen, der eine VM bereitstellt. Dies wird als Tag-2-Vorgang ausgeführt, sobald die VM-Installation abgeschlossen ist. Weitere Informationen zu den Prozessen finden Sie unter https://www.servicenow.com/community/itom-blog/cpg-calling-ansible-job-as-post-provision-step-for-cloud-catalog/ba-p/2271552 Und https://www.servicenow.com/community/itom-blog/cpg-calling-ansible-job-as-day2-operation/ba-p/2270969 .

Wichtig: Beginnend mit dem Release Orlando sind Blaupausen für die Cloud-Bereitstellung in Instanzen verfügbar, für die ein Upgrade von einem früheren Release durchgeführt wurde. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.

Beschreibung

Schritt	Ziel	Siehe diese Themen
1. Erstellen Sie Anmeldeinformationen für Ansible.	Aktivieren Sie Cloud Provisioning and Governance, um auf den Konfigurations-Provider mit den erforderlichen Anmeldeinformationen zuzugreifen.	Ansible Tower-Benutzernamen und -Passwort konfigurieren
2. Erstellen Sie den Workload-Provider-Typ und dann den Provider.	Konfigurieren Sie Cloud Provisioning and Governance, mit dem Konfigurationsverwaltungs-Provider Ihrer Wahl zu arbeiten. Führen Sie dann Discovery für den Provider mit den von Ihnen angegebenen Anmeldeinformationen aus, um die Ressourcen zu finden, die der Provider bereits besitzt.	Erstellen Sie einen Arbeitsauslastungsanbietertyp und Ansible-Konfigurationsverwaltungs-Provider erstellen und Discovery ausführen
3. Erstellen Sie ein Anwendungsprofil mit einer Zuordnung.	Erstellen Sie das Profil, das die Anwendung definiert, die vom Konfigurationsverwaltungs-Provider verwaltet wird. Das Profil basiert auf den erkannten Beständen beim Provider.	Anwendungsprofil erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Ziel	Siehe diese Themen
4. Erstellen Sie eine Blaupause.	Erstellen Sie eine Blaupause mit den Vorgängen *BootstrapNode*, *Register Node* und *ExecuteConfigPackages* für die virtuelle Ressource, die der Konfigurations-Provider verwaltet. Sie können auch die Eingabeparameter im Formular anpassen, damit der Benutzer wichtige Eingaben auswählen kann, z. B. die Anwendungsprofilvorlage, die Organisation und die Anmeldeinformations-ID.	
5. Stellen Sie im Cloudbenutzerportal eine Ressource bereit.	Die Ressource muss bereitgestellt werden, wobei der Stapelstatus die Schritte *BootstrapNode*, *Register Node* und *ExecuteConfigPackages* angibt.	

Ansible Tower-Benutzernamen und -Passwort konfigurieren

Konfigurieren Sie Ansible Tower-Anmeldeinformationen, um über Ihre Instanz auf die Ansible Automation Engine zuzugreifen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Navigieren zu **Alle** > **Orchestration** > **Anmeldeinformationen**, Und klicken Sie dann auf **Neu** .
2. Klicken Sie auf **Ansible Tower-Anmeldeinformationen**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle):

Zur Integration von Cloud Provisioning and Governance mit dem Ansible-Konfigurationsverwaltungskonto müssen Benutzername und Passwort für das Administratorkonto in Ansible konfiguriert werden.

Formularfelder für Ansible Tower-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Benutzername/ Passwort	Geben Sie die Authentifizierungsinformationen für den Ansible Tower-Benutzer mit Administratorrechten ein.

Hinweis: Sie müssen keine anderen Felder konfigurieren

Erstellen Sie einen Arbeitsauslastungsanbietertyp

Erstellen Sie einen Workload-Provider-Typ für jeden neuen Konfigurationsverwaltungs-Provider. Diese Informationen werden im Bestellkatalogformular als Verwaltungsattribute angezeigt, die Ihre Benutzer auswählen können, wenn sie eine virtuelle Ressource über einen Konfigurationsverwaltungs-Provider bereitstellen.

Vorbereitungen

Erforderliche Rolle: cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

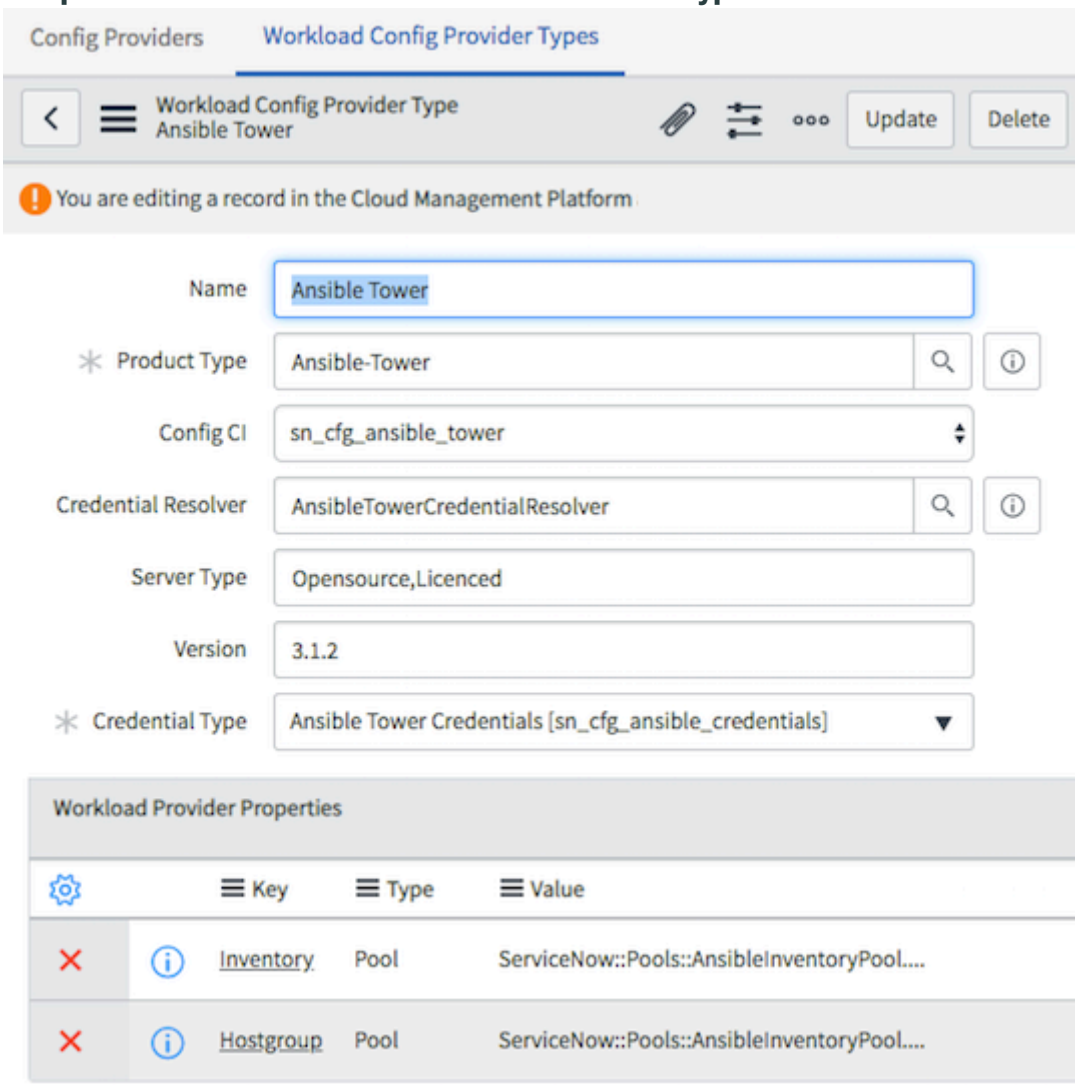
1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Konfigurationsverwaltung**an.
2. Klicken Sie auf **Workload-Konfigurations-Provider-Typen** und dann auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Formular „Workload-Konfigurations-Provider-Typ“

Feld	Beschreibung
Name	Geben Sie einen Namen für den Workload-Provider-Typ ein.
Produkttyp	Ein Cloud-Produkttyp aus der Liste
Konfigurations-CI	Wählen Sie die für den Provider erstellte Konfigurationstabelle aus der Liste aus, die die erkannten Ressourcen anzeigt.
Resolver für Anmeldeinformationen	Wählen Sie einen Anmeldeinformations-Resolver aus der Liste aus.
Servertyp	Wählen Sie den Servertyp für den Provider aus, z. B. „OpenSource“, „Enterprise“ usw.
Version	Geben Sie eine Version für den Provider ein.
Anmeldeinformationstyp	Wählen Sie die Tabelle aus, in der die Anmeldeinformationen für diesen Provider gespeichert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für einen Ansible Tower-Workload-Provider-Typ



4. Fügen Sie im Abschnitt **Workload-Provider-Eigenschaften** Eigenschaften für den Workload-Typ hinzu.
   Zusätzlich zu den vorhandenen Eigenschaften können Sie weitere Eigenschaften hinzufügen. Workload-Provider-Eigenschaften werden im Bestellkatalogformular (im Cloudbenutzerportal) als Verwaltungsattribute angezeigt.

   Beispiel: Für einen Ansible-Anbietertyp **Bestand** , Und **Hostgruppe** Sind obligatorisch. Die Werte für diese Eigenschaften stammen aus Ressourcenpools.

5. Klicken Sie auf **Absenden**.

Ansible-Konfigurationsverwaltungs-Provider erstellen und Discovery ausführen

Erstellen Sie einen Ansible Configuration Management Provider, und führen Sie dann aus Discovery Auf dem Anbieter, um seine Ressourcen zu finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass Sie über einen Ansible-Server und verfügen Ansible-Anmeldeinformationen .
- Wenn Sie Ansible Tower Version 3,6.x oder höher verwenden möchten, stellen Sie sicher, dass die Eigenschaft „Mid.CMP.ansible.api_Version“ auf V2 festgelegt ist. Sie können auf diese Eigenschaft im Abschnitt Eigenschaften des MID-Server-Moduls zugreifen.
- Erforderliche Rolle: cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wichtig: Beginnend mit Orlando Release: Die Cloud-Bereitstellungs-Blueprints sind für Instanzen verfügbar, die von einem vorherigen Release aktualisiert wurden, Sie können jedoch keinen Blueprint erstellen. Vorhandene Blueprints und Katalogelemente, die aus diesen Blueprints erstellt wurden, bleiben unverändert und funktionieren weiter.

Prozedur

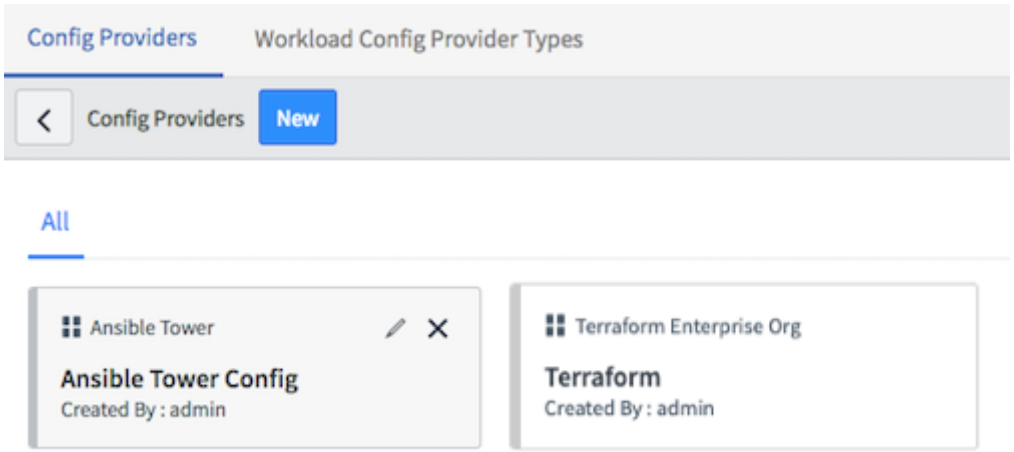
1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Konfigurationsverwaltung**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Hinweis: Die meisten Informationen, die zum Erstellen eines Ansible-Konfigurationsverwaltungsanbieters erforderlich sind, stammen aus dem Ansible TowerServereinstellungen.

Feld	Beschreibung
Name	Beschreibender Name für den Konfigurationsanbieter.
Organisation	Ansible Tower Organisation für Zugriffssteuerung Sie können diese Informationen über die Konsole des Konfigurationsverwaltungs-Providers abrufen.
URL	URL des Ansible Tower. Geben Sie die vollständige URL des ein Ansible TowerEinschließlich https:// <IP> protokoll.
Anbieter	Konfigurations-Provider-Typ. Wählen Sie Aus **Ansible Tower** Aus der Dropdown-Liste.
Servertyp	Ansible Tower-Servertyp.
Anmeldeinformation	Anmeldeinformationen für den Zugriff auf den Ansible-Server. Weitere Informationen zum Erstellen von Anmeldeinformationen für Ansible-Server finden Sie unter Ansible-Anmeldeinformationen .
Version	Version des Konfigurationsanbieters, den Sie erstellen. **Hinweis:** Für Ansible Tower-Versionen über 3.1.2 wählen Sie 3.4.0 aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Absenden**.
5. Wählen Sie die Ansible Tower-Konfigurations-Provider-Karte aus.



6. Wählen Sie Aus **Entdecken Sie Jetzt** Um die Ressourcen im Ansible Configuration Management Provider zu finden.

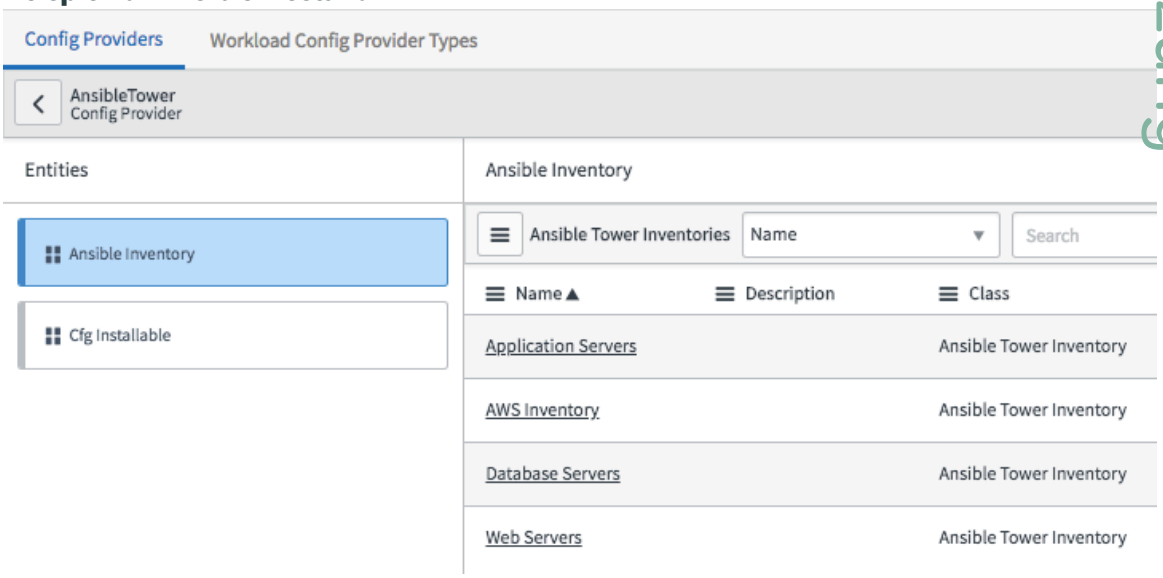
Hinweis: Wenn Sie Ressourcen über die Schnittstelle des Konfigurationsverwaltungsanbieters bereitstellen oder anderweitig ändern, müssen Sie die Discovery manuell erneut über die Seite „Anbieter konfigurieren“ ausführen. Sie können keine geplante Discovery für Konfigurationsverwaltungs-Provider erstellen.

Die erkannten Ressourcen werden unter **Entitäten** angezeigt.

Die folgenden Ansible Tower-Ressourcen werden erkannt:

- **Ansible Inventory** : Zeigt die erkannten Anwendungen und virtuellen Ressourcen an.
- **Cfg Installierbar** : Zeigt die tatsächlichen Komponenten an, die bei der Installation der Anwendungen ausgeführt werden. Für Ansible sind die Elemente in dieser Liste Auftragsvorlagen, die auch als bezeichnet werden *Ausführungslisten* In diesem Formular.

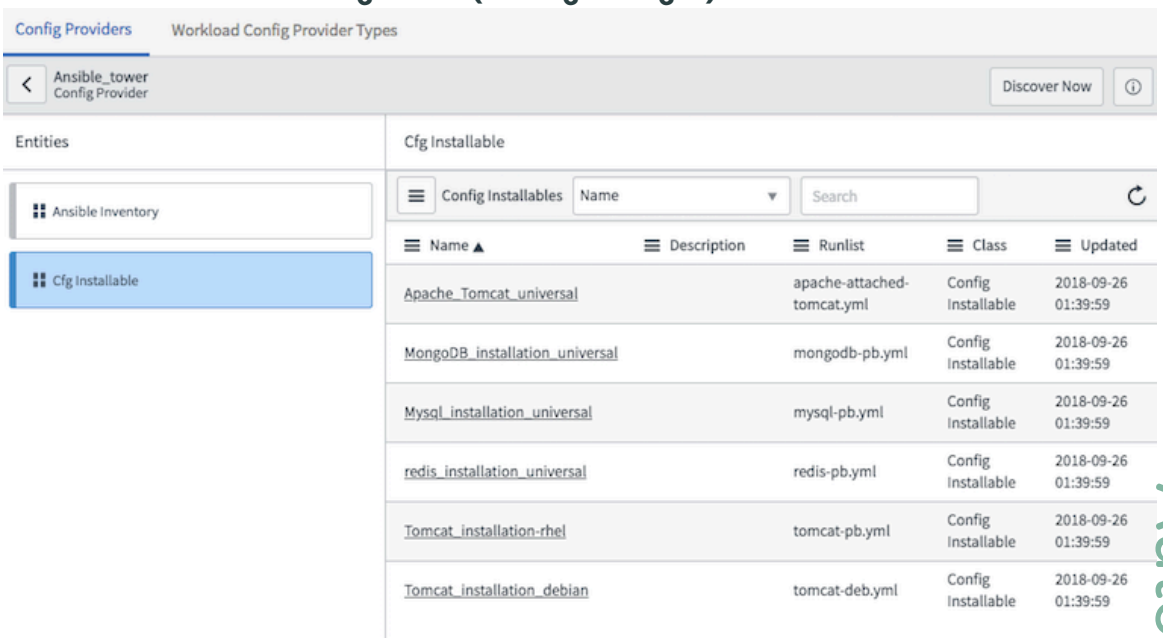
Beispiel für Ansible-Bestand



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

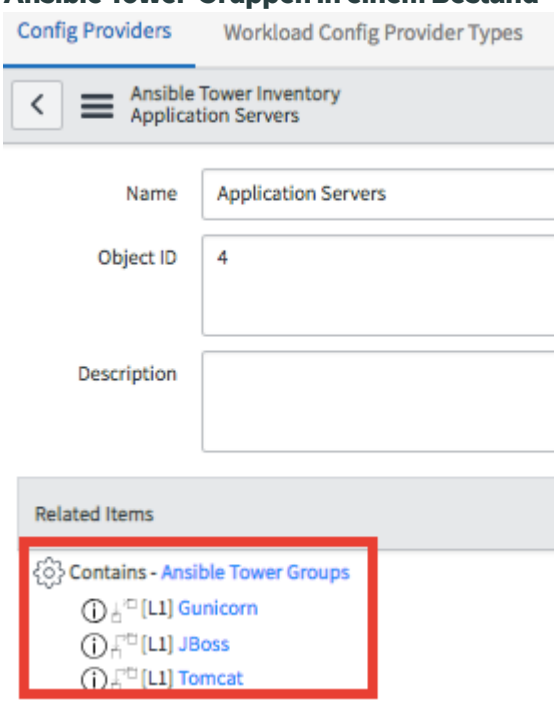
Installierbare Ansible-Konfiguration (Auftragsvorlagen)



7. Wählen Sie Aus **Ansible Inventory** Um die Inhalte zu erkunden.

Hinweis: Teilen Sie Benutzern die unterstützten Anwendungen mit, damit sie die richtige Anwendung aus dem Feld **Hostgruppe** im Cloudbenutzerportal auswählen können. Das Feld **Hostgruppe** zeigt alle möglichen Anwendungen (in Ansible *Gruppen* genannt), nicht nur die, die der Konfigurationsverwaltungs-Provider unterstützt. Daher schlägt die Bereitstellung fehl, wenn der Anwender eine nicht unterstützte Anwendung auswählt.

Ansible Tower-Gruppen in einem Bestand



Nächste Maßnahme

Nachdem ein Anwender eine Ressource bereitgestellt hat , Der Stapelstatus gibt an, wie das System die Schritte „Knoten erstellen“, „Bootstrap“ und „ExecuteConfigPackage“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

durchläuft. Sie können die IP-Adresse einer virtuellen Maschine im Anwenderportal abrufen, indem Sie zu navigieren **Stapel** > **{Category}** Und Auswahl der neuen virtuellen Maschine. Öffnen Sie den Konfigurationsverwaltungs-Provider-Server, um die neu bereitgestellte Ressource auf dem vom Benutzer angegebenen Knoten anzuzeigen.

Cloud Provisioning and Governance: Terraform Connector

Verwenden Sie ServiceNow® Cloud Provisioning and Governance: Terraform Connector Dient zum Generieren von Katalogelementen aus Terraform Vorlagen und verwenden Sie sie, um Ressourcen in verschiedenen Clouds bereitzustellen und zu verwalten.

Erste Schritte

Untersuchen	Konfigurieren
Erfahren Sie mehr über Cloud Provisioning and Governance: Terraform Connector Anwendung.	Planen und konfigurieren Sie Ihre Implementierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
Verwenden Sie Cloud Provisioning and Governance: Terraform Connector App zum Erkennen von Ressourcen aus Terraform Umgebung, erstellen Sie Katalogelemente, und verwalten Sie sie.	Rufen Sie Details zu Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Problembehandlung und Hilfe

- Cloud Provisioning and Governance -forum auf der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Cloud Provisioning and Governance: Terraform Connector erkunden

Ob Sie Ihre Implementierung von beginnen oder erweitern Cloud Provisioning and Governance: Terraform Connector, Erfahren Sie mehr über die verfügbaren Funktionen, die bei der Bereitstellung und Verwaltung von Cloud-Ressourcen in verschiedenen öffentlichen und privaten Clouds helfen.

Die Cloud Provisioning and Governance: Terraform Connector Ist in integriert Cloud Provisioning and Governance Anwendung und hilft Ihnen, Katalogelemente aus zu erstellen oder zu aktualisieren Terraform Vorlagen. Dann können Sie die Katalogelemente verwenden, um die Cloud-Ressourcen bereitzustellen.

Schlüsselfunktionen von Cloud Provisioning and Governance: Terraform Connector

- Erkennen Sie Terraform Vorlagen und Arbeitsbereiche aus dem Terraform Umgebung.
- Erstellen Sie Katalogelemente aus dem Terraform Vorlagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erkennen Sie Änderungen in Terraform Vorlage und verwenden Sie den IAC-Change-Aufgaben-Workflow, um das Katalogelement zu aktualisieren.
- Verwenden Sie die Unterstützung für mehrere Repositorys.
- Geben Sie Metadaten an, um die Formularfelder und Werte des Katalogelements zu füllen.
- Reduzieren Sie Terraform Cloud Lizenzkosten durch Verwendung von erkanntem Terraform Arbeitsbereiche zum Bereitstellen der Cloud-Infrastruktur.

Verwenden Terraform Als Konfigurationsanbieter

Verwenden Sie Terraform Open Source, Terraform Enterprise, Und Terraform Cloud Konfigurieren Sie den Provider, um Ressourcen in den folgenden Clouds bereitzustellen.

Ab diesem Release können Sie OpenTofu mit verwenden Cloud Provisioning and Governance. Sie müssen über Administratorrechte verfügen, um den Aliasnamen für zu konfigurieren Terraform Open Source Auf vm-Host-Ebene.

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud-Anbieter
- VMware vSphere
- IBM Cloud Platform (Veraltet)

Darüber hinaus können Sie verwenden Cloud Provisioning and Governance: Terraform Connector Um Ressourcen für bereitzustellen Oracle Cloud Infrastructure (OCI) über die App Cloud Provisioning and Governance: Oracle Cloud (OCI) Add-on für Terraform Connector. Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Oracle Cloud-Add-on (OCI) für Terraform Connector an.

Beginnend mit Cloud Provisioning and Governance: Terraform Connector Version 1,5.2, die App unterstützt keine Bereitstellungsressourcen für IBM Cloud Platform.

Erkennen Sie die IAC-Vorlagen (Infrastructure as Code)

Verwenden Cloud Provisioning and Governance: Terraform Connector Um die IAC zu erkennen (Terraform) Vorlagen aus dem Terraform Umgebung. Terraform Enterprise Oder Terraform Cloud Organisationen verwenden verschiedene Versionssteuerungssysteme, um zu speichern Terraform Vorlagen. Cloud Provisioning and Governance: Terraform Connector Kann die in den folgenden VCS gespeicherten Vorlagen erkennen:

- Öffentlich und selbst gehostet GitHub
- Öffentlich und selbst gehostet GitLab
- Öffentlich und selbst gehostet Microsoft Azure DevOps

Weitere Informationen finden Sie unter Führen Sie die IAC aus Discovery.

Verwenden Sie die hierarchische Struktur mehrerer Repositorys mit Unterstützung der Terraform Connector IAC-Discovery-Fähigkeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Katalogelemente aus dem Terraform Vorlagen

Verwenden Sie Cloud Provisioning and Governance: Terraform Connector App zum Erstellen von Katalogelementen aus erkannten Terraform Vorlagen und verwenden Sie sie, um Ressourcen in verschiedenen Clouds bereitzustellen. Weitere Informationen finden Sie unter Erstellen Sie ein Katalogelement aus dem Terraform Vorlage.

Erkennen Sie Änderungen in Terraform Vorlagen

Verwenden Sie IAC Discovery Um Änderungen in zu erkennen Terraform Vorlagen, die in vorhandenen Katalogelementen verwendet werden. Wenn Cloud Provisioning and Governance: Terraform Connector Erkennt eine Änderung in Terraform Vorlage erstellt eine IAC-Change-Aufgabe. Sie können die IAC-Change-Aufgabe verwenden, um das betroffene Katalogelement zu aktualisieren oder zu deaktivieren und dann ein weiteres Katalogelement aus dem zu erstellen Terraform Vorlage. Weitere Informationen zur Aufgabe zum Ändern von Katalogelementen finden Sie unter Verwalten Sie Terraform Vorlagenbasierte Katalogelemente.

Reduzieren Terraform Cloud Lizenzkosten

Erkannte verwenden Terraform Arbeitsbereiche zum Bereitstellen der Katalogelemente aus dem Terraform Vorlagen. Die Wiederverwendung des Arbeitsbereichs hilft Ihnen bei der Verwaltung von Terraform Cloud Lizenzkosten durch Vermeidung der Erstellung von Arbeitsbereichen.

Cloud Provisioning and Governance: Terraform Connector konfigurieren

Machen Sie sich mit dem allgemeinen Workflow für die Konfiguration von vertraut Cloud Provisioning and Governance: Terraform Connector Anwendung.

Führen Sie die folgenden Schritte aus, um zu konfigurieren Cloud Provisioning and Governance: Terraform Connector Anwendung:

1. Installieren Sie Cloud Provisioning and Governance: Terraform Connector. Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector installieren.
2. Wenn Sie eine Nebenversion oder Patch-Version von verwenden möchten Terraform Open Source, Terraform Enterprise, Oder Terraform Cloud, Fügen Sie dem Datensatz des Anbieters der Arbeitsauslastungskonfiguration die Nebenversion oder die Patch-Version hinzu. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
3. Zu verwenden Terraform Open Source Als Konfigurationsanbieter für Cloud Provisioning and Governance, Gehen Sie wie folgt vor:
   a. Zuweisen Terraform Fähigkeit zu MID-Server. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Server-Fähigkeiten .
   b. Erstellen Sie einen Terraform Open Source Konfigurations-Provider. Weitere Informationen finden Sie unter Erstellen Sie einen Terraform Open Source Konfigurations-Provider.
4. Zu verwenden Terraform Enterprise Oder Terraform Cloud Als Konfigurationsanbieter für Cloud Provisioning and Governance, Gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Zuweisen Terraform Enterprise Und REST-Fähigkeiten für MID-Server. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Server-Fähigkeiten .

b. Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider. Weitere Informationen finden Sie unter Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider.

5. Erkennen Sie Ressourcen aus dem Terraform Umgebung. Weitere Informationen finden Sie unter Führen Sie die IAC aus Discovery.

Cloud Provisioning and Governance: Terraform Connector installieren

Sie können installieren Cloud Provisioning and Governance: Terraform Connector Anwendung (com.sn_CMP_terraform), wenn Sie die Administratorrolle innehaben.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfung des folgenden Elements: Cloud Provisioning and Governance: Terraform Connector Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.
- Stellen Sie sicher Cloud Provisioning and Governance Die Anwendung (com.snc.Cloud.mgmt) wird in installiert und aktiviert ServiceNow AI Platform. Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Cloud Provisioning and Governance: Terraform Connector Anwendung (Com.sn_CMP_terraform) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Wenn Sie verwenden möchten Cloud Provisioning and Governance: Terraform Connector Mit Terraform Open Source, Erstellen Sie einen Terraform Open Source Konfigurations-Provider.
- Wenn Sie verwenden möchten Cloud Provisioning and Governance: Terraform Connector Mit Terraform Enterprise, Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider.

Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform

Fügen Sie Nebenversionen oder Patch-Versionen von hinzu Terraform(Terraform Open Source, Terraform Enterprise, Oder Terraform Cloud) Zum Datensatz des Arbeitsauslastungsanbietertyps.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem Cloud Provisioning and Governance: Terraform Connector Unterstützt Folgendes Terraform Versionen:

- Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1,2.0.
- Terraform Enterprise Versionen 1.1.9 und 1.2.0 .
- Terraform Cloud Versionen 1.1.9 und 1.2.0

Um Vorlagen zu verwenden, die von einer Nebenversion oder einer Patch-Version unterstützt werden, z. B. Version 0.12.29, fügen Sie die Versionsnummer dem Datensatz vom Typ Arbeitsauslastungsanbieter hinzu. Verwenden Sie dann die Nebenversionen oder Patch-Versionen, um Konfigurationsanbieter in zu erstellen Cloud Provisioning and Governance.

Prozedur

1. Navigieren Sie zu `https://<instance-name>/sn_CMP_Workload_Provider_type_list.do`
2. Wählen Sie aus Terraform Geben Sie ein, deren Nebenversion oder Patch-Version Sie verwenden möchten.
3. Ändern Sie den Anwendungsbereich in **Cloud-Bereitstellung und -Governance: Terraform-Connector** .
4. In **Version** Geben Sie im Formular „Anbietertyp für Arbeitsauslastungskonfiguration“ die Nebenversionen oder Patch-Versionen als kommagetrennte Werte ein.
5. Wählen Sie **Absenden**.

Erstellen Sie einen Terraform Open Source Konfigurations-Provider

Erstellen Sie einen Terraform Open Source Konfigurieren Sie den Provider in Cloud Provisioning and Governance. Die Terraform Open Source Konfigurations-Provider aktiviert Cloud Provisioning and Governance Um zu erkennen Terraform Open Source Installierbare Konfigurationen (Terraform Vorlagen) und erkennen Sie Änderungen daran.

Warum und wann dieser Vorgang ausgeführt wird

Ab diesem Release können Sie OpenTofu mit verwenden Cloud Provisioning and Governance. Sie müssen über Administratorrechte verfügen, um den Aliasnamen für auf vm-Hostebene zu konfigurieren.Stellen Sie sicher, dass der Server auf ausgeführt wird Windows Oder Linux Betriebssystem.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass unterstützt wird Terraform Open Source Version ist auf dem Server installiert. Cloud Provisioning and Governance: Terraform Connector Unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1,2.0.
- Wenn Sie eine Nebenversion oder Patch-Version von verwenden möchten Terraform Open Source CLI: Stellen Sie sicher, dass die Nebenversion oder die Patch-Version dem Anbieter der Arbeitsauslastungskonfiguration hinzugefügt wird. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
- Stellen Sie sicher, dass MID-Server Kann auf zugreifen Terraform Server.
- Stellen Sie sicher, dass MID-Server Hat Terraform Fähigkeit.
- Fügen Sie als neuer Anwender die Terraform-MID-Fähigkeit hinzu, um Ressourcen mit dem Terraform Open-Source-Host (VM) bereitzustellen. Fügen Sie Cloud-Provider-spezifische MID-Fähigkeit (AWS, Azure, VMware, Google) hinzu, um Ressourcen aus der Cloud nach der Bereitstellung von Terraform Open Source-Katalogelementen zu erkennen. Beispiel: Wenn Sie eine VM mit Terraform Open-Source in Google bereitstellen, benötigen Sie MID mit Terraform- und Google-Fähigkeit. Beide Fähigkeiten können auf demselben oder auf verschiedenen MIDs festgelegt werden. MID mit Terraform-Fähigkeit sollte in der Lage sein, eine Verbindung mit dem Terraform-Host (VM) herzustellen, und das mit Google-Fähigkeit muss google Cloud erreichen können. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Server-Fähigkeiten .
- Stellen Sie sicher, dass alle Vorlagen in separaten Verzeichnissen gespeichert werden und sich alle Vorlagenverzeichnisse im selben Basisverzeichnis befinden.
- Stellen Sie sicher, dass Terraform Connector Zugriff auf die Terraform-Registrierung (registry.hashicorp.com) hat.

Erforderliche Rolle: cloud_admin

Prozedur

1. **Wahlweise:** Wenn Sie bereitgestellt haben Terraform Open Source Auf einem Linux Server, erstellen Sie SSH Private Key-Anmeldeinformationen für den Server in ServiceNow AI Platform.

   a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.

   b. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Anmeldeinformationen**an.

   c. Wählen Sie **Neu**.

   d. Wählen Sie Aus **Anmeldeinformationen für privaten SSH-Schlüssel** .

   e. Füllen Sie im Formular die Felder aus.
   Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Referenz zum Formular „Anmeldeinformationen für privaten SSH-Schlüssel“.

   f. Wählen Sie den zugehörigen Link Test-Anmeldeinformationen aus.

   g. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Test-Anmeldeinformationen“

Feld	Beschreibung
Zielvorgabe	IP-Adresse des Terraform Server, für den Sie die Anmeldeinformationen erstellen.
MID-Server	MID-Server Die verwendet werden kann, um eine Verbindung mit herzustellen Terraform Server.

h. Wählen Sie **OK**.

i. Wählen Sie **Absenden**.

2. **Wahlweise:** Wenn Sie bereitgestellt haben Terraform Open Source Auf einem Windows Server, erstellen Windows Anmeldeinformationen für den Server in ServiceNow AI Platform.

a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.

b. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Anmeldeinformationen**an.

c. Wählen Sie **Neu**.

d. Wählen Sie Aus **Windows-Anmeldeinformationen** .

e. Füllen Sie im Formular die Felder aus.
Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Windows Referenz des Anmeldeinformationsformulars.

f. Wählen Sie den zugehörigen Link Test-Anmeldeinformationen aus.

g. Füllen Sie im Formular die Felder aus.

Formular „Test-Anmeldeinformationen“

Feld	Beschreibung
Zielvorgabe	IP-Adresse des Terraform Server, für den Sie die Anmeldeinformationen erstellen.
MID-Server	MID-Server Die verwendet werden kann, um eine Verbindung mit herzustellen Terraform Server.

h. Wählen Sie **OK**.

i. Wählen Sie **Absenden**.

3. Erstellen Sie einen Konfigurationsanbieter für Terraform Open Source.

a. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Konfigurationsverwaltung**an.

b. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Füllen Sie im Formular die Felder aus.
Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“.

d. Wählen Sie **Absenden**.

Nächste Maßnahme

Erkennen Sie Terraform Vorlagen aus dem Terraform Open Source Server. Weitere Informationen finden Sie unter Führen Sie die IAC aus Discovery.

Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider

Erstellen Terraform Enterprise Oder Terraform Cloud Konfigurieren Sie den Provider in Cloud Provisioning and Governance. Der Konfigurationsanbieter aktiviert Cloud Provisioning and Governance Um die Arbeitsbereiche und Versionssteuerungssystem-Repositorys (VCS) zu erkennen, die an angehängt sind Terraform Organisation.

Vorbereitungen

- Stellen Sie sicher, dass unterstützt wird Terraform Enterprise Oder Terraform Cloud Version wird verwendet. Cloud Provisioning and Governance: Terraform Connector Unterstützt Folgendes Terraform Versionen:
  - Terraform Enterprise Versionen 1.1.9 und 1.2.0
  - Terraform Cloud Versionen 1.1.9 und 1.2.0
- Dient zur Verwendung einer Nebenversion oder einer Patch-Version von Terraform Enterprise Oder Terraform Cloud Stellen Sie sicher, dass die Nebenversion oder die Patch-Version dem Anbieter der Arbeitsauslastungskonfiguration hinzugefügt wird. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
- Stellen Sie sicher, dass die folgenden Eigenschaften in korrekt konfiguriert sind MID-Server. Die MID-Server Verwendet diese Eigenschaften, um eine Verbindung mit herzustellen Terraform Enterprise Oder Terraform Cloud.
  - `glide.http.proxy_host`
  - `glide.http.proxy_port`
  - `glide.http.proxy_username`
  - `glide.http.proxy_password`

  Weitere Informationen finden Sie unter Knowledge Base Artikel KB0754247 .
- Stellen Sie sicher, dass MID-Server Hat Terraform Enterprise Und REST-Fähigkeiten. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Server-Fähigkeiten .
- Stellen Sie sicher, dass MID-Server Kann mit den in bereitgestellten VCS-Accounts kommunizieren Terraform Enterprise Oder Terraform Cloud Organisation.

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie API-Schlüssel-Anmeldeinformationen für Terraform Enterprise Oder Terraform Cloud Account. Weitere Informationen finden Sie unter Erstellen Sie API-Schlüssel-Anmeldeinformationen für Terraform Account und der unterstützte VCS-Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Erstellen Sie einen Konfigurationsanbieter für Terraform Enterprise Oder Terraform Cloud.

   a. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Konfigurationsverwaltung**an.

   b. Wählen Sie **Neu**.

   c. Füllen Sie im Formular die Felder aus.
   Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“.

   d. Wählen Sie **Absenden**.

Nächste Maßnahme
Erkennen Sie die Arbeitsbereiche und Versionssteuerungssystem-Repositorys (VCS), die an angehängt sind Terraform Im Konfigurationsanbieter angegebene Organisation. Weitere Informationen finden Sie unter Führen Sie die IAC aus Discovery.

Erstellen Sie API-Schlüssel-Anmeldeinformationen für Terraform Account und der unterstützte VCS-Account

Erstellen Sie API-Schlüssel-Anmeldeinformationen für Terraform Account- und unterstützte VCS-Accounts (Version Control System), die enthalten Terraform Vorlagen-Repositorys.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Eine API-Schlüssel-Anmeldeinformation ist ein gesicherter Datensatz in der ServiceNow AI Platform Der einen API-Schlüssel wie speichert Terraform Enterprise, Terraform Cloud, Oder VCS-Account-API-Schlüssel. Cloud Provisioning and Governance: Terraform Connector Verwendet die API-Schlüssel-Anmeldeinformationen, um eine Verbindung mit dem Account herzustellen und seine Ressourcen zu erkennen.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Anmeldeinformationen**an.
3. Wählen Sie **Neu**.
4. Wählen Sie Aus **API-Schlüssel-Anmeldeinformationen** .
5. Füllen Sie im Formular die Felder aus.
   Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen.
6. Wählen Sie **Absenden**.

Verwenden Sie die Struktur mehrerer Repositorys mit Terraform Connector App

Sie können jetzt mehrere erkennen Terraform Konfigurationen aus einem Repository auf beliebiger Ordnerebene mit Terraform Enterprise Konfigurations-Provider.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie aus Führen Sie die IAC aus Discovery Schritte und geben Sie an, was Repository, Verzweigungen und Ordnerpfade für die Erkennung berücksichtigt werden müssen Terraform Konfigurationen mit diesen Schritten.

Prozedur

1. Fügen Sie Repositorys und Verzweigungen hinzu, die Sie für die Erkennung berücksichtigen möchten Terraform Konfigurationen.
2. Verwenden **<Repository-Name>::<Branch-Name>** Format, um eine Verzweigung aus einem Repository einzubeziehen.
3. Um mehrere Repository- und Verzweigungszuordnungen anzugeben, verwenden Sie Kommas (,).

   Beispiel: Repo1::Branch1, Repo2::Branch2.

   Verlassen Sie die Feldbank, wenn Sie alle Repositorys und Verzweigungen in diesen VCS erkennen möchten.
4. Wählen Sie Aus **Möchten Sie Unterordnerpfade für Discovery angeben** Wenn Sie erkennen möchten Terraform Konfigurationen aus bestimmten Ordnerpfaden des Repositorys.
5. In **Ordnerpfadliste** Fügen Sie die Liste der durch Komma (,) getrennten Ordnerpfade hinzu, um Terraform-Konfigurationen daraus zu erkennen.
   - Der Ordnerpfadfilter gilt für alle Repository-Verzweigungen, die in der „Aufnahmeliste für Repo und Verzweigung“ enthalten sind.
   - Alle Terraform Konfigurationen, die Sie anhand eines bestimmten Ordnerpfads erkennen möchten, müssen sich in Unterordnern befinden, die nur eine Ebene darunter in der Ordnerhierarchie liegen. Beispiel: **/gcp/vm** Ordnerpfad hat einen Terraform Konfiguration für virtuelle Maschine,
   - Geben Sie An **/gcp** In Ordnerpfadliste zum Erkennen der vm Terraform Konfiguration.

Führen Sie die IAC aus Discovery

Führen Sie die IAC-Discovery (Infrastructure as Code) aus, um die Ressourcen von zu identifizieren Terraform Umgebung.

Vorbereitungen

- Stellen Sie sicher, dass Sie über die entsprechenden API-Anmeldeinformationen für die VCS-Accounts (Version Control System) verfügen, die in bereitgestellt werden Terraform Enterprise Oder Terraform Cloud Organisationen. Weitere Informationen finden Sie unter Erstellen Sie API-Schlüssel-Anmeldeinformationen für Terraform Account und der unterstützte VCS-Account.
- Stellen Sie sicher Terraform Open Source Ordner, die enthalten Terraform Vorlagen haben eindeutige Namen. Wenn mehrere Terraform Vorlagenordner haben denselben Namen. Es werden mehrere Change-Aufgaben erstellt, auch wenn alle Vorlagen möglicherweise keine Variablenänderungen enthalten.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Abhängig vom Konfigurationsanbieter, Cloud Provisioning and Governance: Terraform Connector Erkennt die folgenden Ressourcen aus dem Terraform Umgebung:

Terraform Open Source

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die IAC Discovery Erkennt die installierbaren Konfigurationsdateien (Terraform Vorlagen) aus dem Terraform Open Source Server.

Terraform Enterprise oder Terraform Cloud

Die IAC Discovery Erkennt die folgenden Elemente:

- Arbeitsbereiche: Terraform In bereitgestellte Arbeitsbereiche Terraform Organisation.
- VCS: In bereitgestellte VCS-Repositorys und -Verzweigungen Terraform Organisation.
- Agent-Pools:

  Terraform Cloud Verwendet Agents und Agent-Pools, um mit der lokalen Infrastruktur zu kommunizieren. Stellen Sie Service Desk-Mitarbeiter im selben Netzwerk wie Ihre Infrastruktur bereit, um eine Verbindung zwischen der Infrastruktur und herzustellen Terraform Cloud. Weitere Informationen zu Service Desk-Mitarbeitern und Agent-Pools finden Sie unter Terraform Cloud Agents an.

  Cloud Provisioning and Governance: Terraform Connector Erkennt die in erstellten Agent-Pools Terraform Cloud. Die erkannten Agents können Sie im Konfigurationsverwaltungsmodul für Ihren Konfigurations-Provider anzeigen. Im Katalogbestellungsformular können Sie mit einem Agent-Pool-Filter einen aktiven Service Desk-Mitarbeiter auswählen, der mit dem privaten kommuniziert VMware Infrastruktur.

  Hinweis: Die Option „Agent-Pools“ wird im Formular „Konfigurationsverwaltung“ und im Formular „Kataloganordnung“ angezeigt, wenn die folgenden Bedingungen erfüllt sind:

  - Sie haben erstellt VMware Agent-Pools in Terraform Cloud Organisation.
  - Sie haben VMware Vorlagen für Terraform Enterprise.

- Installierbare cfg-Dateien: Terraform Vorlagen, die in den Repositorys des VCS-Accounts gespeichert sind, haben bereitgestellt Terraform Organisation.

  Hinweis: Um zu erkennen Terraform Vorlagen aus VCS, Cloud Provisioning and Governance: Terraform Connector Erfordert die API-Schlüssel-Anmeldeinformationen des VCS-Accounts.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Konfigurationsverwaltung**an.
3. Wählen Sie aus Terraform Anbieterkarte.
4. Wählen Sie Aus **Entdecken Sie Jetzt** .

   Hinweis: Sie können die IAC nicht abbrechen Discovery Auftrag nach dem Auslösen.

5. **Wahlweise:** Zu verwenden Cloud Provisioning and Governance: Terraform Connector Mit Terraform Enterprise Oder Terraform Cloud, Erkennen Sie Terraform Vorlagen, die in den bereitgestellten VCS gespeichert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie aus **Tfe-Vcs** Registerkarte.

b. Wählen Sie in der Liste TFE-VCS den VCS-Account aus, der den enthält Terraform Vorlagen, für die Sie verwenden möchten Cloud Provisioning and Governance Katalogelementerstellung.

c. Wählen Sie in der Dropdown-Liste Anmeldeinformationen die API-Anmeldeinformationen des ausgewählten VCS-Accounts aus.

d. Wählen Sie unter zugehörige Links die Option aus **Suchen Sie Verzweigungen und Repositorys** .

e. Wiederholen Sie den Schritt 5.bBis 5.dFür alle VCS-Accounts, die enthalten Terraform Vorlagen, für die Sie verwenden möchten Cloud Provisioning and Governance Katalogelementerstellung.

6. Erstellen Sie einen Discovery-Zeitplan für Infrastructure as Code (IAC).
Der IAC-Discovery-Zeitplan hilft bei der Erkennung neuer Elemente Terraform Vorlagen, Arbeitsbereiche, Agent-Pools und VCS-Verzweigungen für den angegebenen Konfigurationsanbieter. Es erkennt auch Änderungen in bereits erkannten Terraform Vorlagen. Wenn Cloud Provisioning and Governance: Terraform Connector Erkennt eine Änderung an der Vorlagenvariablen oder den Vorlagenmetadaten und erstellt automatisch IAC-Change-Aufgaben für die betroffenen Katalogelemente.

a. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **IaC-Discovery**an.

b. Wählen Sie **Neu**.

c. Füllen Sie im Formular die Felder aus.

Formular „IAC-Discovery-Zeitpläne“

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name des IAC Discovery Zeitplan.
Anbieter	Konfigurationsverwaltungsanbieter, für den Sie den Discovery-Zeitplan erstellen.
Aktiv	Option zum Aktivieren oder Deaktivieren des Zeitplans
Ausführen	Häufigkeit der Zeitplanausführung. Konfigurieren Sie die Häufigkeit der Zeitplanausführung im Feld Ausführen und den zugehörigen Formularfeldern.

d. Wählen Sie **Absenden**.

Nächste Maßnahme

- Verwenden Sie die Struktur mehrerer Repositorys mit Terraform Connector App Mit IAC-Discovery
- Wenn Cloud Provisioning and Governance: Terraform Connector Erkennt neu Terraform Vorlagen, die Sie für die Bereitstellung von Cloud-Ressourcen verwenden möchten, erstellen Sie ein Katalogelement aus der erkannten Vorlage. Weitere Informationen finden Sie unter Erstellen Sie ein Katalogelement aus dem Terraform Vorlage.
- Wenn Cloud Provisioning and Governance: Terraform Connector Hat Änderungen in einer vorhandenen Vorlage erkannt. Führen Sie eine der folgenden Aktionen aus, um die zugehörige IAC-Change-Aufgabe zu lösen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktualisieren Sie das betroffene Katalogelement gemäß aktualisiert Terraform Vorlage.
- Deaktivieren Sie das betroffene Katalogelement, und erstellen Sie dann ein Katalogelement gemäß der aktualisierten Vorlage.

Weitere Informationen finden Sie unter Verwalten Sie Terraform Vorlagenbasierte Katalogelemente.

Domänentrennung und Cloud Provisioning and Governance: Terraform Connector

Domänentrennung wird für Cloud Provisioning and Governance: Terraform Connector unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Cloud Provisioning and Governance: Terraform Connector Integration mit Cloud Provisioning and Governance Und entspricht Cloud Provisioning and Governance Domänentrennung. Weitere Informationen finden Sie unter Domain Separation und Cloud Provisioning and Governance.

Upgrade von wird durchgeführt Terraform Umgebung

Machen Sie sich mit den allgemeinen Workflows für das Upgrade von vertraut Terraform Umgebung.

Upgrade Wird Durchgeführt Terraform Open Source

Upgrade-Methoden für Terraform Open Source

Upgrade-Methode	Beschreibung
Aktualisieren Sie das vorhandene Terraform Open Source Installation in einer neueren unterstützten Version	**Hinweis:** Wenn Sie ein Upgrade der vorhandenen durchführen möchten Terraform Open Source Bei der Installation kann es zu einer längeren Upgradezeit kommen. Führen Sie die folgenden Aktionen aus, um ein Upgrade des vorhandenen durchzuführen Terraform Open Source Installation: 1. Führen Sie ein Upgrade von durch Terraform Open Source Server auf eine Version, die von unterstützt wird Cloud Provisioning and Governance: Terraform Connector. Weitere Informationen zum Upgrade von Terraform finden Sie unter Upgrade-Leitfäden in Terraform Dokumentation an. Cloud Provisioning and Governance: Terraform Connector Unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1,2.0. 2. Testen und ändern Sie die vorhandenen Terraform Vorlagen, um die Kompatibilität mit dem Ziel sicherzustellen Terraform Open Source Version. 3. Aktualisieren Sie Terraform Open Source Version, die in erwähnt wird Terraform Open Source Konfigurations-Provider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Methoden für Terraform Open Source (Fortsetzung)

Upgrade-Methode	Beschreibung
Richten Sie einen neuen ein Terraform Server mit dem gewünschten Terraform Open Source Version	Führen Sie die folgenden Aktionen aus, um einen neuen einzurichten Terraform Server mit dem gewünschten Terraform Open Source Version: **1.** Erstellen Sie einen Linux Oder Windows Server für Terraform Open Source Installation. **2.** Installieren Sie ein Terraform Open Source Version, die von unterstützt wird Cloud Provisioning and Governance: Terraform Connector. Cloud Provisioning and Governance: Terraform Connector Unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1,2.0. **3.** Kopieren Sie die vorhandene Terraform Vorlagen für die neuen Terraform Server. **Hinweis:** Stellen Sie sicher, dass alle Vorlagen in separaten Verzeichnissen gespeichert werden und sich alle Vorlagenverzeichnisse im selben Basisverzeichnis befinden. **4.** Testen und ändern Sie die kopierte Terraform Vorlagen, um die Kompatibilität mit dem Ziel sicherzustellen Terraform Open Source Version. **5.** Erstellen Sie einen Terraform Open Source-Konfigurationsanbieter. Weitere Informationen finden Sie unter Erstellen Sie einen Terraform Open Source Konfigurations-Provider. **6.** Entfernen Sie die alten Katalogelemente gemäß der Geschäftsstrategie Ihrer Organisation, und legen Sie die alten dann außer Kraft Terraform Server.

Upgrade Wird Durchgeführt Terraform Enterprise Und Terraform Cloud

Testen und ändern Sie die vorhandenen Terraform Vorlagen, um die Kompatibilität mit dem neuen sicherzustellen Terraform Enterprise Oder Terraform Cloud Version.

Hinweis: Die Stapel und Terraform Arbeitsbereiche sind an gebunden Terraform Version, über die sie bereitgestellt wurden. Daher dasselbe Terraform Version wird zum Bereitstellen und Aufheben der Bereitstellung eines Stapels oder verwendet Terraform Arbeitsbereich.

Cloud Provisioning and Governance: Terraform Connector verwenden

Machen Sie sich mit den allgemeinen Anwendungsfällen und Nutzungs-Workflows für vertraut Cloud Provisioning and Governance: Terraform Connector Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie zu Terraform Eingabeparameter mit Cloud Provisioning and Governance Katalogelement

Erstellen Sie eine JSON-Datei, um die in der Vorlagendatei verwendeten Variablen zu speichern, damit Sie sie erkannten Ressourcen, Pools und Filtern zuordnen können. Sie können Variablen oder Parameter aus verwenden Terraform Vorlage zum Zuordnen zu Feldern im Bereitstellungsformular für Katalogelemente.

Vorbereitungen

Erforderliche Rolle: Cloud_Designer

Warum und wann dieser Vorgang ausgeführt wird

Cloud Provisioning and Governance: Terraform Connector Unterstützt diese Fähigkeit für Terraform Open Source, Terraform Enterprise, Und Terraform Cloud.

Wichtig: Wenn Sie verwenden Terraform Vorlagen zum Erstellen von Katalogelementen. Der Wert „Standort“ gibt das Rechenzentrum oder die Region an, um die Konfigurationselemente und -Stapel bereitzustellen. Verwenden Sie die Metadatendatei, um andere Variablen basierend auf erkannten Ressourcen, Netzwerken, Profilen, Pools und Filtern usw. zuzuordnen.

Dient zum automatischen Ausfüllen von Formularfeldern im Katalogerstellungsformular während der Verwendung Terraform Vorlagen: Gehen Sie wie folgt vor:

- Geben Sie die Schlüssel-Wert-Paare in der JSON-Datei für Variablen an, die in definiert sind Terraform Vorlage.
- Konfigurieren Sie Variablen, um Felder und Daten in automatisch auszufüllen **Cloud-Anwenderportal** > **Cloud-Katalog** > **Neu** > **Bereitstellung** Seite.

Weitere Informationen zum Binden eines Parameters an einen Ressourcenpool finden Sie unter Binden Sie einen Parameter an einen Ressourcenpool.

Prozedur

1. Erstellen Sie eine JSON-Datei in dem Verzeichnis oder Repository, das die Grundlage für das Katalogelement ist.

   Wichtig: Benennen Sie die JSON-Datei Metadaten.snc Und speichern Sie sie in demselben Verzeichnis oder Repository wie die Vorlagendatei (.tf). Diese Benennungskonvention ermöglicht die Erkennung und Analyse von Metadaten.snc JSON-Datei als Teil der installierbaren Konfiguration.

2. Geben Sie den entsprechenden Pool und Filter als Datentyp für an Terraform Variable in Metadaten.snc JSON-Datei.

```
"Metadata": {
 "SNC::Parameter::Metadata": {
  "rgName": {
   "datasource": "ServiceNow::Pools:: ResourceGroupPool.getByLDC"
  },
  "Network": {
   "datasource": "ServiceNow::Pools::NetworkPool.getObjectsByLDC"
  },
  "Subnet": {
   "datasource": "ServiceNow::Pools:: SubnetPool.getObjectsByNetwork",
   "datasourceFilter": { "Network": "Network" }
  }
 }
```

Automatische Übersetzung

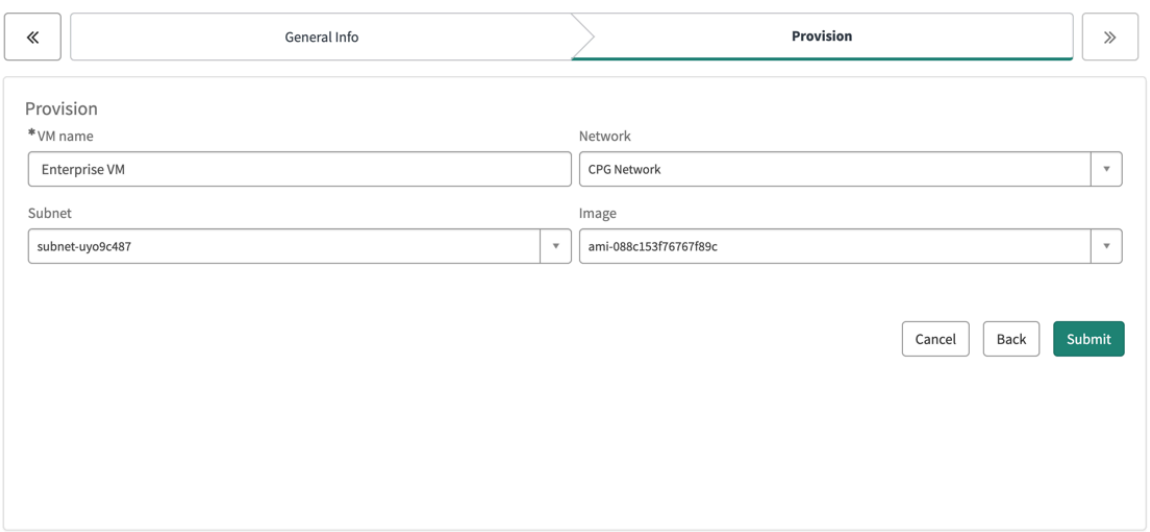
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}
```

Der Wert, den Sie im Variablenfeld von angeben Metadaten.snc Die Datei wird im Abschnitt „Bereitstellung“ des Formulars „Katalogelement“ ausgefüllt.

Das folgende Bild zeigt die Felder auf der Registerkarte Bereitstellung des Katalogformulars. Die Werte werden basierend auf den in definierten Variablen automatisch ausgefüllt Metadaten.snc Datei.

Beispiel: Automatisch gefüllte Werte im Abschnitt „Bereitstellung“ des Katalogerstellungsformulars



Füllen Sie das Rechenzentrum in Terraform-basierte Katalogelemente aus

In einer beliebigen Anforderung für ein Katalogelement mit Terraform Vorlagen: Der Wert „erforderlicher Standort“ gibt das Rechenzentrum oder die Region an, in der die Konfigurationselemente und -Stapel bereitgestellt werden sollen. Sie können eine Variable mit dem Namen verwenden *region*In Terraform Vorlage, die dem Feld Standort im Anforderungsformular zugeordnet werden soll.

Vorbereitungen

Erforderliche Rolle: Cloud_Designer

Prozedur

Definieren Sie in der Vorlagendatei, die die Grundlage für das Katalogelement ist, eine Variable mit dem Namen *region*.

```
variable "region" {
          type="string"
        }
```

- Das für definierte Feld *region*Variable wird nicht im Abschnitt „Bereitstellung“ des Anforderungsformulars für das Katalogelement angezeigt (das Feld „Standort“ dient diesem Zweck).
- Der Wert, den der Anwender für das Feld Standort im Anforderungsformular angibt, konfiguriert das Rechenzentrum oder die Region für die Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Katalogelement aus dem Terraform Vorlage

Erstellen Sie ein Katalogelement aus dem Terraform Vorlage zum anfordern der Bereitstellung von Cloud-Ressourcen. Aktivierte Katalogelemente werden im Cloud-Anwenderportal angezeigt.

Vorbereitungen

- Stellen Sie sicher, dass ein geeignetes Terraform Konfigurationsanbieter ist verfügbar. Weitere Informationen zum Erstellen des Konfigurationsanbieters finden Sie unter Erstellen Sie einen Terraform Open Source Konfigurations-Provider Und Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider.
- Stellen Sie sicher, dass Terraform Vorlage funktioniert (d. h. Sie können die Vorlage direkt mit verwenden Terraform System zur Bereitstellung der angegebenen Cloud-Ressourcen). Weitere Informationen zu finden Terraform Vorlagen finden Sie unter Terraform Sprachdokumentation an.
- Stellen Sie sicher, dass der Anbieterblock von Terraform Vorlage entspricht der folgenden Syntax:
  - Anbieterblocksyntax für Microsoft Azure Cloud:

```
provider "azurerm" {

 subscription_id = "${var.subscriptionId}"
 client_id       = "${var.clientId}"
 client_secret   = "${var.clientSecret}"
 tenant_id       = "${var.tenantId}"
}
```

  - Anbieterblocksyntax für Amazon Web Services Cloud:

```
provider "aws" {
 access_key     = "${var.access_key}"
 secret_key     = "${var.secret_key}"
 region         = "${var.region}"
}
```

  - Anbieterblocksyntax für Google Cloud Platform

```
terraform {
 required_providers {
   google = {
     source  = "hashicorp/google"
     version = "5.10.0"
   }
 }
}

provider "google" {
 credentials = var.credentials
 project     = var.project
 region      = var.region
}
```

  - Anbieterblocksyntax für VMware Cloud:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
provider "vsphere" {
  user              = "${var.user}"
  password          = "${var.password}"
  vsphere_server    = "${var.vsphere_server}"
}
```

Hinweis: Geben Sie keine Anmeldeinformationen in fest Terraform Vorlage. Verwenden Sie entsprechend Terraform Variablen zum Abrufen der Anmeldeinformationen von ServiceNow AI Platform.

- Stellen Sie sicher, dass die Variablendefinitionsdatei (Variable.tf , .Tfvars , Oder .Tfvars.JSON) Enthält die Definition der im Anbieterblock verwendeten Variablen.
- Wenn Sie verwenden Terraform Enterprise Oder Terraform Cloud, Stellen Sie sicher, dass MID-Server Kann eine Verbindung mit VCS-Accounts (Version Control System) herstellen, die in bereitgestellt werden Terraform Organisation.

  Dient zum Überprüfen der Konnektivität mit den in bereitgestellten VCS-Accounts Terraform Organisation, führen Sie den entsprechenden Curl-Befehl auf der aus MID-Server.

  GitHub

  ```
  curl -H "Authorization: <API credential>
   https://<github-api-host>/user/repos?per_page=100&page=1"
  ```

  GitLab

  ```
  curl -H "Authorization: <API credential>"
   https://<gitlab-api-host>/api/v4/projects?visibility=private&per_page=100&page=1
  ```

  Microsoft Azure DevOps

  ```
  curl -H "Authorization: <API credential>
   https://<azure-devops-api-host>/<organization>/<project>/_apis/git/repositories?api-version=6.0"
  ```

  Wo,

  - *`organization`*Ist der Name von Microsoft Azure DevOps Organisation.
  - *`project`*Ist der Name von Microsoft Azure DevOps Projekt.

  Weitere Informationen zu den API-Anmeldeinformationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Die Cloud Provisioning and Governance: Terraform Connector Die App unterstützt Folgendes Terraform Datentypen:

- Zeichenfolge
- Nummer
- Bool
- Liste
- Tupel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuordnen
- Objekt

Prozedur

1. Erstellen Sie ein Cloud-Katalogelement.

   a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.

   b. Navigieren zu **Entwurf** > **Cloud-Katalogelemente**an.

   c. Wählen Sie **Neu**.

   d. Füllen Sie im Formular die Felder aus.

   Formular „Cloud-Katalogelement“

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name des Katalogelements.
Quelle	Quelle des Katalogelements. Wählen Sie Aus **Konfigurationsverwaltungsvorlage** Aus der Dropdown-Liste.
Provider-Typ	Terraform Konfigurations-Provider-Typ, den Sie verwenden möchten. ▪ Zu verwenden Terraform Enterprise Oder Terraform Cloud, Wählen Sie aus **Terraform Enterprise** . ▪ Zur Verwendung eines Linux-basierten Terraform Open Source Server, wählen Sie aus **Terraform-Umgebung** . ▪ Zur Verwendung eines Windows-basierten Terraform Open Source Server, wählen Sie aus **Terraform Windows-Umgebung** .
Anbieter	Name des Terraform Konfigurations-Provider, den Sie verwenden möchten.

   e. Speichern Sie das Formular „Cloud-Katalogelement“.

2. Ordnen Sie ein zu Terraform Vorlage mit dem Katalogelement.

   a. Wählen Sie in der zugehörigen Liste Cloud-Vorlagen die Option aus **Neu** .

   b. Wählen Sie in der Dropdown-Liste „installierbare Konfiguration“ die Option aus Terraform Vorlage, die Sie verwenden möchten.

   c. Speichern Sie ServiceNow Formular „Cloud-Vorlagen-Versionen“.

   Hinweis: Ein Katalogelement kann mehrere Versionen der Cloud-Vorlage enthalten, aber nur eine Version kann aktiv sein.

   d. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Cloud-Vorlage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Um Formularfelder für Katalogelemente hinzuzufügen oder zu entfernen, bearbeiten Sie die Variablensätze, die dem Katalogelement zugeordnet sind.
4. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren des Katalogelements.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme
Überprüfen Sie, ob das Katalogelement im Cloud-Anwenderportal angezeigt wird.

Verwalten Sie Terraform Vorlagenbasierte Katalogelemente

Verwenden Sie eine Change-Aufgabe „Infrastructure as Code“ (IAC), um zu erstellen oder zu aktualisieren Terraform Vorlagenbasierte Katalogelemente. Die IAC-Change-Aufgabe trägt dazu bei, sicherzustellen, dass die Katalogelemente an den neuesten Infrastrukturspezifikationen ausgerichtet sind, die in codiert sind Terraform Vorlage.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Cloud Provisioning and Governance: Terraform Connector Die App erkennt eine Änderung der Variablen auf der Terraform Vorlagendatei (.TF) oder die Metadaten (Metadaten.snc) Datei erstellt Change-Aufgaben. Die Change-Aufgaben werden Anwendern zugewiesen, die die Katalogelemente erstellt haben (Anwender mit der Rolle [sn.CMP.Cloud_Service_Designer]). Je nach in den Vorlagenvariablen oder den Metadaten erkanntem Change werden Sie von der Katalogelementaufgabe aufgefordert, eine der folgenden Aktionen auszuführen:

- Erstellen Sie ein Katalogelement aus der geänderten Vorlagenversion.

  Ein neues Katalogelement wird erstellt. Dabei wird eine Nummer an den bestehenden Namen des Katalogelements angehängt. Wenn das vorhandene Katalogelement beispielsweise `Linux VM` heißt, wird das neue Katalogelement unter dem Namen `Linux VM1` erstellt.

- Aktualisieren Sie das vorhandene Katalogelement gemäß der aktualisierten Vorlagenversion.

  Wenn Sie das vorhandene Katalogelement gemäß der aktualisierten Vorlagenversion aktualisieren möchten, wird eine neue Version der Vorlage erstellt und aktiviert, während die vorhandene Vorlagenversion stillgelegt und inaktiv gemacht wird.

Hinweis: Der Name des Terraform-Konfigurationsanbieters muss zwischen den Umgebungen übereinstimmen, während Terraform-vorlagenbasierte Katalogelemente exportiert werden. Wenn der Konfigurationsanbieter beispielsweise in der Entwicklungsumgebung als TFE bezeichnet wird, sollte er auch in der Zielumgebung (UAT, prod usw.) den Namen „Gleiche“ (TFE) haben.

Bis Sie eine der oben genannten Aktionen ausführen, wird das Katalogelement deaktiviert. Wenn sich das Katalogelement im deaktivierten Status befindet, können Cloud-Anwender nicht darauf zugreifen.

Die Cloud Provisioning and Governance: Terraform Connector Erstellt eine IAC-Change-Aufgabe für einen Terraform Vorlagenbasiertes Katalogelement, wenn eine der folgenden Bedingungen erfüllt ist:

- Mindestens eine Variable wird der Quelle hinzugefügt Terraform Vorlage.
- Mindestens eine Variable wird aus der Quelle gelöscht Terraform Vorlage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine oder mehrere Variablen, die in der Quelle verwendet werden Terraform Vorlage durchläuft eine Datentypänderung.
- Standardwert von mindestens einer Variablen ändert sich.

Hinweis: Die Aufhebung der Bereitstellung des betroffenen Stapels löst die Aufhebung der Bereitstellung am Ende des Cloud-Providers aus

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren zu **IaC** > **Change-Aufgaben**an.
3. Öffnen Sie die entsprechende Change-Aufgabe.
4. **Wahlweise:** Passen Sie die in erkannten neuen oder aktualisierten Variablen an Terraform Vorlage.
   a. Wählen Sie aus **Passen Sie Variablen An** Zugehöriger Link.
   b. Bearbeiten Sie den Standardwert von neu oder aktualisiert Terraform Variablen aus der zugehörigen Liste Terraform-Aufgabenmetadaten.

   Hinweis: Der im Variablendatensatz von erwähnte Standardwert Terraform Die zugehörige Liste „Aufgabenmetadaten“ überschreibt den in erwähnten Standardwert Terraform Vorlage.
5. **Wahlweise:** Wählen Sie aus **Changes** Link zur Empfehlungsnachricht, um einen von der IAC-Discovery erkannten Differenzvergleich im Vorlageninhalt anzuzeigen.
6. Füllen Sie im Formular die Felder aus.
   Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector Terraform Referenz des Katalogelementaufgabenformulars.
7. Wählen Sie **Aktualisieren**.

Ordnen Sie Anmeldeinformationen zu Cloud Provisioning and Governance Und Terraform

Ordnen Sie mit der Funktion der Zuordnung von Anmeldeinformationen Zwischen Cloud Provisioning and Governance Und Terraform Anmeldeinformationszuordnung verwenden.

Vorbereitungen

Die neueste Cloud Provisioning and Governance: Terraform Connector Muss über installiert werden ServiceNow Store an.

Erforderliche Rolle: sn_cmp.cloud_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

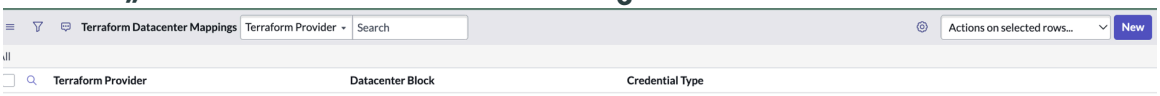
Verwenden Sie Modul „Anmeldeinformationszuordnung“ zum Durchführen von Anmeldeinformationen und Service-Account-Zuordnungen für Rechenzentrums-Anmeldeinformationen, die von verwendet werden Terraform Anbieter für die Bereitstellung von Rechenzentrumsressourcen und Cloud Provisioning and Governance Für Discovery.

Prozedur

1. Navigieren zu **Alle** > **Entwurf** > **Zuordnung von Anmeldeinformationen**an.
2. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Terraform-Rechenzentrumszuordnung“



3. Füllen Sie im Formular die Felder aus.

Terraform Formular „Rechenzentrumszuordnungen“

Feld	Beschreibung
Terraform Anbieter	Name des Terraform Anbieter.
Rechenzentrumsblock	Der Ressourcenblock, dessen Anmeldeinformationen Sie zuordnen Die Suchtabelle.
Anmeldeinformationstyp	Der entsprechende Anmeldeinformationstyp Aus der Suchtabelle. Beispiel: Azure Serviceprinzipal [Azure_Service_principal].
Resolver für Anmeldeinformationen	Ein entsprechendes MID-Server Skripteinbindung aus der Suchtabelle. Beispiel: Suchen Sie das TerraformProviderCredentialResolver-Skript und wählen Sie es aus.

4. Wählen Sie **Absenden**.
   Die Terraform Der Datensatz für Anbieteranmeldeinformationen wird erstellt und in angezeigt Terraform Liste der Rechenzentrumszuordnungen.
5. Navigieren Sie im von Ihnen erstellten Datensatz zu **Zuordnungen Von Anmeldeinformationen** Zugehörige Liste, und wählen Sie dann aus **Neu** .

   a. Füllen Sie das Formular **Zuordnung von Anmeldeinformationen** aus.

Feld	Beschreibung
Anbieter-Authentifizierungsschlüssel	Feldname des Authentifizierungsschlüssels (Variable), wie vom Provider verwendet. Zum Beispiel die Terraform Anbieterblock für (Amazon Web Services) AWS Verwendet das Feld `Secret_key` .
Discovery-Anmeldeinformationsschlüssel	Das entsprechende Feld in den Discovery-Anmeldeinformationen aus der Suchtabelle. Beispiel: `Access_key` Feld in Terraform Entspricht `Geheimer Schlüssel` Feld in ServiceNow Instanz.
Terraform Rechenzentrumszuordnung	Rechenzentrum, für das Sie die Anmeldeinformationen zuordnen.

   b. Wählen Sie **Absenden**.

6. Wählen Sie aus **Service-Account-Zuordnungen** Registerkarte und wählen Sie dann aus **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Füllen Sie das Formular **Servicekontozuordnung** aus.

Feld	Beschreibung
Anbieter-Authentifizierungsschlüssel	Feldname des Authentifizierungsschlüssels (Variable), wie vom Provider verwendet. Zum Beispiel die Terraform Anbieterblock für AWS Verwendet das Feld `Secret_key` .
Feld für Service-Account	Feldname des Servicekontos (Variable) aus der Suchtabelle, dessen Anmeldeinformationen Sie dem Provider-Authentifizierungsschlüssel zuordnen.
Terraform Rechenzentrumszuordnung	Rechenzentrum, für das Sie die Anmeldeinformationen zuordnen.

b. Wählen Sie **Absenden**.

Sie haben die Feldwerte zugeordnet, die Sie unter den zugehörigen Listen „Anmeldeinformationszuordnung“ und „Service-Account-Zuordnung“ hinzugefügt haben Terraform Anbieter.

Ordnen Sie zu Terraform Umgebungsvariable mit dem Ressourcenblock des Rechenzentrums

Ordnen Sie zu Terraform Umgebungsvariable mit Cloud Provisioning and Governance Rechenzentrum-Ressourcenblock. Nach der Zuordnung der Umgebungsvariable können Sie sie verwenden, um anwenderdefinierte Eingabeparameter während der Ressourcenbereitstellung über zu übergeben Terraform Enterprise.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Zum Festlegen von Terraform Umgebungsvariable bedingt verwenden Sie einen geskripteten Ausdruck. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**an.
   Das Cloud-Administratorportal wird in einer neuen Browserregisterkarte geöffnet.
2. Auswahlvorgang **Entwurf** > **Ressourcenblöcke**an.
3. Wählen Sie die entsprechende Karte für das logische Rechenzentrum aus.
4. Legen Sie den Ressourcenblock des logischen Rechenzentrums auf fest **Entwurf** status.
5. Wählen Sie die Registerkarte **Vorgänge** aus.
6. Wählen Sie in der Dropdown-Liste Schnittstelle die Option aus **Terraform Orchestration-Schnittstelle** .
7. Auswahlvorgang **Schritte** > **Flow.Subflow.TFEProvision**an.
8. Legen Sie fest **terraform_variables** Textfeld zum Schlüssel-Wert-Paar der Umgebungsvariablen.
   Beispiel: **{"USER_AGENT_PROVIDER_NAME":"AGENTVALUE"}**
9. Legen Sie den Ressourcenblock des logischen Rechenzentrums auf fest **Veröffentlicht** status.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: Terraform Connector-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Cloud Provisioning and Governance: Terraform Connector.

Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“

Cloud Provisioning and Governance Verwendet den Konfigurationsanbieter, um mit zu interagieren Terraform Bereitstellung.

Feld	Beschreibung
Name	Name des Konfigurationsanbieters.
Anbieter	Konfigurations-Provider-Typ. • Terraform Enterprise: Wählen Sie diesen Wert aus, um eine zu erstellen Terraform Enterprise Konfigurations-Provider. • Terraform Umgebung: Wählen Sie diesen Wert aus, um eine Linux-basierte zu erstellen Terraform Open Source Konfigurations-Provider. • Terraform Windows Umgebung: Wählen Sie diesen Wert aus, um eine Windows-basierte zu erstellen Terraform Open Source Konfigurations-Provider.
Organisation	Terraform Organisation, die enthält Terraform Arbeitsbereiche und Vorlagen-Repositorys. Dieses Feld wird angezeigt, wenn Sie auswählen Terraform Enterprise Aus der Dropdown-Liste Anbieter.
URL	Basis-URL von Terraform API-Server oder IP-Adresse des Terraform Server. • Dient zum Erstellen eines Konfigurationsanbieters für Terraform Open Source, Geben Sie IP:Port des ein Terraform Server. • Dient zum Erstellen eines Konfigurationsanbieters für Terraform Enterprise Geben Sie die Basis-URL des ein Terraform Enterprise API-Server. • Dient zum Erstellen eines Konfigurationsanbieters für Terraform Cloud, Eingabetaste https://app.terraform.io/api/v2
Basisverzeichnis	Verzeichnis, in dem alle Einzelpersonen enthalten sind Terraform Vorlagenverzeichnisse befinden sich. Dieses Feld wird angezeigt, wenn Sie auswählen Terraform Umgebung oder Terraform Windows Umgebung aus der Dropdown-Liste „Anbieter“.
Servertyp	Servertyp von Terraform Bereitstellung.
Anmeldeinformation	Anmeldeinformationen für den Zugriff Terraform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Für Linux-basierte Terraform Open Source Server, wählen Sie die entsprechenden SSH Private Key-Anmeldeinformationen aus. • Für Windows-basierte Terraform Open Source Server, wählen Sie die entsprechenden Remote Desktop Protocol (RDP)-Anmeldeinformationen aus. • Für Terraform Enterprise Oder Terraform Cloud, Wählen Sie die entsprechende aus Terraform API-Schlüssel-Anmeldeinformationen.
Version	Unterstützt Terraform Open Source CLI-Version in installiert Terraform Server. Weitere Informationen zu unterstützten finden Sie unter Terraform Open Source Versionen finden Sie im Abschnitt „Voraussetzungen“ von Erstellen Sie einen Terraform Open Source Konfigurations-Provider. Weitere Informationen zu unterstützten finden Sie unter Terraform Enterprise Und Terraform Cloud Versionen finden Sie im Abschnitt „Voraussetzungen“ von Erstellen Sie einen Terraform Enterprise Oder Terraform Cloud Konfigurations-Provider. Beginnend mit Cloud Provisioning and Governance: Terraform Connector Version 1,5.2, Version 1.0.0 ist veraltet. Die veraltete Version stellt dar Terraform Open Source CLI-Versionen 0,11 und 0,12.

Cloud Provisioning and Governance: Terraform Connector Referenz zum Formular „Anmeldeinformationen für privaten SSH-Schlüssel“

Cloud Provisioning and Governance: Terraform Connector Verwendet die Anmeldeinformationen des privaten SSH-Schlüssels, um eine Verbindung mit herzustellen Linux Server, auf dem Terraform Open Source Wird ausgeführt.

Die Linux Der Server unterstützt die folgenden Authentifizierungsmodi:

- Authentifizierung mit Anwendername und Passwort.
- Authentifizierung nur mit dem privaten Schlüssel.
- Authentifizierung mit dem privaten Schlüssel und der SSH-Passphrase.

Feld	Beschreibung
Name	Name des Berechtigungsnachweises
Anwendername	SSH-Anwendername des Linux Server, auf dem Terraform Wird ausgeführt.
Passwort	SSH-Passwort des Linux Server, auf dem Terraform Wird ausgeführt.
SSH-Passwortsatz	SSH-Passphrase von Linux Server, auf dem Terraform Wird ausgeführt.
Privater SSH-Schlüssel	Privater SSH-Schlüssel von Linux Server, auf dem Terraform Wird ausgeführt.

Cloud Provisioning and Governance: Terraform Connector Windows Referenz des Anmeldeinformationsformulars

Cloud Provisioning and Governance: Terraform Connector Verwendet Windows Anmeldeinformationen für die Verbindung mit Windows Server, auf dem Terraform Open Source Wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Berechtigungsnachweises
Anwendername	Remote Desktop Protocol (RDP)-Anwendername für Windows Server, auf dem Terraform Wird ausgeführt.
Passwort	RDP-Passwort für Windows Server, auf dem Terraform Wird ausgeführt.

Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen

Die Cloud Provisioning and Governance: Terraform Connector Verwendet API-Schlüssel-Anmeldeinformationen, um die an gesendeten Anforderungen zu authentifizieren Terraform Enterprise Und Terraform Cloud Und die darin bereitgestellten Versionskontrollsysteme.

Weitere Informationen zu API-Schlüsselberechtigungen und -Token finden Sie unter https://developer.hashicorp.com/terraform/cloud-docs/users-teams-organizations/api-tokens .

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name der Anmeldeinformationen.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

API-Schlüssel	API-Schlüssel, der für den Zugriff auf den Account verwendet werden kann.
	• Terraform Enterprise Oder Terraform Cloud API-Schlüssel: Bearer-Token für den Zugriff Terraform Enterprise Oder Terraform Cloud.
	Stellen Sie sicher, dass der API-Schlüssel der folgenden Syntax entspricht:
	`Bearer <API key>`
	• GitHub API-Schlüssel: API-Token für den Zugriff auf GitHub enterprise- oder Community-Account.
	Stellen Sie sicher, dass das Token der folgenden Syntax entspricht:
	`Token <API key>`
	• GitLab API-Schlüssel: Bearer-Token für den Zugriff auf GitLab enterprise- oder Community-Account.
	Stellen Sie sicher, dass das Token der folgenden Syntax entspricht:
	`Bearer <API key>`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Microsoft Azure DevOps API-Schlüssel: Base-64-codiertes Token für den Zugriff auf Azure DevOps enterprise- oder Community-Account. **Wichtig:** Stellen Sie dem API-Token einen Doppelpunkt (:) voran, und codieren Sie dann die gesamte Zeichenfolge auf Base-64. Stellen Sie sicher, dass das Token der folgenden Syntax entspricht: `Basic <base-64 encoded API key>`
Betrifft	MID-Server, auf den Sie die Anmeldeinformationen anwenden. Wählen Sie Aus **Alle MID-Server**
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen ausführt, wenn versucht wird, sich bei Geräten anzumelden. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Anmeldeinformationsalias	Anmeldeinformationsalias, der die Anmeldeinformationen auflösen kann.

Cloud Provisioning and Governance: Terraform Connector Terraform Referenz des Katalogelementaufgabenformulars

Verwenden Sie Terraform Formular „Katalogelementaufgabe“, um die Aktion anzugeben, die Sie zum Lösen der Katalogelementänderungsaufgabe ausführen möchten.

Terraform Formular „Katalogelementaufgabe“

Feld	Beschreibung
Aktion für Katalogelementaufgabe	Aktion, die Sie ausführen möchten. • Katalogelement mit dieser Vorlagenversion aktualisieren Wählen Sie diese Option aus, um das Katalogelement mit dieser Vorlagenversion zu aktualisieren. Eine neue Version der Vorlage wird erstellt und aktiviert, während die vorhandene Vorlagenversion deaktiviert wird. • Create catalog item with this template (Neues Katalogelement mit dieser Vorlage erstellen) Wählen Sie diese Option aus, um ein Katalogelement mit dem vorhandenen Katalogelementnamen zu erstellen und eine Nummer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terraform Formular „Katalogelementaufgabe“ (Fortsetzung)

Feld	Beschreibung
	an den Katalogelementnamen anzuhängen. Beispiel: Wenn Ihr Katalogelement den Namen hat `Linux-VM` , Der neue Katalog wird mit dem Namen erstellt `Linux-VM 1` . Das Katalogelement wird automatisch aktiviert und kann über das Cloud-Benutzerportal bereitgestellt werden.
Zuweisungsgruppe	Die Zuweisungsgruppe, der Sie die Katalogelementaufgabe zuweisen.
Zugewiesen an	Benutzer, dem Sie die Aufgabe zuweisen
Kurzbeschreibung	Kurze Beschreibung der Aufgabe.
Freigabe	Genehmigungsstatus der Aufgabe
Arbeitsnotizen	Etwaige Notizen, die Sie für den Aufgabendatensatz eingeben möchten

Tag 2-Vorgänge mit Flow Designer subflow

Nutzen Sie das Framework der Workflows, um Ihre Vorgänge an Tag 2 zu automatisieren. Schreiben Sie schnell einen Workflow, der mit einer Cloud API oder einer bestimmten Ressource kommuniziert. Verwenden Sie SSH, PowerShell oder ein ähnliches Tool, um auf die Workflow-Fähigkeiten zuzugreifen und sie dann zu erweitern.

Die Tag-1-Vorgänge stellen Ressourcen in einer Cloud als Teil der Bestellung aus dem ServiceNow-Katalog oder dem Cloud-Katalog bereit. Diese Vorgänge führen zu einem Stapel, der eine Liste der bereitgestellten Ressourcen enthält. Tag-2-Vorgänge können für die Ressourcen ausgeführt werden, die Teil des Stapels sind, oder für die vom System erkannten Ressourcen.

Zuvor mussten Sie zum Ausführen von Tag-2-Vorgängen in Cloud Provisioning and Governance direkt mit der Cloud API (CAPI) interagieren. Dies bedeutete häufig, dass Sie neue APIs schreiben mussten, um einen neuen Vorgang zu unterstützen. Sie können jetzt Subflows verwenden, um Day 2-Vorgänge zuzuordnen und REST-Endpunkte zu erstellen, die Cloud-Anbieter aufrufen und plattformspezifische Aktionen auslösen.

Weitere Informationen

Allgemeine Informationen zu Workflows finden Sie unter:

- Workflow-Übersicht
- Workflow aus einer Tabelle erstellen

Informationen zum Arbeiten mit Variablen in Workflows finden Sie unter:

- Workflow-Eingabevariablen
- Variablen in einem Workflow verwenden

Anmeldeinformationen verarbeiten

Erweitern Sie das Workflow-Modul, um Prozesse zu verwalten und Dinge außerhalb einer Instanz mit Orchestration zu automatisieren. Verwenden Sie die entsprechenden Anmeldeinformationen, die für Aktivitätselemente von Orchestration SSH und PowerShell erforderlich sind: SSH erfordert SSH und PowerShell erfordert Windows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Cloud Provisioning and Governance-Anwendung generiert Anmeldeinformationen (Knotenanmeldeinformationen), nachdem eine VM bereitgestellt wurde. Knotenanmeldeinformationen werden verwendet, um eine Verbindung zu einer VM herzustellen. Zusätzlich zu den Knotenanmeldeinformationen generiert das System SSH-/ Windows-Anmeldeinformationen. Diese Anmeldeinformationen sind für Orchestration erforderlich, was die Automatisierung von Workflows bereitstellt.

Bereits vorhandene VMs

Cloud Provisioning and Governance generiert jetzt SSH-Anmeldeinformationen als private Schlüssel und Windows-Anmeldeinformationen für alle aktiven, bereits vorhandenen VMs, die über Cloud Provisioning and Governance bereitgestellt werden.

Anmeldeinformationen löschen

Wenn Sie die Bereitstellung einer VM aufheben oder sie löschen, werden alle zugehörigen Anmeldeinformationen gelöscht, einschließlich der Knotenanmeldeinformationen und der SSH-Anmeldeinformationen als private Schlüssel bzw. Windows-Anmeldeinformationen sowie des Anmeldeinformationsalias-Tags.

Anmeldeinformationen verwenden

Weitere Detailinformationen finden Sie unter .

Antwortaktion für Cloud Provisioning and Governance erstellen

Erstellen Sie einen Subflow mit den erforderlichen Eingabeparametern, der Cloud Provisioning and Governance benachrichtigt, ob der Flow erfolgreich abgeschlossen wurde oder nicht.

Vorbereitungen

- Stellen Sie sicher, dass Sie mit den Konzepten von vertraut sind , Subflows , Und Aktionsdesigner .
- Erstellen Sie einen Subflow, den Sie für die Vor- oder Nachbereitstellung aufrufen möchten.

Erforderliche Rolle: flow_designer, action_designer oder admin

Warum und wann dieser Vorgang ausgeführt wird

Informieren Sie die Cloud Provisioning and Governance-Anwendung über den Ausführungsstatus von Schritten im Subflow, indem Sie für jeden Schritt eine Antwort ausfüllen.

- Erstellen Sie eine Aktion mit relevanten Eingabeparametern.
- Fügen Sie der Aktion ein Skript hinzu.
- Übergeben Sie eine Korrelations-ID an die Aktion im Subflow.

Die Antwortaktion teilt der Cloud Provisioning and Governance-Anwendung mit, ob ein Schritt im Subflow erfolgreich ausgeführt wird oder ob die Bedingung des Schritts fehlschlägt und zu einem Fehler führt.

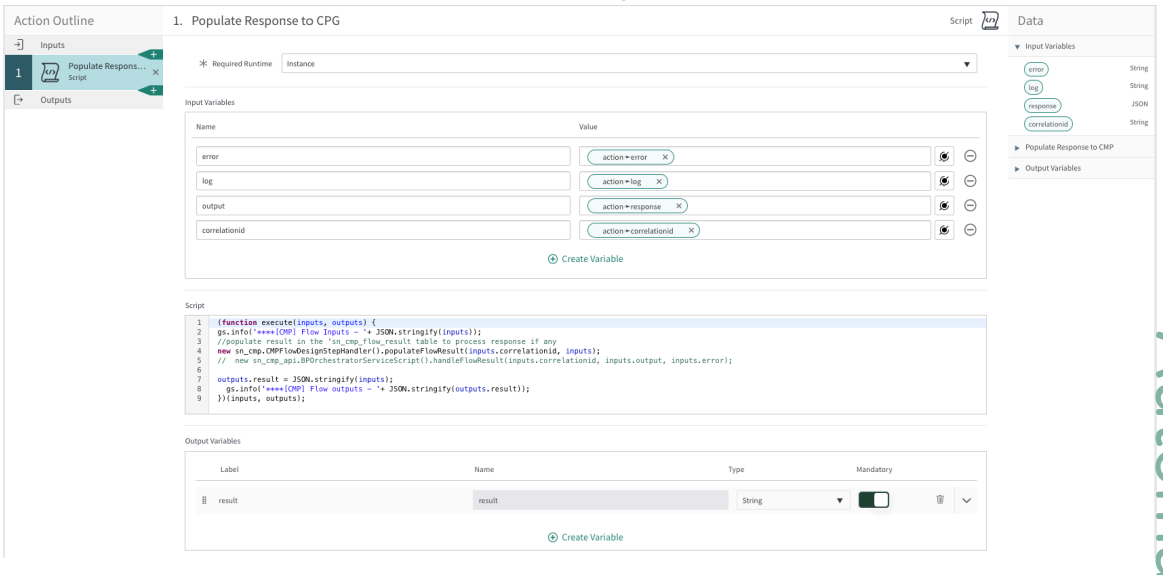
Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Aktionen** Wählen Sie die Registerkarte aus **Neue Aktion** . Weitere Informationen finden Sie unter Erstellen Sie eine Aktion .
2. Füllen Sie die Aktionseigenschaften aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Definieren Sie Aktionseingaben und erstellen Sie sie, um Daten für die Aktionsschritte und Ausgaben verfügbar zu machen.
   Erstellen Sie die folgenden Eingabevariablen: Fehler, Protokoll, Ausgabe und Korrelations-ID.

Beispiel für Antwortaktion an Cloud Provisioning and Governance



4. Wählen Sie einen Skriptaktionsschritt aus, um einen Vorgang für die Aktionseingaben durchzuführen.
5. **Speichern** und **Veröffentlichen** Sie die Aktion.
6. Öffnen Sie im **Flow Designer** den Subflow, den Sie aufrufen.

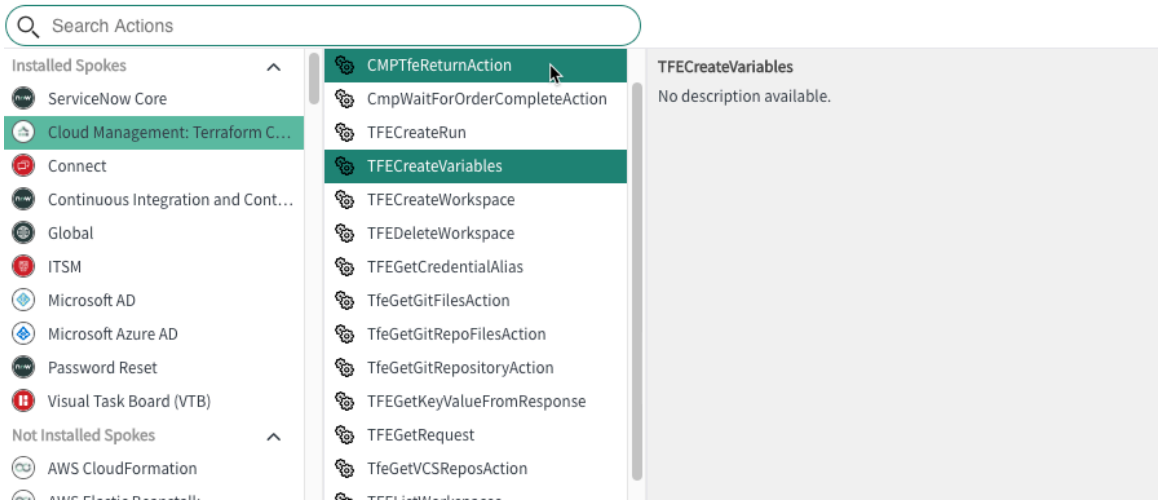
   Hinweis: Stellen Sie sicher, dass die Subflow-Eingabe `flowcorrelationid` im Subflow vorhanden ist.

7. Klicken Sie auf derselben Subflow-Seite auf **Aktionen** Um zu erweitern und zu suchen **Aktionen** , **Subflow** Oder **Flow-Logik** .
8. Wählen Sie Aus Cloud Provisioning and Governance Suchen Sie und die Antwortaktion aus der Dropdown-Liste, und fügen Sie sie hinzu.
9. Wählen Sie für die Eingaben in der Aktion relevante Werte aus der **Datenpillenauswahl** aus.

   Hinweis: Verwenden Sie die Eingabe `flowcorrelationid` aus dem **Datenbereich** für jede Aktion im Subflow, die einen logischen Endschritt aufweist, wieder.

10. **Wahlweise:** Wenn Sie den Terraform Connector für Terraform Enterprise verwenden, führen Sie diese Schritte aus.
    a. Zum Hinzufügen von Aktionen, Flows, Subflows oder Flow-Logik klicken Sie auf **Zum Hinzufügen einer Aktion, einer Flow-Logik oder eines Subflow auswählen**.
    b. Auswahlvorgang **Aktion** > **Cloud-Management: Terraform-Connector**, Und wählen Sie eine Standardaktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die von Ihnen erstellte Aktion sendet eine Antwort an die Cloud Provisioning and Governance-Anwendung und aktualisiert die Reihenfolge mit dem Status des Schritts des Subflows.

Nächste Maßnahme

Testen Sie den Subflow und veröffentlichen Sie ihn, wenn er zum Hinzufügen zu einem Flow oder zum Aufrufen aus einem Skript bereit ist.

Hinweis: Sie können nur Subflows testen oder veröffentlichen, die mindestens eine Aktion enthalten.

Cloud-Katalogelement erstellen

Erstellen Sie, basierend auf einer Vorlage oder einer vorhandenen Blaupause, ein Cloud-Katalogelement für die Bereitstellung und veröffentlichen Sie das Katalogelement, um einen Service bereitzustellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Beim Erstellen eines Katalogelements können Sie das Katalogelement mit einer Vorlage verknüpfen, die entweder nativ für den Cloud-Anbieter ist (z. B. CFT, ARM, GDM) oder bei der es sich um eine Terraform-IaC-Vorlage handelt. Nachdem Sie ein Katalogelement generiert haben, generiert das System automatisch Komponenten wie Variablensätze, Lebenszyklusvorgänge, Regeln sowie Vor- und Nachbereitstellungsvorgänge. Sie können alle diese Komponenten auf der Seite „Katalogelement erstellen“ verwalten.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-Katalogelemente**an.
   Alle von Ihnen erstellten Katalogelemente werden in einer Kartenlayoutansicht aufgelistet. Sie können auf ein inaktives Katalogelement klicken, um es bereitzustellen.
2. Klicken Sie auf **Neu**.
   Der Bildschirm „Cloud-Katalogelemente“ wird angezeigt.
3. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Katalogelement“

Feld	Beschreibung
Name	Name des Katalogelements.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option zur Bereitstellung des Katalogelements. Dieses Kontrollkästchen kann erst aktiviert werden, nachdem Sie eine Blaupause ausgewählt haben.
Symbol	Das Bild wird neben dem Artikelnamen im Katalog als Symbol angezeigt. Sie können Sie ein 16x16-Pixel-Bild hochladen. Wenn kein Bild hochgeladen wird, wird neben diesem Element das Standardsymbol angezeigt. Das hochgeladene Bild überschreibt das Standardbild. Das von Ihnen hochgeladene Bild wird im Servicekatalog angezeigt, nicht in der ServiceNow® Cloud Provisioning and Governance-Anwendung.
Bild	Bild für das Katalogelement. Das von Ihnen ausgewählte Bild wird im Cloudbenutzerportal für das Katalogelement angezeigt (nachdem Sie auf **Einen Stapel starten** geklickt haben).
Kataloge	Namen der Kataloge.
Kategorie	Die Kategorie für das Element wird standardmäßig angezeigt. Sie können die Kategorie ändern. Katalogsuchen finden nur Elemente, die einer Kategorie zugewiesen sind. Die Kategorien werden im Servicekatalog angezeigt. Das Katalogelement kann in mehreren Kategorien angezeigt werden. Zum Hinzufügen von Kategorien klicken Sie auf die Registerkarte **Kategorien**, und dann auf **Neu** oder **Bearbeiten**.
Quelle	Quelltyp (Cloud-Vorlage oder Benutzerdefiniert), mit dem das Katalogelement verknüpft werden soll.
Vorlagentyp	○ Wählen Sie **Cloud-Vorlage** aus, und wählen Sie dann den Vorlagentyp (**ARM-Vorlage** oder **CloudFormation-Vorlage** zum Importieren Cloud-nativer Vorlagen) aus. ○ Wählen Sie **Konfigurationsverwaltungsvorlage** aus, um die Vorlagen der Konfigurationsverwaltungs-Provider Ansible oder Terraform zu verwenden.
Blaupause	Wenn Sie im Feld **Quelle** die Option **Benutzerdefiniert** ausgewählt haben, wählen Sie eine Blaupause aus, die dem Katalogelement zugeordnet werden soll.
Planvorgang	Nachdem Sie das Katalogelement generiert haben, wird der Wert in diesem Feld automatisch eingetragen. Dieses Feld wird nur angezeigt, wenn Sie eine Blaupause auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kurzbeschreibung	Kurzbeschreibung des Katalogelements. Diese Beschreibung wird im Cloudbenutzerportal neben dem Katalogelement angezeigt.
Beschreibung	Vollständige Beschreibung des Katalogelements. Diese Beschreibung wird im Servicekatalog angezeigt, nicht in der Cloud Provisioning and Governance-Anwendung. Sie können Videos, Bilder, Links zu Artikeln der internen Knowledge Base (KB) und Links zu externen Informationsquellen und Anleitungen einbetten.

4. Klicken Sie auf **Absenden**.
   Das Katalogelement und alle zugehörigen Komponenten wie Variablensätze, Lebenszyklusvorgänge und Regeln werden generiert und als Registerkarten auf der Seite „Cloud-Katalogelement“ angezeigt.

   Hinweis: Wenn Sie **Vorlage** aus der Liste „Quelltyp“ ausgewählt haben, müssen Sie eine Vorlage erstellen und die Vorlage dem Katalogelement zuordnen.

   Die zugehörigen Links sind Aktionen, die Sie für das Katalogelement ausführen können.

Aktion	Beschreibung
Katalogelement exportieren	Exportiert alle Komponenten (z. B. Blaupausen, Ressourcenblöcke, Regeln) des Katalogelements aus einer Umgebung in die andere. Weitere Informationen finden Sie unter Verschieben von Cloud Provisioning and Governance-Inhalten zwischen Umgebungen.
Elementdiagnose	Identifiziert mögliche Probleme mit den Katalogelementdaten und der Konfiguration. Siehe Elementdiagnosebericht
Attribute verwalten	Weitere Informationen finden Sie unter Vorgangsattribute verwalten.
Katalogelement zurücksetzen	Setzt alle Anpassungen zurück, die Sie am Katalogelement vorgenommen haben (bis zur letzten von Ihnen vorgenommenen Änderung).

Nächste Maßnahme

Auf Cloud-Vorlage basierendes Katalogelement erstellen an.

Zugehörige Informationen

Katalogelement aus einer Terraform-Vorlage erstellen

Veröffentlichen Sie einen Blueprint als Cloud-Katalogelement

Sie können ein Katalogelement direkt aus einer Blaupause erstellen und veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Blueprints**an.
2. Öffnen Sie eine Blaupause (im Entwurfsmodus), klicken Sie auf die Registerkarte **Katalog**, und klicken Sie dann auf **Katalogelement erstellen**.
   Das Dialogfeld „Blaupausenkatalog erstellen“ wird angezeigt.
3. Geben Sie einen Namen für das Katalogelement in das Feld **Name** ein, und klicken Sie auf **Speichern**.
   Das Katalogelement wird generiert und auf der Registerkarte **Katalog** angezeigt.
4. Klicken Sie auf das Katalogelement, um Aktualisierungen am Katalogelement vorzunehmen.
   Der Bildschirm „Cloud-Katalogelement“ wird angezeigt.
5. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

Auf Cloud-Vorlage basierendes Katalogelement erstellen

Erstellen Sie eine Cloud-Vorlage, und ordnen Sie die Vorlage einem Katalogelement zu. Sobald Sie eine Vorlage erstellt haben, können Sie die Vorlage erneut verwenden, um zusätzliche Katalogelemente für die Services zu erstellen, die Sie bereitstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Vorlage erstellen, indem Sie eine generische Vorlagendatei hochladen, eine Vorlage von einer öffentlichen URL importieren oder den Inhalt einer vorhandenen Vorlage kopieren und einfügen. AWS CloudFormation-Vorlagen (CFT) bieten Unterstützung für JSON und YAML. Azure Resource Manager-Vorlagen (ARM) bieten Unterstützung für JSON. Die folgenden Inhaltstypen für URLs öffentlicher Vorlagen werden unterstützt:

- Text/Plain
- Application/JSON
- YAML MIME

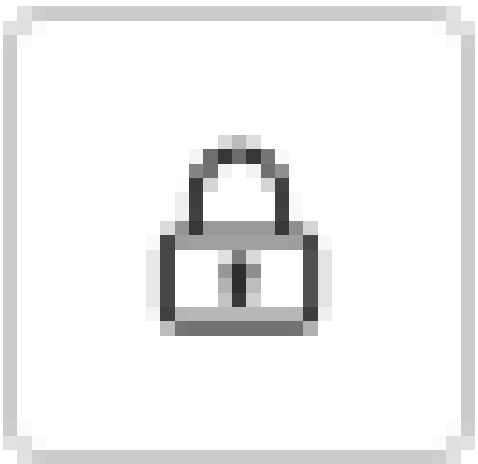
Hinweis: Katalogelemente, die auf Vorlagen in früheren Releases basierten, werden nun so behandelt, als ob sie auf Blaupausen basieren.

Sie können eine Vorlage beliebig oft aktualisieren. Mit jeder Aktualisierung wird eine neue Version der Vorlage erstellt. Eine Vorlage kann einen von drei Status haben: **Entwurf**, **Aktiv** oder **Verlauf**. Wenn Sie eine Vorlage erstellen und nicht aktivieren, befindet sich die Vorlage im Entwurfsstatus. Sobald Sie die Vorlage aktiviert haben, ändert sich der Status in „Aktiv“. Wenn Sie eine andere Vorlage erstellen und diese aktivieren, wird der Status der vorherigen aktiven Vorlage in „Verlauf“ geändert. Zu jeder Zeit ist nur eine Vorlage im Status „Aktiv“. Jedes Mal, wenn Sie eine Vorlage aktivieren, wird die vorherige aktive Vorlage dem Verlauf zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente** Und erstellen Sie dann ein Katalogelement, oder öffnen Sie ein vorhandenes Katalogelement.
2. Klicken **Cloud-Vorlagen** > **Neu** Und geben Sie dann eine aussagekräftige Kurzbeschreibung in ein **Kurzbeschreibung** Feld.
3. Geben Sie die **Erfassungsmethode** an.

Option	Bezeichnung
Import aus URL	Importieren Sie eine Vorlage, indem Sie eine öffentliche URL angeben, unter der sich die Vorlage befindet. Wählen Sie diese Option aus, und klicken Sie dann auf das Sperrsymbol (), um das Feld **Cloud-Vorlagen-URL** zu entsperren. Geben Sie die öffentliche URL in dieses Feld ein. **Hinweis:** Für die öffentliche URL werden nur die Protokolle HTTP und HTTPS unterstützt. FTP wird nicht unterstützt. Stellen Sie sicher, dass die Größe der Vorlage den Standardwert von 3 MB nicht überschreitet. Sie können den Standardwert der Dateigröße ändern, indem Sie den Wert in der Eigenschaft `sn_cmp.template_content_size_supported_inbyte` in der Tabelle „sys_properties“ ändern. Geben Sie die Dateigröße in Byte ein. Es gibt auch eine Standardzeitüberschreitung von 5 Minuten für eine HTTP-Anforderung. Sie können den Wert für die Zeitüberschreitung in der Eigenschaft `sn_cmp.template_url_import_http_timeout` in der Tabelle „sys_properties“ ändern. Geben Sie den neuen Wert in Millisekunden ein.
Eine Datei hochladen	Laden Sie eine Vorlage von Ihrer lokalen Workstation hoch.

Automatische Übersetzung

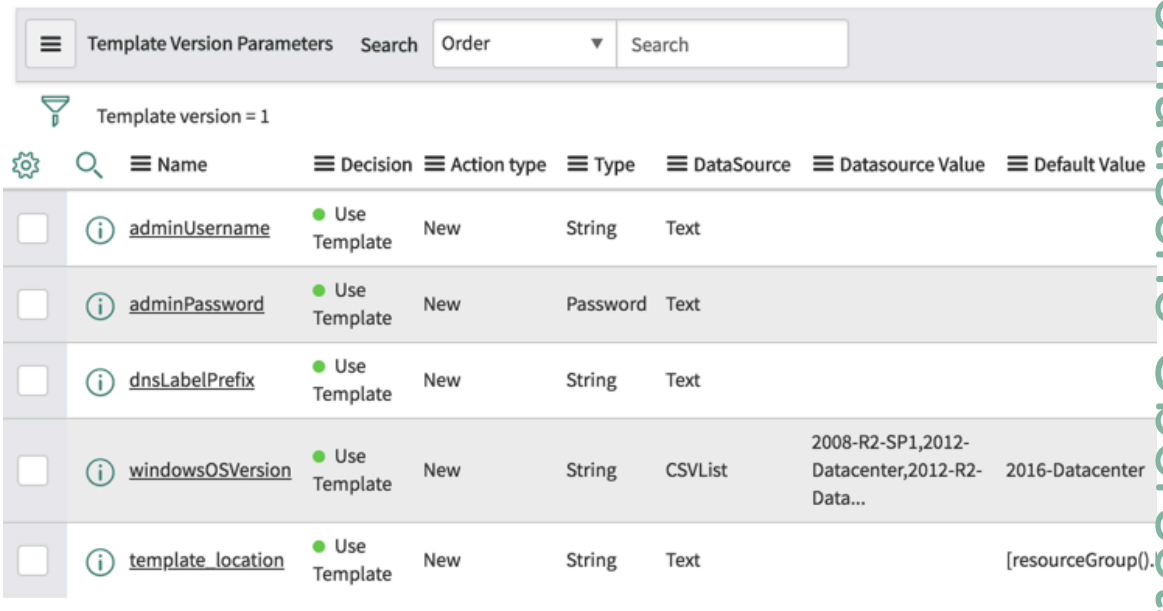
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Vorlagen-Textkörper verwenden	Fügen Sie den Inhalt der Vorlagendatei in das Feld **Text** ein.

Nachdem Sie die **Erfassungsmethode** angegeben haben, wird die Vorlage validiert, und die Ergebnisse werden in den Feldern **Validierungsstatus** und **Validierungsnachricht** angezeigt.

4. Klicken Sie auf **Absenden**.
   Die Vorlage wird erstellt, und die Seite „Cloud-Katalogelement“ wird geöffnet.
5. Wenn dies die erste Version der Vorlage ist, überspringen Sie diesen Schritt, andernfalls im **Cloud-Vorlagen** Registerkarte öffnen Sie die Vorlage (derzeit im Entwurfsstatus), um die Parameter der Vorlagenversion anzuzeigen.

   Hinweis: Die erste Version einer Vorlage, die Sie erstellen und veröffentlichen, weist keine Konfliktprobleme auf. Wenn Sie die Vorlage aktualisieren, kann ein Konflikt auftreten. Wenn ein Parameter **Aktionstyp** den Wert **Aktualisieren** hat, dann geben Sie einen Wert für **Entscheidung** an.



6. Öffnen Sie jeden Parameter, der für **Entscheidung** einen Wert von **Ausstehend** hat, wählen Sie einen Wert aus, und klicken Sie dann auf das Häkchen .

Option	Bezeichnung
Aktualisierung überspringen	Die Aktualisierungen der Vorlage werden verworfen.
Vorlage verwenden	Die Aktualisierungen der Vorlage werden angewendet.

7. Nachdem Sie alle **ausstehenden** Entscheidungen aktualisiert haben, klicken Sie auf **Aktivieren**.
   Der Status der Vorlage ändert sich von **Entwurf** in **Aktiv**, und das System generiert das Katalogelement.

CloudFormation-JSON-Codebeispiel zum Erstellen einer AWS EC2-Instanz

Referenz-Codebeispiel zum Bereitstellen einer Amazon AWS Cloud EC2-Instanz

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS EC2-Instanzen mit CloudFormation bereitstellen

- Überprüfen Sie beim Entwerfen eines Katalogelements die CloudFormation-Vorlage, um die Services zu identifizieren, die bereitgestellt werden. Vergewissern Sie sich, dass entsprechende Berechtigungen für die Services gewährt werden können, damit keine Fehler aufgrund fehlender Berechtigungen auftreten, wenn der Stapel bestellt wird. Weitere Informationen finden Sie unter Konfigurieren Sie Berechtigungen in der AWS-Konsole
- Nehmen Sie die erforderlichen Änderungen vor, indem Sie dieses Codebeispiel als Referenz verwenden.

```
{
  "AWSTemplateFormatVersion":"2010-09-09",
  "Description":"AWS CloudFormation Sample Template
EC2InstanceWithSecurityGroupSample: Create an Amazon EC2 instance running the Amazon
Linux AMI. The AMI is chosen based on the region in which the stack is run. This example
creates an EC2 security group for the instance to give you SSH access. **WARNING** This
template creates an Amazon EC2 instance. You will be billed for the AWS resources used if you
create a stack from this template.",
  "Parameters":{
    "KeyName":{
      "Description":"Name of an existing EC2 KeyPair to enable SSH access to the instance",
      "Type":"AWS::EC2::KeyPair::KeyName",
      "Default":"admin-Default",
      "ConstraintDescription":"must be the name of an existing EC2 KeyPair."
    },
    "InstanceType":{
      "Description":"WebServer EC2 instance type",
      "Type":"String",
      "Default":"t2.micro",
      "AllowedValues":[
        "t1.micro",
        "t2.nano",
        "t2.micro",
        "t2.small",
        "t2.medium",
        "t2.large",
        "m1.small",
        "m1.medium",
        "m1.large",
        "m1.xlarge",
        "m2.xlarge",
        "m2.2xlarge",
        "m2.4xlarge",
        "m3.medium",
        "m3.large",
        "m3.xlarge",
        "m3.2xlarge",
        "m4.large",
        "m4.xlarge",
        "m4.2xlarge",
        "m4.4xlarge",
        "m4.10xlarge",
        "c1.medium",
        "c1.xlarge",
        "c3.large",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "c3.xlarge",
        "c3.2xlarge",
        "c3.4xlarge",
        "c3.8xlarge",
        "c4.large",
        "c4.xlarge",
        "c4.2xlarge",
        "c4.4xlarge",
        "c4.8xlarge",
        "g2.2xlarge",
        "g2.8xlarge",
        "r3.large",
        "r3.xlarge",
        "r3.2xlarge",
        "r3.4xlarge",
        "r3.8xlarge",
        "i2.xlarge",
        "i2.2xlarge",
        "i2.4xlarge",
        "i2.8xlarge",
        "d2.xlarge",
        "d2.2xlarge",
        "d2.4xlarge",
        "d2.8xlarge",
        "hi1.4xlarge",
        "hs1.8xlarge",
        "cr1.8xlarge",
        "cc2.8xlarge",
        "cg1.4xlarge"
      ],
      "ConstraintDescription":"must be a valid EC2 instance type."
    },
    "SSHLocation":{
      "Description":"The IP address range that can be used to SSH to the EC2 instances",
      "Type":"String",
      "MinLength":"9",
      "MaxLength":"18",
      "Default":"0.0.0.0/0",
      "AllowedPattern":"(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\\d{1,2})",
      "ConstraintDescription":"must be a valid IP CIDR range of the form x.x.x.x/x."
    },
    "Network":{
      "Description":"The Network to the EC2 instances",
      "Type":"String"
    },
    "AvailabilityZone":{
      "Description":"The AZ of the EC2 instance",
      "Type":"String"
    },
    "SubnetPool":{
      "Description":"The IP address range that can be used to SSH to the EC2 instances",
      "Type":"String"
    }
  },
  "Metadata":{
    "SNC::Parameter::Metadata":{
      "SubnetPool":{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "datasource":"ServiceNow::Pools::SubnetPool.getObjectsByNetwork",
        "datasourceFilter":{
          "Network":"Network"
        }
      },
      "Network":{
        "datasource":"ServiceNow::Pools::NetworkPool.getObjectsByLDC"
      },
      "KeyName":{
        "datasource":"ServiceNow::Pools::CloudKeyPairPool.getObjectsByLDC"
      }
    }
  },
  "Mappings":{
    "AWSInstanceType2Arch":{
      "t1.micro":{
        "Arch":"PV64"
      },
      "t2.nano":{
        "Arch":"HVM64"
      },
      "t2.micro":{
        "Arch":"HVM64"
      },
      "t2.small":{
        "Arch":"HVM64"
      },
      "t2.medium":{
        "Arch":"HVM64"
      },
      "t2.large":{
        "Arch":"HVM64"
      },
      "m1.small":{
        "Arch":"PV64"
      },
      "m1.medium":{
        "Arch":"PV64"
      },
      "m1.large":{
        "Arch":"PV64"
      },
      "m1.xlarge":{
        "Arch":"PV64"
      },
      "m2.xlarge":{
        "Arch":"PV64"
      },
      "m2.2xlarge":{
        "Arch":"PV64"
      },
      "m2.4xlarge":{
        "Arch":"PV64"
      },
      "m3.medium":{
        "Arch":"HVM64"
      },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "m3.large":{
      "Arch":"HVM64"
    },
    "m3.xlarge":{
      "Arch":"HVM64"
    },
    "m3.2xlarge":{
      "Arch":"HVM64"
    },
    "m4.large":{
      "Arch":"HVM64"
    },
    "m4.xlarge":{
      "Arch":"HVM64"
    },
    "m4.2xlarge":{
      "Arch":"HVM64"
    },
    "m4.4xlarge":{
      "Arch":"HVM64"
    },
    "m4.10xlarge":{
      "Arch":"HVM64"
    },
    "c1.medium":{
      "Arch":"PV64"
    },
    "c1.xlarge":{
      "Arch":"PV64"
    },
    "c3.large":{
      "Arch":"HVM64"
    },
    "c3.xlarge":{
      "Arch":"HVM64"
    },
    "c3.2xlarge":{
      "Arch":"HVM64"
    },
    "c3.4xlarge":{
      "Arch":"HVM64"
    },
    "c3.8xlarge":{
      "Arch":"HVM64"
    },
    "c4.large":{
      "Arch":"HVM64"
    },
    "c4.xlarge":{
      "Arch":"HVM64"
    },
    "c4.2xlarge":{
      "Arch":"HVM64"
    },
    "c4.4xlarge":{
      "Arch":"HVM64"
    },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"c4.8xlarge":{
  "Arch":"HVM64"
},
"g2.2xlarge":{
  "Arch":"HVMG2"
},
"g2.8xlarge":{
  "Arch":"HVMG2"
},
"r3.large":{
  "Arch":"HVM64"
},
"r3.xlarge":{
  "Arch":"HVM64"
},
"r3.2xlarge":{
  "Arch":"HVM64"
},
"r3.4xlarge":{
  "Arch":"HVM64"
},
"r3.8xlarge":{
  "Arch":"HVM64"
},
"i2.xlarge":{
  "Arch":"HVM64"
},
"i2.2xlarge":{
  "Arch":"HVM64"
},
"i2.4xlarge":{
  "Arch":"HVM64"
},
"i2.8xlarge":{
  "Arch":"HVM64"
},
"d2.xlarge":{
  "Arch":"HVM64"
},
"d2.2xlarge":{
  "Arch":"HVM64"
},
"d2.4xlarge":{
  "Arch":"HVM64"
},
"d2.8xlarge":{
  "Arch":"HVM64"
},
"hi1.4xlarge":{
  "Arch":"HVM64"
},
"hs1.8xlarge":{
  "Arch":"HVM64"
},
"cr1.8xlarge":{
  "Arch":"HVM64"
},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "cc2.8xlarge":{
      "Arch":"HVM64"
    }
  },
  "AWSRegionArch2AMI":{
    "us-east-1":{
      "PV64":"ami-2a69aa47",
      "HVM64":"ami-6869aa05",
      "HVMG2":"ami-a41a3fb3"
    },
    "us-west-2":{
      "PV64":"ami-7f77b31f",
      "HVM64":"ami-7172b611",
      "HVMG2":"ami-caf253aa"
    },
    "us-west-1":{
      "PV64":"ami-a2490dc2",
      "HVM64":"ami-31490d51",
      "HVMG2":"ami-00347e60"
    },
    "eu-west-1":{
      "PV64":"ami-4cdd453f",
      "HVM64":"ami-f9dd458a",
      "HVMG2":"ami-e2f7bd91"
    },
    "eu-central-1":{
      "PV64":"ami-6527cf0a",
      "HVM64":"ami-ea26ce85",
      "HVMG2":"ami-d2ff04bd"
    },
    "ap-northeast-1":{
      "PV64":"ami-3e42b65f",
      "HVM64":"ami-374db956",
      "HVMG2":"ami-4c78d52d"
    },
    "ap-northeast-2":{
      "PV64":"NOT_SUPPORTED",
      "HVM64":"ami-2b408b45",
      "HVMG2":"NOT_SUPPORTED"
    },
    "ap-southeast-1":{
      "PV64":"ami-df9e4cbc",
      "HVM64":"ami-a59b49c6",
      "HVMG2":"ami-f3f95990"
    },
    "ap-southeast-2":{
      "PV64":"ami-63351d00",
      "HVM64":"ami-dc361ebf",
      "HVMG2":"ami-3a122e59"
    },
    "ap-south-1":{
      "PV64":"NOT_SUPPORTED",
      "HVM64":"ami-ffbdd790",
      "HVMG2":"ami-21a7d34e"
    },
    "us-east-2":{
      "PV64":"NOT_SUPPORTED",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "HVM64":"ami-f6035893",
        "HVMG2":"NOT_SUPPORTED"
      },
      "sa-east-1":{
        "PV64":"ami-1ad34676",
        "HVM64":"ami-6dd04501",
        "HVMG2":"NOT_SUPPORTED"
      },
      "cn-north-1":{
        "PV64":"ami-77559f1a",
        "HVM64":"ami-8e6aa0e3",
        "HVMG2":"NOT_SUPPORTED"
      }
    }
  },
  "Resources":{
    "EC2Instance":{
      "Type":"AWS::EC2::Instance",
      "Properties":{
        "InstanceType":{
          "Ref":"InstanceType"
        },
        "KeyName":{
          "Ref":"KeyName"
        },
        "SubnetId":{
          "Ref":"SubnetPool"
        },
        "ImageId":{
          "Fn::FindInMap":[
            "AWSRegionArch2AMI",
            {
              "Ref":"AWS::Region"
            },
            {
              "Fn::FindInMap":[
                "AWSInstanceType2Arch",
                {
                  "Ref":"InstanceType"
                },
                "Arch"
              ]
            }
          ]
        }
      }
    },
    "InstanceSecurityGroup":{
      "Type":"AWS::EC2::SecurityGroup",
      "Properties":{
        "GroupDescription":"Enable SSH access via port 22",
        "SecurityGroupIngress":[
          {
            "IpProtocol":"tcp",
            "FromPort":"22",
            "ToPort":"22",
            "CidrIp":{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
              "Ref":"SSHLocation"
            }
          }
        ]
      }
    }
  },
  "Outputs":{
    "InstanceId":{
      "Description":"InstanceId of the newly created EC2 instance",
      "Value":{
        "Ref":"EC2Instance"
      }
    },
    "AZ":{
      "Description":"Availability Zone of the newly created EC2 instance",
      "Value":{
        "Fn::GetAtt":[
          "EC2Instance",
          "AvailabilityZone"
        ]
      }
    }
  }
}
```

Vorbereitstellungsvorgänge erstellen

Vorbereitstellungsvorgänge optimieren die Bereitstellung von Katalogelementen, indem Aufgaben wie Benachrichtigungen, Workflows oder Skripts vor der Bereitstellung automatisiert werden. Durch die Konfiguration dieser Vorgänge werden manuelle Schritte vermieden, was Zeit und Aufwand spart, da das System die angegebenen Aktionen automatisch ausführt, wenn eine Bereitstellungsanforderung übermittelt wird, z. B. die Benachrichtigung von Anwendern über den bevorstehenden Elementbereitstellungsprozess.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können Vorbereitstellungsaufgaben nur für Katalogelemente erstellen, die auf Vorlagen basieren.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente**an.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Pre Provisioning Operation** (Vorbereitstellungsvorgang), klicken Sie auf **Neu**, und füllen Sie das Formular aus.

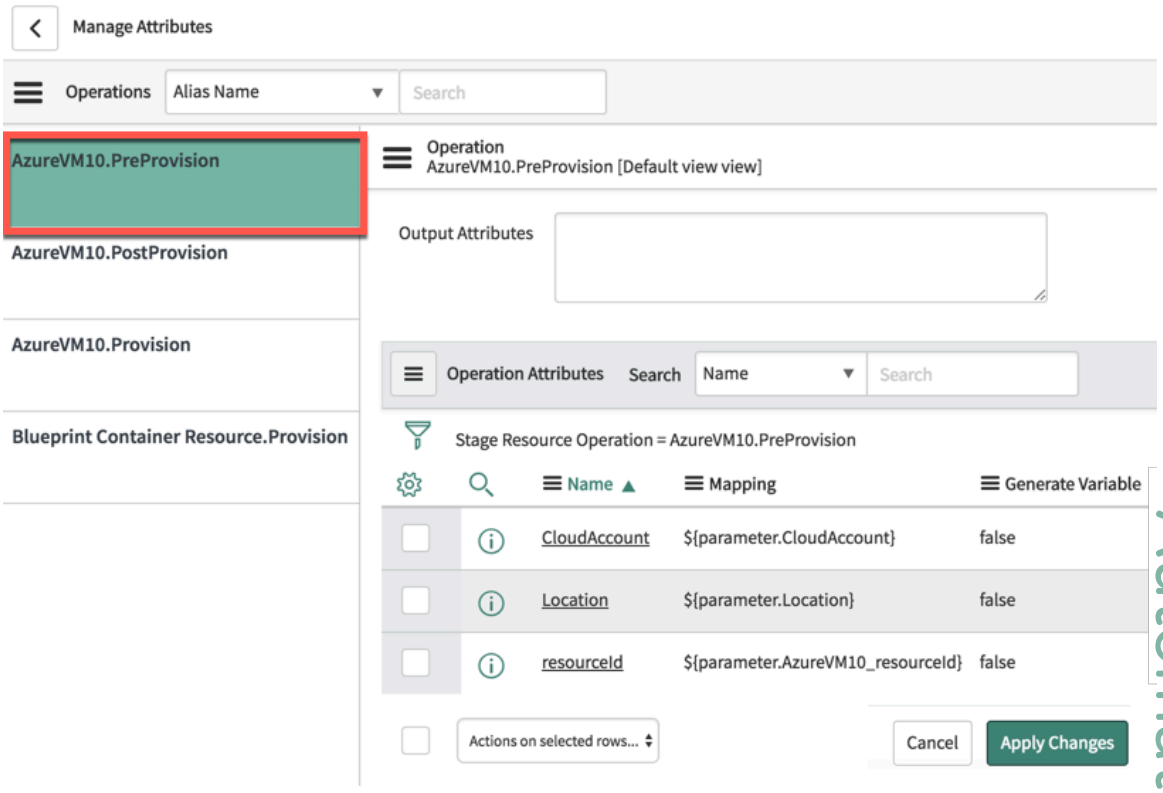
Feld	Beschreibung
Schritttyp	Vorbereitstellungsvorgänge. Abhängig vom Typ des ausgewählten Vorbereitstellungsvorgangs werden zusätzliche Felder angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ CAPI: ▪ CAPI-Provider ▪ CAPI-Methode ▪ CAPI-Version ○ InstanceScript: Skript: Geben Sie den Namen des Skripts ein. ○ Ressource: ▪ Ressourcenschnittstelle ▪ Schnittstellenvorgang ○ Flow: Wählen Sie einen Subflow aus. Alle aktiven Subflows in der Instanz werden aufgelistet. **Hinweis:** Weitere Informationen finden Sie unter Subflows .
Reihenfolge	Reihenfolge der Vorbereitstellungsvorgänge. Geben Sie die Reihenfolge ein, in der der Vorbereitstellungsvorgang aufgerufen werden soll. Niedrigere Zahlen werden zuerst aufgerufen. Wenn Sie beispielsweise 2 für CAPI und 3 für InstanceScript eingeben, wird zuerst CAPI und dann das InstanceScript aufgerufen. Wenn Sie keinen Wert in dieses Feld eingeben, gibt das System automatisch einen Wert in Schritten von 20 ein.
Aktiviert	Option zum Aktivieren des Vorbereitstellungsvorgangs, der aufgerufen werden soll.

3. Klicken Sie auf **Absenden**.
   Parameter für Vorbereitstellungsvorgänge werden als Vorgangsattribute auf der Seite „Attribute verwalten“ erstellt.
4. Klicken Sie zum Hinzufügen von Werten für die Attribute des Vorbereitstellungsvorgangs auf **Attribute verwalten**.
   Der Bildschirm „Attribute verwalten“ wird angezeigt.
5. Klicken Sie auf **PreProvision**.
   Alle Attribute für den Vorbereitstellungsvorgang werden aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Erstellen Sie entweder Ausdruckszuordnungen für ein Attribut (in der) **Zuordnung** Feld) oder generieren Sie Variablen für ein Attribut.
   Weitere Informationen finden Sie unter Vorgangsattribute verwalten.
7. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
   Alle Konfigurationen, die Sie an den Attributen vorgenommen haben, werden gespeichert, und Sie kehren zum Bildschirm „Cloud-Katalogelemente“ zurück.

Post-Bereitstellungsvorgänge erstellen

Erstellen Sie Aufgaben nach der Bereitstellung für neu bereitgestellte Katalogelemente, indem Sie Subflows, Skripts, CAPI-Aufrufe oder Ressourcenvorgänge definieren. Um die Effizienz zu erhöhen, richten Sie einen Vorgang nach der Bereitstellung ein, sodass kein manueller Aufruf erforderlich ist. Dieser Ansatz verbessert das Zeitmanagement und stellt die nahtlose Ausführung der gewünschten Aktionen für das Katalogelement nach der Ressourcenbereitstellung sicher.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Sie können Post-Bereitstellungsvorgänge nur für Katalogelemente erstellen, die auf Vorlagen basieren.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente**an.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Post-Bereitstellungsvorgang**, und klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

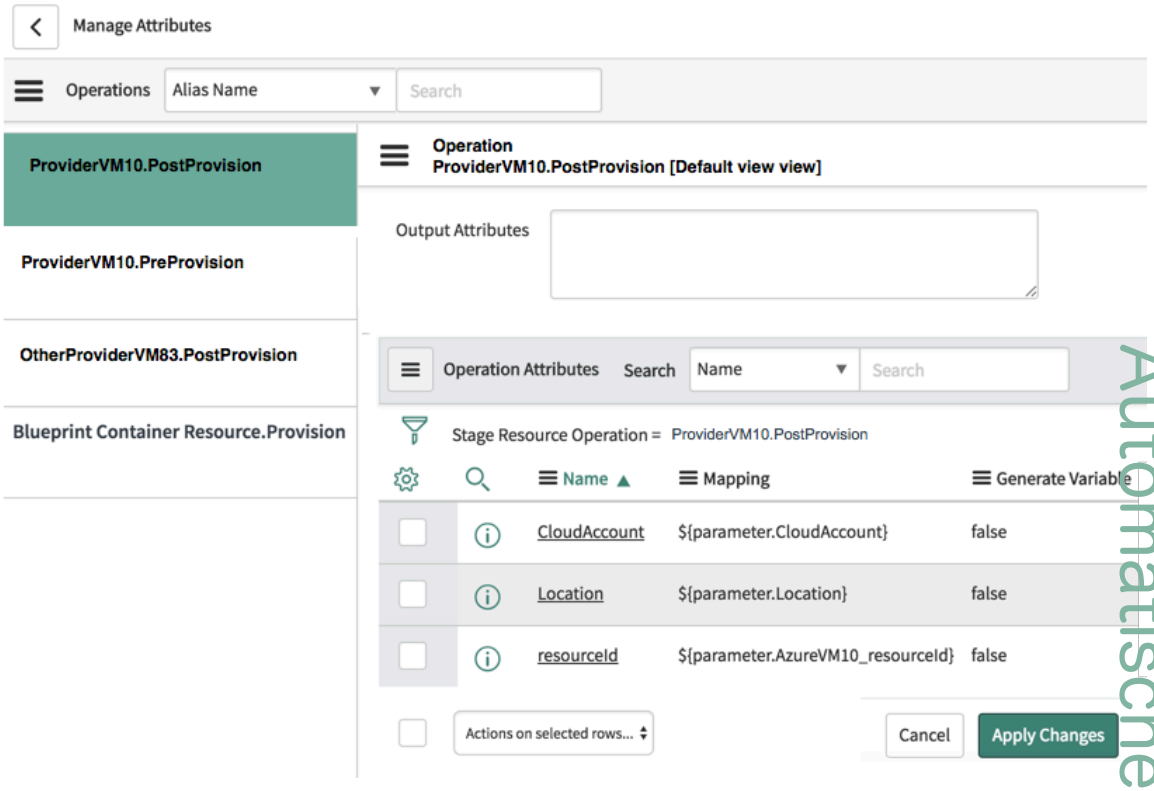
Formular zur Vorgangseinrichtung

Feld	Beschreibung
Schritttyp	Post-Bereitstellungsvorgang. Abhängig vom Typ des ausgewählten Post-Bereitstellungsvorgangs werden zusätzliche Felder angezeigt. ○ CAPI: ▪ CAPI-Provider ▪ CAPI-Schnittstelle ▪ CAPI-Methode ▪ CAPI-Version ○ InstanceScript: Skript: Geben Sie den Namen des Skripts ein. ○ Ressource: ▪ Ressourcenschnittstelle ▪ Schnittstellenvorgang ○ Flow: Wählen Sie einen Subflow aus. Alle aktiven Subflows in der Instanz werden aufgelistet. **Hinweis:** Weitere Informationen finden Sie unter Subflows .
Reihenfolge	Reihenfolge von Post-Bereitstellungsvorgängen. Geben Sie die Reihenfolge (in Zahlen) ein, in der der Post-Bereitstellungsvorgang aufgerufen werden soll. Wenn Sie beispielsweise den Wert 2 für CAPI und den Wert 3 für InstanceScript eingeben, wird zuerst CAPI und dann das InstanceScript aufgerufen. Wenn Sie keinen Wert in dieses Feld eingeben, gibt das System automatisch einen Wert in Schritten von 20 ein.
Aktiviert	Option zum Aktivieren des Post-Bereitstellungsvorgangs, der aufgerufen werden soll.

4. Klicken Sie auf **Absenden**.
   Parameter für den Post-Bereitstellungsvorgang werden automatisch als Vorgangsattribute im Formular „Attribute verwalten“ erstellt.
5. So legen Sie Attributwerte für einen Post-Bereitstellungsvorgang fest:
   a. Klicken Sie auf den zugehörigen Link **Attribute verwalten**.
      Das Formular „Attribute verwalten“ wird geöffnet.
   b. Wählen Sie den zu aktualisierenden Post-Bereitstellungsvorgang aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Attribute für den ausgewählten Vorgang werden in der Liste der Vorgänge angezeigt. Sie können entweder Ausdruckszuordnungen (wie in der Spalte **Zuordnung**) für ein Attribut erstellen oder Variablen für ein Attribut generieren. Weitere Informationen finden Sie unter Vorgangsattribute verwalten.



c. Bearbeiten Sie im Formular „Vorgangsattribute“ die Werte im Feld **Zuordnung** nach Bedarf.

d. Um einen Wert festzulegen und das Feld nicht für Cloud-Benutzer anzuzeigen, setzen Sie **Variable generieren** auf „false“.

Für Post-Bereitstellungsvorgänge für VMware können Sie die folgenden Attributwerte festlegen:

Post-Bereitstellungsvorgangsattribute für VMware

Attributname	Im Zuordnungsausdruck festzulegendes <Wertfeld>
NodeCredential	$(capiResolver.NodeCredentialResolver#nodeCredentialId=<AnmeldeSysID>) **Hinweis:** Sie müssen die Anmeldeinformationen manuell erstellen, um die sys_id im Ausdruck angeben zu können.
NodeAddress	$(Script:CMPVMUtils.getReachableIp[arg=$(Stack.items[<VM-Name>].attributes[sys_id])])
ScriptExpression	${CloudScript.scripts.]]>}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
Alle Konfigurationen werden gespeichert, und die Seite „Cloud-Katalogelemente“ wird geöffnet.

Prä- oder Post-Bereitstellungsvorgänge mit Subflows einem vorlagebasierten Katalogelement hinzufügen

Sie können einen Vorgang nach der Bereitstellung mithilfe von Subflows für ein vorlagenbasiertes Katalogelement erstellen.

Vorbereitungen

- Die Anwendung Orchestration wurde installiert.

Erforderliche Rolle: Cloud-Benutzer, -Designer, -Admin, sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel fügen Sie einem vorhandenen Katalogelement, das Sie durch Erfassen einer Vorlage erstellen, einen Subflow als Prä- oder Post-Bereitstellungsvorgang hinzu.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente**an.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Prä-Bereitstellungsvorgang** oder **Post-Bereitstellungsvorgang**, und klicken Sie auf **Neu**.
3. Geben Sie im Formular die folgenden Feldwerte ein oder wählen Sie sie aus.
4. Wählen Sie in der Liste **Schritttyp** als Vorgangsschritttyp **Flow** aus.
5. Klicken Sie auf das Lupensymbol beim Feld **Flow**.
6. Wählen Sie in der Nachschlageliste **Subflow** einen aktiven Subflow aus.
   In der Suchtabelle sind alle aktiven Flows und Subflows in der Instanz aufgelistet.

   Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

7. Geben Sie im Feld **Reihenfolge** eine Reihenfolge für diesen Vorgang an.
8. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um den Vorgang zu aktivieren.
9. Klicken Sie auf **Absenden**.
   Der Schritt des Subflow-Vorgangs wird dem Katalogelement angefügt und in der zugehörigen Liste „Prä-Bereitstellungsvorgang“ oder „Post-Bereitstellungsvorgang“ angezeigt.

Nächste Maßnahme

- Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden in der zugehörigen Liste „Schlüsselwerte“ automatisch ausgefüllt.
- Klicken Sie auf den Subflow-Vorgangsschritt in der entsprechenden zugehörigen Liste, um Eingabeparameter hinzuzufügen oder zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Stellen Sie sicher, dass der Eingabeparameter `flowcorrelationid` im Subflow mit der folgenden Ausdruckszeichenfolge erstellt wird:

Schlüssel	Wert
flowcorrelationid	$(Script:CMPFlowStepHandler.generateCorrelationId)

- Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden in der zugehörigen Liste „Schlüsselwerte“ automatisch ausgefüllt.
- Erstellen Sie einen Schrittantwortprozessor. Weitere Informationen finden Sie unter Konfigurieren Sie einen Antwortprozessor .
- Erstellen Sie eine Antwortaktion für Cloud Provisioning and Governance

Katalogelement sichtbar machen

Sie können die in Cloud-Management erstellten Katalogelemente im Standardserviceportal verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu einem Cloud-Katalogelement.
2. Hinzufügen **Servicekatalog** Oder Ihren spezifischen Katalog zu **Katalogelement**an.
3. Speichern Sie es.
4. Wählen Sie Aus **Kategorien** Aus zugehörigen Listenelementen.
5. Bearbeiten Sie die Kategorien, und fügen Sie eine Kategorie aus hinzu **Servicekatalog** Oder Ihren spezifischen Katalog.
6. Besuchen Sie die Servicekatalogseite oder Ihre spezifische Katalogseite.
   Das neue Katalogelement wird angezeigt.

Variablensatz für Cloud Provisioning and Governance erstellen

Reduzieren Sie die Anzahl der erforderlichen Schritte zum Erstellen und Verwalten mehrerer Katalogelemente und Bestellleitfäden, indem Sie Variablensätze erstellen. Bei Variablensätzen müssen Sie nicht für jedes Katalogelement einzeln Variablen erstellen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Erstellen Sie eine Sammlung strukturierter Variablen, die mithilfe von Variablensätzen für mehrere Katalogelemente und Bestellleitfäden wiederverwendet werden können.

Ein neuer Variablensatz ist relevant zum Hinzufügen, wenn bestimmte Anforderungsformularvariablen für die Ausführung von Aktionen wie einer Aktion nach der Bereitstellung oder zum Sammeln zusätzlicher Informationen wie anwenderdefinierter Tags erforderlich sind.

Sie können den Variablensatz ändern, und die Änderungen werden auf alle Katalogelemente angewendet, die dem Variablensatz zugeordnet sind. Mit Variablensätzen können Sie auch Katalog-Clientskripts und UI-Richtlinien definieren, die für die Variablen im Satz gelten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie ein Katalogelement generieren, werden automatisch zwei Variablensätze (**Allgemeine Informationen** und **Bereitstellung**) erstellt. Erstellen Sie so viele Variablensätze wie nötig.

Prozedur

1. Öffnen Sie ein Cloud-Katalogelement, und klicken Sie auf der Registerkarte **Variablensätze** auf **Neu**. Der Bildschirm „Variablensatz“ wird angezeigt.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Titel	Eindeutiger Name für den Variablensatz.
Interner Name	(Eindeutiger) Name des Variablensatzes für die interne Verwendung. **Hinweis:** Wenn dieses Feld leer ist, wird sein Wert basierend auf dem Feld **Titel** für alle Variablentypen mit Ausnahme von Bruch, Containeraufteilung und Container-Ende automatisch ausgefüllt.
Layout	Für das Layout werden folgende Auswahlmöglichkeiten angezeigt: **1 Spalte breit**, **2 Spalten breit, wechselnde Seiten** oder **2 Spalten breit, eine Seite, dann die andere**.
Reihenfolge	Reihenfolgennummer für den Variablensatz.
Beschreibung	Beschreibung des Variablensatzes.

3. Klicken Sie auf **Absenden**.
   Der neue Variablensatz wird erstellt und auf der Registerkarte **Variablensätze** angezeigt. Öffnen Sie den neuen Variablensatz, und klicken Sie auf der Registerkarte **Cloud-Variablen** auf **Neu**, um Variablen für den Satz zu erstellen.

Vorgangsattribute verwalten

Sie können Attributwerte für Katalogelemente angeben, damit Cloud-Benutzer Katalogelemente ordnungsgemäß bereitstellen können. Sie können Attribute für Bereitstellungs-, Prä- und Post-Bereitstellungsvorgänge konfigurieren und verwalten.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

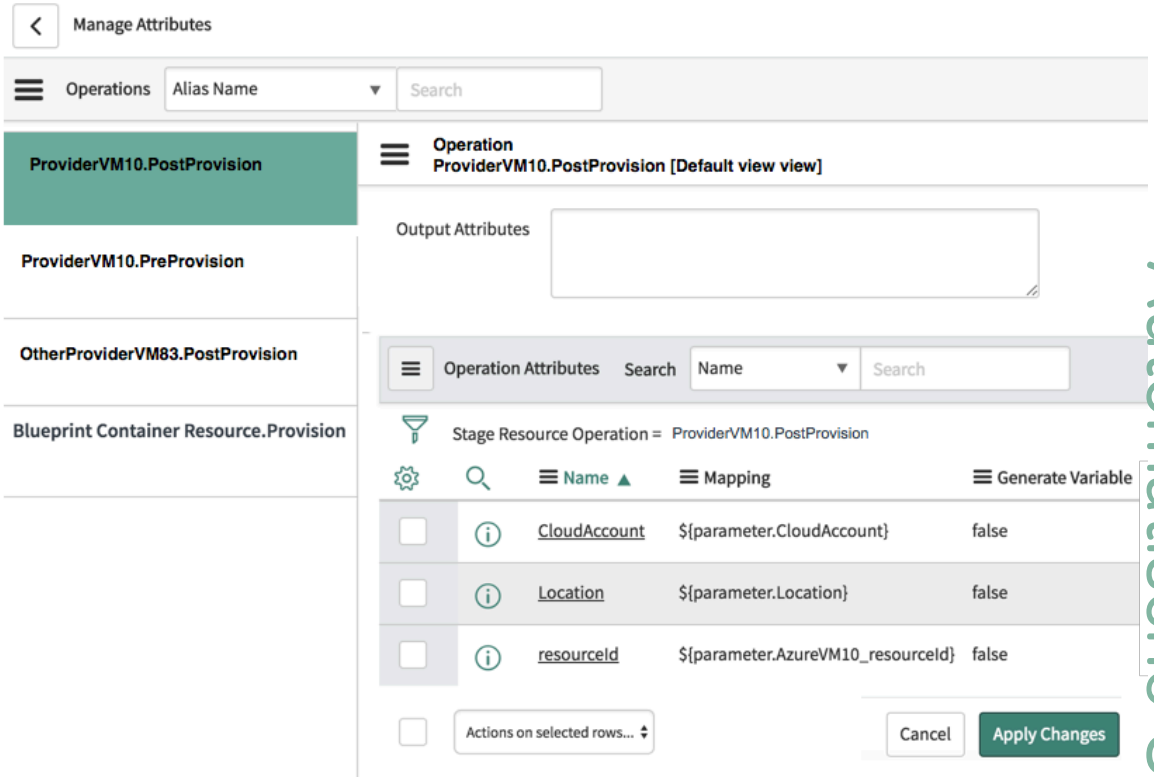
Warum und wann dieser Vorgang ausgeführt wird

Die Attribute für Bereitstellungs-, Prä- und Post-Bereitstellungsvorgänge werden automatisch generiert. Sie können Variablen für diese Attribute generieren und auch neue Attribute für den Ressourcenvorgang erstellen. Sie können auch die zugehörigen Listen „Vorgang vor der Bereitstellung“, „Post-Bereitstellungsvorgang“ und „Lebenszyklusvorgänge“ verwenden, um Variablen für Orchestration-Attribute zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente**an.
2. Öffnen Sie ein Katalogelement, und klicken Sie auf die zugehörige Liste „Vorgang vor der Bereitstellung“ oder „Post-Bereitstellungsvorgang“.
   Auf der Seite „Vorgangsschritt“ werden die Vorgänge aufgelistet.



3. Klicken Sie auf einen Vorgang, um die entsprechenden Attribute anzuzeigen.
4. Konfigurieren Sie die Attribute für jeden Vorgang.
   - **Zuordnung**: Rufen Sie die automatisch generierten Zuordnungswerte für jedes Attribut auf. Zuordnungen geben an, wo die Informationen im System abgerufen werden. Zum Ändern der Ausdruckszuordnungen doppelklicken Sie auf den Zuordnungswert und geben Sie neue Werte ein. Klicken Sie dann auf das Häkchensymbol ( ). Ausdrücke können die Werte für Informationen enthalten, die dynamisch im System generiert werden, z. B. die Werte für die Auswahlen, die Benutzer im Cloudbenutzerportal treffen. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.
   - **Variable generieren**: Generiert eine Variable für ein Attribut. Doppelklicken Sie auf den Wert (`false`), wählen Sie **Wahr** aus, und klicken Sie auf das Häkchensymbol ( ).
5. Klicken Sie auf **Änderungen übernehmen**, nachdem Sie alle erforderlichen Änderungen vorgenommen haben.
   Alle Konfigurationen, die Sie an den Attributen vorgenommen haben, werden gespeichert, und Sie kehren zum Bildschirm „Cloud-Katalogelemente“ zurück.

Cloud-Bereitstellungs-Blueprints

Eine Blaupause ist eine spezialisierte Katalogelementvorlage zum Anbieten von Cloud-Services oder Stapeln für Cloud-Benutzer. Blaupausen können mit jedem Service Provider

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für Cloud-Services verwendet werden, z. B. Amazon AWS Cloud oder Microsoft Azure Cloud. Blaupausen aus dem Orlando-Release können nur eingeschränkt verwendet werden.

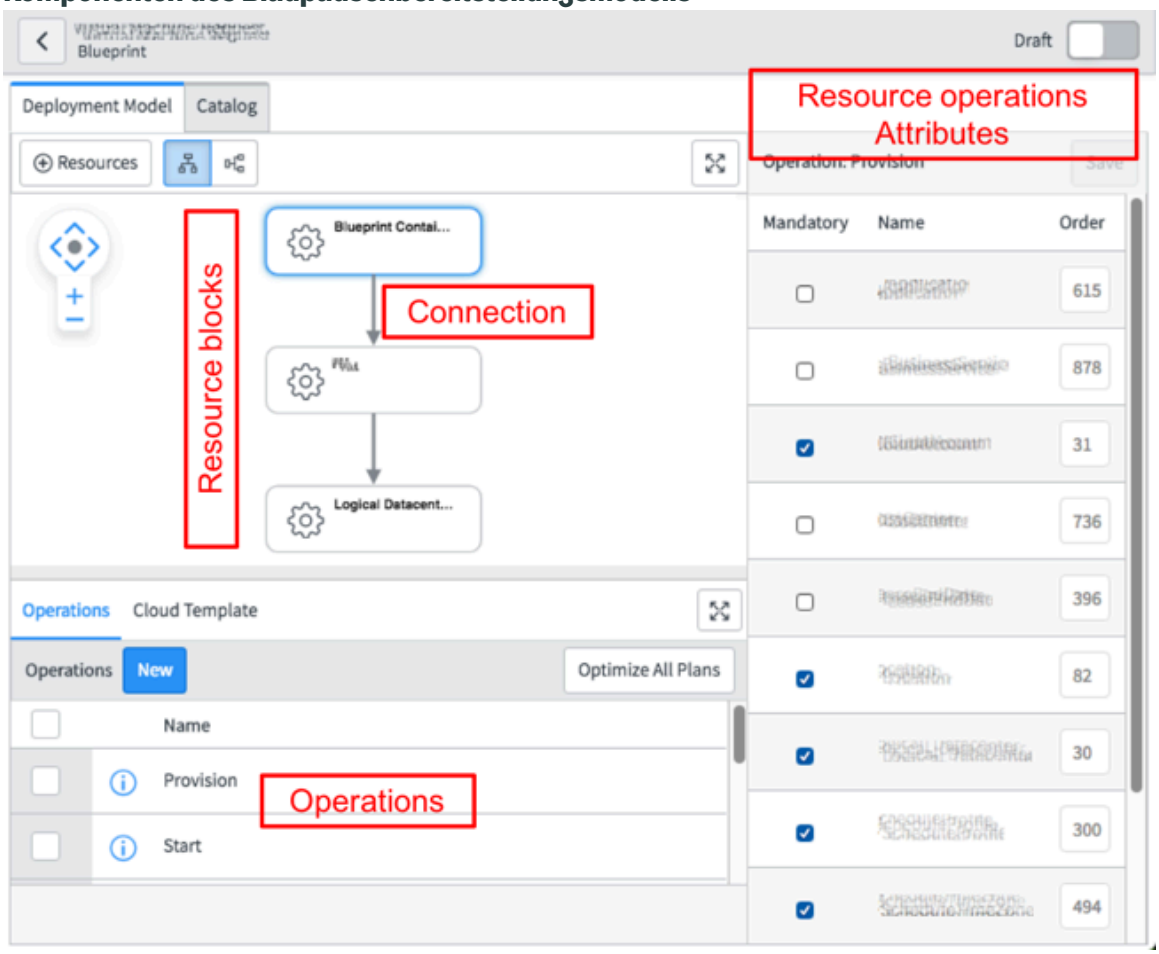
Komponenten von Blaupausen

Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Die Blaupause ist der Mechanismus, der an den Cloud-Provider übergeben wird, um die Cloud-Assets einzurichten. Das Anfordern eines Cloud-Katalogelements wird als *Starten eines Stapels* bezeichnet. Nachdem das Cloud-Asset abgerufen wurde, kann es erkannt und verwaltet werden.

Komponenten des Blaupausenbereitstellungsmodells



Ressourcenblöcke

Die in der Blaupause (Katalogelement) enthaltenen Cloud-Ressourcen. Beispielsweise kann ein Ressourcenblock einen virtuellen Computer, eine auf der VM ausgeführte App und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen über das Rechenzentrum enthalten, das die VM hostet. Auch als *Ressourcen* bezeichnet.

Verbindungen

Die Beziehung zwischen Ressourcen. Beispielsweise hat die VM eine Hostbeziehung mit der App. Es gibt zwei Arten von Verbindungen: *Einschluss* und *Angehängt*.

- Einschluss: Eine Verbindung, bei der der Ressourcenblock einen weiteren enthält. Diese Beziehung wird visuell als Beziehung von oben nach unten dargestellt, wie im Bild gezeigt. Beispielsweise muss der Blaupausencontainer mindestens einen weiteren Ressourcenblock enthalten.
- Angehängt: Eine Verbindung zwischen Ressourcen, die eine Bindung für die direkte Kommunikation untereinander erfordern. Die Beziehung wird visuell nebeneinander dargestellt. Beispielsweise stellt die Bindung zwischen einem virtuellen Computer und einem Speicher eine Angehängt-Beziehung dar.

Betrieb

Die Aktionen, die an Ressourcenblöcken oder am Ressourcenstapel ausgeführt werden, um die Ressourcen zu verwalten. Beispielsweise kann der Cloud-Benutzer eine Ressource bereitstellen, starten und stoppen.

Ressourcenvorgänge

Die Schritte zum Ausführen des Vorgangs für die Ressource. Um beispielsweise das Katalogelement bereitzustellen, muss das System die VM und die darauf ausgeführte App bereitstellen. Klicken Sie auf einen Vorgang, um Detailinformationen für die Ressourcenvorgänge anzuzeigen.

Attribute

Die Details der Ressource. Attribute können im Katalogelementformular als Katalogeigenschaften angezeigt werden. Beispielsweise kann die Blaupause die Version der App bereitstellen, die für die VM bereitgestellt werden soll.

Einschränkungen

Eine Attributoption zur Einschränkung eines cloudunabhängigen Ressourcenblocks, z. B. eines logischen Rechenzentrums, zur Verwendung mit einem bestimmten Cloud-Provider. Beispielsweise kann ein logisches Rechenzentrum auf Amazon AWS Cloud beschränkt werden. Wenn Sie später zu Microsoft Azure Cloud oder einem anderen Cloud-Provider wechseln oder einen solchen hinzufügen, können Sie die Einschränkung nach Bedarf ändern.

Planungsblaupausen

Planen Sie vor dem Erstellen von Blaupausen die Stapel, die Sie im Servicekatalog anbieten möchten. Bereiten Sie die folgenden Informationen vor, bevor Sie mit der Entwicklung beginnen.

Ressourcenblöcke

Planen Sie die Ressourcenblöcke, die Sie in Blaupausen verwenden möchten. Stellen Sie sicher, dass die entsprechenden Ressourcenblöcke für die Verwendung in Blaupausen verfügbar sind, und fügen Sie sie bei Bedarf hinzu.

Serviceangebote (Stapel)

Zum Planen eines Serviceangebots oder Stapel stellen Sie die benötigten Ressourcenblöcke und deren Verbindungen grafisch dar.

Cloud-Konten und Rechenzentren

Rufen Sie eine Liste der Cloud-Konten und Rechenzentren ab, die der Cloud-Administrator konfiguriert hat. Stellen Sie fest, ob welche eingeschränkt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekatalogvariablen und -variablensätze

Stellen Sie sicher, dass Sie wissen, wie Servicekatalogelemente Variablen und Variablensätze verwenden. Das Verständnis von Servicekatalogelementen und -prozessen hilft Ihnen, Blaupausen besser zu verstehen.

Beginnen Sie hier

Cloud Provisioning-Blaupause erstellen

Cloud Provisioning-Blaupause erstellen

Verwenden Sie den Blaupausendesigner, um benutzerdefinierte Blaupausen für die Cloud Provisioning and Governance-Anwendung zu erstellen. Blaupausen sind im Orlando-Release veraltet.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

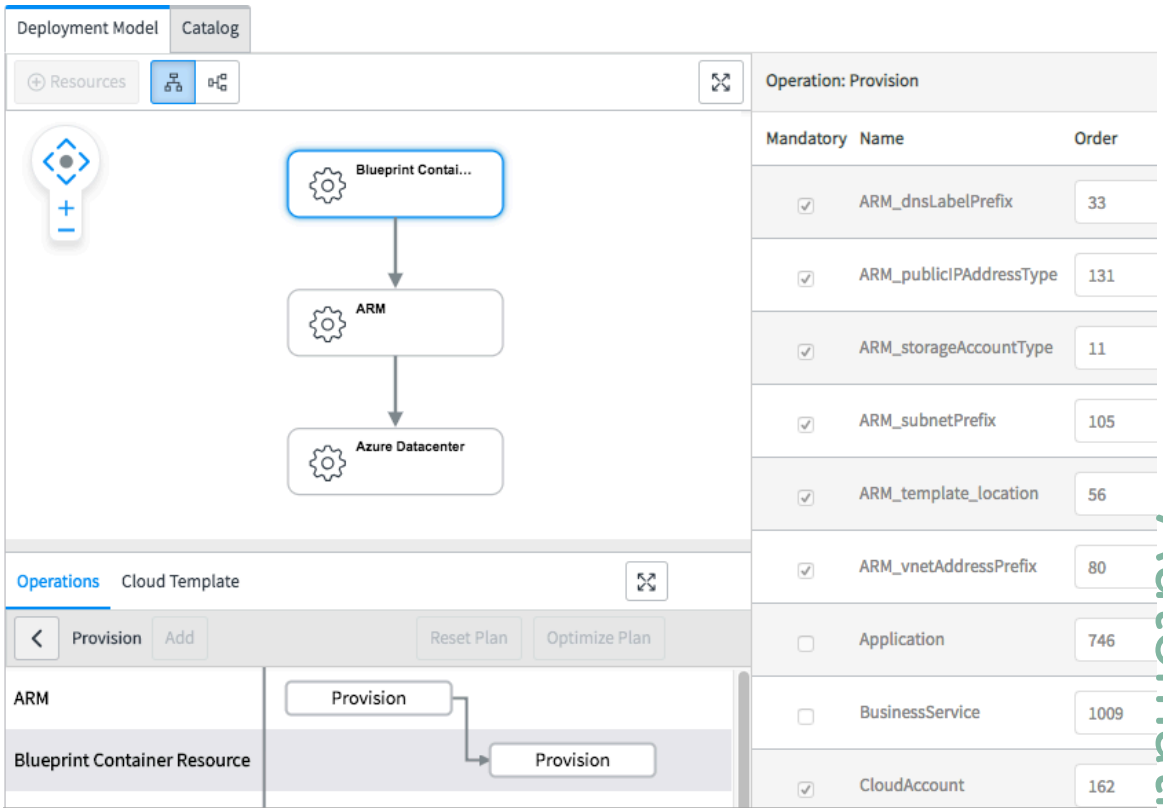
Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Blueprints**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und geben Sie die **Kategorie** des Service an.
   Standardmäßig werden mehrere Kategorien bereitgestellt.
3. Klicken Sie auf **Absenden**.
   Das System erstellt den Blaupausendatensatz und zeigt die Registerkarte „Bereitstellungsmodell“ des Blaupausendesigners an. Die Registerkarte „Bereitstellungsmodell“ ist eine visuelle Canvas, auf der Sie Ressourcenblöcke ablegen. Jeder Ressourcenblock stellt ein CI in einem mehrschichtigen Anwendungsstapel dar. Das Bereitstellungsmodell gibt die Ressourcen und Verbindungen zwischen Ressourcen für die Cloud-Elemente an, die Sie definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zum Hinzufügen einer Ressource zum Bereitstellungsmodell klicken Sie auf **Ressourcen**, und wählen Sie die Ressource aus der Liste aus.
   Die Ressourcen werden auf der Canvas angezeigt. Verschieben Sie die Ressource an eine für das gewünschte Modell geeignete Stelle. Fügen Sie beliebig viele Ressourcen hinzu.
5. Verbinden Sie die Containerressource mit der ersten Ressource, die bereitgestellt werden soll.
   Zum Erstellen einer Verbindung zwischen Ressourcen wählen Sie die übergeordnete Ressource aus, klicken auf das Verbindungsfeld in der Ressource und legen die Verbindung in einer Ressource mit einer gepunkteten Kontur ab. Das System lässt bestimmte Verbindungen nicht zu (z. B. kann ein AWS-Rechenzentrum keine ARM-Ressource hosten).
6. Fügen Sie alle Ressourcen hinzu, die die Blaupause bilden, und verbinden Sie sie.
   Sie müssen alle Ressourcen hinzufügen und verbinden, bevor Sie Vorgänge und Attribute im Abschnitt **Vorgänge** konfigurieren. Während Sie die Ressourcen auf der Registerkarte „Bereitstellungsmodell“ aktualisieren, generiert das System die Cloud-Vorlage: eine vollständige Darstellung der Blaupause als YAML-Skript. Sie können die Darstellung der Cloud-Vorlage für das Bereitstellungsmodell exportieren und später in die Cloud Provisioning and Governance-Anwendung auf einer anderen Instanz importieren.
7. Konfigurieren Sie die Vorgänge, die das System für die Ressourcen durchführt, und die während der Vorgänge zu verwendenden Attribute.
   Standardmäßig werden die Vorgänge **Bereitstellung**, **Stoppen**, **Starten** und **Bereitstellung aufheben** bereitgestellt. Sie können entweder einen vorhandenen Vorgang auswählen oder einen neuen Blaupausenvorgang erstellen.
   - Wählen Sie einen bestehenden Vorgang aus: Wählen Sie im Abschnitt **Vorgänge** das Kontrollkästchen **Bereitstellung** für den Vorgang aus, und klicken Sie auf **Bereitstellung**, um ein Diagramm anzuzeigen. Sie können das Diagramm neu anordnen, indem Sie Vorgänge löschen und hinzufügen. Sie können für die Cloud Provisioning and Governance-Anwendung auf **Alle Pläne optimieren** klicken, um einen für Sie optimierten Vorschlag für einen Plan zu erhalten. Die Cloud Provisioning and Governance-Anwendung untersucht die von Ihnen erstellte Blaupause und schlägt basierend auf den Attributen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungen und Abhängigkeiten der einzelnen Ressourcen einen optimierten Plan zur Ausführung vor. Alle Attribute für den Vorgang **Bereitstellung** werden im Fenster angezeigt. Sie können beliebige Attribute aktivieren oder deaktivieren. Nach der Konfiguration des Vorgangs **Bereitstellung** können Sie den nächsten Vorgang auswählen und seine Attribute nach Bedarf konfigurieren.

- Erstellen Sie einen neuen Blaupausenvorgang: Klicken Sie im Abschnitt **Vorgänge** auf **Neu**. Das Dialogfeld „Neuer Blaupausenvorgang“ wird angezeigt. Geben Sie einen Namen ein, wählen Sie einen Vorgangstyp aus, geben Sie Eingabeparameter für den neuen Vorgang ein, und klicken Sie auf **Speichern**. Der neue Blaupausenvorgang wird im Abschnitt **Vorgänge** angezeigt.

8. Wenn Sie den Entwurf der Blaupause abgeschlossen haben und sie nicht weiter konfigurieren möchten, klicken Sie auf den Umschalter **Entwurf**, um den Plan zu veröffentlichen.
   Eine Nachricht weist darauf hin, dass Ihre Blaupause veröffentlicht wurde. Um mit der Konfiguration der Blaupause fortzufahren, überspringen Sie diesen Schritt.
9. Zum Konfigurieren von Parametern wie Variablensätzen, Regeln und Lebenszyklusvorgängen für das Blaupausenkatalogelement klicken Sie auf die Registerkarte **Katalog** und dann auf den Katalog.
   Der Bildschirm „Cloud-Katalogelement“ wird angezeigt.
10. Klicken Sie auf **Aktualisieren**, wenn Sie Änderungen am Formular vorgenommen haben.
11. Klicken Sie auf **Veröffentlichen**, um die Blaupause zu veröffentlichen.
    Zum Anzeigen aller veröffentlichten Katalogelemente klicken Sie auf der Zielseite der Blaupausen auf **Veröffentlicht**.

Ausführungsplan einen Ressourcenvorgang hinzufügen

Das Basissystem enthält eine große Anzahl vordefinierter Ressourcenvorgänge. In seltenen Fällen können Sie einen benutzerdefinierten Vorgang für eine Ressource hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Klicken Sie im Blaupause-Designer auf die Registerkarte **Vorgänge**, und wählen Sie den entsprechenden Blaupausenvorgang aus.
   Beispielsweise können Sie den Vorgang **Bereitstellung** auswählen.
2. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld „Ressourcenvorgang hinzufügen“ wird angezeigt.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Ressource	Wählen Sie eine Ressource für den auszuführenden Vorgang aus.
Schnittstelle	Wählen Sie eine Schnittstelle für die Ressource aus.
Vorgang	Wählen Sie den für den Schritt auszuführenden Vorgang aus. Standardmäßig werden die Vorgänge **Bereitstellung**, **Stoppen**, **Starten** und **Bereitstellung aufheben** bereitgestellt. Sie benötigen mindestens einen Bereitstellungsvorgang, damit ein Benutzer ein Cloud-Katalogelement bestellen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Der neue Vorgang wird dem Vorgangsdiagramm hinzugefügt. Das System fügt die entsprechenden Parameter für den Vorgang hinzu.
5. Klicken Sie auf das Kontrollkästchen **Formularparameter erstellen**, um einen Parameter auszuwählen. Die Parameter unterscheiden sich je nach Vorgang. Geben Sie einen Zuordnungsausdruck für den ausgewählten Parameter in das Feld **Zuordnung** ein. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.
6. Klicken Sie auf **Speichern**.

Blaupausenvorgänge parallel ausführen

Sie können Ihre Blaupausenressourcenvorgänge linear oder parallel ausführen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig werden die Vorgänge für Blaupausenressourcen seriell aufgeführt und folgen einer Reihenfolge. Sie können Vorgänge parallel ausführen, indem Sie sie in Verzweigungen anordnen. Identifizieren Sie die in einer Blaupause angegebenen Vorgänge, die keine Abhängigkeiten aufweisen und parallel ausgeführt werden können. Ordnen Sie solche Vorgänge in einer einzelnen Verzweigung an. Der Blaupausendesigner führt diese Vorgänge gemeinsam aus. Wenn in einer Verzweigung ein Fehler auftritt, werden die Vorgänge in der betroffenen Verzweigung nicht mehr ausgeführt. Die Vorgänge in den anderen Verzweigungen, die nicht vom Fehler betroffen sind, werden jedoch weiterhin ausgeführt. Die parallele Art der Ausführung von Vorgängen verkürzt somit die Zeit in Bereitstellungsstapel.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Blueprints**an.
2. Klicken Sie auf eine Blaupause, klicken Sie auf die Registerkarte **Modell zur Bereitstellung** und klicken Sie dann auf **Vorgänge**.
   Alle Vorgänge für die Blaupause werden aufgelistet.
3. Klicken Sie auf einen Vorgang, um ein Diagramm anzuzeigen.
   Sie können das Diagramm neu anordnen, indem Sie Vorgänge löschen und hinzufügen.
4. Sie können für die Cloud Provisioning and Governance-Anwendung auf **Plan optimieren** klicken, um einen für Sie optimierten Vorschlag für einen Plan zu erhalten.
   Die Cloud Provisioning and Governance Die Anwendung betrachtet den von Ihnen erstellten Blueprint, und basierend auf den Attributen, den Zuordnungen und den Abhängigkeiten der einzelnen Ressourcen schlägt die Anwendung einen optimierten Plan zur Ausführung vor.

Blaupausenattribute

Wenn Sie einer Ressource einen Blaupausenvorgang hinzufügen, fügt das System die entsprechenden Attribute hinzu. Sie können festlegen, ob die Attribute als Katalogeigenschaften im Formular verfügbar gemacht werden sollen, wenn das System den Vorgang ausführt.

Allgemeine Attribute für den Bereitstellungsvorgang für virtuelle Computer

Attribut	Beschreibung
VmFolderName	Name des Ordners des virtuellen Computers.
ResourceGroupName	Der Name der Ressourcengruppe, zu dem die Ressource gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribut	Beschreibung
StackName	Der Name des Stapels, den der Benutzer bereitstellt.
CloudAccount	Das Cloud-Konto, zu dem der Ressourcenstapel gehört.
OSProfile	Das Ressourcenprofil, in diesem Fall das Betriebssystemprofil, auf dem die Cloud-Ressource basiert.
DiscoverAndAttachIP	Sucht nach einer freien elastischen IP-Adresse und weist sie einem virtuellen Computer in AWS zu. Wenn eine VM auf einer VPC in AWS bereitgestellt wird, erhält sie standardmäßig keine öffentliche IP. Wenn keine elastischen IPs verfügbar sind, kann der VM keine IP zugewiesen werden.

⚠ **Warnung:** Es wird empfohlen, `KeyPreference` nicht zu verwenden. Wenn Sie das Attribut verwenden, setzen Sie `KeyPreference` nicht auf Benutzer.

Blaupausenregel konfigurieren

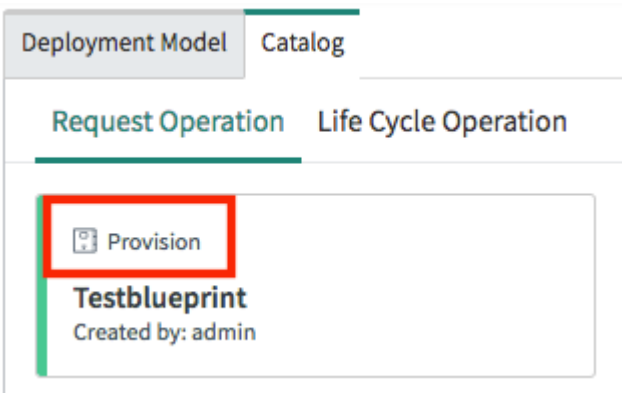
Konfigurieren Sie eine Regel, die Aktionen enthält, die das System für Blaupausenattribute durchführen kann.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Öffnen Sie eine Blaupause, die das Attribut enthält, für das Sie eine Regel erstellen möchten.
2. Klicken Sie auf der Registerkarte **Katalog** auf den Vorgang, der das Attribut enthält, z. B. den Bereitstellungsvorgang.



3. Klicken Sie in der zugehörigen Liste „Variablensätze“ im Formular „Cloud-Katalogelement“ auf den Namen des Variablensatzes, der die Variable enthält.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf den Namen der Variable, für die Sie eine Regel erstellen möchten.
5. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Geben Sie einen Namen und eine Beschreibung ein.
Beschreibung	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

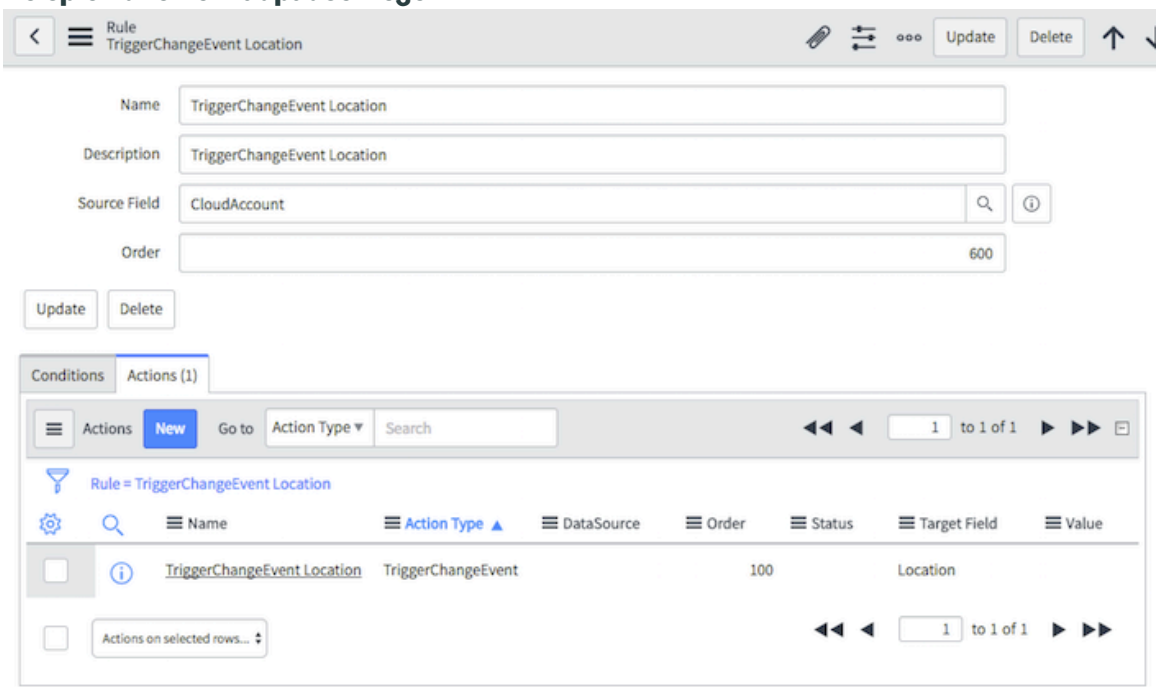
Feld	Beschreibung
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Example:

Diese Beispielregel basiert auf der Eigenschaft `CloudAccount` und enthält eine Aktion, die das System anweist, die Liste der Standorte zu aktualisieren, wenn der Benutzer das Cloud-Konto ändert.

Beispiel für eine Blaupausenregel



Nächste Maßnahme

Konfigurieren Sie eine optionale Bedingung und eine obligatorische Aktion.

Blaupausenregelbedingung konfigurieren

Konfigurieren Sie die Bedingung für eine Eventregel eines Blaupausenformulars, die bestimmt, wann die Aktionen in der Regel ausgeführt werden können. Bedingungen sind optional.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Öffnen Sie eine Regel für eine Variable in einer Blaupause.
2. Klicken Sie in der zugehörigen Liste „Bedingungen“ auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

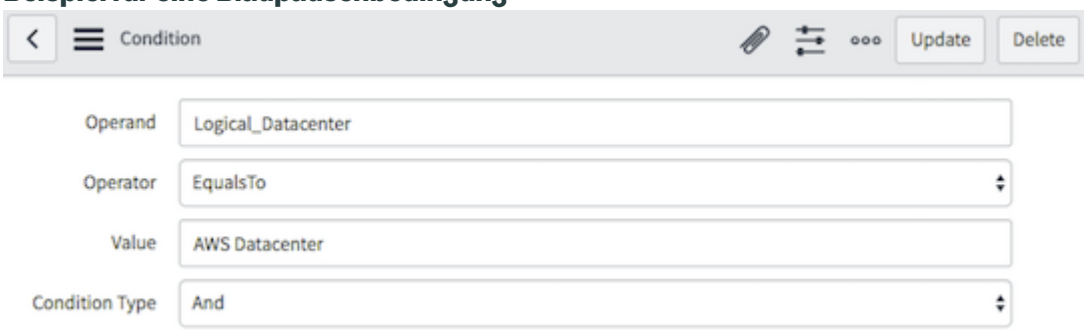
Feld	Beschreibung
Operand	Geben Sie die Eigenschaft ein, für die Sie die Bedingungsauswertung durchführen können. Beispiel: Wenn Ihre Blaupause über eine Eigenschaft verfügt, die den Wert eines Rechenzentrums enthält, geben Sie den Namen der Eigenschaft hier ein.
Operator	Wählen Sie einen Operator aus, der den Operanden auswertet.
Wert	Geben Sie einen Wert ein, dem die ausgewertete Eventregel entsprechen muss.
Bedingungstyp	Wenn Sie mehrere Bedingungen konfigurieren, wählen Sie den logischen Operator aus, der bestimmt, wie das System die Bedingung in Bezug auf die nächste Bedingung auswertet (die nächste Bedingung wird durch das Feld **Auftrag** bestimmt): ○ **UND**: Diese Bedingung muss die nächste Bedingung erfüllen, bevor die Richtlinie ausgeführt werden kann. ○ **ODER** : Diese Bedingung oder die nächste Bedingung, die den Kriterien entspricht, kann die Ausführung der Richtlinie ermöglichen. Wenn Sie keine Option auswählen, wird **UND** standardmäßig verwendet.
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.
Status	Behalten Sie den Status „Aktiv“ bei, damit die Bedingung vom System verarbeitet wird. Ändern Sie den Status in „Inaktiv“, wenn Sie nicht möchten, dass das System die Bedingung verarbeitet.

4. Klicken Sie auf **Absenden**.

Example:

Diese Beispielbedingung gilt, wenn der Benutzer das AWS-Rechenzentrum für die Eigenschaft „Logical_Datacenter“ auswählt, die ein Feld im Katalogelementformular ist:

Beispiel für eine Blaupausenbedingung



Nächste Maßnahme

Blaupausenaktion konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Blaupausenaktion konfigurieren

Konfigurieren Sie Aktionen, die das System ausführt, wenn Attributaktionen von Blaupausenformularen oder Eventaktionen ausgelöst werden. Sie können Aktionen konfigurieren, z. B. ein Feld als Pflichtfeld festlegen, ein Feld anzeigen oder ausblenden oder ein Feld automatisch ausfüllen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Öffnen Sie eine Regel für eine Eigenschaft oder ein Ereignis in einer Blaupause.
2. Klicken Sie in der zugehörigen Liste **Aktionen** auf **Neu**, und füllen Sie das Formular aus.

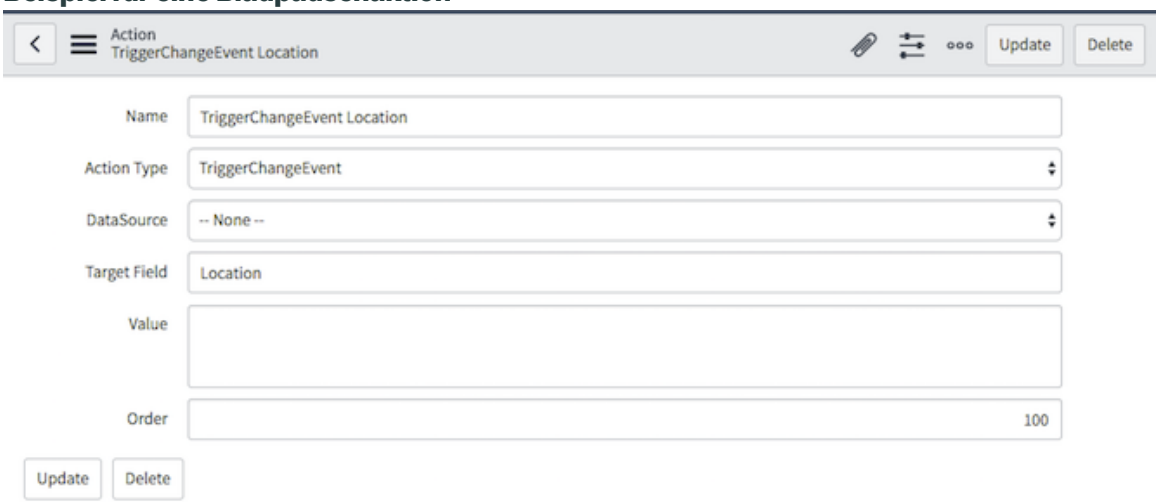
Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name.
Aktionstyp	Wählen Sie einen Aktionstyp aus: ○ **Neu laden**: ○ **Anzeigen**: ○ **Ausblenden**: ○ **MakeMandatory**: ○ **MakeNonMandatory**: ○ **TriggerChangeEvent**: ○ **SetValue**:
Datenquelle	Wählen Sie einen Aktionstyp aus: ○ **Cloud-Konto neu laden**: ○ **Cloud-Standort neu laden**: ○ **Kontingent prüfen**: ○ **Ressourcenprofil neu laden**: ○ **Aus Profil neu laden**:
Zielfeld	Geben Sie den Namen des Felds im Formular ein, für das die Aktion gilt. Wenn Sie beispielsweise **TriggerChangeEvent** für den Aktionstyp ausgewählt haben und sich im Formular etwas ändert, ändert sich der Wert des Feldes, wie in der Blaupausenregel angegeben.
Wert	Geben Sie einen optionalen Wert ein, den Sie dem Zielfeld zuweisen möchten. Wenn Sie beispielsweise **SetValue** für das Feld **Aktionstyp** ausgewählt haben und den **Ressourcengruppennamen** aktualisieren möchten, können Sie den Wert `${ResourceGroup}` verwenden, der die Namen der Ressourcengruppen aus der Blaupause abruft.
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
4. **Wahlweise:** Geben Sie einen **Schlüssel** und **Wert** in die zugehörige Liste „KeyValues“ ein.
   Der Wert im Feld **Wert** wird auf das Attribut im Feld **Schlüssel** angewendet.
5. Erstellen Sie so viele Aktionen wie nötig.

Example:
Diese Beispielaktion gilt für das Beispiel einer Blaupausenregel, das auf dem Attribut „CloudAccount“ basiert. Diese Aktion weist das System an, die Liste der Standorte zu aktualisieren, wenn der Benutzer das Cloud-Konto ändert.

Beispiel für eine Blaupausenaktion



Nächste Maßnahme
Veröffentlichen Sie einen Blueprint als Cloud-Katalogelement.

Formularkonfiguration mit Blaupausen

Blaupausen steuern, was dem Benutzer auf dem Katalogbestellformular angezeigt wird. Sie können das Formular so konfigurieren, dass Felder ein- oder ausgeblendet werden, Felder mit Standardwerten ausgefüllt werden und andernfalls basierend auf Kriterien ein eindeutiges Formular für den Benutzer erstellt wird.

Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Sie können außerdem die Werte in Formularfeldern mithilfe von Richtlinien ändern. Beispiele finden Sie unter Cloud-Richtlinie erstellen und Richtlinienaktionsskript erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten der Blaupausenformularkonfiguration

Blaupausen verwenden diese Komponenten, um zu steuern, wie das System Katalogformularfelder verwendet:

- *Katalogvariablen* definieren die grundlegende Struktur jedes Felds in Katalogbestellformularen.
- *Regeln* geben eine Aktion an, die das System für ein Feld ausführt, wenn eine Bedingung erfüllt ist.
- *Skripts* fragen Informationen aus dem System ab, die Sie benötigen, um den Kataloganforderer anzuzeigen, Formularfelder auszufüllen und die von Benutzern übermittelten Daten zu verarbeiten.
- *UI-Gruppen* fassen zugehörige Felder auf einer Registerkarte zusammen. Benutzer können Registerkarten durchlaufen, um alle Formularfelder auszufüllen.

Beginnen Sie hier

Diese Aufgaben zeigen Ihnen die Grundlagen der Formularkonfiguration mit Blaupausen:

- Bestellformular für Cloud-Katalogelement Felder hinzufügen
- Standardwerte für die Sichtbarkeit von Cloud-Katalogelementen steuern
- Variablensatz für Cloud Provisioning and Governance erstellen

Beispiele

Diese Beispiele führen Sie durch die Formularkonfiguration basierend auf einem bestimmten Ziel: Konfigurationsbeispiele für das Cloud-Katalogformular.

Bestellformular für Cloud-Katalogelement Felder hinzufügen

Sie können einem Cloud-Katalogformular Felder hinzufügen, wenn der Anwender zusätzliche Informationen eingeben soll, die über die Bereitstellung eines Standard-Blueprints hinausgehen.

Vorbereitungen

- Sie benötigen eine Blaupause, die Sie im Katalog veröffentlicht haben. Die Blaupause sollte im Entwurfsstatus vorliegen. Lesen Sie Cloud Provisioning-Blaupause erstellen, wenn Sie diese Voraussetzung nicht erfüllt haben.
- Standardmäßig werden Cloud-Elemente im Cloud-Katalog anstatt im Standardservicekatalog Ihrer Instanz angezeigt. Blaupausen verwenden jedoch mehrere Funktionen aus dem Standardservicekatalog. Es wird empfohlen, sich mit der Funktionsweise des Servicekatalogs vertraut zu machen. Informationen zu den ersten Schritten finden Sie unter Servicekatalog .
- Erforderliche Rolle: sn_cmp.cloud_service_designer

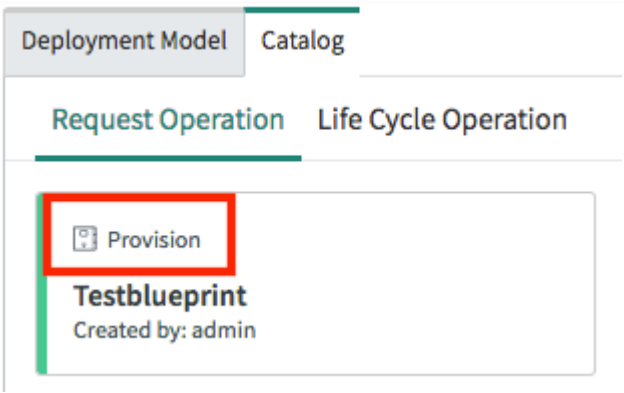
Warum und wann dieser Vorgang ausgeführt wird

Felder werden in Blaupausen als Variablen dargestellt. Zum Hinzufügen eines Felds fügen Sie einem Vorgang in einer Blaupause eine Variable hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie eine Blaupause, die Sie bereits erstellt haben.
2. Klicken Sie auf die Registerkarte **Katalog**, und klicken Sie dann auf den Vorgang, dem Sie die Variable hinzufügen möchten, z. B. Bereitstellung.



Das Formular „Cloud-Katalogelement“ wird geöffnet.

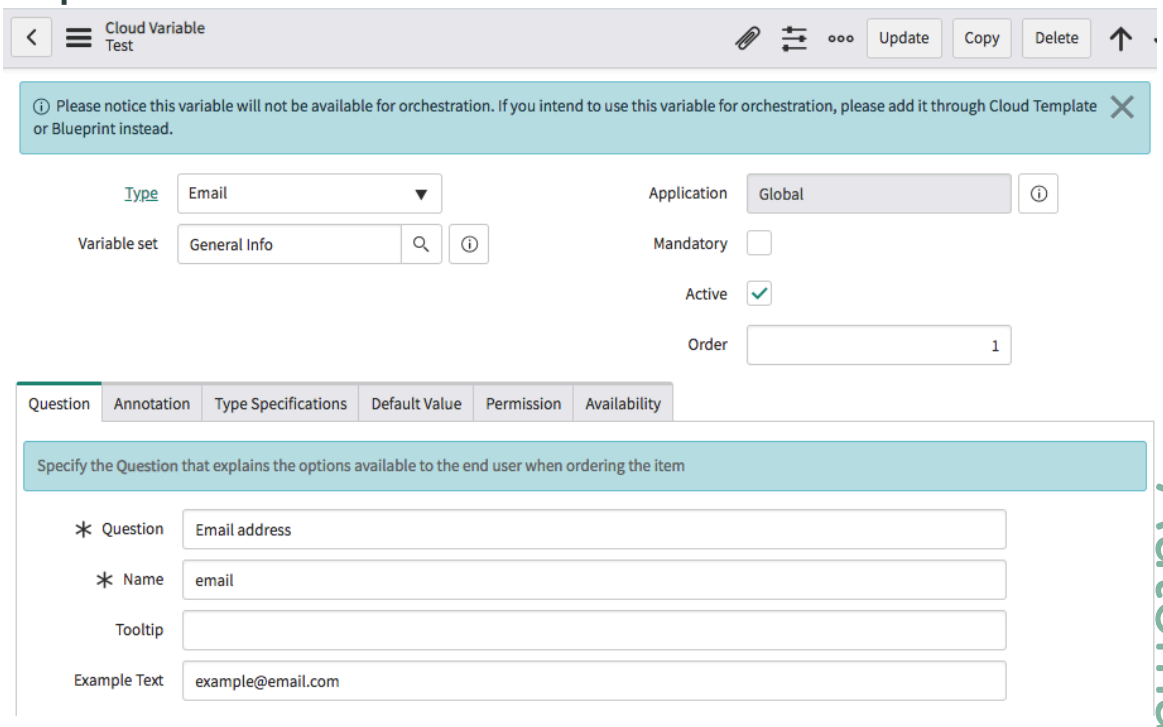
3. Klicken Sie in der zugehörigen Liste „Variablensätze“ unten auf den Satz, zu dem die Variable gehören soll. Klicken Sie beispielsweise auf „Allgemeine Informationen“, ein Standardvariablensatz für alle Blaupausen, damit das Feld auf der ersten Registerkarte des Katalogbestellformulars angezeigt wird.
Das Formular „Variablensatz“ wird geöffnet.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ unten auf **Neu**.
5. Füllen Sie die wichtigen Formularfelder aus, z. B.:

Feld	Beschreibung
Typ	Wählen Sie den Typ der Variable aus, z. B. **Einzeiliger Text** für ein Textfeld, **Kontrollkästchen** oder **Datum**.
Registerkarte „Frage“	Geben Sie unter **Frage** einen Namen ein. Dies ist der Wert, den der Benutzer auf dem Katalogbestellformular für das Feld sieht. Das Feld **Name**, das der tatsächliche Name der Variable ist, wird automatisch mit dem gleichen Wert in Kleinbuchstaben ausgefüllt.
Andere Registerkarten	Füllen Sie andere Felder auf den verbleibenden Registerkarten aus, um die Sichtbarkeit des Felds, den Formularhilfetext, den Standardwert und die Zugriffsrechte zu steuern.

Hinweis: Diese Variable ist nicht für die Orchestrierung verfügbar. Wenn Sie diese Variable für die Orchestrierung verwenden möchten, fügen Sie sie stattdessen über Cloud-Vorlage oder Blaupause hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielvariable für eine E-Mail-Adresse

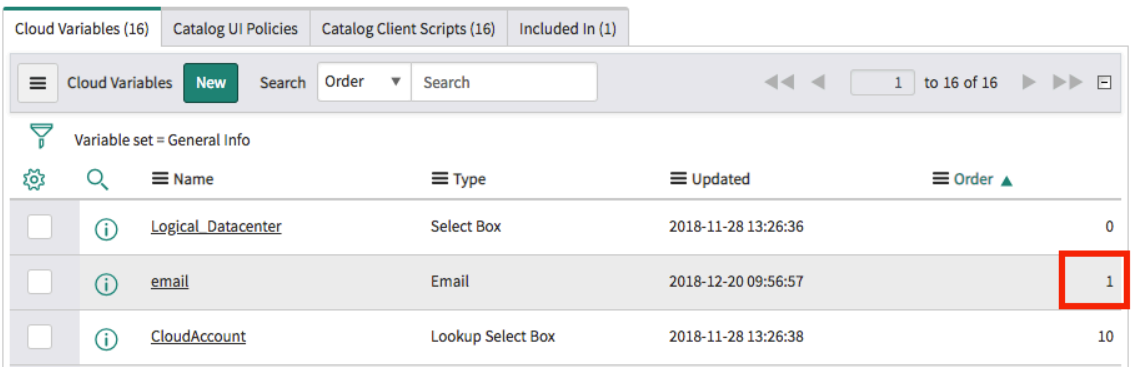


6. Klicken Sie auf **Absenden**.

   Das Formular „Variablensatz“ wird geöffnet und zeigt die neue Variable in der zugehörigen Liste „Cloud-Variablen“ an.

7. Ändern Sie den Wert in der Spalte **Reihenfolge**, um die Position des Felds auf dem Formular zu steuern.

   Hinweis: Ein niedrigerer Wert für die Reihenfolge verschiebt das Feld im Formular nach oben und umgekehrt.

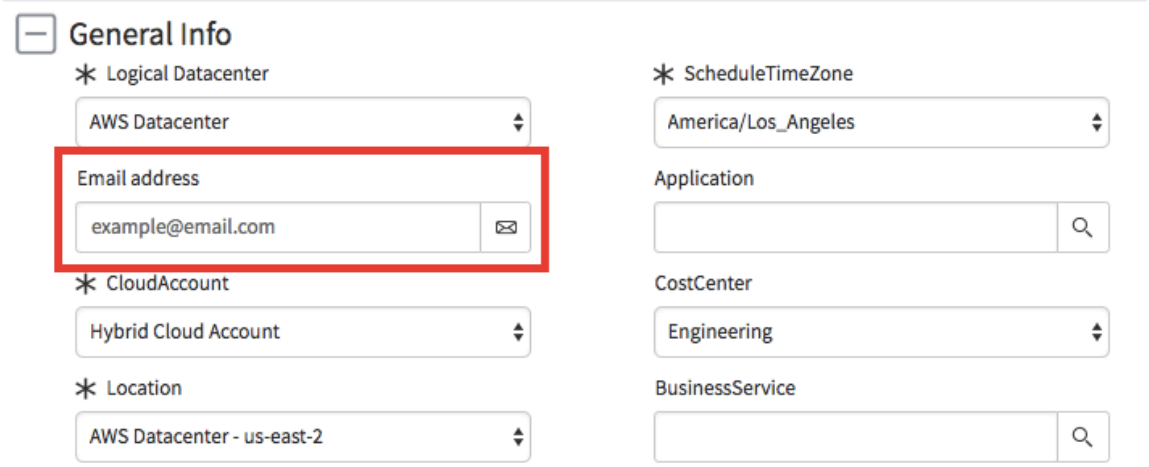


   In diesem Beispiel ist die Reihenfolge auf **1** festgelegt, was bedeutet, dass das Feld „E-Mail-Adresse“ nach dem Feld „Logisches Rechenzentrum“ und vor dem Feld „Cloud-Konto“ angezeigt wird.

8. Klicken Sie im Formularbanner oben links auf **Testen**, um sich eine Vorschau des Bestellformulars anzusehen, wie es einem Benutzer im Cloud-Katalog angezeigt würde.
   Das Formular wird mit dem von Ihnen erstellten neuen Feld angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie oben links im Formular auf den Zurück-Pfeil.
10. Schalten Sie das Katalogelement auf **Veröffentlichen** um.

Standardwerte für die Sichtbarkeit von Cloud-Katalogelementen steuern

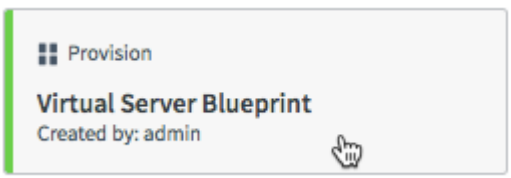
Mithilfe von Blaupausen können Sie steuern, wie Formularfelder Benutzern im Cloud-Katalog angezeigt werden. Beispielsweise können Sie steuern, wo die Felder Benutzern im Katalogelementformular angezeigt werden und ob sie schreibgeschützt oder obligatorisch sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die zu ändernde Blaupause, und schalten Sie sie von **Veröffentlicht** auf **Entwurf** um.
2. Klicken Sie auf die Registerkarte **Katalog**.
   Die Unterregisterkarte „Anforderungsvorgang“ wird geöffnet und zeigt die veröffentlichten Katalogelemente für den Bereitstellungsvorgang an.
3. Klicken Sie auf die Kachel **Bereitstellung** für das Katalogelement.
   Die Einstellungen im Bereitstellungsvorgang steuern das Formular, das dem Benutzer bei der ersten Anforderung des Elements angezeigt wird, bevor es bereitgestellt wird.



   Das Formular „Cloud-Katalogelement“ wird geöffnet.
4. Klicken Sie in der zugehörigen Liste „Variablensätze“ unten auf den Satz, zu dem die Variable gehören soll.
   Klicken Sie beispielsweise auf **Allgemeine Informationen** , Eine Standardvariable, die für alle Blueprints festgelegt ist, damit das Feld auf der ersten Registerkarte des Katalogauftragsformulars angezeigt wird.
5. Wählen Sie im Formular „Variablensatz“ die Variable aus, die Sie ändern möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Führen Sie im Formular „Cloud-Variable“ eine der folgenden Aktionen aus.

An	Aktion
Feld zum Pflichtfeld machen	Markieren Sie die Checkbox **Pflichtfeld**. Entfernen Sie das Häkchen aus dem Kontrollkästchen, um das Feld optional zu machen.
Feld schreibgeschützt machen	Klicken Sie auf die Registerkarte **Verfügbarkeit**, und aktivieren Sie dann das Kontrollkästchen **Schreibgeschützt**. Entfernen Sie das Häkchen aus dem Kontrollkästchen, um das Feld bearbeitbar zu machen. Verwenden Sie diese Option, um automatisch einen Wert im Feld auszufüllen, den der Benutzer nicht ändern kann.
Feld ein- oder ausblenden	Klicken Sie auf die Registerkarte **Verfügbarkeit**, und aktivieren Sie dann das Kontrollkästchen **Sichtbar**.
Feld auf eine andere Registerkarte verschieben	Wählen Sie einen anderen **Variablensatz** aus. **Allgemeine Informationen** und **Bereitstellung** werden im Basissystem bereitgestellt, und Sie können zusätzliche Formular-UI-Gruppen konfigurieren. Informationen zum Hinzufügen einer neuen Registerkarte für die Organisation von Feldern im Katalogelement finden Sie unter Variablensatz für Cloud Provisioning and Governance erstellen.
Standardwert festlegen	Klicken Sie auf die Registerkarte **Standardwert**, und geben Sie den Wert unter **Standardwert** ein. Wenn das Feld nicht schreibgeschützt ist, können Benutzer den Wert im Cloud-Katalogformular ändern. Referenzfelder müssen die Sys-ID des Datensatzes verwenden, der den Standardwert darstellt.
Hilfe für den Benutzer hinzufügen	Führen Sie einen der folgenden Schritte aus: ○ Klicken Sie auf die Registerkarte **Frage**, und fügen Sie im Feld **Tooltip** einen Wert hinzu, um eine Blase mit dem Text anzuzeigen, wenn der Benutzer den Mauszeiger über das Feld bewegt. ○ Klicken Sie auf die Registerkarte **Anmerkung**, wählen Sie **Hilfe anzeigen** aus, und geben Sie dann Werte in den Feldern **Hilfetext** oder **Anweisungen** ein, um über dem Feld zusätzlichen Text für den Benutzer anzuzeigen.

7. Klicken Sie auf **Aktualisieren**.

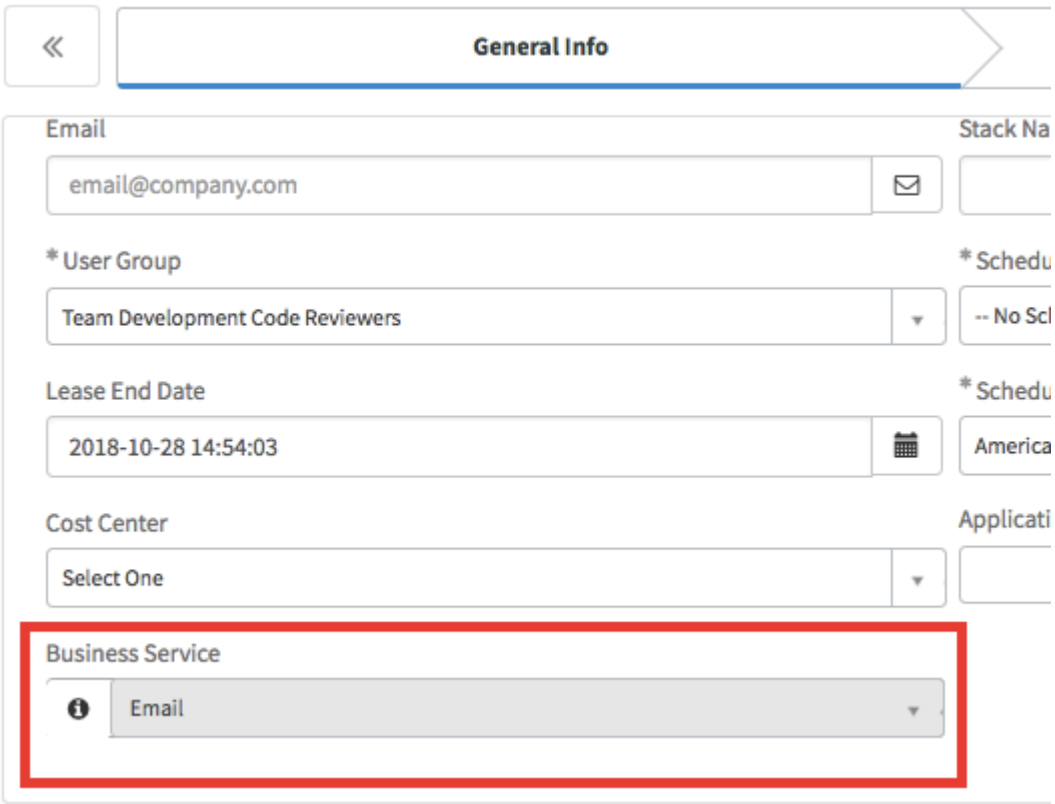
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Schalten Sie das Katalogelement auf **Veröffentlichen** um.

Example:
In diesem Beispiel gilt für das Feld „Business Service“ Folgendes:

- Es wird basierend auf der Sys-ID des Datensatzes mit dem im Datensatz des Business Service „E-Mail“ in der Tabelle „cmdb_ci_service“ ausgefüllt.
- Es ist schreibgeschützt, sodass Benutzer es nicht ändern können.
- Es ist obligatorisch, da es als erforderlich erachtet wird, bevor das System die virtuelle Ressource bereitstellen kann.
- Es enthält Hilfetext, der dem Benutzer mitteilt, dass die Standardauswahl „E-Mail“ ist.

Auf dem Katalogbestellformular wird das Feld wie in der folgende Grafik angezeigt:



Konfigurationsbeispiele für das Cloud-Katalogformular

Mehrere Beispiele werden bereitgestellt, um Ihnen das Verständnis zu erleichtern, wie Bestellformulare des Cloud-Katalogs bearbeitet werden. Diese Beispiele decken Blaupausenregeln, Blaupausenvariablen und Blaupausenformular-UI-Gruppen ab.

Beispiel	Ziel	Verwendete Blaupausenkomponenten
Standort basierend auf dem Cloud-Konto ausfüllen	Verwenden Sie vorhandene Blaupausenregeln, um zu veranschaulichen, wie das Feld „Standort“ basierend auf dem vom Benutzer	Dieses Beispiel veranschaulicht die Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel	Ziel	Verwendete Blaupausenkomponenten
	ausgewählten Cloud-Konto ausgefüllt wird.	
Feld aus einem Cloud-Katalogformular entfernen	Blenden Sie das Feld „Kostenstelle“ im Katalogformular aus, wenn der Kataloganforderer zur Datenbankgruppe gehört.	Dieses Beispiel veranschaulicht Folgendes: • Regeln • Ressourcenpools
Stapelnamen mit einem Skript ausfüllen	Geben Sie dem Kataloganforderer einen vordefinierten Stapelnamen, der die ID des Kataloganforderers enthält. Das Feld kann weiterhin vom Benutzer bearbeitet werden, damit er es bei Bedarf ändern kann.	Dieses Beispiel veranschaulicht Folgendes: • Regeln • Ressourcenpools • Geskriptete Werte
Bestellformular für Cloud-Katalogelement Felder hinzufügen	Erstellen Sie eine Katalogvariable und -eigenschaft, und verwenden Sie diese zum Veröffentlichen eines neuen Felds in einem Formular.	Dieses Beispiel veranschaulicht Folgendes: • Katalogvariablen • Feldreihenfolge • Regeln • Ressourcenpools • Geskriptete Werte
Standardwerte für Cloud-Katalogformularfelder festlegen	Legen Sie einen Standardwert für eine Eigenschaft und eine Blaupausenregel fest.	Dieses Beispiel veranschaulicht Folgendes: • Standardvariablen • Regeln
UI-Gruppe mit zusätzlichen Feldern hinzufügen	Gruppieren Sie Katalogformularfelder in Registerkarten, um das Formular besser zu organisieren und den Benutzer von einem Einstellungssatz zu einem anderen zu führen.	Dieses Beispiel veranschaulicht die UI-Gruppen (Registerkarten).

Standort basierend auf dem Cloud-Konto ausfüllen

Dieses Beispiel führt Sie durch einen vorhandenen Satz von Blaupausenregeln, der standardmäßig von Cloud Provisioning and Governance bereitgestellt wird.

Vorbereitungen

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Cloud-Bereitstellungs-Blueprints
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

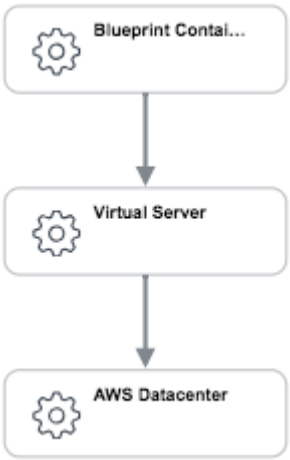
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

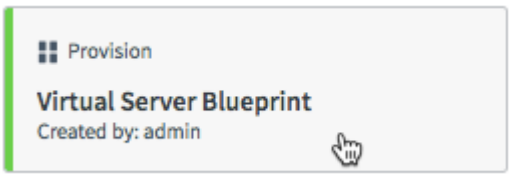
Das Ziel dieses Beispiels ist es, Ihnen zu zeigen, wie ein Standardsatz von Blaupausenregeln die Aufgabe erfüllt, das Feld „Standort“ basierend auf dem Cloud-Konto auszufüllen. Da dieses Beispiel Sie durch die Standarddaten führt, müssen Sie keine Datensätze erstellen, wenn Sie diese Schritte ausführen.

Diese Blaupause, die einen virtuellen Server umfasst, der in einem AWS-Rechenzentrum bereitgestellt werden kann, wird zur Illustration des Beispiels verwendet:



Prozedur

1. Öffnen Sie eine ähnliche Blaupause mit einem virtuellen Server oder ähnlichem.
2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



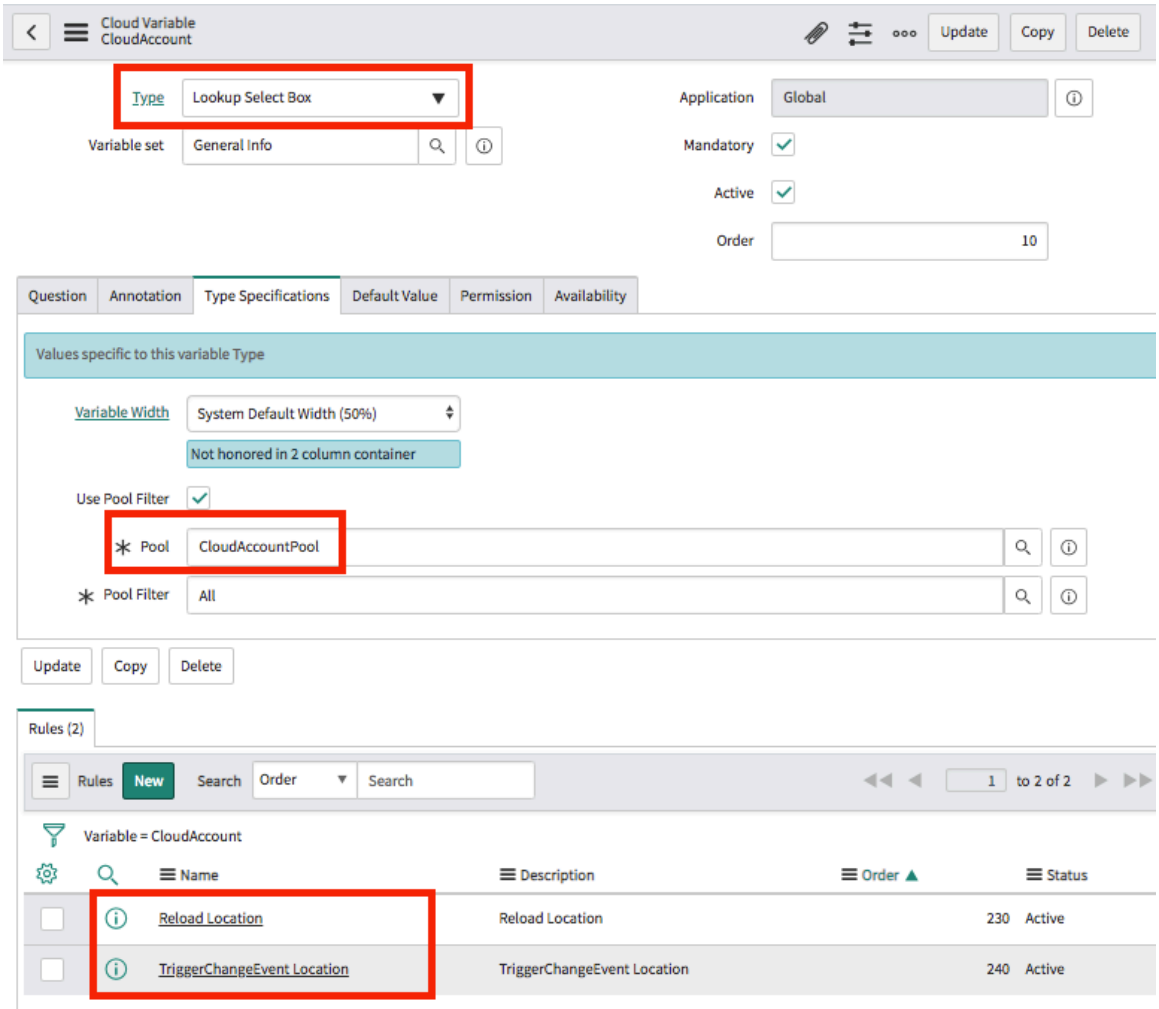
3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste Variablensätze.
4. Klicken Sie auf die Variable **CloudAccount**, um das Cloud-Variablenformular zu öffnen.

   Beachten Sie folgende Elemente:

   - In der zugehörigen Liste „Regeln“ unten werden zwei Regeln bereitgestellt:
     - „ReloadLocation“ lädt den Wert im Feld „Umzug“ neu. Diese Regel wird zuerst ausgeführt, da sie eine niedrigere Reihenfolgennummer als die andere Regel hat.
     - „TriggerChangeEvent Location“ weist das System an, die Aktionen für die Regeln auszulösen, die bereits für die Standortvariable konfiguriert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld **Auswahlfeld für Suche** gibt an, dass das Feld „Cloud-Konto“ eine Auswahl für den Benutzer bietet. Die Optionen, die der Benutzer auswählen kann, stammen aus dem CloudAccountPool im Feld **Typspezifikationen**.

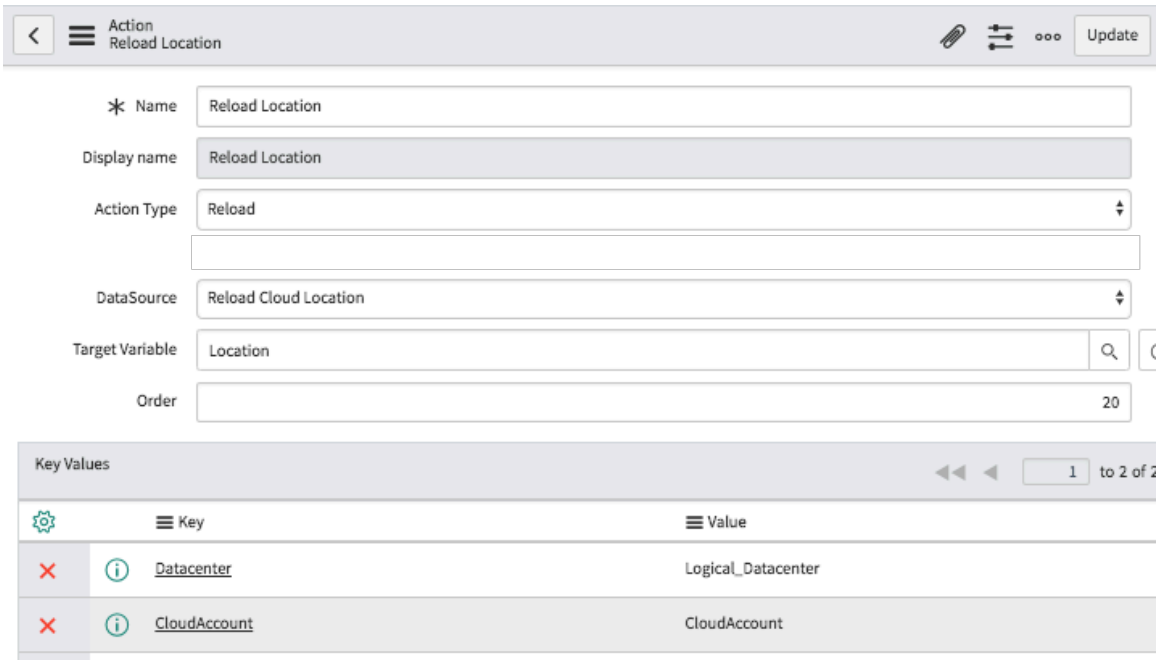


5. Klicken Sie auf die Regel **Standort neu laden**, und klicken Sie dann in der zugehörigen Liste „Aktionen“ auf die Aktion **Standort neu laden**.

   Beachten Sie folgende Elemente:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der **Aktionstyp** ist **Neu laden**, was das System anweist, das Katalogelementformular neu zu laden, sodass ein neuer Wert für das in der **Zielvariable** angegebene Feld (der**Standort**), ausgefüllt werden kann.



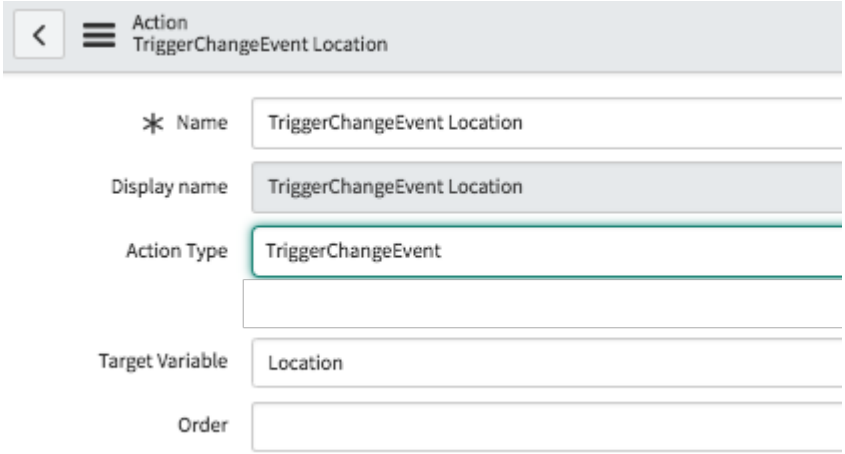
- Das Feld **DataSource** weist das System an, den Standort neu zu laden.
- Die Liste **KeyValues**, die nur verwendet wird, wenn Sie einen Aktionstyp **Neu laden** angeben, legt fest, dass der Benutzer über das Formular das Cloud-Konto übergibt. Das Cloud-Konto ist erforderlich, um den richtigen Wert für den Standort neu zu laden, da der Standort aus einem Pool geladen wird. Dieser Pool verfügt über einen Filter, der die Eingabe des Cloud-Kontos erfordert, um die richtigen Standortoptionen zurückzugeben.

6. Navigieren Sie zurück zum Katalogeigenschaftsformular „CloudAccount“, und öffnen Sie die andere Regel: **TriggerChangeEvent Location**.
7. Klicken Sie auf die zugehörige Liste **Aktionen**, öffnen Sie die Aktion **TriggerChangeEvent Location**, und klicken Sie dann in der zugehörigen Liste „Aktionen“ auf die Aktion **TriggerChangeEvent Location**.

   Beachten Sie folgende Elemente:

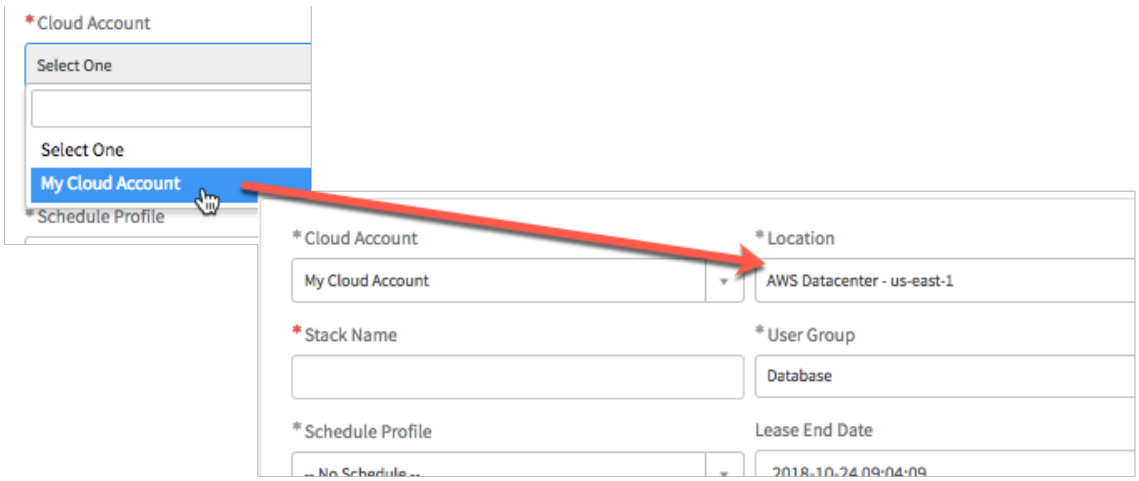
   - Der **Aktionstyp** ist **TriggerChangeEvent**, was das System anweist, die Aktionen für die Regeln auszulösen, die bereits für die Standorteigenschaft konfiguriert sind. Standardmäßig sind bereits mehrere Regeln für die Standorteigenschaft konfiguriert. Dazu gehören Regeln, die andere Felder wie **BS-Profil**, **Netzwerk** usw. neu laden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Es sind keine **KeyValues** erforderlich, da diese Aktion keine Aktion zum erneuten Laden ist.

Das Ergebnis dieser beiden Regeln für das Attribut „CloudAccount“ wird im folgenden Beispiel veranschaulicht:



8. Führen Sie diese Schritte aus, um zu sehen, warum das System den Wert **AWS-Rechenzentrum – us-east-1** im Feld **Standort** ausgefüllt hat und wie das System bestimmt, welcher Standort mit dem Wert von **Mein Cloud-Konto** verknüpft ist:

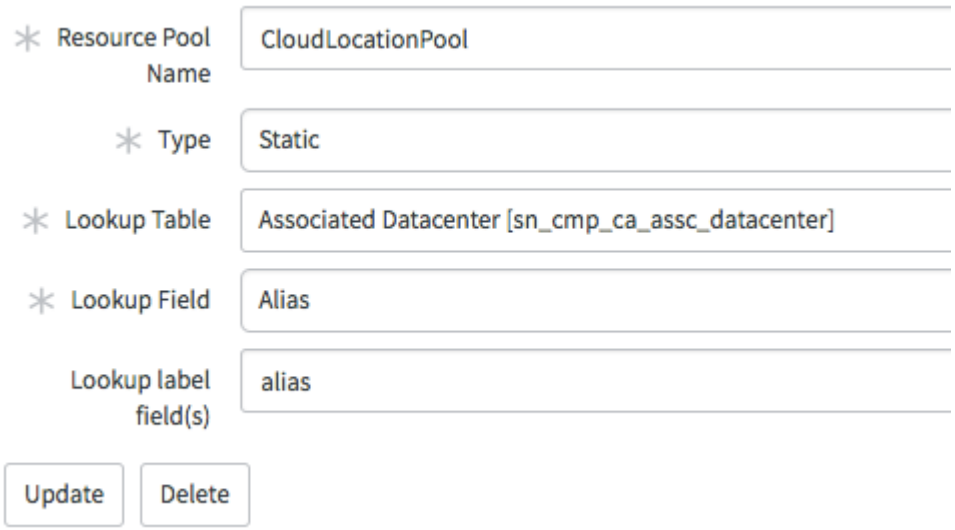
   a. Öffnen Sie in der gleichen Blaupause den Variablensatz **Allgemeine Informationen** und dann den Parameter **Standort**.

   b. Klicken Sie auf die Registerkarte **Typspezifikationen**.

      Beachten Sie die Werte, die für das Feld **Standort** aus dem `CloudLocationPool`-Ressourcenpool ausgefüllt werden können.

   c. Navigieren zu **Verwalten** > **Ressourcenpools**, Offen **CloudLocationPool** , Und beachten Sie diese Elemente:

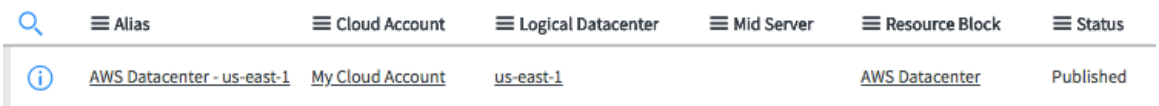
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Die Standorte stammen aus den Datensätzen in der **Suchtabelle**, die in diesem Beispiel die Tabelle **Zugeordnetes Rechenzentrum [sn_cmp_ca_assc_datacenter]** ist.
- Der tatsächliche Wert, der Benutzern im Feld „Standort“ auf dem Katalogelementformular angezeigt wird, stammt aus dem **Suchfeld**. In diesem Beispiel gibt das **Suchfeld** die Spalte „Alias“ aus der Tabelle „Zugeordnetes Rechenzentrum“ [sn_cmp_ca_assc_datacenter] an. Die Spalte **Alias** enthält die tatsächlichen, vom Benutzer lesbaren Namen für alle Standorte.

d. Wechseln Sie zur Standardoberfläche Ihrer Instanz, nicht zum Adminportal, und geben Sie `sn_cmp_ca_assc_datacenter.list` in den Navigationsfilter ein.

Die Liste der Rechenzentren, die bereits Cloud-Konten zugeordnet sind, wird angezeigt.



Beachten Sie, dass das Cloud-Konto **Mein Cloud-Konto** bereits **AWS-Rechenzentrum – us-east-1** zugeordnet ist. Dies ist der Wert, den der Benutzer im Feld „Standort“ sieht. Das System konnte diesen Wert aufgrund der Zuordnung in der Tabelle „Zugeordnetes Rechenzentrum“ anzeigen. Das System hat diese Zuordnung erstellt, als Ihr Cloud Provisioning and Governance-Administrator das Cloud-Konto für AWS erstellt und dann Discovery für das Rechenzentrum „us-east-1“ in diesem Cloud-Konto ausgeführt hat.

Es ist möglich, dass mehrere Rechenzentren mit **Mein Cloud-Konto** verknüpft sind. In diesem Fall werden im Feld „Standort“ alle zugehörigen Rechenzentren neu geladen. Da das Feld „Standort“ vom Typ „Auswählen“ ist, kann der Benutzer im Feld den gewünschten Standort auswählen.

Feld aus einem Cloud-Katalogformular entfernen

Entfernen Sie ein Feld aus dem Cloud Provisioning and Governance Katalogformular, wenn der Anwender einer bestimmten Gruppe angehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Cloud-Bereitstellungs-Blueprints
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

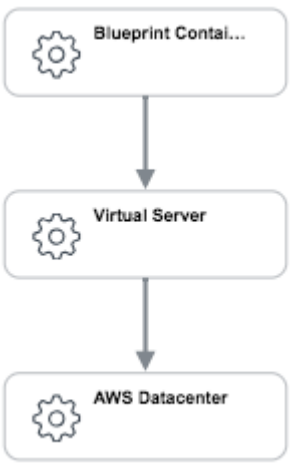
Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieses Beispiels ist, das Feld „Kostenstelle“ im Katalogformular auszublenden, wenn der Kataloganforderer zur Datenbankgruppe gehört. Sie können einem Beispiel wie diesem folgen, wenn Sie Katalogelementfelder basierend auf Werten in anderen Feldern ein- oder ausblenden möchten.

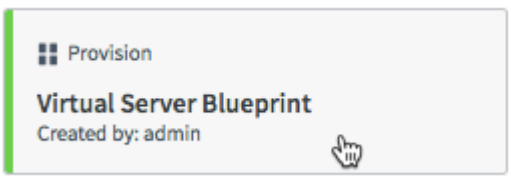
Prozedur

1. Blaupause mit einem virtuellen Server erstellen

   In diesem Beispiel wird eine Blaupause mit einem virtuellen Server in einem AWS-Rechenzentrum verwendet.



2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste Variablensätze.
4. Klicken Sie auf die Variable **CostCenter**, um das Cloud-Variablenformular zu öffnen.
5. Konfigurieren Sie die Regel, die die Kostenstelle basierend auf der Benutzergruppe entfernt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der zugehörigen Liste **Regeln** auf **Neu**.

b. Füllen Sie die Felder **Name** und **Beschreibung** aus.

c. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

6. Konfigurieren Sie die Bedingung, die erfordert, dass die Benutzergruppe „Datenbank“ ist:

a. Klicken Sie in der zugehörigen Liste **Bedingungen** auf **Neu**.

b. Füllen Sie im Formular die Felder aus.

Feld	Einzugebender oder auszuwählender Wert	Beschreibung
Operand	UserGroup	Dieser Wert ist das Feld „Benutzergruppe“, das der Benutzer auswählt.
Operator	--Keine--	Behalten Sie den Wert **--Keine--** bei, da diese Bedingung die einzige Bedingung ist, die Sie konfigurieren müssen. Wenn Sie weitere Bedingungen hinzufügen, können Sie einen anderen Operator auswählen, um zu bestimmen, wie das System diese Bedingung im Verhältnis zu den anderen auswertet.
Wert	287ee6fea9fe198100ada7950d0b1b73	Dieser Wert ist die Sys-ID der Benutzergruppe „Datenbank“, die als Teil der Demodaten in Ihrer Instanz bereitgestellt wird. Siehe SYS-ID Weitere Informationen finden Sie unter .

c. Klicken Sie auf **Absenden**.

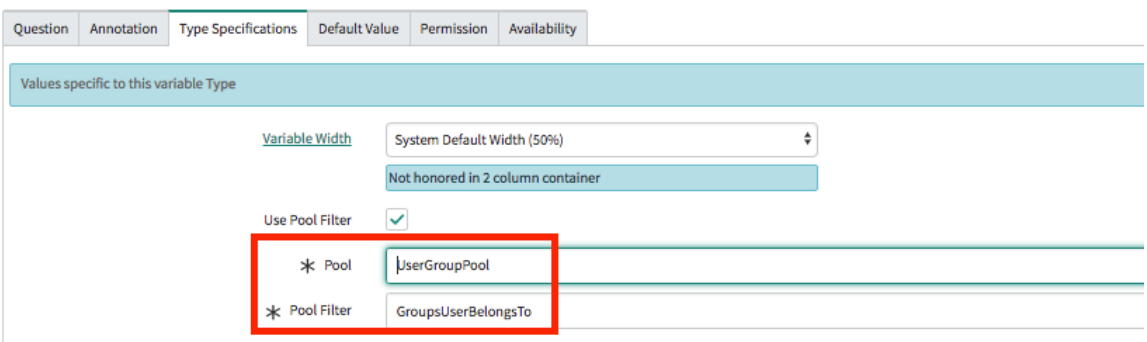
7. Um zu verstehen, warum die Sys-ID der Benutzergruppe für das System erforderlich ist, führen Sie die folgenden Schritte aus:

a. Öffnen Sie die Blaupause erneut, und klicken Sie erneut auf den Vorgang „Bereitstellung“.

b. Klicken Sie in der zugehörigen Liste **Variablensätze** auf **Allgemeine Informationen**.

c. Klicken Sie auf die Variable **UserGroup**.

Beachten Sie, dass das System auf der Registerkarte **Typspezifikationen** Benutzergruppen aus **UserGroupPool** ausfüllt. Das System führt den geskripteten Poolfilter mit dem Namen **GroupsUserBelongsTo** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Ressourcenpools**an.

e. Suchen und öffnen Sie **UserGroupPool**.

Beachten Sie, dass die Werte für den Pool aus der Tabelle im Feld **Suchtabelle** abgeleitet sind, das in diesem Fall ist die Gruppentabelle [sys_user_group] ist.

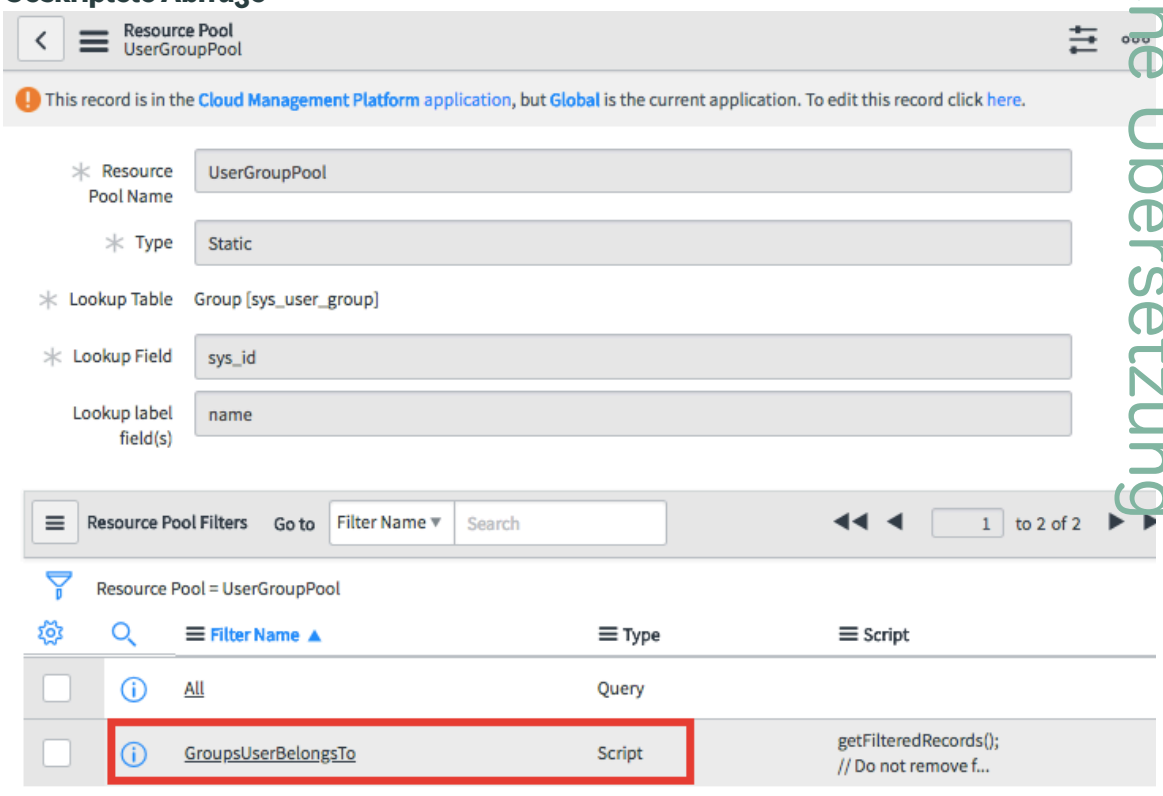
Beachten Sie auch, dass die zugehörige Liste „Ressourcenpoolfilter“ zwei Abfragen enthält:

- **All** ist eine generische Abfrage, die die Liste aller Datensätze aus der **Suchtabelle** zurückgibt. Der von dieser Tabelle zurückgegebene Wert stammt aus dem **Suchfeld**, in diesem Fall der Sys-ID. Das System ignoriert jedoch die Abfrage `All` in diesem Fall, da die geskriptete Abfrage vorhanden ist.
- **GroupsUserBelongsTo** ist eine geskriptete Abfrage, die die Sys-ID der Datensätze in der **Suchtabelle** zurückgibt.

Wichtig: Wenn eine geskriptete Abfrage vorhanden ist, verwendet das System diese anstelle der generischen *ALL*-Abfrage.

Sowohl die generische Abfrage als auch die geskriptete Abfrage geben die Sys-ID des Datensatzes in der Suchtabelle zurück. Tatsächlich ignoriert hier das System aber die **All**-Abfrage und den im **Suchfeld** angegebenen Wert und verwendet das Skript **GroupsUserBelongsTo**.

Geskriptete Abfrage



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stapelnamen mit einem Skript ausfüllen

Dieses Beispiel zeigt, wie der Name des Stapels, den ein Benutzer im Cloud Provisioning and Governance-Katalog anfordert, mithilfe der Benutzer-ID ausgefüllt wird. Im Beispiel wird eine Skripteinbindung verwendet, die Sie über eine Blaupausenregelaktion aufrufen können.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Cloud-Bereitstellungs-Blueprints
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

In diesem Beispiel wird eine Skripteinbindung verwendet. Wenn Sie ähnliche Skripteinbindungen erstellen möchten, machen Sie sich mit den Glide System APIs vertraut, die Teil Ihrer Instanz sind. Auf der Entwicklerwebsite finden Sie eine umfassende Liste aller APIs. Siehe Skripteinbindungen Weitere Informationen dazu, wie das System diese Skripts verwendet.

Warum und wann dieser Vorgang ausgeführt wird

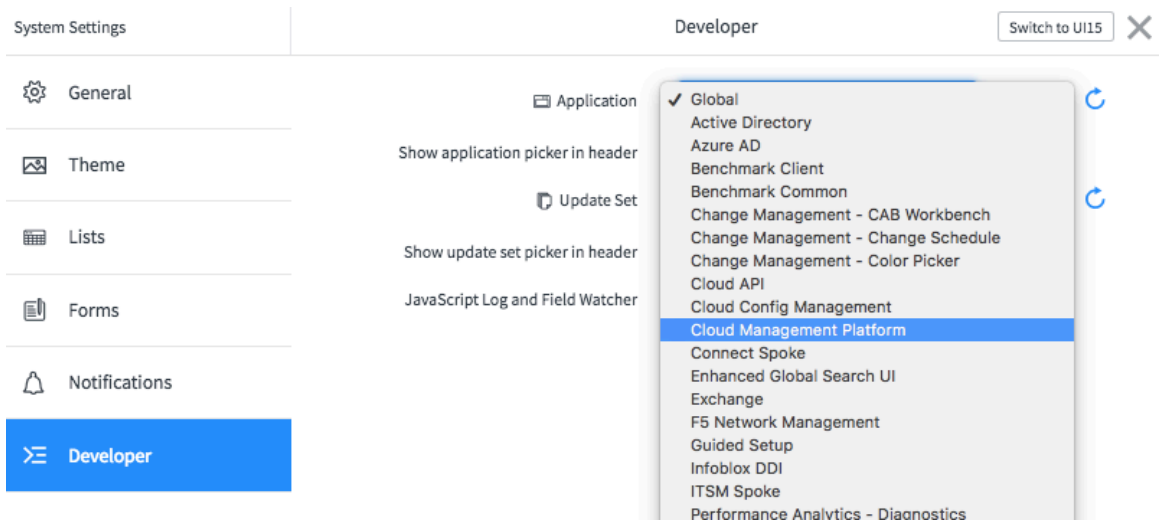
Das Ziel dieses Beispiels besteht darin, die ID des Kataloganforderers zu verwenden und im Feld „Stapelname“ auszufüllen. Das Feld kann weiterhin bearbeitet werden. Folgen Sie einem Beispiel wie diesem, wenn Sie eine Benennungs- oder Bezeichnungskonvention für bestimmte Werte locker erzwingen möchten, dem Benutzer aber dennoch erlauben möchten, den gewünschten Text einzugeben.

Prozedur

1. Erstellen Sie eine Skripteinbindung, die die Benutzer-ID der das Katalogelement anfordernden Person zurückgibt:

   a. Klicken Sie auf der Standardoberfläche für die Instanz (nicht im Cloud-Adminportal) oben links auf das Zahnradsymbol ( ), und klicken Sie dann auf **Entwickler**.

   b. Wählen Sie im Feld **Anwendung** die Option **Cloud Provisioning and Governance** aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Anwendungsbereich Ihrer Instanz ändert sich in **Cloud Provisioning and Governance**. Diese Auswahl bedeutet, dass die Cloud Provisioning and Governance-Anwendung die Skripteinbindung finden kann.

c. Schließen Sie das Fenster „Systemeinstellungen“.

d. Navigieren zu **Systemdefinition** > **Skripteinbindungen**an.

e. Klicken Sie auf **Neu**.

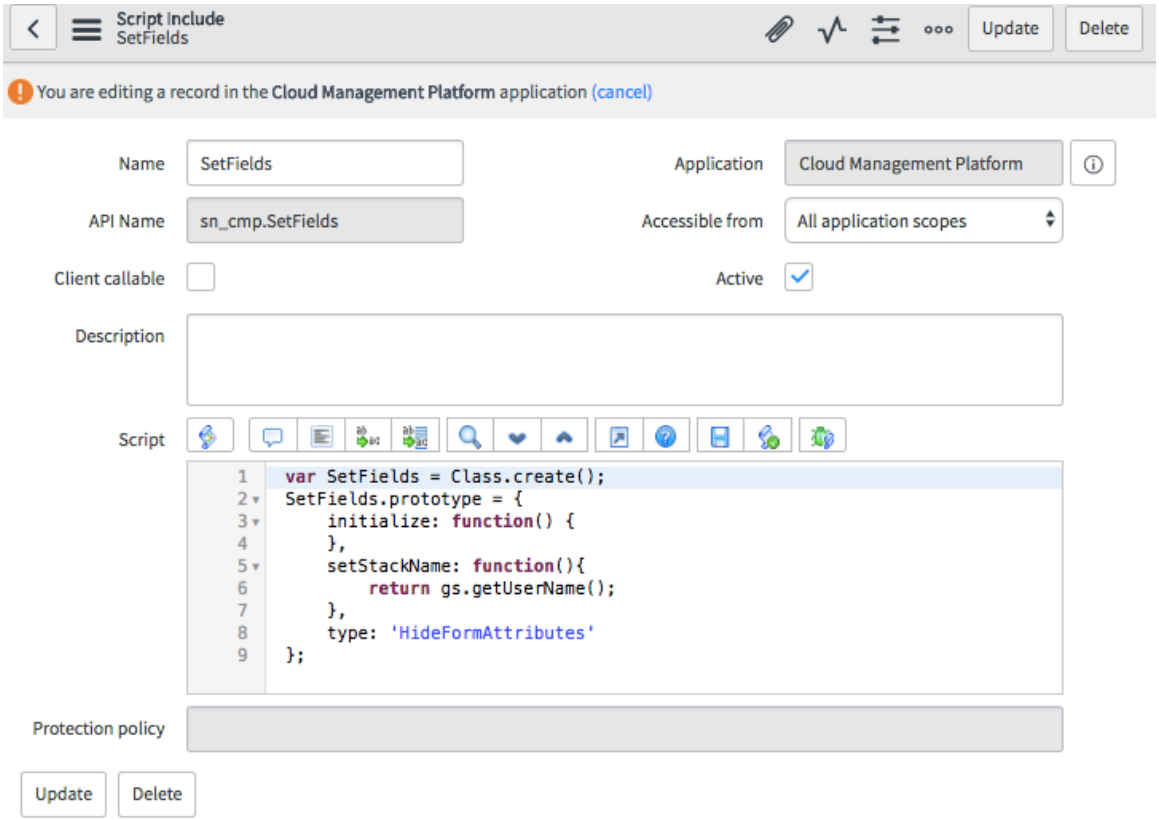
f. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ohne Leerzeichen an.
Zugänglich von	Wählen Sie **Alle Anwendungsbereiche** aus.
Skript	Geben Sie dieses Skript ein:

```
var SetFields = Class.create();
SetFields.prototype = {
 initialize: function() {
 },
 setStackName: function(){
  return gs.getUserName();
 },
 type: 'HideFormAttributes'
};
```

Die Funktion `setStackName ()` gibt den Benutzernamen des Katalogelementanforderers zurück. Sie können diese Funktion über eine Blaupausenregelaktion aufrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

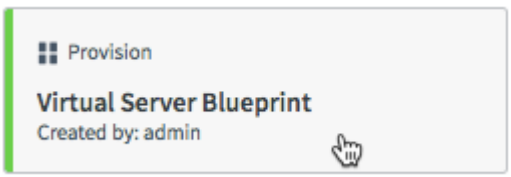


g. Klicken Sie auf **Absenden**.

h. Klicken Sie erneut oben links auf das Zahnradsymbol ( ), und ändern Sie die **Anwendung** wieder in **Global**.

2. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Blueprints** Und öffnen Sie den entsprechenden Blueprint.

3. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



4. Klicken Sie auf die Schaltfläche **Stapelname** Variablensatz in der zugehörigen Liste Variablensätze.

Beachten Sie, dass Stapelname ein einzeiliges Textfeld ist, das Texteingaben akzeptiert.

5. Erstellen Sie eine Regel zum Ausfüllen des Stapelnamens:

a. Scrollen Sie nach unten zum Ende des Formulars, und klicken Sie in der zugehörigen Liste **Regeln** auf **Neu**.

b. Geben Sie einen Namen und eine Beschreibung ein.

c. Klicken Sie auf **Absenden**.

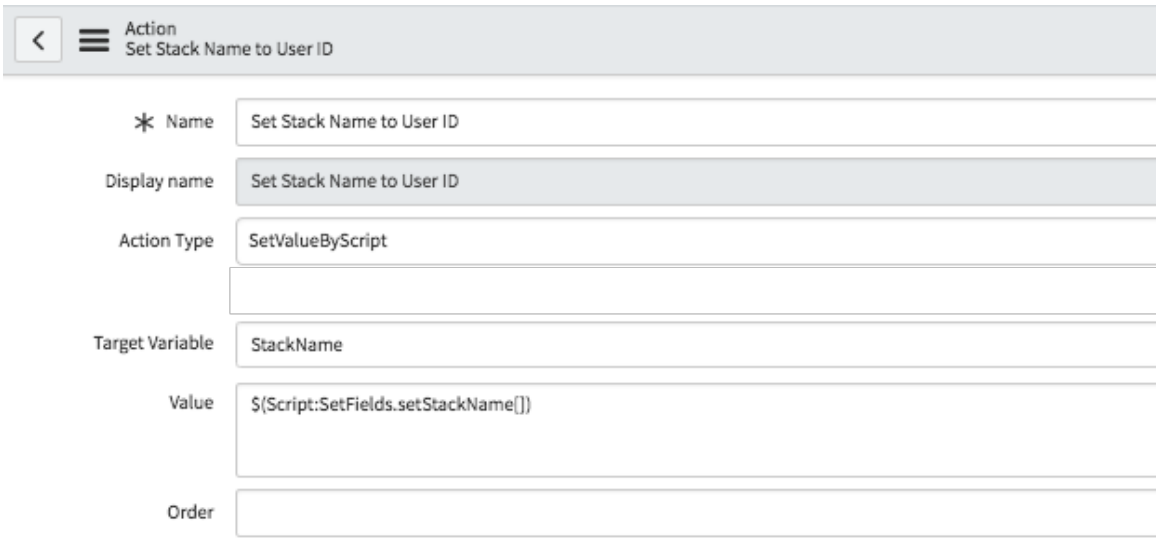
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Konfigurieren Sie die Aktion wie folgt:

a. Scrollen Sie nach unten zum Ende des Formulars „Regel“, und klicken Sie in der zugehörigen Liste **Aktion** auf **Neu**.

b. Konfigurieren Sie die Regel wie folgt:

Feld	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen und eine Beschreibung an, z. B. `Stapelnamen auf Benutzer-ID festlegen`.
Aktionstyp	Wählen Sie **SetValueByScript** aus, um das System anzuweisen, die im Feld **Wert** angegebene Skripteinbindung aufzurufen.
Zielvariable	Wählen Sie **Stapelname** aus, um das System anzuweisen, den Wert des Felds „Stapelname“ festzulegen.
Wert	Rufen Sie die Methode in der Skripteinbindung auf, die die Benutzer-ID zurückgibt. Der Aufruf muss die folgende Syntax haben: `$(Script:ScriptIncludeName.methodName[])` Verwenden Sie in diesem Beispiel `$(Script:SetFields.setStackName[])`.

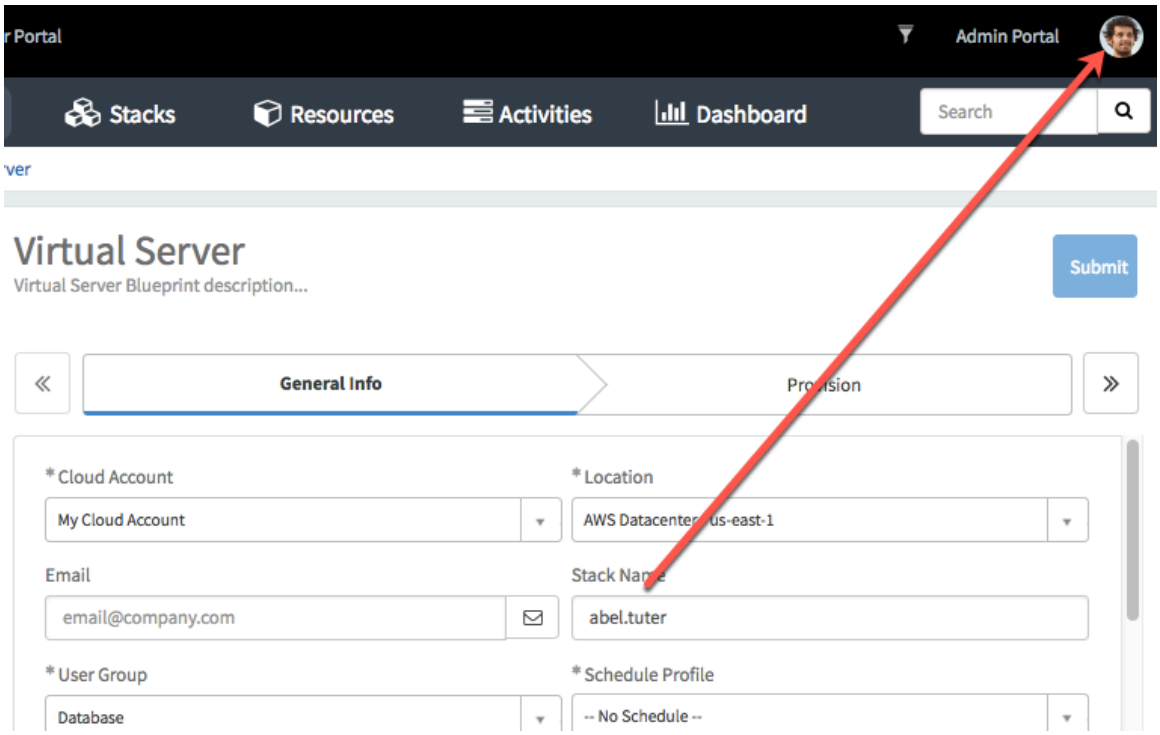


c. Klicken Sie auf **Absenden**.

Ergebnis

Im Cloud-Benutzerportal wird im Katalogbestellformular für den Bereitstellungsvorgang die Benutzer-ID des angemeldeten Benutzers angezeigt. In diesem Beispiel wird der Benutzer „Able Tutor“ verwendet, der im Basissystem als Demodaten bereitgestellt wird. Der Wert im Feld **Stapelname** ist der gleiche Wert wie im Feld „Benutzer-ID“ der Tabelle „Benutzer“ [sys_user]. Das Profilsymbol für denselben angemeldeten Benutzer wird auch oben rechts im Cloud-Benutzerportal angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Standardwerte für Cloud-Katalogformularfelder festlegen

Sie können Standardwerte für alle Benutzer festlegen oder Felder basierend auf Bedingungen mit Standardwerten ausfüllen. Dieses Beispiel zeigt, wie ein Zeitplanprofil und ein Business Service als Standards festgelegt werden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Cloud-Bereitstellungs-Blueprints
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieses Beispiels ist die Anzeige eines Standardwerts für das Zeitplanprofil und den Business Service. Jedes Feld leitet seine Werte unterschiedlich ab:

- Das Zeitplanprofil leitet seine Werte von einem Poolfilter ab, der einen Textwert zurückgibt. Daher müssen Sie den Standardwert festlegen, indem Sie den richtigen, übereinstimmenden Text für eine der Zeitplanprofiloptionen anwenden, die dem Benutzer in einer Liste angezeigt werden.
- Der Business Service leitet seine Werte aus einer Referenz auf die Tabelle „Service“ [cmdb_ci_service] ab. Daher müssen Sie den Wert festlegen, indem Sie die Sys-ID des Datensatzes angeben, den Sie anzeigen möchten.

Im Beispiel in diesem Thema werden die Werte auf verschiedene Arten festgelegt:

- Der Standardwert für das Zeitplanprofil wird direkt in der Eigenschaft „Zeitplanprofil“ festgelegt und gilt für alle Benutzer ohne Bedingungen. Sie können dies tun, um die Verwendung virtueller Ressourcen für alle Benutzer auf einen bestimmten Zeitplan zu beschränken, z. B. nur während der Geschäftszeiten.

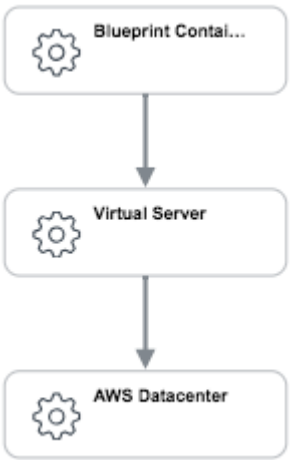
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Standardwert für den Business Service wird mithilfe einer Aktion in einer Blaupausenregel festgelegt. Sie können eine Regel zum Festlegen eines Standardwerts verwenden, wenn der Wert nur dann als Standard festgelegt werden soll, wenn bestimmte Bedingungen erfüllt sind. Wenn der Benutzer beispielsweise zu einer Benutzergruppe gehört, die nur einen Business Service verwendet, legen Sie den Wert für den Benutzer so fest, dass er nicht eine lange Liste aller Business Services in Ihrer Organisation durchsuchen muss.

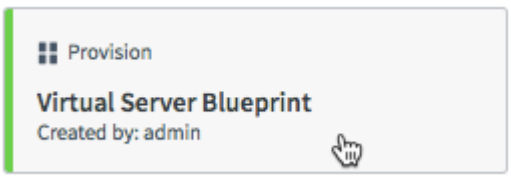
Prozedur

1. Blaupause mit einem virtuellen Server erstellen

   In diesem Beispiel wird eine Blaupause mit einem virtuellen Server in einem AWS-Rechenzentrum verwendet.



2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



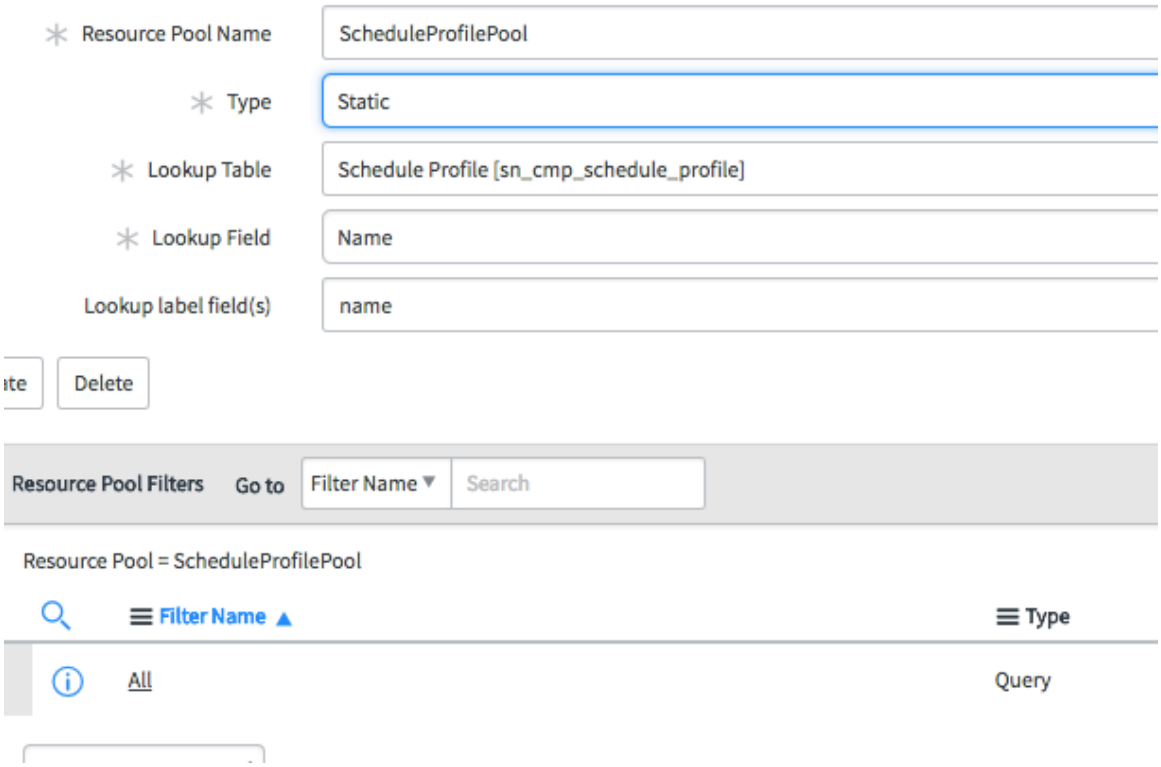
3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste Variablensätze.
4. Klicken Sie auf die Variable **ScheduleProfile**.

   Beachten Sie, dass das Feld **Pool** auf der Registerkarte **Typspezifikationen** den Pool angibt, aus dem die Werte für das Zeitplanprofil abgeleitet werden: ScheduleProfilePool.

   Der Pool **ScheduleProfilePool** gibt den Filter **Alle** an, der die Werte im Feld „Name“ der Tabelle „Zeitplanprofil“ [sn_cmp_schedule_profile] zurückgibt. Diese Werte sind statische Textwerte, was bedeutet, dass Sie den genauen Textwert für den

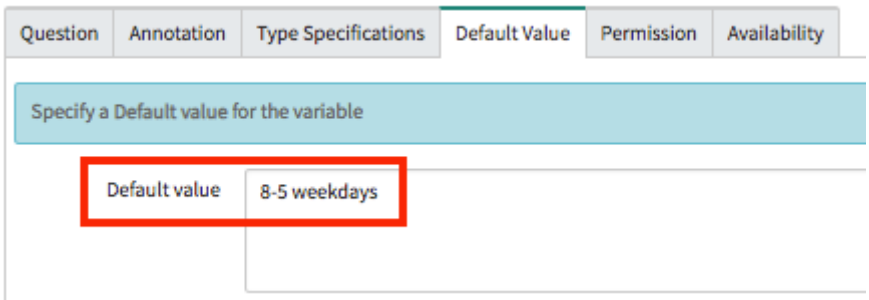
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Namen des Zeitplanprofils angeben können, das Sie als Standard festlegen möchten.



5. Geben Sie auf der Registerkarte **Standardwert** des Eigenschaftsformulars „ScheduleProfile“ den Text ein, der dem Wert im Feld „Name“ aus der Tabelle „Zeitplanprofil“ [sn_cmp_schedule_profile] entspricht.

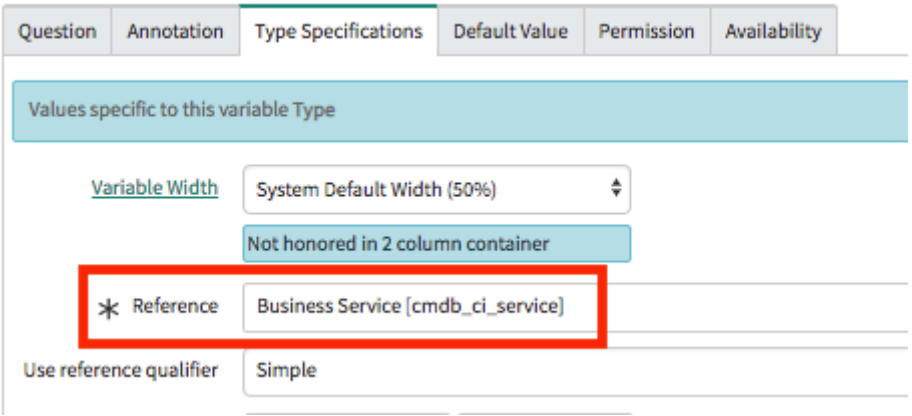
   In diesem Beispiel beträgt dieser Wert `Wochentage von 8–17.00 Uhr`.



6. Klicken Sie auf **Aktualisieren**.
7. Klicken Sie auf die Variable **BusinessService**.

   Beachten Sie, dass das Feld **Referenz** auf der Registerkarte **Typspezifikationen** die Tabelle „Service“ [cmdb_ci_service] angibt, aus der die Werte für den Business Service abgeleitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Standardmäßig müssen Sie zum Verweisen auf einen bestimmten Datensatz in einer Tabelle die Sys-ID des Datensatzes kennen.

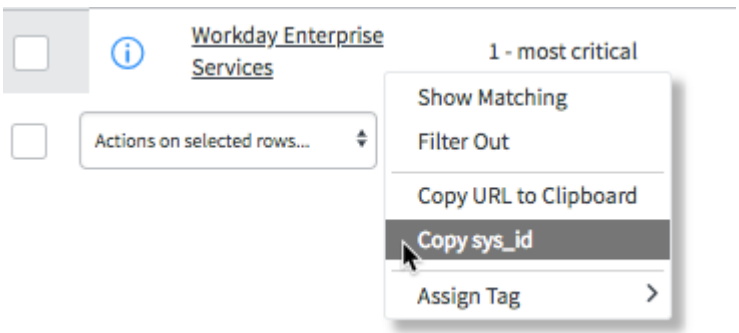
8. So rufen Sie die Sys-ID eines Business Service ab:

a. Geben Sie in der Hauptoberfläche für die Instanz (nicht im Cloud-Adminportal) `cmdb_ci_service.list` im Anwendungsfilter ein.

b. Suchen Sie den Business Service, den Sie als Standard festlegen möchten.

c. Klicken Sie mit der rechten Maustaste auf den Datensatz, und wählen Sie **sys_id kopieren** aus.

In diesem Beispiel wird **Workday Enterprise Services** verwendet.



9. Erstellen Sie im Variablenformular **BusinessService** eine Regel, eine Aktion und eine Bedingung mit diesen Werten:

a. Klicken Sie in der zugehörigen Liste **Regel** auf **Neu**.

b. Geben Sie einen Namen und eine Beschreibung ein.

c. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

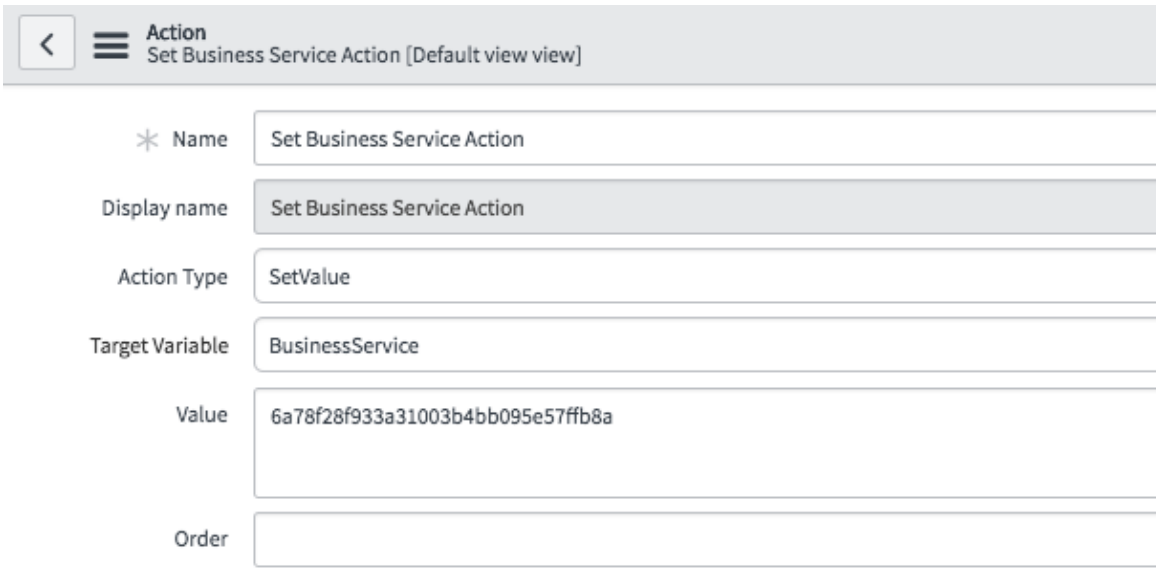
d. Klicken Sie in der zugehörigen Liste **Aktion** für die Regel auf **Neu**.

e. Geben Sie einen Namen an, und konfigurieren Sie dann diese Felder wie angegeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

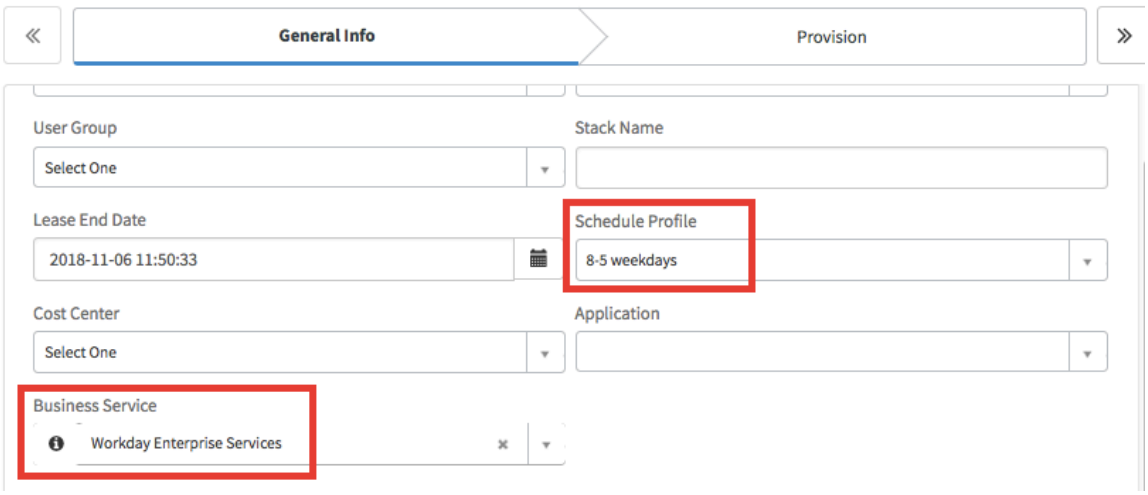
Feld	Wert
Aktionstyp	**SetValue** Diese Option weist das System an, das Feld in den von Ihnen angegebenen Wert zu ändern. Die Auswahl dieser Option entspricht der Eingabe eines Standardwerts im Eigenschaftsformular.
Zielfeld	**BusinessService**
Wert	Die Sys-ID des Business Service, den Sie kopiert haben.

In diesem Beispiel ist der Business Service standardmäßig auf „Workday Enterprise Services“ festgelegt, was im System mit der Sys-ID dargestellt wird, die Sie bereits kopiert haben.



f. Klicken Sie auf **Absenden**.

Ergebnis



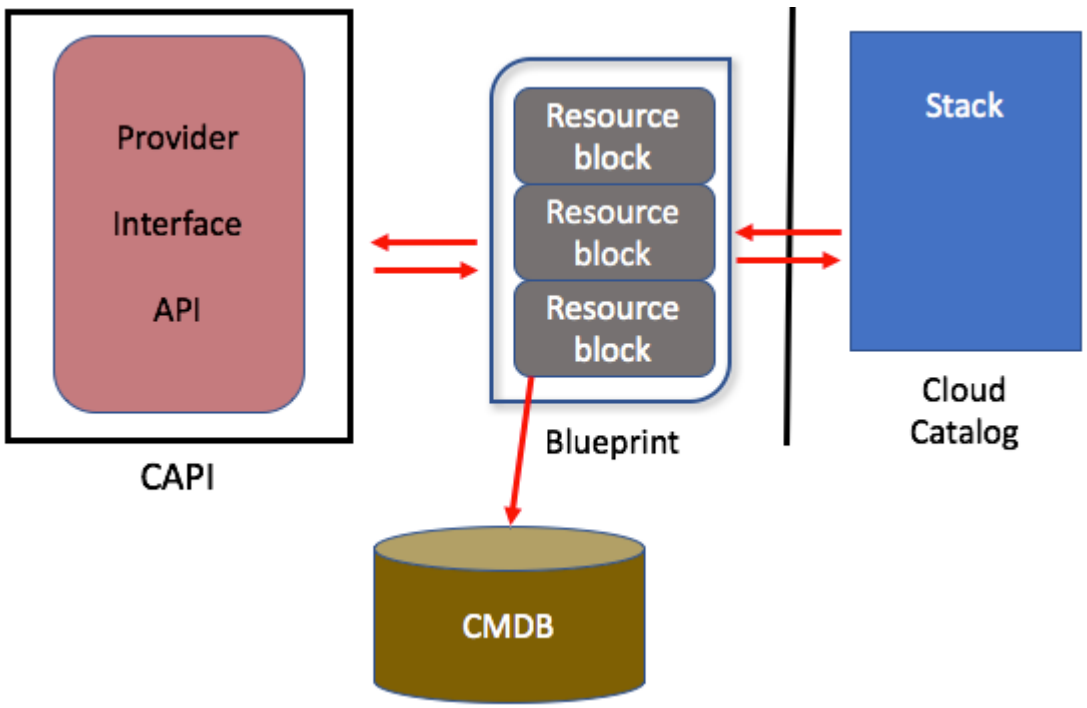
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Sie können eine Bedingung oder mehrere Bedingungen erstellen, die erfüllt sein müssen, bevor das System den Standardwert für den Business Service festlegt. Beispiel: Sie möchten den Standardwert des Business Service nur dann in „Workday Enterprise Services“ ändern, wenn die Gruppe, der der Benutzer angehört, die Gruppe „Workday Admins“ ist.

Ressourcenblöcke in Cloud Provisioning and Governance

Ressourcenblöcke fungieren als eine Art Middleware-Komponente zwischen Katalogelementen, der Cloud API (CAPI) und der CMDB.

Die folgende Grafik zeigt, wie Ressourcenblöcke zwischen andere Komponenten im System passen:



Blaupausen

Jeder Ressourcenblock wird zu einem Baustein innerhalb einer Blaupause. Die Blaupause wird schließlich zu einem Katalogelement (auch Stapel genannt), das ein Benutzer aus dem Cloud-Katalog bereitstellt.

Cloud-API (CAPI)

Jeder Ressourcenblock definiert zulässige Vorgänge wie „Bereitstellung“ und „Bereitstellung aufheben“. Diese Vorgänge rufen verschiedene Komponenten in der CAPI auf, um den vom Stapel empfangenen Vorgang auszuführen.

Die CMDB

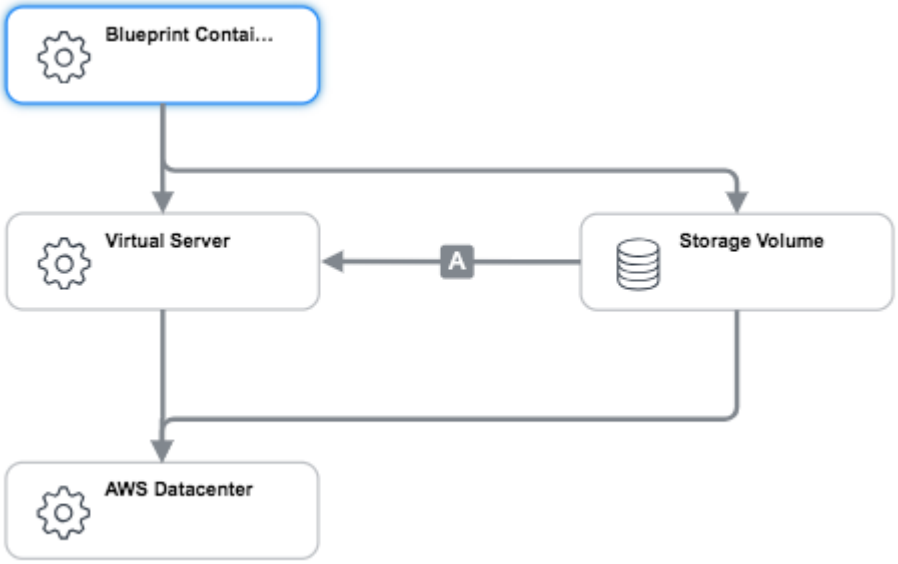
Jeder Ressourcenblock basiert auf einem CI-Typ der CMDB. Ressourcenblöcke haben auch einen Antwortprozessor, der Antworten vom Cloud-Provider verarbeitet, um eine Art von Aktion in der CMDB durchzuführen, z. B. das Erstellen oder Aktualisieren eines CI.

Verbindungen von Ressourcenblöcken

Ressourcenblöcke sind in Blaupausen miteinander verbunden. Beispielsweise ist in dieser Blaupause ein Ressourcenblock eines virtuellen Servers mit Speicher verbunden. Der virtuelle Server und der Speicher sind beide mit einem AWS-Rechenzentrum-Ressourcenblock verbunden.

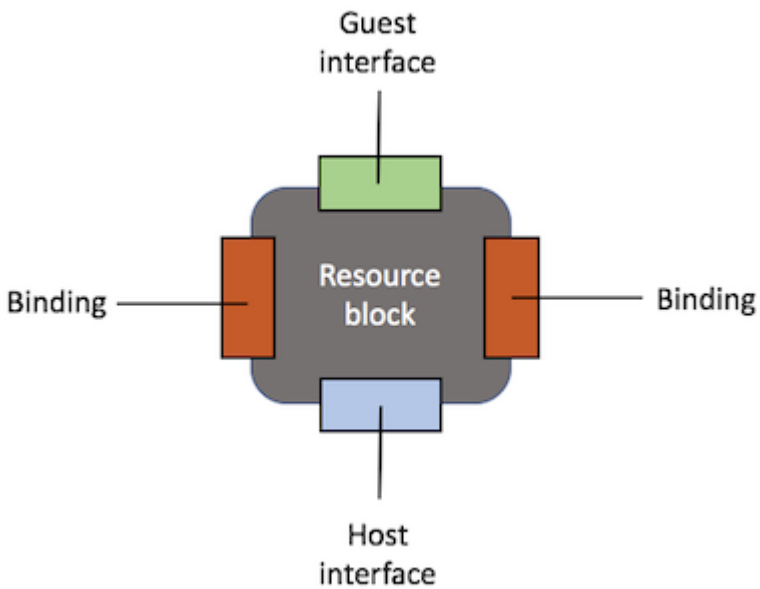
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Blaupause: Server mit Speicher



Damit diese Verbindungen erfolgreich hergestellt werden können, muss jeder Ressourcenblock einen Schnittstellentyp angeben. Diese Grafik veranschaulicht diese Schnittstellen:

Schnittstellentypen für Ressourcenblöcke



- Die *Gastschnittstelle* stellt eine Verbindung mit der darüber befindlichen Ressource her. Die Gastschnittstelle enthält die *Vorgänge* (auch *Vorgangssignaturen* genannt), mit denen Benutzer Aktionen für ihre Ressource ausführen können.
- Die *Hostschnittstelle* stellt eine Verbindung mit der Ressource unter dem Ressourcenblock in der Blaupause her. Die Hostschnittstelle enthält auch Vorgangssignaturen.
- Die *Bindungen* verbinden angrenzende Ressourcen.

Ressourcenblöcke können beliebig viele Gastschnittstellen, Hostschnittstellen und Bindungen aufweisen. Verbindungen können in verschiedene Richtungen hergestellt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vertikale Verbindungen erfordern, dass die Hostschnittstelle des oberen Ressourcenblocks der Gastschnittstelle des unteren Ressourcenblocks entspricht.

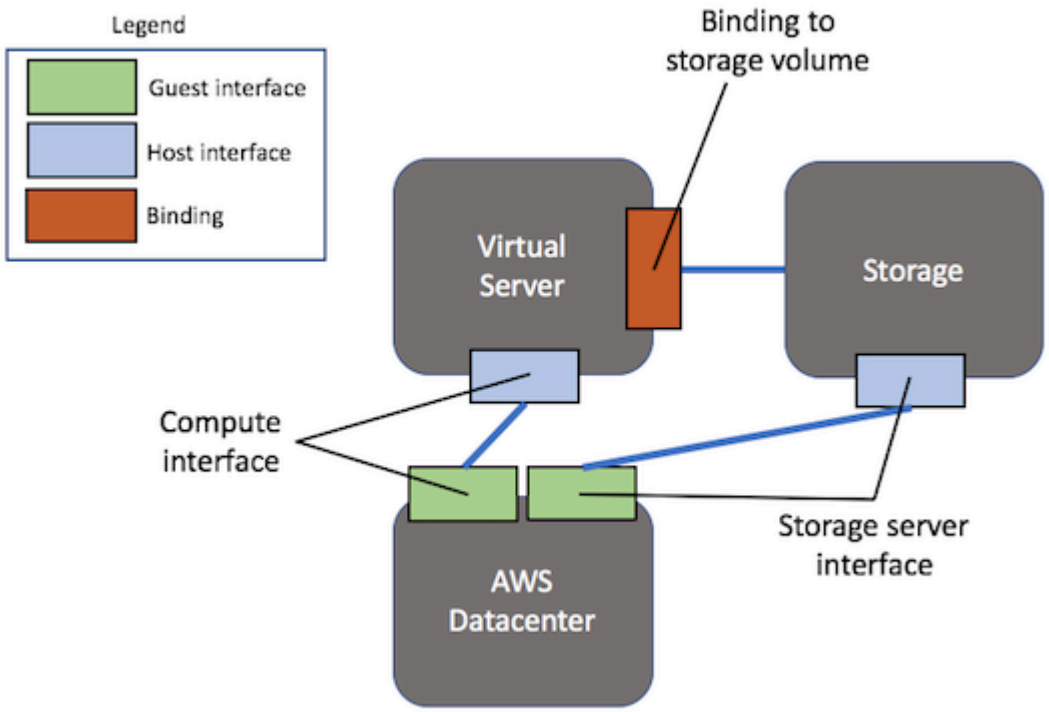
  Hinweis: In Blaupausen wird diese vertikale Verbindung als *Containment*-Verbindung bezeichnet.

- Horizontale Verbindungen binden eine Ressource an eine andere, aber beide Ressourcen müssen sich über demselben Ressourcenblock befinden.

  Hinweis: In Blaupausen wird diese horizontale Verbindung als *Angehängt*-Verbindung bezeichnet.

Wenn in dieser Beispielblaupause ein virtueller Server mit angehängtem Speicher in einem AWS-Rechenzentrum verbunden ist, sind die Ressourcenblöcke wie folgt konfiguriert:

Schnittstellen für Ressourcenblöcke



Ressourcenblock	Schnittstellen und Bindungen
Virtueller Server	• Hostschnittstelle: Computing • Bindung: an Speichervolume
AWS-Rechenzentrum	• Gastschnittstelle: Computing • Gastschnittstelle: Speicherserverschnittstelle
Speicher	Hostschnittstelle: Speicherserverschnittstelle Die Bindung zwischen dem virtuellen Server und dem Speicher ist unidirektional. Sie konfigurieren die Bindung für den virtuellen Speicherressourcenblock nur, indem Sie den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenblock	Schnittstellen und Bindungen
	Speicherressourcenblock angeben. Sie müssen keine weitere Bindung für den Speicherressourcenblock konfigurieren.

Gastschnittstellen und Vorgänge

Jede Gastschnittstelle bietet einen Standardsatz von Vorgängen (auch Vorgangssignaturen genannt), mit denen der Benutzer auswählen kann, was er mit einer virtuellen Ressource tun möchte. Der häufigste Vorgang ist die Bereitstellung, was bedeutet, dass eine virtuelle Ressource erstellt wird. Viele Gastschnittstellen und entsprechende Vorgänge werden standardmäßig mit der Cloud Provisioning and Governance-Anwendung bereitgestellt. Sie können diese standardmäßigen Gastschnittstellen für viele Ihrer Ressourcenblöcke verwenden.

Wenn Sie eine neue Gastschnittstelle erstellen müssen, werden diese Vorgänge standardmäßig bereitgestellt:

- Start
- Stoppen
- Bereitstellung
- Aufheben der Bereitstellung
- Bereinigung
- ModifySchedule
- ModifyLease

Details der Ressourcenblockkomponenten

Jeder Ressourcenblock enthält diese Komponenten:

Ebenen

Die logische Ebene im Stapel, zu der dieser Ressourcenblock gehört. Standardmäßig stellt Cloud Provisioning and Governance die Ebenen bereit. Beim Konfigurieren von Ressourcenblöcken können Sie die für Sie relevante auswählen.

Vorgänge für jede Gastschnittstelle

Wie bereits erwähnt, bietet jede Gastschnittstelle Vorgänge. Die häufigsten Vorgänge für einen virtuellen Server sind beispielsweise **Bereitstellung**, **Bereitstellung aufheben**, **Starten**, **Stoppen**.

Eingabeparameter für die einzelnen Vorgänge

Die Eingabeparameter enthalten Werte, die der Cloud-Provider bei der Ausführung von Vorgängen über CAPI verwendet. Diese Parameter enthalten die Informationen, die der Benutzer beim Ausführen eines Vorgangs, z. B. Bereitstellung, für einen Stapel auswählt.

Beispielsweise muss ein Benutzer normalerweise den Standort angeben, bei dem es sich um ein Rechenzentrum handelt, zu dem ein Stapel gehört. Der Wert, den der Benutzer im Feld **Standort** auswählt, wird im Standortparameter gespeichert. Das System verwendet diesen Parameter, der standardmäßig für den Ressourcenblock des virtuellen Servers verfügbar ist, und übergibt ihn an den CAPI-Schnittstellenvorgang `CreateNode`. Der Schnittstellenvorgang

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

`CreateNode` weist den Cloud-Provider an, den tatsächlichen virtuellen Server zu erstellen (oder bereitzustellen).

Schritte für die einzelnen Vorgänge

Jeder Vorgang erfordert einen Schritt, um die tatsächliche Arbeit auszuführen. Jeder Schritt ruft eine bestimmte Schnittstelle und Methode in CAPI auf und übergibt die für diese Methode erforderlichen Eingabeparameter. Beispielsweise stellt der Vorgang **Bereitstellung** für einen virtuellen Server einen Schritt zum Herstellen einer Verbindung und zum Erstellen eines virtuellen Computers sowie einen weiteren Schritt zum Erstellen des Knotens im Cloud-Provider bereit. Jeder Schritt bietet andere Eingabeparameter. Zum Herstellen einer Verbindung und Erstellen eines virtuellen Computers ist neben vielen anderen Parametern das Cloud-Konto erforderlich. Zum Erstellen des Knotens ist kein Cloud-Konto erforderlich.

Sie können jedem Vorgang beliebig viele Schritte hinzufügen. Sie können auch *Ausgabeattribute* verwenden, um Werte in Attributen von einem Schritt an einen anderen Schritt zu übergeben oder Werte von Schritten in einem Vorgang an Schritte in einem nachfolgenden Vorgang zu übergeben. Beispielsweise kann der Vorgang der **Bereitstellung** für einen virtuellen Server ein Ausgabeattribut für die Netzwerkschnittstellen-ID und ein anderes für die Knoten-ID bereitstellen. Wenn der Cloud-Provider die Antwort sendet, werden die tatsächliche ID des Netzwerks und die des Knotens aus der Antwort analysiert und in den Ausgabeattributen gespeichert. Nachfolgende Schritte können dann die IDs zum Ausführen von Aktionen verwenden.

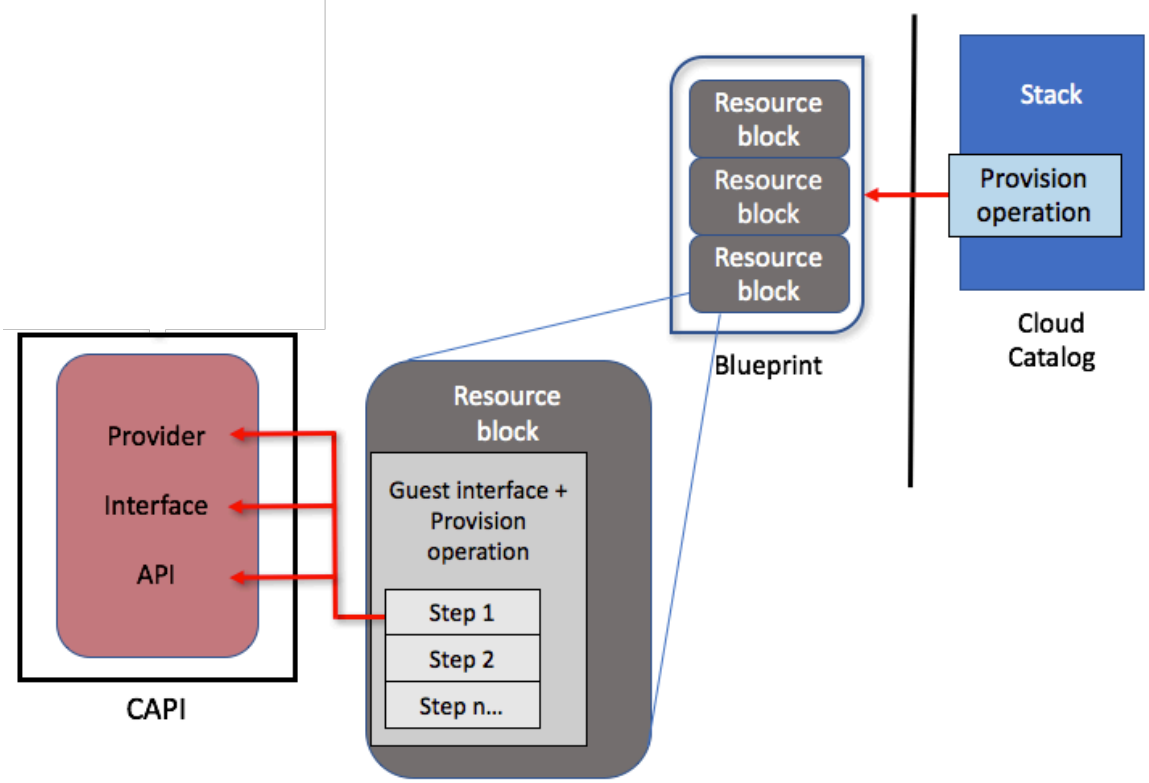
Antwortprozessoren

Antwortprozessoren teilen dem System mit, was in der CMDB zu tun ist. Wenn der Cloud-Provider eine Antwort sendet, nachdem ein Vorgang ausgeführt wurde, verarbeitet der Prozessor die Antwort.

Hinweis: Diese Prozessoren sind Skripts, die im System eingeschlossen sind. Sie sind keine MID Server-Skripteinbindungen wie die CAPI-Skripts, die Sie zur Integration des Cloud-Providers erstellen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenarbeit von Komponenten



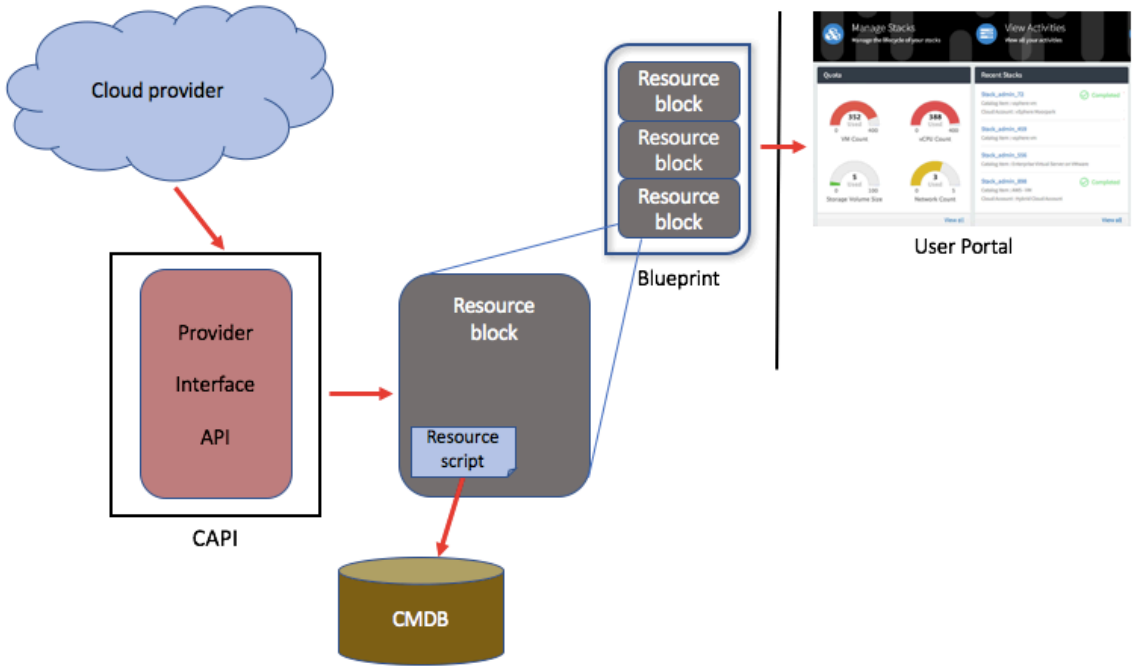
Benutzer können Katalogelemente, auch Stapel genannt, im Cloud-Katalog sehen. Ein Katalogelement basiert auf einer Blaupause, die wiederum aus miteinander verbundenen Ressourcenblöcken besteht.

1. Der Benutzer startet den Prozess, indem er einen Stapel anfordert. Die Anforderung ist der Vorgang **Bereitstellung** im System.
2. Das System führt die Schritte in der angegebenen Reihenfolge für den Vorgang **Bereitstellung** für die Ressourcenblöcke aus, die den Stapel bilden.
3. Jeder Schritt ruft CAPI auf, um die auszuführende Methode zu bestimmen und gleichzeitig Werte für erforderliche Parameter zu übergeben.
4. CAPI arbeitet mit der API des Cloud-Providers zusammen, um die tatsächliche Ressource bereitzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess-Flow beim Erstellen einer Ressource im Cloud-Provider



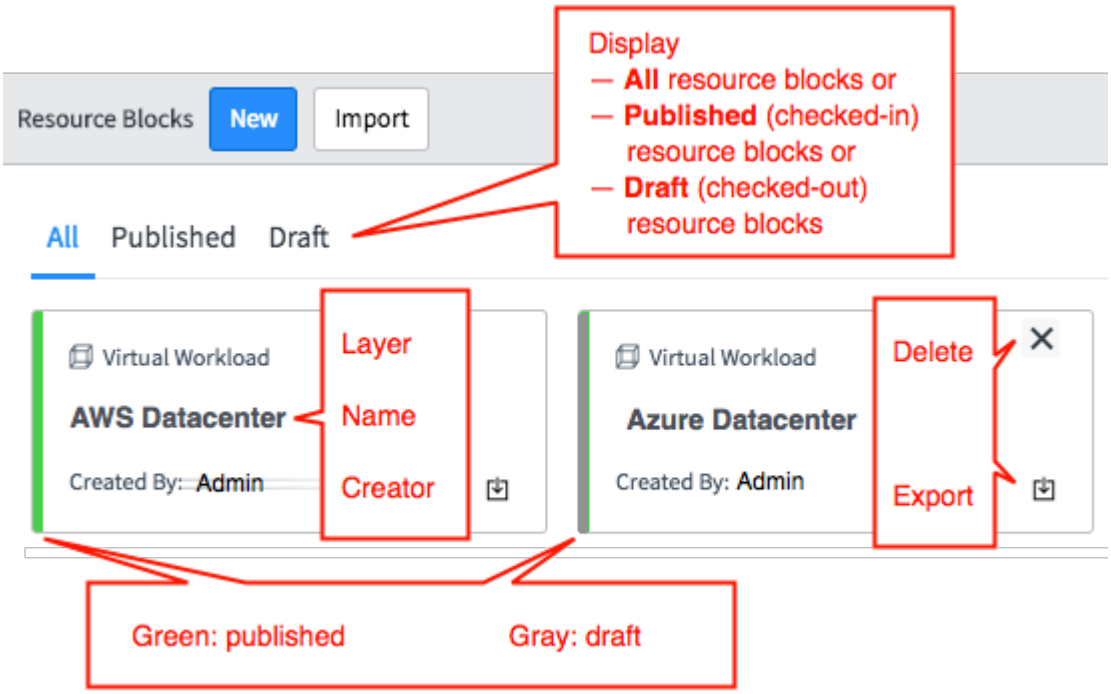
1. Der Cloud-Provider stellt die Ressource bereit und antwortet mit JSON.
2. Das System analysiert die Antwort im Ressourcenskript im Ressourcenblock.
3. Das System aktualisiert die CMDB. Beim Bereitstellen einer neuen Ressource erstellt das System ein CI in der richtigen Tabelle.
4. Der neue Stapel wird im Cloud-Benutzerportal für den zu verwaltenden Benutzer angezeigt.

Die Seite „Ressourcenblöcke“

Verwalten Sie Ressourcenblöcke auf der Seite „Ressourcenblöcke“. Öffnen Sie das Cloud-Administratorportal, und navigieren Sie dann zu **Entwurf** > **Ressourcenblöcke**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten der Seite „Ressourcenblöcke“



Benutzerdefinierten Ressourcenblock erstellen

Wenn die Blöcke im Basissystem nicht die erforderlichen Cloud-Ressourcen bereitstellen, können Sie einen benutzerdefinierten Ressourcenblock erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal** > **Entwurf** > **Ressourcenblöcke** Und klicken Sie auf **Neu** .
2. Geben Sie einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für den Ressourcenblock ein, und geben Sie dann die folgenden Einstellungen ein:

Ebene	Wählen Sie die Ebene aus, die den Typ des Ressourcenblocks darstellt: ○ **Anwendung**: Ressourcen, die Anwendungen sind. Beispielsweise könnte die Anwendung PetStore auf einer Tomcat- oder WebLogic-Plattform vorhanden sein. ○ **Plattform** : Ressourcen, die normalerweise auf einem virtuellen Server wie MySQL, Tomcat oder gehostet werden Apache. ○ **Logisches Rechenzentrum** : Ressourcen, die Rechenzentren ähnlich sind AWS, Azure, Oder vSphere.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	○ **Virtuelle Infrastruktur** : Ressourcen, die virtuell sind und dennoch Infrastruktur für die virtuelle Welt wie bereitstellen NetApp SVM, NetApp CDOT, CISCO ICF Cloud oder VMware NSX. ○ **Virtueller Workload**: Ressourcen, die in einem Rechenzentrum gehostet werden. Beispielsweise virtueller Server, Speichervolume, Netzwerk oder Gateway. **Hinweis:** ○ Anwendungen werden auf Plattformen bereitgestellt. ○ Plattformen werden in logischen Rechenzentren oder virtuellen Infrastrukturen bereitgestellt.
CI-Typ	Wählen Sie den CI-Typ in Ihrem aus CMDB Die der Ressourcenblock darstellt. Wenn der Anwender einen Stapel startet, werden die Cloud-Ressourcen bereitgestellt, und tatsächliche CIs, die für die Ressourcen erstellt werden, werden in erstellt CMDB In diesem CI-Typ. Wenn Sie beispielsweise „Speichervolume“ auswählen, erstellt das System einen Datensatz in der Tabelle „Speichervolume“ [cmdb_ci_storage_volume], wenn der Benutzer ein neues Volume bereitstellt. **Hinweis:** Jeder Ressourcenblock basiert auf einem CI-Typ aus dem CMDB. Stellen Sie sicher, dass nicht mehr als ein Ressourcenblock an einen CI-Typ gebunden ist.
Standardgastschnittstelle Schnittstelle erstellen	Wählen Sie die Gastschnittstelle aus, die die für die Ressource erforderlichen *Vorgänge* enthält. Später können Sie die für diese standardmäßige Gastschnittstelle zu verwendenden Vorgänge weiter definieren und auswählen. Das System bietet Ihnen eine Reihe von Standardvorgängen für jede Schnittstelle. Wenn ein anderer Ressourcenblock eine **Hostschnittstelle** spezifiziert (siehe die Beschreibung zum Feld „Hostschnittstelle“), die dem entspricht, was Sie hier im Feld **Gastschnittstelle** angeben, kann dieser Ressourcenblock ein potentieller Host für diesen Ressourcenblock sein. Wenn Sie das Kontrollkästchen **Schnittstelle erstellen** aktivieren, geben Sie einen Namen für die Gastschnittstelle ein. Das System erstellt die Gastschnittstelle, öffnet den Ressourcenblock, den Sie konfigurieren, im Ressourcenblockformular und listet die neue Schnittstelle in der zugehörigen Liste **Gastschnittstelle der Ressource** auf. Eine Beschreibung der Gastschnittstelle der Ressource finden Sie in den folgenden Schritten. Wenn Sie eine neue Gastschnittstelle erstellen, beachten Sie auch, dass andere Ressourcenblöcke die Schnittstelle verwenden können.
Hostschnittstelle	Wählen Sie die Schnittstelle aus, die der potenzielle Host dieses Ressourcenblocks anbieten muss. Jeder andere Ressourcenblock,

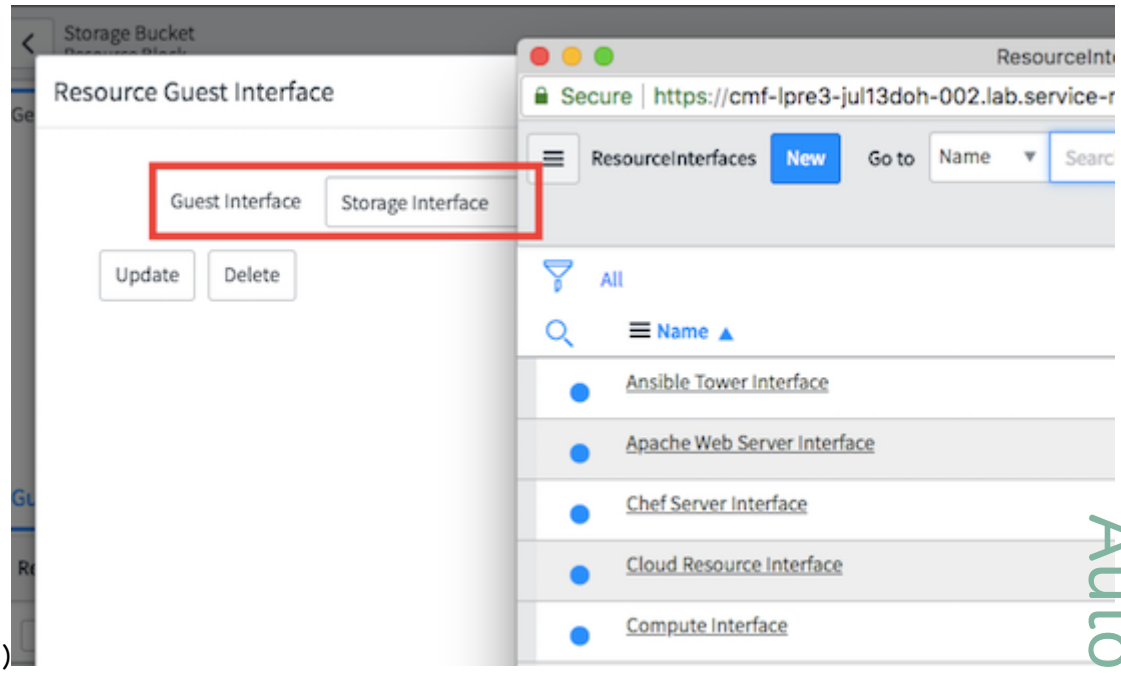
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	der eine standardmäßige Gastschnittstelle desselben Typs bietet, den Sie hier angeben, kann ein Host dieser Ressource werden. Später können Sie eine oder mehrere tatsächliche Hostressourcen auswählen. Beispiel: Standardmäßig AWS Der Ressourcenblock des Rechenzentrums gibt an **Berechnen** Schnittstelle als standardmäßige Gastschnittstelle. Das bedeutet AWS Das Rechenzentrum bietet an **Berechnen** Hostschnittstelle zu anderen Ressourcenblöcken, über die eine Verbindung mit hergestellt werden soll AWS Rechenzentrum. Geben Sie die **Computing**-Schnittstelle hier als Hostschnittstelle des Ressourcenblocks an, damit der Ressourcenblock nach anderen Ressourcenblöcken suchen kann, die die **Computing**-Schnittstelle als Gastschnittstelle verwendet. Da das AWS-Rechenzentrum die **Computing**-Schnittstelle als Gastschnittstelle verwendet, können Sie das AWS-Rechenzentrum später in der zugehörigen Liste „Hostressource“ als tatsächlichen Host auswählen. Andere Ressourcenblöcke, die die **Computing**-Schnittstelle anbieten, indem **Computing** als Gastschnittstelle angegeben wird, sind ebenfalls potenzielle Hosts für diesen Ressourcenblock. Sie müssen wissen, welche Schnittstellen die potenziellen Hostressourcen als Gastschnittstellen anbieten. Und bestimmen Sie, welche Vorgänge Teil dieser Gastschnittstellen sind.

3. Klicken Sie auf **Absenden**.
   Setzen Sie die Aktualisierung der Einstellungen in den zugehörigen Listen bei Bedarf fort.
4. **Wahlweise:** Führen Sie die folgenden Schritte aus, um eine weitere Gastschnittstelle hinzuzufügen.
   Sie können eine zusätzliche Gastschnittstelle angeben, die anderen Ressourcenblöcken angeboten wird. Beispielsweise kann ein Ressourcenblock „Rechenzentrum“ eine **Computing**-Schnittstelle, eine **Netzwerkservicecontainer**-Schnittstelle und eine **Firewall**-Schnittstelle zur Verwendung durch andere Ressourcenblöcke bieten.
   a. Klicken Sie bei **Gastschnittstelle** auf **Neu**.
   b. Wählen Sie im Feld **Gastschnittstelle** eine Schnittstelle aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional)

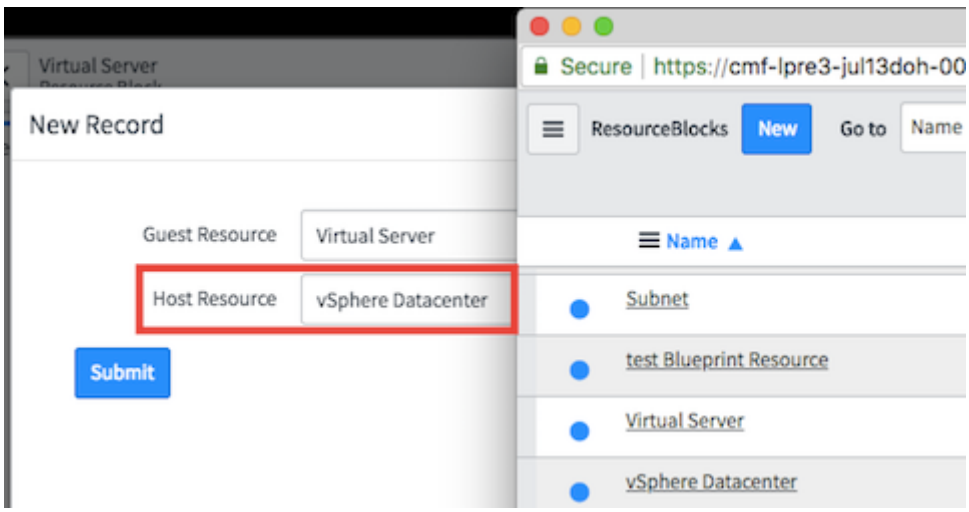


c. Klicken Sie auf **Absenden** oder **Aktualisieren**.

5. Geben Sie bei „Hostressource“ die Ressource an, die diesem Ressourcenblock als Host dienen kann, in der Regel diejenige, die die Schnittstelle anbietet, die Sie im Feld **Hostschnittstelle** angegeben.
Der ausgewählte Hostressourcenblock übernimmt die Bereitstellung dieses Ressourcenblocks. Beispiel: Die Hostressource ist ein Ressourcenblock „Virtueller Computer“, der einen Apache-Webserver hosten kann. Die Auswahl der Hostressource beschränkt die Optionen, die Benutzern bei der Auswahl eines Hosts angezeigt werden.

Example

Wählen Sie zum Beispiel **vSphere-Rechenzentrum** im Feld **Hostressource** aus, damit diese Ressource in einer VMWare Cloud gehostet werden kann.



Hinweis: Sie können nur die Hostressourcen auswählen, die die **Hostschnittstelle** unterstützen, die zuvor für diesen Ressourcenblock angegebenen wurden.

6. Wahlweise: Führen Sie die folgenden Schritte aus, um Bindungen hinzuzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Bindung ist ein weiterer Ressourcenblock, zu dem dieser Ressourcenblock eine Verbindung herstellen kann. Wählen Sie Ressourcenblöcke aus, die die gleiche **Gastschnittstelle** unterstützen, wie für diesen Ressourcenblock konfiguriert wurde.

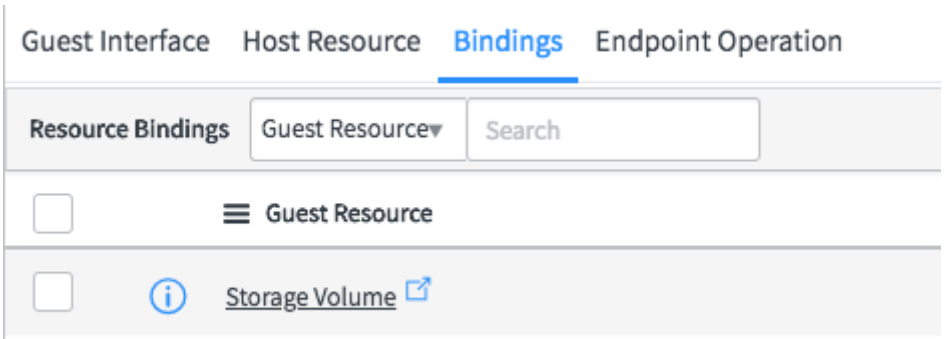
Beim Erstellen einer Blaupause können Sie eine Angehängt-Verbindung zwischen zwei Ressourcenblöcken hinzufügen, die mit dieser Bindung verbunden sind. Für die Konfiguration des Ressourcenblocks ist es wichtig, die Richtung der Bindung zu verstehen. Sie hängen einen virtuellen Server einem Netzwerk an, oder Sie hängen Speicher einem virtuellen Server an. Sie können diese Richtungen nicht umkehren.

a. Klicken Sie unter **Bindungen** auf **Neu**.

b. Wählen Sie im Feld **Hostressource** eine Ressource im Feld **Gastressource** aus.
Die Gastressource ist der Ressourcenblock, den Sie dem aktuellen Ressourcenblock anhängen.

c. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Example
Beispielsweise kann ein virtueller Server eine Verbindung mit virtuellem Speicher herstellen. Standardmäßig stellt das Basissystem einen Ressourcenblock „Virtueller Server“ mit einer Bindung zum Ressourcenblock „Speichervolume“ bereit, um diese Verbindung zu aktivieren.

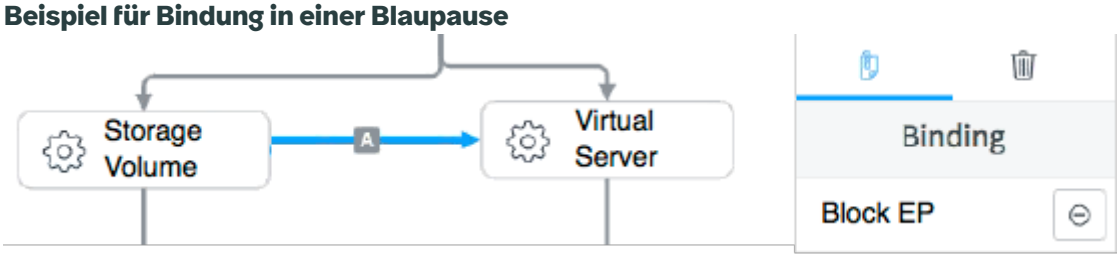


(Optional)

7. Führen Sie die folgenden Schritte aus, um Endpunktvorgänge zwischen den beiden zu bindenden Ressourcen zu konfigurieren.
Die Endpunkte rufen Vorgänge während der Bindung auf. Beispielsweise kann ein Speichervolume einen Endpunkt mit den erforderlichen Bedingungen und den auszuführenden Vorgängen angeben, um eine Verbindung zu einem virtuellen Server herzustellen. Der virtuelle Server muss auch eine Bindungsschnittstelle für das Speichervolume unterstützen.

Implementieren Sie einen Endpunkttyp wie **Block-EP**, damit der virtuelle Server den Endpunkt verwendet. Später, wenn Sie Blaupausen erstellen, erstellen Sie die Bindung zwischen dem Speichervolume und dem virtuellen Server.

Beispiel für Bindung in einer Blaupause



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie unter **Endpunktvorgänge**auf **Neu**.

b. Wählen Sie unter **Bindungsressource** den Ressourcenblock aus, der den Endpunkt dieses Ressourcenblocks verwendet.

c. Wählen Sie den Endpunkttyp aus, den die **Quellressource** darstellt.

d. Wählen Sie unter **Vorgangsimplementierung** die Implementierung aus, die den Vorgang ausführt, den Sie in dieser Endpunktzuordnung definieren.

e. Wählen Sie den **Typ** des Vorgangs aus, der für die Zuordnung ausgeführt werden soll.
Nur Vorgänge, die für den angegebenen **Endpunkt** geeignet sind, werden in der Liste angezeigt.

Ändern Sie nicht die Einstellungen in der **Quellressource**.

f. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Hostressource für einen Ressourcenblock angeben

Hosts, die die **Hostschnittstelle** eines Ressourcenblocks unterstützen, sind potenzielle Hosts für den Ressourcenblock. Sie verwenden die Einstellung **Hostschnittstelle**, um die Optionen, die dem Anforderer des Stapels bei der Auswahl eines Hosttyps angezeigt werden, weiter einzuschränken.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblöcke**an.
2. Wählen Sie den Ressourcenblock aus, und wählen Sie dann **Entwurf** im Formular **Ressourcenblöcke** aus:

3. Klicken Sie in der zugehörigen Liste **Hostressource** auf **Neu**.
Auf dem Formular **Ressourcenhost** sind die **Anwendung** und die **Gastressource** (der Ressourcenblock, den Sie derzeit konfigurieren) bereits angegeben.
4. Geben Sie die **Hostressource** an.
Beispielsweise können Sie für einen virtuellen Server **AWS-Rechenzentrum** oder **Azure-Rechenzentrum** als potenzielle Hosttypen auswählen.
5. Klicken Sie auf **Absenden**.

Geben Sie die Bindungen für Ressourcenblöcke an

Bindungen stellen Endpunktbeziehungen dar. Beispielsweise kann ein Speichervolume einen Endpunkttyp „Block-EP“ (cmdb_ci_endpoint_block) implementieren. Ein virtueller Server verwendet möglicherweise einen Endpunkt dieses Typs. Bindungen müssen die Gastschnittstelle unterstützen, die für den Ressourcenblock angegeben ist.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblöcke**an.
2. Wählen Sie den Ressourcenblock aus, und wählen Sie dann **Entwurf** im Formular **Ressourcenblöcke** aus:

3. Klicken Sie in der zugehörigen Liste **Ressourcenbindungen** auf **Neu**.
4. Auf dem Formular **Ressourcenbindung** sind die **Anwendung** und die **Gastressource** (der Ressourcenblock, den Sie derzeit konfigurieren) bereits angegeben.
   Geben Sie die **Bindungsressource** an.
5. Klicken Sie auf **Absenden**.

Endpunkt-Vorgangszuordnung konfigurieren

Sie können die Endpunktzuordnung eines Speichervolume konfigurieren, um eine Verbindung zu einer Ressource herzustellen.

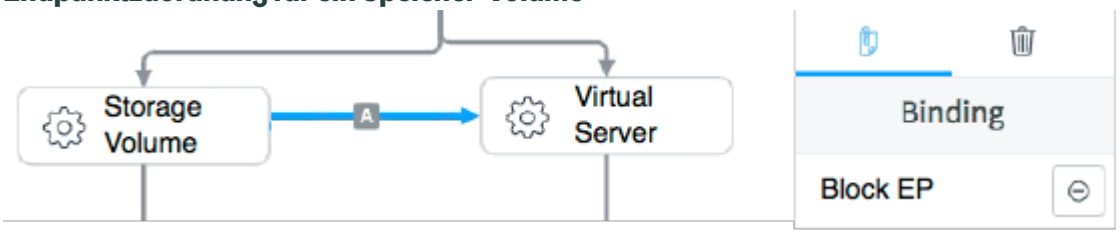
Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Im folgenden Beispiel gibt die für ein Speichervolume konfigurierte Endpunktzuordnung die Bedingungen, die erfüllt sein müssen, und den Vorgang, der ausgeführt werden soll, an, um eine Verbindung zu einer Ressource herzustellen (im Beispiel ein virtueller Server), die eine Bindungsschnittstelle zu einem Speichervolume unterstützt. Das Speichervolume implementiert den Endpunkt (im Beispiel vom Typ „Block-EP“), und der virtuelle Server verwendet den Endpunkt:

Endpunktzuordnung für ein Speicher-Volume



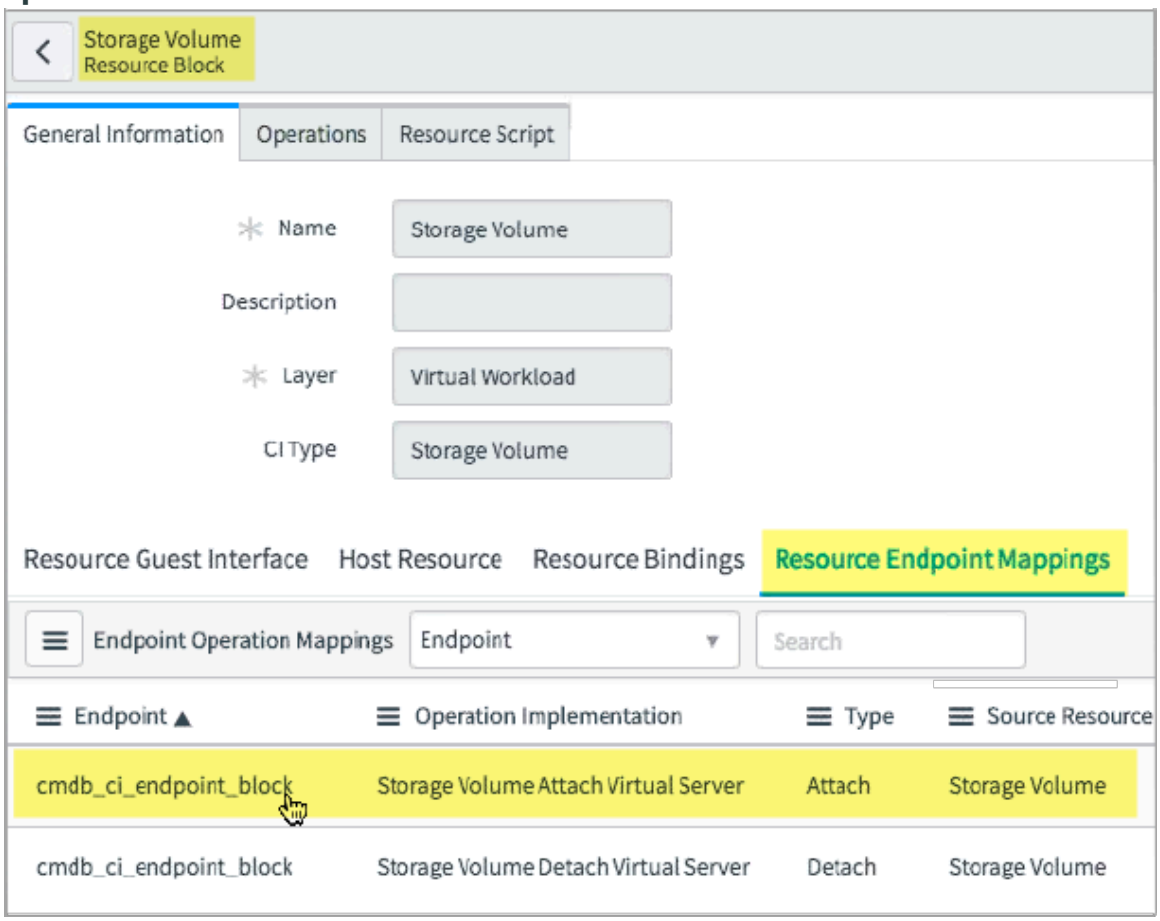
Die Einstellungen in der zugehörigen Liste **Ressourcenendpunkt-Zuordnungen** im Beispiel geben die Bedingungen und eine Aktion an:

- Für einen Ressourcenblock, der eine Bindungsschnittstelle für ein **Speichervolume** unterstützt
- Für eine **Quellressource** mit einem **CI-Typ** von **Speichervolume**
- Mit einem **Endpunkt** vom Typ **Block-EP** (cmdb_ci_endpoint_block)

Verwenden Sie den Vorgang **Anhängen**, um die Verbindung zu implementieren. Verwenden Sie die angegebene **Vorgangsimplementierung**, um den Vorgang **Anhängen** auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume für einen Ressourcenblock



Prozedur

1. Öffnen Sie beim Konfigurieren eines Ressourcenblocks die zugehörige Liste **Ressourcenendpunkt-Zuordnung**, klicken Sie auf **Neu**, und geben Sie dann die folgenden Einstellungen an:

Bindungsressource	Ressourcenblock, der den **Endpunkt** verwendet, den die **Quellressource** darstellt.
Endpunkt	Endpunkttyp, den die **Quellressource** darstellt.
Typ	Typ des Vorgangs, der für die Zuordnung ausgeführt werden soll. Nur Vorgänge, die für den angegebenen **Endpunkt** geeignet sind, werden in der Liste angezeigt.
Vorgangsimplementierung	Implementierung, die zum Ausführen des Vorgangs aufgerufen wird, den Sie in dieser Zuordnung definieren.
Applikation	Schreibgeschützt. Cloud Provisioning and Governance-Anwendung.
Quellressource	Ressourcenblock, der einen **Endpunkt** des von Ihnen angegebenen Typs darstellen kann. Üblicherweise muss diese Einstellung nicht geändert werden.

2. Wiederholen Sie diese Vorgehensweise für die erforderliche Anzahl an Zuordnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabeparameter für Ressourcenblöcke konfigurieren

Sie können Vorgänge für jede Schnittstelle eines Ressourcenblocks konfigurieren, indem Sie Eingabeparameter, Schritte und Ausgabeattribute angeben. Eingabeparameter enthalten Werte, die das System zum Identifizieren und Verwalten einer virtuellen Ressource benötigt, z. B. das Rechenzentrum und die Ressourcengruppe, in der sich die Ressource befindet.

Vorbereitungen

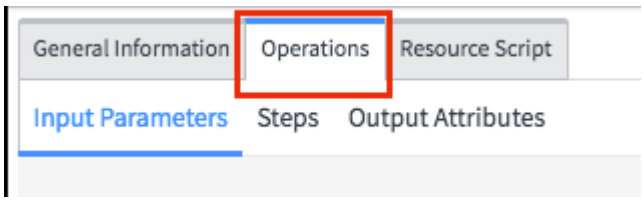
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Das System ordnet dem Ressourcenblock automatisch Standardvorgänge aus der Cloud API (CAPI) zu, wenn Sie ihm Schnittstellen hinzufügen. Es stellt auch Standardeingabeparameter für die einzelnen Vorgänge bereit.

Prozedur

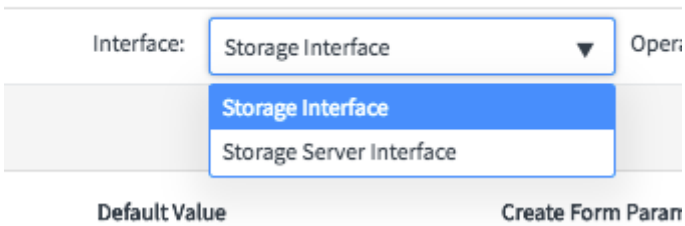
1. Öffnen Sie einen Ressourcenblock, und klicken Sie dann auf die Registerkarte **Vorgänge**.



Die Unterregisterkarte **Eingabeparameter** wird standardmäßig angezeigt.

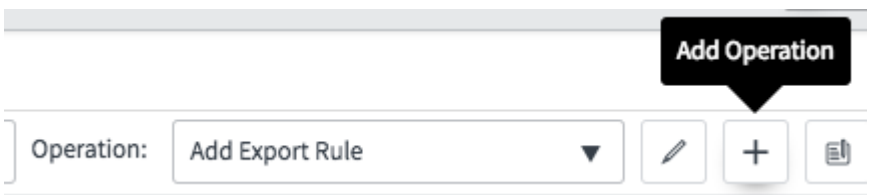
2. Wählen Sie die Schnittstelle aus der Auswahlliste **Schnittstelle** aus.

Die Schnittstellen in dieser Auswahlliste sind von der Liste **Gastschnittstelle der Ressource** auf der Registerkarte **Allgemeine Informationen** abgeleitet, die Sie bereits beim Erstellen eines Ressourcenblocks konfiguriert haben.



3. Wählen Sie den Vorgang aus, für den Sie die Eingabeparameter ändern möchten. Sie können auch einen neuen Vorgang erstellen.

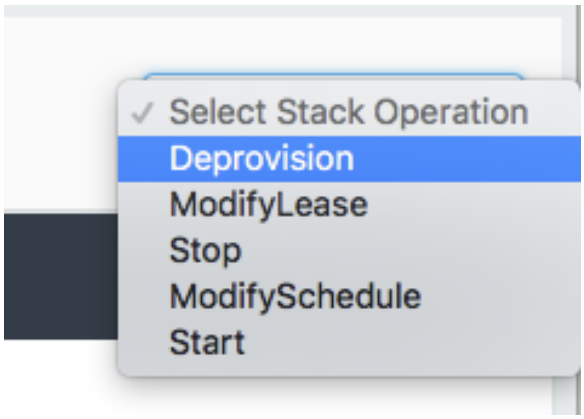
a. Klicken Sie auf das Symbol **Vorgang hinzufügen**.



b. Füllen Sie das Formular aus (siehe Tabelle):

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ein.
Vorgangstyp	Wählen Sie den Vorgangstyp aus der Auswahlliste aus.
Zugriffstyp	Wählen Sie **Öffentlich** aus, um den Ressourcenblockvorgang über das Katalogbestellformular verfügbar zu machen, wenn ein Benutzer einen Stapel verwaltet, dessen Besitzer er ist. Die tatsächlichen Vorgänge werden in einer Liste auf dem Katalogbestellformular angezeigt:  Wählen Sie **Privat** aus, um zu verhindern, dass der Vorgang verwendet wird, wenn ein Benutzer einen Stapel startet. Diese Einstellung gilt auf Katalogelementebene und nicht auf der Ebene des gesamten Stapel. Sie können den Zugriffstyp für den gesamten Stapel beim Konfigurieren von Blaupausen steuern. Beispiel: Sie möchten den Vorgang Bereitstellung aufheben für eine einzelne VM als privat markieren, aber nicht für den gesamten Stapel. Dies ermöglicht dem Benutzer, die Bereitstellung aller Elemente auf einmal aufzuheben, und verhindert, dass der Benutzer nur die Bereitstellung der VM aufhebt.

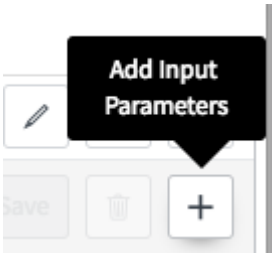
c. Klicken Sie auf **Absenden**.

4. Konfigurieren Sie die Eingabeparameter, um eine Möglichkeit zur Eingabe der Elemente bereitzustellen, die Sie zum Ausführen des ausgewählten Vorgangs benötigen.

Wenn Sie beispielsweise einen Bereitstellungsvorgang für eine AWS-Ressource hinzufügen, benötigen Sie mindestens den Parameter „CloudAccount“ und den Parameter „Standort“, um den Vorgang auszuführen. Sie müssen die Provider API kennen, um zu wissen, was an sie übergeben werden soll. Wenn Sie beispielsweise einen Bereitstellungsvorgang für einen S3-Bucket in AWS hinzufügen möchten, müssen Sie die zulässigen AWS-Vorgänge für Buckets und die Anforderungselemente für Dinge wie das Erstellen eines Bucket (den PUT-Bucket-Vorgang) kennen. Sie finden diese Ressourcen normalerweise in der AWS- und der Azure-Dokumentation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf das Symbol **Eingabeparameter hinzufügen**.



b. Fügen Sie den **Namen** des Parameters hinzu, den Sie von der Cloud-Provider API erhalten haben.
In diesem Beispiel können Sie `CreateBucketConfiguration` für einen AWS S3-Bucket hinzufügen.

c. Wählen Sie in der Spalte **Datenquelle** den Typ des Eingabeparameters aus, den Sie konfigurieren. Dieser Wert gibt die Quelle oder den Standort an, aus dem der Parameterwert stammt:

- **Text**: Ein Textwert, den der Benutzer übergibt.
- **Pools**: Die Abfrage, die für einen Pool ausgeführt werden soll, um einen Wert zu erhalten. Der Pool **Datenquellenwert** muss der folgenden Konvention entsprechen: `ServiceNow::Pools::PoolName.Pool-Filter-Name`. Weitere Informationen zu Pools finden Sie unter Pools und Filter für Cloud Provisioning.
- **CSVList**: Werte aus einer kommagetrennten Werteliste, die Sie in den **Datenquellenwert** eingeben.
- **Array**: Ein Array von Werten. Sie können ihm programmgesteuert ein Array in JavaScript senden. Das Format ist wie folgt: `['abc','def']`.
- **FormData**: Daten, die von dem in der Blaupause konfigurierten Formular übermittelt wurden.
- **ResourceScript**: Ein Ausdruck, der einen Wert übergibt. Der Ausdruck muss im Feld **Zuordnung** dieser Konvention entsprechen:

  `$(Script:script-name.function[arg1=${Übergabewert},arg2=${Übergabewert}])`

- **TLR**: Der Wert, der vom Ressourcencontainer der obersten Ebene über diesem Ressourcenblock in der Blaupause geerbt wurde.

d. Klicken Sie auf **Speichern**.

e. In der Spalte **Zuordnung** können Sie sich die automatisch generierten Zuordnungswerte ansehen. Zuordnungen geben an, wo die Informationen im System abgerufen werden. Sie müssen die Zuordnungswerte nur für Parameter des Typs **ResourceScript** ändern, wo Sie den Ausdruck eingeben müssen.

f. Geben Sie in der Spalte **Standardwert** einen Wert ein, den das System verwenden soll, wenn der Benutzer keinen Wert übergibt oder wenn Sie nichts in den **Datenquellenwert** eingegeben haben.

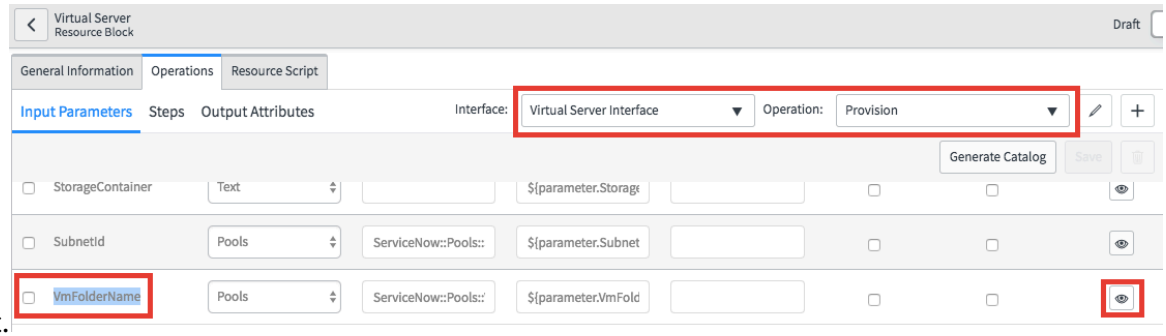
g. Wählen Sie **Formular erstellen** aus, um dieses Attribut im Bestellformular verfügbar zu machen, das dem Benutzer beim Bereitstellen des Stapelelements angezeigt wird.
Sie können auch **Obligatorisch** auswählen, um die Eingabe des Benutzers zu erzwingen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Klicken Sie in der Spalte **Eingeschränkt auf** auf das Eingeschränkt-Symbol ( ), und wählen Sie dann einen Ressourcenblock aus, um das Attribut einzuschränken, das an einen bestimmten Host übergeben werden soll.

In diesem Beispiel konfigurieren Sie einen Ressourcenblock für einen virtuellen Server in vSphere, für den der Name des VM-Ordners (dargestellt durch das Attribut VmFolderName) erforderlich ist. Für andere Rechenzentrumstypen ist der Name des VM-Ordners nicht erforderlich. Daher können Sie VmFolderName auf den Ressourcenblock des vSphere-Rechenzentrums beschränken.

Dieses Bild zeigt, wie das Attribut „VMFolderName“ auf das vSphere-Rechenzentrum beschränkt ist.



Vorgangsschritte einem Ressourcenblock hinzufügen

Nachdem Sie Vorgänge und Eingabeparameter für Ihren Ressourcenblock konfiguriert haben, fügen Sie für jeden Vorgang Schritte hinzu, um dem System mitzuteilen, welche Cloud API (CAPI) aufgerufen werden soll. Jeder Schritt ist ein eigener Aufruf von CAPI.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Klicken Sie im Ressourcenblock unter **Vorgänge** auf die Unterregisterkarte **Schritte**.
2. Klicken Sie auf **Schritt hinzufügen**.
3. Füllen Sie die Formularfelder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus: ○ **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen. ○ **Hostressourcenvorgang aufrufen**: Wählen Sie diese Option aus, um einen Vorgang (auch Vorgangssignatur genannt) aus der Hostschnittstelle zu verwenden, die Sie bereits für diesen Ressourcenblock angegeben haben. ○ **Skript aufrufen**: Wählen Sie diese Option aus, um eine Methode aus einer vorhandenen MID Server-Skripteinbindung aufzurufen. ○ **Flow aufrufen**: Wählen Sie diese Option aus, um Subflows aus einer Liste aktiver Subflows aufzurufen.
API-Anbieter [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den AWS-Provider bereit, der über Produkte verfügt, von denen einige Provider-Namen aufweisen. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. Beispielsweise stellt die **Blob-Speicher-Schnittstelle** die **CreateContainer**-Schnittstelle bereit, die das System während der Bereitstellung verwendet.
API-Methode [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **CreateContainer** erforderlich, um Speicher bereitzustellen.
CAPI-Version [Vorgangstyp = Cloud API aufrufen]	Geben Sie eine Version für die CAPI API ein.
Hostschnittstelle [Vorgangstyp = Hostressourcenvorgang aufrufen]	Wählen Sie die Schnittstelle aus, über die ein Vorgang aufgerufen werden soll. Sie können nur die Schnittstelle auswählen, die Sie auf der Registerkarte **Allgemeine Informationen** des Ressourcenblocks konfiguriert haben. Um die Schnittstelle zu ändern, navigieren Sie zurück zur Registerkarte **Allgemeine Informationen** und wählen Sie einen anderen Wert im Feld **Hostschnittstelle** aus.
Schnittstellenvorgang	Wählen Sie den Vorgang der Hostschnittstelle aus. Wenn Sie beispielsweise die Schnittstelle **Speicherserver** auswählen, können Sie alle Vorgänge in dieser Schnittstelle aufrufen, z. B. `CreateStorageVolume`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
[Vorgangstyp = Hostressourcenvorgang aufrufen]	
Skripts [Vorgangstyp = Skript aufrufen]	Geben Sie das Skript ein, das Sie aufrufen möchten, und geben Sie auch die Methode im Skript an. Verwenden Sie folgende Syntax: `Skriptname.Methode`.
Flow [Vorgangstyp = Flow aufrufen > Subflow]	Wählen Sie den Subflow aus der Liste „Subflows“ aus. Wenn Sie beispielsweise einen Subflow für die Terraform Enterprise-Bereitstellung auswählen, können Sie den vorhandenen Subflow einfach wiederverwenden, um die Eingaben und Ausgaben entsprechend zu füllen.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

Bei der Azure-API und der Methodenzuordnung „CreateNode“ können Sie sehen, dass der Endpunktvorgang ein Skript ist. Es ruft die MID Server-Skripteinbindung auf, die Ihnen die Funktion *`createNode()`* anzeigt. Diese Funktion verwendet die Skripteinbindung *`AzureComputeVirtualMachine`*. Nehmen Sie sich Zeit, um sich diese Skripteinbindung anzusehen und sie zu verstehen.

4. Klicken Sie auf **Absenden**.

   Die Registerkarten **Eingabe** und **Antwortprozessor** werden für den Schritt angezeigt.

5. Konfigurieren Sie auf der Registerkarte **Eingabe** die CAPI-Vorgangseingaben.

   Öffnen Sie auf der CAPI-Schnittstelle (in diesem Fall die Schnittstelle **Blob-Speicher**) die Methode *`CreateContainer`*. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

   Denken Sie daran, dass die Parameter auf der Registerkarte **Eingabeparameter** durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie dazu **Zuordnung** Wert aus **Eingabeparameter** Registerkarte in **Wert** Feld auf der **Schritte** > **Eingabe** Registerkarte

   Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: `${parameter.arg1}`.

6. Wenn für nachfolgende Schritte in diesem Vorgang oder nachfolgenden Vorgängen die Übergabe von Parameterwerten aus diesem Schritt erforderlich ist, konfigurieren Sie Ausgabeattribute.

   Beispielsweise kann der Vorgang der Bereitstellung für einen virtuellen Server ein Ausgabeattribut für die Netzwerkschnittstellen-ID und ein anderes für die Knoten-ID bereitstellen. Wenn der Cloud-Provider die Antwort sendet, werden die tatsächliche ID des Netzwerks und die des Knotens aus der Antwort analysiert und in den Ausgabeattributen gespeichert. Nachfolgende Schritte können dann die IDs zum Ausführen von Aktionen verwenden.

   a. Klicken Sie auf die Registerkarte **Ausgabeattribute**.

   b. Geben Sie Code in der folgenden Schreibweise ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
 "Attribute": "${Value}"
}
```

Der Wert stammt dabei aus einer Zuordnung zur Schnittstelle und zum Vorgang.

Sehen Sie sich als Beispiel das folgende Ausgabeattribut an:

```
{
 "NodeId": "${Compute Interface.CreateNode.Output.resp.nodeId}"
}
```

- `NodeId` ist das Attribut.
- `Compute Interface` gibt die Schnittstelle an.
- `CreateNode` ist der Name der Methode, die den Knoten erstellt.
- `Output.resp` ist ein obligatorischer Teil der Syntax.
- `nodeId`

Ressourcenvorgangsschritt zum Aufrufen eines Subflows hinzufügen

Rufen Sie einen Subflow auf, indem Sie einer Ressource einen Vorgangsschritt hinzufügen und ihn mit einem neuen oder vorhandenen Subflow verknüpfen.

Vorbereitungen

Stellen Sie sicher, dass Orchestration Anwendung ist installiert.

Erforderliche Rolle: Cloud-Benutzer, -Designer oder Administrator

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Ressourcenblöcke**an.
2. Legen Sie den Ressourcenblock auf fest **Entwurf** geben sie den status an, indem Sie die Veröffentlichung umschalten und dann auswählen **Vorgänge** > **Schritte** > **Schritt hinzufügen**an.
   Das Formular Vorgangsschritte hinzufügen wird angezeigt.
3. Von **Vorgangstyp** Liste, wählen Sie aus **Rufen Sie Den Flow Auf** .
4. Von **Inhaltstyp** Liste, wählen Sie aus **Subflow** .

   Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

5. Wählen Sie in der Nachschlageliste **Flow/Subflow** einen aktiven Subflow aus.
6. **Wahlweise:** Geben Sie eine Bedingung im Feld **Bedingung** an.
7. Wählen Sie **Absenden**.
   Der Subflow-Vorgangsschritt wird dem Ressourcenblock angefügt und auf der Seite angezeigt. Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden auf der Registerkarte **Eingabe** automatisch ausgefüllt.
8. In **Eingaben** Wählen Sie die Unterregisterkarte aus + Symbol zum Hinzufügen eines neuen Schrittparameters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Fügen Sie dem Subflow das folgende Schlüssel-Wert-Paar hinzu.

Schlüssel	Wert
flowcorrelationid	$(Script:CMPFlowStepHandler.generateCorrelationId)

9. Wählen Sie aus **Antwortprozessor** Registerkarte und dann das Plus-Symbol auswählen.
Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.
10. Wählen Sie in der Liste **Skriptname** ein Skript für den Antwortprozessor aus.
Damit ein Skript in der Liste **Skriptname** angezeigt wird, muss es bereits auf der Registerkarte **Ressourcenskript** erstellt worden sein. Weitere Informationen finden Sie unter Konfigurieren Sie einen Antwortprozessor .
11. Wählen Sie **Absenden**.
12. Setzen Sie den Ressourcenblock auf den Status **Veröffentlichen**, um Ihre Änderungen zu übernehmen und den Ressourcenblock zu veröffentlichen.

Nächste Maßnahme
Erstellen Sie eine Antwortaktion für Cloud Provisioning and Governance

Cloud Provisioning and Governance-Ressourcenblöcke mit einem Überschreibungsvorgang erweitern

Sie können Ihre vorhandene Gastschnittstelle erweitern, um einen neuen Vorgang zu erstellen. Sie können auch eine neue Gastschnittstelle mit eigenen Vorgängen, Parametern und Eingaben erstellen.

Vorbereitungen
Machen Sie sich mit den Eingabeparametern, Vorgängen und Schritten für Ressourcenblöcke vertraut. Weitere Informationen finden Sie unter Eingabeparameter für Ressourcenblöcke konfigurieren und Vorgangsschritte einem Ressourcenblock hinzufügen.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Cloud Provisioning and Governance-Anwendung ist mit mehreren nützlichen Ressourcenblöcken gebündelt. Erstellen Sie Erweiterungen für die Schnittstellen vorhandener Ressourcenblöcke, um diesen Ressourcenblöcken mehr Funktionalität hinzuzufügen. Nachdem Sie eine Schnittstellenerweiterung erstellt haben, verwenden Sie sie in einer Blaupause, um einen benutzerdefinierten Vorgang auszuführen. Wenn Ihnen beispielsweise die Art der Bereitstellung eines virtuellen Servers nicht gefällt, erweitern Sie die Ressourcenblockschnittstelle des virtuellen Servers, indem Sie Vorgänge hinzufügen oder vorhandene Vorgänge überschreiben.

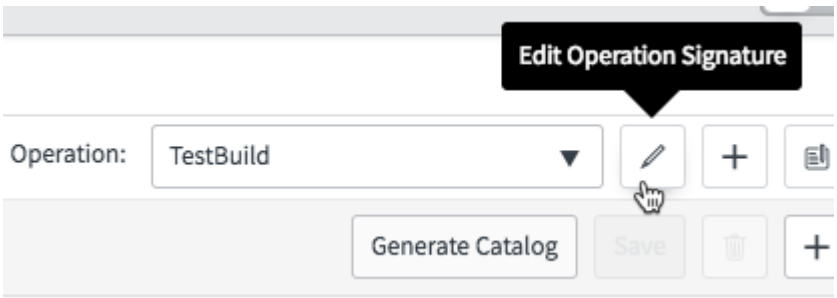
Hinweis: Vorgänge in Ressourcenblöcken werden auch *Vorgangssignaturen* genannt.

Prozedur
1. Öffnen Sie einen Ressourcenblock.
2. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**.
3. Klicken Sie auf die Registerkarte **Vorgänge**.
4. Klicken Sie auf das Symbol **Vorgang überschreiben**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie eine vorhandene Gastschnittstelle aus, oder aktivieren Sie das Kontrollkästchen **Neu erstellen**, um eine neue Gastschnittstelle zu erstellen.
6. **Wahlweise:** Wenn Sie eine Schnittstelle erstellen, geben Sie einen Namen in das Feld **Schnittstelle** ein.
7. Klicken Sie auf **Absenden** oder **Aktualisieren**.
   Der neue Vorgang wird in der Liste **Vorgang** angezeigt. Wenn Sie eine neue Schnittstelle erstellen, wird sie in der Liste **Schnittstelle** angezeigt.
8. Konfigurieren Sie die erforderlichen Eingabeparameter, Schritte und Ausgabeattribute für Ihre neue Gastschnittstelle.
9. So bearbeiten Sie den Vorgang oder ändern den Zugriffstyp:

   a. Klicken Sie auf das Symbol **Vorgangssignatur bearbeiten**.



   b. Ändern Sie bei Bedarf den **Vorgangstyp**, und fügen Sie unten Eingabeparameter hinzu, bearbeiten oder entfernen sie.

   c. Wenn der Blaupausendesigner den Vorgang nur dann direkt an der Ressource ausführen soll, wenn sie instanziiert wird, wählen Sie **Privat** als **Zugriffstyp** aus.

   d. Klicken Sie auf **Aktualisieren**.

10. Nach Abschluss der Anpassungen stellen Sie den Umschalter auf **Veröffentlicht**.
11. Navigieren zu **Cloud-Adminportal** > **Entwurf** > **Blueprints**an.
12. Führen Sie die Schritte in Cloud Provisioning-Blaupause erstellen aus, um eine Blaupause hinzuzufügen.
13. Klicken Sie auf **Vorgänge**, und klicken Sie im Ressourcenblock auf den Vorgang, den Sie ändern möchten.
    Die Standardschnittstelle des Ressourcenblocks wird in der rechten Spalte angezeigt.
14. Klicken Sie auf das Symbol **Ressourcenvorgang bearbeiten** (Bleistift), um die von Ihnen erstellte Schnittstellenerweiterung anzuwenden.
15. Klicken Sie auf **Absenden**.
    Die Blaupause wird mit der benutzerdefinierten Schnittstellenerweiterung ausgeführt.

Ergebnis

Nachdem Sie diesen Ressourcenblock einer Blaupause hinzugefügt haben, können Sie die hinzugefügten Parameter anpassen.

Ressourcenblock ein Ressourcenskript hinzufügen

Ein Ressourcenskript wird während der Bereitstellung auf einer Ressource ausgeführt oder gibt Daten an die CMDB zurück, nachdem eine Ressource bereitgestellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblöcke**an.
2. Öffnen Sie den Ressourcenblock, und legen Sie ihn auf den Status **Entwurf**

fest.
3. Geben Sie auf der Registerkarte **Ressourcenskript** einen eindeutigen und aussagekräftigen **Namen** ein, und definieren Sie dann das Skript:

Skript	Skriptcode.
Typ	Skripttyp: ○ Instanzskript: JavaScript, das einen Vorgang für die Instanz ausführt (z. B. einen Subflow). ○ PowerShell-Skript ○ Python-Skript ○ Antwortprozessor: Konvertiert Rückgabedaten von der externen Cloud API an die Vorgangsimplementierung in ein Format, das von der CMDB akzeptiert wird. ○ Shell-Skript

4. Klicken Sie auf **Absenden**.
Fügen Sie so viele Skripts wie nötig hinzu.

Antwortprozessor konfigurieren

Konfigurieren Sie einen Antwortprozessor für die Verarbeitung von Antworten von Rechenzentren.

Vorbereitungen

- Die CI-Klassentypen für Ihre Ressourcen müssen bereits in der CMDB vorhanden sein. Wenn Sie benutzerdefinierte Produkte oder Provider in CAPI erstellt haben, müssen Sie auch benutzerdefinierte CI-Typen erstellen, damit der Antwortprozessor CIs identifizieren kann. Informationen zum Erstellen von CI-Typen finden Sie unter Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Nachdem jeder Schritt abgeschlossen ist, sendet das Rechenzentrum eine Antwort an die ECC-Warteschlange für den MID-Server. Beispiel: Wenn ein Benutzer einen virtuellen Server in einem AWS-Rechenzentrum bereitstellt, sendet AWS Informationen über den neuen virtuellen Server an die ECC-Warteschlange. Das System muss in der CMDB ein CI für den virtuellen Server erstellen. Dazu wird ein Antwortprozessor verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alternativ dazu können Sie die musterbasierte gezielte Erkennung verwenden, um Antworten aus den Rechenzentren zu verarbeiten. Weitere Informationen finden Sie unter Musterbasierte gezielte Erkennung.

Hinweis: Der Ressourcentyp, für den Sie das Antwortprozessorskript hinzufügen, muss in der Tabelle [sn_CAPI_resource_type] vorhanden sein.

Prozedur

1. Öffnen Sie einen Ressourcenblock, und klicken Sie auf die Registerkarte **Ressourcenskript**.
   Stellen Sie sicher, dass sich der Ressourcenblock nicht im Status „veröffentlicht“ befindet.
2. Klicken Sie auf **Neu**.
3. In **Name** Geben Sie den Namen für das Ressourcenskript ein.
4. Geben Sie ein Skript in das Feld **Skript** ein.
5. Klicken Sie auf **Absenden**.
6. Klicken Sie im Ressourcenblock auf die Registerkarte **Vorgänge**.
7. Klicken Sie auf die Unterregisterkarte **Schritte**.
8. Klicken Sie auf einen Schritt.
9. Klicken Sie bei dem Schritt auf die Registerkarte **Antwortprozessor**.
10. Klicken Sie auf das Hinzufügen-Symbol (+).
11. Wählen Sie im Feld **Skriptname** den Prozessor aus, den Sie gerade erstellt haben.
12. Klicken Sie auf **Absenden**.
    Das Antwortprozessorskript kann die Antwort des Cloud-Providers für den CI-Typ des Ressourcenblocks verarbeiten.

Antwortprozessor für Subflow ausführen

Führen Sie einen Antwortprozessor für einen Subflow aus, um die Subflow-Daten zurück in ein Konfigurationselement (Configuration Item, CI) abzurufen. Der Antwortprozessor erfasst die Daten und sendet die Daten an die CMDB, die die Daten wiederum in ein CI ablegt.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie einen Antwortprozessor für einen Subflow ausführen, müssen Sie einen Subflow erstellen, den Subflow an einen Ressourcenblock-Vorgangsschritt anhängen und dann den Katalog generieren. Um eine Antwort vom Subflow an zurückzugeben Cloud Provisioning and Governance Anwendung muss der Subflow einen Datensatz in der Tabelle „sn_CMP_Flow_result“ mit den entsprechenden Details wie folgt erstellen.

```
flow_type         : 'sys_flow_context'
flow_correlation_id : flowcorrelationid (This variable must be present in the Resource Block as mentioned here Ressourcenvorgangsschritt zum Aufrufen eines Subflows hinzufügen.
flow_output       : String that will be processed by Response Processor
flow_error        : Error string if there is any error
error_detail      : Error detail string if there is any error
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Ressourcenblöcke**an.
2. Öffnen Sie einen Ressourcenblock, der sich im Entwurfsstatus befindet, und navigieren Sie zu **Vorgänge** **Schritte** .
3. Wählen Sie Aus **Schritt Hinzufügen** .
   Das Dialogfeld „Vorgangsschritte hinzufügen“ wird angezeigt.
4. Fügen Sie einen Workflow-Vorgangsschritt hinzu.
   Weitere Informationen finden Sie unter Vorgangsschritte einem Ressourcenblock hinzufügen.
   Der Workflow-Vorgangsschritt wird dem Ressourcenblock angefügt und auf der Seite angezeigt. Alle dem Workflow zugeordneten Eingabeparameter werden auf der Registerkarte **Eingabe** angezeigt.
5. Wählen Sie Aus **Katalog Generieren** .
   Der Workflow wird im Cloudbenutzerportal als Vorgang angezeigt. Wählen Sie den Workflow in der Auswahl **Vorgang auswählen** aus, um den Vorgang auszuführen. Der Status des Vorgangs ist auf der Unterregisterkarte „Vorgang nachverfolgen“ sichtbar.
6. Wählen Sie aus **Antwortprozessor** Registerkarte und dann das Plus-Symbol auswählen.
   Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.

7. Wählen Sie in der Liste **Skriptname** ein Skript für den Antwortprozessor aus.
   Damit ein Skript in der Liste **Skriptname** angezeigt wird, muss es bereits auf der Registerkarte **Ressourcenskript** erstellt worden sein.
8. Wählen Sie **Absenden**.
   Das Skript wird auf der Registerkarte **Antwortprozessor** angezeigt. Sie können das Skript öffnen und ändern.

Beispiel für einen Antwortprozessor für einen virtuellen Server

Das Skript *Create_Virtual_Server_Response_Processor*, das standardmäßig in Cloud Provisioning and Governance verfügbar ist, ist der Antwortprozessor, der die Erstellung von AWS-VM-CIs verarbeitet.

Virtuellen Server erstellen

Das Ressourcenprozessorskript „Create_Virtual_Server_Response_Processor“ ist standardmäßig im Ressourcenblock „Virtueller Server“ verfügbar. Seine Aufgabe besteht darin, einen Datensatz für einen virtuellen Server in der Tabelle „VM-Instanz“ [cmdb_ci_vm_instance] zu erstellen, wenn ein neuer virtueller Server bereitgestellt wird.

Alle Antwortprozessoren haben diese erste Zeile mit diesen allgemeinen Parametern:

```
function processResponse(response, cloudServiceAccountId, ldc, correlationId,step,
 requestorContext) {
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch werden die Antwort des Cloud-Providers und die wichtigen Informationen, wie z. B. die Konto-ID, abgerufen, die erforderlich sind, damit das System das neue CI erstellen kann. Alle diese Parameter sind für alle Antwortprozessoren erforderlich.

Zeile 10 wandelt die Antwort in JSON um, damit sie vom System verarbeitet werden kann. Die Informationen werden in der Variablen „vmResponse“ gespeichert:

```
var vmResponse = global.JSON.parse(response);
```

Immer wenn Sie einen Antwortprozessor erstellen oder bearbeiten, müssen Sie wissen, welche Eingaben für den CI-Typ erforderlich sind. Zeile 11 verarbeitet eine der erforderlichen Eingaben, die Hardware-ID, die für den CMDB-Datensatz erforderlich ist:

```
var hardwareId = vmResponse.hardwareId;
```

Zeile 39 zeigt die Informationen an, die das System benötigt, um den neuen virtuellen Server und zugehörige CIs zu identifizieren, damit die Informationen in der CMDB abgelegt werden können. In diesem Fall identifiziert die Objekt-ID des Servicekontos das dem virtuellen Server zugeordnete Konto, die Objekt-ID des Rechenzentrums das Rechenzentrum, in dem der virtuelle Server ausgeführt wird, und die Objekt-ID der VM-Instanz den virtuellen Server selbst. Dieser Block mit Identifizierungscode verhindert die Erstellung doppelter CIs.

```
var vmInfo = {
   "cmdb_ci_vm_instance": {
    "validator": "virtual_machine_create_update_validator",
    "validator_overrides": {},
    "identification": {
     "cmdb_ci_cloud_service_account": {
      "criterion": {
       "object_id": cloudServiceAccountId
      }
     },
     "cmdb_ci_aws_datacenter": {
      "criterion": {
       "object_id": ldc
      }
     },
     "cmdb_ci_vm_instance": {
      "criterion": {
       "object_id": vmResponse.nodeId
      }
     }
    },
```

Attribute werden in die Felder in der Tabelle „cmdb_ci_vm_instance“ eingetragen. Diese Attribute werden in Zeile 61 definiert:

```
"attributes": {
 "name": vmResponse.nodeName,
 "object_id": vmResponse.nodeId,
 "state": status_map[vmResponse.state],
 "dns_suffix": vmResponse.dnsSuffix,
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "cpus": vmCPUs,
  "memory": vmMemory,
  "disks": vmResponse.volumes.length,
  "disks_size": "",
  "nics": vmResponse.networkInterfaces.length,
  "terminated_on": "",
  "termination_protection": "",
  "ip_address": vmPubIPAddr,
  "assigned_to": reqContext.userId,
  "assignment_group": reqContext.groupId
},
```

Auch Verweise auf andere CIs können im Antwortprozessor enthalten sein. In diesem Fall wird die BS-Vorlage, auf der der virtuelle Server basiert, identifiziert, indem zuerst die Objekt-ID des Servicekontos, dann die des Rechenzentrums und schließlich die der tatsächlichen BS-Vorlage identifiziert wird.

```
"references": {
  "cmdb_ci_os_template": {
    "identification": {
      "cmdb_ci_cloud_service_account": {
        "criterion": {
          "object_id": cloudServiceAccountId
        }
      },
      "cmdb_ci_aws_datacenter": {
        "criterion": {
          "object_id": ldc
        }
      },
      "cmdb_ci_os_template": {
        "criterion": {
          "object_id": imageIdTrim
        }
      }
    },
```

Der folgende Codeblock fügt die Objekt-ID des BS-Images der Attributliste hinzu, damit diese Informationen in den CMDB-Datensatz des virtuellen Servers eingefügt werden können.

```
"attributes": {
  "object_id": imageIdTrim
}
```

Dieser Codeblock führt eine zusätzliche Identifizierung für die Computing-Vorlage (den Hardwaretyp) durch und fügt das Ergebnis dann den Attributen hinzu:

```
"cmdb_ci_compute_template": {
  "identification": {
    "cmdb_ci_cloud_service_account": {
      "criterion": {
        "object_id": cloudServiceAccountId
      }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  },
  "cmdb_ci_aws_datacenter": {
   "criterion": {
    "object_id": ldc
   }
  },
  "cmdb_ci_compute_template": {
   "criterion": {
    "object_id": vmResponse.hardwareId
   }
  }
 },
 "attributes": {
  "object_id": vmResponse.hardwareId,
  "name": vmResponse.hardwareId
 }
}
```

Zusätzliche Codeabschnitte stellen die Beziehung zu Netzwerkschnittstellen her und identifizieren jeden an den virtuellen Server angehängten Speicher.

Dieser obligatorische Codeblock verschiebt die Daten in die CMDB und gibt die JSON-Zeichenfolge zurück:

```
cloudModelString.push(vmInfo);
return global.JSON.stringify(cloudModelString);
```

Ressourcenblock die Terraform Orchestration-Schnittstelle hinzufügen

Nachdem Sie die Terraform-App im Store für Cloud Provisioning and Governance aktiviert haben, werden cloudbasierte Vorgänge für Cloud-Provider unterstützt, die die Terraform Open Source-Edition verwenden. Fügen Sie die Terraform Orchestration-Schnittstelle zum Ressourcenblock hinzu, um cloudbasierte Vorgänge über Terraform-Vorlagen auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cmp_root_admin, sn_cmp.cloud_service_designer

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblock**an.
2. Klicken Sie auf den Ressourcenblock, z. B. **Azure-Rechenzentrum**.
3. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**, um ihn bearbeitbar zu machen.
4. Navigieren zu **Allgemeine Informationen** > **Gastschnittstelle**, Und klicken Sie dann auf **Neu** .
5. Suchen Sie die **Terraform Orchestration-Schnittstelle** in der Liste „Gastschnittstelle“, wählen Sie sie aus, und klicken Sie auf **Absenden**.
6. Klicken Sie auf die Registerkarte **Vorgänge**.
7. Navigieren Sie auf der Registerkarte **Eingabeparameter** zu **Schnittstelle** und wählen Sie **Terraform Orchestration Interface** (Terraform Orchestration-Schnittstelle) aus.
8. Konfigurieren Sie auf der Registerkarte **Eingabeparameter** die CAPI-Vorgangseingaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffnen Sie bei der CAPI-Schnittstelle (in diesem Fall die Schnittstelle **Terraform Orchestration-Schnittstelle**) die Methode `CreateStack`. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

Die Registerkarte **Eingabeparameter** wird durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie dazu **Zuordnung** Wert aus **Eingabeparameter** Registerkarte in **Wert** Feld auf der **Schritte** > **Eingabe** Registerkarte

Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: ${parameter.arg1}.

9. Klicken Sie unter **Vorgänge** auf die Unterregisterkarte **Schritte**.
10. Klicken Sie auf **Schritt hinzufügen**.
11. Füllen Sie die Formularfelder aus.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus. **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen.
API-Anbieter	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den Provider **Terraform OpenSource** bereit, der die **Configuration Orchestration-Schnittstelle** bereitstellt. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. In diesem Beispiel stellt die **Configuration Orchestration-Schnittstelle** mehrere Schnittstellen oder Methoden bereit, die das System während der Bereitstellung verwendet.
API-Methode	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **ExecuteCommand** erforderlich, um Terraform-Vorlagen bereitzustellen.
CAPI-Version	Geben Sie eine Version für die CAPI API ein.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

12. Klicken Sie auf **Absenden**.

    Die Registerkarten **Eingabe** und **Antwortprozessor** werden für den Schritt angezeigt.

13. Konfigurieren Sie auf der Registerkarte **Eingabe** die CAPI-Vorgangseingaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffnen Sie bei der CAPI-Schnittstelle (in diesem Fall die **Configuration Orchestration-Schnittstelle**) die Methode *ExecuteCommand*. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

Denken Sie daran, dass die Parameter auf der Registerkarte **Eingabeparameter** durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie **Zuordnung** Wert aus **Eingabeparameter** Registerkarte in **Wert** Feld auf der **Schritte** > **Eingabe** Registerkarte

Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: ${parameter.arg1}.

Hinweis: Ordnen Sie die Werte für die folgenden Parameter wie in der folgenden Tabelle erläutert zu:

Parameter	Wert
AdditionalParameters	Geben Sie das folgende Skript ein: {"ServerType":"$(Script:sn_cmp_terraform.TerraformCommandUtils.getConfigProviderServerTypeByName[arg=${parameter.WorkloadConfigProvider}])"}
ConfigMgmtProviderInfo	$(capiResolver.NodeCredentialResolver#nodeCredentialId=$(ci.sn_cmp_wl_cfg_mgmt_provider[name=${parameter.WorkloadConfigProvider}].credential))
Knotenadresse	$(ci.cmdb_ci_workload_config_provider[name=${parameter.WorkloadConfigProvider}].url)
Skript Für CreateStapelvorgang	${CloudScript.scripts.TerraformDeploy}
Skript Für DeleteStapelvorgang	${CloudScript.scripts.DestroyTerraform}

14. Auf der Registerkarte **Antwortprozessor** konfigurieren Sie die Antwortprozessoren, indem Sie Ressourcenskripts anhängen.
    Sie haben dem Ressourcenblock beim Erstellen des Ressourcenblocks Ressourcenskripts hinzugefügt.
15. Wählen Sie in der Liste „Vorgang“ den Vorgang **CreateStack** oder **DeleteStack** aus.
16. Klicken Sie bei **Antwortprozessor hinzufügen** auf das Hinzufügen-Symbol +.
17. Klicken Sie auf die Unterregisterkarte **Ressourcenskript**, und klicken Sie dann auf **Neu**.
18. Füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neuer Datensatz

Feld	Beschreibung
Name	Geben Sie einen Namen (z. B. **Create_AzureTF_Stack_Response_Processor**) für das Ressourcenskript ein.
Typ	Wählen Sie einen Typ (**Antwortprozessor**) für das Skript aus.
Skript Ressourcenskript zum Erstellen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`
Skript Ressourcenskript zum Löschen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses);`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	}

19. Wählen Sie in der Liste **Skriptname** das Skript aus, das dem ausgewählten Vorgang entspricht, und klicken Sie auf **Absenden**.
20. Ändern Sie den Status des Ressourcenblocks von **Entwurf** in **Veröffentlicht**.
    Der Ressourcenblock „Rechenzentrum“ wird vom Status „Entwurf“ in den Status „Veröffentlicht“ verschoben, und Sie können keine weiteren Änderungen am Ressourcenblock vornehmen. Sie können einen Ressourcenblock nur ändern, nachdem Sie den Status auf **Entwurf** festgelegt haben.

Ressourcenblock für Microsoft Azure Cloud erstellen

Ressourcenblöcke sind die Bausteine von Cloud-Katalogelementen. Erstellen Sie einen Ressourcenblock für den Microsoft Azure Cloud Platform-Provider basierend auf einem CI-Typ aus der CMDB.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cmp_root_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblöcke**an.
2. Klicken Sie auf **Neu**, um das Dialogfeld „Ressourcenblock erstellen“ zu öffnen, und füllen Sie dann das Formular aus.

   Eine detaillierte Beschreibung der einzelnen Felder finden Sie unter Benutzerdefinierten Ressourcenblock erstellen.

Feld	Beschreibung
Name	Geben Sie einen Namen (**Azure-Rechenzentrum**) für den Ressourcenblock ein.
Beschreibung	Geben Sie eine gültige Beschreibung ein.
Ebene	Wählen Sie den Typ des Ressourcenblocks (**Logisches Rechenzentrum**) aus.
CI-Typ	Wählen Sie den CI-Typ (**Azure-Rechenzentrum**) aus, der den Ressourcenblock darstellt.
Gastschnittstelle	Wählen Sie eine Standardgastschnittstelle (**Computing-Schnittstelle**) aus, die beim Hinzufügen eines Ressourcenblocks zu einer Vorlage verwendet werden soll.

3. Klicken Sie auf **Absenden**.
   Die Ressourcenblockinformationen werden angezeigt.
4. Klicken Sie auf die Unterregisterkarte **Ressourcenskript**, und klicken Sie dann auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen Namen (z. B. **Create_AzureTF_Stack_Response_Processor**) für das Ressourcenskript ein.
Typ	Wählen Sie einen Typ (**Antwortprozessor**) für das Skript aus.
Skript Ressourcenskript zum Erstellen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`
Skript Ressourcenskript zum Löschen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
6. Klicken Sie auf die Unterregisterkarte **Vorgänge**, und klicken Sie dann auf **Schritte**.
7. Wählen Sie **CreateStack** in der Liste **Vorgänge** aus.
8. Klicken Sie auf das Pluszeichen **Schritt hinzufügen**, um das Dialogfeld „Vorgangsschritte hinzufügen“ zu öffnen, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus. **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen.
API-Anbieter [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den Provider **Terraform OpenSource** bereit, der die **Configuration Orchestration-Schnittstelle** bereitstellt. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. In diesem Beispiel stellt die **Configuration Orchestration-Schnittstelle** mehrere Schnittstellen oder Methoden bereit, die das System während der Bereitstellung verwendet.
API-Methode [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **ExecuteCommand** erforderlich, um Terraform-Vorlagen bereitzustellen.
CAPI-Version [Vorgangstyp = Cloud API aufrufen]	Geben Sie eine Version für die CAPI API ein.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

9. Klicken Sie auf **Absenden**.
10. Klicken Sie auf **Antwortprozessor**, und klicken Sie dann auf das Pluszeichen.
    Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.
11. Wählen Sie **Create_AzureTF_Stack_Response_Processor** aus der Liste **Skriptname** aus, und klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Ändern Sie den Status des Ressourcenblocks von **Entwurf** in **Veröffentlicht**.
    Der Ressourcenblock „Azure-Rechenzentrum“ wird vom Status „Entwurf“ in den Status „Veröffentlicht“ verschoben, und Sie können keine weiteren Änderungen am Ressourcenblock vornehmen. Änderungen an einem Ressourcenblock können nur vorgenommen werden, wenn der Status auf **Entwurf** festgelegt ist.

Cloud-Skripts und Cloud-Skriptvorlagen

In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Blaupausen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben.

Cloud-Skripts

Cloud-Skripts sind einfache Java-Skripts, die Plattformfunktionen verwenden. Beispiel für ein Cloud-Skript:

```
function evaluateTemplate() {
 // Template Resolver is a helper function which we will use to fetch a template and replace its
 parameters,
 // var templateResolver=new TemplateResolver(); this comes inbuild
 // templateAttributes below will passed from the user.
 var listDir=templateResolver.getTemplate('Install',templateAttributes);
 return listDir;
}
```

Jedes Cloud-Skript enthält bestimmte Parameter. Parameter sind die Attribute, auf die Sie zugreifen möchten. Ein Parameter enthält einen Namen, einen Standardwert und einen Überschreibungswert. Der Standardwert kann ein Zeichenfolgenliteral, ein Ressourcenblockparameter oder ein komplexer Skriptausdruck sein, der in Ressourcenblöcken verwendet wird.

Ein Cloud-Skript hat standardmäßig Zugriff auf das Objekt *`templateResolver`*. Das Objekt *`templateResolver`* verfügt standardmäßig über eine getTemplate-Methode, deren erster Parameter der Name der Cloud-Skriptvorlage ist. *`templateAttributes`* sind die Cloud-Skriptparameter, die als Teil eines Cloud-Skripts erstellt werden. Bei Bedarf können in *`templateAttributes`* Anpassungen vorgenommen werden. Sehen Sie sich beispielsweise das folgende Codefragment an, wenn der Wert des Parameters *`DevName`* von „John“ in „Emily“ geändert werden muss.

```
function evaluateTemplate() {
 // Template Resolver is a helper function which we will use to fetch a template and replace its
 parameters,
 // var templateResolver=new TemplateResolver(); this comes inbuild
 // templateAttributes below will passed from the user.
 templateAttributes['DevName'] = 'Emily';
 var customNodeName;
 var now_GR = new GlideRecord('some_custom_table_to_query');
 gr.addQuery('some_parameter','some_value');
 gr.query();
 if(gr.next())
   customNodeName=gr.getValue('some_custom_node_name');

 templateAttributes['NodeName'] = customNodeName;
 var listDir=templateResolver.getTemplate('Install',templateAttributes);
 return listDir;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}
evaluateTemplate();
```

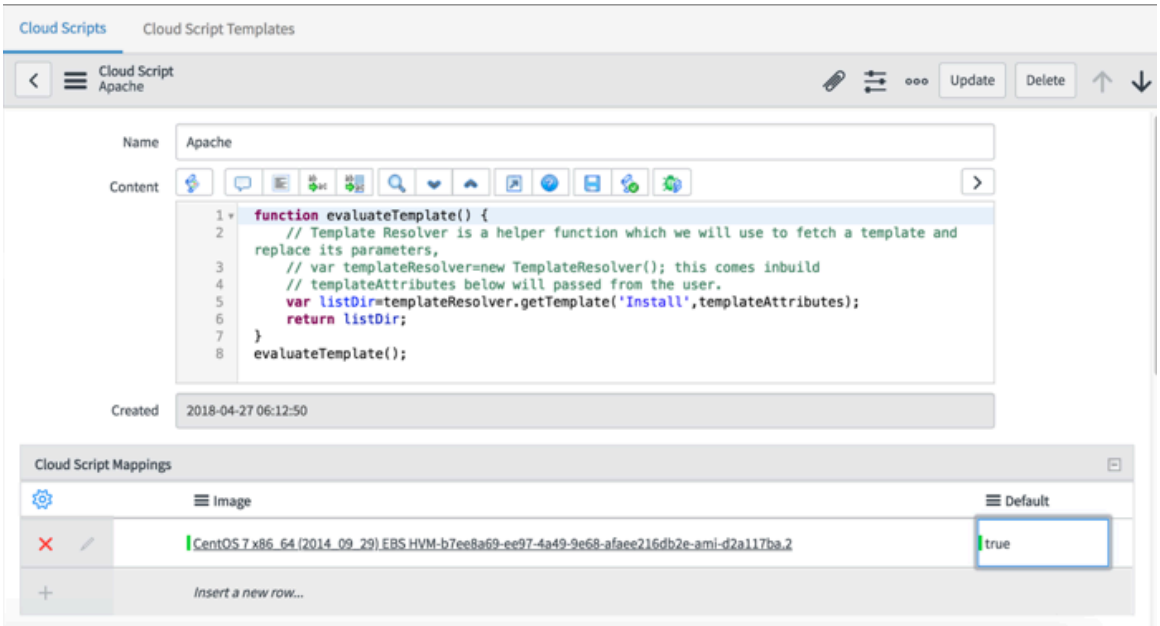
Cloud-Skriptvorlagen

Cloud-Skriptvorlagen sind tatsächliche ausführbare Dateien, die zur Ausführung an einen virtuellen Computer übergeben werden. Cloud-Vorlagen können je nach Ausführungskontext einen beliebigen Typ (Shell/PowerShell/CloudInit) haben. Erstellen Sie zuerst eine Cloud-Vorlage, und ordnen Sie sie dann einem Cloud-Skript zu.

Cloud-Skripts als CloudInit

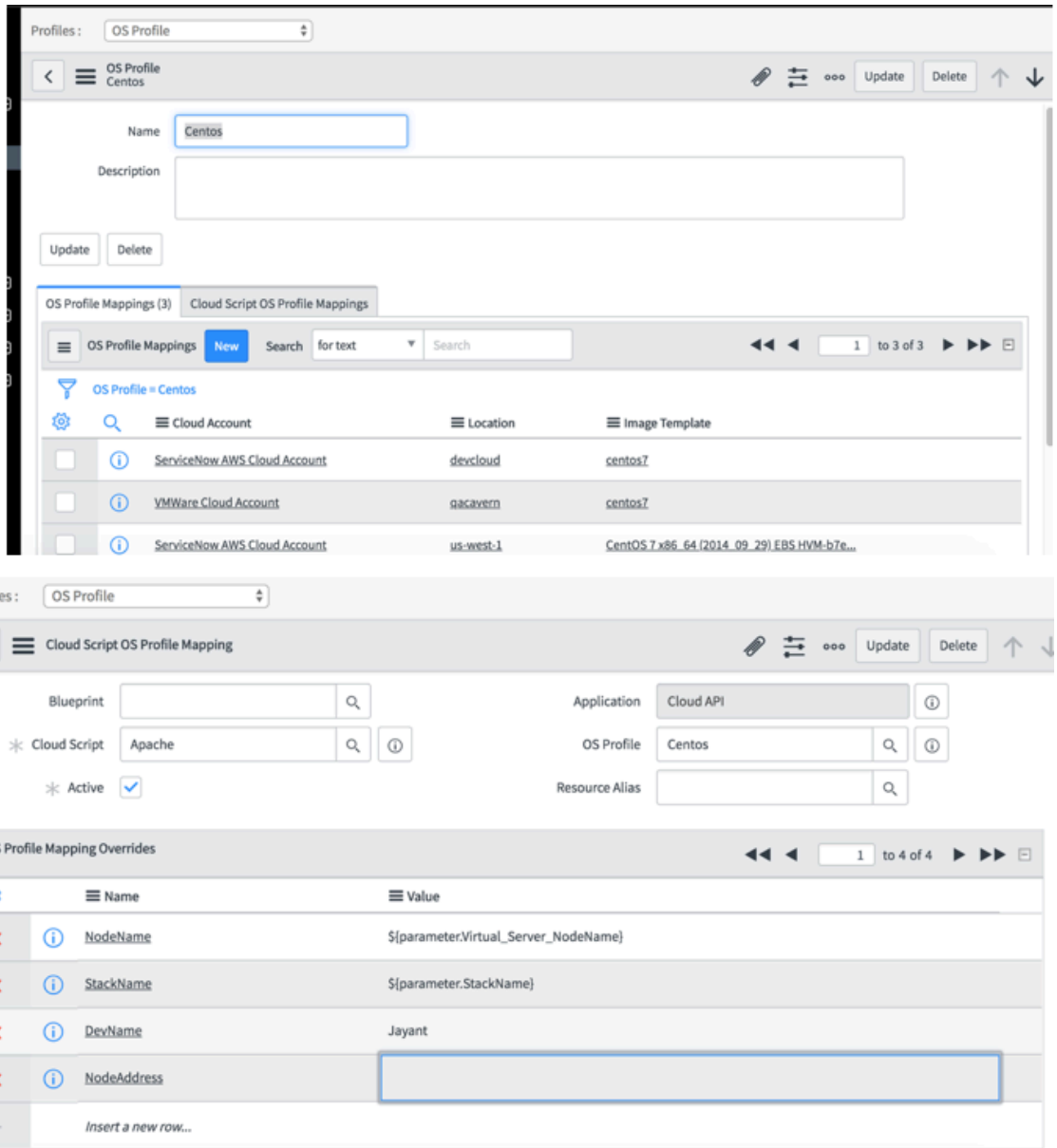
Cloud-Provider bieten eine Möglichkeit, Skripts beim Start von virtuellen Computern auszuführen. In der Cloud-Management-Anwendung können Sie ein cloudinit-Skript auf verschiedenen Ebenen angeben:

- Image-Ebene: Zum Zeitpunkt der Erstellung eines Cloud-Skripts können Sie ein Image angeben, für das dieses Skript ausgeführt werden soll. Sobald ein BS-Profil ausgewählt wird, das dieses bestimmte Image enthält, wird das standardmäßige Cloud-Skript für dieses Image ausgeführt. Im folgenden Beispiel ist ein Apache-Cloud-Skript einem bestimmten Image zugeordnet.



- BS-Profilebene: Sie können ein cloudinit-Skript für einen bestimmten Cloud-Provider und für ein bestimmtes AMI/Image ausführen. Sie können auch generisch einem BS-Profil ein cloudinit-Skript zuordnen, unabhängig vom zugrunde liegenden Image. Im folgenden Beispiel sind dem BS-Profil mehrere Images zugeordnet. Sie können auf der Registerkarte „Cloud-Skript – BS-Profilzuordnungen“ dem BS-Profil ein beliebiges Cloud-Skript zuordnen. Die Zuordnung eines Cloudskripts zu einem BS-Profil hat Vorrang vor der Cloud-Skriptzuordnung auf Image-Ebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In diesem Beispiel wird das Apache-Cloud-Skript dem Centos-BS-Profil zugeordnet. Bei Bedarf können Sie die Skriptparameter im Abschnitt „Überschreibungen der BS-Profilzuordnung“ überschreiben.

- Ressourcenblöcke: Bei der Zuordnung eines Cloud-Skripts zu einem BS-Profil können Sie wählen, ob das Cloud-Skript für einen bestimmten in einer Blaupause verwendeten Ressourcenblock und für einen bestimmten Ressourcenalias ausgeführt werden soll. Weitere Informationen finden Sie unter BS-Profil erstellen.

Cloud-Skripts als Postinit

Sie können Cloud-Skripts als Postinit-Skripts in einem Ressourcenblock verwenden. Sobald Sie einen Ressourcenblock mit einem virtuellen Computer erstellt haben, der bereitgestellt werden soll, können Sie einen ExecuteScript-Vorgang hinzufügen. Der ExecuteScript-Vorgang verwendet einen Skriptparameter (einen Pool von Cloud-Skripts), und Sie können ein beliebiges auszuführendes Skript auswählen. Verwenden Sie das Attribut `ScriptParameters` im ExecuteScript-Vorgang, um beliebige Skriptparameter zu überschreiben. Sie können eine JSON-Zuordnung der Skriptparameter und ihrer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überschreibungswerte bereitstellen. Alle Ausdrücke, die von Cloud-Management unterstützt werden, sind im Attribut `ScriptParamters` anwendbar.

Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen

Erstellen Sie Vorlagen und Skript für die Cloud-Initialisierung, um sie zur VM-Bereitstellung zu verwenden.

Vorbereitungen
Erforderliche Rolle: cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Skripts** > **Cloud-Skriptvorlagen**an.
2. Klicken Sie auf **Neu**, geben Sie den Namen und Inhalt des Skripts ein, und klicken Sie dann auf **Absenden**.

   Erstellen Sie so viele Skriptvorlagen wie nötig.
3. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Skripts**an.
4. Klicken Sie auf **Neu**.
5. Geben Sie einen beschreibenden Namen ein, und erstellen Sie ein Skript, das den Vorlagennamen in der folgenden Codezeile verwendet (`scriptName` ist der Name der Vorlage):

   ```
   templateResolver.getTemplate(scriptName);
   ```

   Hinweis: Weitere Informationen finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.
6. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Um ein Skript zum Zeitpunkt der Bereitstellung einer virtuellen Ressource auszuführen, ordnen Sie das Skript einem BS-Profil zu. Zum Ausführen eines Post-Bereitstellungsskripts erstellen Sie eine Blaupause, und geben Sie das Skript im Vorgang „Skript ausführen“ an. Ein Beispiel finden Sie unter Beispiel: Cloud-Skript für nach der Bereitstellung.

BS-Profil ein Skript zuordnen

Um geskriptete Aktionen während der VM-Bereitstellung auszuführen, können Sie einem BS-Profil ein Skript zuordnen. Das Skript wird auf VMs ausgeführt, die basierend auf der Bildvorlage im BS-Profil erstellt werden.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Warum und wann dieser Vorgang ausgeführt wird
In diesem Verfahren geben Sie ein vorhandenes Skript an. Siehe Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen.

Hinweis: Profilzuordnungen, in denen mehr Details angegeben sind, werden zuerst ausgeführt. Beispielsweise hat eine Zuordnung, in der eine Blaupause, ein Betriebssystemprofil und ein Ressourcenalias angegeben sind, Vorrang vor einer Zuordnung, in der nur ein Betriebssystemprofil angegeben ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Verwalten** > **Ressourcenprofile**an.
2. Wählen Sie in der Liste **Profile** die Option **BS-Profil** aus, und öffnen Sie dann das Profil.
3. Klicken Sie in der zugehörigen Liste „Cloud-Skript – BS-Profilzuordnungen“ auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Plan [Optional]	Wählen Sie eine Blaupause, um das Skript auf einen bestimmten, in der Blaupause verwendeten Ressourcenblock zu beschränken.
Cloud-Skript	Wählen Sie ein Cloud-Skript aus, dem das Betriebssystemprofil zugeordnet werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, wenn das Cloud-Skript nach der Bereitstellung des virtuellen Computers ausgeführt werden soll.
Applikation	Cloud Provisioning and Governance ist automatisch ausgewählt.
BS-Profil	Wenn Sie eine Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause bereitgestellt wird.
Ressourcen-Alias [Optional]	Wenn Sie einen Ressourcenalias für die Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause mit dem angegebenen Ressourcenalias bereitgestellt wird.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Das **Namensattribut** [scriptName] wird in der Liste „Überschreibungen der BS-Profilzuordnung“ aufgeführt.
5. Geben Sie in der Liste „Überschreibungen der BS-Profilzuordnung“ einen Attributnamen und einen Wert ein, die bei der Bereitstellung der Ressource verwendet werden.

Zugehörige Informationen

BS-Profil erstellen

Beispiel: Cloud-Skript für nach der Bereitstellung

Dieses Beispiel zeigt ein Cloud-Skript, das ausgeführt wird, nachdem ein Benutzer einen virtuellen Computer bereitgestellt hat.

Vorbereitungen

- Erforderliche Rolle: cloud_admin
- BS-Ressourcenprofil, das einer Bildvorlage zugeordnet ist. Der Benutzer stellt eine Ressource mithilfe des Profils bereit. Sie müssen hinzufügen Anmeldeinformationen für Standardauthentifizierung Zum Bild.
- Computing-Ressourcenprofil, das einem Hardwaretyp zugeordnet ist.

Warum und wann dieser Vorgang ausgeführt wird

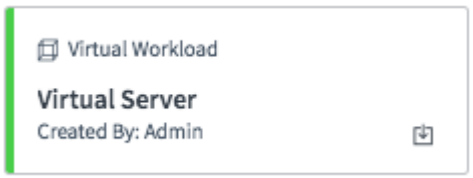
In diesem Beispiel erstellen Sie ein Cloud-Init-Skript, passen einen Ressourcenblock an und stellen eine VM über das Cloudbenutzerportal bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

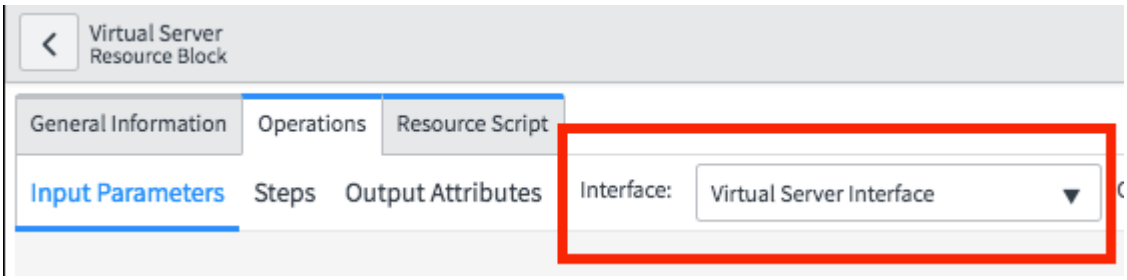
Prozedur

1. Erstellen Sie eine Cloud-Skriptvorlage und ein Cloud-Skript, das auf die Vorlage verweist.
2. Öffnen Sie den Ressourcenblock des virtuellen Servers, und führen Sie die folgenden Schritte aus:

   a. Legen Sie den Umschalter **Entwurf/Veröffentlicht** auf **Entwurf** fest.

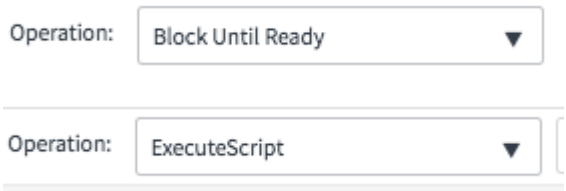


   b. Wählen Sie auf der Registerkarte **Vorgänge** die Option **Virtuelle Serverschnittstelle** aus der Liste **Schnittstelle** aus.



   c. Überprüfen Sie im Feld **Vorgang**, ob diese Vorgänge vorhanden sind:

   - **Blockieren bis bereit**
   - **Skript ausführen**: Dieser Vorgang weist die Blaupause an, ein Skript auszuführen.



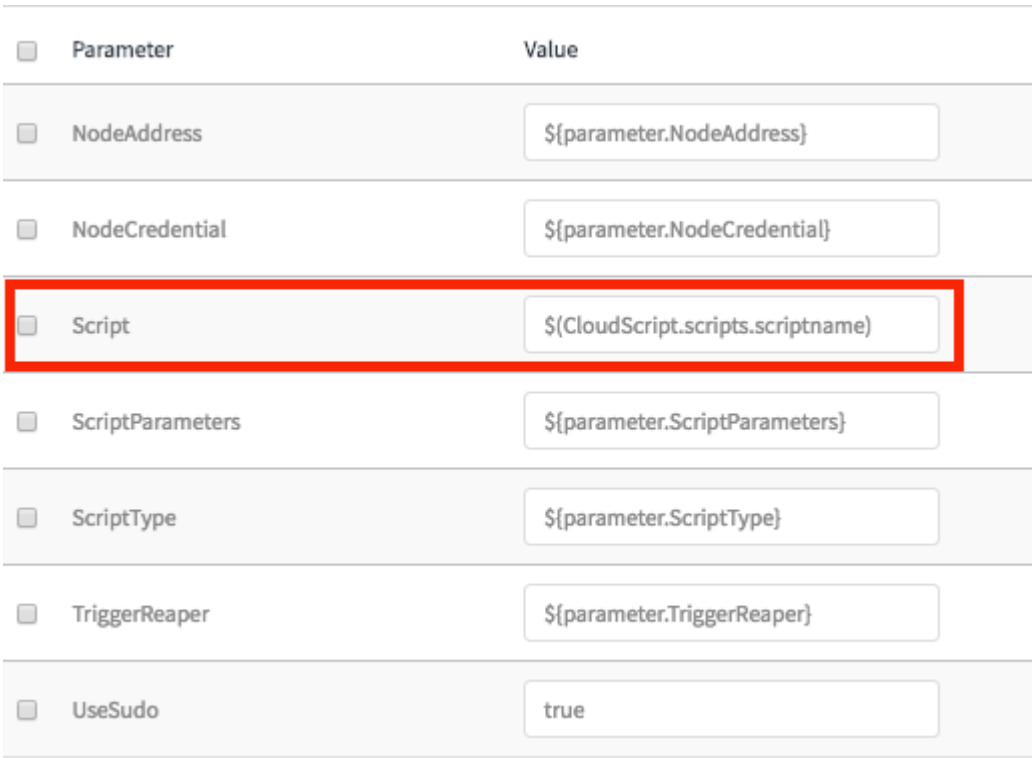
   d. Klicken Sie auf die Registerkarte **Eingabeparameter**, um sich die Eingaben für jeden Vorgang anzusehen.

   e. Fügen Sie auf der Registerkarte **Schritte** nach Bedarf Schritte hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Deaktivieren Sie beim Parameter **Skript** in jedem Schritt das Kontrollkästchen **Skript** und ändern Sie den Ausdruck in der Spalte **Zuordnung** zu dem folgenden Text: `$(CloudScript.scripts.scriptname)`, wobei `scriptname` der Name des Skripts ist, nicht die Skriptvorlage, die Sie zuvor erstellt haben.



3. Veröffentlichen Sie den Ressourcenblock des virtuellen Servers, und verwenden Sie ihn in einer Blaupause, die ihrerseits in einem Katalogelement veröffentlicht wird.
4. Starten Sie einen neuen Stapel, um eine VM bereitzustellen, und geben Sie das BS-Profil und das Computing-Profil an, die Sie als Voraussetzung erstellt haben.

Ergebnis

Auf der Seite „Stapelstatus“ sehen Sie, wie die Vorgänge `CreateNode`, `BlockUntilReady` und `ExecuteShellScript` durchlaufen werden. Der letzte Vorgang hat das von Ihnen erstellte Skript ausgelöst.

Antwortzuordnungen

Die Antwortzuordnung ist der Mechanismus, den CMP verwendet, um alle Ereignisse und Vorgänge in die CMDB zurückzuschreiben.

Mechanismus für Antwortzuordnung

CMP (Cloud Management Platform) wurde entwickelt, um in verschiedenen kritischen Phasen aktiv mit der Cloud-Umgebung zu interagieren, einschließlich Discovery, Bereitstellung, Tag-2-Vorgänge und Lebenszyklusereignisse. Während dieser Prozesse ist CMP erforderlich, um Daten effektiv in der Configuration Management Database (CMDB) aufzuzeichnen und zu speichern. Diese Daten können verschiedene Informationen enthalten, von systemstatus bis zu umfassenden Datensätzen.

Um dies zu erreichen, nutzt CMP seinen Antwortverarbeitungsmechanismus, um die nahtlose und genaue Übertragung von Daten zurück in die CMDB sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen der Antwortzuordnung

- Ordnet das externe Datenformat dem ServiceNow-Format für den IRE-Verbrauch zu.
- Unterstützt einfache, komplexe, geskriptete, Bindungen und Beziehungszuordnungen.
- Wichtig zum Hinzufügen neuer Zuordnungen/Ändern.
- Leistungsfähig, wird in CMP für die letzten Releases verwendet.

Siehe https://www.servicenow.com/community/itom-articles/cmp-using-response-mapping-how-to-populate-cmdb-using-cmp/ta-p/2323213 Um mehr zu erfahren.

Parameterwert mit der AllowedPattern-Eigenschaft validieren

Die Eigenschaft `AllowedPattern` in einer Vorlage von Azure Resource Manager (ARM) oder CloudFormation (CF) führt vor dem Senden einer Bereitstellungsanforderung eine Eingabevalidierung durch.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können Regeln bereitstellen, um einen Parameterwert zu validieren, bevor die Bereitstellungsanforderung an die Cloud gesendet wird. Um bei einer fehlgeschlagenen Validierung mit einer Fehlermeldung benachrichtigt zu werden, geben Sie die Eigenschaft `ConstraintDescription` in der Vorlage an. Sie können die Fehlermeldung in der Eigenschaft `ConstraintDescription` anpassen, um die Nachricht klar und eindeutig zu formulieren. Normalerweise verfügen die CF-Vorlagen bereits über die Eigenschaften `AllowedPattern` und `ConstraintDescription`. Wenn diese Eigenschaften nicht vorhanden sind, können Sie sie wie im folgenden Verfahren erwähnt hinzufügen:

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-Vorlagen**an.
2. Wählen Sie eine Vorlage aus, oder klicken Sie auf **Neu**, um eine neue Cloud-Vorlage zu erstellen. Wenn Sie eine vorhandene Vorlage auswählen, benennen Sie die Vorlage um.
3. Nehmen Sie in einer ARM- oder einer CF-Vorlage im Textfeld **Text** die folgenden Änderungen vor.

   a. Nehmen Sie in einer ARM-Vorlage die folgenden Änderungen vor:

   - Geben Sie im Abschnitt „parameters“ unter „metadata“ `SNC::Parameter::Metadata` ein.
   - Fügen Sie den Schlüssel `AllowedPattern` hinzu, und geben Sie einen gültigen Wertebereich ein.
   - Fügen Sie den Schlüssel `ConstraintDescription` hinzu, und geben Sie eine Fehlermeldung ein.

```
"parameters": {
      "newStorageAccountName": {
         "type": "string",
          "metadata": {
             "description": "Unique DNS Name for the Storage Account where the Virtual
Machine's disks will be placed.",
              "SNC::Parameter::Metadata": {
                 "allowedPattern": "[0-9a-z]{1,11}",
                  "ConstraintDescription": "must be an alphanumeric "
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                    }}}
```

b. Nehmen Sie in einer CF-Vorlage die folgenden Änderungen vor:

- Fügen Sie den Schlüssel *`AllowedPattern`* hinzu, und geben Sie einen gültigen Wertebereich ein.
- Fügen Sie den Schlüssel *`ConstraintDescription`* hinzu, und geben Sie eine Fehlermeldung ein.

```
"Parameters" : {
            "SSHLocation" : {
            "Description" : "The IP address range that can be used to SSH to the EC2
 instances",
            "Type": "String",
            "MinLength": "9",
            "MaxLength": "18",
            "Default": "0.0.0.0/0",
             "AllowedPattern": "(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\\d{1,2})",
             "ConstraintDescription": "must be a valid IP CIDR range of the form x.x.x.x/x."

  }
 }
```

4. Klicken Sie auf **Absenden**.

Cloud-Governance

Governance bezieht sich auf die Einschränkungen, die Sie für verfügbare Cloud-Ressourcen festlegen können.

Governance-Typen

Typ	Beschreibung
Kontingente	Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.
Richtlinien	Eine Cloud-Richtlinie kann einen von einem Anwender festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorab ausfüllen oder ausblenden, anwenderdefinierte Skripts ausführen und aufrufen Cloud-API, Oder starten oder brechen Sie Subflows ab. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.
Pools	Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.
Berechtigungen	Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung
	Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Berechtigungsverwaltung für Cloud-Governance-Rollen

Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Sie können basierend auf der Benutzergruppe detailliert festlegen, welche Aktionen für Benutzer zulässig oder verboten sind. Standardmäßig umfasst jede Rolle Zugriffsrechte, aber nicht alle Benutzer mit der gleichen Rolle können die Datensätze der anderen Benutzer anzeigen oder bearbeiten. Beispielsweise verfügen Benutzer mit der Rolle „cloud_designer“ standardmäßig über vollständigen Lese- und Schreibzugriff auf ihre eigenen Blaupausen, sie haben jedoch keinen Lese- oder Schreibzugriff auf Blaupausen, die von anderen Cloud-Designern erstellt wurden. Wenn Sie möchten, dass sie Zugriff haben, müssen Sie die Benutzer in eine Gruppe mit der Rolle „cloud_designer“ einordnen und dieser Gruppe dann Lese- und Schreibzugriff auf bestimmte Blaupausen geben.

Berechtigungstypen

Zugriff [Lesen]

Benutzer können den Datensatz anzeigen, aber nicht bearbeiten oder löschen.

Verwalten [Erstellen und aktualisieren]

Benutzer können den Datensatz anzeigen und neue Datensätze in derselben Tabelle erstellen und aktualisieren, aber keine Datensätze löschen.

Löschen

Benutzer können angegebene Datensätze oder alle Datensätze in der Tabelle löschen.

Ausführen

Benutzer können eine Aktion für Datensätze in der Tabelle ausführen.

Alle

Benutzer haben Berechtigungen für alle Datensätze in der Tabelle.

Berechtigungsvorschläge

Erwägen Sie, diese Berechtigungen in Ihrer Organisation zu gewähren:

Vorgeschlagene Gruppe und Rolle	Benutzertyp in der Gruppe	Berechtigungsvorschläge	Beschreibung
Katalogbenutzergruppe Cloud-Benutzer [sn_cmp.cloud_service_user]	Benutzer, die ähnliche Elemente aus dem Katalog im Cloudbenutzerportal bestellen.	Zugreifen [lesen] oder ausführen	Katalogelemente können auch nach der Veröffentlichung von Benutzern im Cloudbenutzerportal erst angezeigt werden, nachdem Sie einer Benutzergruppe, der diese Benutzer angehören, Lesezugriff auf die Elemente gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgeschlagene Gruppe und Rolle	Benutzertyp in der Gruppe	Berechtigungsvorschläge	Beschreibung
			Gewähren Sie Cloud-Benutzern Zugriffs- und Ausführungsberechtigungen für die Tabellen „Blaupausenkatalogelement“ und „Cloud-Konto“.
Blaupausendesigner Servicedesigner [sn.cmp.cloud_service_designer]	Benutzer, die Blaupausen entwerfen.	Verwalten [Erstellen und aktualisieren]	Blaupausendesigner können andere Blaupausen oder Katalogelemente standardmäßig nicht anzeigen oder bearbeiten. Zur Zusammenarbeit oder zur Wiederverwendung vorhandener Blaupausen und Katalogelemente benötigen Blaupause-Designer über die Berechtigung „Verwalten“ Zugriff auf die Blaupausen anderer Benutzer.
Cloud-Administratoren Cloud-Administrator [sn_cmp.cloud_admin]	Benutzer, die Cloud-Accounts erstellen und verwalten.	Verwalten [Erstellen und aktualisieren]	Cloud-Administratoren müssen Vorlagen entsprechenden Ressourcenprofile zuordnen. Zur Zusammenarbeit oder zur Wiederverwendung vorhandener Ressourcenprofile und Vorlagen.

Cloud-Berechtigung zuweisen

Weisen Sie eine Berechtigung zu, um basierend auf der jeweiligen Benutzergruppe detailliert festzulegen, welche Aktionen für Benutzer zulässig oder verboten sind.

Vorbereitungen

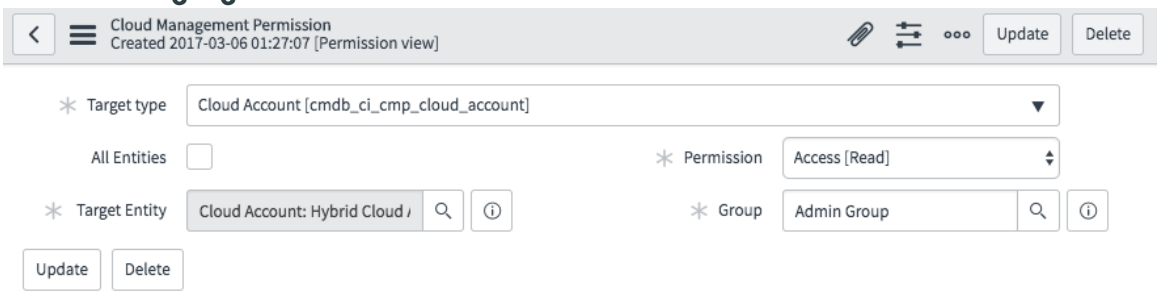
- Erforderliche Rolle: sn_cmp.cloud_governor
- Die Anwendergruppe Auf die Sie die Berechtigung anwenden möchten.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Governance** > **Berechtigung**an.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Leseberechtigungen für Cloud-Konten



Feld	Beschreibung
Zieltyp	Wählen Sie die Cloud-Tabelle aus, zu der der Zieldatensatz gehört.
Alle Entitäten	Wählen Sie diese Option aus, um die Berechtigung auf alle Datensätze in der Tabelle anzuwenden.
Berechtigung	Wählen Sie den Berechtigungstyp aus.
Zielentität	Wählen Sie den Datensatz aus, auf dem die Berechtigung basiert.
Gruppe	Wählen Sie die Benutzergruppe aus.

3. Klicken Sie auf **Absenden**.

Richtlinien für Cloud Provisioning

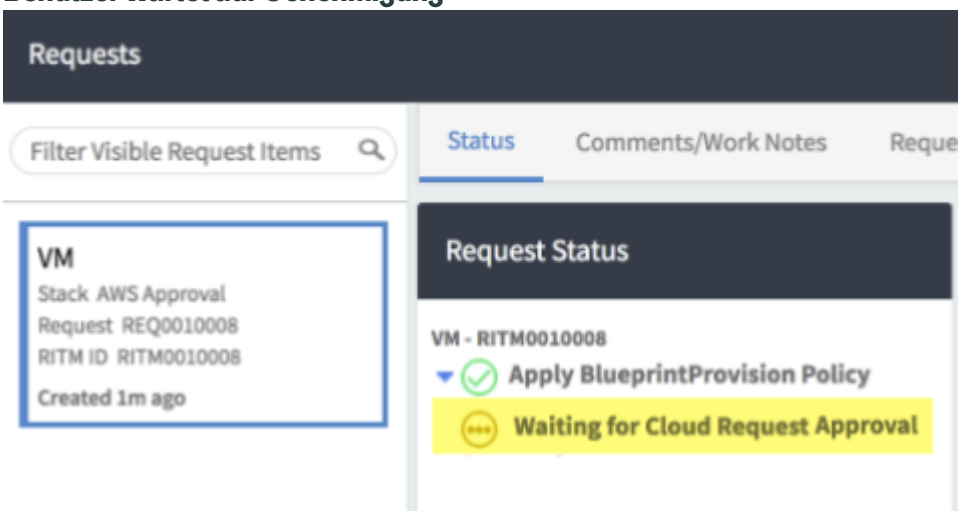
Eine Cloud-Richtlinie kann einen von einem Anwender festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorab ausfüllen oder ausblenden, anwenderdefinierte Skripts ausführen und aufrufen Cloud-API, Oder starten oder brechen Sie Subflows ab. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.

Example: Ein Benutzer fordert einen Stapel an, mit dem eine Genehmigungsrichtlinie ausgelöst wird

1. Ein Benutzer sendet im Cloudbenutzerportal eine Anforderung zur Bereitstellung einer bestimmten Blaupause. Der Prozess der Bereitstellung der Blaupause ist der Auslöser, mit dem das Richtlinienmodul zur Anwendung einer Genehmigungsrichtlinie veranlasst wird. Eine Cloud-Genehmigungsrichtlinie gibt die Anwender an, die eine bestimmte Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann.
2. Vom Richtlinienmodul wird festgestellt, dass die Anforderung die in der Regel für die Richtlinie angegebene Bedingung erfüllt. In diesem Beispiel wird die Bedingung immer dann als „true“ (wahr) bewertet, wenn eine bestimmte Blaupause bereitgestellt wird.
3. Da die Bedingung erfüllt ist, wird vom Richtlinienmodul die Aktion ausgeführt, die auch in der Regel angegeben ist. In diesem Beispiel besteht die Aktion darin, eine Genehmigungsaktion für den Manager anzulegen.
4. Während der Genehmiger (der Manager) die Genehmigungsanforderung überprüft, wird dem Benutzer im Cloudbenutzerportal die Statusmeldung „Warte auf Genehmigung“ angezeigt.
5. Die Blaupause wird nach Genehmigung durch den Manager bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer wartet auf Genehmigung



Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

Richtlinienauslöser

Auslöser sind Ereignisse, die die Richtlinien-Engine in Bewegung setzen. Beispielsweise wird der Auslöser `bei Ende der Katalogelementanforderung` ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Wenn Sie eine Richtlinie definieren möchten, sollten Sie zuerst darüber nachdenken, wie die Richtlinie ausgelöst wird. Beispiele:

- Ein Benutzer fordert einen Vorgang `Stoppen` für einen virtuellen Server an (was den Auslöser `bei Stapelressourcenvorgang` auslöst).
- Eine Ressource erreicht das Ende ihres Leasings (was den Auslöser `bei Leasingende` auslöst).
- Ein Benutzer fordert einen bestimmten Stapel an (was den Auslöser `bei Blaupausenbereitstellung` auslöst).

Sie verweisen normalerweise auf eine Richtlinie anhand des Namens des Auslösers der Richtlinie. Beispielsweise können Sie eine Richtlinie, die durch den Auslöser `bei Leasingende` ausgelöst wird, als „Richtlinie für Leasingende“ bezeichnen. Weitere Informationen zu den Typen von Auslösern, die Sie implementieren können, finden Sie unter Auslöser für Cloud-Richtlinien.

Funktionsweise von Richtlinien

Für jede Richtlinie konfigurieren Sie normalerweise einen Auslöser, der die Richtlinien-Engine startet. Die Richtlinien-Engine setzt die Richtlinie durch, indem sie alle Regeln ausführt, die für die Richtlinie definiert sind. Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

- Einige Richtlinientypen gelten nur für bestimmte Typen von Cloud-Vorgängen, z. B. „Starten“, „Stoppen“, „Bereitstellung“ oder „Bereitstellung aufheben“, oder für ein bestimmtes Ziel, z. B. „bei Bereitstellungsvorgang für Blaupause123“ oder „bei Start von Katalogelement ABC“.
- Sie können eine Richtlinie konfigurieren, die kein Ziel angibt, z. B. „bei jedem Bereitstellungsvorgang für eine Blaupause“ oder „bei jedem Start eines Katalogelements“. Fehler in Richtlinien, die für ein beliebiges Objekt gelten, werden ignoriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn mehrere Richtlinien gelten, können Sie die Reihenfolge angeben, in der die Richtlinien angewendet werden (mit einer Ausnahme, die im folgenden Abschnitt beschrieben wird).
- Richtlinien können mit dynamischen Formularen zusammenarbeiten, damit Sie Formularfelder für Endbenutzer ein- oder ausblenden können. Benutzer sehen nur Informationen, die sie Ihrer Entscheidung nach für das Verständnis und die Erfüllung ihrer Aufgaben benötigen.

Richtliniengruppen

Eine Cloud-Richtliniengruppe ist ein Container für zugehörige Richtlinien. Es empfiehlt sich, Richtlinien, die häufig zusammen verwendet werden oder zusammen betrachtet werden sollen, zu gruppieren. Durch die Gruppierung von Richtlinien können Sie Richtlinien konsistent in Ihrer Organisation anwenden.

Reihenfolge der Ausführung, wenn mehrere Richtlinien gelten

Reihenfolge der Ausführung, wenn mehrere Richtlinien vom Typ „Genehmigung“ gelten:

Wenn mehrere „Genehmigungsrichtlinien“ gelten, werden die Richtlinien in der folgenden Reihenfolge angewendet. (Die Genehmigungsrichtlinien sind `Bei Blueprint-Bereitstellung (Genehmigung)` , `Bei Stapelvorgang (Genehmigung)` , `Bei Stapelressourcenvorgang (Genehmigung)` , Und `Bei Aufgabenkorrektur`):

1. Nur die erste erfolgreiche Genehmigungsrichtlinie wird angewendet. Es werden keine weiteren Genehmigungsrichtlinien angewendet.
2. Wenn die angewendete Genehmigungsrichtlinie mehrere Regeln aufweist, wird nur die erste erfolgreiche Regel verwendet.
3. Wenn eine Regel über mehrere Aktionen verfügt, wird nur die erste erfolgreiche Aktion ausgeführt.
4. Wenn die angewendete Genehmigungsrichtlinie sowohl eine benutzerdefinierte Genehmigung als auch eine ServiceNow-Genehmigung enthält, wird nur der benutzerdefinierte Genehmigungsprozess ausgeführt.

Reihenfolge der Ausführung für alle anderen Richtlinientypen:

- Richtlinien werden in der Reihenfolge angewendet, die durch die Eigenschaftseinstellung **Reihenfolge der Ausführung** angegeben ist.
- Wenn mehrere Richtlinien dieselbe Einstellung **Reihenfolge der Ausführung** aufweisen, wird die Reihenfolge nicht garantiert.

Vorgänge in Richtlinien

Auslöser basieren häufig auf Anwenderanforderungen und den Vorgängen (Start, Stopp, Bereitstellung oder Aufhebung der Bereitstellung), die auf einem Blueprint, einem Katalogelement, einer Ressource oder einem Stapel ausgeführt werden können. Einige Auslösertypen geben keinen Cloud-Vorgang an. Zum Beispiel erfolgt die Auslösung des Auslösers `bei Leasingende` unabhängig von jedem Vorgang.

Richtlinienregeln

Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedingungen: Bedingungen können Anforderungsformulardaten, Ressourcenaktivitäten oder Benutzeraktivitäten berücksichtigen. Beispiele:
  - Ist die angeforderte CPU größer als 32?
  - Handelt es sich um einen Vorgang `Stoppen`?
  - Endet das Leasing für diese Ressource in den nächsten 7 Tagen?
- Aktionen: Wenn alle Bedingungen als „true“ ausgewertet werden, führt die Richtlinien-Engine die in der Regel angegebenen Aktionen aus. Ausdrücke in Richtlinienaktionen können Werte festlegen oder überschreiben. Beispiele:
  - Der vom Benutzer angegebenen Wert wird überschrieben, indem die CPU-Größe auf 16 geändert wird, dann wird der Genehmigungsprozess gestartet (da die Bedingung erfüllt war, dass die angeforderte CPU größer als 32 ist).
  - Eine Genehmigungsaufgabe für den Manager wird erstellt (da die Bedingung erfüllt war, dass ein Vorgang `Stoppen` angefordert wurde).
  - Benachrichtigungen werden an alle Benutzer in der Gruppe „ABC“ gesendet (da die Bedingung erfüllt war, dass der Leasingvertrag in 7 Tagen endet).

Richtlinien-Aktionsskripts

- Verwenden Sie Richtlinienaktionsskripts, um Werte in Cloud-Anforderungen abzurufen, zu aktualisieren oder festzulegen.
- Ihre Instanz verfolgt für Abrechnung und Berichterstellung getaggte Ressourcen nach. Richtlinienaktionsskripts können Ressourcen-Tags hinzufügen und ändern.

Cloud-Richtlinienbeispiel

Eine Basissystem-Cloud-Richtlinie `Leasingende ServiceNow` verwendet den Auslöser `bei Leasingende`, der ausgelöst wird, wenn sich eine virtuelle Ressource dem Enddatum des Leasingvertrags nähert. Wenn die Bedingungen in der Richtlinienregel erfüllt sind, sendet die Richtlinien-Engine eine Benachrichtigung an den Besitzer der Ressource und führt Vorgänge für die Ressource aus.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel arbeiten Sie mit der Richtlinie `Leasingende ServiceNow`. Die Richtlinie führt die folgenden Aktionen aus, wenn die Bedingungen in der Richtlinienregel erfüllt sind:

- Senden einer Benachrichtigung an den Besitzer einer Cloud-Ressource, wenn der Leasingvertrag für die Ressourcen in Kürze ausläuft.
- Ausführen eines Vorgangs `Stoppen` für die Ressource.
- Ausführen eines Vorgangs `Bereitstellung aufheben` für die Ressource.

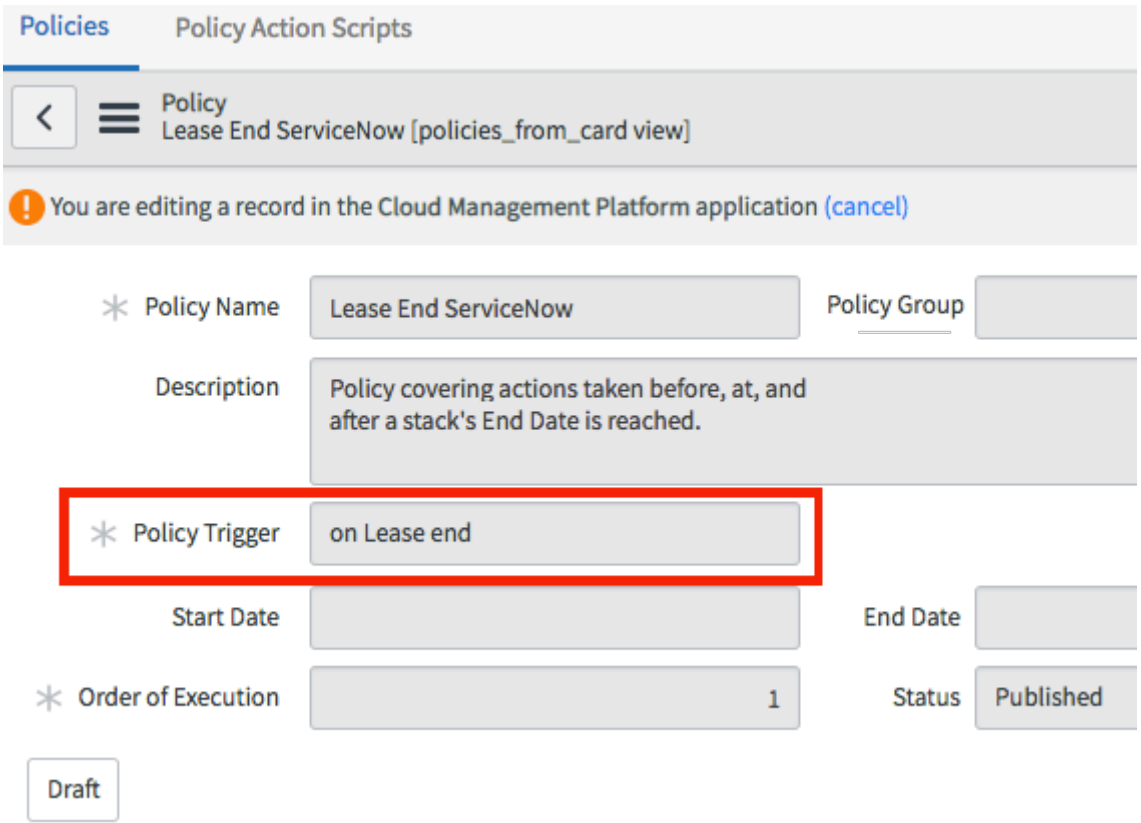
Sie können jede Basissystem-Richtlinie ändern, indem Sie Einstellungen ändern oder die Richtlinie aktivieren oder deaktivieren.

Hinweis: Geplante Start-/Stoppvorgänge werden in der Terraform-Vorlage und den Google Deployment Manager (GDM)-Stapeln nicht unterstützt.

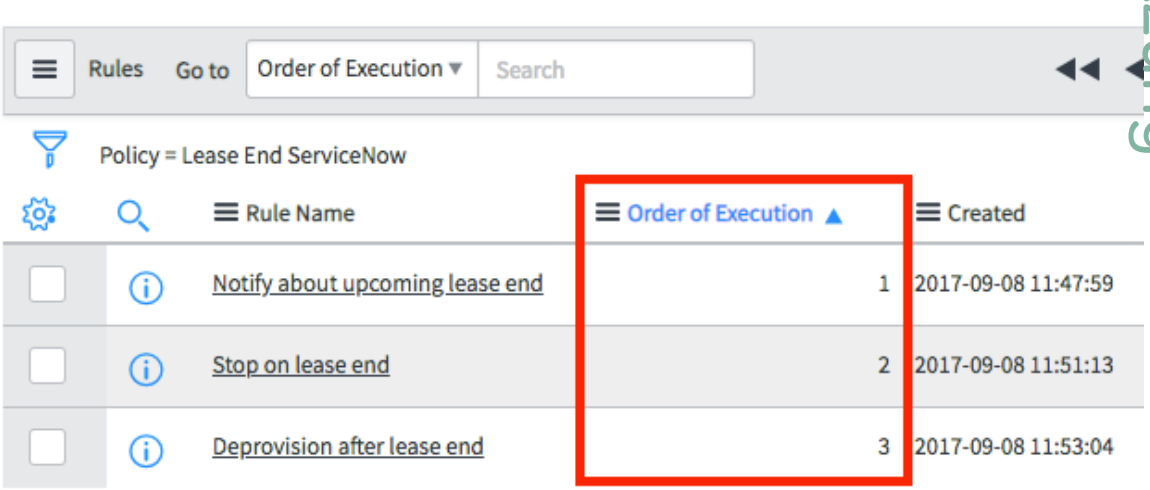
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Suchen Sie nach der Richtlinie **Leasingende ServiceNow**, und öffnen Sie sie.
3. Beachten Sie, dass der Auslöser **bei Leasingsende** lautet, was bedeutet, dass die Richtlinie ausgelöst wird, wenn der Leasingvertrag für die Ressource fast abgelaufen ist.



4. Sortieren Sie die zugehörige Liste „Regeln“ nach **Reihenfolge der Ausführung**.
   Die Regel mit der niedrigsten Nummer wird zuerst ausgeführt.



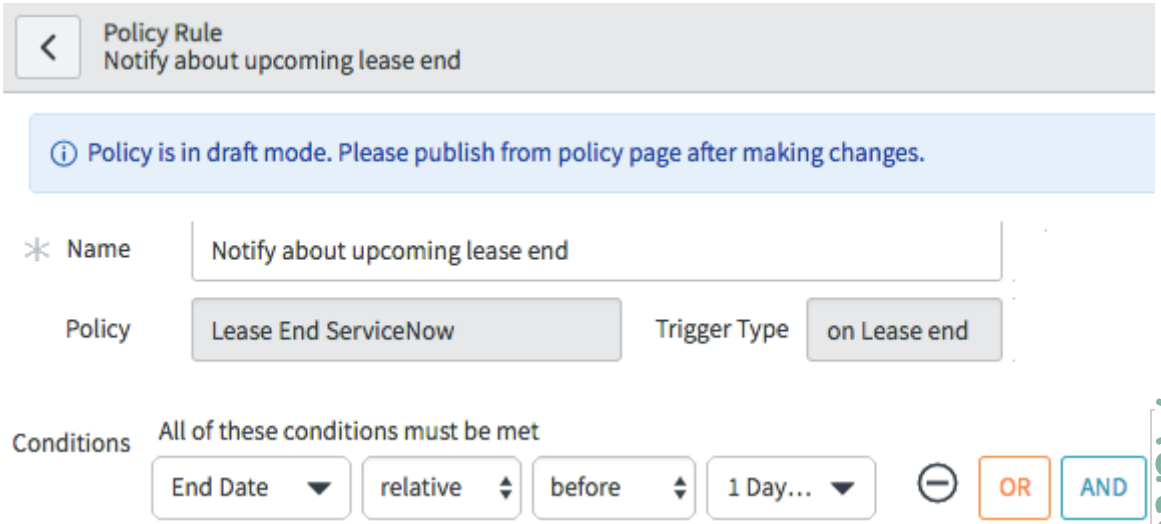
Beachten Sie, dass eine Benachrichtigungsregel zuerst ausgeführt wird, gefolgt von den Vorgängen `Stoppen` und `Bereitstellung aufheben` für die Ressource.

5. Klicken Sie auf die Regel **bei bevorstehendem Leasingende benachrichtigen**.

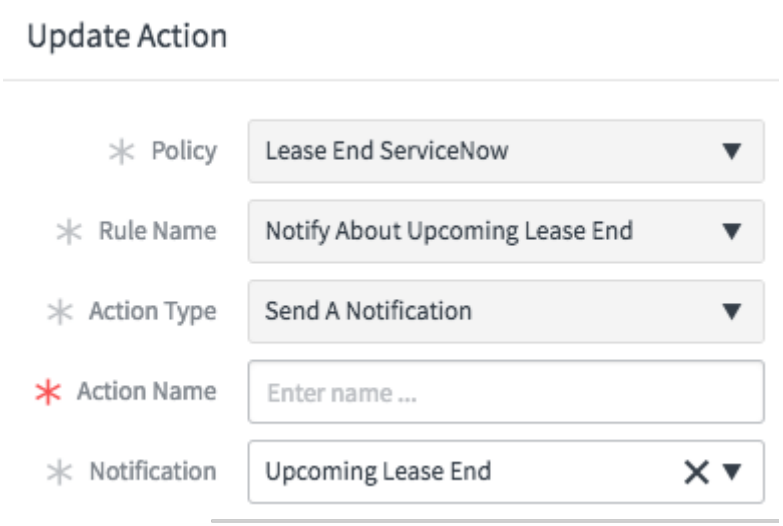
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Beachten Sie, dass die Regel eine Bedingung angibt: Wenn das aktuelle Datum einen Tag vor dem Enddatum liegt, wird `true` zurückgegeben.



7. Klicken Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf den (leeren) **Namen** der Aktion.
8. Geben Sie im Popup-Fenster „Aktion aktualisieren“ einen ein **Aktionsname** (Der Wert ist erforderlich), beachten Sie den Wert von **Benachrichtigung** (Sie werden es im nächsten Schritt verwenden) und schließen Sie dann das Popup-Fenster.



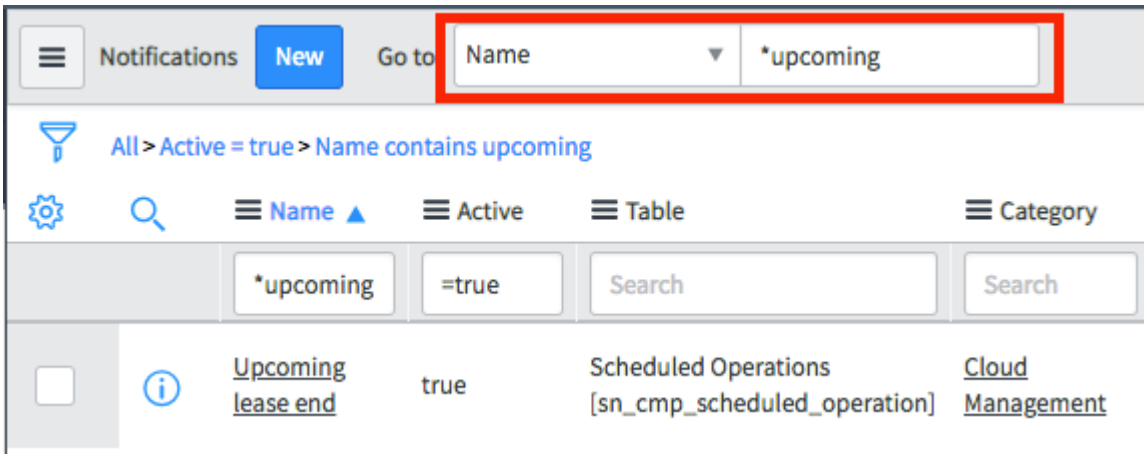
9. Überprüfen Sie die anderen Einstellungen der Benachrichtigungsnachricht:

   a. Auf der -Instanz (nicht der Portal für Cloud-Admin.), navigieren Sie zu **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**an.

   b. Suchen Sie nach der in der Aktion angegebenen Benachrichtigung, indem Sie den Filtertext `*Bevorstehendes Leasingende` für **Name** eingeben, und öffnen Sie sie:

Automatische Übersetzung

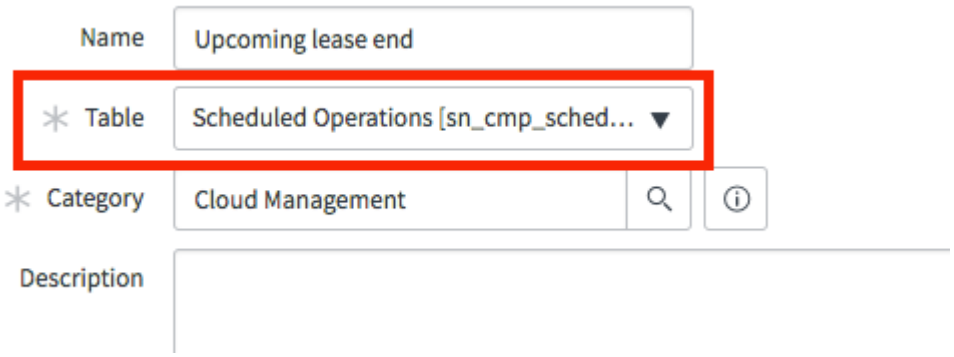
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Klicken Sie auf **Bevorstehendes Leasingende**, um das Benachrichtigungsformular zu öffnen.

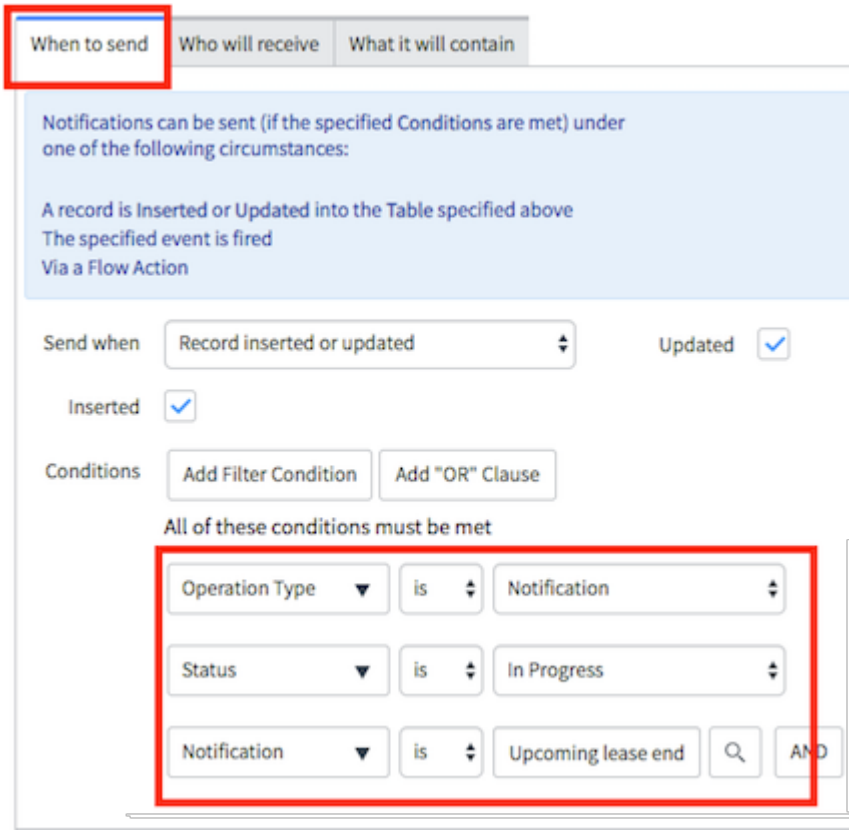
Beachten Sie, dass die Tabelle **Geplante Vorgänge [sn_cmp_scheduled_operation]** angegeben ist.

Hinweis: Sie basieren alle Benachrichtigungen für Cloud Provisioning and Governance auf dieser Tabelle.



d. Beachten Sie auf der Registerkarte **Absendezeitpunkt** die geltenden Bedingungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Bedingung	Beschreibung
Vorgangstyp ist „Benachrichtigung“	Gibt an, dass das Feld **Vorgangstyp** in der Tabelle „Geplante Vorgänge“ **Benachrichtigung** lauten muss.
Status	Gibt an, dass das System die Benachrichtigung auslösen soll, wenn der Status des Datensatzes des geplanten Vorgangs in Bearbeitung ist, anstatt zu warten, bis er abgeschlossen ist.
Benachrichtigung	Gibt an, dass die Benachrichtigung *`Upcoming lease end`* angegeben werden muss.

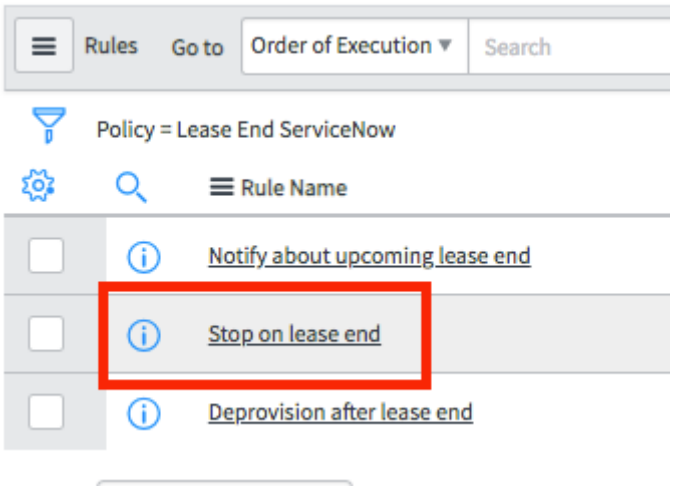
Hinweis: Wenn Sie eine benutzerdefinierte Benachrichtigung erstellen, verwenden Sie die Standardbedingungen, ändern Sie jedoch die Bedingung **Benachrichtigung** in den Namen Ihrer Benachrichtigung.

e. Klicken Sie auf die Registerkarte **Empfänger**.

Beachten Sie, dass der Wert für **Benutzer/Gruppen in Feldern** auf `Target.Assigned to, Target.Owned` festgelegt ist. Verwenden Sie diese Einstellungen, um die Benachrichtigung an den Besitzer der virtuellen Ressource zu senden.

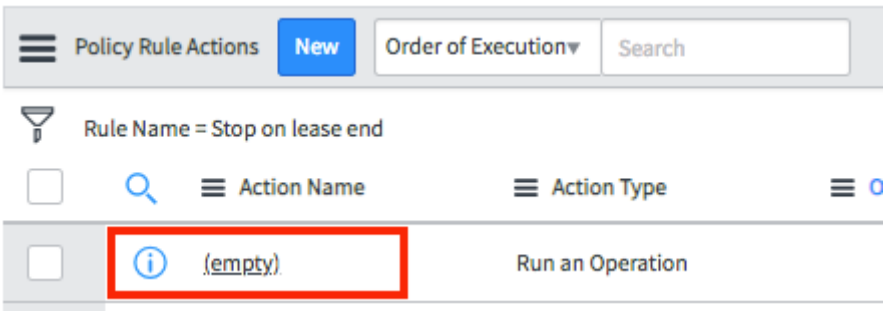
10. Öffnen Sie im Portal für Cloud-Admin. die Richtlinie „Leasingende ServiceNow“ erneut, und öffnen Sie dann die Regel **bei Leasingende stoppen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

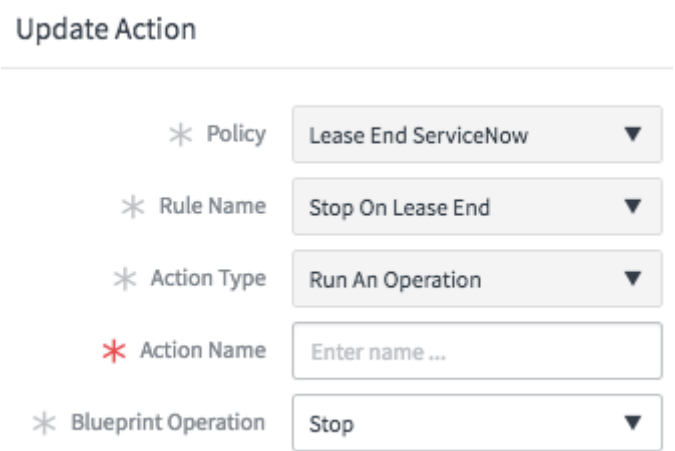


Die Regel hat zwei Aktionen: eine Aktion zum Senden einer Benachrichtigung und die andere Aktion zum Ausführen des Vorgangs *`Stoppen`* für die virtuelle Ressource.

11. Klicken Sie bei dem Vorgang *`Stoppen`* auf den (leeren) **Aktionsnamen** der Aktion.



12. Beachten Sie im Popup-Fenster „Aktualisierungsaktion“ die Einstellungen:



Feld	Beschreibung
Richtlinien- und Regelname	Die Richtlinie und die Regel, zu denen diese Aktion gehört, werden standardmäßig in diesen Feldern angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktionstyp	**Vorgang ausführen** weist die Richtlinien-Engine an, einen Standardvorgang (`Starten`, `Stoppen`, `Bereitstellung aufheben` usw.) für die Ressource auszulösen.
Planvorgang	Das System führt den Vorgang `STOPPEN` für die Ressource aus.

Die andere Regel, **Bereitstellung nach Leasingende aufheben**, führt den Vorgang `Bereitstellung aufheben` für die Ressource aus, damit sie nach dem Leasingenddatum nicht mehr aktiv bleibt.

Nächste Maßnahme

In diesem Beispiel werden die über die Formularkonfiguration verfügbaren Einstellungen verwendet. Beispielskripts, die Sie zusätzlich verwenden könnten, finden Sie unter Richtlinienaktionsskript erstellen.

Auslöser für Cloud-Richtlinien

Auslöser sind Ereignisse, die die Richtlinien-Engine in Bewegung setzen. Beispielsweise wird der Auslöser `bei Ende der Katalogelementanforderung` ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Wenn der Auslöser für eine Richtlinie ausgelöst wird, testet die Richtlinien-Engine die in der Richtlinienregel angegebenen Bedingungen und führt die in der Regel angegebenen Aktionen aus, wenn die Bedingungen erfüllt sind.

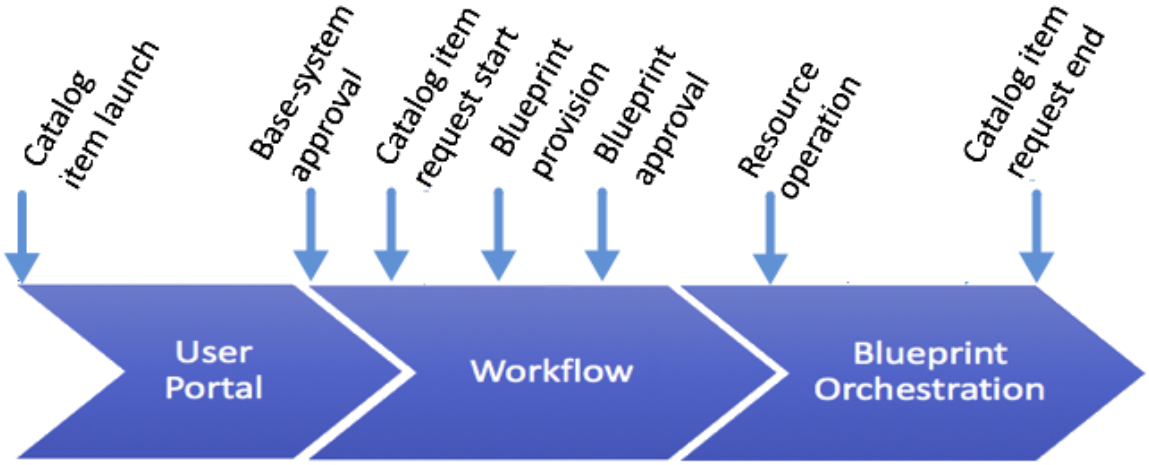
Auslöser

- Sie verweisen normalerweise auf eine Richtlinie anhand des Namens des Auslösers der Richtlinie. Beispielsweise können Sie eine Richtlinie, die durch den Auslöser `bei Leasingende` ausgelöst wird, als „Richtlinie für Leasingende“ bezeichnen.
- Auslöser basieren häufig auf Anwenderanforderungen und den Vorgängen (Start, Stopp, Bereitstellung oder Aufhebung der Bereitstellung), die auf einem Blueprint, einem Katalogelement, einer Ressource oder einem Stapel ausgeführt werden können. Einige Auslösertypen geben keinen Cloud-Vorgang an. Zum Beispiel erfolgt die Auslösung des Auslösers `bei Leasingende` unabhängig von jedem Vorgang.
- Um die Leistung zu optimieren, beschränken Sie die Anzahl der Richtlinien mit allgemeinen Auslösern wie den Auslösern `bei Katalogelement`.
- Ein Auslöser, der kein Ziel (eine Blaupause, ein Katalogelement, einen Stapel oder eine Ressource) angibt, wird immer ausgeführt. Um die Leistung zu optimieren, minimieren Sie daher die Verwendung solcher Richtlinien.

Wichtig: Blueprints sind veraltet. Die Auslöserbeschreibungen, die dem folgenden Zeitlinienschema folgen, gelten auch für die Erstellung Cloud-Vorlagenbasierter Kataloge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitleiste des Bereitstellungsauslösers



Richtlinienauslöser

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind

Auslösername und -aktionen	Beschreibung
on Blueprint provision (bei Blaupausenbereitstellung) Aktionen: • Skript ausführen • Eigenschaft außer Kraft setzen • Prozess abbrechen	Der Auslöser `bei Blaupausenbereitstellung` wird nach der Ausführung der Richtlinien `bei Beginn der Katalogelementanforderung` ausgelöst. Durch eine Richtlinie, die durch den Auslöser `bei Blaupausenbereitstellung` ausgelöst wird, kann ein Skript ausgeführt, ein vom Benutzer angeforderter Attributwert außer Kraft gesetzt oder ein Bereitstellungsvorgang abgebrochen und eine entsprechende Nachricht gesendet werden. Verwenden Sie diesen Auslöser, um einen vom Benutzer eingegebenen Wert außer Kraft zu setzen. Wenn ein Benutzer beispielsweise für ein Attribut einen Wert wie den Stapelnamen auswählt, kann der Name des Stapels durch eine Richtlinie mit diesem Auslöser geändert werden. Darüber hinaus kann durch eine weitere Aktion der Name wieder geändert werden, wenn der Benutzer die Ressource schließlich bereitstellt. Der Benutzer sieht den endgültigen Wert nicht im Formular des Katalogelements, da die Änderung zur Bereitstellungszeit vorgenommen wird. Aktion für eine Richtlinie „bei Blaupausenbereitstellung“ erstellen
Genehmigungsauslöser • **bei Genehmigung des Stapelvorgangs**: Wird während eines beliebigen Stapelvorgangs im Cloudbenutzerportal ausgelöst.	Eine Cloud-Genehmigungsrichtlinie gibt die Anwender an, die eine bestimmte Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann. Genehmiger können den Manager des Benutzers, der eine Anforderung sendet, einen angegebenen Benutzer oder eine bestimmte Gruppe oder Benutzer mit einer bestimmten Rolle einschließen. Sie können mehrere Genehmiger angeben. Genehmigungen erfolgen in der von Ihnen angegebenen Reihenfolge. Eine Richtlinie, die durch einen der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
• **bei Genehmigung des Stapelressourcenvorgangs**: Wird während eines Ressourcenvorgangs (Starten, Stoppen, Bereitstellung usw.) im Cloudbenutzerportal ausgelöst. • **bei Aufgabenremediation**: Wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt. Aktionen: • ServiceNow Genehmigung • Benutzerdefinierte Genehmigung	Genehmigungsauslöser ausgelöst wird, kann Genehmigungs-Subflows starten. Die gezielten Genehmigungsrichtlinien ergänzen die Basissystem-Genehmigungsvorgänge. **Hinweis:** Der Genehmigungsprozess wird ausgeführt, nachdem die Eigenschaften festgelegt wurden, da überschriebene Eigenschaftswerte zu einer Änderung der Kosten führen könnten. `on Blueprint provision (approval)` (bei Blaupausenbereitstellung (Genehmigung)) wird angewendet, bevor die Blaupause bereitgestellt wird. Da durch den Bereitstellungsprozess jedoch Anforderungsdaten (und möglicherweise auch Kosten) geändert werden können, werden Genehmigungsprozesse nach der Bereitstellung der Blaupause ausgeführt. Verwenden Sie `on Stack operation (approval)` (bei Stapelvorgang (Genehmigung)) zum Ausführen eines Genehmigungs-Workflows, wenn ein Vorgang auf einem Stapel ausgeführt wird. Standardmäßig wird eine Change-Anforderung erzeugt, wenn ein Vorgang für einen Stapel ausgeführt wird. Sie erfordert jedoch keine Genehmigung. Durch diesen Auslöser kann eine obligatorische Genehmigung gestartet werden. Verwenden Sie `on Stack operation (approval)` (bei Stapelvorgang (Genehmigung)) zum Ausführen eines Genehmigungs-Workflows, wenn ein Vorgang für eine einzelne Ressource ausgeführt wird, die Teil eines Stapels ist. Standardmäßig wird eine Change-Anforderung erzeugt, wenn ein Vorgang für einen Stapel ausgeführt wird. Sie erfordert jedoch keine Genehmigung. Durch diesen Auslöser kann eine obligatorische Genehmigung gestartet werden. Eine Richtlinie, die von ausgelöst wird `Bei Aufgabenkorrektur` Der Auslöser kann Genehmigungs-Subflows starten. Erstellen Sie eine Aktion für eine Genehmigungsrichtlinie
beim Starten des Katalogelements Aktionen:	Der Auslöser `beim Starten des Katalogelements` wird ausgelöst, wenn ein Bestellformular (Stapelanforderungsformular) für ein Katalogelement gestartet wird. Eine Richtlinie, die durch den Auslöser `beim Starten des Katalogelements` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
• Skript ausführen • Eigenschaft außer Kraft setzen	Verwenden Sie diesen Auslöser, um zu steuern, was der Benutzer beim Öffnen des Formulars im Cloudbenutzerportal sieht. Beispielsweise können Sie einen Standardwert außer Kraft setzen, der dem Benutzer zuerst angezeigt wird. Der Benutzer kann diesen Wert im Katalogelementformular sehen. Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Aktion für eine Richtlinie „beim Starten des Katalogelements“ erstellen
bei Beginn der Katalogelementanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser `bei Beginn der Katalogelementanforderung` wird ausgelöst, nachdem der Benutzer ein Anforderungsformular geöffnet hat. Eine Richtlinie, die von ausgelöst wird `Beim Start der Katalogelementanforderung` Oder `Bei Ende der Katalogelementanforderung` Der Auslöser kann ein Skript oder einen Subflow ausführen. Sie können diesen Auslöser verwenden, um ein benutzerdefiniertes Skript oder einen Workflow auszuführen, mit dem Unternehmensprozesse wie die benutzerdefinierte Genehmigung abgewickelt werden können, bevor die Anforderung des Katalogelements verarbeitet wird. Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen
bei Ende der Katalogelementanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser `bei Ende der Katalogelementanforderung` wird ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Eine Richtlinie, die von ausgelöst wird `Beim Start der Katalogelementanforderung` Oder `Bei Ende der Katalogelementanforderung` Der Auslöser kann ein Skript oder einen Subflow ausführen. Verwenden Sie diesen Auslöser, um einen Workflow zu starten, nachdem eine Katalogelementanforderung verarbeitet wurde. Erwägen Sie diesen Auslöser als einen Schritt nach der Bereitstellung. Beispielsweise könnten Sie einen Workflow zum Installieren von MySQL auf der bereitgestellten Ressource starten. Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
bei Leasing-Ende Aktionen: • Vorgang ausführen • Benachrichtigung senden	Eine Richtlinie, die durch den Auslöser `bei Leasingende` ausgelöst wird, kann eine Benachrichtigung senden oder einen Lebenszyklusvorgang `Starten`, `Stoppen` oder `Bereitstellung aufheben` ausführen. Aktion für eine Richtlinie „Mietvertragsende“ erstellen
beim Start des Ressourcenvorgangs Aktionen: • Skript ausführen • Eigenschaft außer Kraft setzen	Der Auslöser `beim Start des Ressourcenvorgangs` wird ausgelöst, bevor der Katalog für einen Ressourcenvorgang aus dem Cloudbenutzerportal geladen wird. Eine Richtlinie, die durch den Auslöser `beim Start des Ressourcenvorgangs` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte). Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Aktion für eine Richtlinie „beim Start des Ressourcenvorgangs“ erstellen
beim Start der Ressourcenvorgangsanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser `beim Start der Ressourcenvorgangsanforderung` wird ausgelöst, nachdem ein Benutzer eine Ressourcenvorgangsanforderung (`Starten`, `Stoppen`, `Bereitstellung aufheben`) übermittelt hat. Eine Richtlinie, die durch den Auslöser `beim Start der Ressourcenvorgangsanforderung` oder `bei Ende der Ressourcenvorgangsanforderung` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben. Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen
bei Ende der Ressourcenvorgangsanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser `bei Ende der Ressourcenvorgangsanforderung` wird vor Abschluss eines Lebenszyklusvorgangs für eine Ressource (`Starten`, `Stoppen`, `Bereitstellung aufheben`) ausgelöst. Eine Richtlinie, die durch den Auslöser `beim Start der Ressourcenvorgangsanforderung` oder `bei Ende der Ressourcenvorgangsanforderung` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben. Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
bei Ressourcenvorgang Aktionen: • Eigenschaft außer Kraft setzen • Skript ausführen • Cloud-API aufrufen • IP-Adressverwaltung	Der Auslöser `bei Ressourcenvorgang` wird während des Orchestration-Prozesses ausgelöst, wenn ein Benutzer einen Lebenszyklusvorgang `Starten`, `Stoppen` oder `Bereitstellung aufheben` für eine bestimmten Ressource durchführt. Eine Richtlinie, die durch den Auslöser `bei Ressourcenvorgang` ausgelöst wird, kann einen von einem Benutzer angeforderten Attributwert überschreiben, ein Skript ausführen, eine Cloud API aufrufen oder einen IP-Adressenverwaltungsvorgang ausführen. Aktion für eine Richtlinie „bei Ressourcenvorgang“ erstellen

Cloud-Richtlinie erstellen

Eine Cloud-Richtlinie kann einen von einem Anwender festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorab ausfüllen oder ausblenden, anwenderdefinierte Skripts ausführen und aufrufen Cloud-API, Oder starten oder brechen Sie Subflows ab. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.

Vorbereitungen

- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

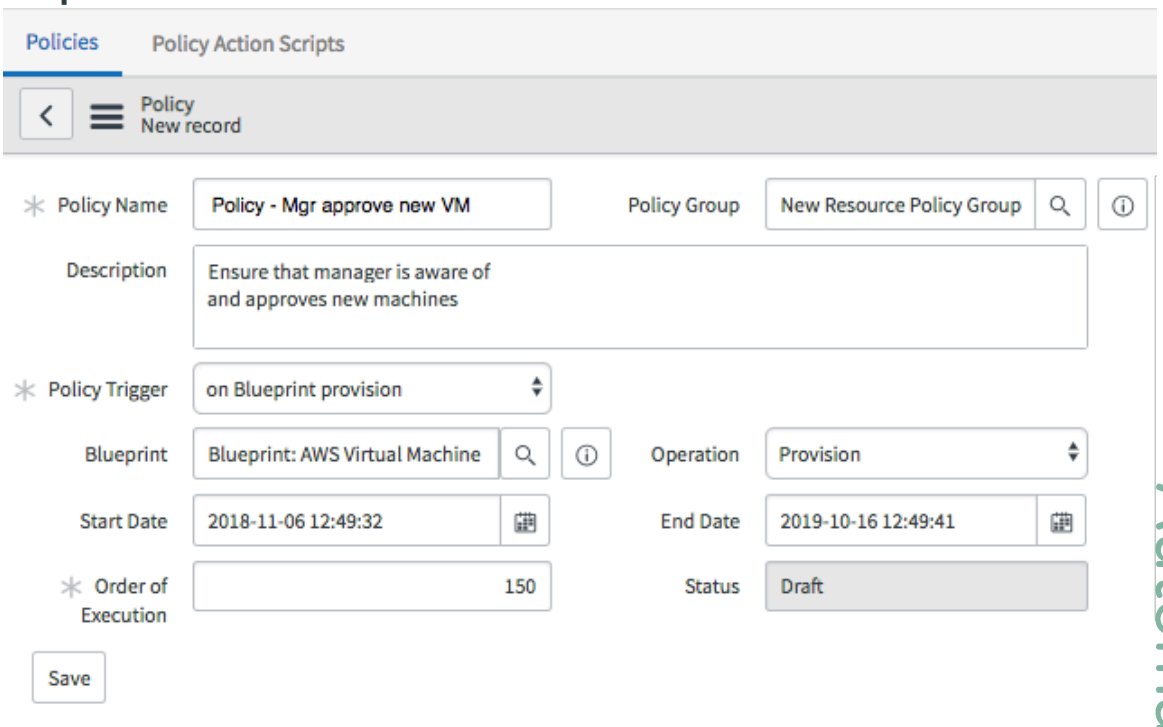
Dieses Verfahren beschreibt alle Richtlinientypen mit Ausnahme von Genehmigungsrichtlinien (`bei Genehmigung der Blaupausenbereitstellung`, `bei Genehmigung des Stapelvorgangs`, `bei Genehmigung des Stapelressourcenvorgangs` und `bei Aufgabenremediation`). Unter Cloud-Genehmigungsrichtlinie erstellen finden Sie Anweisungen zum Erstellen einer Richtlinie mit einem Genehmigungsauslöser.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Richtlinienformular



Feld	Beschreibung
Richtlinienname	Ein beschreibender Name, der das Wort Richtlinie enthält. Beginnen Sie den Namen nicht mit einer Zahl.
Beschreibung	Eine Beschreibung der Absicht der Richtlinie
Richtliniengruppe	Eine Richtliniengruppe, zu der die Richtlinie gehört
Richtlinienauslöser	Auslöser, mit dem festgelegt wird, wann die Richtlinie angewendet werden soll. Zum Beispiel wendet der Auslöser **bei Leasingende** die Richtlinie an, wenn der Leasingvertrag für einen Stapel endet. Weitere Informationen finden Sie unter Auslöser für Cloud-Richtlinien.
Ressourcenblock [wird angezeigt, wenn der Auslöser *bei Ressourcenvorgang* ausgewählt ist]	Ressourcenblock, auf den die Richtlinie angewendet wird
Vorgang [wird angezeigt, wenn der Auslöser *bei Blaupausenbereitstellung*, *bei Genehmigung der Blaupausenbereitstellung* oder *bei Ressourcenvorgang* ausgewählt ist]	Wählen Sie den Vorgang aus, für den die Richtlinie gilt. Beispielsweise kann eine Richtlinie nur für den Vorgang *Bereitstellung aufheben* oder für alle Vorgänge für die Blaupause oder das Katalogelement gelten. **Hinweis:** Wenn kein Vorgang angegeben ist, gilt die Richtlinie für alle Vorgänge. Diese Bedingung kann die Leistung beeinträchtigen. ○ **Alle**: Beliebiger Vorgang wird ausgeführt. ○ **Starten**: Die Ressource wird gestartet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Stoppen**: Die Ressource wird gestoppt. ○ **Bereitstellung**: Die Ressource wird bereitgestellt. ○ **Bereitstellung aufheben**: Die Ressource ist für Benutzer nicht mehr verfügbar. ○ **Skript ausführen**: Ein Skript wird mit der Ressource ausgeführt.
Moment [wird angezeigt, wenn der Auslöser *bei Ressourcenvorgang* ausgewählt ist]	Geben Sie an, wann die Richtlinie durchgesetzt werden soll: ○ **Vor dem Vorgang**: Vor dem Start des angegebenen Vorgangs. ○ **Nach dem Vorgang**: Nach Abschluss des angegebenen Vorgangs. **Hinweis:** Wenn Sie Infoblox integriert haben, verwenden Sie **Vor dem Vorgang** für einen virtuellen vSphere-Computer. Verwenden Sie **Nach dem Vorgang** für AWS- und Azure-Clouds, da AWS und Azure die Zuteilung von IP-Adressen steuern. Sie können die mit Infoblox bereitgestellte IP-Adresse registrieren.
Katalogelement [wird angezeigt, wenn ein Auslöser *beim Starten des Katalogelements*, *bei Beginn der Katalogelementanforderung* oder *bei Ende der Katalogelementanforderung* ausgewählt ist]	Wählen Sie das Katalogelement aus, für das die Richtlinie gilt.
Startdatum/Enddatum	Geben Sie das Startdatum an, ab dem die Richtlinie berücksichtigt werden soll, und das Enddatum, ab dem die Richtlinie nicht mehr berücksichtigt werden soll.
Reihenfolge der Ausführung	Geben Sie eine Zahl an, die die Reihenfolge darstellt, in der die Richtlinie angewendet wird. Eine Richtlinie mit einer niedrigeren Nummer wird vor einer Richtlinie mit einer höheren Nummer ausgeführt. Beispielsweise wird eine Richtlinie mit einer **Reihenfolge** von **100** vor einer Richtlinie mit einer **Reihenfolge** von **200** ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Eigenschaft **Reihenfolge der Ausführung** gilt nicht für `Bei Blueprint-Bereitstellung (Genehmigung)`, `Bei Stapelvorgang (Genehmigung)`, `Bei Stapelressourcenvorgang (Genehmigung)`, Und `Bei Aufgabenkorrektur` -Richtlinien. Weitere Detailinformationen finden Sie unter Cloud-Genehmigungsrichtlinie erstellen.
Status	○ **Veröffentlichte** Richtlinien werden erzwungen. Sie können eine Richtlinie im Status **Veröffentlicht** nicht bearbeiten. Zum Bearbeiten einer Richtlinie im Status **Veröffentlicht** klicken Sie im Formularheader auf **Entwurf**. ○ Sie können Richtlinien im Status **Entwurf** bearbeiten. Richtlinien im Status **Entwurf** werden nicht erzwungen. Zum Durchsetzen einer Richtlinie klicken Sie im Formularheader auf **Veröffentlichen**.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.

Nächste Maßnahme
Konfigurieren Sie eine Cloud-Richtlinienregel für die Richtlinie.

Cloud-Richtlinienregel konfigurieren

Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

Vorbereitungen
Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

- Eine Richtlinie kann mehrere Regeln enthalten. Sie können die Reihenfolge konfigurieren, in der Regeln angewendet werden.
- Jede Regel wird vollständig ausgeführt.
- Jeder Regelfehler beendet die Ausführung. Ausnahme: Richtlinien, für die kein Vorgang angegeben ist.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, und geben Sie einen beschreibenden **Namen** für die Regel ein.

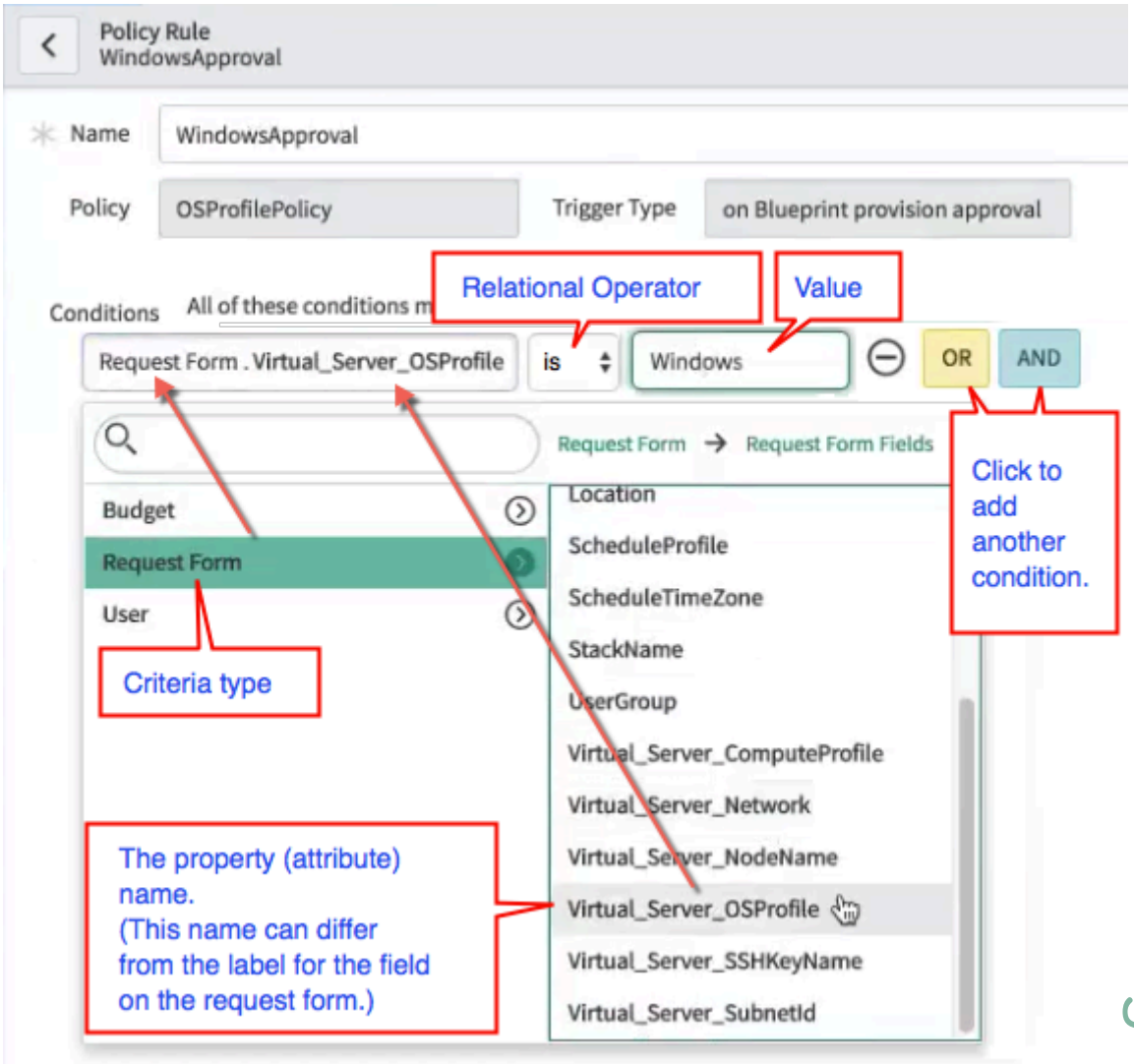
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Regelname darf nicht mit dem Richtliniennamen identisch sein.
- Beginnen Sie den Regelnamen nicht mit einer Zahl.

4. Geben Sie mit dem Condition Builder im Basissystem die **Bedingungen** an, die erfüllt sein müssen, damit die Richtlinien-Engine die Aktionen ausführt.

   Die folgende Beispielregel wird auf eine Genehmigungsrichtlinie für eine Blaupausenbereitstellung angewendet. Die Bedingung ergibt „true“, wenn das Feld **BS-Profil** auf dem Anforderungsformular den Wert „Windows“ aufweist.



Automatische Übersetzung

Feld	Beschreibung
[Kriterientyp]	Wählen Sie eine der folgenden Optionen aus: ○ **Anforderungsformular**: Basieren Sie die Bedingung auf einem Eigenschaftswert (Attributwert) im Anforderungsformular im Cloudbenutzerportal. Geben Sie an, welche Eigenschaft geprüft werden soll. Im Beispiel prüft die Bedingung, ob das Feld „BS-Profil“ auf dem Anforderungsformular den Wert „Windows“ aufweist. ○ **Benutzer**: Basieren Sie die Bedingung auf einer Benutzerrolle oder auf der Gruppe, der der Benutzer angehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

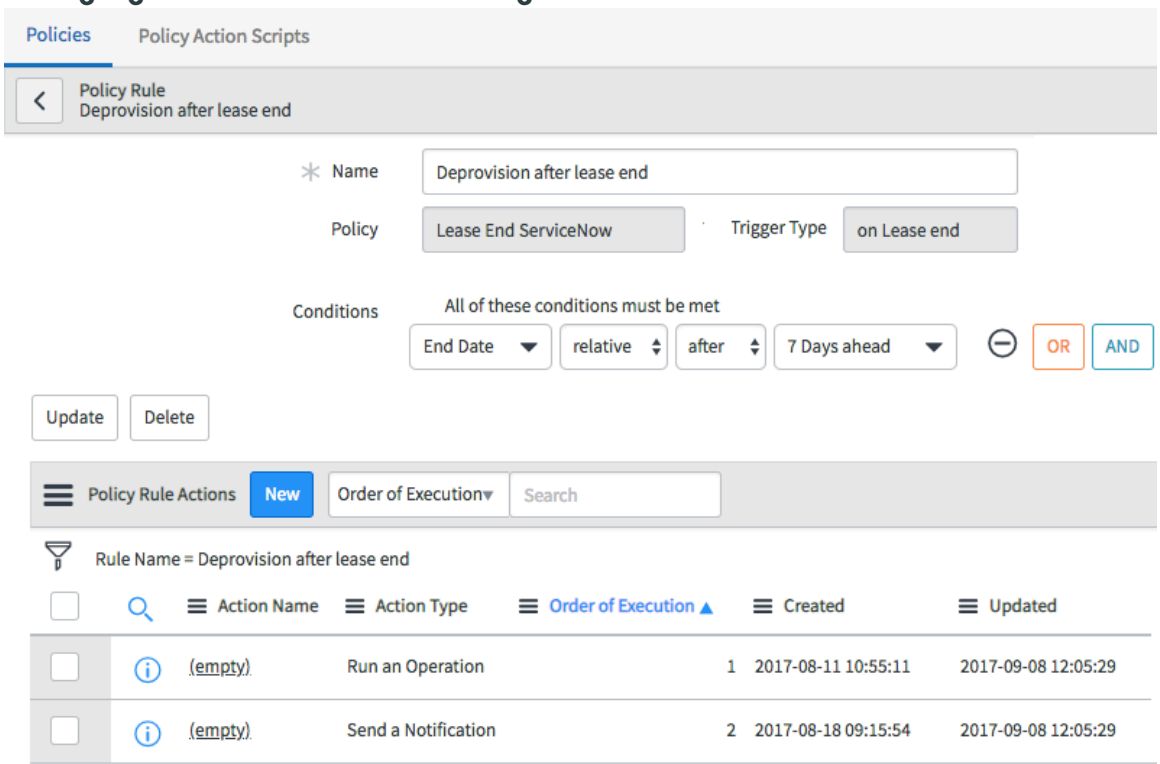
Feld	Beschreibung
	Wählen Sie beispielsweise Folgendes aus, um eine Bedingung zu erstellen, die zutrifft, wenn der Benutzer zur Gruppe „Marketing“ gehört: ▪ [Kriterientyp]: Benutzer ▪ [Benutzerentität]: Gruppe ▪ [Relationale Operatoren]: Entspricht ▪ [Gruppe]: Marketing **Hinweis:** Verwenden Sie verschiedene Kriterien, um eine Bedingung für Richtlinien zu erstellen, die vom Auslöser bei Leasingende ausgelöst werden. Sehen Sie sich das Beispiel unter dieser Tabelle an.
[Relationaler Operator]	Wählen Sie einen entsprechenden Operator aus.
[Wert]	Geben Sie je nach ausgewähltem [Kriterientyp] einen Wert ein oder wählen Sie einen aus. ○ Geben Sie bei **Anforderungsformular** einen Wert für das Attribut ein. ○ Für **Anwender** > **Gruppe**, Wählen Sie eine Gruppe aus. ○ Für **Anwender** > **Rolle**, Wählen Sie eine Rolle aus.
[Logischer Operator]	Wenn Sie mehrere Bedingungen definieren, wählen Sie einen logischen Operator **ODER** oder **UND** aus, der die logische Beziehung zur nächsten Bedingung angibt.

5. Klicken Sie auf **Absenden**.

Example:
Verwenden Sie für Richtlinien, die durch den Auslöser bei Leasingende ausgelöst werden, den Datums-Bedingungsgenerator im Basissystem, um die zu prüfende Bedingung zu konfigurieren. Zusätzlich zur Bedingung zeigt das folgende Beispiel die Aktionen, die die Richtlinien-Engine durchführt, wenn die Bedingung erfüllt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingung und Aktionen für eine Leasingende-Richtlinie



Nächste Maßnahme

Erstellen Sie die Richtlinienaktionen, die ausgeführt werden sollen, wenn alle Bedingungen der Regel als „true“ ausgewertet werden.

Ausdrücke in Cloud Provisioning and Governance verwenden

Ausdrücke in Richtlinienaktionen können Werte festlegen oder überschreiben. Ausdrücke in Blaupausen können auf Attribute von Ressourcen zugreifen und Werte Anforderungsformularfeldern zuordnen. Ausdrücke sind in Ressourcenblöcken, Blaupausen, Richtlinien und überall sonst verfügbar, wo Cloud Provisioning and Governance Skripts zulässt.

Ausdrücke verwenden

Ausdrücke können die Werte für Informationen enthalten, die dynamisch im System generiert werden, z. B. die Werte für die Auswahlen, die Benutzer im Cloudbenutzerportal treffen. Ausdrücke sind in Ressourcenblöcken, Blaupausen, Richtlinien und überall sonst verfügbar, wo Cloud Provisioning and Governance Skripts zulässt.

Ausdrücke in Ressourcenblöcken verwenden

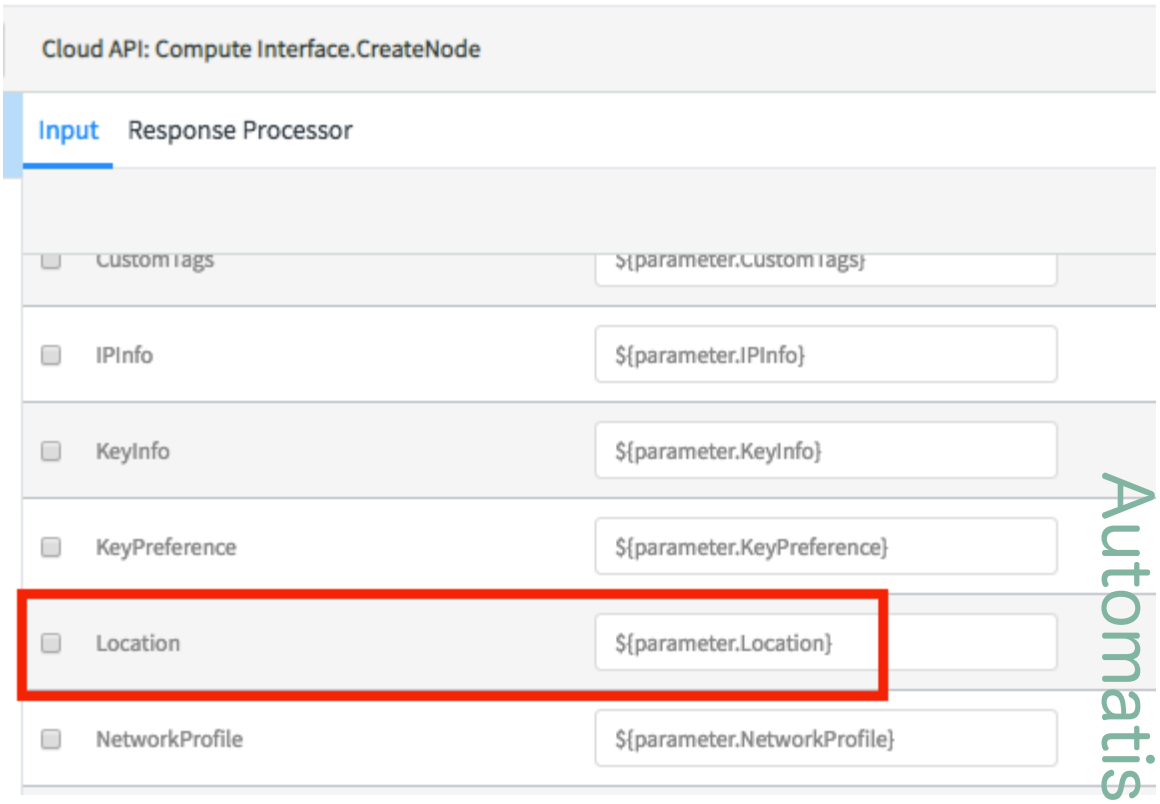
Jeder Ressourcenblockvorgang verwendet einen Ausdruck, der einen Wert für jeden Parameter enthält. Der Ausdruck kann hartcodierte Werte, Daten aus dem Stapel, den der Benutzer im Cloudbenutzerportal bereitstellt, Daten in der CMDB und Daten, die aus Skripts abgeleitet sind, verwenden. Standardmäßig generiert Cloud Provisioning and Governance eine Reihe von Parametern und ihren Ausdrücken für jeden Ressourcenblockvorgang.

Beispiel: Der Parameter *`Location`*, der das Rechenzentrum enthält, zu dem eine Ressource gehört, verwendet den Ausdruck `${parameter.Location}`.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausdrücke in einem Ressourcenblock



Ausdrücke in Blaupausen verwenden

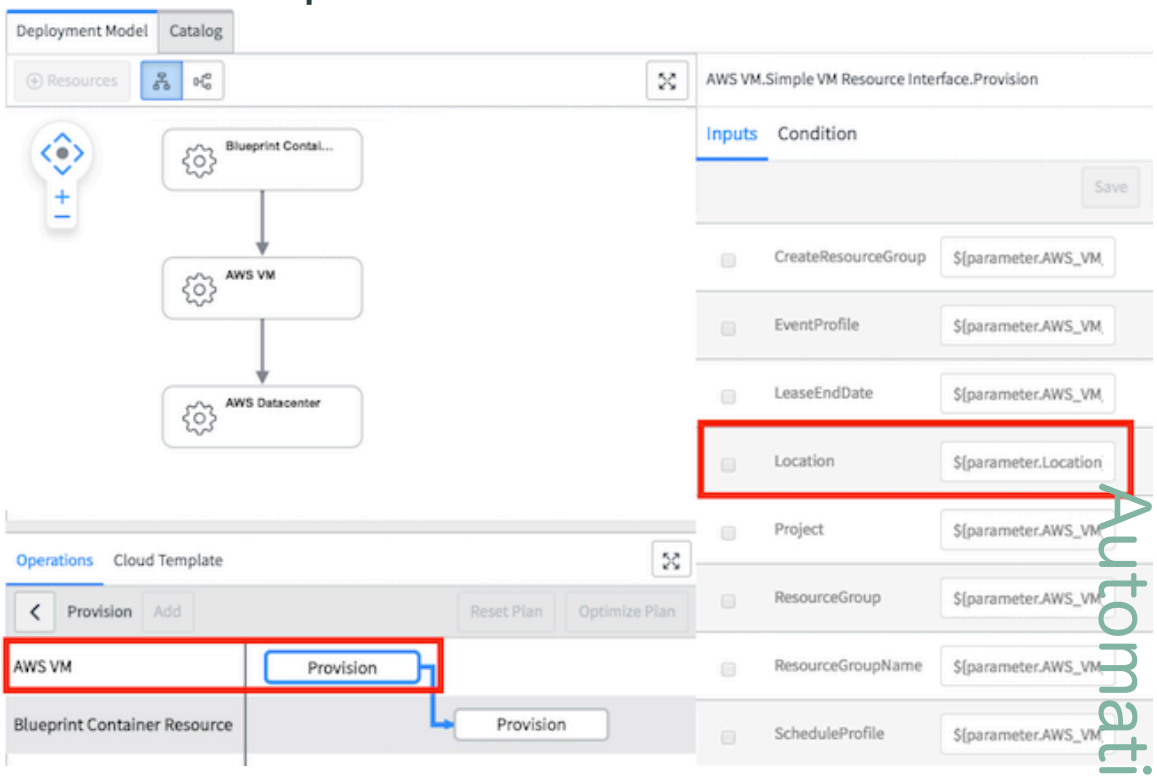
Blaupausen können Ausdrücke verwenden, um Eingabeparameter für jeden Vorgang in einem Ressourcenblock zuzuordnen. Standardmäßig zeigt die Blaupause die gleichen Parameter und Werte an, die im Ressourcenblock angegeben sind.

Sie können auf Blaupausenattribute mit Ausdrücken zugreifen. Der Ausdruck in der Spalte **Zuordnung** definiert Blaupausenattribute für jeden Vorgang in einem Schritt. Beispielsweise kann auf das Attribut **Standort**, das auf dem Stack-Anforderungsformular angezeigt wird, über den Ausdruck `${parameter.Location}` zugegriffen werden. Der Standortparameter mit dem Wert `${parameter.Location}` wird auf der Registerkarte **Eingaben** angezeigt, wenn Sie einen Blaupausenvorgang auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

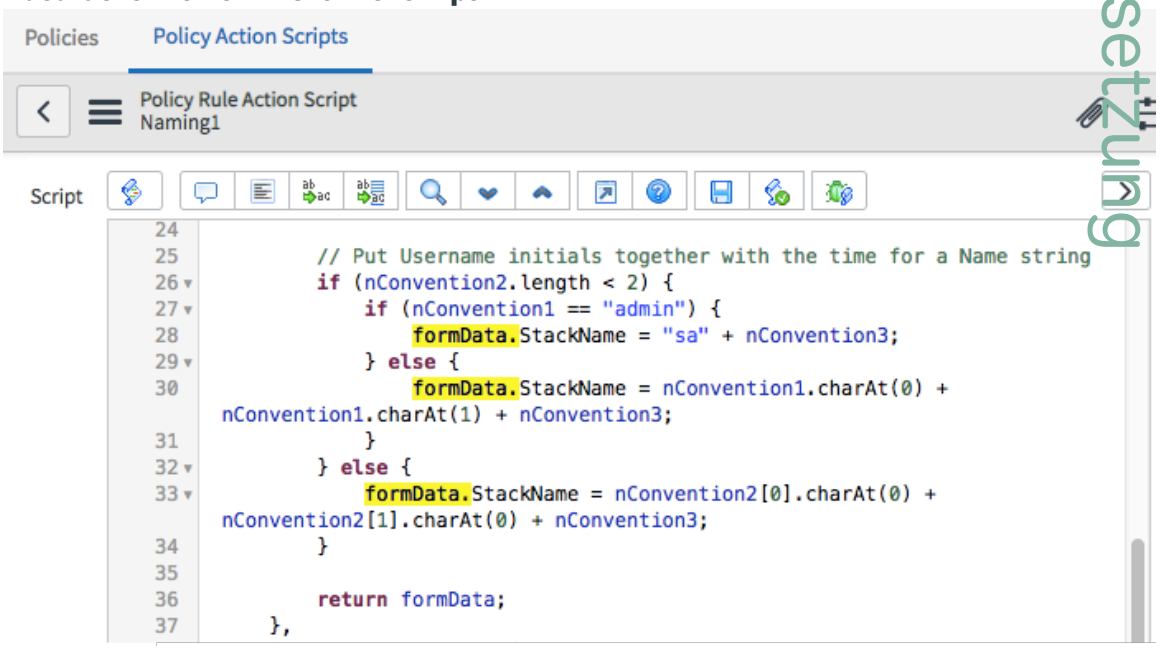
Ausdrücke in einer Blaupause



Ausdrücke in Richtlinienaktionen verwenden

Richtlinienaktionen können Ausdrücke verwenden, um Parameterwerte zu überschreiben, die Benutzer in einem Anforderungsformular im Cloudbenutzerportal übermitteln. Sie können auch in Stack-Vorgängen auf Benutzerdaten zugreifen und diese überschreiben. Verwenden Sie beispielsweise den folgenden Ausdruck, um einen Stapel umzubenennen: `formData.Stackname = "Ihre-Namenskonvention";`.

Ausdrücke in einem Richtlinienskript



Sie können auf Blaupausenattribute mit Ausdrücken zugreifen. Der Ausdruck in der Spalte **Zuordnung** definiert Blaupausenattribute für jeden Vorgang in einem Schritt. Beispielsweise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

kann auf das Attribut **Standort**, das auf dem Anforderungsformular für einen virtuellen Computer angezeigt wird, über den Ausdruck ${ param eter.Location} zugegriffen werden.

Ausdruckstypen

Definitionsausdrücke

Definitionsausdrücke sind eine Form der frühen Bindung (oder statischen Bindung). Diese Bindungen beziehen sich auf die Bindung zur Kompilierungszeit und werden ausgewertet, wenn der Benutzer das Stapelanforderungsformular übermittelt (wenn die Stapel- oder Ressourcenbereitstellung beginnt). Definitionsausdrücke haben keinen Zugriff auf die Daten, die während Orchestration generiert werden. Definitionsausdrücke werden in geschweifte Klammern eingeschlossen. Beispiel: ${parameter.CloudAccount}

Laufzeitausdrücke

Laufzeitausdrücke sind eine Form der späten Bindung (oder dynamischen Bindung). Diese Bindungen beziehen sich auf die Bindung zur Laufzeit und haben Zugriff auf die Daten, die während Orchestration erstellt werden (z. B. Stapelelemente). Laufzeitausdrücke werden ausgewertet, wenn sie während einer Ausführung von Orchestration aufgerufen werden. Laufzeitausdrücke werden normalerweise für Dot-Walking mit Daten in Tabellen verwendet. Laufzeitausdrücke sind in Klammern eingeschlossen. Beispiel: $(Stack.items[VM1].attributes[node_id])

Definitions-/Laufzeitausdrücke

Einige Ausdrücke enthalten sowohl Definitions- als auch Laufzeitausdrücke.

Komplexe Ausdrücke

Sie können Ausdrücke beliebigen Typs in anderen Ausdrücken verschachteln.

Syntax und Beispiele für Definitionsausdrücke

Die zulässige Syntax verwendet ein Dollarzeichen und geschweifte Klammern. Diese Typen sind verfügbar:

- ${parameter.}. Verwenden Sie diese Art von Ausdruck, um Werte aus Eingabeattributen von Prozessen wie der Bereitstellung von Blaupausen abzurufen. Daten werden nicht aus Tabellen abgerufen.
- ${Stack.items[]}. Verwenden Sie diese Syntax für den Zugriff auf Attribute bestimmter Elemente in einem Stapel.
- ${randomNumber}. Verwenden Sie diese Syntax, um eine Zufallszahl zu generieren. Beispielsweise können Sie eine VM mit einem zufälligen Knotennamen oder Stapelnamen bereitstellen.

Beispiele für Definitionsausdrücke

Beispiel	Beschreibung
${parameter.BillingCode}	Dieser Ausdruck zeigt, wie ein Abrechnungscode-Parameter in einer Blaupause angezeigt wird.
${parameter.formData.CatalogAttributeType}	Dieser Ausdruck verwendet ein Katalogattribut, das von einem Benutzer übermittelt wird, während der Benutzer das Formular für ein Katalogelement im Cloudbenutzerportal ausfüllt.
${parameter.userData.userId}	Dieser Ausdruck verwendet die ID eines Benutzers, während der Benutzer das Formular für ein Katalogelement im Cloudbenutzerportal ausfüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Definitionsausdrücke (Fortsetzung)

Beispiel	Beschreibung
${Stack.items[Virtueller Server].attributes[sys_id]}	Dieser Ausdruck ruft die sys_id eines virtuellen Servers ab, der Teil eines Stapels ist. „Virtueller Server“ ist der Alias eines Ressourcenblocks, der im Stapel verwendet wird.

Syntax und Beispiele für Laufzeitausdrücke

Die zulässige Syntax verwendet ein Dollarzeichen und Klammern. Diese Typen sind verfügbar:

- $(ci.tablename), wobei tablename eine Tabelle im System ist, normalerweise eine CI-Tabelle in der CMDB. Verwenden Sie diese Syntax, um auf Werte von Feldern in der Tabelle zuzugreifen.
- $(Stack.items[]). Verwenden Sie diese Syntax für den Zugriff auf Attribute bestimmter Elemente in einem Stapel.

Beispiele für Laufzeitausdrücke

Beispiel	Beschreibung
$(ci.cmdb_ci_cloud_subnet[sys_id=1223123123123123123].cidr)	Dieser Ausdruck führt ein Dot-Walking mit der Tabelle „Cloud-Subnetz“ durch, sucht den spezifischen Datensatz mit der angegebenen sys_id und übernimmt den Wert aus der Spalte cidr.
$(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}])	Dieser Ausdruck kombiniert Ausdrücke der Typen Laufzeit und Definition. Das Gleichheitszeichen „=“ wird verwendet, um einen Wert für eine Übereinstimmung auszuwerten. Der Ausdruck führt ein Dot-Walking für die Tabelle „IP-Pool“ durch und sucht nach dem Subnetz mit der Subnetz-ID, die der Benutzer übermittelt hat.
$(ci.cmdb_ci_cloud_subnet[${parameter.formData.SubnetId}].cidr)	Dieser Ausdruck kombiniert Ausdrücke der Typen Laufzeit und Definition. Der Ausdruck übernimmt den Wert des Felds **cidr** aus einem Subnetz, das der Benutzer bei der Bereitstellung ausgewählt hat. Die eckigen Klammern [] geben an, dass der Ausdruck die Tabelle „Cloud-Subnetz“ per Dot-Walking auswertet und dann den Wert für „Subnetz“ betrachtet, den der Benutzer für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Laufzeitausdrücke (Fortsetzung)

Beispiel	Beschreibung
	eine Blaupausenbereitstellung übermittelt hat. Der Ausdruck erfasst den Wert des Felds **cidr** und geht dann zu dem Wert im Feld **cidr** der sys_id des Subnetzes.
$(Stack.items[Virtueller Server].attributes[sys_id])	Wie auch im Beispiel zum Definitionsausdruck ruft dieser Ausdruck die sys_id eines virtuellen Servers ab, der Teil eines Stapels ist.

Beispielausdruck

$(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=$(Stack.items[Virtueller Server].attributes[sys_id])])].private_ip)

- *$(ci*: Laufzeitausdruck zum Abrufen von Daten aus der Tabelle.
- *cmdb_ci_nic*: CI für Netzwerkschnittstellenkarte (NIC).
- *$(Script*: Skriptbasierter Ausdruck.
- *CMPVMNICs*: Skripteinbindung.
- *getNICs*: Funktion in einer Skripteinbindung.
- *arg*: Argumente für die Funktion in der Skripteinbindung. Argumente werden durch Komma (,) getrennt, wenn mehrere Attribute vorhanden sind.
- *$(Stack.items*: Laufzeit-Stapelausdruck zum Abrufen eines Stapelelements aus einem Stapel. Argument ist der in der Blaupause angegebene Alias.
- *Virtual Server*: Alias der in der Blaupause verwendeten Ressource.
- *$(Stack.items[Virtual Server].attributes[sys_id])*: Ruft die sys_id der Ressourceninstanz des Stapelelements („Virtueller Server“) in einem Stapel ab.
- *private_ip*: Attribut von cmdb_ci_nic. Bei Bedarf durch öffentliche IP-Adresse ersetzen.

Ausdrücke

Simple parameter mapping expression

Dieser Ausdruckstyp ruft Werte aus Eingabeattributen von Prozessen ab, z. B. Blaupausenvorgängen, Ressourcenblöcken und Richtlinien. Daten werden nicht aus Tabellen abgerufen. Er ordnet Werte einer Ebene einer anderen zu, z. B. von einer Blaupause zu einer Ressource zur Cloud API.

- Typ: Definition
- Syntax: ${parameter.}
- Beispiele:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ${parameter.BillingCode} gibt den Abrechnungscode zurück.
- ${parameter.formData.CatalogAttributeType} akzeptiert ein Katalogattribut, das auf dem Anforderungsformular im Cloudbenutzerportal übermittelt wird.
- ${parameter.userData.userId} verwendet die ID eines Benutzers, der das Anforderungsformular im Cloudbenutzerportal bearbeitet.

Stack item expression

Jedes Stapelelement wird durch eine CI-Instanz in der CMDB dargestellt. Verwenden Sie Stapelelementausdrücke, um Eigenschaften der ersten Ebene im CI oder im Stapelelement selbst zu suchen, die das Stapelelement unterstützen.

- Typ: Definition/Laufzeit
- Syntax: ${Stack.items[]} oder $(Stack.items[])
- Beispiele:

  ${Stack.items[VirtualServer1].attributes[sys_id]} ist ein Ausdruck vom Typ Definition, der die sys_id eines virtuellen Servers in einem Stapel abruft. VirtualServer1 ist der Alias eines Ressourcenblocks, der im Stapel verwendet wird.

  $(Stack.items[VirtualServer2].attributes[sys_id]) ist ein Ausdruck vom Typ Laufzeit, der die sys_id eines virtuellen Servers in einem Stapel abruft.

  ${Stack.items[vm1].attributes[node_id]} liest das Attribut node_id des CI, das für die VM erstellt wurde. vm1 ist der Name des Stapelelements (oder der Alias der Ressource in der Blaupause).

  $(Stack.items[vm1].status) liest den Status des Stapelelements.

Property override expressions in policies

In Richtlinien können Sie Eigenschaften überschreiben, indem Sie einen Wert aus dem System abrufen oder eine Zufallszahl verwenden. Sie können Daten sowohl aus den Formularen im Cloudbenutzerportal als auch von dem Benutzer verwenden, der den Vorgang auf dem Formular ausgeführt hat.

- Typ: Definition/Laufzeit
- Syntax: ${parameter.formData.xyz} oder ${this.parameter.userData.xyz}
- Beispiele:

  Der folgende Wert kann den Stapelnamen auf *Stack_Bob.Smith@company.com* festlegen: Stack_${parameter.userData.userId}

  Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest, indem Sie das Subnetz aus der Tabelle „IP-Pool“ verwenden:

  $(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}])

  In Skripts können Sie Werte wie folgt zuweisen:

  formData.App_Server_NodeName = "MyNodeName";

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

this.parameter.userData.userId == 'servicenowuserId';

- Siehe auch Richtlinienaktionsskript erstellen.

Script expression

Im Beispiel ist VMProperties eine Skripteinbindung mit einer Funktion namens getIP. Ein Skriptausdruck ist auch ein Beispiel für einen komplexen Ausdruck (der Ausdruck ist verschachtelt).

- Typ: Laufzeit
- Syntax: $(Script:scriptName.function[])
- Beispiele:

  $(Script:VMPropertiesUtil.getIP[arg=$(Stack.items[VM1].attributes[object_id])])

  Ausdruck für private IP:$(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=$(Stack.items[Virtual Server].attributes[sys_id])])].private_ip)

  Ausdruck für öffentliche IP: $(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=$(Stack.items[Virtual Server].attributes[sys_id])])].public_ip)

  Ausdruck zum Abrufen des Anmeldeinformationsalias: $(Script:CMPVMUtils.getCredentialAlias[arg=${Stack.items[Virtual Server].attributes[sys_id]}])

  Ausdruck zum Abrufen der IP-Adresse: $(Script:CMPVMUtils.getReachableIp[arg=$(Stack.items[Virtual Server].attributes[sys_id])])

CI lookup expression

Greift auf Werte von Feldern in einer Tabelle zu, normalerweise eine CI-Tabelle in der CMDB.

- Typ: Definition/Laufzeit
- Syntax: $(ci.tableName)
- Beispiele:

  $(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}]) kombiniert Laufzeit- und Definitionsausdrücke. Der Operator „=“ wertet einen Wert für eine Übereinstimmung aus. Der Ausdruck führt ein Dot-Walking für die Tabelle „IP-Pool“ durch und sucht nach dem Subnetz mit der Subnetz-ID, die der Benutzer übermittelt hat.

  $(ci.cmdb_ci_cloud_subnet[${parameter.formData.SubnetId}].cidr) ruft den Wert des Felds cidr aus einem Subnetz ab, das der Benutzer während der Bereitstellung angegeben hat. Der Ausdruck führt ein Dot-Walking für die Tabelle „Cloud-Subnetz“ durch, betrachtet den Subnetzwert, den der Benutzer in einer Blaupausenbereitstellung angegeben hat, extrahiert den Wert des Felds cidr und geht dann zum Wert im Feld cidr der sys_id des Subnetzes.

Random number expression

Generiert eine Zufallszahl. Beispielsweise können Sie eine VM mit einem zufälligen Knotennamen oder Stapelnamen bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Typ: Laufzeit
- Syntax und Beispiel: `${randomNumber}`

Scratchpad expression/Resource operation output attribute expression

Liest Ausgabeattribute aus einem Vorgang in einen anderen Vorgang.

- Typ: Laufzeit
- Syntax: variiert
- Beispiel: Ausgaben für einen Vorgang festlegen/verfügbar machen:

  `${Compute Interface.CreateNode.Output.resp.nodeId}`

  So lesen Sie die Ausgabeattribute (wobei `VM1.Provision` der Vorgang ist, dessen Ausgabeattribute gelesen werden):

  `$(Outputs[VM1.Provision].NodeId)`

Conditions in expressions

Sie können bedingte Ausdrücke in Blaupausenschritten und Ressourcenvorgangsschritten verwenden, um den Schritt bedingt auszuführen oder zu überspringen. Die bedingten Ausdrücke sind Javascript-Ausdrücke und unterstützen das Ersetzen von Ausdrücken.

- Typ: Definition/Laufzeit
- Syntax: variiert
- Beispiele:

  '${parameter.CloudAccount}'=='Amazon Cloud Account'

  '$(Stack.items[vm1].attributes[node_id]) '== 'VM1'

Complex expression

Sie können Ausdrücke schachteln. Im Beispiel ordnet `${parameter.ServerID}` die sys_id des CI zu und wird ersetzt, bevor der äußere Ausdruck angewendet wird.

- Typ: beliebig
- Syntax: variiert
- Beispiel: `$(ci.cmdb_ci_vm_instance[${parameter.ServerID}].name)`

Order context

Dieser Ausdruck ist für Lebenszyklusvorgänge nützlich und ermöglicht Ihnen das Dot-Walking für die Bestellattribute als Teil der Tabelle *sn_cmp_order*.

- Typ: Laufzeit
- Syntax: `$(context.order.column_name)`
- Beispiele:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anforderungselement: `$(context.order.sc_req_item)`
- Dot-Walking für Anforderungselementobjekt: `$(context.order.sc_req_item.number)`
- Gemischter Ausdruck (Konstante + Ausdruck): `"ram $(context.order.sc_req_item.number)"`

Aktion für eine Richtlinie „bei Blaupausenbereitstellung“ erstellen

Der Auslöser ***`bei Blaupausenbereitstellung`*** wird nach der Ausführung der Richtlinien ***`bei Beginn der Katalogelementanforderung`*** ausgelöst. Durch eine Richtlinie, die durch den Auslöser ***`bei Blaupausenbereitstellung`*** ausgelöst wird, kann ein Skript ausgeführt, ein vom Benutzer angeforderter Attributwert außer Kraft gesetzt oder ein Bereitstellungsvorgang abgebrochen und eine entsprechende Nachricht gesendet werden.

Vorbereitungen

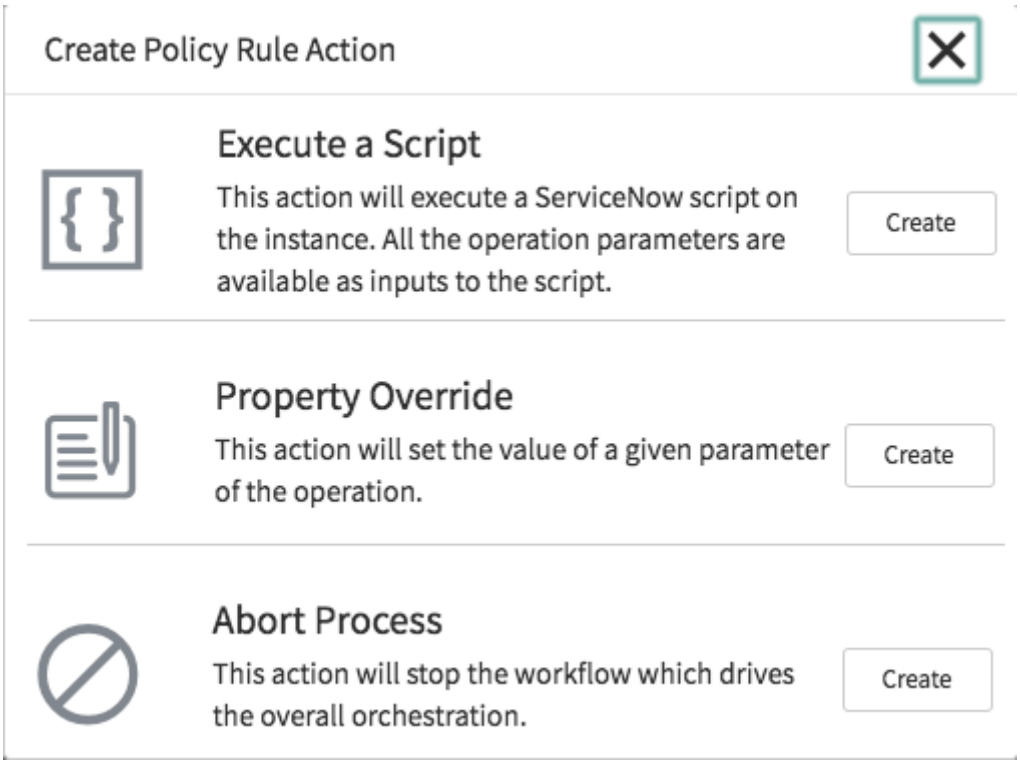
Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Cloud-Richtlinienregel konfigurieren

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

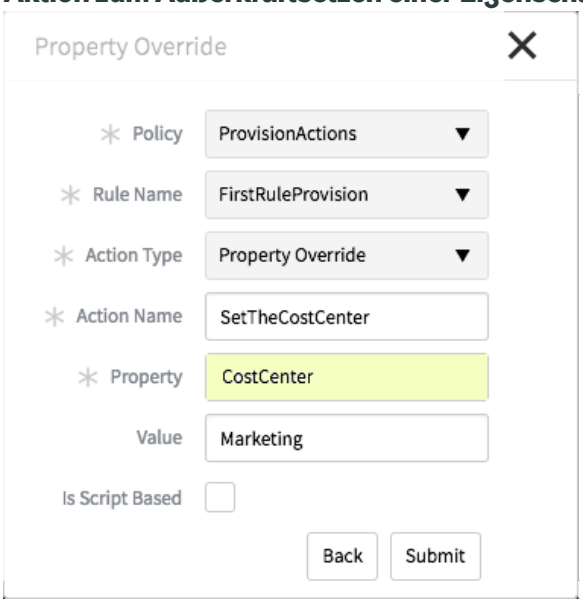


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben. **Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren**  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ○ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_${parameter.userData.userId}` ○ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet=${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ○ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`

Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an.
	Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)` des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel `MyStack` (MeinStapel).
	`customScript : function( formData){`
	`// Manipulation of form parameter is only supported here.`
	`// Change in any other attributes will be ignored`
	`// data available for manipulation are`
	`// Form Data - Ex. StackName can be accessed`
	`// through formData.StackName`
	`// formData.StackName = "MyStack";`
	`// User Data - Ex. User Id can be accessed`
	`// through this.parameters.userData`
	`// if(this.parameter.userData.userId == 'servicenowuserId')`
	`formData.StackName = "MyStack";`
	`return formData;`
	`},`

Einstellung für die Aktion „Prozess abbrechen“

Feld	Beschreibung
Nachricht	Geben Sie die Nachricht ein, die der anfordernden Person bei Abbruch des Prozesses angezeigt werden soll.

Erstellen Sie eine Aktion für eine Genehmigungsrichtlinie

Eine Richtlinie, die durch einen der Genehmigungsauslöser ausgelöst wird, kann Genehmigungs-Subflows starten. Die Genehmigungsauslöser sind (`Bei Blueprint-Bereitstellung (Genehmigung)` , `Bei Stapelvorgang (Genehmigung)` , `Bei Stapelressourcenvorgang (Genehmigung)` , Und `Bei Aufgabenkorrektur` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

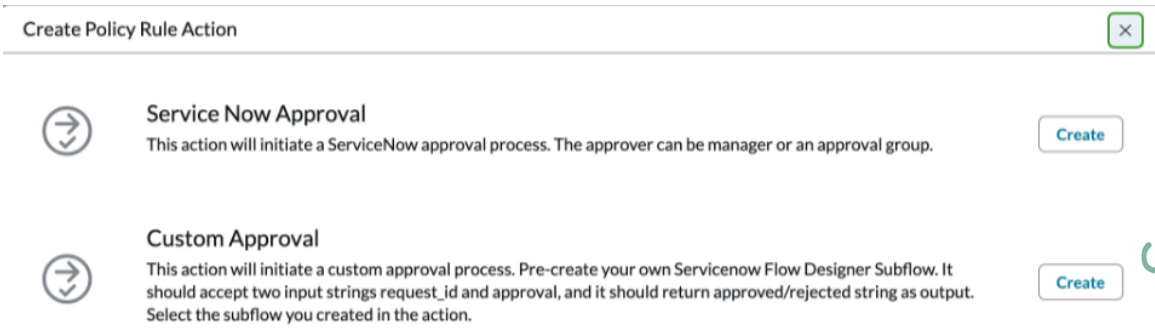
Warum und wann dieser Vorgang ausgeführt wird

Wenn mehrere „Genehmigungsrichtlinien“ gelten, werden die Richtlinien in der folgenden Reihenfolge angewendet. (Die Genehmigungsrichtlinien sind `Bei Blueprint-Bereitstellung (Genehmigung)` , `Bei Stapelvorgang (Genehmigung)` , `Bei Stapelressourcenvorgang (Genehmigung)` , Und `Bei Aufgabenkorrektur`):

1. Nur die erste erfolgreiche Genehmigungsrichtlinie wird angewendet. Es werden keine weiteren Genehmigungsrichtlinien angewendet.
2. Wenn die angewendete Genehmigungsrichtlinie mehrere Regeln aufweist, wird nur die erste erfolgreiche Regel verwendet.
3. Wenn eine Regel über mehrere Aktionen verfügt, wird nur die erste erfolgreiche Aktion ausgeführt.
4. Wenn die angewendete Genehmigungsrichtlinie sowohl eine benutzerdefinierte Genehmigung als auch eine ServiceNow-Genehmigung enthält, wird nur der benutzerdefinierte Genehmigungsprozess ausgeführt.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben.



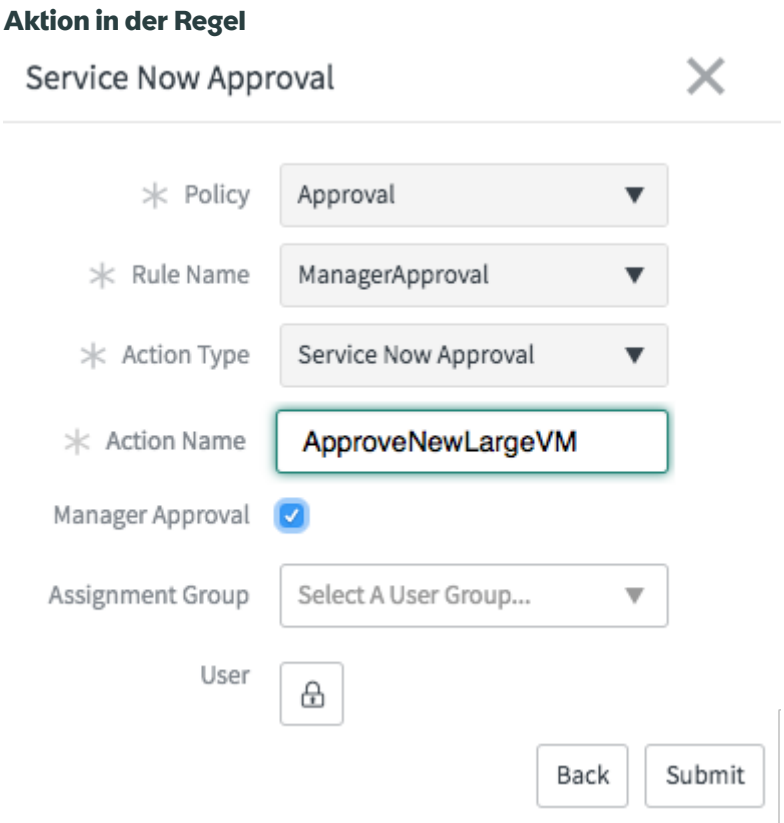
5. Wählen Sie eine der folgenden Aktionen aus.
   - **Anwenderdefinierte Genehmigung** Führt den von Ihnen angegebenen Subflow aus. Der Subflow muss einen Wert von zurückgeben **Genehmigt** Um den Vorgang abzuschließen. Folgen **Service Now-Genehmigung** Für Anwendungsfall.
   - **Service Now-Genehmigung** unterstützt unterschiedliche Genehmiger basierend auf dem Auslöser für die Richtlinie:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auslöser	Subflow	Verfügbare Genehmiger
on Blueprint provision (approval) (bei Blaupausenbereitstellung (Genehmigung))	Cloud-Genehmigung-Subflow	▪ Managergenehmigung ▪ Zuweisungsgruppe ▪ Benutzer (Sperre)
bei Genehmigung des Stapelvorgangs	Subflow Für Change-Anforderung Für Cloud-Vorgang	Zuweisungsgruppe
on Stack resource operation (approval) (bei Stapel-Ressourcenvorgang (Genehmigung))	Subflow Für Change-Anforderung Für Cloud-Vorgang	Zuweisungsgruppe

6. Geben Sie im Genehmigungsformular einen eindeutigen und aussagekräftigen **Aktionsnamen** an.



7. Wenn Sie auswählen **Anwenderdefinierte Genehmigung** Geben Sie den Subflow an, und klicken Sie dann auf **Übermitteln** Und wenn Sie auswählen **ServiceNow-Genehmigung** , Geben Sie an, wer die Cloud-Aktivität genehmigen soll.

Genehmigungsfelder

Feld	Beschreibung
Managergenehmigung	Eine oder alle der folgenden Optionen: ○ Aktivieren Sie das Kontrollkästchen **Managergenehmigung**, um festzulegen, dass der Manager des Genehmigers die Anforderung ebenfalls genehmigen muss. Der Standardgenehmigungs-Subflow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	geht zuerst an den Manager, dann an die Gruppe und schließlich an den Anwender. ○ Wählen Sie eine Benutzergruppe aus der Liste **Zuweisungsgruppe** aus. ○ Deaktivieren Sie die **Benutzer**-Sperre, wählen Sie einen Benutzer aus der Liste aus, und aktivieren Sie die Sperre anschließend wieder.
Zuweisungsgruppe	Wählen Sie die Zuweisungsgruppe zur Genehmigung der Anforderung aus. Jeder Anwender in der Gruppe kann die Aktion mit dem Standard-Subflow genehmigen. Die Genehmigung wird dann an die im Feld **Benutzer** angegeben Benutzer gesendet. **Hinweis:** Benutzer in einer Zuweisungsgruppe, die nicht über die Rolle „ITIL“ verfügen, erhalten standardmäßig immer noch einen Genehmigungsdatensatz und eine Benachrichtigung. Sie können die Genehmigung jedoch nicht erteilen. Weisen Sie die Rolle „ITIL“ allen Benutzern oder Benutzergruppen zu, die Vorgänge und Bereitstellungen genehmigen müssen.
Anwender	Wählen Sie mindestens einen Benutzer aus, für den die Genehmigungsaktion gilt. Alle ausgewählten Anwender müssen die Aktion mit dem Standard-Subflow genehmigen.

Aktion für eine Richtlinie „beim Starten des Katalogelements“ erstellen

Der Auslöser `beim Starten des Katalogelements` wird ausgelöst, wenn ein Bestellformular (Stapelanforderungsformular) für ein Katalogelement gestartet wird. Eine Richtlinie, die durch den Auslöser `beim Starten des Katalogelements` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte).

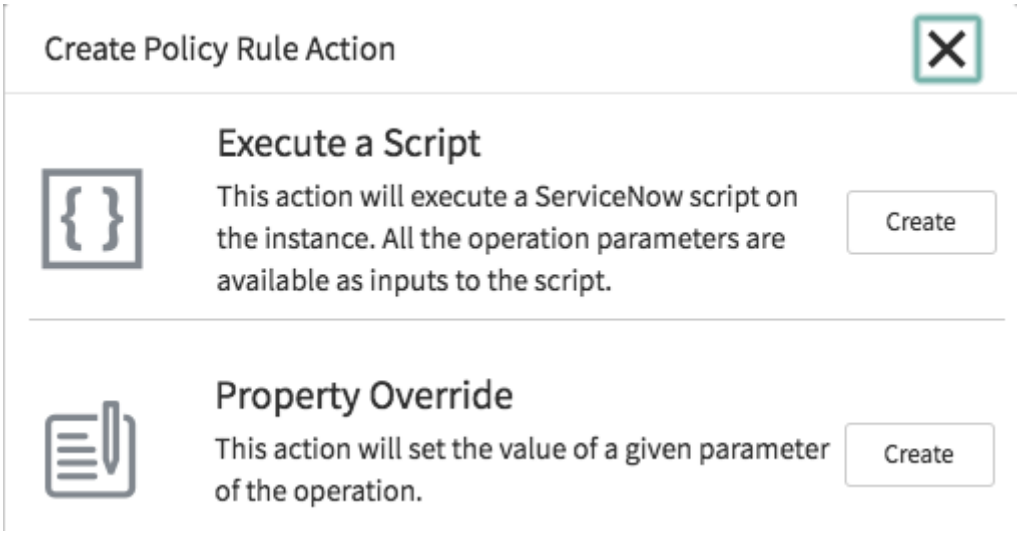
Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



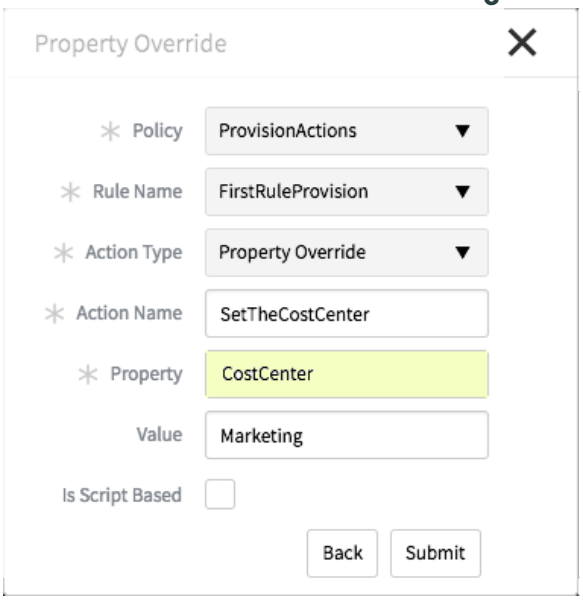
Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ○ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: ${parameter.formData.CatalogAttributeType} ○ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: ${parameter.userData.userId} Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: Stack_ ${parameter.userData.userId} ○ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: $(ci.sn_cmp_ip_pool[subnet=${parameter.formData.Subnet Id}]) entnimmt das Subnetz aus der Tabelle „IP-Pools“. ○ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: ${randomNumber}
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an. Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt function (formData) des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel MyStack (MeinStapel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	customScript : function(formData){
	// Manipulation of form parameter is only supported here.
	// Change in any other attributes will be ignored
	// data available for manipulation are
	// Form Data - Ex. StackName can be accessed
	// through formData.StackName
	// formData.StackName = "MyStack";
	// User Data - Ex. User Id can be accessed
	// through this.parameters.userData
	// if(this.parameter.userData.userId == 'servicenowuserId')
	formData.StackName = "MyStack";
	return formData;
	},

Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen

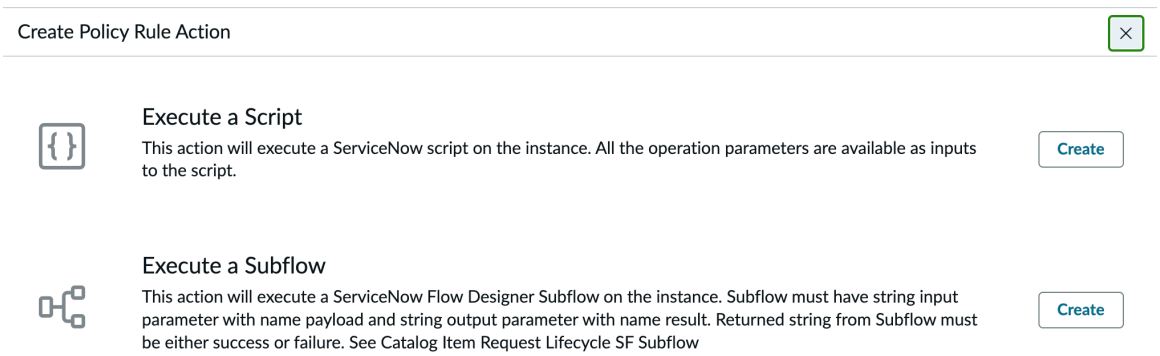
Der Auslöser `bei Beginn der Katalogelementanforderung` wird ausgelöst, nachdem der Benutzer ein Anforderungsformular geöffnet hat. Der Auslöser `bei Ende der Katalogelementanforderung` wird ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Eine Richtlinie, die von ausgelöst wird `Beim Start der Katalogelementanforderung` Oder `Bei Ende der Katalogelementanforderung` Der Auslöser kann ein Skript oder einen Subflow ausführen.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

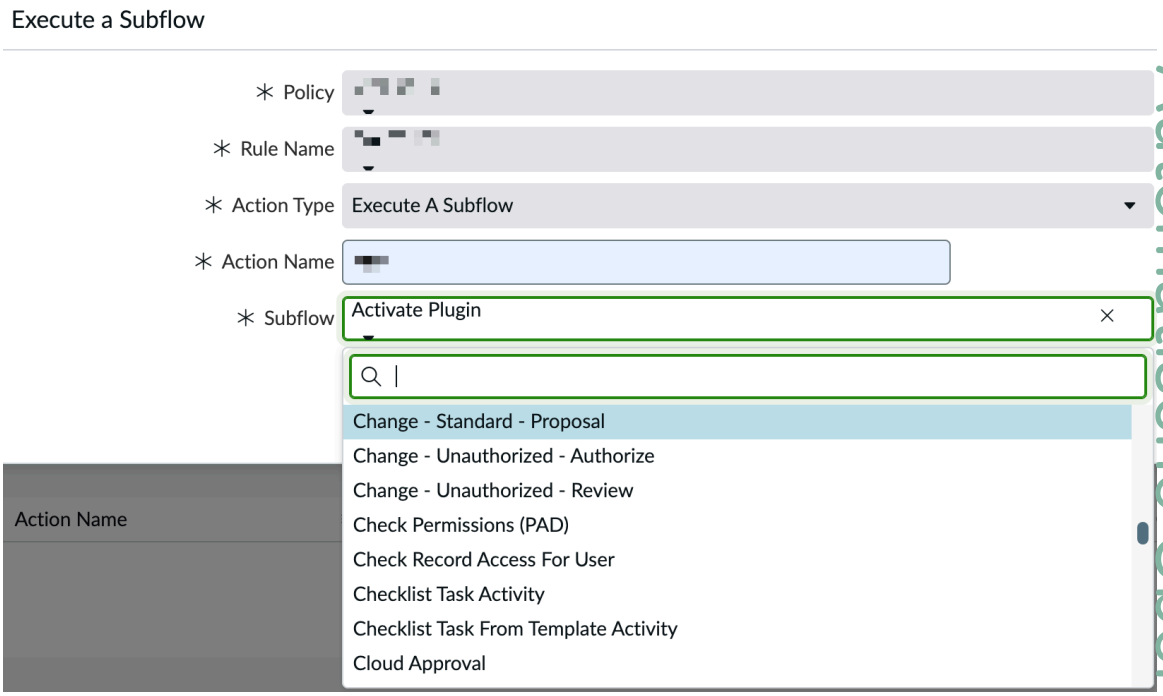


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Konfigurieren einer Aktion „Subflow ausführen“ zum Ausführen von Basissystem Subflow „Change-Anforderung“



Einstellungen für die Aktion „Subflow ausführen“

Feld	Beschreibung
Aktionsname	Geben Sie einen eindeutigen und aussagekräftigen Namen für die Aktion an, die den Subflow startet.
Subflow	Wählen Sie den auszuführenden Subflow aus.

Aktion für eine Richtlinie „Mietvertragsende“ erstellen

Eine Richtlinie, die durch den Auslöser `bei Leasingende` ausgelöst wird, kann eine Benachrichtigung senden oder einen Lebenszyklusvorgang `Starten`, `Stoppen`oder `Bereitstellung aufheben` ausführen.

Vorbereitungen

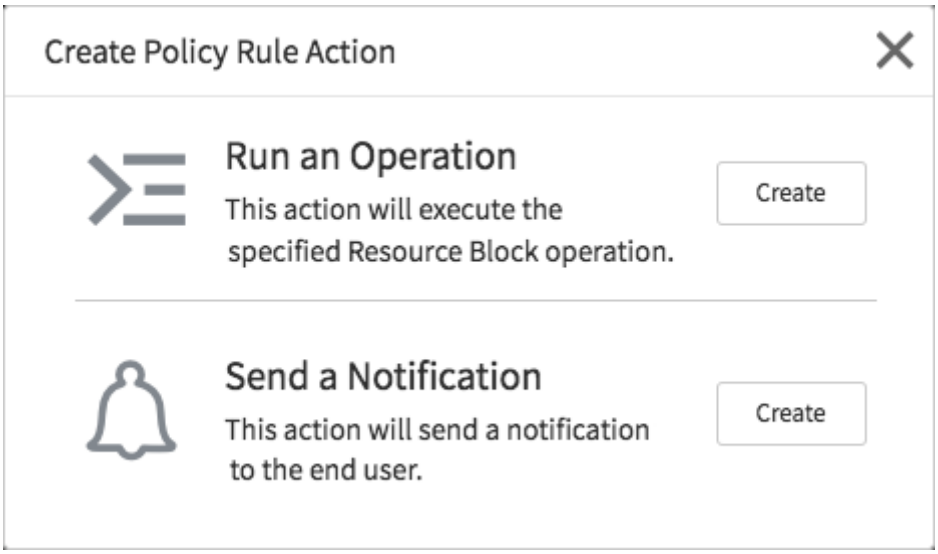
- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.



Einstellungen für die Aktion „Vorgang ausführen“

Feld	Beschreibung
Planvorgang	Geben Sie **Start**, **Stopp** oder **Aufheben der Bereitstellung** an.

Einstellungen für die Aktion „Benachrichtigung senden“

Feld	Beschreibung
Benachrichtigung	Wählen Sie den Text der Benachrichtigung aus: ○ Lease End Date Reached (Mietenddatum erreicht) ○ Stack Decommissioned (Lease End) (Stapel stillgelegt (Mietende)) ○ Upcoming Lease End (Bevorstehendes Mietende)

Aktion für eine Richtlinie „bei Ressourcenvorgang“ erstellen

Der Auslöser `bei Ressourcenvorgang` wird während des Orchestration-Prozesses ausgelöst, wenn ein Benutzer einen Lebenszyklusvorgang `Starten`, `Stoppen` oder `Bereitstellung aufheben` für eine bestimmten Ressource durchführt. Eine Richtlinie, die durch den Auslöser `bei Ressourcenvorgang` ausgelöst wird, kann einen von einem Benutzer angeforderten Attributwert überschreiben, ein Skript ausführen, eine Cloud API aufrufen oder einen IP-Adressenverwaltungsvorgang ausführen.

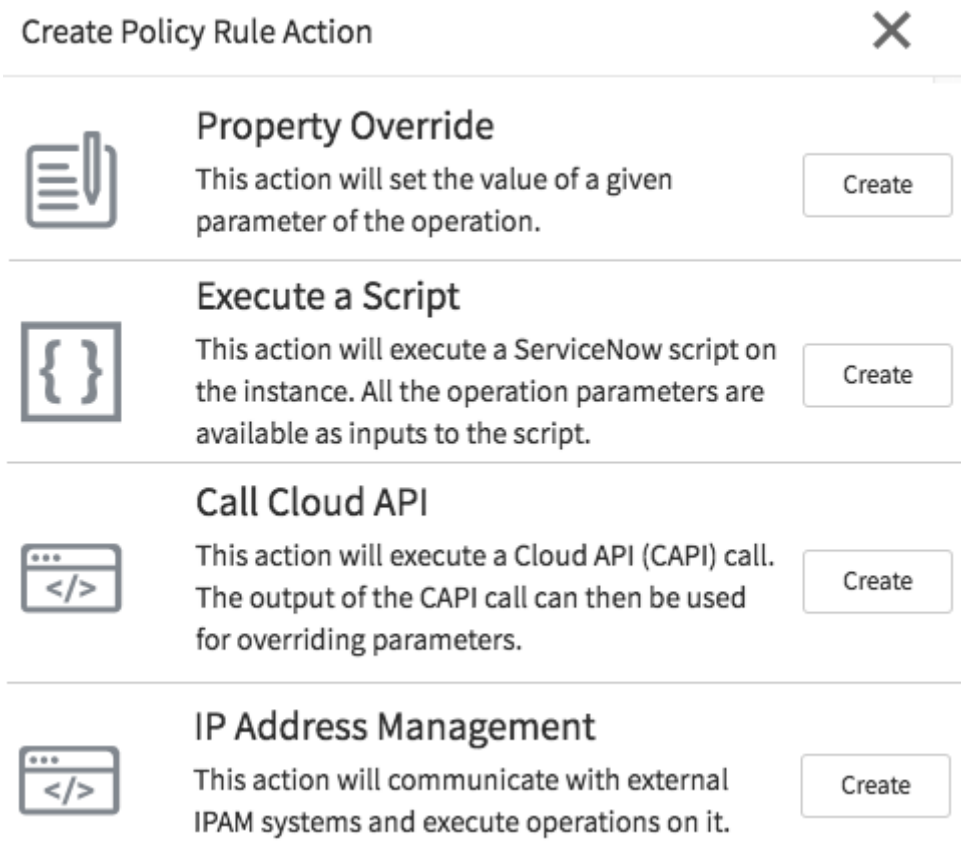
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

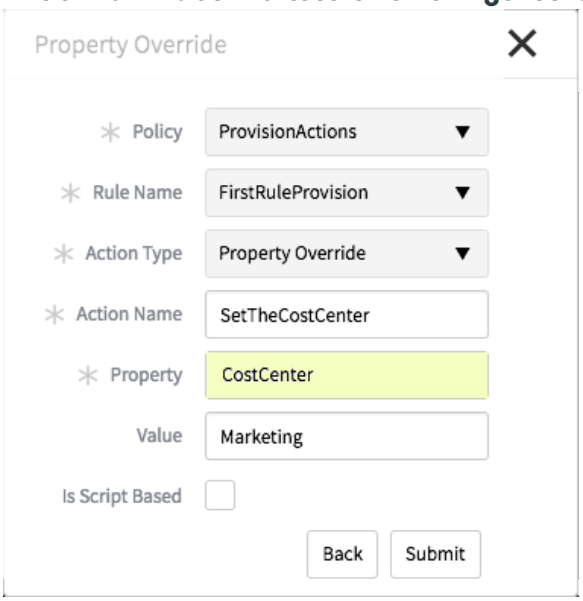


Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben. **Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren**  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ○ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ○ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_ ${parameter.userData.userId}` ○ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet=${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ○ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an. Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel MyStack (MeinStapel).
	`customScript : function( formData){`
	`// Manipulation of form parameter is only supported here.`
	`// Change in any other attributes will be ignored`
	`// data available for manipulation are`
	`// Form Data - Ex. StackName can be accessed`
	`// through formData.StackName`
	`// formData.StackName = "MyStack";`
	`// User Data - Ex. User Id can be accessed`
	`// through this.parameters.userData`
	`// if(this.parameter.userData.userId == 'servicenowuserId')`
	`formData.StackName = "MyStack";`
	`return formData;`
	`},`

Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Wenn Sie den Aktionstyp **Cloud-API aufrufen** auswählen und den Datensatz speichern, wird die zugehörige Liste „Richtlinienregel-Aktionsattribute“ mit den Attributen ausgefüllt, die an den Provider zu übergeben sind. Wenn Sie eine Integration mit Infoblox vornehmen, müssen Sie das Feld **DNSSuffix** konfigurieren. Wenn Sie z. B. einen Host erstellen, wird der Wert im Feld **DNSSuffix** in Infoblox für den neu erstellten virtuellen Computer angezeigt.

Einstellungen für die Aktion „Cloud-API aufrufen“

Feld	Beschreibung
Aktionsname	Geben Sie einen beschreibenden Namen für die Aktion ein. In aufeinander folgenden Richtlinienaktionen für dieselbe Richtlinie können Sie in einem Feld vom Typ **Wert** auf diesen Namen verweisen. Er bezieht sich auf die JSON-Nutzlast, die nach einem API-Aufruf vom Cloud Provider empfangen wird. Um beispielsweise auf eine zugewiesene IP-Adresse zu verweisen, die von der Aktion mit dem Namen *`RefAction`* zurückgegeben wurde, können Sie den folgenden Ausdruck im Feld **Wert** einer anderen Richtlinienaktion verwenden: $(parameter.RefAction.Allocated_IP}.
Provider	Geben Sie den Cloud Provider aus der API-Bibliothek ein.
Version	Geben Sie die Version aus der API-Bibliothek ein.
Schnittstelle	Wählen Sie eine CAPI-Schnittstelle aus. Wählen Sie für Infoblox die **IPAM-Schnittstelle** aus.
Vorgang	Wählen Sie einen durchzuführenden CAPI-Schnittstellenvorgang aus. Für Infoblox wählen Sie **CreateHostRecord** oder **DeleteHostRecord**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Berechtigungen	Geben Sie die sys_ID der erforderlichen Anmeldeinformationen ein. Sie können auch einen Ausdruck wie den folgenden verwenden: `$(ci.sn_cmp_infoblox_server[$(ci.sn_cmp_ip_pool[subnet=${parameter.formData.SubnetId}].provider_instance)].infoblox_server_credential)`
Endpunkt-URL	Geben Sie die Endpunkt-URL des Connectors aus der API-Bibliothek ein. Bei Infoblox ist dies die IP-Adresse des Infoblox-Servers.

Einstellungen für die Aktion „IP-Adressverwaltung“

Feld	Beschreibung
Name der IPAM-Methode	Wählen Sie den Namen der IPAM-Methode aus. Für Infoblox wählen Sie eine der folgenden Optionen aus: ○ **IP-Adresse freigeben**: Geben Sie eine IP-Adresse von Infoblox frei, wenn die Bereitstellung eines Computers beendet wird. ○ **IP-Adresse registrieren**: Registrieren Sie einen neuen virtuellen Computer bei Infoblox. Diese Option wird von AWS- und Azure-Clouds verwendet. ○ **IP-Adresse reservieren**: Reservieren Sie eine neue IP-Adresse. Diese Option wird von einer vSphere-Cloud verwendet. Siehe IP-Adressen für AWS- und Azure-VMs in Infoblox registrieren, IP-Adressen für VMware vSphere-VMs in InfoBlox reservieren und IPAM-Integration.

Aktion für eine Richtlinie „beim Start des Ressourcenvorgangs“ erstellen

Der Auslöser `beim Start des Ressourcenvorgangs` wird ausgelöst, bevor der Katalog für einen Ressourcenvorgang aus dem Cloudbenutzerportal geladen wird. Eine Richtlinie, die durch den Auslöser `beim Start des Ressourcenvorgangs` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte).

Vorbereitungen

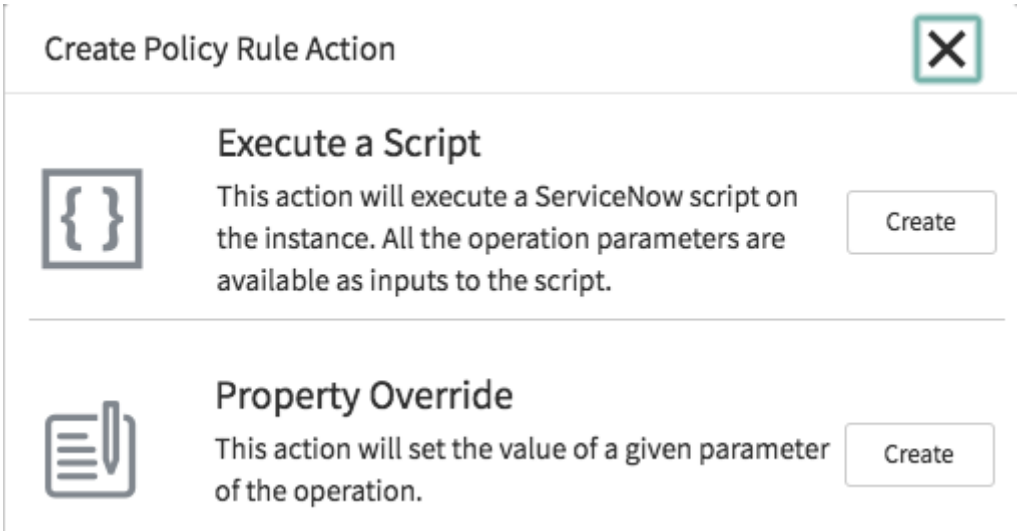
- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.



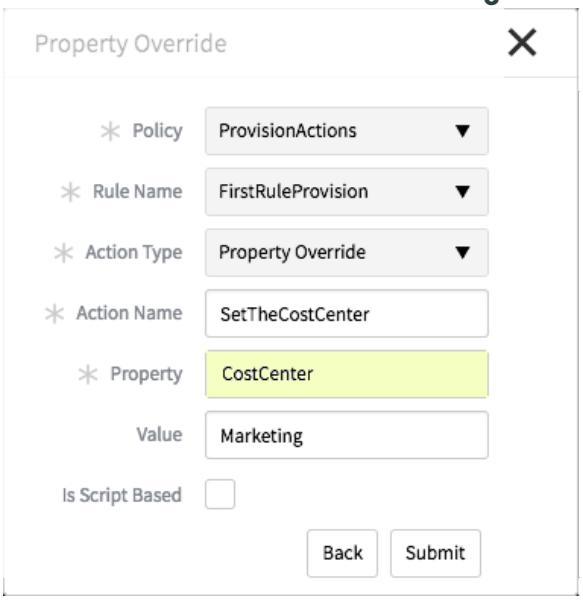
Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ○ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: ${parameter.formData.CatalogAttributeType} ○ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: ${parameter.userData.userId} Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: Stack_ ${parameter.userData.userId} ○ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: $(ci.sn_cmp_ip_pool[subnet=${parameter.formData.Subnet Id}]) entnimmt das Subnetz aus der Tabelle „IP-Pools“. ○ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: ${randomNumber}
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an. Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt function (formData) des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel MyStack (MeinStapel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	customScript : function(formData){
	// Manipulation of form parameter is only supported here.
	// Change in any other attributes will be ignored
	// data available for manipulation are
	// Form Data - Ex. StackName can be accessed
	// through formData.StackName
	// formData.StackName = "MyStack";
	// User Data - Ex. User Id can be accessed
	// through this.parameters.userData
	// if(this.parameter.userData.userId == 'servicenowuserId')
	formData.StackName = "MyStack";
	return formData;
	},

Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen

Eine Richtlinie, die durch den Auslöser `beim Start der Ressourcenvorgangsanforderung` oder `bei Ende der Ressourcenvorgangsanforderung` ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

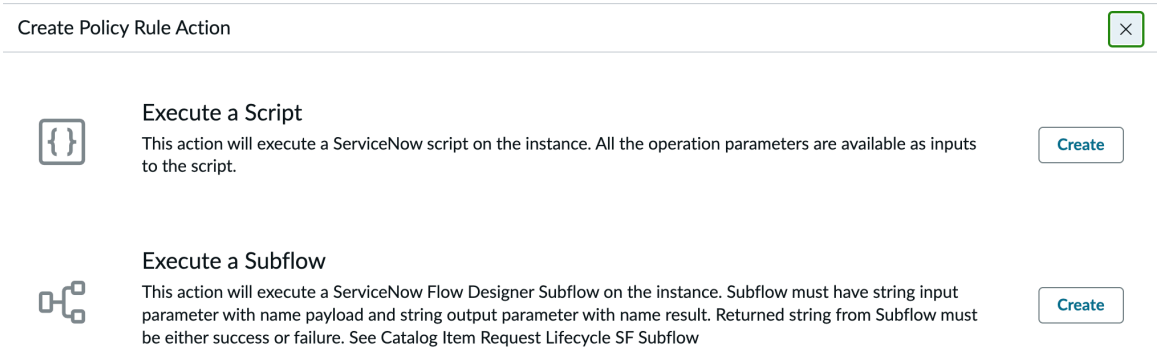
Warum und wann dieser Vorgang ausgeführt wird

- Der Auslöser `beim Start der Ressourcenvorgangsanforderung` wird ausgelöst, nachdem ein Benutzer eine Ressourcenvorgangsanforderung (`Starten`, `Stoppen`, `Bereitstellung aufheben`) übermittelt hat.
- Der Auslöser `bei Ende der Ressourcenvorgangsanforderung` wird vor Abschluss eines Lebenszyklusvorgangs für eine Ressource (`Starten`, `Stoppen`, `Bereitstellung aufheben`) ausgelöst.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



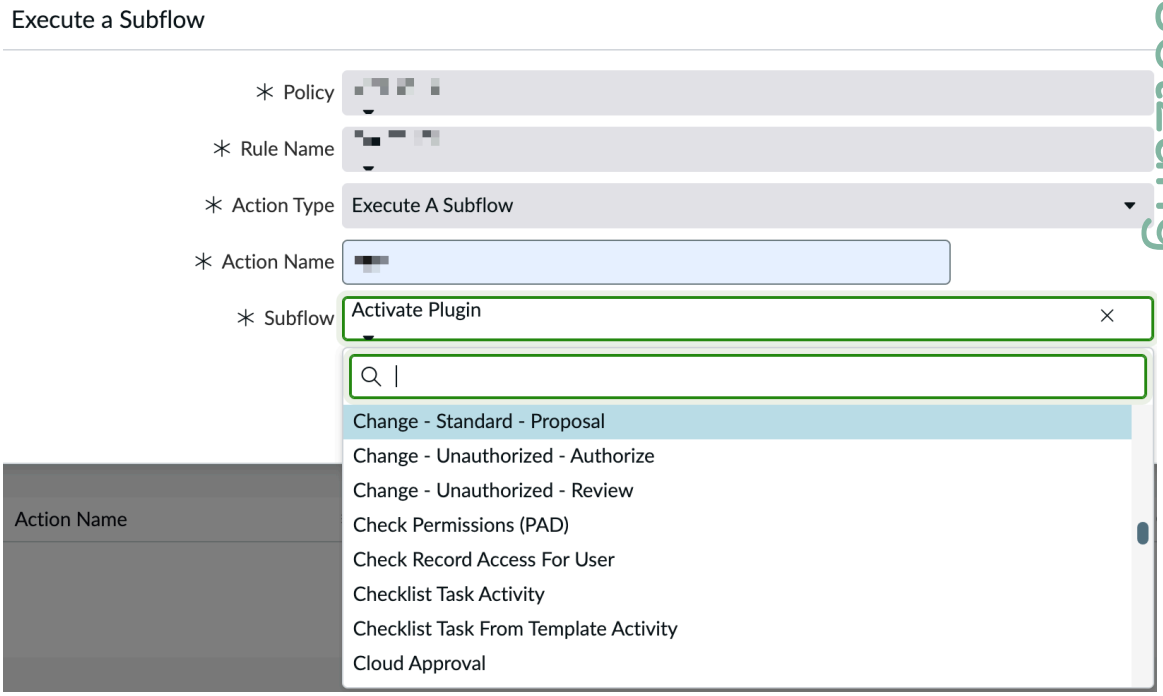
Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Subflow ausführen“

Feld	Beschreibung
Aktionsname	Geben Sie einen eindeutigen und aussagekräftigen Namen für die Aktion an, die den Subflow startet.
Subflow	Wählen Sie den auszuführenden Subflow aus.

Konfigurieren einer Aktion „Subflow ausführen“ zum Ausführen von Basissystem Subflow „Change-Anforderung“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion für eine Richtlinie „bei Ressourcengrenzen überschritten“ erstellen

Legen Sie fest `on Resource limits exceeded`Richtlinie zur automatischen Ausführung der Genehmigung Subflows Oder senden Sie Benachrichtigungen, wenn ein Bestellformular für ein vorlagenbasiertes Katalogelement übermittelt wird, das die definierte Ressourcengrenze oder Quotenwerte überschreitet.

Vorbereitungen

Sie müssen die folgenden Elemente konfiguriert haben:

- Mindestens eine Cloud-Richtliniengruppe
- C Laut-Richtlinie
- A Prävalenzrichtlinie
- E E-Mail-Benachrichtigung
- Erstellen Sie einen Subflow in Workflow-Studio

Erforderliche Rolle: sn_cmp.cloud_governor oder cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Für die Basissystem-Richtlinienaktion `On resource limit exceeded` ist standardmäßig eine ServiceNow-Standardregel für Genehmigungsrichtlinien konfiguriert. Wenn Sie andere Aktionen auslösen möchten, z. B. Benachrichtigungen oder eine anwenderdefinierte Genehmigung subflow Wenn das Ressourcenlimit überschritten wird, können Sie entweder die Richtlinienaktion des Basissystems ändern oder eine anwenderdefinierte Richtlinie für Ihre Instanz erstellen.

Prozedur

1. Ändern oder erstellen Sie eine Cloud-Richtlinienaktion, die den Auslöser `on Resource limit exceeded` verwendet.
   a. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
   b. Ändern Sie eine Basissystem-Richtlinie, oder erstellen Sie einen neuen Richtliniendatensatz.
      - a. Öffnen Sie die Basissystem-Richtlinie **Resource Order Control** (Steuerung von Ressourcenbestellungen).
      - b. Ändern Sie den Namen der Richtlinie, das Start- und Enddatum sowie die Reihenfolge der Ausführung.
      - c. Ändern Sie die Bedingungen der Richtlinienregeln.
      - Klicken Sie auf **Neu**, um einen neuen Richtliniendatensatz zu erstellen.

      Weitere Informationen finden Sie unter Erstellen Sie eine Cloud-Richtlinie .
2. Ändern Sie in der zugehörigen Liste „Regeln“ die Basissystemregel, oder erstellen Sie eine neue Regel.
   - Öffnen Sie die Basissystemregel `approveresourcelimit`, mit der die Aktion ausgeführt werden soll, und passen Sie sie an.
   - Erstellen Sie eine Richtlinienregel.

   Weitere Informationen finden Sie unter Cloud-Richtlinienregeln konfigurieren.
3. Geben Sie eine Richtlinienaktion an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.

b. Klicken Sie neben der Aktion, die ausgeführt werden soll, wenn das Kontingent überschritten wird, auf **Erstellen**.

Optionen	Schritte
ServiceNow A Proval	**a.** Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. **b.** Wählen Sie die Option **Managergenehmigung** aus, um den Antrag zur Genehmigung durch den Manager automatisch zu senden. **c.** Wählen Sie die **Zuweisungsgruppe** aus, für die diese Aktion gilt.
Anwenderdefinierte Genehmigung	**a.** Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. **b.** Wählen Sie einen vorhandenen anwenderdefinierten Workflow in aus **Untergeordnet Flow** Feld.
Senden Sie ein N Verhandlung	**a.** Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. **b.** Wählen Sie im Feld **Benachrichtigung** eine Benachrichtigungsvorlage aus. Die Basissystem-Benachrichtigungs-E-Mail für die Richtlinienaktion „bei Ressourcengrenzen überschritten“ wird in der Suchtabelle angezeigt, wenn Sie die Basissystem-Richtlinie verwenden.

4. Klicken Sie auf **Absenden**.

Aktion für eine Richtlinie „bei Aufgabenremediation“ erstellen

Der Auslöser `bei Aufgabenremediation` wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt. Eine Richtlinie, die von ausgelöst wird `Bei Aufgabenkorrektur` Der Auslöser kann Genehmigungs-Subflows starten.

Vorbereitungen

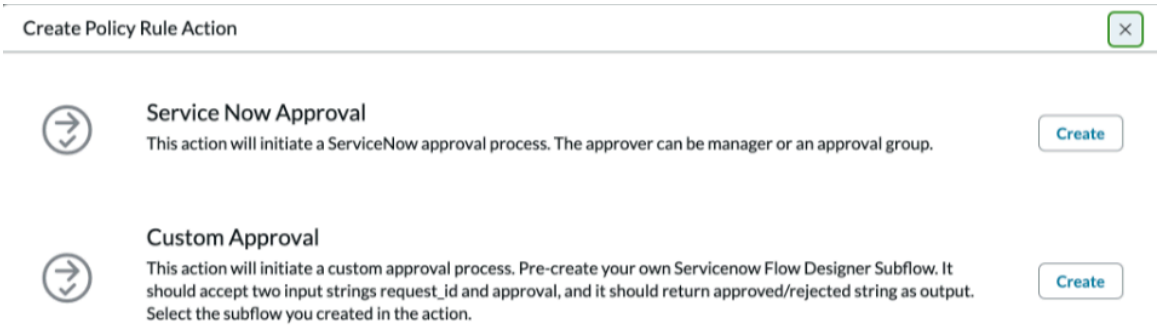
- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

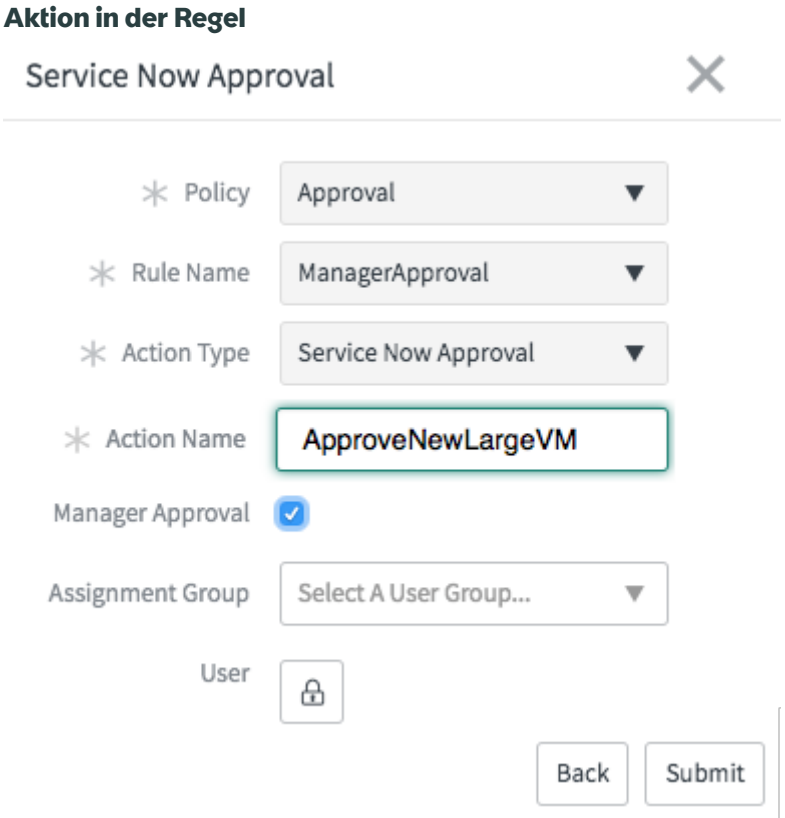
1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und legen Sie die Richtlinie auf fest **Entwurf** status bei Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben.



5. Wählen Sie eine der folgenden Optionen aus.
   - **Anwenderdefinierte Genehmigung** Führt den von Ihnen angegebenen Subflow aus. Der Subflow muss einen Wert von zurückgeben **Genehmigt** Um den Vorgang abzuschließen.
   - **Service Now-Genehmigung** unterstützt unterschiedliche Genehmiger basierend auf dem Auslöser für die Richtlinie:
     - Managergenehmigung
     - Zuweisungsgruppe
     - Benutzer (Sperre)
6. Geben Sie im Genehmigungsformular einen eindeutigen und aussagekräftigen **Aktionsnamen** an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wenn Sie auswählen **Anwenderdefinierte Genehmigung** Geben Sie den Subflow an, und klicken Sie dann auf **Übermitteln** Und wenn Sie auswählen **ServiceNow-Genehmigung** , Geben Sie an, wer die Cloud-Aktivität genehmigen soll.

Genehmigungsfelder

Feld	Beschreibung
Managergenehmigung	Eine oder alle der folgenden Optionen: ○ Aktivieren Sie das Kontrollkästchen **Managergenehmigung**, um festzulegen, dass der Manager des Genehmigers die Anforderung ebenfalls genehmigen muss. Der Standardgenehmigungs-Subflow geht zuerst an den Manager, dann an die Gruppe und schließlich an den Anwender. ○ Wählen Sie eine Benutzergruppe aus der Liste **Zuweisungsgruppe** aus. ○ Deaktivieren Sie die **Benutzer**-Sperre, wählen Sie einen Benutzer aus der Liste aus, und aktivieren Sie die Sperre anschließend wieder.
Zuweisungsgruppe	Wählen Sie die Zuweisungsgruppe zur Genehmigung der Anforderung aus. Jeder Anwender in der Gruppe kann die Aktion mit dem Standard-Subflow genehmigen. Die Genehmigung wird dann an die im Feld **Benutzer** angegeben Benutzer gesendet. **Hinweis:** Benutzer in einer Zuweisungsgruppe, die nicht über die Rolle „ITIL“ verfügen, erhalten standardmäßig immer noch einen Genehmigungsdatensatz und eine Benachrichtigung. Sie können die Genehmigung jedoch nicht erteilen. Weisen Sie die Rolle „ITIL“ allen Benutzern oder Benutzergruppen zu, die Vorgänge und Bereitstellungen genehmigen müssen.
Anwender	Wählen Sie mindestens einen Benutzer aus, für den die Genehmigungsaktion gilt. Alle ausgewählten Anwender müssen die Aktion mit dem Standard-Subflow genehmigen.

Richtlinienaktionsskript erstellen

Verwenden Sie Richtlinienaktionsskripts, um Werte in Cloud-Anforderungen abzurufen, zu aktualisieren oder festzulegen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Verwenden von Skripts finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf der Registerkarte **Richtlinien-Aktionsskripts** auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie einen Namen eingegeben haben, wird ein Skript mit einer Variablen angezeigt, die den von Ihnen eingegebenen Namen verwendet.

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine andere Kategorie aus, oder behalten Sie die in einem früheren Schritt erstellte Kategorie bei.
Skript	Ändern Sie die Funktion `customScripts` im Skript. Dies ist der einzige Teil des Skripts, den Sie ändern müssen.

Example:
Das folgende Beispielskript ermittelt, ob der Benutzer zu einer Benutzergruppe gehört, und überschreibt dann den benutzerdefinierten Wert des Knotennamens des Anwendungsservers mit dem Wert **MyNodeName**.

```
customScript : function(formData){
  var groups = this.parameters.userData.groups;
    if( groups.length > 0){
      formData.App_Server_NodeName = "MyNodeName";
    }
  return formData;
},
```

Dieses Beispiel gibt eine zufällige Zahl zurück:

```
customScript : function(formData){
  var min = 10000;
  var max = 99999;
  var num = Math.floor(Math.random() * (max - min + 1)) + min;
  formData.randomNumber = num + "";
  return formData;
},
```

Dieses Beispielskript fügt dem Leasingdatum mithilfe der GlideDateTime -Klasse im Basissystem drei Stunden hinzu.

```
var SetLeaseShort = Class.create();
SetLeaseShort.prototype = Object.extendsObject(sn_cmp.PolicyExecutionBase, {
 customScript : function(formData){
  // Manipulation of form parameters are supported. Changes in any other attributes
            // will be ignored.
  // The data available for manipulation is as follows:
  // Form Data -  for example: StackName can be accessed through formData.StackName
  // formData.StackName = "MyStack";
  // User Data  - for example: User Id can be accessed through this.parameters.userData
  // if(this.parameter.userData.userId == 'servicenowuserId')
  // this.info("id = " + formData.StackName);

  // var leaseValue = now();
  // leaseValue = leaseValue.setHours(leaseValue.getHours()+4);
  // formData.LeaseEndDate = leaseValue;

  if (formData.hasOwnProperty("LeaseEndDate")) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  gdt = new GlideDateTime();
  // 10800 = 3 hours
  gdt.addSeconds(10800);
  formData.LeaseEndDate = gdt.getDisplayValue();
 }
 return formData;
},
execute: function() {
 if(this.parameters !=  null && this.parameters.formData != null){
       var inputData = JSON.parse(JSON.stringify(this.parameters.formData));
    var outputFormData = this.customScript(inputData);
        if( outputFormData != null){
           this.parameters.formData = outputFormData;
        }
     }
 var output = {};
 output.answer = this.parameters;
 return JSON.stringify(output);
},
type : 'SetLeaseShort'
});

var SetLeaseShortObj = new SetLeaseShort(inputAttributes);
var outputParams = SetLeaseShortObj.execute();
gs.info( "Output of script is = " + outputParams);
```

Dieses Beispielskript legt das benutzerdefinierte Namensfeld **Azure Wordpress DNS** im Formular auf denselben Namen wie den Stapelnamen fest:

```
var WordpressFill = Class.create();
WordpressFill.prototype = Object.extendsObject(sn_cmp.PolicyExecutionBase, {
 customScript : function(formData){
  // Manipulation of form parameters are supported. Changes in any other attributes
       // will be ignored.
  // The data available for manipulation is as follows:
  // Form Data -  for example: StackName can be accessed through formData.StackName
  // formData.StackName = "MyStack";
  // User Data  - for example: User Id can be accessed through this.parameters.userData
  // if(this.parameter.userData.userId == 'servicenowuserId')
  //this.info("id = " + formData.StackName);

  formData.Azure_Wordpress_v6_vmDnsName = formData.StackName;

  return formData;
 },
 execute: function() {
  if(this.parameters !=  null && this.parameters.formData != null){
        var inputData = JSON.parse(JSON.stringify(this.parameters.formData));
     var outputFormData = this.customScript(inputData);
         if( outputFormData != null){
            this.parameters.formData = outputFormData;
         }
      }
  var output = {};
  output.answer = this.parameters;
  return JSON.stringify(output);
 },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 type : 'WordpressFill'
});

var WordpressFillObj = new WordpressFill(inputAttributes);
var outputParams = WordpressFillObj.execute();
gs.info( "Output of script is = " + outputParams);
```

Zugehörige Informationen

Beispiel für ein Richtlinienaktionsskript zum Kennzeichnen von Ressourcen mit Tags

Beispiel für ein Richtlinienaktionsskript zum Kennzeichnen von Ressourcen mit Tags

Ihre Instanz verfolgt für Abrechnung und Berichterstellung getaggte Ressourcen nach. Richtlinienaktionsskripts können Ressourcen-Tags hinzufügen und ändern. In diesem Beispiel wird eine Speichervolume-Ressource mit Tags versehen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

Unter Benutzerdefiniertes Tag für Cloud-Ressourcen erstellen finden Sie Informationen zum Erstellen und Verwenden von Tags in Cloud Provisioning and Governance.

Prozedur

1. Auf der Portal für Cloud-Admin., Navigieren Sie zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf der Registerkarte **Richtlinienaktionsskripts** auf **Neu**, und geben Sie einen eindeutigen und beschreibenden **Namen** ein.
3. Klicken Sie auf das Suchsymbol für **Aktionsskriptkategorie**, klicken Sie auf **Neu**, um eine neue Kategorie zu erstellen, und klicken Sie dann auf **Absenden**.
4. Geben Sie auf der Seite „Richtlinienregel-Aktionsskript“ das Skript für die Ressource ein, die Sie taggen möchten.
5. Klicken Sie Auf **Übermitteln** Zum Speichern des Skripts.
   Das Skript wird in der Liste angezeigt.
6. Klicken Sie auf der Registerkarte „Richtlinien“ auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** für die Richtlinie ein, füllen Sie das Formular mit den folgenden Beispieleinstellungen aus, und klicken Sie dann auf **Speichern** .

Richtlinienauslöser	bei Ressourcenvorgang
Ressourcenblock	Speicher-Laufwerk
Vorgang	Storage Volume Interface.Provision
Moment	Vor dem Vorgang

7. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, geben Sie für den **Namen** den Wert **Add Custom Tags for Storage (Benutzerdefinierte Tags für Speicher hinzufügen)** ein, akzeptieren Sie die Standardeinstellungen, und klicken Sie dann auf **Absenden**.
8. Klicken Sie in der zugehörigen Liste „Richtlinienregelaktionen“ auf **Neu**.
9. Klicken Sie unter „Skript ausführen“ auf **Erstellen**, füllen Sie das Formular mit den folgenden Beispieleinstellungen aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	CreateCustomTagsForStorage
Aktionsskriptkategorie	ScriptsForCustomTags
Aktionsskript	AddCustomTagsForStorage

10. Klicken Sie auf der Seite „Richtlinienregel“ auf **Aktualisieren**.
11. Kehren Sie zur Seite „Richtlinie“ zurück, und klicken Sie dann auf **Veröffentlichen**.

Ergebnis
Starten Sie im Portal für Cloud-Admin. den Stapel, der der Speicherressource zugeordnet ist. Sie können dann bestätigen, dass die Tags angewendet wurden.

Cloud-Genehmigungsrichtlinie erstellen

Eine Cloud-Genehmigungsrichtlinie gibt die Anwender an, die eine bestimmte Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann. Genehmiger können den Manager des Benutzers, der eine Anforderung sendet, einen angegebenen Benutzer oder eine bestimmte Gruppe oder Benutzer mit einer bestimmten Rolle einschließen. Sie können mehrere Genehmiger angeben. Genehmigungen erfolgen in der von Ihnen angegebenen Reihenfolge.

Vorbereitungen
Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

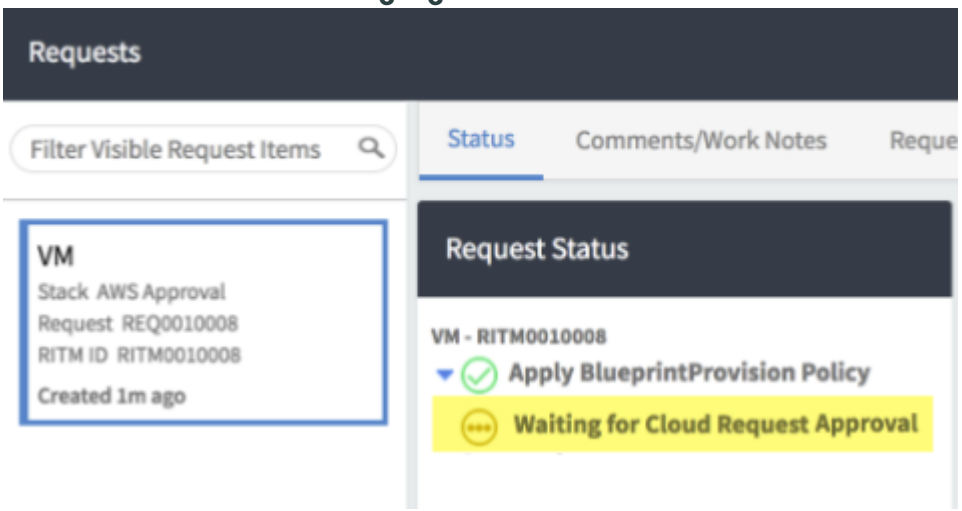
Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel fordert ein Benutzer einen Stapel an, der eine Genehmigungsrichtlinie auslöst.

1. Ein Benutzer sendet im Cloudbenutzerportal eine Anforderung zur Bereitstellung einer bestimmten Blaupause. Der Prozess der Bereitstellung der Blaupause ist der Auslöser, mit dem das Richtlinienmodul zur Anwendung einer Genehmigungsrichtlinie veranlasst wird. Eine Cloud-Genehmigungsrichtlinie gibt die Anwender an, die eine bestimmte Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann.
2. Vom Richtlinienmodul wird festgestellt, dass die Anforderung die in der Regel für die Richtlinie angegebene Bedingung erfüllt. In diesem Beispiel wird die Bedingung immer dann als „true“ (wahr) bewertet, wenn eine bestimmte Blaupause bereitgestellt wird.
3. Da die Bedingung erfüllt ist, wird vom Richtlinienmodul die Aktion ausgeführt, die auch in der Regel angegeben ist. In diesem Beispiel besteht die Aktion darin, eine Genehmigungsaktion für den Manager anzulegen.
4. Während der Genehmiger (der Manager) die Genehmigungsanforderung überprüft, wird dem Benutzer im Cloudbenutzerportal die Statusmeldung „Warte auf Genehmigung“ angezeigt.
5. Die Blaupause wird nach Genehmigung durch den Manager bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer wartet auf Genehmigung



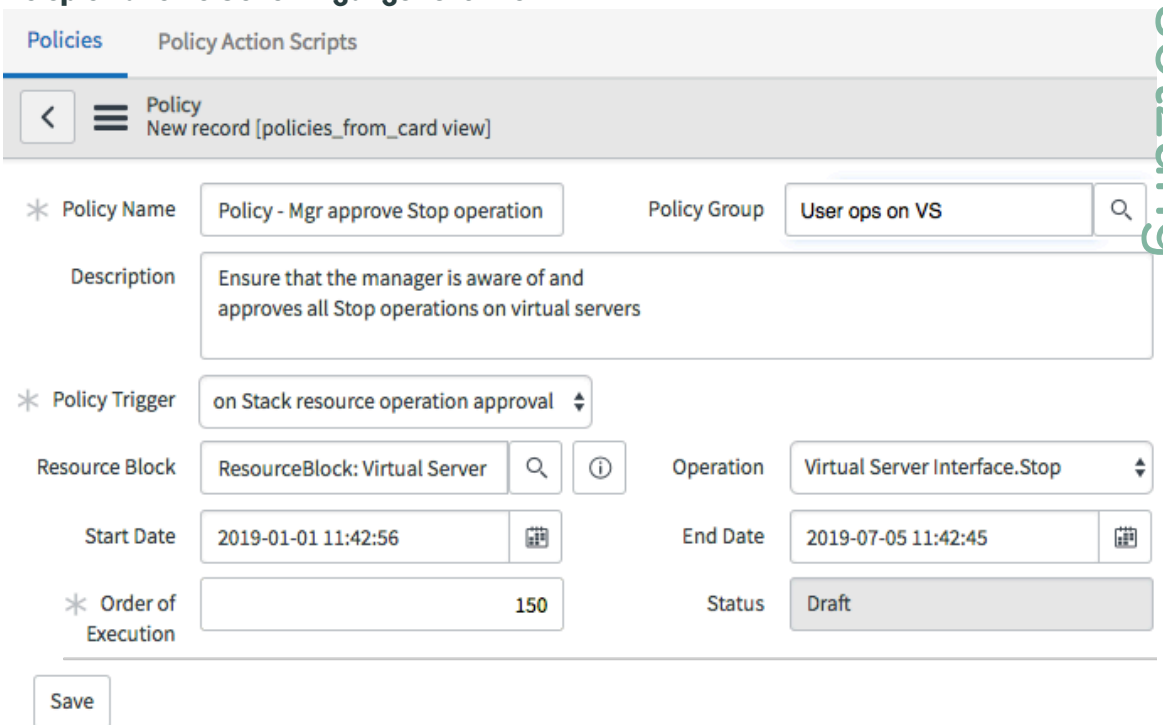
Die gezielten Genehmigungsrichtlinien ergänzen die anwendungsweite Genehmigung.

- **bei Genehmigung des Stapelvorgangs**: Wird während eines beliebigen Stapelvorgangs im Cloudbenutzerportal ausgelöst.
- **bei Genehmigung des Stapelressourcenvorgangs**: Wird während eines Ressourcenvorgangs (Starten, Stoppen, Bereitstellung usw.) im Cloudbenutzerportal ausgelöst.
- **bei Aufgabenremediation**: Wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Beispiel für eine Genehmigungsrichtlinie



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein, der das Wort `Richtlinie` enthält. Beginnen Sie den Namen nicht mit einer Zahl.
Beschreibung	Geben Sie eine eindeutige Beschreibung der Absicht der Richtlinie ein.
Richtliniengruppe	Optional: Wählen Sie eine Richtliniengruppe aus. Jede Richtlinie in der Gruppe wird erzwungen.
Richtlinienauslöser	Wählen Sie einen Auslöser aus, der angibt, wann die Richtlinie angewendet werden soll. Die folgenden Auslöser können Genehmigungsrichtlinien starten: ○ bei Genehmigung der Blaupausenbereitstellung ○ bei Genehmigung des Stapelvorgangs ○ bei Genehmigung des Stapelressourcenvorgangs ○ bei Aufgabenremediation
Blaupause [wird angezeigt, wenn der Auslöser **bei Genehmigung der Blaupausenbereitstellung** oder **bei Genehmigung des Stapelvorgangs** ausgewählt ist]	Wählen Sie die Blaupause aus, für die die Richtlinie gilt. ○ Wenn keine Blaupause angegeben ist, gilt die Richtlinie für jede Blaupause. Diese Einstellung kann die Leistung beeinträchtigen. ○ Sie können einer Blaupause mehrere Richtlinien zuweisen. Wenn mehrere Richtlinien gleichzeitig ausgeführt werden, kann die Leistung jedoch beeinträchtigt werden. Veröffentlichen Sie eine Richtlinie nur dann, wenn sie erzwungen werden soll.
Vorgang [wird angezeigt, wenn der Auslöser **bei Genehmigung des Stapelressourcenvorgangs** ausgewählt ist] Überprüfer: Wird dies auch für „bei Genehmigung des Stapelvorgangs“ angezeigt?	Wählen Sie den Vorgang aus, für den die Richtlinie gilt. Beispielsweise kann eine Richtlinie nur für den Vorgang `Bereitstellung aufheben` oder für alle Vorgänge für die Blaupause oder das Katalogelement gelten. **Hinweis:** Wenn kein Vorgang angegeben ist, gilt die Richtlinie für alle Vorgänge. Diese Bedingung kann die Leistung beeinträchtigen. ○ **Alle**: Beliebiger Vorgang wird ausgeführt. ○ **Starten**: Die Ressource wird gestartet. ○ **Stoppen**: Die Ressource wird gestoppt. ○ **Bereitstellung**: Die Ressource wird bereitgestellt. ○ **Bereitstellung aufheben**: Die Ressource ist für Benutzer nicht mehr verfügbar. ○ **Skript ausführen**: Ein Skript wird mit der Ressource ausgeführt.
Startdatum/Enddatum	Geben Sie das Startdatum an, ab dem die Richtlinie durchgesetzt werden soll, und das Enddatum, ab dem die Richtlinie nicht mehr durchgesetzt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge der Ausführung	Geben Sie eine Zahl an, die die Reihenfolge darstellt, in der die Richtlinie angewendet wird. Eine Richtlinie mit einer niedrigeren Nummer wird vor einer Richtlinie mit einer höheren Nummer ausgeführt. Beispielsweise wird eine Richtlinie mit einer **Reihenfolge** von **100** vor einer Richtlinie mit einer **Reihenfolge** von **200** ausgeführt.
Status	Eine neue Richtlinie befindet sich im Status **Entwurf**. Klicken Sie im Header des Formulars auf **Veröffentlichen**, um die Richtlinie durchzusetzen. Sobald eine Richtlinie veröffentlicht ist, müssen Sie sie auf den Status **Entwurf** setzen, um sie zu aktualisieren.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
4. Wenn Sie bereit sind, die Richtlinie durchzusetzen, klicken Sie auf **Veröffentlichen**.

Nächste Maßnahme

Konfigurieren Sie mindestens eine Cloud-Richtlinienregel.

Cloud-Richtliniengruppe erstellen

Eine Cloud-Richtliniengruppe ist ein Container für zugehörige Richtlinien. Es empfiehlt sich, Richtlinien, die häufig zusammen verwendet werden oder zusammen betrachtet werden sollen, zu gruppieren. Durch die Gruppierung von Richtlinien können Sie Richtlinien konsistent in Ihrer Organisation anwenden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Öffnen Sie eine Cloud-Richtlinie, und klicken Sie auf das Suchsymbol für die **Richtliniengruppe**.
3. Wählen Sie die Gruppe aus, der die Richtlinie hinzugefügt werden soll.
   - Um die Richtlinie einer vorhandenen Gruppe hinzuzufügen, wählen Sie die Gruppe aus und klicken Sie dann auf **Absenden**.
   - Zum Erstellen einer Richtliniengruppe, der die Richtlinie hinzugefügt werden soll, klicken Sie in der Liste „Richtliniengruppen“ auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** an, und klicken Sie dann auf **Absenden**. Die Richtlinie wird der neuen Gruppe hinzugefügt.

Cloud-Richtlinie exportieren oder importieren

Zum Sichern, Verschieben oder Wiederherstellen einer Richtlinie können Sie die Richtlinie als Update Set exportieren und importieren. Das Update Set enthält Regeln, Bedingungen, Aktionen, Skripts und Skriptkategorien.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Richtlinien**an.
2. Führen Sie die folgende Aktion aus, um eine Richtlinie zu exportieren:

   a. Klicken Sie auf das Exportsymbol für die Richtlinie.

   Die Instanz generiert ein Update Set.

3. Zum Importieren einer Richtlinie installieren Sie das Update Set wie folgt:

   a. Navigieren Sie in der Instanz, in die importiert werden soll, zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

   c. Klicken Sie im Popup-Fenster „XML importieren“ auf **Datei auswählen**, wählen Sie die Datei aus, und klicken Sie dann auf **Hochladen**.

Wenn eine Richtlinie, die Sie aus der Quellumgebung exportiert haben, in der Zielumgebung vorhanden ist und beide Richtlinien die gleiche sys_id haben, wird die Richtlinie in der Zielumgebung aktualisiert.

Trouble?

Hinweis: Wenn die Richtlinie, die Sie aus der Quellumgebung exportiert haben, in der Zielumgebung vorhanden ist und die Richtlinien unterschiedliche sys_ids aufweisen, tritt während des Importvorgangs ein Fehler auf. Sie müssen eine andere Richtlinie aus der Quellumgebung exportieren oder die gleichnamige Richtlinie in der Zielumgebung löschen.

Zugehörige Informationen

System-Update Sets

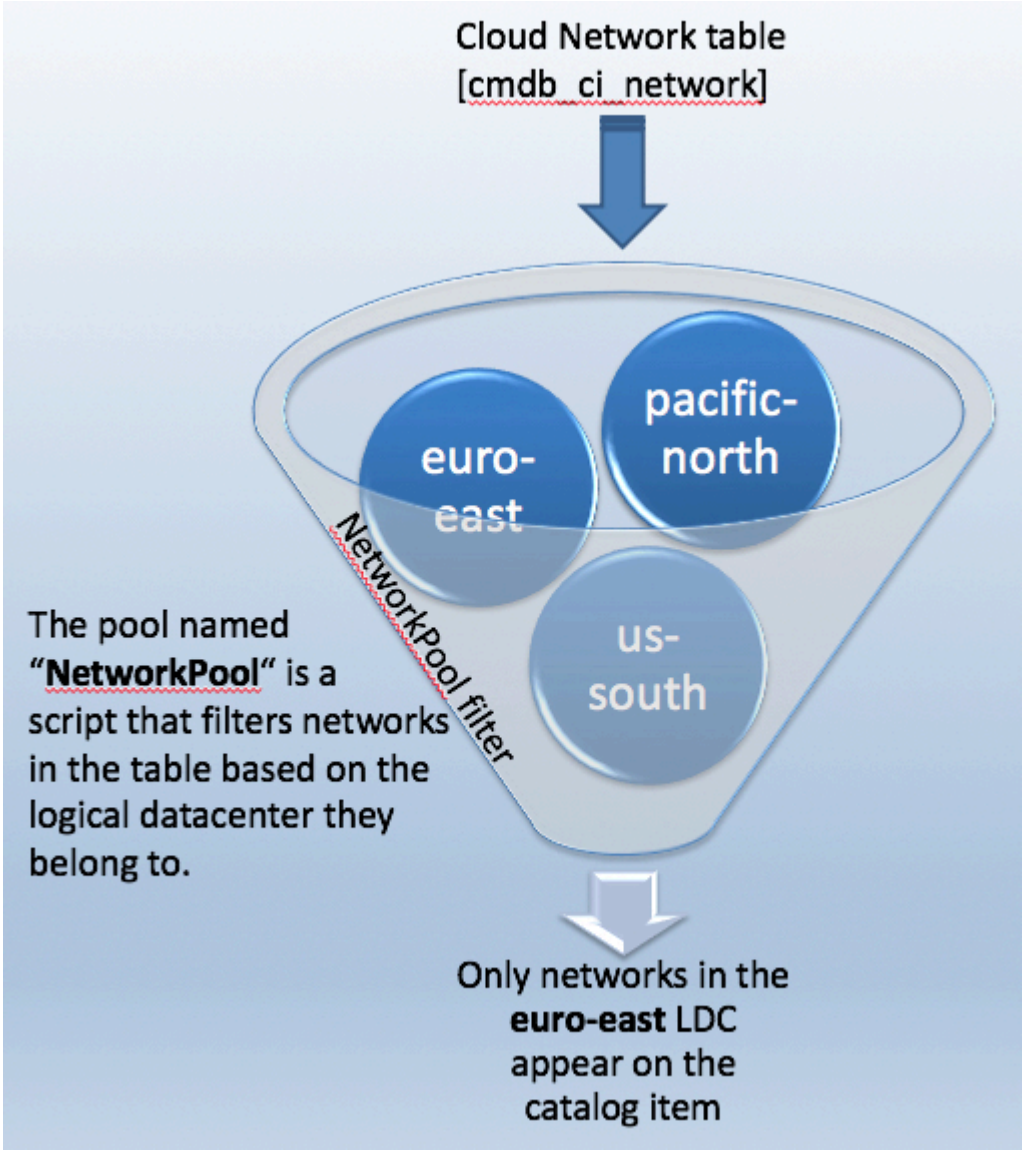
Pools und Filter für Cloud Provisioning

Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.

Beispiel für die Verwendung eines Pools

Um einen Benutzer auf die Netzwerke in einem bestimmten logischen Rechenzentrum zu beschränken, verwenden Sie den `NetworkPool` genannten Ressourcenpool, der mit der Tabelle „Cloud-Netzwerk“ [cmdb_ci_network] ausgeführt wird. Der Ressourcenpool verwendet ein Skript zum Filtern von Netzwerken basierend auf dem Rechenzentrum, zu dem das Netzwerk gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Funktionsweise von Pools

Die Benennungskonvention für Pools lautet:

```
get<thisItem>By<condition>
```

Dabei ist `condition` die Entität der obersten Ebene, die die Beziehung zwischen den Rückgabewerten bildet. Beispielsweise filtert `getObjectIdByServiceAccount` alle ObjectIDs, die auf dem angegebenen Servicekonto gehostet werden.
Abfragetabellen werden nur anhand der angegebenen Bedingung gefiltert. Alle Datensätze, die der Bedingung entsprechen, werden daher zurückgegeben.

Pools und Blaupausen

Beim Konfigurieren von Blaupausen geben Sie Variablen für das Formularverhalten an. Sie können Ressourcenpools als Datenquelle für jede Variable angeben und auswählen, welche Ressourcenpools verwendet werden sollen. Die Variable verwendet dann die gefilterten Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenpool in Basissystem

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
AnsibleInventoryPool	Ansible Tower-Bestand [sn_cfg_ansible_Inventory]	Skript	Filtert den Namen von Ansible Tower Inventory.
ApplicationPool	Applikation	Abfrage	Filtert die Namen von Anwendungen.
AnwendungsprofilePool	Anwendungsprofil [sn_CMP_Application_Profile]	Skript	Filtert den Namen von Anwendungsprofilen.
AvailabilityZonePool	Verfügbarkeitszone [cmdb_ci_av availability_zone]	Skript	Filtert Verfügbarkeitszonen basierend auf dem logischen Rechenzentrum, zu dem sie gehören. getNameByLDC: Filtert Verfügbarkeitszonen basierend auf dem logischen Rechenzentrum, zu dem sie gehören. Die Terraform-Vorlage für IBM erfordert den Namen der Verfügbarkeitszone als Eingabe für die Bereitstellung.
AzureDevOpsPipelinePool	Installierbare Konfiguration [sn_CMP_cfg_installable]	Skript	Filtert die installierbaren Konfigurationen.
AzureDevOpsProjectPool	Azure DevOps-Projekt [sn_itom_csc_cp_Azure_devops_Project]	Skript	Filtert Projekte basierend auf dem Konfigurationsanbieter.
BusinessServicePool	Service [cmdb_ci_service]	Abfrage	Filtert die Namen von Business Services.
ChefServerPool	Chef-Server [sn_cfg_chef_server]	Skript	Filtert Chef-Server-Anmeldeinformationen nach Chef-Server.
CloudAccountPool	Cloud-Konto [cmdb_ci_cmp_cloud_account]	Abfrage	Filtert die Namen von Cloud-Accounts.
CloudKeyPairPool	[cmdb_ci_cloud_key_pair]	Skript	getObjectIdByServiceAccount: Filtert Cloud-Schlüsselpaare basierend auf dem Servicekonto, zu dem sie gehören.
ComputeProfilePool	Computing-Profil [sn_cmp_compute_profile]	Skript	Filtert Computing-Profile nach dem logischen Rechenzentrum und dem Cloud-Konto, zu denen sie gehören.
ConfigMgmtPool		Skript	Filter Konfigurationsmanagement-Arbeitsauslastungsanbieter.
CostCenterPool	Kostenstelle [cmn_cost_center]	Skript	Filtert, um nur die Kostenstellen aufzulisten, zu denen der Benutzer gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
DatastorePool	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Skript	Filtert Datenspeicher basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
HardwareTypePool	[cmdb_ci_compute_template]	Skript	getObjectIdByAvailabilityZone: Filtert Hardwarevorlagen basierend auf der Verfügbarkeitszone, zu der sie gehören.
ImagePool	[cmdb_ci_os_template]	Skript	getObjectIdByServiceAccount: Filtert die resourceId des BS-Images nach Servicekonto. In IBM Cloud beziehen sich BS-Images nicht auf ein Rechenzentrum, sondern werden auf der Servicekonto-Ebene gehostet. Terraform erfordert die resourceId als Eingabe für die Bereitstellung.
IPAddressPool	Cloud-IP-Adresse [cmdb_ci_cloud_ip_address]	Abfrage	Filtert die IP-Adresse.
Starten Sie KonfigurationPool	Server-Array-Startkonfiguration [cmdb_ci_sa_Launch_config]	Abfrage	Filtert den Konfigurationspool.
NetworkInterfacePool	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Skript	Filtert den Netzwerkschnittstellenpool.
NetworkPool	Cloud-Netzwerk [cmdb_ci_network]	Skript	• Filtert Netzwerke basierend auf dem logischen Rechenzentrum, zu dem sie gehören. • getObjectIdByLDC: Filtert Netzwerk-IDs basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
OSProfilePool	BS-Profil [sn_cmp_os_profile]	Skript	Filtert Computing-Profile nach dem logischen Rechenzentrum und dem Cloud-Konto, zu denen sie gehören.
ProjectsPool	Projekt [pm_project]	Abfrage	Filtert die Namen von Projekten.
ResourceGroupPool	Ressourcengruppe [cmdb_ci_resource_group]	Skript	Filtert Ressourcengruppen basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
ZeitplanZonePool	Auswahl [sys_choice]	Skript	Filtert geplante Zeitzonen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
SecurityGroupPool	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Skript	• getByNetwork: Filtert die Sicherheitsgruppe nach dem Netzwerk, zu dem sie gehört. • getObjectIdByServiceAccount: Filtert Sicherheitsgruppen-IDs basierend auf dem Servicekonto, zu dem sie gehören.
SecurityGroupProfilePool	Computing-Sicherheitsgruppenprofil [sn_cmp_security_grp_profile]	Abfrage	Filtert die Namen von Sicherheitsgruppenprofilen.
SSHKeyPool	CMP-SSH-Schlüsselpaar [sn_cmp_ssh_credentials]	Skript	Filtert Benutzerschlüssel nach Benutzer.
StorageAccountPool	Cloud-Speicherkonto [cmdb_ci_cloud_storage_account]	Skript	Filtert Cloud-Speicherkonten basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
StorageVolumePool	Speichervolume [cmdb_ci_storage_volume]	Abfrage	Filtert die Namen von Speichervolumes.
SubnetPool	Cloud-Subnetz [cmdb_ci_cloud_subnet]	Skript	• Filtert das Subnetz nach dem Netzwerk, zu dem es gehört. • getObjectIdByNetwork: Filtert Subnetze basierend auf dem Netzwerk, zu dem sie gehören.
UserGroupPool	Gruppe [sys_user_group]	Skript	Gibt nur die Gruppen zurück, zu denen der Benutzer gehört.
VirtualMachinePool	[sn_cmp_resource_pool]	Skript	getByAvailabilityZone: Filtert VM-IDs basierend auf der Verfügbarkeitszone, zu der sie gehören.
VmFolderPool	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Skript	Filtert VM-Ordner basierend auf dem logischen Rechenzentrum, zu dem sie gehören.

Erstellen Sie einen Ressourcenpool

Ressourcenpools steuern basierend auf Blaupauseneinstellungen die Werte, die einem Benutzer in einem Katalogelement angezeigt werden, wenn er eine Ressource anfordert. Nur Werte, die den Poolfilter oder das Skript passieren, werden als Optionen auf dem Anforderungsformular für Katalogelemente angezeigt.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor

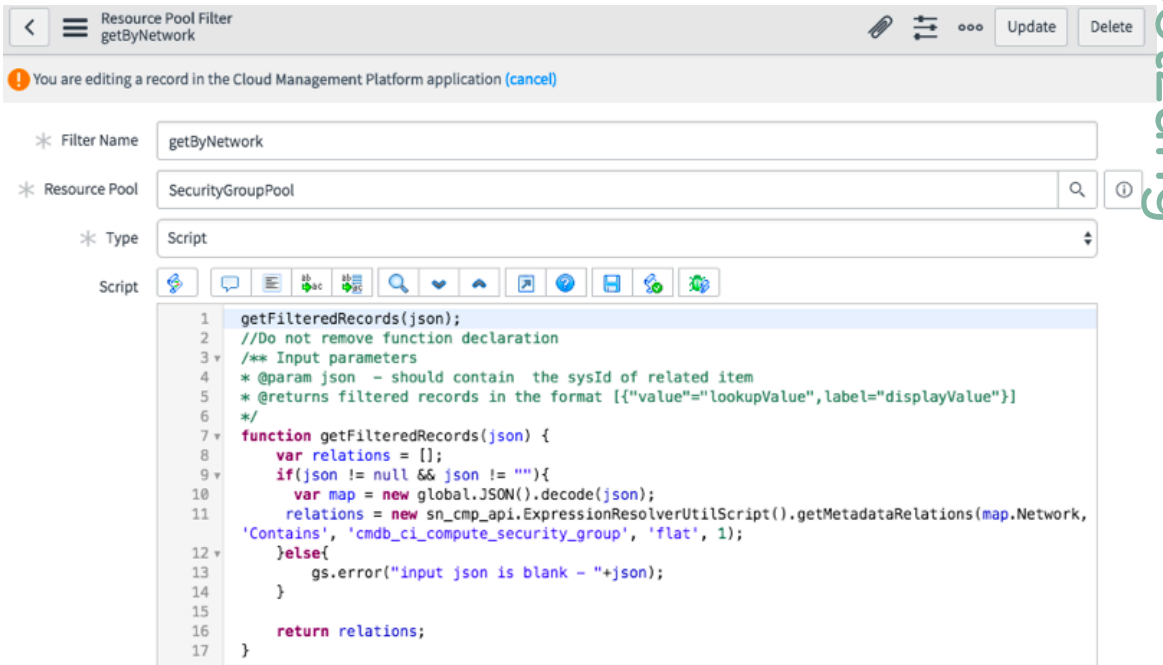
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Ressourcenpools**an.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Ressourcenpoolnamen** ein, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Typ	Wählen Sie den Typ aus, der festlegt, ob die Gesamtzahl der verfügbaren Werte für die Option, die der Benutzer auswählt, gleich bleibt (Statisch) oder um eins verringert wird (Rückläufig).
Suchtabelle	Wählen Sie die Tabelle aus, die die Datensätze enthält, die als Optionen im Katalogelement für die Ressource angezeigt werden sollen.
Suchfeld [Nicht erforderlich, wenn ein Skript verwendet wird. Dieses Feld wird ignoriert, wenn Sie einen Skriptfilter konfigurieren.]	Wählen Sie das Tabellenfeld aus, das die Werte enthält, die dem Benutzer angezeigt werden sollen. Der Anzeigewert für das Suchfeld wird im Cloudbenutzerportal nicht verwendet. Verwenden Sie stattdessen das/die **Suchbezeichnungsfeld(er)**.
Suchbezeichnungsfelder [Nicht erforderlich, wenn ein Skript verwendet wird. Dieses Feld wird ignoriert, wenn Sie einen Skriptfilter konfigurieren.]	Geben Sie das Suchbezeichnungsfeld ein, das dem Benutzer angezeigt werden soll.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
4. Klicken Sie in der zugehörigen Liste „Ressourcenpoolfilter“ auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Filternamen** ein, und füllen Sie dann das Formular aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

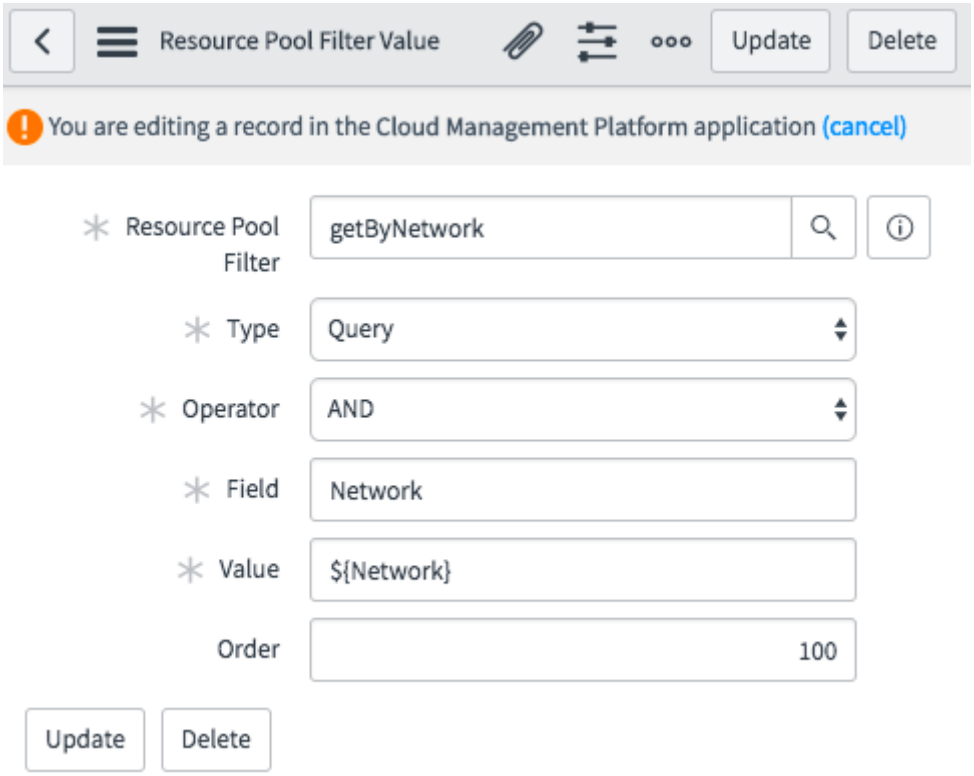
Feld	Beschreibung
Ressourcenpool	Wählen Sie den Ressourcenpool aus, zu dem der Filter gehört.
Typ	Wählen Sie den Typ des Filters aus: ○ **Abfrage**: Führen Sie eine Abfrage für die Datensätze in der Tabelle durch, die Sie für die **Suchtabelle** angegeben haben, basierend auf dem von Ihnen angegebenen **Suchfeld**. ○ **Skript**: Führen Sie ein Skript zum Filtern der Datensätze aus. Geben Sie den Code in das Textfeld **Skript** ein.

Der Ressourcenpoolfilter wird erstellt.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Wenn Sie einen Filterwert an den Pool zurückgeben müssen und dieser Wert einer anderen Tabelle zugeordnet ist, erstellen Sie einen Datensatz in der zugehörigen Liste „Ressourcenpool-Filterwerte“.
6. Klicken Sie in der zugehörigen Liste „Ressourcenpool-Filterwerte“ auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Aktualisieren**.

Feld	Beschreibung
Ressourcenpool Filter	Geben Sie den Namen des Filters ein, zu dem der Filterwert gehört.
Typ	Geben Sie den Typ des Filterwerts ein: ○ **Abfrage**: ○ **Metadatenregel**:
Metadaten-Regelname [Wird angezeigt, wenn Sie als Typ Metadatenregel auswählen]	Geben Sie den Metadaten-Regelnamen ein. Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Metadatenregel** ausgewählt wird.
Operator	Wählen Sie eine der folgenden Optionen aus: ○ **UND** ○ **ODER**
Feld	Geben Sie das Feld in der **Suchtabelle** ein. Beispielsweise **CloudAccount**.
Wert	Geben Sie den Wert, den Sie an den Ressourcenpool zurückgeben, im Format ${feld} ein, wobei feld der Wert im Feld **Feld** ist. Beispielsweise **${CloudAccount}**.
Reihenfolge	Geben Sie eine Reihenfolgennummer ein, die bestimmt, wann der Wert relativ zu anderen Ressourcenpool-Filterwerten angewendet wird. Niedrigere Werte werden zuerst angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Ressourcenpoolfilter wird erstellt.

Binden Sie einen Parameter an einen Ressourcenpool

Um die Katalogbestellung weniger fehleranfällig zu machen, können Sie einen Parameter an binden *Ressourcenpool* (Ein Pool, der in bereitgestellt wird Basissystem). Parameter, die auf einer Ressourcenpoolliste basieren, nur angegebene Werte aus vorhandenen Tabellen im Katalogreihenformular in der Cloudbenutzerportal.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Das Katalogbestellformular listet nur Parameterwerte auf, für die die **Datenquelle** angegeben ist. Wenn Sie beispielsweise den Parameter `Resource Group Name` in Ihrer Vorlage verwenden, können Sie das Feld **Ressourcengruppenname** im Metadatenabschnitt an einen vorhandenen SN-Pool (`ResourceGroupPool`) binden.

Wenn Sie einen Ressourcenblock mithilfe einer Cloud-Vorlage erstellen, können Sie einen Parameter im Metadatenabschnitt der Azure Resource Manager- (ARM) oder CloudFormation-Vorlage (CF) an einen SN-Pool binden. Alle SN-Pools werden im Verfahren aufgelistet.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-Katalogelemente**an.
2. Wählen Sie eine vorhandene Vorlage aus, oder klicken Sie auf **Neu**, um eine neue Cloud-Vorlage zu erstellen.

   Wenn Sie eine vorhandene Vorlage auswählen, benennen Sie die Vorlage um.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im nächsten Schritt ändern Sie die Vorlagendefinition für den entsprechenden Vorlagentyp (wählen Sie ARM oder CloudFormation aus). Sie geben den SN-Poolfilter als Wert für *datasource* an.

SN-Pools, die als Datenquellenwert verwendet werden sollen

SN-Pool	Filter
AvailabilityZonePool	getAllObjects: Ruft alle Verfügbarkeitszonen ab. getObjectsByLDC: Ruft die Verfügbarkeitszone abhängig vom LDC ab.
HardwareTypePool	
ImagePool	
LoadBalancerPool	Alle: Ruft alle Lastenausgleichsmodule ab.
NetworkPool	getAllObjects: Ruft alle Netzwerke ab. getObjectsByLDC: Ruft die Netzwerke abhängig vom LDC ab.
ResourceGroupPool	getObjectsByLDC: Ruft die Ressourcengruppen abhängig vom LDC ab.
SecurityGroupPool	getObjectsByNetwork: Ruft alle Sicherheitsgruppen ab.
SecurityGroupProfilePool	Alle: Ruft alle Sicherheitsgruppenprofile ab.
SSHKeyPool	UserKeys: Ruft alle SSH-Schlüssel ab.
StorageAccountPool	getObjectsByLDC: Ruft die Speicherkonten abhängig vom LDC ab.
StorageVolumePool	Alle: Ruft alle Speichervolumes ab.
SubnetPool	getObjectsByNetwork: Ruft alle Subnetze ab.
VirtualMachinePool	getByAvailabilityZone: Ruft alle virtuellen Computer ab.

3. Ändern Sie eine ARM-Vorlagendefinition:

   a. Fügen Sie das Attribut *SNC::Parameter::Metadata* im Metadatenabschnitt *parameters* hinzu.

   b. Für *SNC::Parameter::Metadata*Attribut, hinzufügen *Datenquelle* Als Schlüssel und geben Sie einen SN-Poolfilter für den Wert ein, z. B. StorageAccountPool.getObjectsByLDC Wie in diesem Beispiel gezeigt.

```
"parameters": {
   "newStorageAccountName": {
    "type": "string",
    "metadata": {
      "description": "Unique DNS Name for the Storage Account where the Virtual
 Machine's disks will be placed.",
       "SNC::Parameter::Metadata": {
       "allowedPattern": "[0-9a-z]{1,11}",
       "ConstraintDescription": "must be a alphanumeric ",
       "datasource":"ServiceNow::Pools::StorageAccountPool.getObjectsByLDC",

      }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    }
  }
```

4. Ändern Sie eine CloudFormation-Vorlagendefinition:

   a. Fügen Sie das Attribut hinzu `SNC::Parameter::Metadata`Und definieren Sie den Namen des anwenderdefinierten Attributs (`VpcId`) Mit `datasource`.
   Für `datasource`Wert: Geben Sie einen SN-Poolfilter ein, z. B. Netzwerkpool.getObjectsByLDC In diesem Beispiel.

   b. Definieren Sie das Zuordnungsattribut `datasourceFilter`, um den benutzerdefinierten Namen (`VpcId`) an den tatsächlichen Attributnamen (`Network`) zu binden.

```
"Parameters" : {

    "VpcId" : {
    "Type" : "AWS::EC2::VPC::Id",
    "Description" : "VpcId of your existing Virtual Private Cloud (VPC)",
    "ConstraintDescription" : "must be the VPC Id of an existing Virtual Private Cloud."
  },

  "SubnetId" : {
    "Type" : "AWS::EC2::Subnet::Id",
    "Description" : "SubnetId of an existing subnet (for the primary network) in your Virtual
Private Cloud (VPC)",
    "ConstraintDescription" : "must be an existing subnet in the selected Virtual Private
Cloud."
  }
 },
 "Metadata": {
       "SNC::Parameter::Metadata": {
           "VpcId":{
              "datasource":"ServiceNow::Pools::NetworkPool.getObjectsByLDC",
              "datasourceFilter":{"Network":"VpcId"}
           },
           "SubnetId":{
              "datasource":"ServiceNow::Pools::SubnetPool.getObjectsByNetwork",
              "datasourceFilter":{"Network":"VpcId"}
           }

       }
  }
```

5. Klicken Sie auf **Absenden**.

6. Nachdem der Ressourcenblock, die Blaupause und die Katalogelemente erstellt wurden, sieht der Benutzer des Cloud-Service im Katalogbestellformular nur die Werteliste der Pooldaten für den Parameter.

Beispiel-Ressourcenpool, der die Auswahlmöglichkeiten auf die Kostenstelle beschränkt

Sie können Ressourcenpools mit Blaupausen verwenden, um die Auswahlmöglichkeiten im Cloud-Kataloganforderungsformular zu beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfall: Kostenstellenauswahl beschränken

In diesem Beispiel werden die Kosten des Cloud-Assets mit dem Budget der Kostenstelle des Benutzers verrechnet. Basissystem **UserCostCenter** Ressourcenpool stellt sicher, dass ein Benutzer nur Ressourcen in seiner Kostenstelle auswählen kann.

Annahmen

- Das Plugin „Cost Management“ [con.snc.cost_management] ist aktiv.
- Kostenstellen sind definiert, und den Kostenstellen sind Benutzer zugeordnet.
- Mindestens eine Blaupause ist definiert. In diesem Beispiel wird eine Blaupause mit dem Namen **Virtueller AWS-Server** verwendet.
- Ihnen ist die Rolle „sn_cmp_cloud_admin“ zugewiesen, und Sie kennen JavaScript- und JSON-Skripting.

Komponenten

Ressourcenpoolfilter überprüfen

1. Navigieren Sie im Cloud-Administratorportal zu **Verwalten** > **Ressourcenpools**an.
2. Öffnen Sie den **CostCenterPool**, und überprüfen Sie die zugehörigen Ressourcenpoolfilter.
   - **Alle** ist ein Abfragefilter, der alle Kostenstellen in der Tabelle zurückgibt.
   - **UserCostCenter** ist ein Skriptfilter, der die Kostenstelle sucht, die dem Benutzer zugeordnet ist, der das Element bestellt.

   Dies ist das Skript für den Filter **UserCostCenter**:

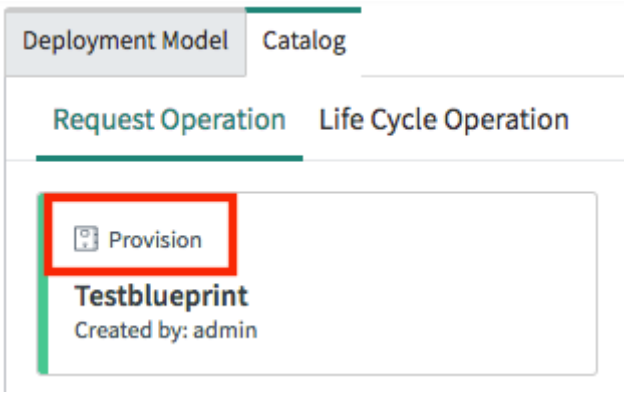
```
getFilteredRecords();
//Do not remove function declaration
/**
* @returns filtered records in the format
 [{"value"="lookupValue",label="displayValue"}]
*/
function getFilteredRecords() {
 var filteredRecords = [];
 var userId = gs.getUserID();
 var userGr = new GlideRecord('sys_user');
 if (userGr.get(userId)){
  var costCenterId = userGr.getValue('cost_center');
  if (costCenterId){
   var costCenterGr = new GlideRecord('cmn_cost_center');
   if (costCenterGr.get(costCenterId)){
    var costCenter = {};
    costCenter.value = costCenterGr.getUniqueValue();
    costCenter.label = costCenterGr.getValue('name');
    filteredRecords.push(costCenter);
   }
  }
 }

 //force to string
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

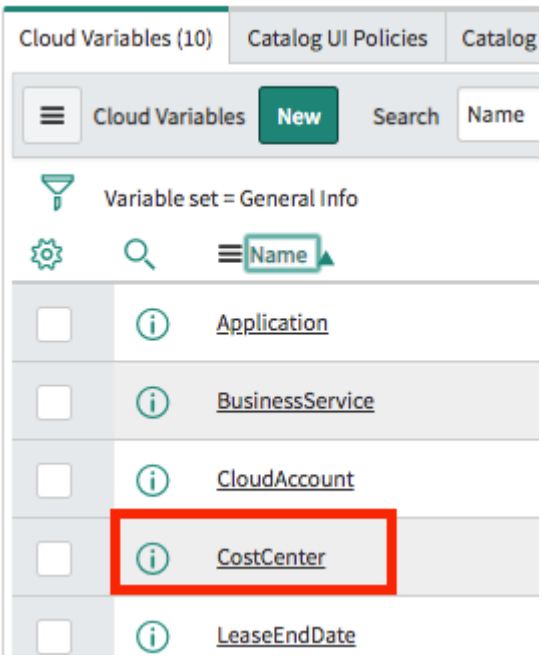
```
return new global.JSON().encode(filteredRecords);
}
```

Parameter des Blaupausenkatalogformulars

1. Navigieren zu **Entwurf** > **Blueprints**, Und klicken Sie dann auf die Kachel für den Blueprint, den Sie öffnen möchten.
2. Mit dem Blueprint in **Entwurf** status, klicken Sie auf **Bereitstellung** Vorgangskachel auf der **Katalog** > **Anforderungsvorgang** Registerkarte



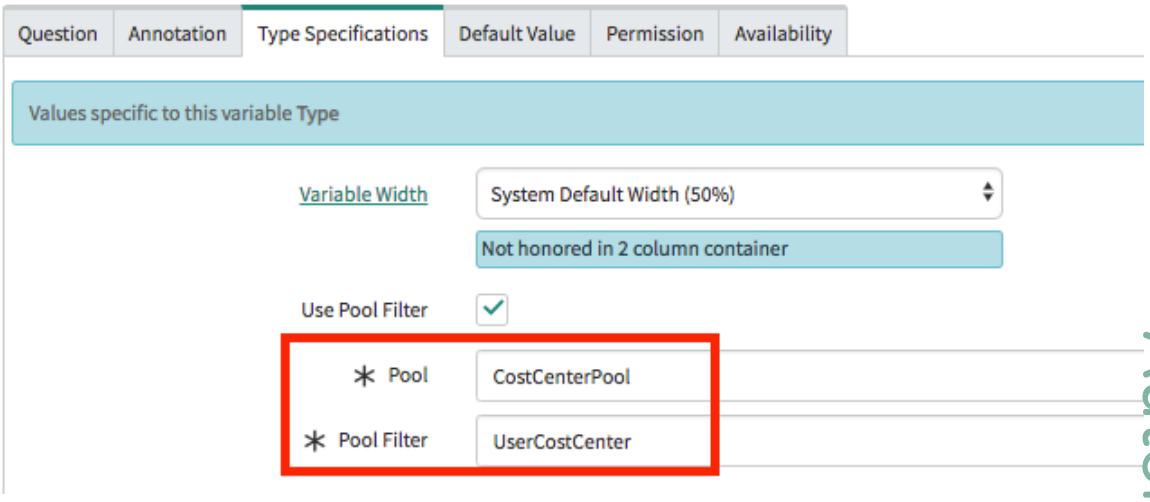
3. Klicken Sie in der zugehörigen Liste „Variablensätze“ auf den Variablensatz **Allgemeine Informationen**. Standardmäßig befindet sich die Variable „CostCenter“ in diesem Variablensatz.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf die Variable **CostCenter**.



5. Klicken Sie auf dem Formular „Cloud-Variable“ auf die Registerkarte **Typspezifikationen**.
6. Sehen Sie sich die Felder **Pool** und **Poolfilter** an, die auf den Ressourcenpool und Filter verweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

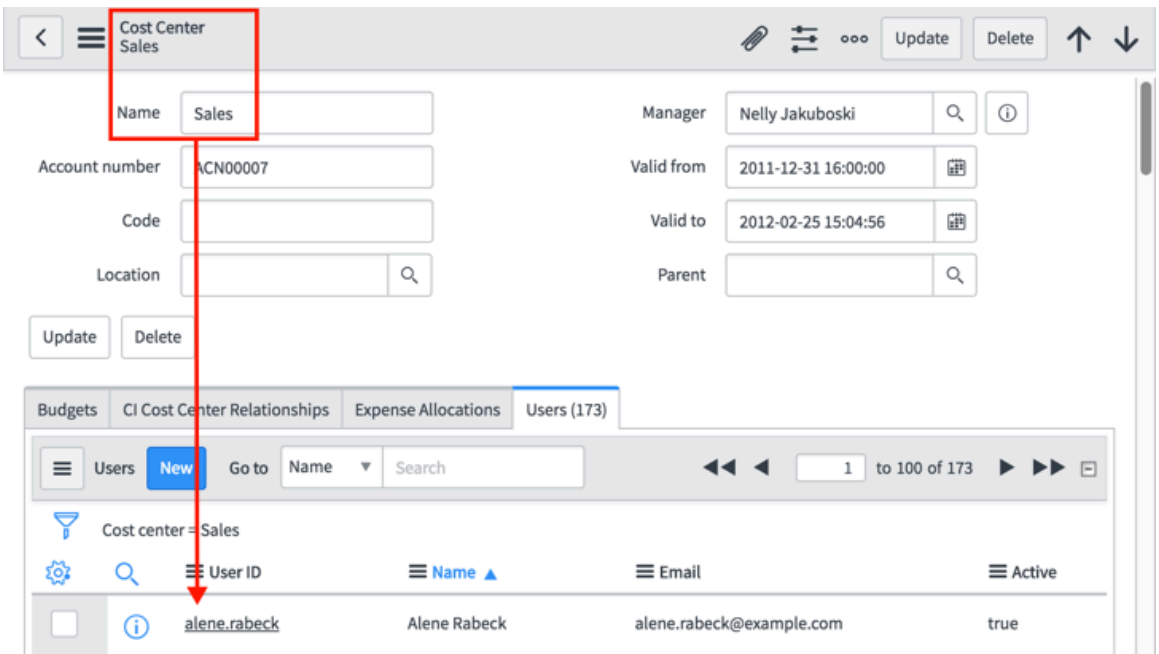
- `CostCenterPool` ist der Name des Ressourcenpools.
- `UserCostCenter` ist das Filterskript, das die Kostenstellenoptionen für die Auswahl durch den Benutzer abruft.



7. Legen Sie die Blaupause auf **Veröffentlicht** fest.

Kostenstellenbenutzer

Identifizieren Sie einen Benutzer, der Mitglied einer Kostenstelle ist und Zugriff auf das Cloudbenutzerportal hat.



Ressourcenpoolfilter testen

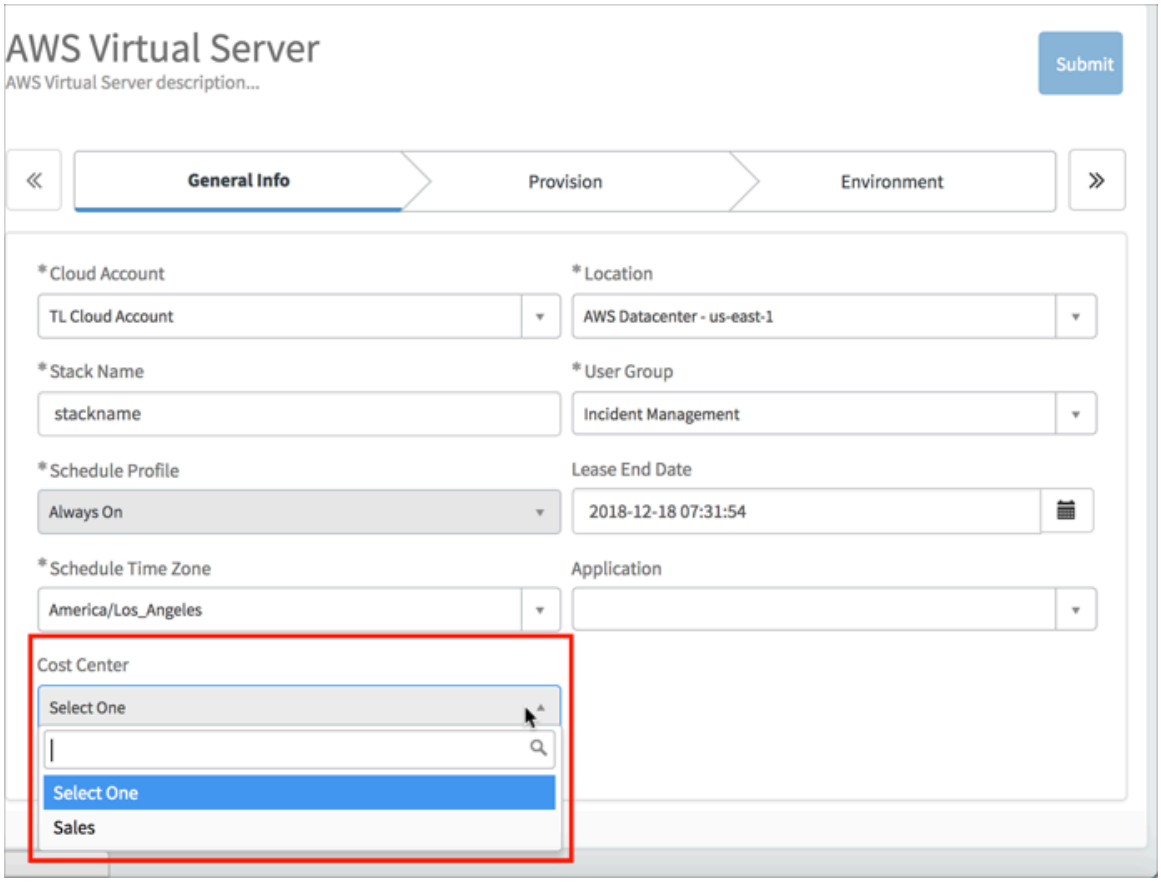
Nach der Überprüfung der Komponenten dieses Anwendungsfalls testen Sie das Cloud-Katalogelement, um sicherzustellen, dass Benutzer nur ihre Kostenstelle auswählen können.

1. Nehmen Sie in diesem Beispiel die Identität der Benutzerin **Alene Rabeck** an.
2. Klicken Sie im Cloudbenutzerportal auf **Einen Stapel starten**, und wählen Sie dann das Cloud-Katalogelement aus (in diesem Beispiel **Virtueller AWS-Server**).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Überprüfen Sie die Auswahlmöglichkeiten in der Liste **Kostenstelle**.



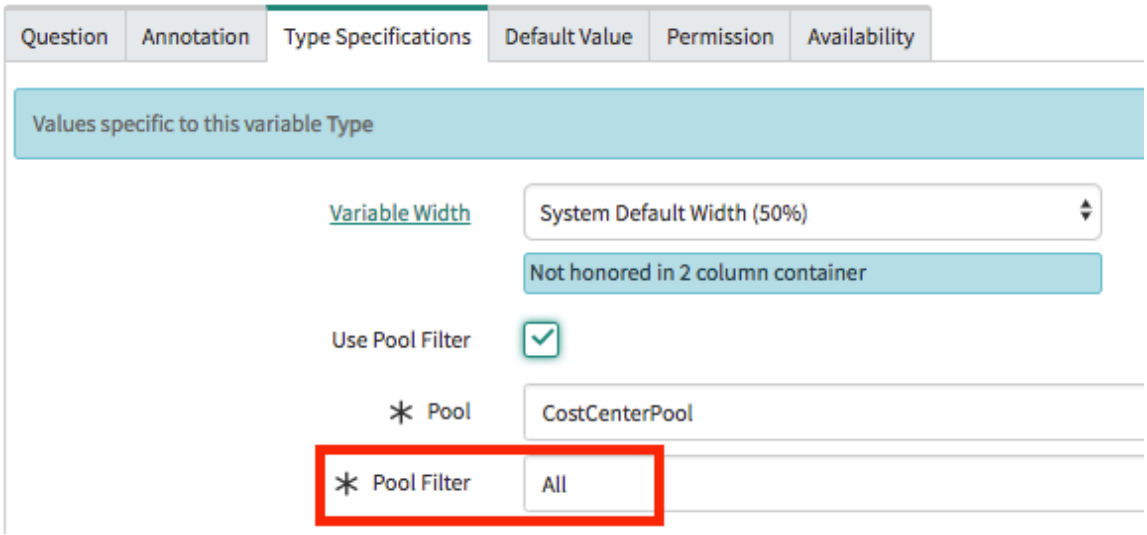
Mit dem Datenquellenwert `CostCenterPool::UserCostCenter` für dieses Katalogelement ist die einzige Option für die **Kostenstelle** die Kostenstelle, bei der der Benutzer Mitglied ist.

Ressourcenpoolfilter ändern

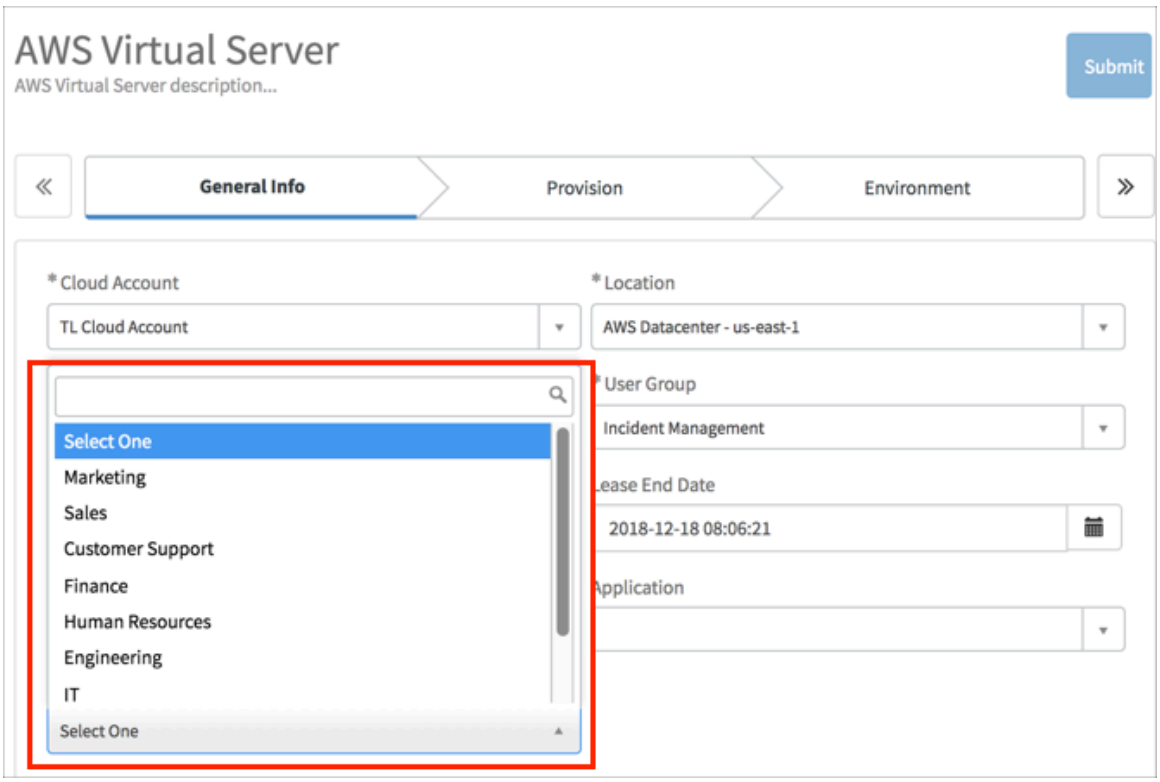
Testen Sie, ob der Ressourcenpoolfilter das Verhalten des Felds **Kostenstelle** steuert, indem Sie ihn ändern und sich die Ergebnisse ansehen.

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Blueprints** Und klicken Sie dann auf **Virtueller AWS-Server** .
2. Klicken Sie auf die Vorgangskachel **Bereitstellung**.
3. Klicken Sie in der zugehörigen Liste „Variablensätze“ auf den Variablensatz **Allgemeine Informationen**. Standardmäßig befindet sich die Variable „CostCenter“ in diesem Variablensatz.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf die Variable **CostCenter**.
5. Klicken Sie auf dem Formular „Cloud-Variable“ auf die Registerkarte **Typspezifikationen**.
6. Bearbeiten Sie das Feld **Poolfilter**, um den Filter von `UserCostCenter` in `All` zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Aktualisieren** und anschließend auf **Veröffentlichen**.
8. Nehmen Sie in diesem Beispiel die Identität der Benutzerin **Alene Rabeck** an.
9. Starten Sie im Cloudbenutzerportal einen Stapel, und wählen Sie dann **Virtueller AWS-Server** aus.
10. Stellen Sie sicher, dass alle Kostenstellen aufgelistet sind.



Kontingente und Steuerungen für Ressourcenbestellungen

Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie wenden Kontingente auf eine Ressource, z. B. einen virtuellen Server, ein Rechenzentrum oder eine generische Cloud-Ressource sowie auf Benutzer einer bestimmten Gruppe an. Sie können für die Ressource ein Limit pro Benutzer und ein Gesamtlimit für die Gruppe festlegen. Beispielsweise kann ein Kontingent die Anzahl der zulässigen virtuellen Server für Benutzer in der Gruppe **Datenbank** beschränken.

Nachdem diese Art von Kontingent festgelegt wurde, erhalten Benutzer, die versuchen, zusätzliche virtuelle Server bereitzustellen, eine Fehlermeldung und sie können erst mit der Bereitstellung virtueller Server fortfahren, wenn die Ressourcenanzahl wieder unter dem Kontingentgrenzwert liegt. Wenn ein Benutzer zu mehr als einer Gruppe gehört, erhält er als Kontingent das kombinierte Gesamtlimit der beiden Gruppen.

Hinweis: Sie können für Ressourcen auch Beschränkungen pro Rechenzentrum festlegen, indem Sie Kapazitätsgrenzen in Cloud-Accounts verwenden. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.

Ressourcenblocktypen, Kontingenttypen und Attribute

Sie können Benutzern oder Gruppen Kontingente für die folgenden Ressourcenblocktypen zuweisen:

- Virtuelle Server
- Speicherlaufwerkgröße
- Netzwerk
- Stapel

Kontingenttypen enthalten:

Summe

Die Summe aller Attribute für eine Ressource, z. B. die Summe aller virtuellen CPUs.

Anzahl

Die Gesamtanzahl der Attribute für eine Ressource, z. B. die Anzahl der virtuellen Computer.

Cloud-Kontingentdefinition erstellen

In einer Cloud-Kontingentdefinition werden die Einschränkungen für einen Ressourcenblock angegeben. Sie können Vorlagen verwenden oder manuell verschiedene Konfigurationstypen für jede Kontingentdefinition erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Quote**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Kontingentdefinition“

Feld	Beschreibung
Kontingentdefinition	Eindeutiger Bezeichner für die Kontingentdefinition. Normalerweise ist dies Ressourcenname_count oder Ressourcenname_size. Zum Beispiel: Network_Count, VM_Count oder StorageVolume_Size.
Kontingenttyp	Typ der festzulegenden Kontingenteinschränkung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Anzahl ○ Größe
Ressourcenname	Der Ressourcenblocktyp, auf den das Kontingent angewendet werden soll. Wählen Sie diesen aus der Nachschlageliste aus. Wählen Sie für vorlagenbasierte Cloud-Ressourcen beispielsweise „Cloud-Ressource“ aus. Weitere Informationen finden Sie unter Ressourcenblöcke in Cloud Provisioning and Governance.
Berechnungseinheit	Einheit, in der dieses Kontingent berechnet wird: ○ GB ○ Einzel
CI-Klasse	CMDB-CI-Klasse, die aus der Nachschlageliste ausgewählt werden soll
Attribut	Spaltenname aus dem zugrunde liegenden CI-Typ für den Ressourcenblock, der den Wert enthält, der mit dem Kontingent eingeschränkt werden soll. Beispiel: Wenn Ihr Kontingent die CPU-Anzahl auf einem virtuellen Server begrenzt, lautet die Tabelle des zugrunde liegenden CI-Typs „cmdb_ci_vm_instance“. Die Spalte **cpus** enthält diese CPU-Daten. Geben Sie daher `cpus` ein. Sie können auch `instance` eingeben.
Vorlage [optional]	Tabellenname eines Ressourcentyps, z. B. Hardwaretyp [cmdb_ci_compute_template] oder Image [cmdb_ci_os_template]
Vorlagenattribut [optional]	Spalte aus der Tabelle, die Sie im Feld „Vorlage“ angegeben haben. Dies ist das Attribut, für das das Kontingent festgelegt wird. Beispiel: Wenn Sie die Vorlage [cmdb_ci_compute_template] ausgewählt haben und ein Kontingent für die virtuellen CPUs festlegen möchten, geben Sie `vcpus` ein. In dieser Spalte wird die Anzahl der virtuellen CPUs für alle Datensätze in der Tabelle [cmdb_ci_compute_template] gespeichert.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
   Die zugehörigen Listen „Kontingentkonfigurationen“, „Standardkontingente“ und „Cloud-Vorlagenressourcen“ werden angezeigt.
5. Klicken Sie in der zugehörigen Liste „Kontingentkonfigurationen“ auf **Neu**.
6. Füllen Sie die Felder im Formular aus.

Formular „Kontingentkonfigurationen“

Feld	Beschreibung
Gruppenname	Eindeutiger Name für die Konfigurationsgruppe
Maximaler Gruppengrenzwert	Maximales Kontingent der Gruppe
Kontingentdefinitionstyp	Der Name der Kontingentdefinition.
Grenzwert pro Benutzer	Maximales Kontingent der einzelnen Benutzer in der Gruppe

7. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. **Wahlweise:** Sie können optionale Standardkontingente angeben, die für den Ressourcenblock festgelegt werden, indem Sie in der zugehörigen Liste „Standardkontingente“ auf **Neu** klicken und dann das Formular ausfüllen.

Formular „Standardkontingente“

Feld	Beschreibung
Maximaler Gruppengrenzwert	Maximales Kontingent der Gruppe
Kontingentdefinition	Die Kontingentdefinition, für die Sie die Standardwerte festlegen.
Grenzwert pro Benutzer	Kontingentgrenze, die für die einzelnen Benutzer in dieser Gruppe gilt

9. Klicken Sie auf **Absenden**.
10. Ordnen Sie das Katalogelement zu, für das das von Ihnen definierte Kontingent gilt, indem Sie in der zugehörigen Liste „Cloud-Vorlagenressourcen“ auf **Neu** klicken.

> **Hinweis:** Wenn Sie einem Katalog kein Kontingent zuordnen, wird für den betreffenden Katalog kein Kontingent berechnet.

11. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Vorlagenressourcen“

Feld	Beschreibung
Domäne	Domäne, auf die dieses Kontingent angewendet wird
Kontingentdefinition	Name der Kontingentdefinition, die Sie anwenden
Katalogelement	Katalogelement oder Cloud-Ressource, das/die Sie dem Kontingent zuordnen

12. Klicken Sie auf **Absenden**.

Ergebnis

Sie haben die Cloud-Kontingentdefinitionen und Kontingentgrenzen für Benutzer und Benutzergruppen festgelegt.

Zugehörige Informationen

Ressourcenblöcke in Cloud Provisioning and Governance

Steuerungen für Ressourcenbestellungen für vorlagenbasierte Cloud-Katalogelemente

Verwenden Sie Steuerungen für Ressourcenbestellungen, um mithilfe von Kontingentdefinitionen und -richtlinien Kontingentprüfungen für vorlagenbasierte Katalogelemente durchzuführen. Mit Kontingentgrenzen können Sie die Bereitstellung oder Bestellung von Ressourcen für Benutzer und Gruppen steuern. Konfigurieren Sie Richtlinienaktionen, um Benachrichtigungen, einen Genehmigungs-Subflow oder beides auszulösen.

Steuerungen für Ressourcenbestellungen

Mit den Steuerungen für Ressourcenreihenfolgen können Sie die Kontingentgrenze von Ressourcen steuern, die über vorlagenbasierte Kataloge bereitgestellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontingentprüfungen für auf Cloud-Vorlagen basierende Katalogelemente sind ab Release Zurich verfügbar.

Sie können jetzt Quotengrenzen vorlagenbasierten Katalogen zuordnen und Benachrichtigungen oder einen Genehmigungs-Subflow auslösen, wenn die von Ihnen für einen Anwender oder eine Anwendergruppe angegebene Ressourcengrenze oder Quotendefinitionen überschritten wird. Weitere Informationen finden Sie unter Ressourcenquote .

Verwenden Sie Ressourcensteuerungen, um die folgenden Aktionen auszuführen:

- Berechnen Sie das Kontingent und die Kapazität für vorlagenbasierte Katalogelemente.
- Legen Sie bei der Bereitstellung für Cloud-Benutzer Grenzen für das Stapelkontingent fest.
- Erstellen Sie eine Richtlinie, die ausgelöst werden soll, wenn eine Kontingentgrenze überschritten wird.
- Fügen Sie eine Richtlinienbenachrichtigung und eine Anforderung zur Genehmigung bei Überschreiten einer Kontingentgrenze hinzu.
- Zeigen Sie im Cloud-Benutzerportal Benutzer- und Benutzergruppenkontingente für vorlagenbasierte Kataloge an.

Funktionsweise von Steuerungen für Ressourcenbestellungen

Steuerungen für Ressourcenbestellungen werden nur angewendet, wenn das Kontingent überschritten wurde. Wenn das Kontingent während der Katalogbereitstellung zum ersten Mal überschritten wird, nachdem Steuerelemente für Ressourcenbestellungen konfiguriert wurden, werden die Cloud-Ressourcen weiterhin bereitgestellt. Wenn Cloud-Benutzer jedoch erneut versuchen, eine Ressource bereitzustellen, bei der die konfigurierten Kontingentgrenzen überschritten werden, wird die für die Richtlinie zur Steuerung von Ressourcenbestellungen eingerichtete Richtlinienaktion „bei Ressourcengrenzen überschritten“ ausgelöst.

Hinweis: Wenn einem vorlagenbasierten Katalog kein Kontingent zugeordnet ist, finden für diesen Katalog keine Kontingentberechnungen statt, selbst wenn Benutzer ihre Kontingentgrenzen überschreiten.

Angenommen, Sie geben eine Kontingentgrenze von 20 GB für ein Speichervolume eines Cloud-Benutzers an, und der Benutzer stellt ein Speichervolume mit 40 GB bereit. Beim ersten Mal wird das Speichervolume bereitgestellt, obwohl die Kontingentgrenze überschritten wird. Die Bereitstellung schlägt jedoch fehl, wenn der Benutzer das nächste Mal versucht, eine Cloud-Ressource mit mehr als 20 GB bereitzustellen.

Stapelanzahl-Kontingent

Mit dem Stapelanzahl-Kontingent wird im Basissystem ein Standardkontingent für vorlagenbasierte Cloud-Katalogelemente eingeführt. Für das Stapelanzahl-Kontingent werden alle aktiven Stapel (identifiziert durch die CI-Klasse `Stack`) gezählt, die von Benutzern und Benutzergruppen bereitgestellt werden. Das Stapelanzahl-Kontingent gilt für alle vorlagenbasierten Cloud-Ressourcen. Sie müssen dabei keine Katalogelemente zu bestehenden Kontingentdefinitionen zuordnen. Sobald das Stapelkontingent aktiviert ist, wird das Kontingent jedes Mal berechnet, wenn ein Benutzer aus der Gruppe, die dem Stapelkontingent zugeordnet ist, eine Cloud-Ressource bereitstellt. Wenn Benutzer aus der zugeordneten Gruppe versuchen, Ressourcen über das festgelegte Stapelkontingent hinaus bereitzustellen, werden die Richtlinie zur Steuerung von Ressourcenbestellungen und die Richtlinienaktion `on Resource Limit exceeded` ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das im Basissystem bestehende Stapelanzahl-Kontingent beinhaltet keine vordefinierten Standardkontingente, mit denen vor dem Upgrade auf Zurich erstellte Stapel beibehalten werden. Um das Stapelanzahl-Kontingent zu aktivieren, müssen Sie standardmäßige Kontingentgrenzen für Benutzer und Benutzergruppen festlegen.

Richtlinie zur Steuerung von Ressourcenbestellungen

Die Richtlinie zur Steuerung von Ressourcenbestellungen ist eine Basissystem-Richtlinie, die standardmäßig den Status „Entwurf“ aufweist. Sie können die Standardrichtlinie an Ihre Anforderungen anpassen und sie veröffentlichen oder eine neue Richtlinie erstellen und Kontingente, Regeln und Aktionen definieren, um Steuerungen für Ressourcenbestellungen zu aktivieren. Die Richtlinienaktion „bei Ressourcengrenzen überschritten“ löst die Anwendung der Richtlinie zur Steuerung von Ressourcenbestellungen aus, sobald bei einer Ressource die definierte Kontingentgrenze überschritten wird. Sie können festlegen, ob ein Genehmigungs-Subflow, eine Benachrichtigung oder eine Kombination aus beidem initiiert werden soll, wenn die Richtlinie über die Ressourcengrenze überschritten wird. Weitere Informationen finden Sie unter Aktion für eine Richtlinie „bei Ressourcengrenzen überschritten“ erstellen.

Hinweis: Sobald das Kontingent des Benutzers oder der Benutzergruppe überschritten wurde, können Sie nur dann Katalogelemente bereitstellen, wenn die Richtlinie veröffentlicht wird. Das liegt daran, dass das aktuelle Systemverhalten von Kontingenten eine weitere Bereitstellung verhindert und die Anforderung nicht weiter verarbeitet.

Nächste Schritte

Steuerungen für Ressourcenbestellungen einrichten

Erstellen Sie Kontingentdefinitionen und Richtlinien, die auf Cloud-Vorlagen basierenden Katalogelementen zugeordnet sind. Verwenden Sie Richtlinienregeln und -Aktionen, um einen Genehmigungs-Subflow oder eine Benachrichtigung auszulösen, wenn die für die Gruppe oder den Anwender definierte Kontingentgrenze überschreitet.

Vorbereitungen
Voraussetzungen:

- Mindestens eine Cloud-Richtliniengruppe
- Auf Cloud-Vorlagen basierende Katalogelemente
- Stellen Sie sicher, dass Ihre CMDB über die ereignisgesteuerte Discovery aktualisiert wird, um eine genaue Kontingentdurchsetzung zu gewährleisten.
- Stellen Sie sicher, dass Sie beim Konfigurieren von Kontingentdefinitionen einem Katalog in der zugehörigen Liste „Cloud-Vorlagenressourcen“ ein Kontingent zuordnen.

Erforderliche Rolle: sn_cmp.cloud_governor

Warum und wann dieser Vorgang ausgeführt wird
Beachten Sie Folgendes, bevor Sie mit der Einrichtung von Steuerungen für Ressourcenbestellungen beginnen:

- Das Kontingent wird nur für die Ressourcenblöcke berechnet, die an eine CI-Klasse in der CMDB gebunden sind. Wenn Sie benutzerdefinierte Ressourcenblöcke erstellen, die der CI-Klasse in der CMDB nicht zugeordnet sind, findet für diese Ressourcentypen keine Kontingentberechnung statt.
- Wenn Sie sowohl die Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) als auch eine Genehmigungsrichtlinie „bei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Blaupausenbereitstellung“ konfiguriert haben, hat die Genehmigungsrichtlinie „bei Blaupausenbereitstellung“ Vorrang vor der Genehmigungsrichtlinie zur Steuerung von Ressourcenbestellungen.

Prozedur

1. Definieren Sie das Kontingent, oder verwenden Sie eine Kontingentdefinition des Basissystems für einen Ressourcenblock.

   a. Navigieren Sie im Cloud-Administratorportal zu **Bedingungen** > **Quote** > **Kontingentdefinition**an.

   b. Legen Sie Kontingentdefinitionen fest.

   Für die Basissystem-Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) ist standardmäßig die ServiceNow-Standardregel für Genehmigungsrichtlinien konfiguriert. Wenn Sie andere Aktionen wie Benachrichtigungen oder einen anwenderdefinierten Genehmigungs-Subflow auslösen möchten, wenn das Ressourcenlimit überschritten wird, können Sie entweder die Richtlinienaktion des Basissystems ändern oder eine anwenderdefinierte Richtlinie für Ihre Instanz erstellen.

   - Ändern Sie eine Kontingentdefinition des Basissystems, indem Sie die Werte der Standardkontingente pro Benutzer und Benutzergruppe und die Benutzergruppen festlegen, für die das jeweils definierte Kontingent gilt.

     Für die folgenden vordefinierten Basissystemkontingente sind Standardkontingente definiert:

     - `VM_Count`
     - `vCPUs Count`
     - `StorageVolume_Size`
     - `Stack_Count`
     - `Network_Count`

     Wichtig: `Stack_Count` gilt nur für vorlagenbasierte Cloud-Ressourcen.

   - Erstellen Sie eine Kontingentdefinition.

     Weitere Informationen finden Sie unter Cloud-Kontingentdefinition erstellen.

2. Ordnen Sie das Kontingent einem vorlagenbasierten Cloud-Katalogelement zu.

   Wichtig: Wenn vorlagenbasierten Katalogen beim Konfigurieren von Kontingentdefinitionen keine Kontingente zugeordnet werden, finden für die betreffenden Kataloge keine Kontingentberechnungen statt, selbst wenn benutzerdefinierte Kontingente überschritten werden. Weitere Informationen finden Sie unter Cloud-Kontingentdefinition erstellen

   a. Klicken Sie in der zugehörigen Liste „Cloud-Vorlagenressourcen“ auf **Neu**.

   b. Wählen Sie im Feld **Katalogelement** das Katalogelement aus, dem Sie diese Kontingentdefinition zuordnen möchten.

   c. Klicken Sie auf **Absenden**.

3. Konfigurieren Sie eine Richtlinienregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Bedingungen** > **Richtlinien**an.

b. Öffnen Sie die Basissystem-Richtlinie Resource Order Control (Steuerung von Ressourcenbestellungen). Die Basissystem-Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) weist standardmäßig den Status „Entwurf“ auf.

c. Navigieren Sie zur zugehörigen Liste „Regeln“, und ändern Sie entweder eine Basissystemregel, oder konfigurieren Sie eine neue Regel, wenn es zahlreiche Anpassungen gibt.

- Wählen Sie das Basissystem aus *approveresourcelimit*Regel und ändern Sie sie, um eine Richtlinienaktion einzubeziehen, die einen anwenderdefinierten Subflow oder eine Benachrichtigung auslöst.

  Hinweis: Standardmäßig ist für die Regel *approveresourcelimit* nur die ServiceNow-Genehmigungsaktion konfiguriert.

- Klicken Sie auf **Neu**, und konfigurieren Sie eine neue Richtlinienregel.

  Weitere Informationen finden Sie unter Cloud-Richtlinienregeln konfigurieren.

4. Konfigurieren Sie eine Richtlinien-Regelaktion.

- Wählen Sie in der zugehörigen Liste „Richtlinienregelaktionen“ die Aktion „Richtlinienregel genehmigen“ des Basissystems aus, um eine Benachrichtigung oder einen anwenderdefinierten Genehmigungs-Subflow einzubeziehen.
- Erstellen Sie eine Cloud-Richtlinienregelaktion in der zugehörigen Liste „Richtlinienregelaktionen“, um anwenderdefinierte Genehmigungs-Subflows oder Benachrichtigungen auszulösen, wenn Sie im vorherigen Schritt eine Richtlinienregel erstellt haben.

  Weitere Informationen finden Sie unter Erstellen Sie eine Aktion für die Richtlinie „bei Überschreitung des Ressourcenlimits“ .

  Hinweis: Vergewissern Sie sich, dass im Feld **Richtliniengruppe** die Richtliniengruppe ausgewählt ist, für die diese Richtlinie gelten soll.

5. Veröffentlichen Sie die Richtlinie, um Steuerungen für Ressourcenbestellungen zu aktivieren, indem Sie auf **Aktualisieren** und dann auf **Veröffentlichen** klicken.

Ergebnis

Basierend auf der Richtlinienregelaktion, die Sie für die Richtlinie zur Steuerung der Ressourcenbestellung konfiguriert haben, wird entweder eine E-Mail-Benachrichtigung oder ein Genehmigungs-Subflow oder beides ausgelöst, wenn die angegebene Quote überschritten wird.

Wenn Sie eine Genehmigungsrichtlinie konfiguriert haben, erhält die anfordernde Person eine Benachrichtigung, dass die Genehmigungsanforderung bei Überschreitung des festgelegten Kontingents an einen zuständigen Genehmiger gesendet wurde. In der Regel hat der zugewiesene Genehmiger die Vorlage angelegt, die zum Erstellen der Cloud-Ressource verwendet wird, und verfügt über die Rolle *sn_cmp.cloud_service_designer*.

Dashboard für Cloud-Vorgänge anzeigen

Das Dashboard für Cloud-Vorgänge schlüsselt Cloud-Serviceanforderungen Ihrer Endbenutzer und Cloud-Stapel auf, die Sie im Cloudbenutzerportal anbieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

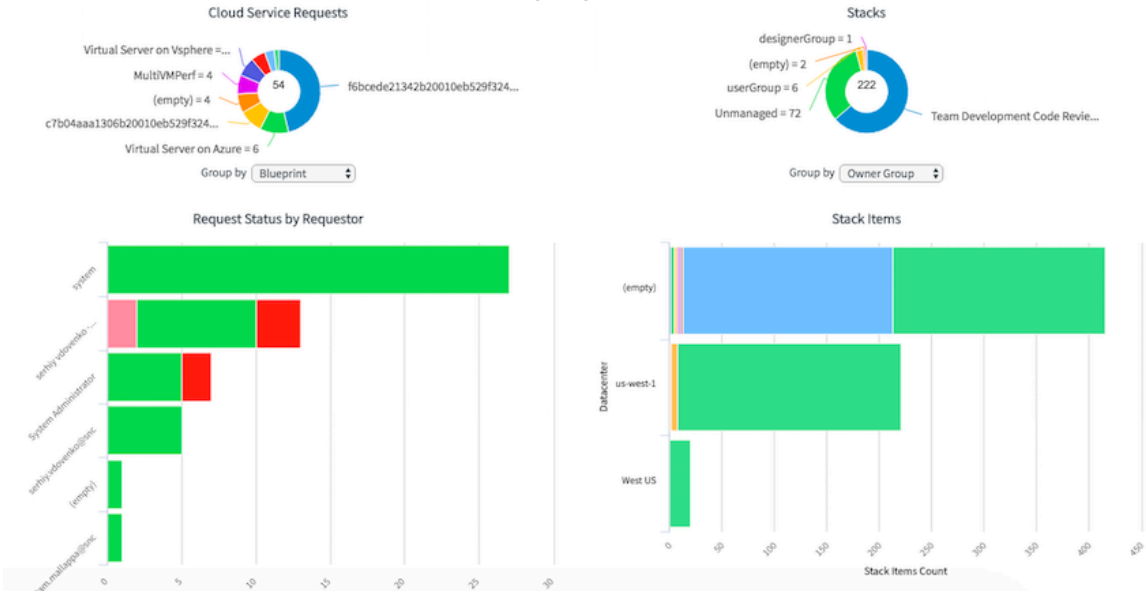
Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Betreiben** > **Dashboard für Cloud-Vorgänge**an.

   Das Dashboard für Cloud-Vorgänge wird mit Cloud-Serviceanforderungen und Stapeln angezeigt. Anforderungen werden im Balkendiagramm unten auch nach anfordernder Person aufgeschlüsselt. Stapel werden nach Rechenzentren aufgeschlüsselt.

Beispiel für das Dashboard für Cloud-Vorgänge



2. Führen Sie einen der folgenden Schritte aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen:

Ziel	Aktion
Daten nach einem anderen Attribut gruppiert anzeigen	Wählen Sie einen Wert in der Auswahlliste **Grup pieren nach** unter einem Diagramm aus.
Aktualisierte Daten anzeigen	Zeigen Sie auf eines der Diagramme, bis das Aktualisierungssymbol ( ) angezeigt wird, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol angezeigt wird ( ), und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

Berichte zur Cloud-Ursachenanalyse verwenden

Berichte zur Ursachenanalyse helfen Ihnen bei der Problembehandlung in Cloud Provisioning and Governance. Verwenden Sie die Berichte, um Details zum Cloud-Orchestrierungspfad und zum Cloud API-Pfad anzuzeigen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Betreiben** > **Ursachenanalyse-Dashboard**an.

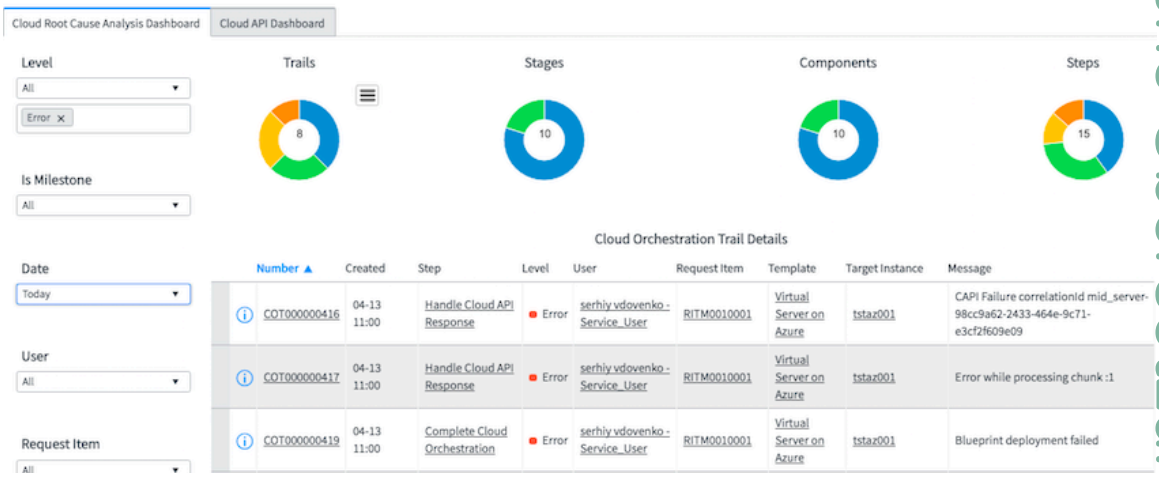
   Das Ursachenanalysedashboard wird standardmäßig mit dem **Cloud-Ursachenanalysedashboard** angezeigt. Dadurch erhalten Sie eine grafische Zusammenfassung des Cloud-Orchestrierungspfads mit Pfaddatensätzen unter den Berichten. In diesen Diagrammen sind Datensätze nach verschiedenen Attributen gruppiert:

   - **Pfade**: Gruppiert Daten nach der Vorlage, der Komponente, z. B. einem Ressourcenblock oder einer Blaupause, für die eine Cloud Provisioning and Governance-Aktion angewendet wurde.
   - **Phasen**: Gruppiert Daten nach der Phase, die angibt, wann die Transaktion stattgefunden hat.
   - **Komponenten**: Gruppiert Daten nach der Komponente im System, die an der Transaktion beteiligt war.
   - **Schritte**: Gruppiert Daten nach dem beschreibenden Schritt, der einer Phase und einer Komponente zugeordnet ist.

   Unter Cloud-Orchestrierungspfad finden Sie eine Liste der möglichen Schritte.

   Anforderungen werden im Balkendiagramm unten auch nach anfordernder Person aufgeschlüsselt. Stapel werden nach Rechenzentren aufgeschlüsselt.

   Cloud-Ursachenanalysedashboard

2. Wählen Sie eine Option aus, um die Tag-Daten abzurufen, die Sie für den Bericht benötigen.

Ziel	Aktion
Daten filtern	Wählen Sie eine der Optionen aus, z. B. **Ebene**, **Datum** oder **Anforderungselement**.
Aktualisierte Daten anzeigen	Zeigen Sie auf einen der Diagramme oben, bis das Aktualisierungssymbol ( ) Wird angezeigt, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol ( ) Wird angezeigt, und wählen Sie dann aus **Speichern Sie als PNG** Oder **Speichern Sie als JPEG** .

Automatische Übersetzung

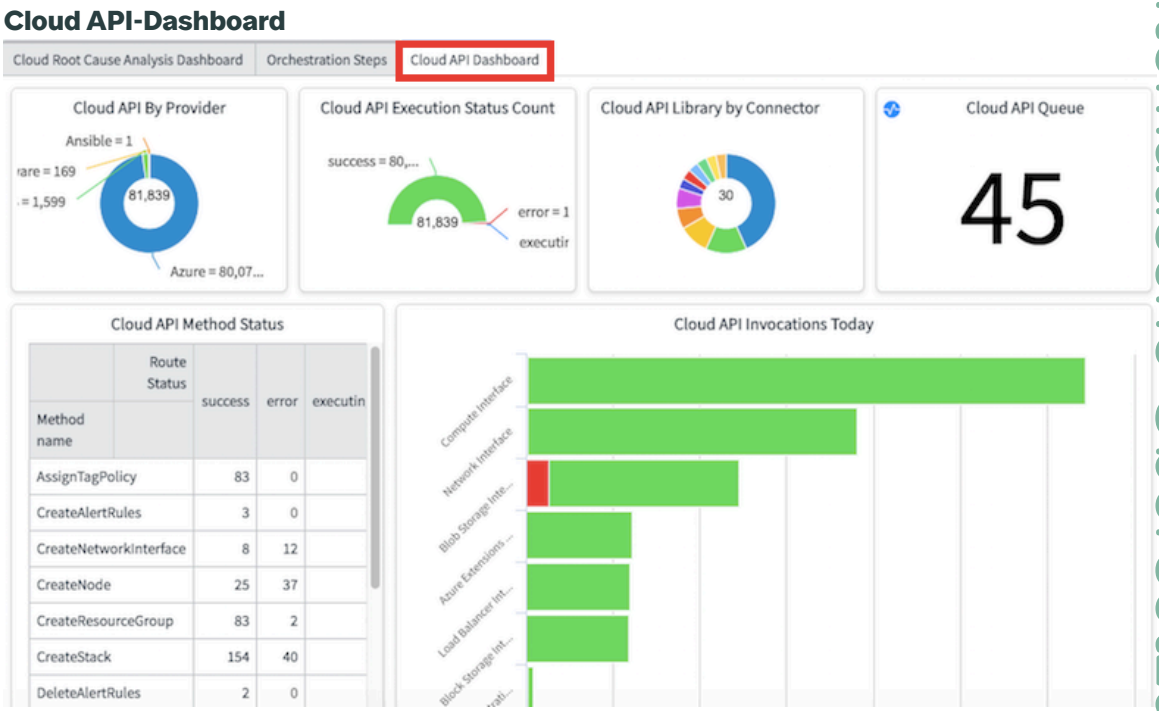
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die **Nummer** einer beliebigen Cloud-Orchestrierungs-API, um diesen bestimmten Datensatz anzuzeigen.
   Siehe Cloud-Orchestrierungspfad für Feldbeschreibungen.
4. Zum Anzeigen von Berichten zum Cloud API-Pfad klicken Sie auf die Registerkarte **Cloud API-Dashboard**.

   Dieses Dashboard zeigt Ihnen mehrere Berichte für den Cloud API-Pfad, gruppiert nach Provider, Status und Connectors. Sie können auch Informationen zu den Methoden und APIs sehen, die heute aufgerufen wurden.

   Hinweis:

   Beginnend mit Zurich Das Cloud-API-Dashboard wird ausgeblendet und in neuen Instanzen nicht mehr aktiviert, wird jedoch weiterhin unterstützt. Die Anwendung „Cloud-Servicekatalog“ bietet diese Funktionalität jetzt. Die Anwendung wird auf die zukünftige Einstellung vorbereitet.



5. Klicken Sie auf beliebige Daten in den Diagrammen, um die jeweiligen Datensätze des Cloud API-Pfads zu öffnen.
   Unter Cloud API-Pfad finden Sie Beschreibungen der Formularfelder des Cloud API-Pfads.

Cloud API-Pfad

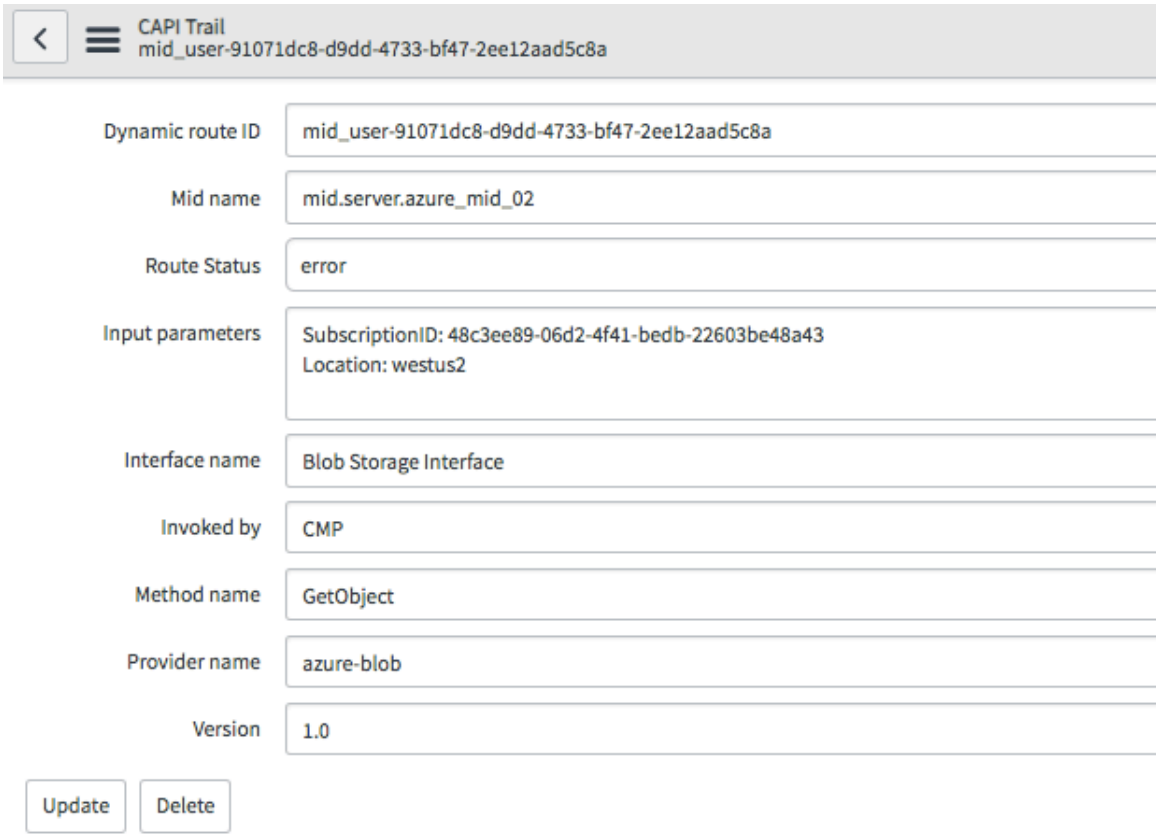
Der Cloud API-Pfad ist ein Aktivitätsprotokoll für alle Aktivitäten, die die Cloud API verwenden und den MID-Server durchlaufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhalte des Cloud API-Pfads

CAPI-Pfadformular



Feld	Beschreibung
ID der dynamischen Route	Eine automatisch generierte ID-Nummer für den Eintrag.
MID-Name	Der Name des MID-Server s, über den die Discovery ausgeführt wurde.
Routenstatus	Gibt an, ob der von der API ausgeführte Discovery-Vorgang erfolgreich war. Mögliche Werte sind: • **Erfolg** • **Fehler** • **Wird ausgeführt**
Eingabeparameter	Der Eingabeparameter, von dem der API-Pfad-Datensatz generiert wurde. Dieser Wert ist normalerweise das Rechenzentrum, in dem Discovery ausgeführt wurde.
Schnittstellenname	
Aufgerufen durch	Dieser Wert ist immer **CMP**, wenn Discovery ausgeführt wird.
Methodenname	Der Schnittstellenvorgang von der Cloud-API, von der dieser Datensatz verarbeitet wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Providername	Der Cloud Provider
Version	Die in der Cloud-API angegebene Version

CAPI-Pfadprotokolle

Die zugehörige Liste „CAPI-Pfadprotokolle“ enthält weitere Details zum Eintrag des Cloud API-Pfads. Die folgenden Protokollschlüsseltypen sind verfügbar:

Protokollschlüssel	Beschreibung
route_data	Informationen zu den Cloud-API-Aufrufen
dynamic_route	Informationen über die tatsächliche Route, über die die Daten geflossen sind, einschließlich URIs.
route_result	Die von der Instanz empfangene Nutzlast oder eine Beschreibung des Ergebnisses der Datenübertragung. Die Nutzlast
chunk_number	Die Anzahl der Datenblöcke, die die Instanz empfangen hat
route_status	Gibt an, ob die Routenverbindung und die Übertragung der Nutzlast erfolgreich war
route_error	Der aufgetretene Fehler. Zum Beispiel der Fehler `Failed to list loadbalancer Failed: HTTP-Fehlercode: 403` (Auflistung des Lastenausgleichsmoduls fehlgeschlagen: HTTP-Fehlercode: 403) bedeutet, dass Ihre Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte.
error_detail	Weitere Details über den Fehler, einschließlich der Cloud Provisioning and Governance-API und des entsprechenden Connectors, der beim Discovery-Versuch verwendet wurde, und die Fehler, die der Cloud Provider ausgegeben hat.

Beispiel für einen „route_error“:

```
Failed to list loadbalancer Failed : HTTP error code : 403
```

Beispiel für den Eintrag „error_detail“ für denselben Fehler:

```
com.snc.cmp.connector.cloud.loadbalancer.component.LoadBalancerException: Failed to list
 loadbalancer Failed : HTTP error code : 403
      at
 com.snc.cmp.connector.cloud.loadbalancer.customizer.impl.AWSLoadBalancerCustomizer.listL
oadBalancers(AWSLoadBalancerCustomizer.java:56)
 at
 com.snc.cmp.connector.cloud.loadbalancer.component.LoadBalancerProducer.process(LoadBa
lancerProducer.java:46)
 at
 org.apache.camel.util.AsyncProcessorConverterHelper$ProcessorToAsyncProcessorBridge.pro
cess(AsyncProcessorConverterHelper.java:61)
      at org.apache.camel.processor.SendProcessor.process(SendProcessor.java:145)
      ...
```

In diesen beiden Einträgen wird angegeben, dass die Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte. Die Schnittstelle des Lastenausgleichsmoduls gibt den ersten Fehler aus, da das Lastenausgleichsmodul das erste Gerät ist, das Zugriff auf die Cloud-Ressource ermöglicht. Die Fehler `org.apache.camel` weisen auf Weiterleitungsfehler aufseiten von Amazon Web Services hin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der entsprechende Fehler auf der Instanzseite wird im Cloud-Orchestrierungspfad erfasst.

Zugehörige Informationen

Cloud-Orchestrierungspfad

Cloud API-Pfad öffnen

Öffnen Sie den Cloud API-Pfad, um Probleme wie fehlgeschlagene Richtlinien oder fehlgeschlagene Discovery von Cloud-Ressourcen zu debuggen und zu beheben.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Betreiben** > **Pfade**an.
2. Auf der Registerkarte **Cloud API-Pfad** filtern und sortieren Sie die Liste der Datensätze aus dem Cloud API-Pfad nach Bedarf.
   Wenn Sie z. B. nach einer fehlgeschlagenen Discovery suchen, filtern Sie die Liste, sodass in der Spalte **Routenstatus** nur Einträge mit **Fehler** anzeigt werden.
3. Klicken Sie auf einen Link in der Spalte „Erstellt“, um den Datensatz des Cloud API-Pfads zu öffnen.
4. Öffnen Sie in der zugehörigen Liste „CAPI-Pfadprotokolle“ den Protokolldatensatz, der die gewünschten Informationen anzeigt.
   Öffnen Sie beispielsweise **route_error** oder **error_detail**, um einen fehlgeschlagenen Vorgang zu debuggen.

Dashboards und Berichte von Cloud Provisioning and Governance

Mit Dashboards können Cloud-Administratoren und Cloud-Benutzer Berichte wie Cloud-Abrechnungsdaten und Cloud Tag-Nutzung anzeigen lassen.

Zeigt Setup-Optionen für die Abrechnung für Cloud Provisioning and Governance. Folgen Sie diesem kurzen Video, um mehr über zu erfahren Cloud Provisioning and Governance Dashboards.

Wichtig: Ab Release Zurich ist das Abrechnungs-Dashboard nicht mehr verfügbar, wenn Sie die App ServiceNow Store Cloud-Einblicke heruntergeladen haben. Folgendes ändert sich

- Sie werden standardmäßig zur Homepage von Cloud-Einblicke weitergeleitet.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Im Widget „Aktuelle Monatsausgaben“ und im Widget „Budget“ des Cloud-Benutzerportals werden keine Daten angezeigt, wenn Cloud-Einblicke in der Instanz aktiviert ist.

Cloud-Kosten auf dem Abrechnungsdashboard anzeigen

Das Abrechnungsdashboard bietet eine umfassende Informationsübersicht zur Cloud-Nutzung und zu Kostentrends sowie Kosten-Zusammenfassungen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Wichtig: Auf das **Abrechnungsdashboard** können Sie nur zugreifen, wenn Sie die App ServiceNow Store Cloud-Einblicke nicht heruntergeladen und aktiviert haben. Wenn Sie die App Cloud-Einblicke aktiviert haben, können Sie nur zum Abrechnungsdashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

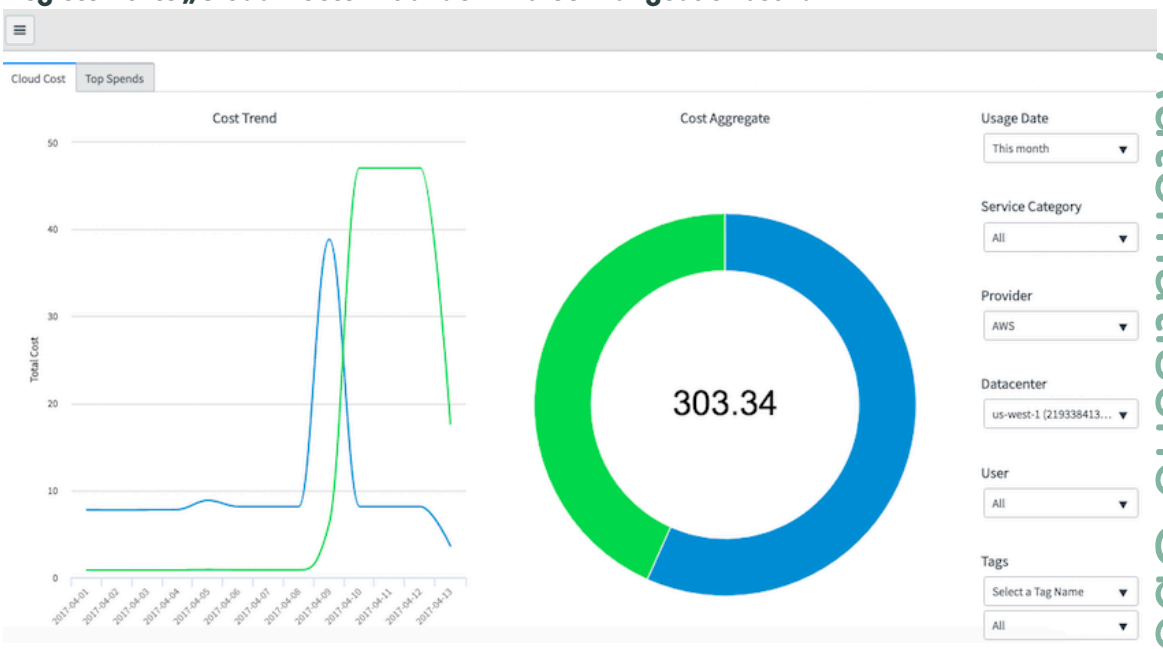
Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Analysieren** > **Abrechnung** > **Abrechungsdashboard**an.

   Das Abrechnungsdashboard zeigt standardmäßig die Registerkarte **Cloud-Kosten** an. Auf dieser Registerkarte werden die folgenden zwei Diagramme angezeigt:

   - **Kostentrend**: Ein Liniendiagramm, in dem die täglichen Kosten für das ausgewählte **Nutzungsdatum** dargestellt werden.
   - **Gesamtkosten**: Gesamtkosten für jeden Tag-Wert für das ausgewählte Tag **Gruppieren nach**.

   Registerkarte „Cloud-Kosten“ auf dem Abrechnungsdashboard

2. Führen Sie eine der folgenden Aktionen aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen.

Ziel	Aktion
Aktualisieren Sie den Abrechnungszeitraum	Wählen Sie eine neue Option aus der Auswahlliste Verwendungsdaten.
Siehe Daten, die nach einem anderen Tag gruppiert sind	Wählen Sie einen Wert in der Auswahlliste **Gruppieren nach** unter jedem Diagramm.
Nach Tag-Werten filtern	Wählen Sie in der Liste einen Tag-Wert aus.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Ringdiagramme, bis das Optionssymbol ( ) angezeigt wird, und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

3. Um die Bereiche mit der höchsten Ausgabenstufe anzuzeigen, klicken Sie auf die Registerkarte **Höchste Ausgaben**.
   Balkendiagramme zeigen standardmäßig die Gesamtkosten für jedes Tag an. Sie können die Daten weiter nach **Servicekategorie**, **Provider** und **Rechenzentrum** filtern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf einen beliebigen Teil der Diagramme, um Kostendatensätze für die ausgewählten Kriterien anzuzeigen.
   Die Listenansicht der Kostendatensätze wird angezeigt. Sie können Informationen wie die Nutzungsmenge und spezifische Kosten pro Nutzungsdatum anzeigen.

Beispiel für Kostendatensätze

Usage date	Service Category	Resource	Usage profile	Usage quantity	Cost
2017-04-08	Compute	flow-vm	Data Transfer ($0 / GB)	0.020323	0
2017-04-08	Compute	flow-vm	Data Transfer ($0.08199078 / GB)	0.02444	0.00200385
2017-04-08	Compute	flow-vm	Hourly ($0.06172149 / Hour)	24	1.48131575

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

Das Tag-Dashboard zeigt alle getaggten Ressourcen an. Verwenden Sie das Tag-Dashboard, um bestimmte Tag-Werte für eine Gruppe von Ressourcen wie Stapel oder virtuelle Computer anzuzeigen.

Vorbereitungen

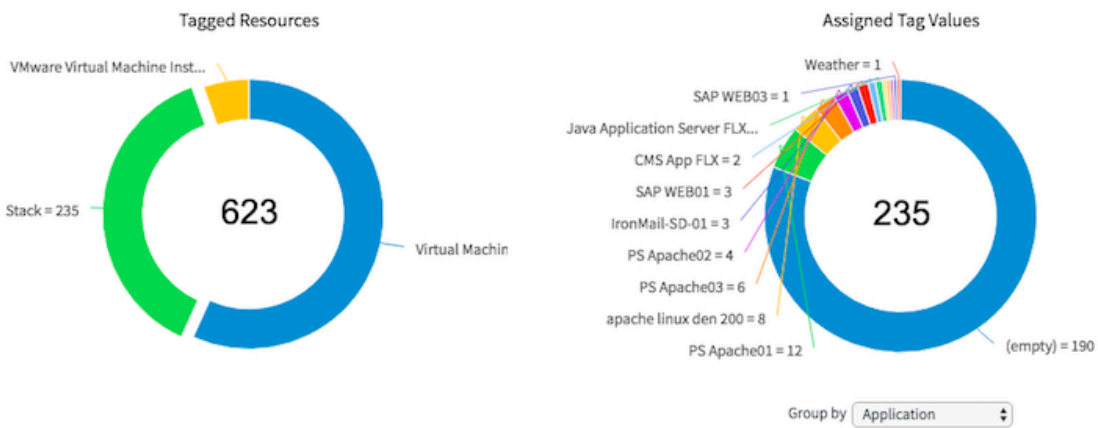
Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Analysieren** > **Tag**an.

   Die Registerkarte **Tag-Dashboard** zeigt das Tag-Dashboard an, auf dem alle mit Tags gekennzeichneten Ressourcen nach Tags aufgeschlüsselt sind.

Tag-Dashboard



2. Führen Sie eine der folgenden Aktionen aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen.

Ziel	Aktion
Tag-Werte für eine bestimmte Ressourcengruppe ansehen	Klicken Sie auf einen Abschnitt des Ringdiagramms **Getaggte Ressourcen**.
Siehe Daten, die nach einem anderen Tag gruppiert sind	Wählen Sie einen Wert in der Auswahlliste **Gruppieren nach** unter dem Ringdiagramm **Zugewiesene Tag-Werte** aus.

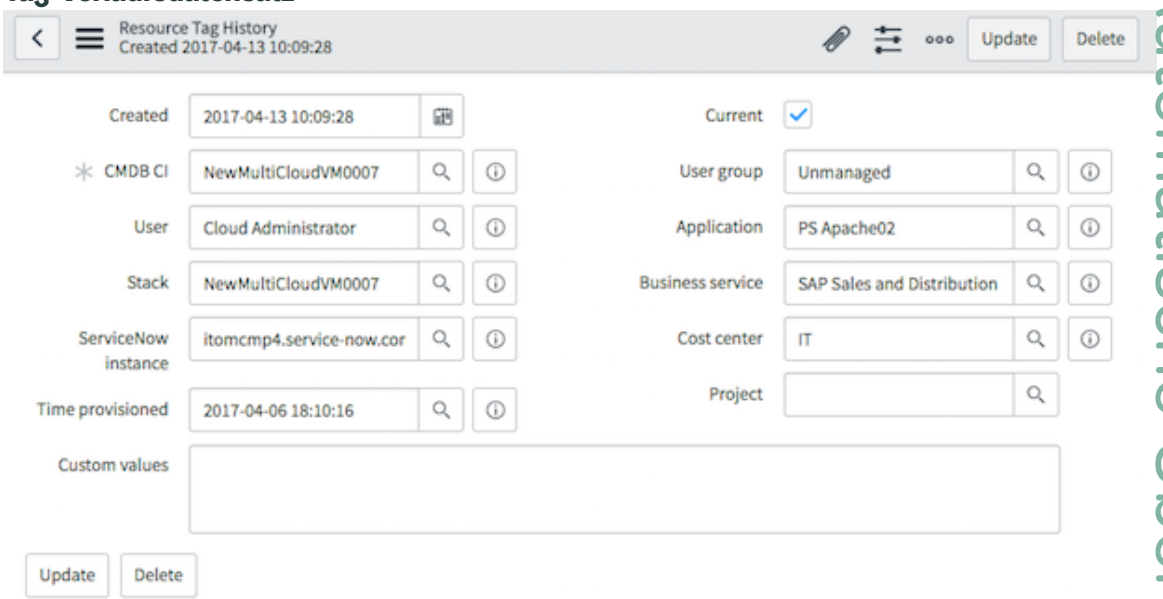
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ziel	Aktion
Aktualisierte Daten anzeigen	Zeigen Sie auf eines der Diagramme, bis das Aktualisierungssymbol ( ) angezeigt wird, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol ( ) angezeigt wird, und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

3. Klicken Sie zum Anzeigen eines bestimmten Tag-Verlaufsdatensatzes auf einen beliebigen Abschnitt im Diagramm **Zugewiesene Tag-Werte**.
Eine Liste mit Tag-Verläufen wird angezeigt, die der CI-Klasse für den ausgewählten Tag-Wert entsprechen.

Tag-Verlaufsdatensatz



Feld	Beschreibung
Erstellt	Das Datum, an dem der Tag-Verlauf erstellt wurde.
Aktuell	Wenn ausgewählt, gibt dies an, ob der aktuelle Datensatz der aktuellste Datensatz ist.
CMDB CI	Das tatsächliche CI in der CMDB. Klicken Sie auf das Datensatzsymbol, um das CI-Formular anzuzeigen.
Benutzergruppe	Das diesem CI zugeordnete Gruppen-Tag.
Anwender	Das diesem CI zugeordnete Benutzer-Tag.
Applikation	Das diesem CI zugeordnete Anwendungs-Tag.
Stapel	Das diesem CI zugeordnete Stapel-Tag.
Business Service	Das diesem CI zugeordnete Business Service-Tag.
ServiceNow instance	Das diesem CI zugeordnete Instanz-Tag.
Kostenstelle	Das diesem CI zugeordnete Kostenstellen-Tag.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeit der Bereitstellung	Das Datum, an dem der Computer bereitgestellt wurde.
Projekt	Das diesem CI zugeordnete Projekt-Tag.
Benutzerdefinierte Werte	Alle diesem CI zugeordneten benutzerdefinierten Werte.

Budgetbasierte Benachrichtigung und Genehmigung

Administratoren können ein Budget für eine Gruppe und einen Benutzer innerhalb der Gruppe zuweisen. Wenn der Benutzer oder die Gruppe den Schwellenwert für das Budgetlimit erreicht, werden sie darüber benachrichtigt.

Wichtig:

- Die budgetbasierte Benachrichtigungs- und Genehmigungsfunktion ist nicht mehr verfügbar, wenn Sie für die Cloud-Abrechnung die App Cloud-Einblicke verwenden.
- Sie können die Funktion „Budgetverbrauch“ nur weiterhin verwenden, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden oder wenn Sie die native Abrechnungsfunktion von Cloud Provisioning and Governance erneut aktiviert haben.

Administratoren können ein wöchentliches, monatliches, vierteljährliches oder jährliches Budget (in USD) zuweisen. Das für einen Benutzer und das für eine Gruppe festgelegte Budget sind voneinander unabhängig. Beispielsweise kann eine Gruppe mit fünf Benutzern ein Budget von 100 USD haben, und jedem Benutzer in dieser Gruppe kann ein Limit von 25 USD zugewiesen werden. Eine Organisation entscheidet über die Budgetfrequenz, und alle Gruppen in dieser Organisation folgen derselben Frequenz. Wenn sich eine Organisation beispielsweise für ein monatliches Budget entscheidet, folgen alle Gruppen und Benutzer in dieser Organisation einem monatlichen Budget. Weitere Informationen finden Sie unter Budgets konfigurieren.

Für jede neue Gruppe und jeden neuen Benutzer wird ein Standardbudget angegeben. Eine neue Gruppe erhält ein Standardbudget von 1000 USD, ein neuer Benutzer ein Standardbudget von 100 USD.

Administratoren können das Budget jederzeit erhöhen oder verringern. Wenn der Benutzer oder die Gruppe den Schwellenwert des Budgets erreicht, erfolgt eine Benachrichtigung. Benachrichtigungen werden als Teil des Abrechnungsprozesses ausgelöst. Die Discovery für die Abrechnung wird für jeden Benutzer und jede Gruppe geplant. Am Ende der Abrechnungs-Discovery wird ein Vergleich zwischen dem Budgetlimit und den tatsächlichen Kosten durchgeführt. Wenn der Schwellenwert erreicht oder überschritten wurde, werden Benachrichtigungen ausgelöst.

Administratoren können eine Richtlinie einrichten. Wenn die Budgetgrenze dann einen bestimmten Schwellenwert erreicht oder überschreitet, erteilt der Administrator eine Genehmigung für den Benutzer oder die Gruppe, die Ressourcen weiterhin zu verwenden. Beispielsweise kann der Administrator eine Richtlinie für eine Gruppe erstellen, bei der beim Erreichen von 90 % des Budgetschwellenwerts der Gruppe eine Genehmigung erforderlich ist, damit die Gruppe weiterhin Ressourcen verbrauchen kann. Wenn der Administrator keine Richtlinie für das Budget erstellt, kann der Benutzer oder die Gruppe die Ressourcen weiterhin verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Budgetdetails in unter anzeigen **Analysieren** > **Budgetverbrauch**an. Sie können sich die Details zum Budgetverbrauch für einen Benutzer oder auch für eine Gruppe ansehen.

Budgets konfigurieren

Sie können Budgets für Gruppen und für Benutzer in dieser Gruppe konfigurieren. Sie können einen Budgetzeitraum für die Gruppe einrichten und einer Gruppe und jedem Benutzer in dieser Gruppe ein Budgetlimit zuweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Bedingungen** > **Budget**an.
2. Klicken Sie neben **Budgetkonfiguration** auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Gruppenname	Wählen Sie in der Liste eine Gruppe aus.
Budgetzeitraum	Wählen Sie einen Budgetzeitraum für die Gruppe aus: wöchentlich, monatlich, vierteljährlich oder jährlich.
Obergrenze für Gruppe	Geben Sie ein Budgetlimit für die Gruppe ein. Standardmäßig liegt das Budgetlimit für jede neue Gruppe bei 1000 USD.
Grenzwert pro Benutzer	Geben Sie ein Budgetlimit für jeden Benutzer in der Gruppe ein. Standardmäßig liegt das Budgetlimit für jeden neuen Benutzer bei 100 USD.

4. Klicken Sie auf **Absenden**.

Tags für Cloud-Ressourcen

Mithilfe von Tags werden Cloud-Ressourcen kategorisiert, um umfangreichere und detailliertere Nachverfolgungs- und Abrechnungsberichtsdaten bereitzustellen.

Erstellen Sie Tags, damit Cloud Provisioning and Governance Cloud-Ressourcen nach der Bereitstellung automatisch kategorisieren kann. Jedes Tag verknüpft ein bestimmtes Schlüssel:Wert-Paar mit einer angeforderten Cloud-Ressource, z. B. Anwendung=HRMS.

Nach der Bereitstellung der Cloud-Ressource werden die Schlüssel:Wert-Informationen in Tags Teil der Metadaten der Ressource und zusammen mit allen anderen Parametern der Ressource gespeichert. Da eine Cloud-Ressource mehrere Tags haben kann, können Sie Kostenelemente aus mehreren Perspektiven betrachten.

Tag-Definitionen

Tag-Definitionen sind Datensätze, die einen Tag-Namen einem Werttyp zuordnen. Folgende Werttypen sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Werttyp	Beschreibung
Variable	Ein Wert, den der Benutzer eingibt oder aus einer Auswahlliste auswählt. Dieser Wert wird als Servicekatalogvariable gespeichert. Wenn eine Tabelle einem Variablen-Tag zugeordnet ist, werden die Werte in dem als **Anzeigefeld** markierten Feld dem Benutzer angezeigt, wenn er die Instanz anfordert. In den meisten Fällen ist dies das Feld „Name“. Beispielsweise werden dem Benutzer die Namen der Business Services in der Tabelle „Service“ angezeigt. Wenn in der Tag-Definition keine Tabelle angegeben ist, wird dem Benutzer ein Textfeld angezeigt.
Skript	Ein Skript, das einen Wert von der Instanz abruft, z. B. die aktuelle Zeit auf der Instanz. Das Skript muss den Wert über die Basissystem-API abrufen und den Wert an die Antwortvariable zurückgeben. Beispiel: Das Skript zum Abrufen der aktuellen Zeit auf der Instanz lautet: `answer = new GlideDateTime().getValue();`

Standard-Tags

Diese Tags werden standardmäßig bereitgestellt.

Wichtig: Deaktivieren Sie nicht die Standard-Tags, da diese Aktion alle entsprechenden Katalogelementvariablen löscht.

Standard-Cloud-Tags

Bezeichnung	Name	Werttyp	Tabelle mit Auswahloptionen
Applikation	Anwendung	Variable	Anwendung [cmdb_ci_appl]
Business Service	business_service	Variable	Service [cmdb_ci_service]
Kostenstelle	cost_center	Variable	Kostenstelle [cmn_cost_center]
Projekt	Projekt	Variable	N/V
ServiceNow instance	sn_instance	Skript	N/V
Stapel	stack	Variable	Stapel [sn_cmp_stack]
Zeit der Bereitstellung	time_provisioned	Skript	N/V
Anwender	user	Auftragsfeld	Benutzer [sys_user]
Benutzergruppe	user_group	Variable	Gruppe [sys_user_group]

Cloud-Administratoren können auch benutzerdefinierte Tags erstellen, die den spezifischen Anforderungen des Unternehmens entsprechen. Beispielsweise können Sie ein Standort-Tag erstellen, um den Standort der Ressource nachzuverfolgen.

AWS-Tags

Für Ressourcen in Amazon Web Services (AWS) generierte Tags werden an AWS gesendet und sind auch über die AWS-Konsole verfügbar.

Zugehörige Informationen

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefiniertes Tag für Cloud-Ressourcen erstellen

Cloud-Administratoren können zur Kategorisierung von Cloud-Ressourcen zusätzlich zu den Standard-Tags benutzerdefinierte Tags erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Ressource vor dem Vorhandensein eines bestimmten Tags bereitgestellt wurde, muss dieses Tag dem Datensatz für diese Ressource manuell hinzugefügt werden.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Analysieren** > **Tag** > **Tag-Verwaltung** > **Tag-Definitionen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Bezeichnung	Name, der Cloud-Benutzern auf dem Bildschirm angezeigt werden soll.
Name	Name des Schlüssels. Der Name wird in allen Tabellen zusammen mit dem Wert gespeichert.
Werttyp	Der Typ des Werts für dieses Tag.
Variablenname	Der Name der Variable. Diese Option wird angezeigt, wenn Sie **Variable** als Werttyp auswählen.
Tabelle [optional]	Die Tabelle, die die Auswahlmöglichkeiten für das Werttypfeld **Variable** enthält. Wählen Sie eine Tabelle aus dem System aus. Wenn Sie keine Tabelle auswählen, wird Cloud-Benutzern ein leeres Textfeld für die Variable angezeigt.
Sortierfeld	Das Feld auf dem Anforderungsformular. Klicken Sie neben **Zum Auswählen klicken** auf den Abwärtspfeil, und wählen Sie dann das Feld aus der Tabelle „Aufträge“ [sn_cmp_order] aus.
Aktiv	Ein Indikator, der angibt, ob das Tag verwendet wird. Wählen Sie diese Option aus, um das Tag auf alle neuen Anforderungen anzuwenden.

Zugehörige Informationen

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

Abrechnungsdaten mithilfe von benutzerdefinierten Tags aus bereitgestellten Ressourcen gruppieren

Konfigurieren Sie benutzerdefinierte Tags zum Anzeigen und Analysieren von Abrechnungsdaten mithilfe von benutzerdefinierten Tags, die in bereitgestellten Ressourcen vorhanden sind.

Vorbereitungen

- Führen Sie eine Cloud Discovery in Cloud Provisioning and Governance für bereitgestellte Ressourcen durch.
- Führen Sie einen Abrechnungs-Download-Auftrag für das zugeordnete Servicekonto aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Rolle „Beitragender bei Ressourcenrichtlinien“ im Azure-Servicekonto und sn_cmp.cloud_admin in der Instanz.

Warum und wann dieser Vorgang ausgeführt wird

Bereitgestellte Ressourcen mit vorhandenen Tags werden als Teil der Cloud Discovery erkannt. Vorhandene Tags werden in der Tag-Verwaltung als benutzerdefinierte Tags betrachtet. Standardmäßig werden die importierten (benutzerdefinierten) Tags nicht im Abrechnungsdashboard angezeigt, sodass Sie keine Abrechnungsdaten mithilfe importierter (benutzerdefinierter) Tags filtern und analysieren können.

Wichtig: Ab dem Release Rome werden die Abrechnungs- und Budgetierungsfunktionen nicht mehr unterstützt, wenn Cloud Provisioning and Governance in einer nicht domänengetrennten Instanz ausgeführt wird. Wenn Sie Cloud Provisioning and Governance jedoch in einer domänengetrennten Instanz verwenden, ändert sich die Funktionalität für Abrechnungs- und Budgetierungsfunktionen nicht.

Prozedur

1. In **Cloud-Administratorportal** , Navigieren Sie zu **Analysieren** > **Tag** > **Tag-Verwaltung**an.

   Die Liste **Tag-Definitionen** zeigt erkannte Ressourcen an, die mit vorhandenen Tags versehen sind, die als „Benutzerdefiniert“ gekennzeichnet sind.

2. Öffnen Sie einen Tag-Datensatz vom Typ **Benutzerdefiniert**.
3. Ändern Sie im Formular „Tag-Definition“ das Tag von „Benutzerdefiniert“ in „ServiceNow (Benutzerdefiniert)“:
   a. Wählen Sie im Feld **Tag-Typ** die Option **ServiceNow (Benutzerdefiniert)** aus.
   b. Kopieren Sie den Wert aus dem Feld **Bezeichnung** in das Feld **Variable**.
   c. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Sichtbar**.
   d. Wählen Sie **Aktualisieren**.
4. Wiederholen Sie die Schritte 2 und 3 für alle benutzerdefinierten Tags, die Sie im Abrechnungsdashboard aktivieren möchten.
5. Führen Sie Cloud Discovery erneut aus, um aktualisierte Tags des Typs „ServiceNow (Benutzerdefiniert)“ anzuzeigen.

   Weitere Informationen finden Sie unter Cloud-Discovery .

6. Führen Sie den Abrechnungszeitplan aus.
   a. In **Cloud-Administratorportal** , Navigieren Sie zu **Analysieren** > **Abrechnung** > **Abrechnungszeitplan**an.
   b. Erstellen Sie einen Zeitplan, oder öffnen Sie einen vorhandenen Zeitplan.
   c. Wählen Sie **Jetzt ausführen**.
   d. Wählen Sie im Fenster **Abrechnungsdaten abrufen** einen Datumsbereich aus, und klicken Sie dann auf **Herunterladen**.

   Die Tags vom Typ ServiceNow (Benutzerdefiniert) werden jetzt im Feld „Tags“ des Abrechnungsdashboards angezeigt.

Nächste Maßnahme

Lassen Sie Cloud-Kosten auf dem Abrechnungsdashboard anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lebenszyklusvorgänge für erkannte Ressourcen konfigurieren und durchführen

Konfigurieren Sie Lebenszyklusvorgänge für Cloud-Ressourcen, die nicht mit ServiceNow® Cloud Provisioning and Governance bereitgestellt wurden. Stellen Sie Ressourcen bereit, und ändern Sie Ressourcenblockvorgänge, um Tag-2-Vorgänge für Cloud-Ressourcen auszuführen, die mit Cloud-Discovery erkannt, aber nicht mit Cloud Provisioning and Governance bereitgestellt wurden.

Vorbereitungen

- Weisen Sie das Configuration Item (CI) einem Benutzer zu, der den Vorgang ausführt.
- Erforderliche Rolle: sn_cmp.cloud_service_user, root_admin, admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Ressource aus dem Cloud Provisioning and Governance-Katalog bereitgestellt wird, können Sie Basissystem-Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen. Wenn jedoch eine Ressource als Teil von Cloud-Discovery erkannt und nicht von Cloud Provisioning and Governance bereitgestellt wurde, sind die gleichen Vorgänge (Starten, Stoppen, Bereitstellung aufheben) nicht standardmäßig verfügbar. Das folgende Verfahren gilt für einen Vorgang „Stoppen“ auf einem virtuellen Computer, der nicht von Cloud Provisioning and Governance bereitgestellt wurde.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Entwurf** > **Ressourcenblöcke**an.
2. Suchen und öffnen Sie die Ressource/das CI, für die/das Sie Lebenszyklusvorgänge ausführen möchten.
3. Stellen Sie den Umschalter auf **Entwurf**, um den Ressourcenblock bearbeitbar zu machen.
4. In ausgewählt **Ressourcenblock** > **Vorgänge** Wählen Sie die erforderliche Registerkarte aus **Schnittstelle** Und **Vorgang** Aus ihren jeweiligen Listen.

   Hinweis: Die Felder **Schnittstelle** und **Vorgänge** sind nur für Ressourcen verfügbar, die erkannt, aber nicht dem Katalog hinzugefügt oder darin generiert wurden.

5. Klicken Sie auf das Symbol **Vorgang überschreiben**.
6. Geben Sie im Dialogfeld **Vorgang überschreiben** einen Namen für den Schnittstellenvorgang ein. Das Kontrollkästchen **Neu erstellen** ist standardmäßig aktiviert.
7. Klicken Sie auf **Absenden**.
   Sie haben den ausgewählten Vorgang für die von Ihnen erstellte Schnittstelle aktiviert.
8. Klicken Sie auf dem Formular **Eingabeparameter** auf das Symbol **Eingabeparameter hinzufügen**.
9. Geben Sie für den Parameter **Name** den Wert `resourceID` ein, und klicken Sie auf **Speichern**.
   Standardmäßig wird ein vom System zugewiesener Ausdruck generiert und im Feld **Zuordnung** angezeigt.
10. Ersetzen Sie für den Parameter `ServerID` den Standardausdruck im Feld **Zuordnung** durch `${parameter.resourceId}`, und klicken Sie auf **Speichern**.
11. Navigieren zu **Vorgänge** > **Schritte** Unterregisterkarte.
12. Ändern Sie auf dem Formular **Eingabe** den Wert des Parameters `NodeId` in `${parameter.resourceId}`.
13. Navigieren Sie zurück zum Formular **Eingabeparameter**, und klicken Sie auf **Katalog generieren**.
14. Stellen Sie den Umschalter auf **Veröffentlicht**, um den Ressourcenblock erneut zu veröffentlichen.
    Sie haben den Ressourcenvorgang für diese Ressource/dieses CI konfiguriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. **Wahlweise:** Navigieren zu **Cloud-Anwenderportal** > **Ressourcen** > **VM-Instanz**, Und wählen Sie die VM-Instanz aus, für die Sie den Ressourcenvorgang erstellt haben.
16. **Wahlweise:** Wählen Sie den neuen Schnittstellenvorgang, den Sie erstellt haben, aus der Liste **Ressourcenvorgänge auswählen** aus.

Nächste Maßnahme

Navigieren Sie zu **Cloud-Anwenderportal** > **Ressourcen** > **VM-Instanz** Und wählen Sie den neuen Schnittstellenvorgang aus, den Sie aus erstellt haben **Wählen Sie Ressourcenvorgänge Aus** Liste.

Musterbasierte gezielte Erkennung

Erkennen Sie automatisch neu bereitgestellte Cloud-Ressourcen und speichern Sie ihre Informationen mithilfe der musterbasierten gezielten Erkennung in der ServiceNow® ServiceNow® Configuration Management Database (CMDB).

Nachdem die Cloud die in der Ressourcenvorlage genannten Ressourcen bereitgestellt hat, z. B. Azure Resource Manager (ARM) oder CloudFormation Template (CFT), sendet sie eine Antwort an die Anwendung Cloud Provisioning and Governance. Die Antwort enthält Informationen zu den bereitgestellten Ressourcen. Cloud Provisioning and Governance verwendet diese Informationen, um eine Erkennung (gezielte Erkennung) zu starten und so nur die neu bereitgestellten oder geänderten Ressourcen zu erkennen und ihre Attribute in der entsprechenden CI-Klasse in der CMDB zu aktualisieren.

Die musterbasierte gezielte Erkennung bietet eine einfachere Alternative zum vorhandenen CAPI-basierten Ansatz. Cloud Provisioning and Governance verwendet Muster zur Erkennung einzelner Ressourcen, um nur die neu bereitgestellten oder geänderten Ressourcen zu erkennen. Im Gegensatz zu den anderen Mustern durchsucht das Einzelressourcen-Erkennungsmuster nicht die gesamte Cloud-Landschaft nach Änderungen. Es erkennt nur die neu bereitgestellten oder geänderten Ressourcen eines bestimmten Typs.

Die Tabelle „Cloud-Ressourcentypen“ [sn_capi_resource_type] speichert die 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster, das zum Erkennen der Ressource verwendet wird. Cloud Provisioning and Governance verwendet die Tabelle sn_capi_resource_type, um das entsprechende Muster für den angegebenen Ressourcentyp zu identifizieren. Weitere Informationen zu Mustern finden Sie unter Von ITOM-Sichtbarkeit verwendete Discovery-Muster .

Im Basissystem unterstützt Cloud Provisioning and Governance die musterbasierte gezielte Erkennung für eine Vielzahl von Ressourcentypen. Bei Bedarf können Sie benutzerdefinierte Muster verwenden, die Sie für die gezielte Erkennung erstellt haben. Weitere Informationen finden Sie unter Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen.

Cloud Provisioning and Governance überprüft die folgenden Bedingungen, um die musterbasierte gezielte Erkennung aufzurufen:

- Die CAPI-basierte gezielte Erkennung ist für den Ressourcentyp nicht implementiert.
- Die Systemeigenschaft *sn_cmp.targeted.disco.patterns* ist auf **True** festgelegt.
- Die Tabelle sn_capi_resource_type enthält eine 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster.

Wenn Sie beispielsweise CFT zur Bereitstellung eines Amazon-S3-Buckets verwenden, liest Cloud Provisioning and Governance den Ressourcentyp aus der Cloud-Antwort (AWS::S3::Bucket) und identifiziert dann das entsprechende Muster (AWS S3) aus der Tabelle sn_capi_resource_type. Dann ruft die Anwendung das Muster auf, um nur den neu bereitgestellten Amazon-S3-Bucket zu erkennen und seine Attribute

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der entsprechenden CI-Klasse in der CMDB zu aktualisieren (Tabelle „Cloud-Objektspeicher“ [cmbd_ci_cloud_object_storage]).

Wenn für den Ressourcentyp sowohl eine CAPI-basierte gezielte Erkennung als auch eine musterbasierte gezielte Erkennung implementiert ist, verwendet das System die CAPI-basierte gezielte Erkennung.

Wenn für den Ressourcentyp keine CAPI-basierte und musterbasierte gezielte Erkennung implementiert ist, wird der Ressourcentyp in der Tabelle „Cloud-Ressourcen“ [cmdb_ci_cmp_resource] als generische Cloud-Ressource klassifiziert. In solchen Fällen können Sie ein Einzelressourcen-Erkennungsmuster erstellen und es dem Ressourcentyp zuordnen. Weitere Informationen finden Sie unter Erstellen oder passen Sie Muster an Und Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen.

Zugehörige Informationen

Antwortprozessor konfigurieren

Eine CAPI-Schnittstelle erstellen oder erweitern

Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen

Definieren Sie eine 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster in der Tabelle „Cloud-Ressourcentypen“ [sn_capi_resource_type]. Die Funktion der musterbasierten gezielten Erkennung verwendet diese Informationen, um das entsprechende Muster aufzurufen und die bereitgestellte Ressource zu erkennen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung Cloud Provisioning and Governance bereitgestellt wurde.
- Stellen Sie sicher, dass die neuesten Versionen von Discovery und Service-Mapping installiert sind.
- Vergewissern Sie sich, dass der Anwendungsbereich „Cloud-API“ ist.

Erforderliche Rolle: sn_cmp.cloud_service_designer oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie zur Tabelle sn_capi_resource_type.
2. Wählen Sie den entsprechenden Ressourcentyp-Datensatz aus.
3. Füllen Sie die Felder des Formulars aus.

   Die in dieser Tabelle angegebenen Beispielwerte stellen eine 1:1-Beziehung zwischen dem Ressourcentyp AWS::S3::Bucket und dem entsprechenden Einzelressourcen-Erkennungsmuster (Amazon AWS S3) her.

Feld	Beschreibung
Name	Cloud-Ressourcentyp, den Sie erkennen möchten. Beispiel: AWS::S3::Bucket
Produkt	(Optional) Produktkategorie. Beispiel: AWS Simple Storage Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
CI-Klasse	Name der CI-Tabelle in der CMDB. Das System schreibt die erkannten Informationen in diese Tabelle. Beispiel: Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]
Muster	Ein Einzelressourcen-Erkennungsmuster zum Erkennen der Ressource. Beispiel: Amazon AWS S3
Abhängigkeitssequenz	(Optional) Reihenfolge zum Auslösen des Musters.

4. Wählen Sie **Aktualisieren**.

Tools zur Problembehandlung für Cloud Provisioning and Governance

Die Anwendung Cloud Provisioning and Governance bietet mehrere Tools zur Behebung von Fehlern, die bei der Discovery von Cloud-Konten, der Bereitstellung und Verwaltung von Cloud-Ressourcen und der Aktualisierung der CMDB auftreten können.

Diese Tools zur Problembehandlung sind verfügbar:

Cloud-Orchestrierungspfad

Der Cloud-Orchestrierungspfad ist ein Aktivitätsprotokoll für alle Cloud-Ressourcenaktivitäten auf der Instanz. Verwenden Sie den Cloud-Orchestrierungspfad, um nach Fehlern zu suchen, die bei Cloud-Ressourcen auftreten, wie z. B. Anmeldeinformationsfehler bei Discovery oder API-Ausführungsfehler.

Anweisungen dazu finden Sie unter Cloud-Orchestrierungspfad öffnen.

Cloud-API-Pfad

Der Cloud API-Pfad ist ein Aktivitätsprotokoll für alle Aktivitäten, die die Cloud API verwenden und den MID-Server durchlaufen. Verwenden Sie den Cloud API-Pfad, um API-Aufrufe und -Fehler im Zusammenhang mit weitergeleiteten Daten, spezifischen API-Routenfehlern und Java-Laufzeitausnahmen anzuzeigen.

Anweisungen dazu finden Sie unter Cloud API-Pfad öffnen.

Ursachenanalysedashboard

Das Ursachenanalysedashboard fasst Datensätze aus dem Cloud-Orchestrierungspfad und dem Cloud API-Pfad zusammen und stellt sie in nützlichen, filterbaren Listen und Diagrammen dar.

Anweisungen dazu finden Sie unter Berichte zur Cloud-Ursachenanalyse verwenden.

Cloud-Orchestrierungen

Cloud-Orchestrierungen sind die Aufträge, die Ihre Instanz für jeden versuchten Vorgang für einen Stapel verarbeitet hat. Verwenden Sie Datensätze der Cloud-Orchestrierung, um Statusnachrichten zu Vorgängen anzuzeigen, die für Cloud-Ressourcen ausgeführt wurden, und um Details zu jedem API-Schritt abzurufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

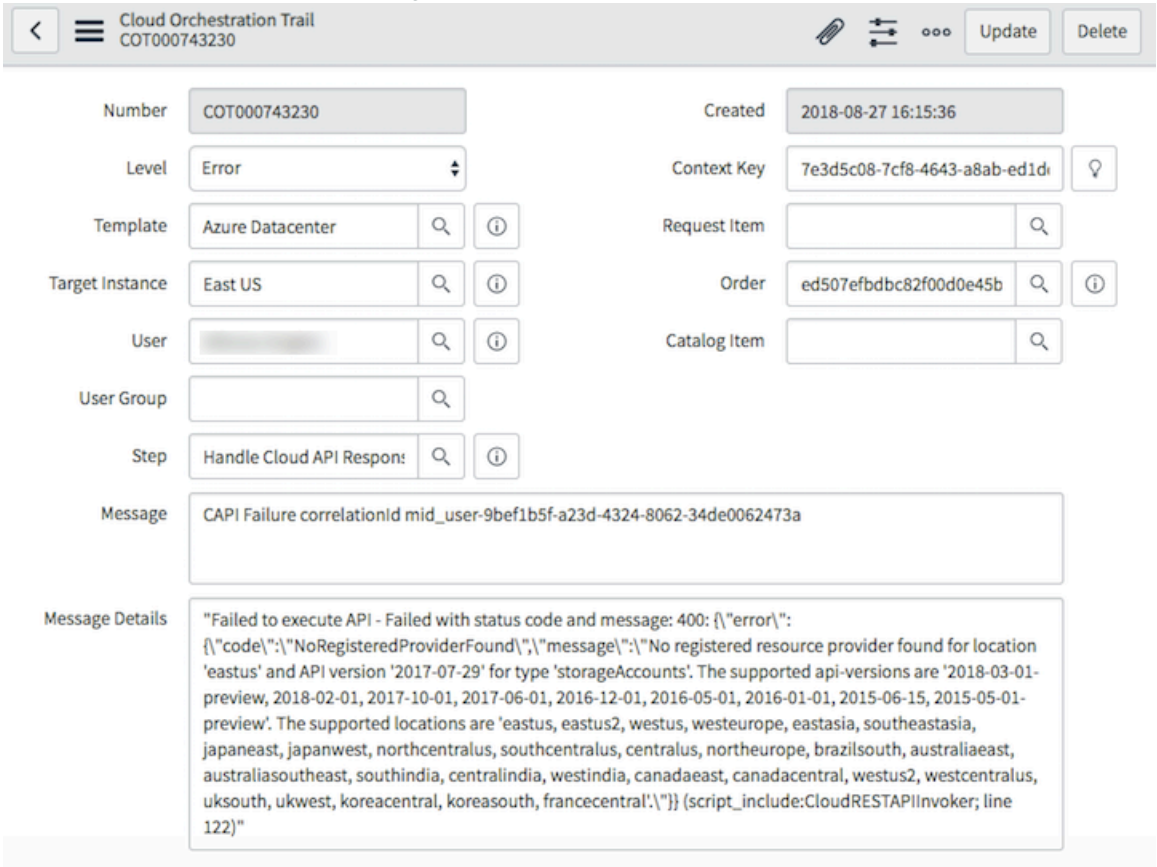
Anweisungen dazu finden Sie unter Cloud-Orchestrierungen öffnen.

Cloud-Orchestrierungspfad

Der Cloud-Orchestrierungspfad ist ein Aktivitätsprotokoll für alle Cloud-Ressourcenaktivitäten auf der Instanz.

Inhalt von Cloud-Orchestrierungspfaden

Formular „Cloud-Orchestrierungspfad“



Feld	Beschreibung
Nummer	Eine automatisch generierte Nummer für den Pfadeintrag
Ebene	Eine der folgenden Möglichkeiten: • Debuggen • Info • Warnen • Fehler
Vorlage	Die Komponente, z. B. ein Ressourcenblock oder eine Blaupause, auf die eine Cloud Provisioning and Governance-Aktion angewendet wurde
Vorlageninstanz	Das Rechenzentrum, in dem sich die Cloud-Ressource befindet
Anwender	Der an der Transaktion beteiligte Benutzer
Benutzergruppe	Die Benutzergruppe, zu der der Benutzer gehört

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellt	Zeitpunkt (Datum und Uhrzeit), zu dem der Eintrag vom System erstellt wurde
Meilenstein	Gibt an, ob diese Transaktion ein Meilenstein ist. Sie können das Formular so konfigurieren, dass Sie dieses Feld sehen.
Anforderungselement	Die für die Transaktion generierte Service Catalog-Anforderung
Schritt	Der Schritt, bei dem zusätzliche Informationen über die Transaktion identifiziert werden, einschließlich der Komponente und der Phase. Sie können das Formular so konfigurieren, dass Sie dieses Feld sehen.
Katalogelement	Das Katalogelement (sofern vorhanden), das an der Ausführung beteiligt war
Nachricht	Die Fehlermeldung oder die Nachricht über den erfolgreichen Abschluss. Diese kann Elemente wie die ID der entsprechenden Nachricht im Cloud-API-Pfaddatensatz oder die aufgerufene Cloud-API enthalten.
Nachrichtendetails	Details zum Fehler, z. B. HTTP-Fehler

Beispiel für eine Fehlermeldung:

```
Failed to list loadbalancer Failed : HTTP error code : 403
```

Hier wird angegeben, dass die Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte. Die Schnittstelle des Lastenausgleichsmoduls gibt den ersten Fehler aus, da das Lastenausgleichsmodul das erste Gerät ist, das Zugriff auf die Cloud-Ressource ermöglicht.

Ein entsprechender Fehler auf dem MID Server wird im Cloud API-Pfad erfasst.

Schritte, Phasen und Komponenten

Jeder Eintrag der Cloud-Orchestrierung verfügt über identifizierende Attribute, die erklären, worum es bei der auslösenden Transaktion ging. *Schritte* gruppieren diese Attribute und identifizieren die *Komponente* im System, die an der Transaktion beteiligt war, sowie die *Phase*, in der die Transaktion stattfand.

Sie können das Formular „Cloud-Orchestrierungspfad“ so konfigurieren, dass das Feld **Schritt** angezeigt wird, wenn es noch nicht sichtbar ist.

Schritt	Komponente	Phase
API-Parameter anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Konfigurationsparameter anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Endpunktbindung anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Richtlinie anwenden	Richtlinienmodul	Workflow- und Richtlinienausführung
Richtlinienregelaktion anwenden	Richtlinienmodul	Workflow- und Richtlinienausführung
Cloud-API aufrufen	BP-DSL-Executor	Cloud-Orchestrierung
Cloud API-Connector aufrufen	CAPI-Probe	Cloud-API-Orchestrierung
Cloud-Übereinstimmung überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Rechenzentrumskapazität überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Komponente	Phase
Ressourcenblockrichtlinien überprüfen	BP-DSL-Executor	Cloud-Orchestrierung
Benutzerberechtigungen überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Benutzerkontingent überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Cloud-Orchestrierung abschließen	BP-DSL-Executor	Cloud-Orchestrierung
Kategorieelementrichtlinie ausführen	Dynamische Formulare	Katalogelementanforderung
Formularregeln ausführen	Dynamische Formulare	Katalogelementanforderung
Ressourcenblockvorgang ausführen	BP-DSL-Executor	Cloud-Orchestrierung
Ressourceninstanzskript ausführen	BP-DSL-Executor	Cloud-Orchestrierung
Kontingentdetails abrufen	Dynamische Formulare	Katalogelementanforderung
Antwort abrufen	CAPI-Orchestrator	Cloud-API-Orchestrierung
Cloud API-Antwort verarbeiten	BP-DSL-Executor	Cloud-Orchestrierung
Antwort der Richtlinienausführung verarbeiten	BP-DSL-Executor	Cloud-Orchestrierung
Antwort und Chunking verarbeiten	CAPI-Probe	Cloud-API-Orchestrierung
Cloud-Orchestrierung aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Richtlinien-Engine aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Vorprozessualen Workflow aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Kategorieelement starten	Katalogelement	Katalogelementanforderung
Aufrufer benachrichtigen	CAPI-Orchestrator	Cloud-API-Orchestrierung
BP-Ausführungsplan vorbereiten	BP-DSL-Executor	Cloud-Orchestrierung
Ausführbare API vorbereiten	CAPI-Orchestrator	Cloud-API-Orchestrierung
API-Routenanforderung veröffentlichen	CAPI-Orchestrator	Cloud-API-Orchestrierung
Cloud API-Antwort senden	CAPI-Probe	Cloud-API-Orchestrierung
Formular mit Filtern anzeigen	Dynamische Formulare	Katalogelementanforderung
Formular absenden	Katalogelement	Katalogelementanforderung
Eingaben validieren	BP-DSL-Validierung	Cloud-Orchestrierung

Unter Berichte zur Cloud-Ursachenanalyse verwenden finden Sie Anweisungen zum Zugriff auf Berichte im Zusammenhang mit dem Cloud-Orchestrierungspfad.

Zugehörige Informationen

Cloud API-Pfad

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Orchestrierungspfad öffnen

Öffnen Sie den Cloud-Orchestrierungspfad, um Probleme wie fehlgeschlagene Richtlinien oder fehlgeschlagene Discovery von Cloud-Ressourcen zu debuggen und zu beheben.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Betreiben** > **Pfade**an.
2. Auf der Registerkarte **Cloud-Orchestrierungspfad** filtern und sortieren Sie die Liste der Datensätze aus dem Orchestrierungs-API-Pfad nach Bedarf.
   Wenn Sie z. B. nach einer fehlgeschlagenen Discovery suchen, filtern Sie die Liste, sodass in der Spalte **Ebene** nur Einträge mit **Fehler** anzeigt werden.
3. Klicken Sie auf einen Link in der Spalte **Erstellt**, um den Datensatz des Orchestration-API-Pfads zu öffnen.
4. Öffnen Sie in der zugehörigen Liste „CAPI-Pfadprotokolle“ den Protokolldatensatz, der die gewünschten Informationen anzeigt.
   Öffnen Sie beispielsweise **route_error** oder **error_detail**, um einen fehlgeschlagenen Vorgang zu debuggen.

Cloud-Orchestrierungen öffnen

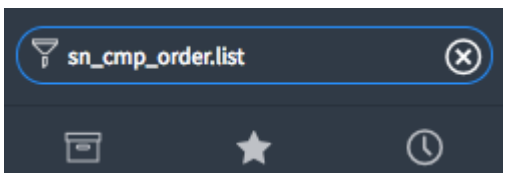
Cloud-Orchestrierungen zeigen die Aufträge an, die Ihre Instanz für jeden versuchten Vorgang für einen Stapel verarbeitet hat. Sie zeigen auch die Werte der Felder an, die der Benutzer über das Cloudbenutzerportal gesendet hat. Verwenden Sie Cloud-Orchestrierungen zur Behebung von Problemen, die auftreten, wenn ein Benutzer eine Cloud-Ressource bereitstellt oder einen anderen Vorgang für eine vorhandene Cloud-Ressource ausführt.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

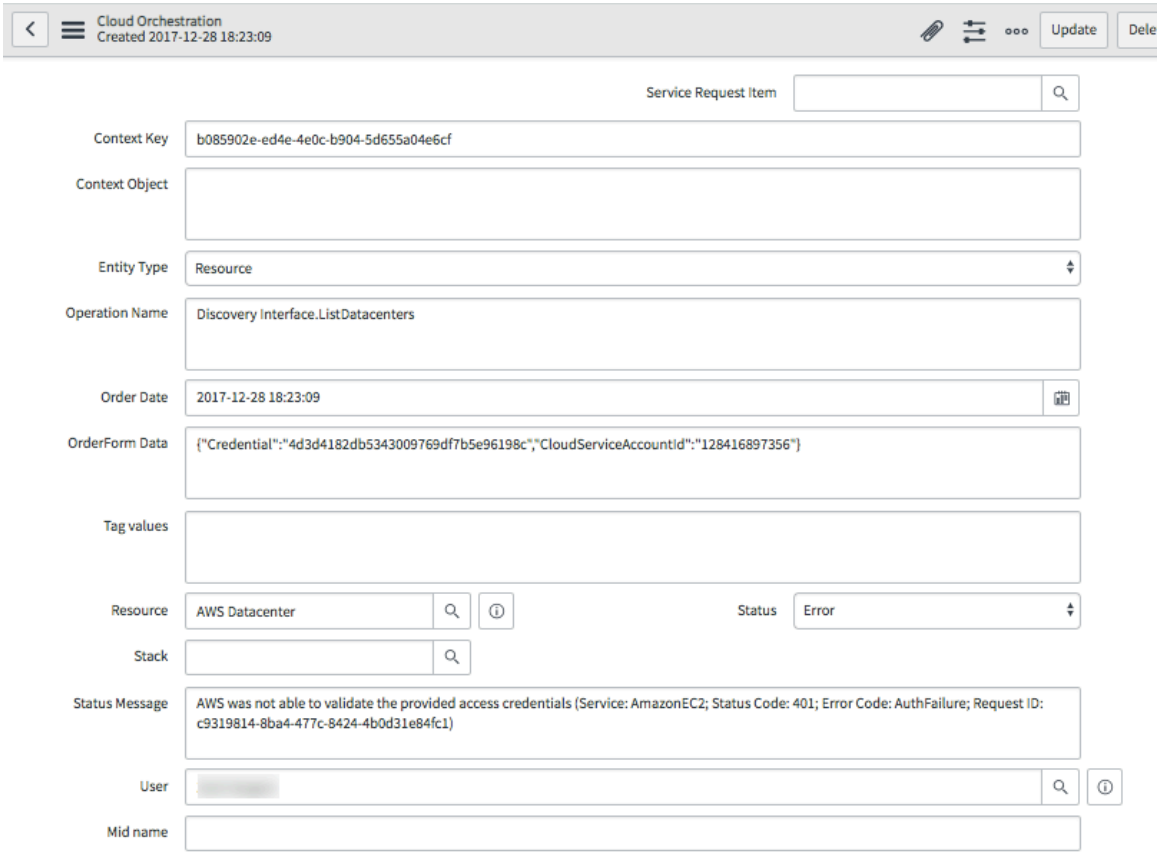
1. Geben Sie auf der Instanz (nicht im Cloudbenutzerportal) den folgenden Text in den Anwendungsfilter ein:

   Die Liste der Cloud-Orchestrierungen wird angezeigt.
2. Sortieren und filtern Sie die Liste, um den gesuchten Fehler oder eine andere Meldung zu finden.

   Um zum Beispiel die Liste nach Datum zu sortieren, klicken Sie auf die Spalte **Auftragsdatum**. Um nur aufgetretene Fehler anzuzeigen, klicken Sie mit der rechten Maustaste in einer Zelle auf **Fehler** und wählen Sie **Übereinstimmungen anzeigen** aus.
3. Öffnen Sie einen Datensatz der Cloud-Orchestrierung, indem Sie auf das Feld **Auftragsdatum** klicken.
4. Überprüfen Sie die Formularfelder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Beispielformular zeigt den Typ der Nachricht, die Sie sehen können, wenn ein Vorgang aufgrund von falschen Anmeldeinformationen fehlschlägt. Das Feld „OrderForm-Daten“ zeigt die Sys-ID des Anmeldeinformationsdatensatzes und die Servicekonto-ID an.

Feld	Beschreibung
Serviceanforderungselement	Eine Service Catalog-Anforderung (falls vorhanden), die dieser Transaktion zugeordnet ist.
Kontextschlüssel	Ein Schlüsselbezeichner für diese Nachricht.
Kontextobjekt	Dieses Feld ist normalerweise leer.
Kontextinstanz	Die in Transaktionen für einen Stapel verwendete Blaupause oder der in Transaktionen für eine Cloud-Ressource verwendete Ressourcenblock.
Besitzerinstanz Besitzertabelle	Die Besitzerinstanz ist der Ressourcenblock, in dem die Transaktion stattgefunden hat. Dieses Feld wird nur ausgefüllt, wenn der **Entitätstyp** gleich **Ressource** ist. Die Besitzertabelle für die Bereitstellung eines Stapels ist immer „Stapel“ [sn_cmp_stack]. Andernfalls ist die Tabelle der CI-Typ der Ressource, z. B. „VM-Instanz“ [sn_cmp_vm_instance].
Entitätstyp	Gibt an, ob die Transaktion in einer **Blaupause** oder einer **Ressource** (Ressourcenblock) aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorgangsname	Die Schnittstelle und der Vorgang, der ausgelöst wird.
Auftragsdatum	Das Datum der Transaktion.
OrderForm-Daten	Die über das Benutzerformular übermittelten Daten.
Tag-Werte	Alle an der Transaktion beteiligten Tag-Werte.
Ressource	Der Ressourcenblock, in dem der Vorgang stattgefunden hat. Dieses Feld wird nur ausgefüllt, wenn der Wert des Felds „Entitätstyp“ **Ressource** ist.
Status	Der Status der Nachricht. Wenn Sie einen Fehler anzeigen lassen, wird die Option **Fehler** aufgelistet.
Stapel	Der Stapel, zu dem diese Ressource gehört.
Statusnachricht	Die Statusnachricht, die das Problem erläutert. Durchsuchen Sie die Dokumentation des Cloud-Providers nach den Statuscodes und Nachrichten, die in diesem Feld angezeigt werden. Der Cloud-Provider stellt Ihnen möglicherweise Lösungen zur Verfügung.
Anwender	Der Benutzer, der den Vorgang ausgelöst hat.
MID-Name	Dieses Feld kann den Namen des an der Transaktion beteiligten MID-Server s anzeigen. Es bleibt häufig leer.

Verschieben von Cloud Provisioning and Governance-Inhalten zwischen Umgebungen

Sie können Inhalte in der Cloud Provisioning and Governance-Anwendung aus einer Umgebung in eine andere verschieben. Entwickeln Sie beispielsweise eine Anwendung in einer Umgebung, und verschieben Sie dann die Anwendung und alle zugehörigen Abhängigkeiten zu Test- oder Produktionszwecken in eine andere Umgebung.

Inhaltsentitäten, die verschoben werden können

Die Anwendung Cloud Provisioning and Governance besteht aus Code, Ressourcen, Inhalten und Konfigurationen.

Sie können die folgenden Inhaltsentitäten zwischen Umgebungen verschieben:

- Blaupausen
- Ressourcenblöcke
- Cloud-APIs

Verwenden Sie die Update Sets, um die Inhaltsentitäten zu verschieben. Update Sets sind XML-Dateien, die den gesamten Inhalt in benannte Sets gruppieren und diese Sets dann als Einheit zu Test- oder Bereitstellungszwecken in andere Systeme verschieben. Informationen zur Funktionsweise von System-Update-Sätzen finden Sie unter System-Update-Sätze .

Abhängigkeiten von Inhaltsentitäten

Jede der Inhaltsentitäten weist einige direkte Abhängigkeiten auf, die automatisch mit dem Inhalt in die neue Umgebung verschoben werden.

Die direkten Abhängigkeiten für jede dieser Inhaltsentitäten sind folgende:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsentität	Abhängigkeiten
Blaupause	• Ressourcenblöcke • Cloud-APIs • MID-Skripts • Ressourcenpools • Richtlinien • Skript umfasst Folgendes • Cloud-Skripts
Ressourcenblöcke	• Ressourcenpools • Richtlinien für Ressourcenvorgänge • Skript umfasst Folgendes • Cloud-APIs • Abhängige Ressourcenblöcke • MID-Skripts
Cloud-API	MID-Skripts

Zugehörige Informationen

Eine Blaupause aus einer Umgebung in eine andere verschieben

Einen Ressourcenblock aus einer Umgebung in die andere verschieben

Eine Cloud-API aus einer Umgebung in die andere verschieben

Eine Blaupause aus einer Umgebung in eine andere verschieben

Mit Update Sets können Sie eine Blaupause und ihre Abhängigkeiten zwischen Umgebungen verschieben. Über Update Sets können Sie eine Blaupause und ihre Abhängigkeiten in einem benannten Set gruppieren und dann als Einheit in andere Systeme verschieben, um sie dort zu testen oder bereitzustellen. Beispielsweise können Sie eine Blaupause aus einer Entwicklungsumgebung in eine Produktionsumgebung verschieben.

Vorbereitungen

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Update Sets exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Warum und wann dieser Vorgang ausgeführt wird

Verpacken Sie die Blaupause als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in eine andere Umgebung.

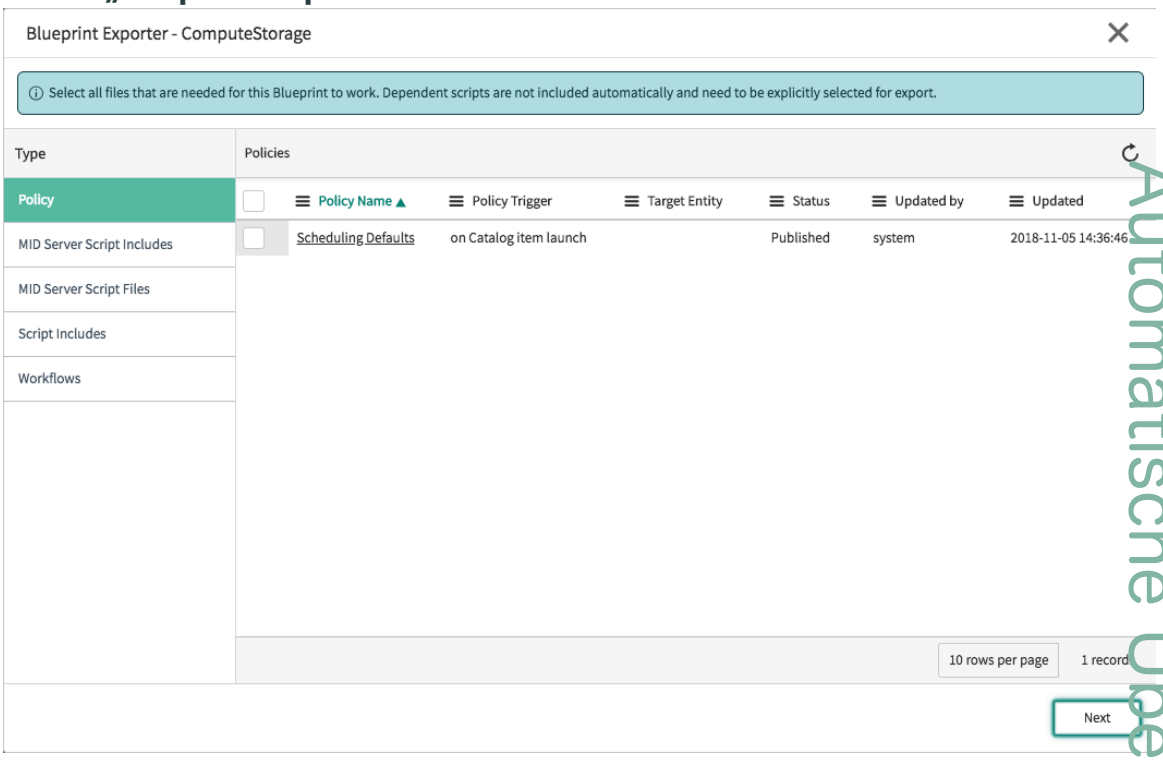
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Blueprints**an.
   Alle Blaupausen, egal ob veröffentlicht oder Entwurf, werden im Fenster „Blueprints“ (Blaupausen) angezeigt.
2. Exportieren Sie die Blaupause.

   a. Klicken Sie für die Blaupause, die Sie exportieren möchten, auf das Symbol „Exportieren“ ( ).

Fenster „Blaupausenexport“



Das Fenster „Blueprint Exporter“ (Blaupausenexporteur) enthält eine Liste aller indirekten Abhängigkeiten (Richtlinie, MID Serverskript-Einbindungen, MID Serverskript-Dateien, Skripteinbindungen und Workflows) für den Plan. Objekte wie Richtlinien, Pools, MID-Skripts, Skripteinbindungen und Workflows sind nicht direkt Teil einer Blaupause, aber eine Blaupause kann davon abhängen, dass diese Objekte ordnungsgemäß funktionieren.

   b. Klicken Sie im Fenster „Blueprint Exporter“ (Blaupausenexporteur) auf ein Objekt in der Spalte „Type“ (Typ).
   Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Blaupause exportieren möchten. Wenn Sie beispielsweise MID Server-Skripteinbindungen auswählen, werden alle entsprechenden Skripteinbindungen in der rechten Spalte angezeigt. Wenn ein Workflow Subworkflows enthält, wählen Sie den übergeordneten Workflow und alle Subworkflows aus, damit der Workflow exportiert werden soll. Wenn einem Workflow benutzerdefinierte Aktivitäten zugeordnet sind, exportieren Sie diese zuerst und anschließend den Workflow.

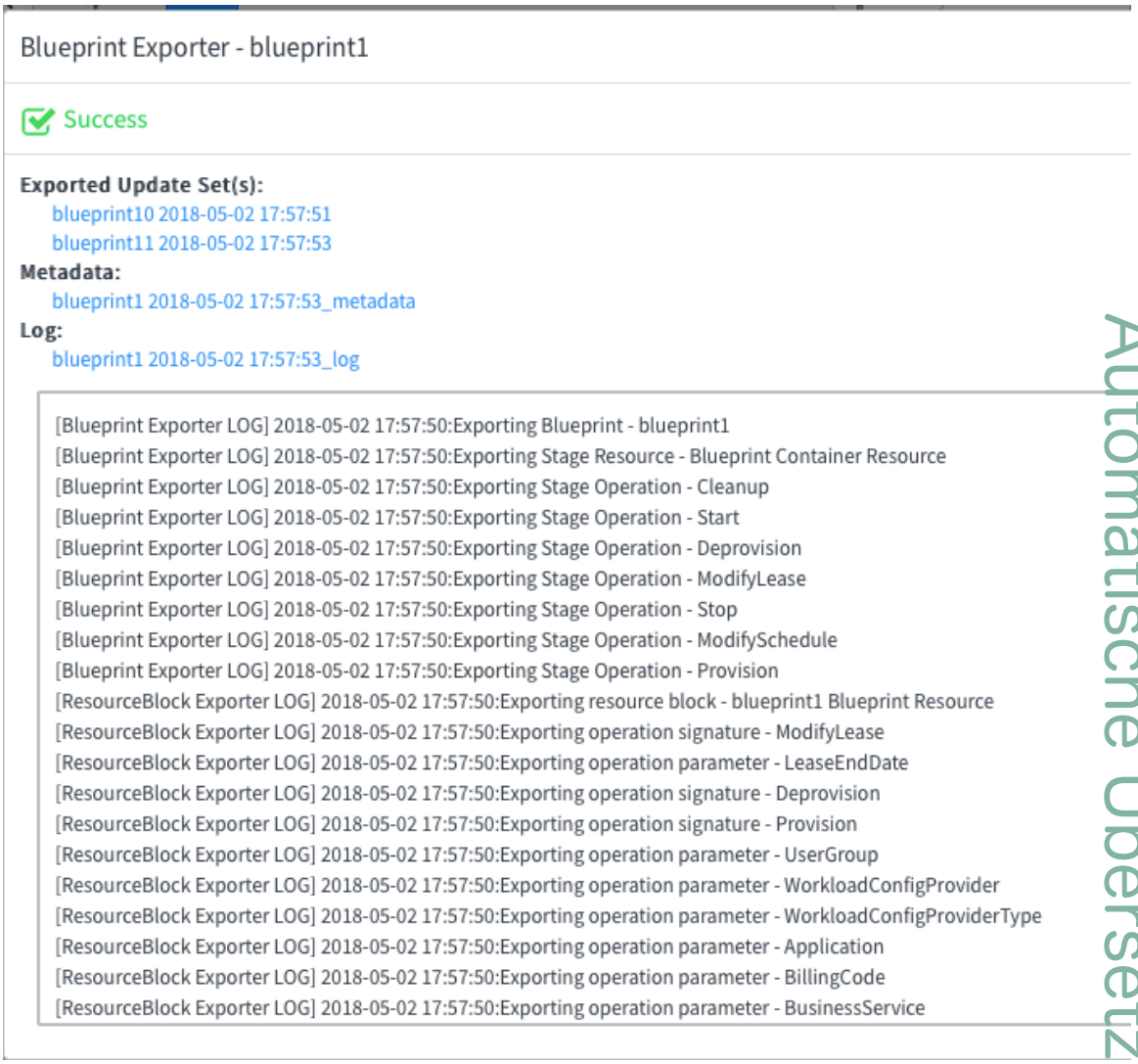
   c. Klicken Sie auf **Next** (Weiter).
   Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten aufführt, die Sie in das Export-Update Set aufgenommen haben.

   d. Klicken Sie auf **Update Set exportieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fenster „Blueprint Exporter“ (Blaupausenexporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass die Blaupause mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)“ (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen. Wenn die Dateien jedoch nicht automatisch heruntergeladen werden, führen Sie folgende Schritte aus.



Automatische Übersetzung

Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Angenommen, die Blaupause, die Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
   Wenn die Dateien nicht heruntergeladen werden, führen Sie die nachstehenden Schritte aus.

   a. Klicken Sie auf die Metadatendatei.
   Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei blueprint10 die erste zu exportierende Datei, gefolgt von der Datei blueprint11.

   b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

c. Zum Herunterladen der ersten XML-Datei (in diesem Beispiel ist dies blueprint10) auf das System klicken Sie **Export to XML** (In XML exportieren).
Importieren Sie alle exportierten Dateien in eine andere Umgebung. Benutzer mit der Administratorrolle können die Dateien importieren. Beispiel: Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies blueprint11), und laden Sie diese Datei ebenfalls auf das System herunter.

4. Importieren Sie die Blaupause.

a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator Retrieved Update Sets (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).

Hinweis: Wenn in der Zielumgebung eine Blaupause vorliegt, die Sie aus der Quellumgebung exportiert haben und beide Blaupausen eine andere sys_id haben, wird beim Importieren der Blaupause ein Fehler angezeigt und der Importvorgang wird beendet. Exportieren Sie eine andere Blaupause aus der Quellumgebung oder löschen Sie in der Zielumgebung die Blaupause mit dem identischen Namen. Wenn in der Zielumgebung eine Blaupause vorliegt, die Sie aus der Quellumgebung exportiert haben und beide Blaupausen die gleiche sys_id haben, wird die Blaupause in der Zielumgebung mit der Blaupause aktualisiert, die Sie aus der Quellumgebung exportiert haben.

5. Um sicherzustellen, dass der Blueprint in die neue Umgebung importiert wird, wechseln Sie zu Ihrer Instanz in der neuen Umgebung und in Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Blueprints**an.
Die von Ihnen importierte Blaupause sollte in den aufgeführten Blaupausen angezeigt werden.

Einen Ressourcenblock aus einer Umgebung in die andere verschieben

Verwenden Sie Update-Sätze, um Ressourcenblöcke und ihre Abhängigkeiten zwischen Umgebungen mühelos zu übertragen. Gruppieren Sie sie in einem benannten Satz, um eine nahtlose Bewegung für Tests oder Bereitstellungen zu ermöglichen. Vereinfachen Sie Prozesse, z. B. die Übertragung eines Ressourcenblocks von der Entwicklung in die Produktion, um effiziente und organisierte Übergänge über verschiedene Systeme hinweg sicherzustellen.

Vorbereitungen

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Update Sets exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

Warum und wann dieser Vorgang ausgeführt wird

Verpacken Sie den Ressourcenblock als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in die andere Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

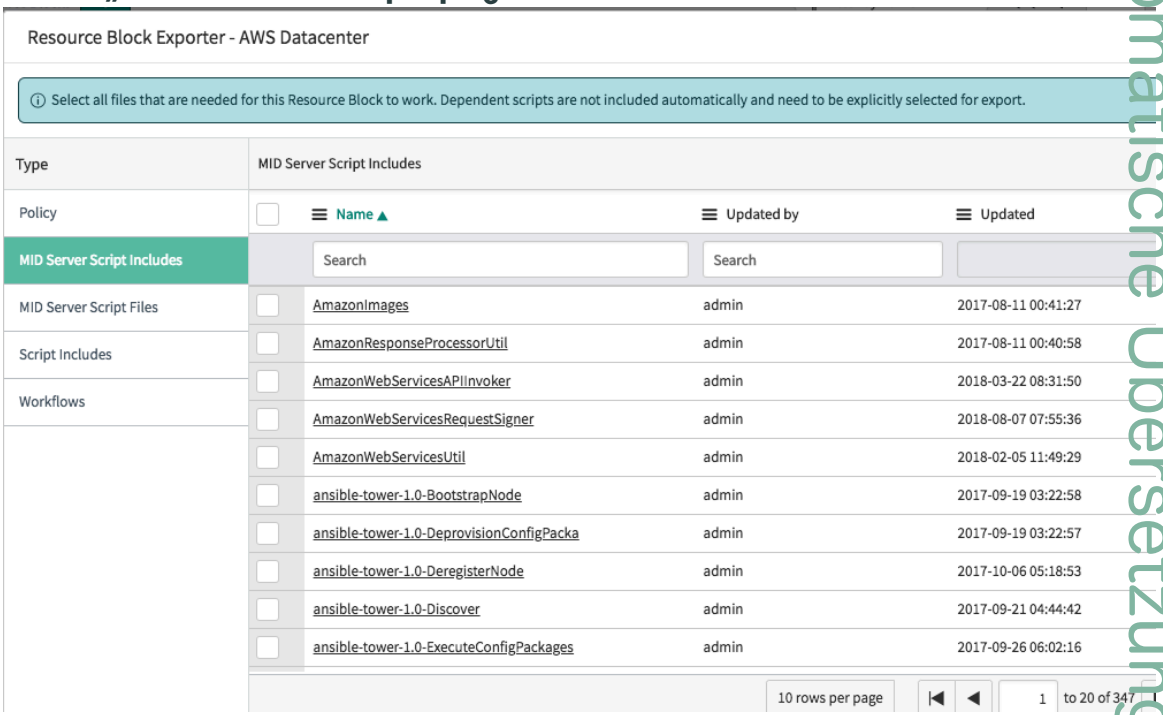
Hinweis: Wenn ein Ressourcenblock, den Sie aus der Quellumgebung exportieren, in der Zielumgebung vorhanden ist, führt der Import dieses Ressourcenblocks zu zwei Ressourcenblöcken mit demselben Namen: einem Ressourcenblock, der vor dem Import vorhanden war, und einem anderen Ressourcenblock, den Sie gerade importiert haben. Beispiel: Wenn Sie den Ressourcenblock „AWS-Rechenzentrum“ aus der Entwicklungsumgebung exportieren und bereits ein Ressourcenblock mit demselben Namen in der Produktionsumgebung vorliegt, liegen nach dem Import des Ressourcenblocks „AWS-Rechenzentrum“ in die Produktionsumgebung zwei Ressourcenblöcke mit dem identischen Namen „AWS-Rechenzentrum“ in der Produktionsumgebung vor.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Ressourcenblöcke**an.
   Alle Blaupausen, egal ob veröffentlicht oder Entwurf, werden im Fenster „Resource Blocks“ angezeigt.
2. Exportieren Sie den Ressourcenblock.

   a. Klicken Sie für den zu exportierenden Ressourcenblock auf das Symbol „Export Resource Block“ (Ressourcenblock exportieren) ( ).

Fenster „Ressourcenblock-Exportprogramm“



   a. Klicken Sie im Fenster „Resource Block Exporter“ (Ressourcenblock-Exporteur) auf ein Objekt in der Spalte „Type“ (Typ).

      Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Blaupause exportieren möchten. Wenn Sie beispielsweise MID Server-Skripteinbindungen auswählen, werden alle entsprechenden Skripteinbindungen in der rechten Spalte angezeigt.

      Wenn ein Workflow Unter-Workflows enthält, wählen Sie den übergeordneten Workflow und alle Unter-Workflows aus, damit der Workflow exportiert wird. Wenn einem Workflow benutzerdefinierte Aktivitäten zugeordnet sind, exportieren Sie diese zuerst und anschließend den Workflow.

   b. Klicken Sie auf **Next** (Weiter).

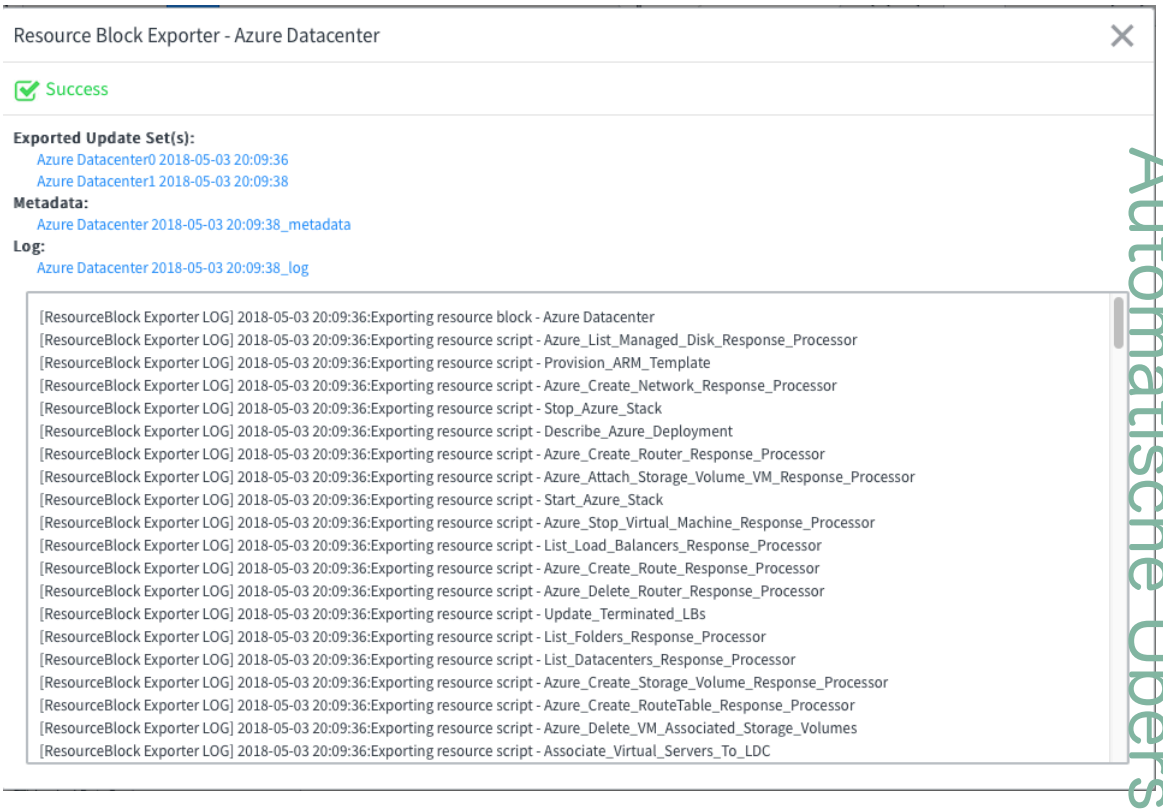
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten aufführt, die Sie in das Export-Update Set aufgenommen haben.

c. Klicken Sie auf **Export Update Set** (Update Set exportieren).

Das Fenster „Resource Block Exporter“ (Ressourcenblock-Exporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass der Ressourcenblock mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)“ (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen.



Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Angenommen, der Ressourcenblock, den Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
Wenn die Dateien nicht heruntergeladen werden, führen Sie die nachstehenden Schritte aus.

a. Klicken Sie auf die Metadatendatei.
Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei Azure Datacenter0 die erste zu exportierende Datei, gefolgt von der Datei Azure Datacenter1.

b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.
Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Um die erste XML-Datei in das System herunterzuladen (in diesem Beispiel ist dies Azure Datacenter0), klicken Sie auf **In XML exportieren**.

d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies Azure Datacenter1), und laden Sie diese Datei auf das System herunter.
Sie müssen alle exportierten Dateien in eine andere Umgebung importieren. Beispiel: Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

4. Importieren Sie den Ressourcenblock.

a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator Retrieved Update Sets (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).

> **Hinweis:** Wenn in der Zielumgebung ein Ressourcenblock vorliegt, den Sie aus der Quellumgebung exportiert haben und beide Ressourcenblöcke eine andere sys_id haben, wird beim Import des Ressourcenblocks ein Fehler angezeigt und der Importvorgang wird beendet. Exportieren Sie einen anderen Ressourcenblock aus der Quellumgebung oder löschen Sie in der Zielumgebung den Ressourcenblock mit dem identischen Namen. Wenn in der Zielumgebung ein Ressourcenblock vorliegt, den Sie aus der Quellumgebung exportiert haben und beide Ressourcenblöcke die gleiche sys_id haben, wird der Ressourcenblock in der Zielumgebung mit dem Ressourcenblock aktualisiert, den Sie aus der Quellumgebung exportiert haben.

5. Um sicherzustellen, dass der Ressourcenblock in die neue Umgebung importiert wird, wechseln Sie zu Ihrer Instanz in der neuen Umgebung und in Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Ressourcenblöcke**an.
Der importierte Ressourcenblock sollte in den aufgeführten Ressourcenblöcken angezeigt werden.

Eine Cloud-API aus einer Umgebung in die andere verschieben

Mit Update Sets können Sie eine Cloud-API zwischen Umgebungen verschieben. Über Update Sets können Sie eine Cloud-API und ihre Abhängigkeiten in einem benannten Set gruppieren und dann als Einheit in andere Systeme verschieben, um sie dort zu testen oder bereitzustellen. Beispielsweise können Sie Cloud-APIs aus einer Entwicklungsumgebung in eine Produktionsumgebung verschieben.

Vorbereitungen

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Datensätze exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

Warum und wann dieser Vorgang ausgeführt wird

Verpacken Sie die Cloud-API als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in die andere Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

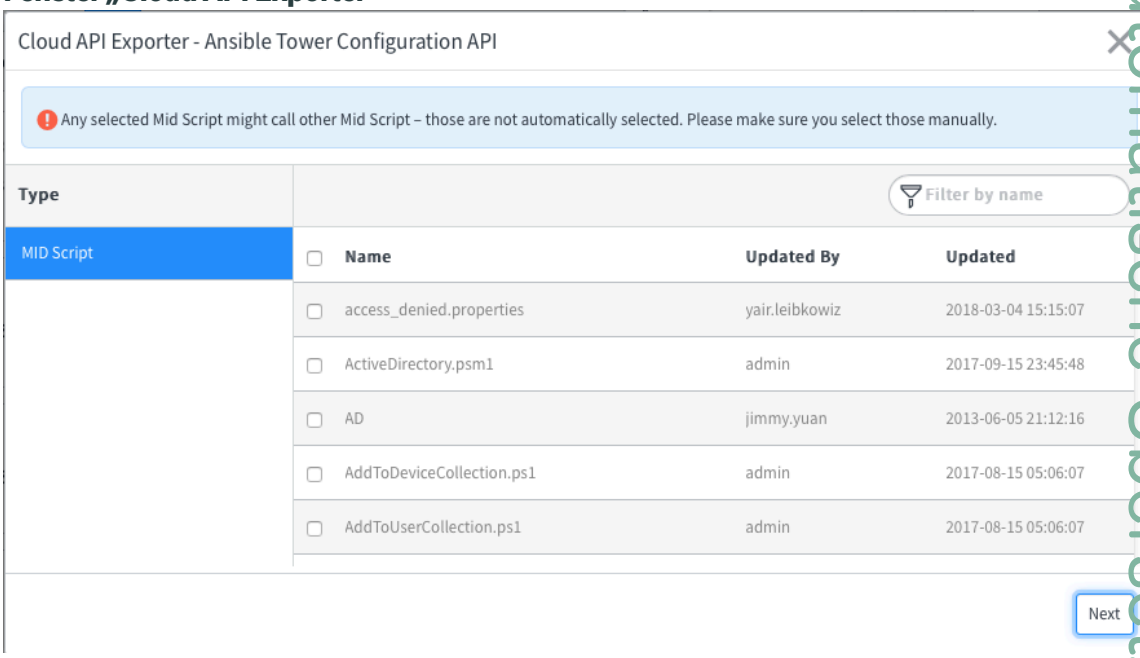
Hinweis: Wenn eine Cloud-API, die Sie aus der Quellumgebung exportieren, in der Zielumgebung vorhanden ist, führt der Import dieser Cloud-API zu zwei Cloud-APIs mit demselben Namen: einer Cloud-API, die vor dem Import vorhanden war, und einer anderen Cloud-API, die Sie gerade importiert haben. Beispiel: Wenn Sie die Ansible-Konfigurations-API aus der Entwicklungsumgebung exportieren und bereits eine Cloud-API mit demselben Namen in der Produktionsumgebung vorliegt, führt der Import der Ansible-Konfigurations-API in die Produktionsumgebung zu zwei Cloud-APIs mit demselben Namen, „Ansible Configuration API“, in der Produktionsumgebung.

Prozedur

1. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-API** > **API**an.
   Alle Cloud-APIs werden im Cloud-API-Fenster angezeigt.
2. Exportieren Sie die Cloud-API.

   a. Klicken Sie auf das Symbol für den Export von Cloud-APIs (), damit die Cloud-API exportiert wird.

Fenster „Cloud API Exporter“



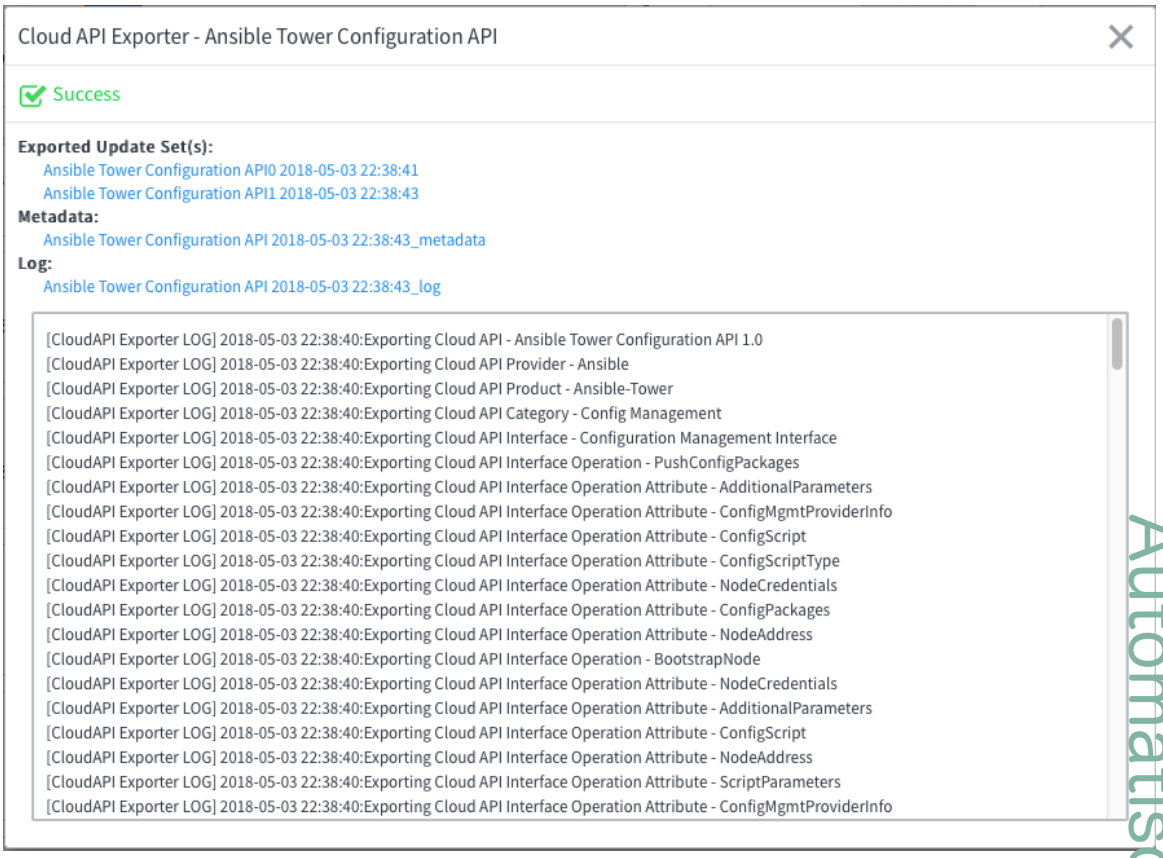
   b. Klicken Sie im Fenster „Cloud API Exporter“ (Cloud-API-Exporter) auf ein Objekt in der Spalte „Type“ (Typ).
   Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Cloud-API exportieren möchten. Wenn Sie beispielsweise „MID Script“ (MID-Skript) auswählen, werden alle entsprechenden MID-Skripts in der rechten Spalte angezeigt.

   c. Klicken Sie auf **Next** (Weiter).
   Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten der Cloud-API aufführt, die Sie in das Export-Update Set aufgenommen haben.

   d. Klicken Sie auf **Export Update Set** (Update Set exportieren).
   Das Fenster „Cloud API Exporter“ (Cloud-API-Exporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass die Cloud-API mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)“ (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Die Cloud-API, die Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
   Wenn die Dateien nicht heruntergeladen werden, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf die Metadatendatei.
   Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei namens Ansible Tower-Konfiguration API0 die erste zu exportierende Datei, gefolgt von der Datei Ansible Tower-Konfiguration API1.

   b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.
   Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

   c. Zum Herunterladen der ersten XML-Datei (in diesem Beispiel ist dies API0 2018-05-03) auf das System klicken Sie **Export to XML** (In XML exportieren).

   d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies API1 2018-05-03), und laden Sie diese Datei auf das System herunter.
   Importieren Sie alle exportierten Dateien in eine andere Umgebung. Beispiel: Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Importieren Sie die Cloud-API.

   a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator Retrieved Update Sets (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

   c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).
   Die Cloud-API wird in die neue Umgebung importiert.

5. Um sicherzustellen, dass der Blueprint in die neue Umgebung importiert wird, wechseln Sie zu Ihrer Instanz in der neuen Umgebung und in Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-API** > **API**an.
   Die von Ihnen importierte Cloud-API sollte in der Liste der Cloud-APIs angezeigt werden.

Cloud-API (CAPI)

Die Cloud-API (CAPI) ermöglicht die Integration von Cloud Provisioning and Governance von Cloud-Providern mit REST APIs.

CAPI-Komponenten

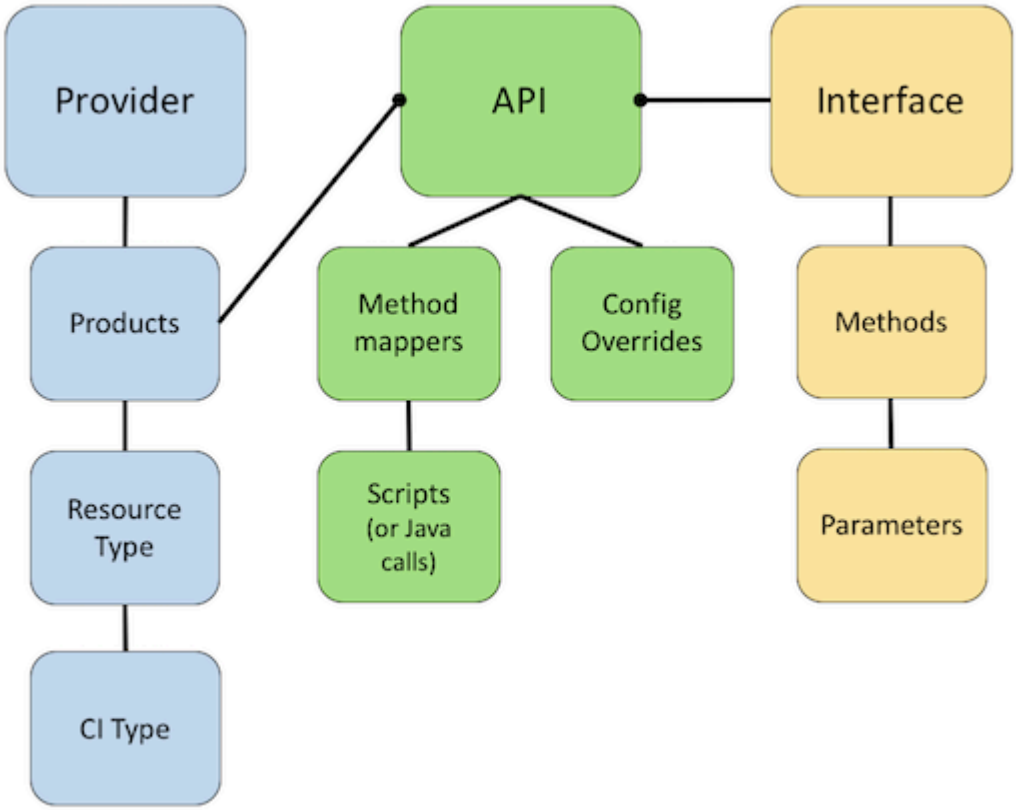
Die Integration mit Cloud-Providern erfolgt über REST-Aufrufe wie PUT, GET, POST und DELETE. CAPI bietet das Framework für die Integration einer REST API von Cloud-Anbietern, was Ihrer Instanz die Kommunikation mit dem Cloud-Anbieter ermöglicht, um Cloud-Ressourcen zu verwalten.

Siehe Durchsuchen Sie APIs nach Produkt Um mehr zu erfahren.

CAPI umfasst folgende Komponenten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI-Übersicht



Anbieter

Cloud-Anbieter sind die Clouds, mit denen Sie eine Verbindung herstellen können. Standardmäßig umfasst Cloud Provisioning and Governance die am häufigsten verwendeten Anbieter wie AWS, Azure und VMware. Jeder Anbieter verfügt über viele Produkte, von denen jedes Ressourcentypen bereitstellt. Jeder Ressourcentyp wird einem einzelnen CI-Typ zugeordnet. Zum Beispiel enthält `AWS provider` das Produkt `AWS Elastic Compute Cloud`, was den Ressourcentyp `AWS::EC2::Instance` umfasst. Dieser Ressourcentyp ist eine der gängigsten Cloud-Ressourcen, die Sie erstellen können. Der Ressourcentyp wird direkt dem CI-Typ der VM-Instanz [cmdb_ci_vm_instance] zugeordnet, wobei virtuelle Maschinen in der CMDB gespeichert werden.

Schnittstellen

Schnittstellen definieren das Framework, das das System benötigt, um die REST-Aufrufe zu strukturieren, die von den Cloud-Provider-APIs erwartet werden. Schnittstellen definieren den *Betrieb*, d. h. die *Methoden*, und die für die einzelnen Methoden erforderlichen *Parameter*.

Schnittstellen können wiederverwendet werden. Wenn Sie CAPI um neue Produkte und APIs erweitern, können Sie vorhandene Schnittstellen verwenden, um dieselben REST-Aufrufe durchzuführen.

APIs

CAPI-APIs sind die Kernkomponente von CAPI, über die ein Produkt und eine Schnittstelle miteinander verbunden sind. Die APIs enthalten den tatsächlichen Code, den das System ausführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jede CAPI-API enthält die folgenden Komponenten:

- *CAPI-Methodenzuordnungen* stellen die Methoden bereit , die den in der Schnittstelle definierten Vorgängen zugeordnet sind. Über CAPI-Methodenzuordnungen erstellen Sie MID-Server Skripteinbindungen in JavaScript, um dem Cloud-Anbieter genau mitzuteilen, was zu tun ist. Über die Skripteinbindungen wird die Verbindung zum Cloud-Anbieter hergestellt.

  Hinweis: Wenn Sie benutzerdefinierte CAPI-APIs erstellen, stellt das System eine leere Skripteinbindung bereit, die Sie anpassen können. Sie können bei Bedarf auch vorhandene Skripteinbindungen in Methodenzuordnungen ändern. Allerdings verwenden viele der Standard-APIs, die mit der Anwendung Cloud Provisioning and Governance geliefert werden, keine änderbaren Skripteinbindungen. Die Verbindungen sind in Java fest codiert. Sie können diese APIs weiterhin in neuen von Ihnen erstellten Ressourcenblöcken verwenden, aber die APIs können nicht geändert werden.

- *API-Konfigurationsüberschreibungen* enthalten die Identität (z. B. einen Schlüssel) und Anmeldeinformationen (z. B. den geheimen Schlüssel) und andere wichtige Parameter, die der Cloud-Anbieter benötigt. Diese Parameter helfen dem Cloud-Anbieter, die Vorgänge in der den CAPI-Methodenzuordnungen zugehörigen Liste durchzuführen. API-Konfigurationsüberschreibungen sind erforderlich, da Anmeldeinformationsdaten nicht enthalten sind, wenn das System die API des Cloudanbieters über REST aufruft. Ressourcenblöcke verwenden die Parameter und Werte, die Sie in den API-Konfigurationsüberschreibungen definieren, um den Anmeldeinformationsspeicher abzufragen. Wenn die API ausgeführt wird, werden die Attribute für alle Methodenaufrufe in den von Ihnen verwendeten Skripteinbindungen verfügbar gemacht.

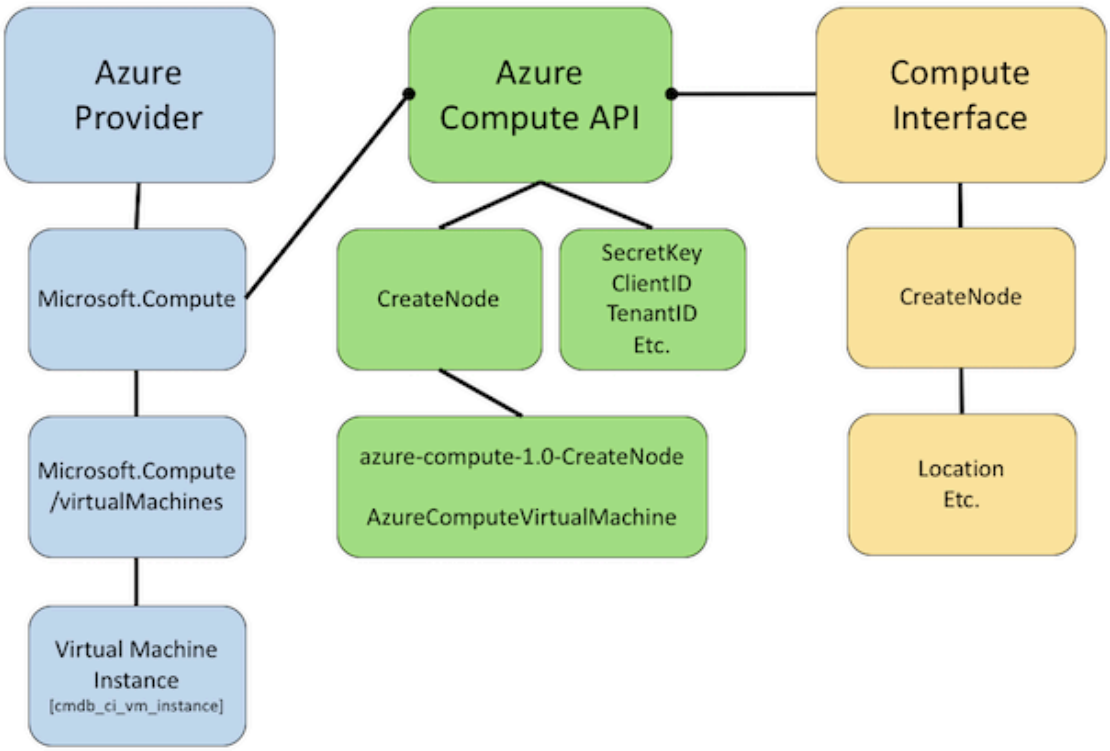
  Die Überschreibungen gelten nur für diese API. Die Überschreibungen überschreiben nichts in anderen APIs.

Da mehrere Versionen einer CAPI-API mit geringfügigen Abweichungen definiert werden können, kann eine vorhandene API erweitert werden (ohne sie zu überschreiben), während die gewünschte Funktionalität beibehalten wird.

Dieses Bild zeigt die Komponenten von CAPI, die verwendet werden, wenn ein virtueller Azure-Computer mit den Standard-CAPI-Einstellungen bereitgestellt wird, die mit Cloud Provisioning and Governance bereitgestellt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI Azure



In diesem Beispiel ist das Produkt `Microsoft.Compute` beim Anbieter `Azure` enthalten. Azure verwendet das Produkt `Microsoft.Compute` für virtuelle Computer. In Ihrem Fall ist das Produkt `Microsoft.Compute` dem Ressourcentyp `Microsoft.Compute/virtualMachines` zugeordnet, der mit dem CI-Typ `Virtual Machine Instance` in der CMDB verknüpft ist.

Die Schnittstelle `Compute` enthält Definitionen für Methoden wie `CreateNode`, die definiert, wie der tatsächliche virtuelle Computer erstellt wird. Von den vielen Parametern, die `CreateNode` verwendet, erfasst `Location` das Rechenzentrum, in der sich der virtuelle Computer befindet.

`Azure Compute API` verbindet das Produkt `Microsoft.Compute` und die in der Schnittstelle `Compute` definierte Struktur. Die Implementierung der Methode `CreateNode` ruft das Script Include `azure-compute-1.0-CreateNode` MID-Server auf , das das Script Include `AzureComputeVirtualMachine` MID-Server aufruft. Die Script Includes führen die tatsächlichen Aufrufe der Azure-API aus. Für den Zugriff auf das Azure-Konto werden die Methoden `SecretKey`, `ClientID`, `TenantID` sowie weitere Methoden in Konfigurationsüberschreibungen übergeben.

So führt CAPI eine Integration mit der Instanz durch

CAPI integriert die folgenden Komponenten in die Instanz:

Cloud Provisioning and Governance Ressourcenblöcke

Ein Ressourcenblock stellt eine einzelne Cloud-Ressource dar, z. B. einen virtuellen Server, virtuellen Serverspeicher oder ein Rechenzentrum. Ein Ressourcenblock kann auch als CI-Typ in der CMDB angesehen werden. Viele Ressourcenblöcke werden zu einer Blaupause zusammengefasst, die Benutzern im Cloud-Katalog als Katalogelement (auch Stapel genannt) angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im System kann jeder Ressourcenblock als Container angesehen werden, der auf CAPI verweist und Antworten des Cloud-Anbieters mit einem bestimmten CI verknüpft. Ressourcenblöcke verwenden Folgendes:

- *Operative Schritte*, die CAPI für jeden Vorgang aufrufen, z. B. den Bereitstellungsvorgang, und erforderliche Parameterwerte weitergeben, die der Cloud-Anbieter zum Ausführen des Vorgangs benötigt.
- *Antwortprozessoren*, die die REST-Antwort des Anbieters verarbeiten und analysieren und Datensätze in der CMDB aktualisieren.

Die CMDB

Jeder Ressourcenblock basiert auf einem CI-Typ der CMDB. Für Cloud Provisioning and Governance basieren alle cloud-bezogenen CI-Typen auf der Klasse `Virtual Machine Object CI`, die alle Attribute bereitstellt, die für alle standardmäßig unterstützten Cloud-Ressourcen benötigt werden. Wenn in Basissystem kein CI-Typ für eine Cloudressource vorhanden ist, müssen eine neue CI-Klasse erstellt und die erforderlichen Attribute hinzugefügt werden.

Wenn Sie eine neue CI-Klasse erstellen, müssen Sie auch Folgendes erstellen:

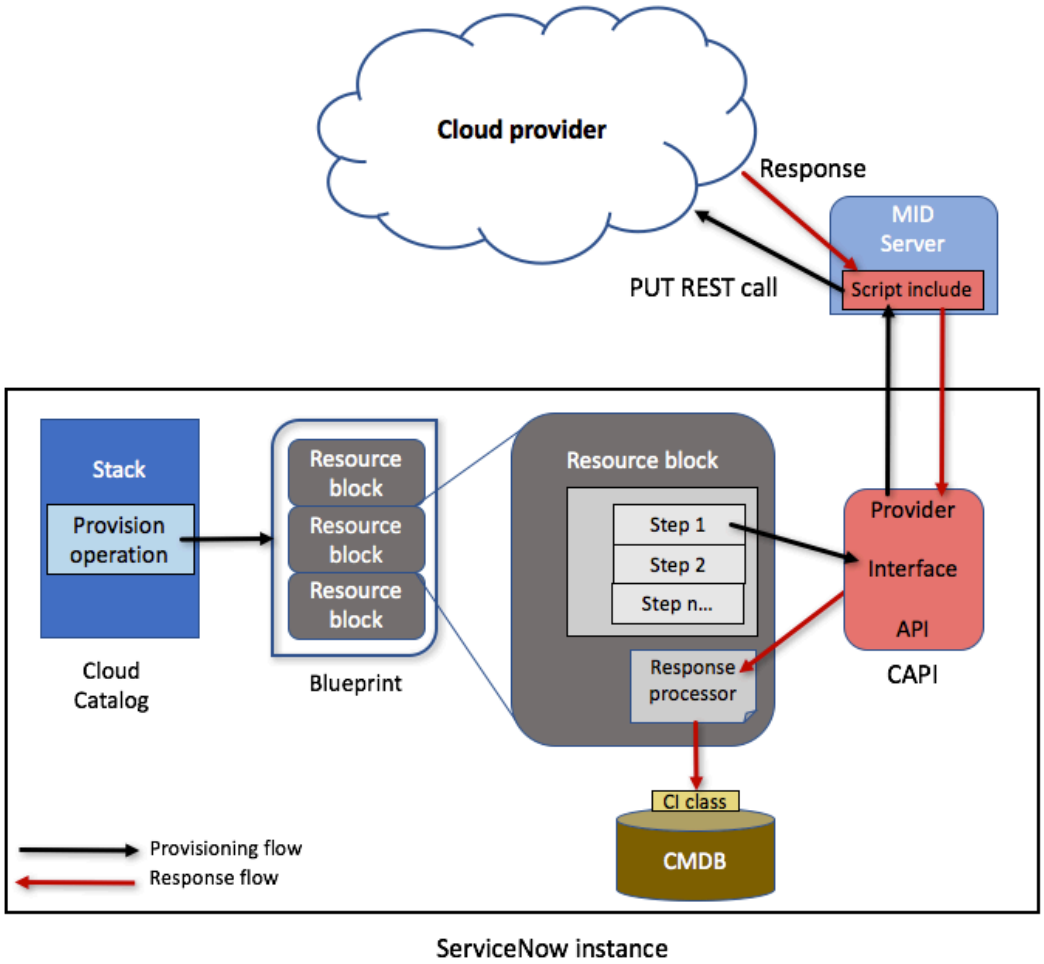
- Eine *CI-Klasse* für jede der Ressourcen, die den Benutzern zur Verfügung stehen. Alle CI-Klassen basieren auf der VM-Objektklasse.
- Eine *Identifizierungsregel*, die eine Objekt-ID angibt. Immer, wenn Komponenten von Cloud-Management auf eine bestimmte Cloud-Ressource in der CMDB verweisen, benötigen sie die Objekt-ID, um die richtige Cloud-Ressource zu finden.
- Eine *Beziehungsregel*, die angibt, wie die CI-Klasse für die Ressource mit anderen CI-Klassen verknüpft ist. Beispielsweise muss eine CI des Typs `virtual server` eine Beziehung des Typs `Hosted on::Hosts` mit einer CI des Typs `datacenter` haben. Diese Beziehungsregeln sind für die *Eindeutigkeit* von CIs erforderlich, wenn sie von der Engine für Identifizierung und Abgleich (Identification and Reconciliation Engine = IRE) verarbeitet werden. Die Kombination aus Servicekonto, Objekt-ID der Ressource und Datencenter (oder Standort), in dem sich die Ressource befindet, bestimmt die Eindeutigkeit.

Script Include MID-Server

Jeder Vorgang in der CAPI-API verfügt über eine Script Include MID-Server, die Sie konfigurieren. Die Script Include ruft die JavaScript-Klassen auf, die sich bereits in anderen Skripteinbindungen im System befinden, oder die von Ihnen erstellt wurden. Letzten Endes wird die Aufruferklasse aufgerufen, um den REST-Aufruf auszulösen. MID-Server-Skripteinbindungen werden auf der Instanz ServiceNow konfiguriert, aber auf MID-Server ausgeführt.

Dieses Bild zeigt, wie die Komponenten zusammenarbeiten, wenn ein Benutzer eine Ressource aus Cloudbenutzerportal bereitstellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



REST-Aufrufe zum Cloud-Anbieter

REST-Aufrufe zum Cloud-Provider werden über die Skripteinbindungen MID-Server ausgelöst, auf die von geskripteten CAPI-Methodenzuordnungen in CAPI-API-Datensätzen verwiesen wird. Zum Erstellen eigener CAPI-APIs oder zum Erstellen benutzerdefinierter MID-Server-Skripteinbindungen (die Teil der CAPI-Methodenzuordnungen sind) müssen Sie Folgendes berücksichtigen:

- Die Klassen, die Sie aus Skripteinbindungen des Typs MID-Server aufrufen können. Weitere Informationen finden Sie unter CAPI-Klassen in MID-Server-Skripteinbindungen.
- So implementiert der Cloud-Anbieter REST: Siehe:
  - Referenz zu Azure REST API
  - AWS-Handbücher und API-Referenzen

Um beispielsweise zu erfahren, wie ein REST-Aufruf an Azure zum Erstellen einer Ressourcengruppe zu tätigen ist, lesen Sie dieses Azure-Thema: Resource Groups - Creat Or Update (Ressourcengruppen – Erstellen oder Aktualisieren). Sie finden die von Azure benötigten Aspekte Endpunkt, Parameter und Anforderungstext sowie die von Azure bereitgestellten Antworten. Sie können Folgendes sehen:

- Der Endpunkt ist `management.azure.com`.
- Die Methode, die mit einem PUT-Vorgang aufgerufen wird, ist `subscriptions/{subscriptionId}/resourcegroups/{resourceGroupName}?api-version=2018-02-01`, wobei Sie die Abonnement-ID, den Ressourcengruppennamen und die API-Version angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denken Sie daran, dass die REST API-Aufrufe innerhalb der Skripteinbindungen vom Typ MID-Server stattfinden , die CAPI-API-Methodenzuordnungen zugeordnet sind. Sie rufen die Methoden auf, die CAPI bereits für Sie bereitstellt, indem Sie die von `CloudAPIBase` und `CloudRESTAPIInvoker` erweiterten Klassen verwenden. Sie können auch weitere Skripteinbindungen erstellen, um diese Basisklassen zu erweitern und eigene Klassen zu erstellen. Machen Sie sich mit diesen Basisklassen und den darin verfügbaren Methoden vertraut.

Hier geht es los

1. Überprüfen Sie CAPI-APIs, die mit bereitgestellt werden Cloud Provisioning and Governance Standardmäßigan.
2. Überprüfen Sie die CAPI-Klassen, die standardmäßig bereitgestellt werden. Diese Klassen können über die Skripteinbindungen von MID-Server in Ihren CAPI-API-Vorgängen aufgerufen werden.
3. Sehen Sie sich eine Vorstellung der Bereitstellung eines virtuellen Azure-Computers und eines virtuellen AWS-Computers an, um zu sehen, wie die Komponenten zusammenarbeiten. Die exemplarische Vorgehensweise für Azure verwendet eine Skripteinbindung von MID-Server, damit Sie die verschiedenen beim Bereitstellungsvorgang verwendeten CAPI-Klassen einsehen können. Die AWS-Vorstellung verwendet keine Skripteinbindung von MID-Server.
4. Einem vorhandenen Provider in CAPI ein Produkt hinzufügen.
5. Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen.
6. Eine CAPI-Schnittstelle erstellen oder erweitern.
7. Eine CAPI-API erstellen und eine benutzerdefinierte MID-Server-Skripteinbindung, die die REST-Aufrufe beim Cloud-Anbieter ausführt. Für neue CAPI-APIs wird immer eine leere Skripteinbindung von MID-Server generiert. Ändern Sie sie mit den Aufrufen anderer JavaScript-Klassen und -Methoden, z. B. den Methoden in der Aufrufer-Klasse.

Standard-CAPI-APIs

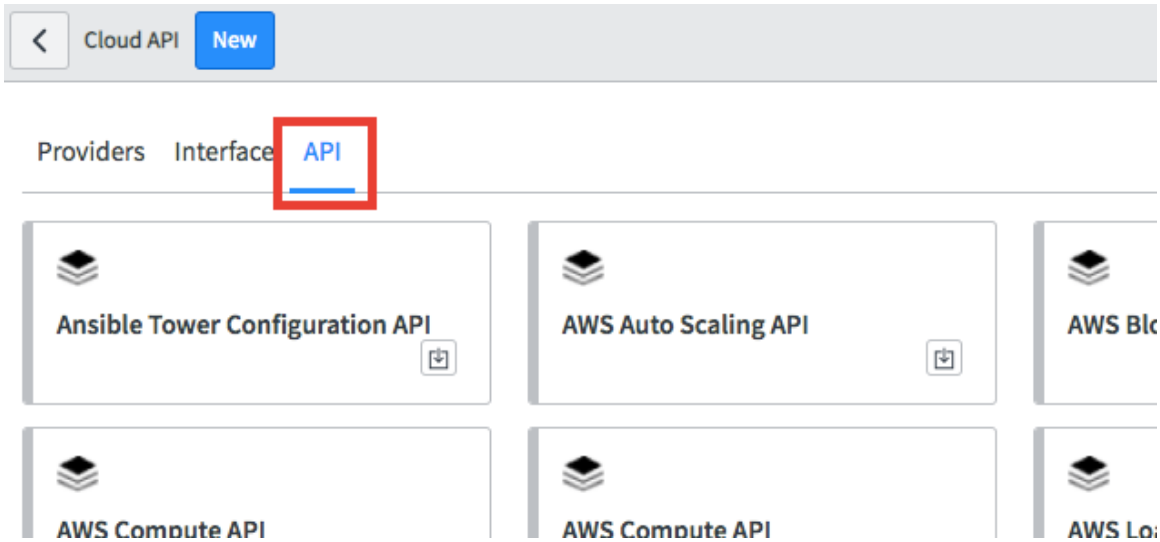
Mit der Anwendung Cloud Provisioning and Governance werden standardmäßig mehrere CAPI-APIs bereitgestellt.

CAPI-APIs beziehen sich auf die API-Datensätze, die ein CAPI-Produkt und eine CAPI-Schnittstelle verknüpfen. Sie verweisen nicht auf die CAPI-*Klassen*, die über Skripteinbindungen von MID-Server in CAPI-APIs aufgerufen werden können. Eine Übersicht über CAPI-Klassen finden Sie unter CAPI-Klassen in MID-Server-Skripteinbindungen.

Zeigen Sie Cloud-APIs an, indem Sie zu navigieren **Cloud-API** > **Bibliothek** In Basissystem Instanzschnittstelle, oder indem Sie zu navigieren **Entwurf** > **Cloud-API** In Portal für Cloud-Admin..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI-APIs



Hinweis: Geskriptete Connectors können Sie mit MID-Server-Skripteinbindungen anpassen.

API	Schnittstelle	Produkt	Geskriptet
Konfigurations-API von Ansible Tower	Schnittstelle zur Konfigurationsverwaltung	Ansible Tower	JA*
Automatisch skalierende AWS-API	Schnittstelle zur automatischen Skalierung	AWS Elastic Compute Cloud	JA*
AWS Blob Storage API	Blob Storage-Schnittstelle	AWS Simple Storage Service	NEIN
AWS Blob Storage API	Blob Storage-Schnittstelle	AWS Elastic Block Storage	NEIN
AWS Compute-API	Compute-Schnittstelle	AWS Elastic Compute Cloud	NEIN
AWS Compute-API	Compute-Schnittstelle	AWS Elastic Compute Cloud	JA*
AWS Load Balancer API	Load Balancer-Schnittstelle	AWS Elastic Load Balancer	NEIN
AWS-Netzwerk-API	Netzwerkschnittstelle	AWS Virtual Private Cloud	NEIN
AWS Stack Orchestration API	Stack-Orchestrierungsschnittstelle	AWS CloudFormation	JA*
Azure-Warnungs-API	Event-Schnittstelle	Azure-Warnung	JA*
Azure Blob Storage API	Blob Storage-Schnittstelle	Microsoft.Storage	JA*
Azure Block Storage API	Blob Storage-Schnittstelle	Microsoft.BlockStorage	JA*
Azure Compute-API	Compute-Schnittstelle	Microsoft.Compute	JA*
Azure-Erweiterungen-API	Azure-Erweiterungsschnittstelle	Microsoft.Compute	JA*
Azure Load Balancer API	Load Balancer-Schnittstelle	Microsoft.LoadBalancer	JA*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API	Schnittstelle	Produkt	Geskriptet
Azure-Netzwerk-API	Netzwerkschnittstelle	Microsoft.Network	JA*
Azure Stack Orchestration API	Stack-Orchestrierungsschnittstelle	Azure ARM	JA*
Infoblox IPAM-API	IPAM-Schnittstelle	Infoblox	NEIN
ServiceNow Store IPAM-API	IPAM-Schnittstelle	ServiceNow	JA*
SSH-API	SSH-Schnittstelle	SSH	NEIN
vSphere Block Storage-API	Blob Storage-Schnittstelle	VMware VDisk	NEIN
vSphere Compute-API	Compute-Schnittstelle	VMware vSphere	NEIN

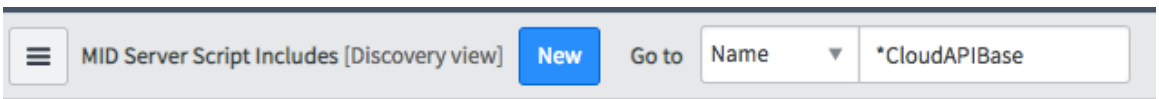
* Sie können anpassen, wie geskriptete APIs REST-Aufrufe an den Cloud-Anbieter tätigen.

CAPI-Klassen in MID-Server-Skripteinbindungen

Cloud Provisioning and Governance bietet mehrere JavaScript-Klassen, die REST-Aufrufe an Cloud-Anbieter durchführen. Diese Klassen werden von MID-Server-Skripteinbindungen (standardmäßig für Azure) oder von Java-Aufrufen im System (standardmäßig für AWS) aufgerufen. Wenn Sie benutzerdefinierte Anbieter, Schnittstellen oder CAPI-APIs (für alle Cloud-Anbieter) erstellen, können Sie die MID-Server-Skripteinbindungen zum Aufrufen der Klassen verwenden.

Hinweis: In CAPI-APIs gibt es keine MID-Server-Skripteinbindungen (in Methodenzuordnungen), die Sie anpassen können, um die AWS-Klassen aufzurufen. Standardmäßig führen die CAPI-APIs für AWS Java-Aufrufe durch, um dann die AWS-Klassen aufzurufen. Wenn Sie jedoch CAPI-APIs erstellen, können Sie auch benutzerdefinierte Skripteinbindungen zum Aufrufen der Klassen erstellen.

Zeigen Sie CAPI-Klassen an, indem Sie zu navigieren **MID-Server** > **Skripteinbindungen** In Basissystem Instanzschnittstelle (nicht die Portal für Cloud-Admin.). Den Namen einer Klasse suchen Sie im Suchfeld **Go to** (Wechseln zu) über die Spalte **Name**:



Basisklassen

Die folgenden Basisklassen sind standardmäßig verfügbar. Sie bilden eine Grundlage für die Azure- und AWS-Klassen, die die tatsächlichen REST-Aufrufe vornehmen.

CloudAPIBase

CloudAPIBase ist eine anbieterunabhängige API, die mit allen Arten von Cloud-APIs kommuniziert. Sie bietet Funktionen für das grundlegende Debugging und die Protokollierung sowie für das Sammeln von Proxyinformationen auf MID-Server. Darüber hinaus definiert sie Header, Parameter, Endpunkte und this.parameter.

AWSCloudAPIBase

Diese Klasse wurde von CloudAPIBase erweitert und bietet Funktionen, die den Aufrufer auffordern, GET-, PUT-, POST- und DELETE-Anforderungen zu stellen. Die Klasse bietet die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option einer `executeAction`-Methode, die eine AWS-Implementierung von GET ist, oder der invoke-Methode, die REST API-Aufrufe bereitstellt.

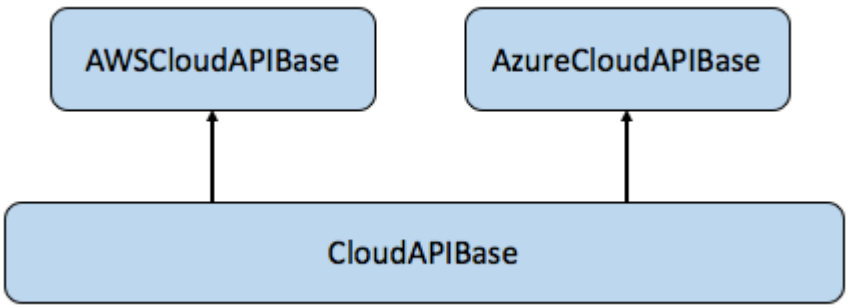
AzureCloudAPIBase

Diese Klasse wurde von CloudAPIBase erweitert und bietet Funktionen für die folgenden Aktionen:

- Ressourcen-IDs abrufen
- Endpunkteigenschaften abrufen
- Ressourcen auflisten
- Den Aufrufer aufrufen, GET-, PUT-, POST- und DELETE-Anforderungen zu senden.

AzureCloudAPIBase verwendet die Methode `_invokeRequest`, um REST API-Aufrufe an Azure mithilfe der Standard-REST API-Aufrufe zu tätigen.

Basis-APIs



Aufrufende Klassen

Aufruferklassen führen die tatsächlichen REST-Aufrufe an den Cloud-Anbieter durch. Wenn Sie benutzerdefinierte CAPI-Schnittstellen und APIs erstellen, sollten Sie *`CloudRestAPIInvoker`* erweitern, wenn Sie REST-Aufrufe erstellen möchten.

CloudRestAPIInvoker

Diese Klasse ist eine abstrahierte Klasse für REST API-Aufrufe. Wenn Header und/oder Parameter vorhanden sind, die mit einer Anforderung gesendet werden sollen, müssen Klassen, die den Aufrufer implementieren, dieses Objekt erweitern. Sie müssen auch Überschreibungen für *`getEndpointUrl`* bereitstellen, um den Zielendpunkt auszugeben, sowie für *`getHeaders`* und *`getParameters`*. Bei Azure REST APIs erfordert die Authentifizierung beispielsweise die Übergabe eines Tokens als Header. Die Erweiterung, die dies implementiert, sollte eine Antwort von *`getHeaders`* bereitstellen, die die Erstellung oder den Abruf des Tokens durchführt und dies festlegt. Dieses Basisobjekt ruft *`getHeaders`* auf und sendet alles, was auf die Anforderung zurückgegeben wird. Diese Klasse stellt auch eine *`getResponse`* -Methode für die Behandlung der Antwort des Cloud-Anbieters bereit.

Wenn Sie eine benutzerdefinierte CAPI-API erstellen, sollten Sie *`CloudRestAPIInvoker`* erweitern, um REST-Aufrufe an den Cloud-Provider zu tätigen.

AmazonWebServicesAPIInvoker

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Klasse wurde von `CloudRestAPIInvoker` erweitert und stellt Methoden für REST API-Aufrufe an den Cloud-Anbieter bereit.

AzureAPIInvoker

Diese Klasse wurde von `CloudRestAPIInvoker` erweitert und bietet Funktionen, die die folgenden REST API-Aufrufe an Azure Resource Manager vornehmen:

- Legt Dienstprinzipal, Header und Parameter für REST-Aufrufe fest.
- Ruft Endpunkt-URL, Token (Client-ID, Mandanten-ID und geheime Schlüssel) sowie Header/Parameter ab.
- Ruft den JSON-Antworttextkörper vom Cloud-Anbieter ab und decodiert ihn.

AzureEAAPIInvoker

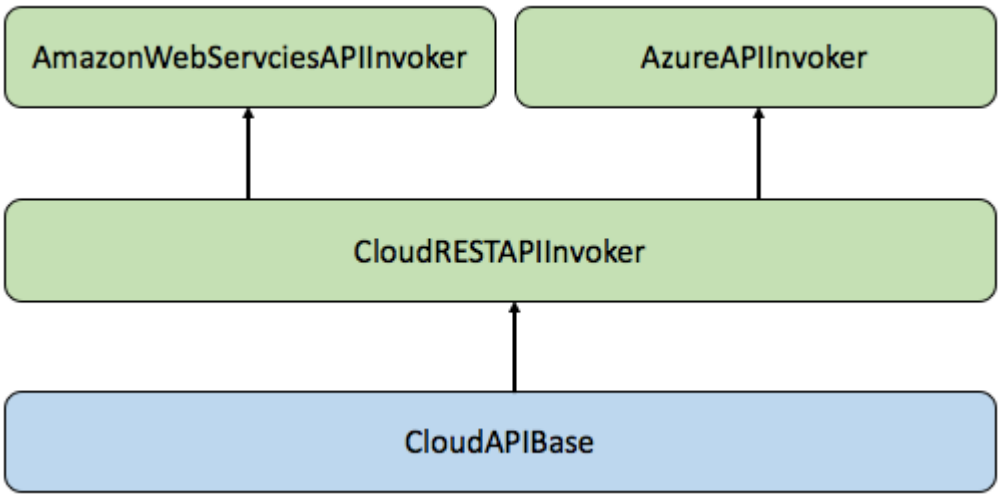
Diese Klasse gibt das Token für den Zugriff auf die REST API von Azure Enterprise Agreement (EA) zurück.

AzureStorageAPIInvoker

Diese Klasse führt REST-Aufrufe für Azure-Speicher durch. Die Funktionen in dieser Klasse können Token, Antwort, Header und Parameter abrufen.

Diese Grafik zeigt, wie die Basisklassen zur Erweiterung von AWS-spezifischen und Azure-spezifischen Klassen verwendet werden:

REST-Aufrufe werden aufgerufen



Ausnahmen

RESTAPIException

Diese Basisklasse behandelt Ausnahmen, die während des REST-Aufrufs auftreten können. Sie gibt den Antwortcode vom Cloud-Provider zurück.

AWSAPIException

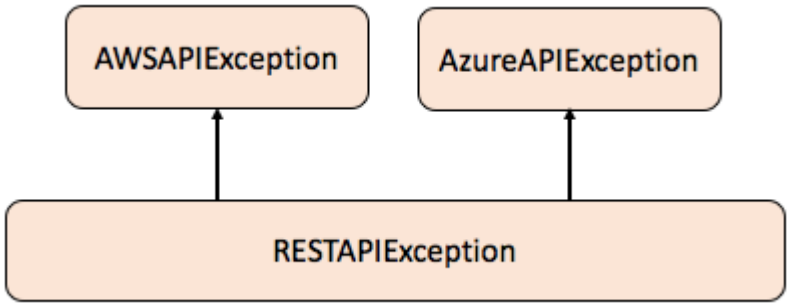
Diese Klasse behandelt Ausnahmen, die während des REST-Aufrufs auftreten können.

AzureAPIException

Diese Klasse löst bei Bedarf während des Aufrufs der Azure-API eine Laufzeitausnahme aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Handhabung von Ausnahmen



Klassen für Anmeldeinformationen

CloudRESTRequestSigningUtil

Diese Klasse verwendet Überschreibungen, die in CAPI-API-Konfigurationsüberschreibungen angegeben sind. Die Klasse *`AmazonWebServicesRequestSigner`* erweitert diese Klasse. Für Azure sind viele Signierer in die Skripteinbindungen von MID-Server für Methodenzuordnungen in Azure-CAPI-APIs integriert.

AmazonWebServicesRequestSigner

Diese Klasse richtet eine sichere Sitzung für den REST API-Aufruf ein, indem Informationen zu einer Anforderung abgerufen und eine Zeichenfolge mit signature v4- -Signatur für die Anforderung erstellt wird. Diese Klasse wird von CloudRESTRequestSigningUtil erweitert.

Andere Azure-Klassen

Klassen, die AzureCloudAPIBase erweitern

Klasse	Beschreibung
AzureAlertRule	Klasse zum Erstellen und Löschen von Azure-Warnungsregeln.
AzureAuthorizationPolicy	Klasse zum Zuweisen von Tag-Richtlinien.
AzureComputeAvailabilitySet	Klasse für das Abrufen von Azure-Verfügbarkeitssätzen. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/availabilitysets
AzureComputeHardware	Klasse zum Abrufen von Azure-Größen. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinesizes
AzureComputeImage	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Bildern. Siehe: https://docs.microsoft.com/en-us/rest/api/manageddisks/images/images-rest-api
AzureComputeVirtualMachine	Klasse für die Verarbeitung von Azure-API-Aufrufen zu virtuellen Computern. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/virtualmachines VM-Größen und -Kapazitäten: https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-sizes https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-linux-sizes Von Cloud-Init unterstützte Versionen: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/using-cloud-init
AzureDeployment	Klasse für die Azure ARM-Vorlagenbereitstellung.
AzureDeploymentOperation	Klasse für den Betrieb der Azure ARM-Vorlagenbereitstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassen, die AzureCloudAPIBase erweitern (Fortsetzung)

Klasse	Beschreibung
AzureImages	Klasse für die Verarbeitung von Azure-Bildern.
AzureLoadBalancer	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Lastenausgleichsmodulen. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163651.aspx
AzureLocalNetworkGateways	Klasse zum Erstellen und Abrufen von Gateways für lokale Netzwerke.
AzureNetworkNIC	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Netzwerkschnittstellen-Karten. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163579.aspx
AzureNetworkPublicIP	Klasse für die Verarbeitung von Azure-API-Aufrufen zu öffentlichen IP-Adressen. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163638.aspx
AzureNetworkRouter	Klasse für die Verarbeitung von Azure-API-Aufrufen zur Routingtabelle. Siehe: https://docs.microsoft.com/en-us/rest/api/network/route-tables
AzureNetworkSecurityGroup	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Netzwerkschnittstellen-Karten. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163579.aspx
AzureNetworkVirtualNetwork	Klasse für die Verarbeitung von Azure-API-Aufrufen zu virtuellen Netzwerken.
AzureProvider	Klasse zum Abrufen von Azure-Anbieterdetails, wie Anbieter-URL und Version.
AzureRegion	Klasse zum Abrufen von Azure-Regionen.
AzureResource	Behandelt das Objekt, auf das ObjectID in den Parametern verweist. Außerdem wird die API-Version abgerufen. Diese Klasse ist hauptsächlich zum Abrufen nicht unterstützter Typen oder zum Löschen von Ressourcen gedacht.
AzureResourceGroupManager	Klasse für die Verarbeitung von Azure ARM-Ressourcengruppen.
AzureResponseUtil	Klasse zum Übersetzen der Azure-API-Antwort in ein DTO-Objekt.
AzureStorageAccount	Klasse für die Verarbeitung von Azure-API-Aufrufen zum Speicherkonto. Siehe: //https://msdn.microsoft.com/en-us/library/azure/mt163638.aspx
AzureStorageBlob	Klasse zum Erstellen und Bearbeiten von Speichercontainern und Blobs.
AzureStorageManagedDisk	Klasse für die Verarbeitung von Azure-API-Aufrufen zum verwalteten Datenträger. Siehe: https://docs.microsoft.com/en-us/rest/api/manageddisks/disks/disks-create-or-update
AzureSubscription	Klasse zum Abrufen von Azure-Abonnements.
AzureVirtualNetworkGateways	Klasse zum Erstellen und Bearbeiten von Gateways für virtuelle Netzwerke.
AzureCloudEAAPIBase	Basisobjekt für Azure EA-API-Handler. Azure EA-APIs haben die Basis-URL https://consumption.azure.com und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassen, die AzureCloudAPIBase erweitern (Fortsetzung)

Klasse	Beschreibung
	erfordern die Registrierungsnummer im Pfad. Diese Klasse verarbeitet das Aktivieren der Parameter „EnrollmentNumber“ und „EnrollmentToken“.

Andere AWS-Klassen

Klasse	Beschreibung
AmazonImages	Klasse für die Verarbeitung von Amazon Computerimages. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html
AmazonResponseProcessorUtil	Klasse für die Verarbeitung der AWS REST API-Antwort.
AWSAutoScalingGroups	Klasse für die Verarbeitung von AWS API-Aufrufen zum Erstellen und Bearbeiten von Autoskalierungsgruppen .
AWSCloudFormation	Handler für AWS CloudFormation-API-Aufrufe.
AWSEC2	Handler für AWS EC2 API-Aufrufe.
AWSKeyValuePair	Klasse zum Importieren und Bearbeiten von Schlüsselpaaren.
AWSLaunchConfigurations	Hilfsklasse.
AWSS3	Handler für AWS S3 API-Aufrufe.
AWSTopics	Klasse mit AWS-Themen .

Azure VM-Bereitstellung – exemplarische Vorstellung

Dieses Beispiel führt Sie durch die Komponenten von Cloud Provisioning and Governance, die während der Bereitstellung eines virtuellen Computers in einem Azure-Rechenzentrum in Betrieb sind. Zu den behandelten Themen gehören Blaupausen, Ressourcenblöcke, die Cloud-API (CAPI) und Skripteinbindungen MID-Server.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Diese erläuternde Vorstellung beginnt mit einer Linux-VM, die ein Benutzer bereits in Azure bereitgestellt hat. Anschließend werden Ihnen die Blaupause mit der VM, den Ressourcenblöcken und den in den Ressourcenblöcken angegebenen CAPI-Aufrufen vorgesellt. Abschließend zeigt Ihnen die Vorführung, wie eine MID-Server-Skripteinbindung über mehrere CAPI-Aufrufe die tatsächlichen REST-Aufrufe an die Azure-API durchführt.

In diesem Beispiel werden Standardressourcenblocks und Skript Includes verwendet, die in Ihrer Instanz verfügbar sind. Deshalb können Sie, obwohl Sie möglicherweise keine bereitgestellte VM auf Ihrer Instanz haben, trotzdem diese Schritte befolgen und die in diesem Beispiel verwendeten Komponenten anzeigen, um die Arbeitsweise der Komponenten zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel für einen virtuellen Computer in AWS finden Sie unter VM-Bereitstellung bei AWS – Beispiel-Vorstellung.

Hinweis: Die Begriffe *virtueller Computer*, *VM* (für „Virtual Machine“) und *virtueller Server* sind in diesem Beispiel synonym.

Prozedur

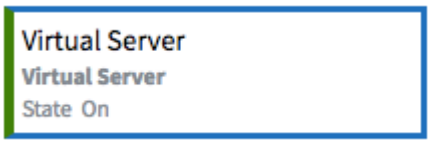
1. Betrachten Sie eine eingerichtete VM im Cloud User Portal und richten Sie den Fokus auf einige Details zur VM:

   a. In Basissystem Instanzschnittstelle öffnen Cloudbenutzerportal(**Cloud-Anwenderportal**) an.

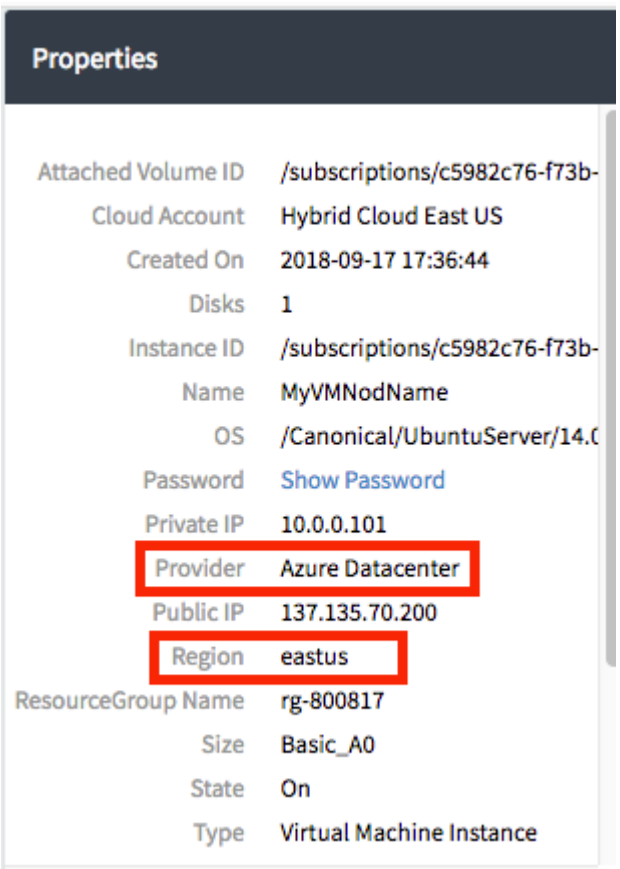
   b. Rufen Sie auf Cloudbenutzerportal eine bereitgestellte VM in einem Stapel auf, z. B. diese VM, indem Sie auf **Stapel** und dann auf den Namen des Stapels klicken.

      In diesem Beispiel heißt der Stapel **MyAzureVM**.

   c. Klicken Sie unter **Resources**(Ressourcen) auf den virtuellen Computer im Stapel.



   d. Rufen Sie die Eigenschaften der VM auf; beachten Sie, dass sie sich in einem **Azure-Rechenzentrum** in der Region **Eastus** befindet.



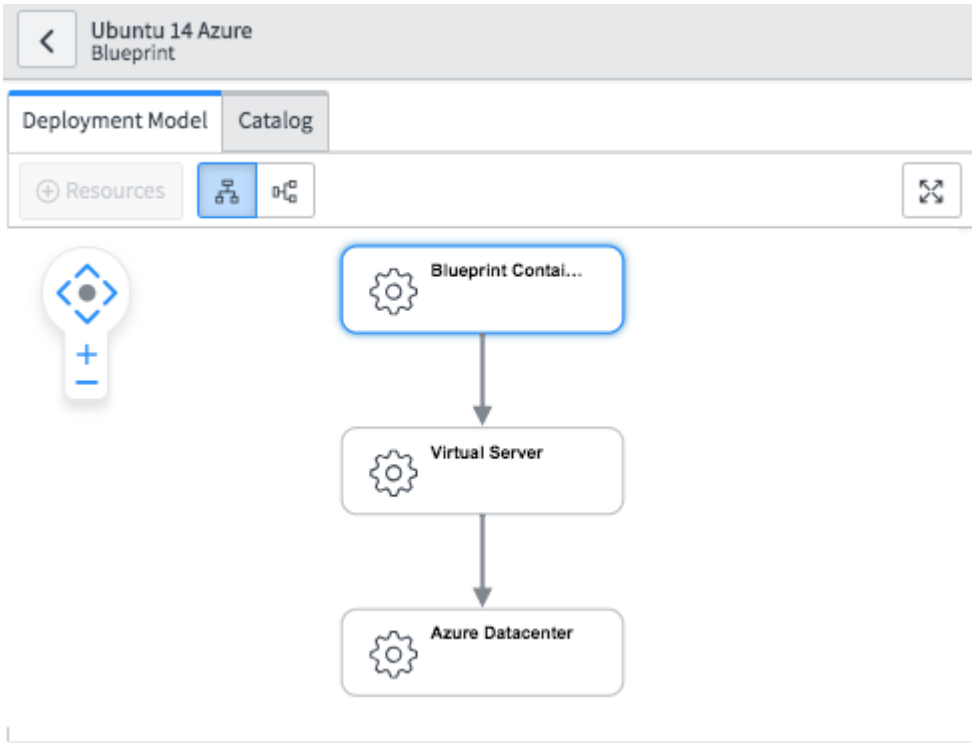
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

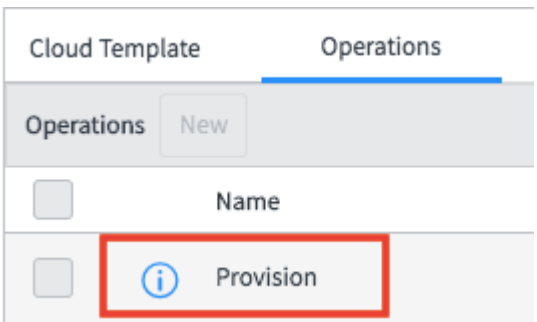
2. Sehen Sie sich die Blaupause an, auf der die VM basiert:

a. Navigieren zu **Entwurf** > **Blueprints**, Und öffnen Sie dann einen Blueprint mit einem virtuellen Server im Azure-Rechenzentrum. Die **Bereitstellungsmodell** Standardmäßig wird die Registerkarte angezeigt, die Ihnen die verschiedenen Komponenten des Blueprints anzeigt.

Diese Beispiel-Blaupause hat drei Komponenten: den Container, den virtuellen Server, der die bereitgestellte VM ist, und das Azure-Rechenzentrum.



b. Klicken Sie unten auf die Registerkarte **Vorgänge** und dann auf **Bereitstellung**.

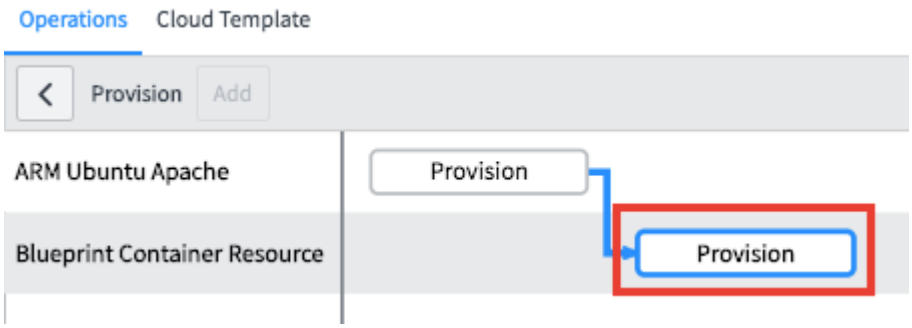


Der Bereitstellungsvorgang ist der Vorgang, den das System beim Erstellen der VM ausgelöst hat. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

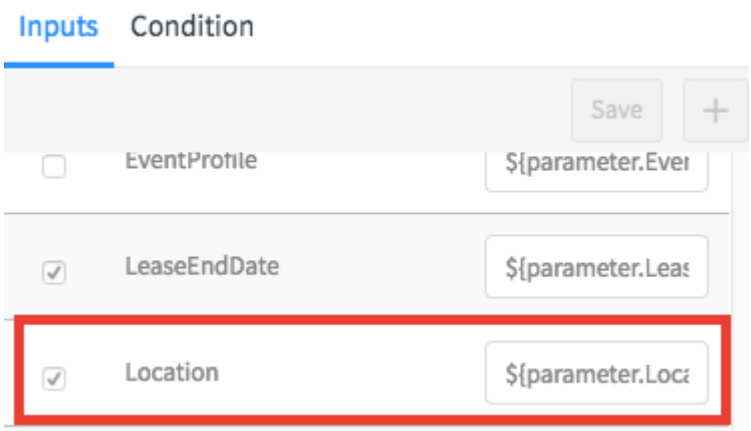
c. Klicken Sie auf den Block **Bereitstellung** für die Container-Ressource der Blaupause.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Beachten Sie, dass einer der Parameter auf der rechten Seite in der Inputs-Liste „Location“ lautet. Dieser Parameter speichert den Statuswert, der aussagt, wo die VM im Datencenter lebt.

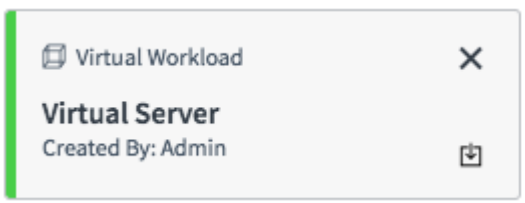


Eingaben können auf Container-Ebene festgelegt werden, wie in diesem Beispiel, oder auf einem beliebigen anderen Ressourcenblock. Standardmäßig ist der *Location*-Parameter bereits für Sie im Blaupause-Container-Ressourcenblock festgelegt, sodass Sie ihn in jeder Blaupause wie dieser verwenden können. Wenn Sie den Status der Blaupause auf **Entwurf** wechseln, können Sie dem Container-Ressourcenblock der Blaupause weitere Parameter hinzufügen. Dem Ressourcenblock des virtuellen Servers können Sie keine Parameter hinzufügen. Für diese Anleitung werden keine weiteren Parameter benötigt.

3. Betrachten Sie die Ressourcenblöcke des virtuellen Servers und des Azure-Rechenzentrums, die in dieser Blaupause verwendet werden:

a. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Ressourcenblöcke**an.

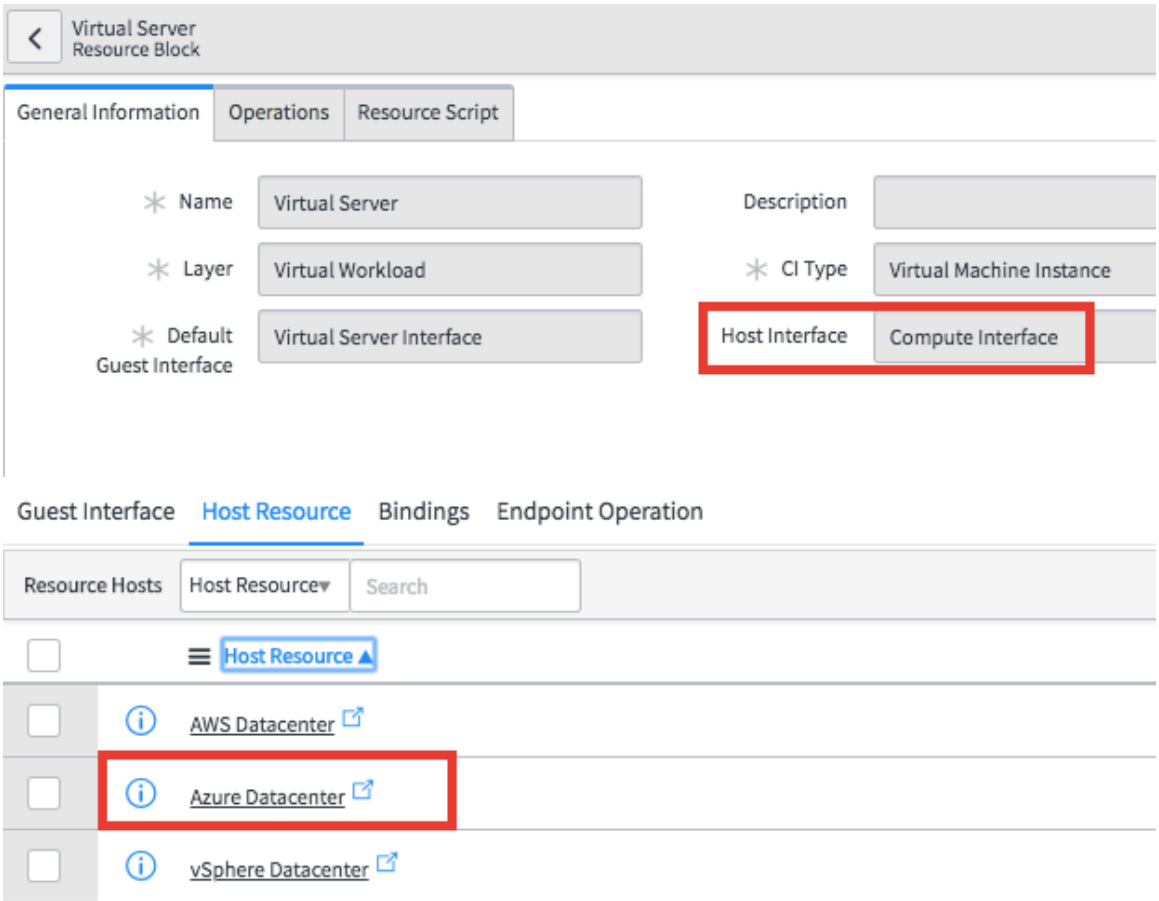
b. Suchen und öffnen Sie den Ressourcenblock **Virtueller Server**, der standardmäßig mit Cloud Provisioning and Governance bereitgestellt wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie im Ressourcenblock-Formular auf die zugehörige Liste **Hostressource**, um die Liste der unterstützten Host-Ressourcenblöcke anzuzeigen.

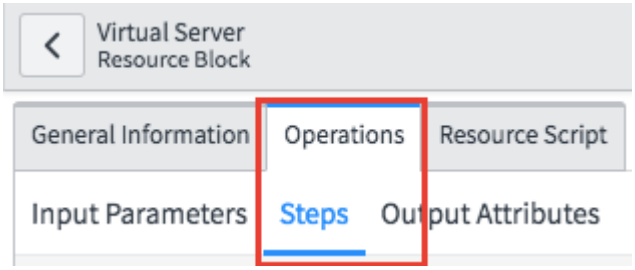
d. Beachten Sie die Host-Schnittstelle und die Host-Ressource, die bereits angegeben wurden:



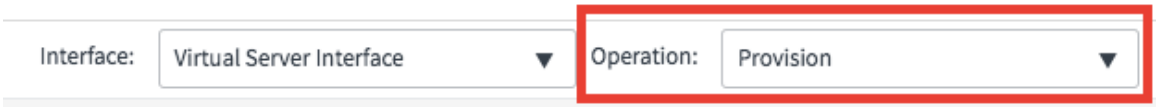
- Das Feld **Host Interface** (Host-Schnittstelle) gibt die Schnittstelle an, die mit der Gastschnittstelle im Ressourcenblock, der den virtuellen Computer hostet, übereinstimmen muss. In diesem Fall ist die Host-Schnittstelle die Compute-Schnittstelle, die auch die Gastschnittstelle auf dem Azure Datacenter-Ressourcenblock ist. Standardmäßig stellt der Rechenzentrum-Ressourcenblock mehrere Gastschnittstellen bereit, über die sich andere Ressourcenblöcke mit dem Datacenter verbinden können, beispielsweise der virtuelle Speicher.
- Die Spalte **HostResource** in der zugehörigen Liste **Host Resource** (Host-Ressource) gibt bereits **Azure Datacenter** (Azure-Rechenzentrum) an, was bedeutet, dass der Azure-Rechenzentrum-Ressourcenblock ein gültiger Host für diese VM ist.

e. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

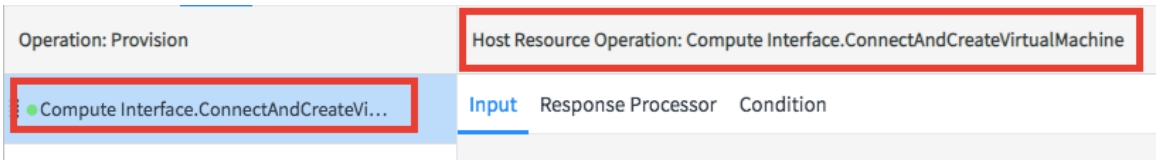


f. Wählen Sie in der Liste **Vorgang** die Option **Bereitstellung** aus.



Denken Sie daran, dass es der Bereitstellungsvorgang ist, mit dem das System die VM erstellt. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

g. Beachten Sie den Schritt, der in der Liste angezeigt wird, und die vollständige Schrittbeschreibung, die über den Eingabeparametern angezeigt wird:



(Schritt für Bereitstellung)

- **Host Resource Operation:** (Hostressourcenvorgang) gibt an, dass dieser Schritt einen Vorgang für die Hostressource (das Azure-Rechenzentrum in diesem Beispiel) aufruft.
- **Compute Interface** (Compute-Schnittstelle) ist die Gastschnittstelle im Azure-Rechenzentrum, die dieser Schritt verwendet.
- **ConnectAndCreateVirtualMachine** ist der Vorgang im Azure-Rechenzentrum, den dieser Schritt aufruft.

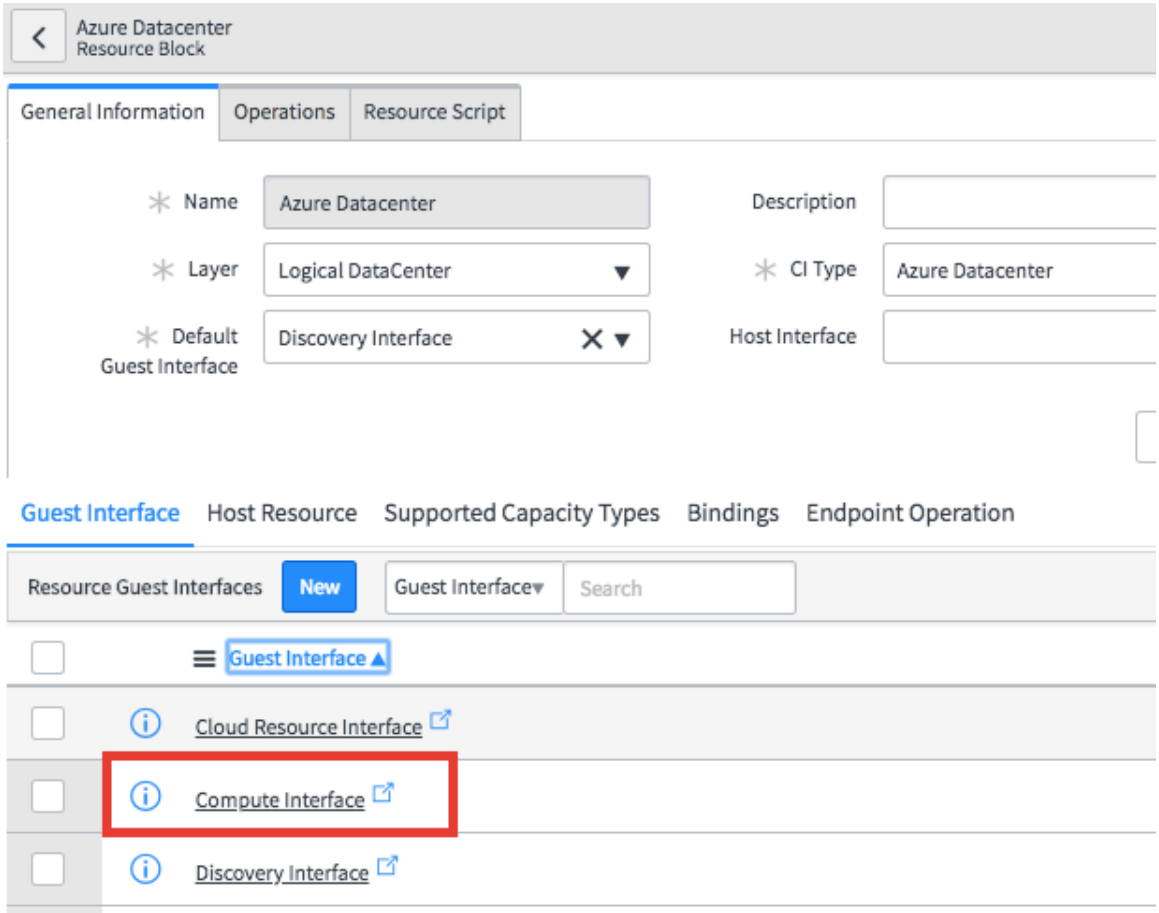
Hinweis: In diesem Fall ruft der Schritt einen Vorgang von einem anderen Ressourcenblock auf: dem Azure-Rechenzentrum. Schritte können CAPI auch direkt aufrufen, und dann kann CAPI REST-Aufrufe an die Cloud-Provider-API ausführen. Das sehen Sie, wenn Sie sich den Ressourcenblock des Azure-Rechenzentrums ansehen.

h. Navigieren Sie zurück zu **Entwurf** > **Ressourcenblöcke**an.

i. Öffnen Sie den Ressourcenblock **Azure Datacenter** (Azure-Rechenzentrum), der den Host-Ressourcenblock darstellt, mit dem der virtuelle Server verbunden ist.

j. Beachten Sie die unterstützten Gastschnittstellen in der zugehörigen Liste **Guest Interface** (Gastschnittstelle):

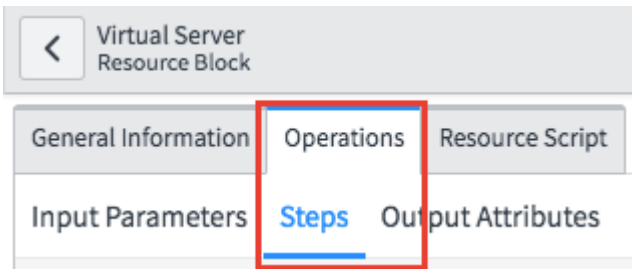
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



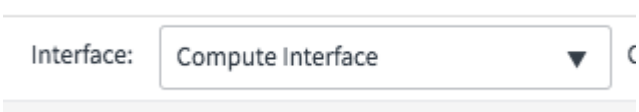
(Azure-Rechenzentrum mit Compute-API)

Diese Gastschnittstellen sind die Schnittstellen, die das Azure-Rechenzentrum anderen Ressourcenblöcken zur Verfügung stellt. Die Option **Compute Interface** (Compute-Schnittstelle) wird bereitgestellt, damit der Ressourcenblock des virtuellen Servers, der die Compute-Schnittstelle als Host-Schnittstelle angibt, eine Verbindung zum Rechenzentrum herstellen kann.

k. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



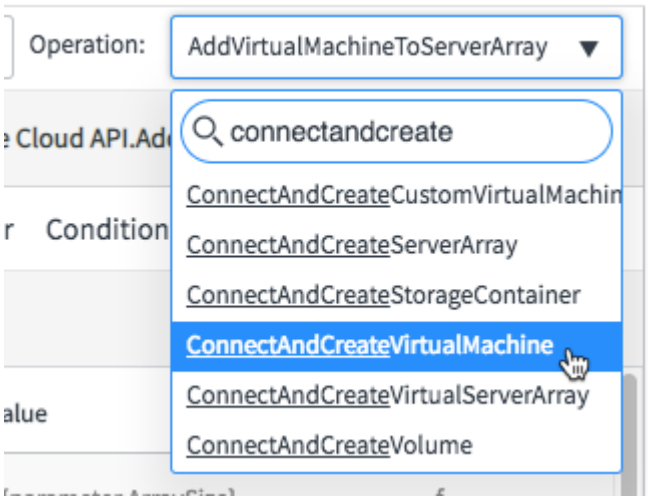
l. Wählen Sie in der Liste **Interface** (Schnittstelle) die Option **Compute Interface** (Compute-Schnittstelle) aus, wenn sie nicht bereits ausgewählt ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

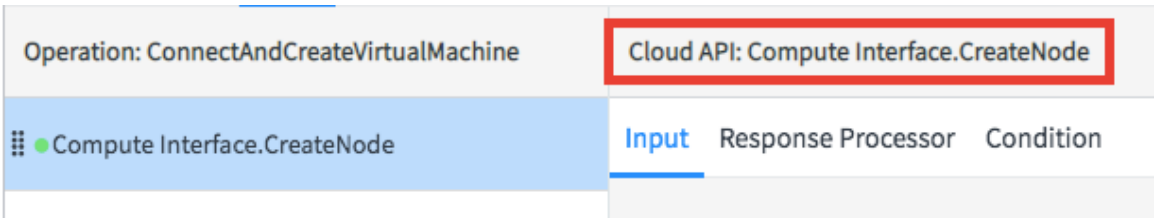
Denken Sie daran, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

m. Suchen Sie in der Liste **Operation** (Vorgang) die Option **ConnectAndCreateVirtualMachine** und wählen Sie sie aus.



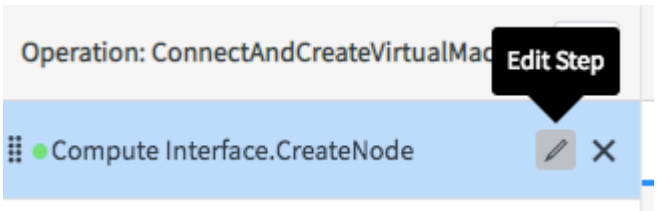
Dabei ist zu berücksichtigen, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

n. Zu beachten ist der CAPI-Aufruf, der im einzigen Schritt für den Vorgang „ConnectAndCreateVirtualMachine“ verwendet wird:



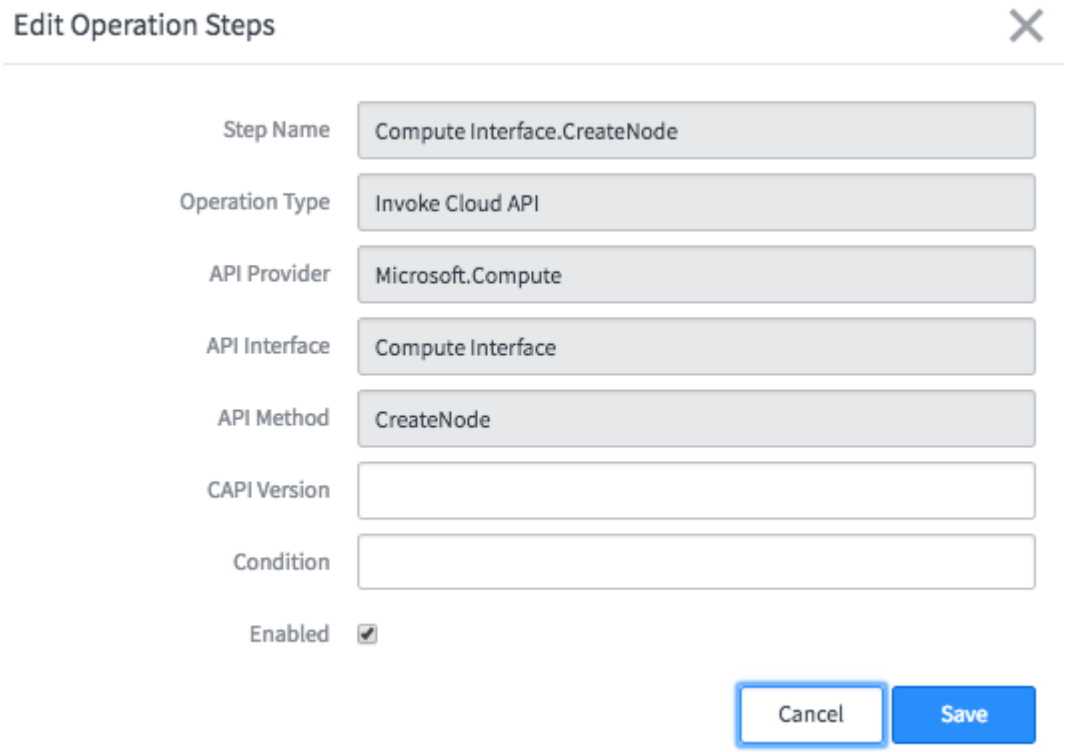
- **Cloud API:** (Cloud-API) Gibt an, dass dieser Schritt CAPI aufruft, sodass CAPI einen REST-Aufruf an den Cloud-Anbieter ausführen kann, der in diesem Fall Azure ist.
- **Compute Interface** (Compute-Schnittstelle) gibt die CAPI-Schnittstelle vor, die von diesem Schritt aufgerufen wird.
- **CreateNode** gibt die Methode an, die ausgeführt wird. Wie der Name schon sagt, weist diese Methode den Cloud-Anbieter an, den virtuellen Computer zu erstellen.

o. So öffnen Sie die Schrittkonfiguration: Der Ressourcenblock muss den Status **Draft** (Entwurf) aufweisen. Zeigen Sie dann auf den hervorgehobenen (blauen) Schritt, und klicken Sie auf das Symbol **Edit Step** (Schritt bearbeiten).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

p. Sehen Sie sich die Schrittkonfiguration an, und hier insbesondere die Einstellungen, die in CAPI integriert werden:



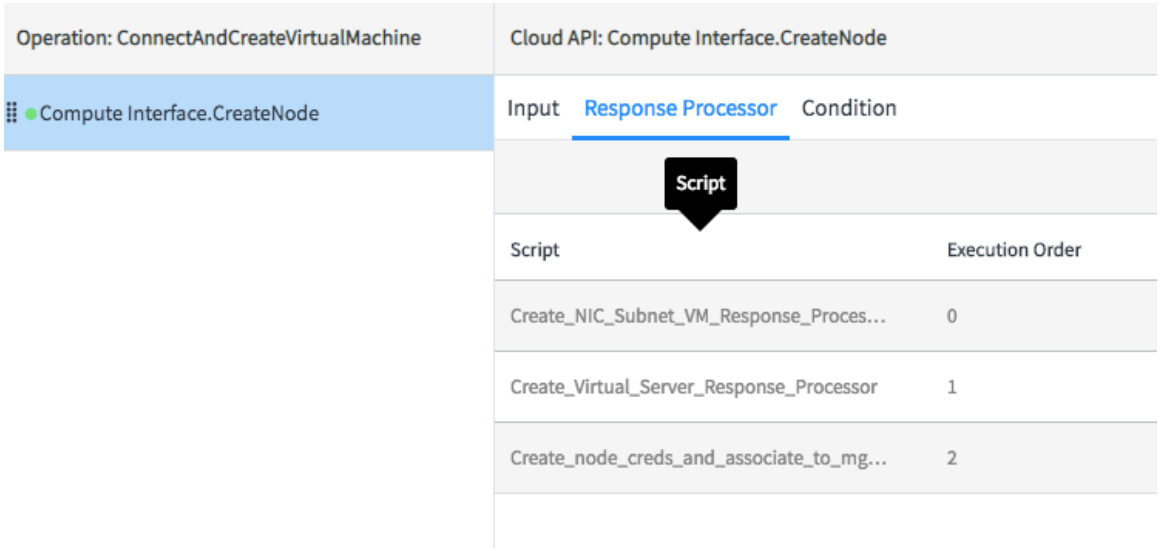
Feld	Beschreibung
Vorgangstyp	**Invoke Cloud API** (Cloud-API aufrufen) gibt an, dass dieser Schritt die CAPI über den angegebenen Anbieter, die angegebene Schnittstelle und die angegebene Methode aufrufen soll.
API-Anbieter (der eigentlich das Produkt ist)	**Microsoft.Compute** ist ein Produkt (nicht der tatsächliche Anbieter), das zum Azure-Anbieter gemäß der Definition in CAPI gehört.
API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist ein Produkt, das zum Azure-Anbieter gemäß der Definition in CAPI gehört.
API-Methode	**CreateNode** ist die Methode, die Azure zum Erstellen der VM aufruft.

Hinweis: Die CAPI-API-Definition verbindet den Anbieter (Azure), das Produkt (Microsoft.Compute), die Schnittstelle (Compute Interface) und die Methode (CreateNode).

q. Schließen Sie das Fenster.

r. Klicken Sie bei ausgewähltem Schritt **Compute Interface.CreateNode** auf **Response Processor** (Antwortprozessor); beachten Sie dabei das Skript **Create_Virtual_Server_Response_Processor**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Skript ist der Antwortprozessor, der die CMDB in Ihrer Instanz aktualisiert, nachdem der virtuelle Computer erstellt wurde.

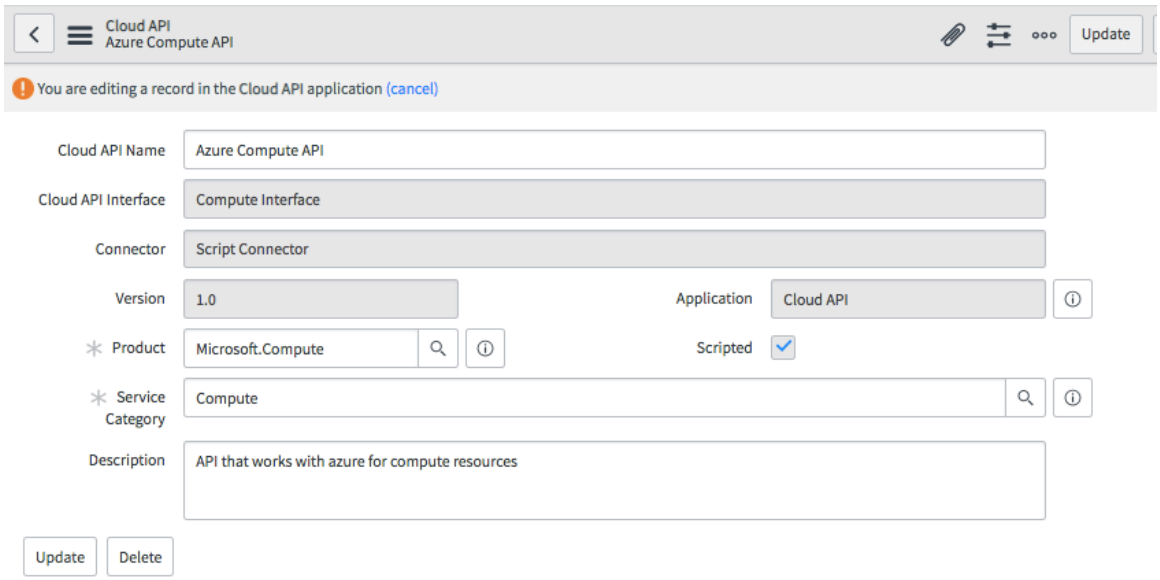
s. Zeigen Sie eine Erklärung des Skripts und das Beispiel an, das Teil des Themas ist Erstellen Sie einen Antwortprozessor .
Wenn Sie die Überprüfung von diesem Themas abgeschlossen haben, kehren Sie zu diesem Thema zurück.

4. Sehen Sie sich die CAPI-Komponenten an, die zusammenarbeiten, um den virtuellen Computer bereitzustellen:

a. Navigieren Sie im Cloud-Administratorportal zu **Entwurf** > **Cloud-API**an.

b. Klicken Sie auf die Registerkarte **API** und suchen Sie dann nach einer offenen **Azure Compute-API**.

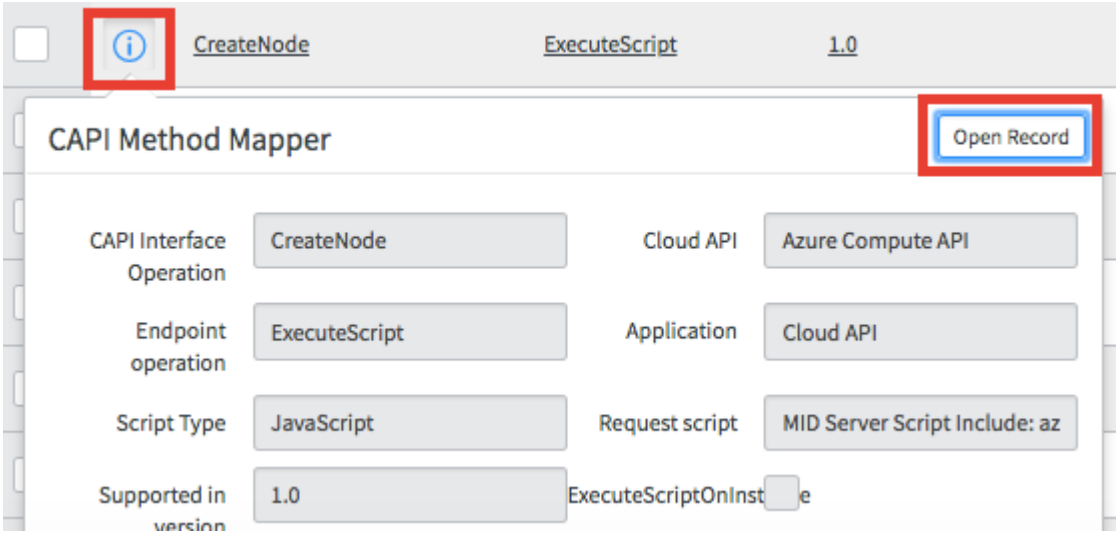
c. Sehen Sie sich an, wie diese CAPI-API eine *Schnittstelle* und ein *Produkt* miteinander verknüpft:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

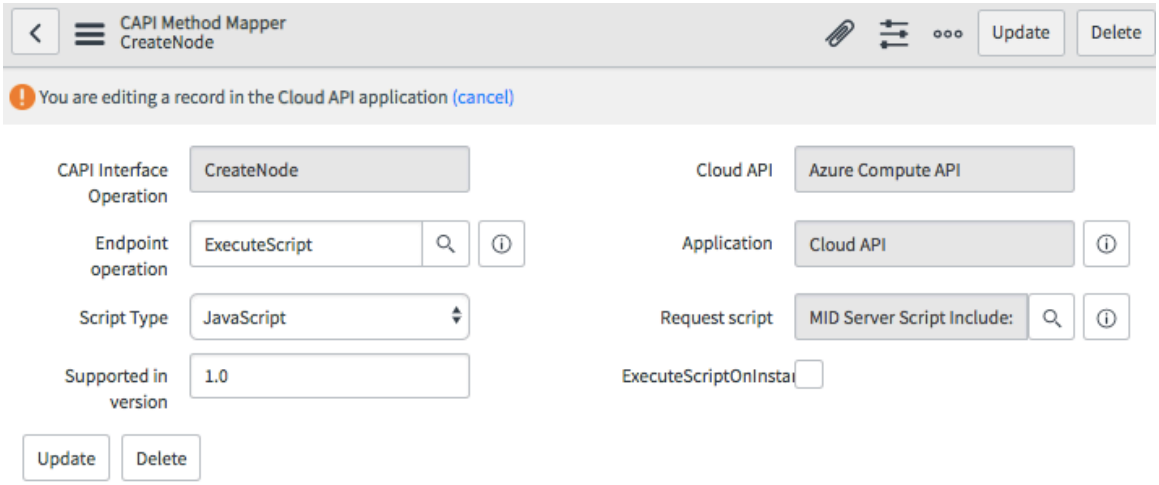
Feld	Beschreibung
Cloud-API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist die gleiche Schnittstelle, die im Ressourcenblock angegeben ist. Die Schnittstelle enthält die Definition für Methoden, einschließlich der Methode `CreateStack`.
Connector	**Script Connector** (Script-Connector) gibt an, dass diese CAPI eine Skripteinbindung MID-Server für jeden Vorgang bereitstellt. Die Skripteinbindung ruft die API auf. Sie können die Skripteinbindung ändern oder sogar eine neue erstellen.
Version	**1.0** gibt die Version der API an. Sie können über mehrere Versionen dieser API mit unterschiedlichen Versionsnummern verfügen. Beachten Sie, dass im Schritt im Ressourcenblock für das Rechenzentrum, den der virtuellen Computer erstellt, ein Versionsfeld bereitgestellt wird. Obwohl dieses Feld im Beispiel leer war, da nur eine Version dieser API vorhanden ist, können Sie eine andere Versionsnummer angeben.
Produkt	**Microsoft.Compute** ist das Produkt, das zum Anbieter in CAPI gehört. Dieses Produkt wird standardmäßig mit Cloud Provisioning and Governance geliefert und ist eines der am häufigsten verwendeten Produkte zum Erstellen virtueller Computer in Azure.

d. Klicken Sie in der zugehörigen Liste „CAPI Method Mappers“ (CAPI-Methodenzuordnungen) auf das Symbol für die Datensatzvorschau für den Datensatz `CreateNode`, und klicken Sie dann auf **Open Record** (Datensatz öffnen).



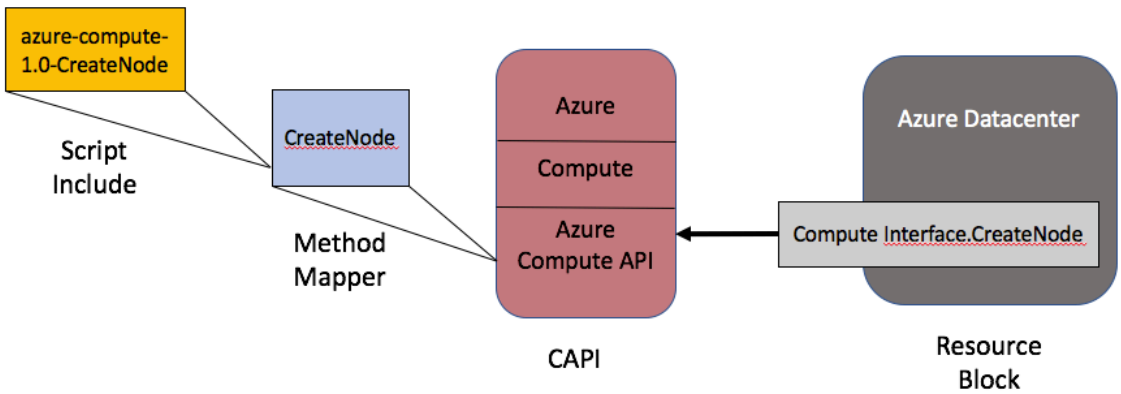
e. Sehen Sie sich die Methodenzuordnung für `CreateNode` an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie, dass **Endpoint Operation** (Endpunktvorgang) **Execute Script** (Skript ausführen) ist, was anzeigt, dass eine anpassbare Skripteinbindung zum Aufrufen von Funktionen in CAPI verwendet wird, die letztlich die REST-Aufrufe an Azure durchführt. Die Skripteinbindung *azure-compute-1.0-CreateNode* MID-Server ist im Feld **Request script** (Skript anfordern) angegeben.

Dieses Schaubild zeigt, wie die Komponenten – vom Ressourcenblock bis zur Skripteinbindung – verbunden sind:



f. Klicken Sie auf das Datensatzsymbol (ⓘ) für das **Anforderungsskript**.

Die Skripteinbindung *azure-compute-1.0-CreateNode* MID-Server wird geöffnet.

g. Überprüfen Sie den Inhalt des Skripts.

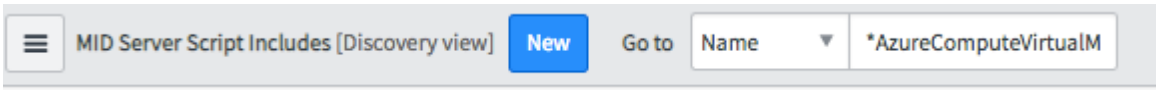
```
createNode();
function createNode(){
  var acp = new AzureComputeVirtualMachine(this.parameters, this.headers);
  var vm = acp.createVirtualMachine();

  return vm;
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Skript ruft die Funktion *createVirtualMachine* in der Klasse *AzureComputeVirtualMachine* auf. Dies gibt den erstellten virtuellen Computer zurück. Die Klasse *AzureComputeVirtualMachine* erweitert *AzureCloudAPIBase*, eine der Basis-APIs in Cloud Provisioning and Governance.

h. Um anzuzeigen *AzureComputeVirtualMachine*Klasse, die ein ist MID-Server Skripteinbindung öffnen Basissystem Instanzschnittstelle (nicht die Portal für Cloud-Admin.) Und navigieren Sie dann zu **MID-Server** > **Skripteinbindungen**an.

i. Suchen Sie nach *AzureComputeVirtualMachine* und öffnen Sie sie.



j. Überprüfen Sie die Funktion createVirtualMachine:

Die Funktion definiert viele Variablen, die zum Erstellen eines virtuellen Computers erforderlich sind, einschließlich *Location* (Rechenzentrum), den Namen des virtuellen Computers usw.

```
var location = this.parameters.get('Location');
var vmName = this.parameters.get('NodeName');
...
```

Diese Codezeile ruft die Funktion _performVMOperation in derselben Skripteinbindung auf und übergibt die erforderlichen Parameter. Beachten Sie, dass ein leerer Wert '' für den Parameter action (Aktion) weitergeleitet wird:

```
var response = this._performVMOperation(subscriptionId, resourceGroup, vmName, '',
 'PUT', jsonObj.encode(params));
```

Die Funktion _performVMOperation ruft die Funktion _invokeRequest auf, die sich in der Klasse *AzureCloudAPIBase* befindet:

```
return this._invokeRequest(this.pathDefault, param, method, requestBody);
```

Die PUT-Methode für den REST-Aufruf wird im Parameter *method* angegeben.

Sehen Sie sich Skripteinbindung *AzureCloudAPIBase* MID-Server an . Die Funktion _invokeRequest ruft zuerst die Funktion _getEndpoint auf, um den Endpunkt abzurufen, sowie die Funktion _getAPIInvoker , um die Klasse *AzureAPIInvoker* als die Klasse zu identifizieren, die den tatsächlichen PUT-Aufruf aufruft:

```
var apiInvoker = this._getAPIInvoker(apiEndpoint, this.apiVersion);
```

AzureAPIInvoker ist von *CloudRESTAPIInvoker* erweitert, was die Basisfunktionen für alle Aufrufer bereitstellt. Sobald die richtige Aufruferklasse identifiziert ist, wird eine *response*-Variable erstellt, die den von der Funktion invokePut in *CloudRESTAPIInvoker* zurückgegebenen Wert enthält:

```
response = apiInvoker.invokePut(requestBody);
```

Sehen Sie sich *CloudRESTAPIInvoker* an, die Basisklasse für alle Aufrufer. Die Funktion *invokePut* gibt die PUT-Methode an und ruft getRequest auf. Sie gibt die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwort der Funktion *getResponse* zurück, die einen Statuscode und die Antwort von Azure abruft. In dieser Aufruferklasse wird die Verbindung zu Azure hergestellt.

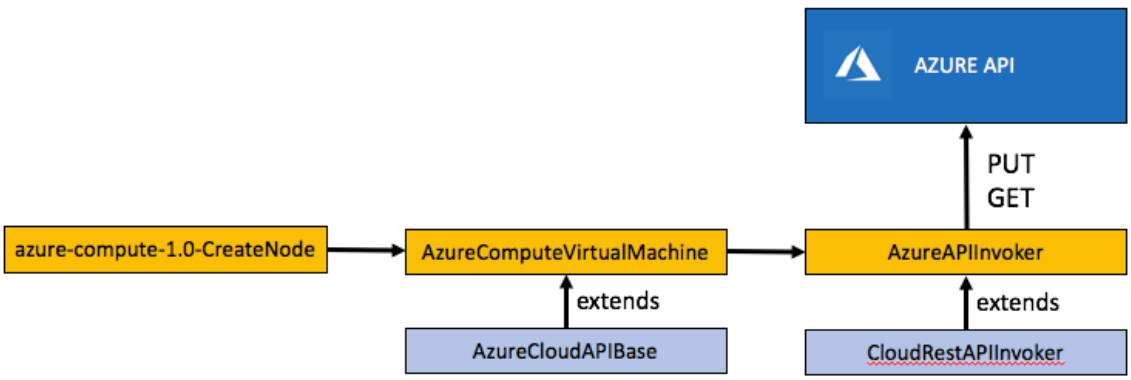
Kehren Sie zu Skripteinbindung *AzureComputeVirtualMachine* MID-Server zurück, und suchen Sie diese Zeilen:

```
var response = this._performVMOperation(subscriptionId, resourceGroup, vmName, '',
 'PUT', jsonObj.encode(params));
this._compareVMState(response.id, 'PowerState/running');
var nodeResponse = this.getVirtualMachine(response.id);
```

Denken Sie daran, dass die Variable *response* vom Aufruf an _performVMOperation zurückgegeben wird, was die Antwort vom API-Aufrufer umfasst, der die PUT-Methode ausgelöst hat. Die Variable *nodeResponse* enthält die Antwort der Funktion getVirtualMachine-, die die ID des virtuellen Computers in der Antwort weiterleitet. Die Funktion getVirtualMachine ruft _getVMInfo auf, die ebenfalls die Funktion _invokeRequest- aufruft, die bereits zuvor aufgerufen wurde. Dieser Aufruf stellt eine weitere Verbindung zum Aufrufer dar, der die eigentlichen REST-Aufrufe durchführt. In diesem Fall ist der REST-Aufruf ein GET REST-Aufruf von Azure, um die Identität des virtuellen Computers zu erhalten.

Die Zeile return nodeResponse; gibt *nodeResponse* in der Funktion createVirtualMachine zurück, die von der Skripteinbindung MID-Server im Vorgang *createNode* aufgerufen wurde.

Diese Grafik zeigt die beteiligten Klassen:



Automatische Übersetzung

k. Navigieren Sie zurück zum API-Formular von Azure Compute.

l. Klicken Sie auf die zugehörige Liste **API Config Overrides** (API-Konfigurationsüberschreibungen), und überprüfen Sie die für die Authentifizierung erforderlichen Elemente.

Konfigurationsparameter und Überschreibungswert	Beschreibung
ClientID $(CloudCredential.client_id)	Die Client-ID ist erforderlich, um die Anwendung in Azure zu identifizie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsparameter und Überschreibungswert	Beschreibung
EndpointURL $(CloudCredential.URL)	Die Endpunkt-URL ist die autorisierende Eingabe in Azure.
SecretKey $(CloudCredential.secret_key)	Der geheime Schlüssel wird zur Autorisierung des Clients verwendet.
TenantID $(CloudCredential.tenant_id)	Die Mandanten-ID ist der global eindeutige Bezeichner für den Mandant
EnrollmentNumber $(CloudCredential.sn_cmp_ea_credential.enrollment_number) EnrollmentToken $(CloudCredential.sn_cmp_ea_credential.access_key)	Die Azure-Registrierungsnummer und das Token dienen dem Zugriff auf

Unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern finden Sie weitere Informationen zu den Azure-Informationen, die in diesen Überschreibungen verwendet werden.

m. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, Und klicken Sie dann auf **Schnittstelle** Registerkarte.

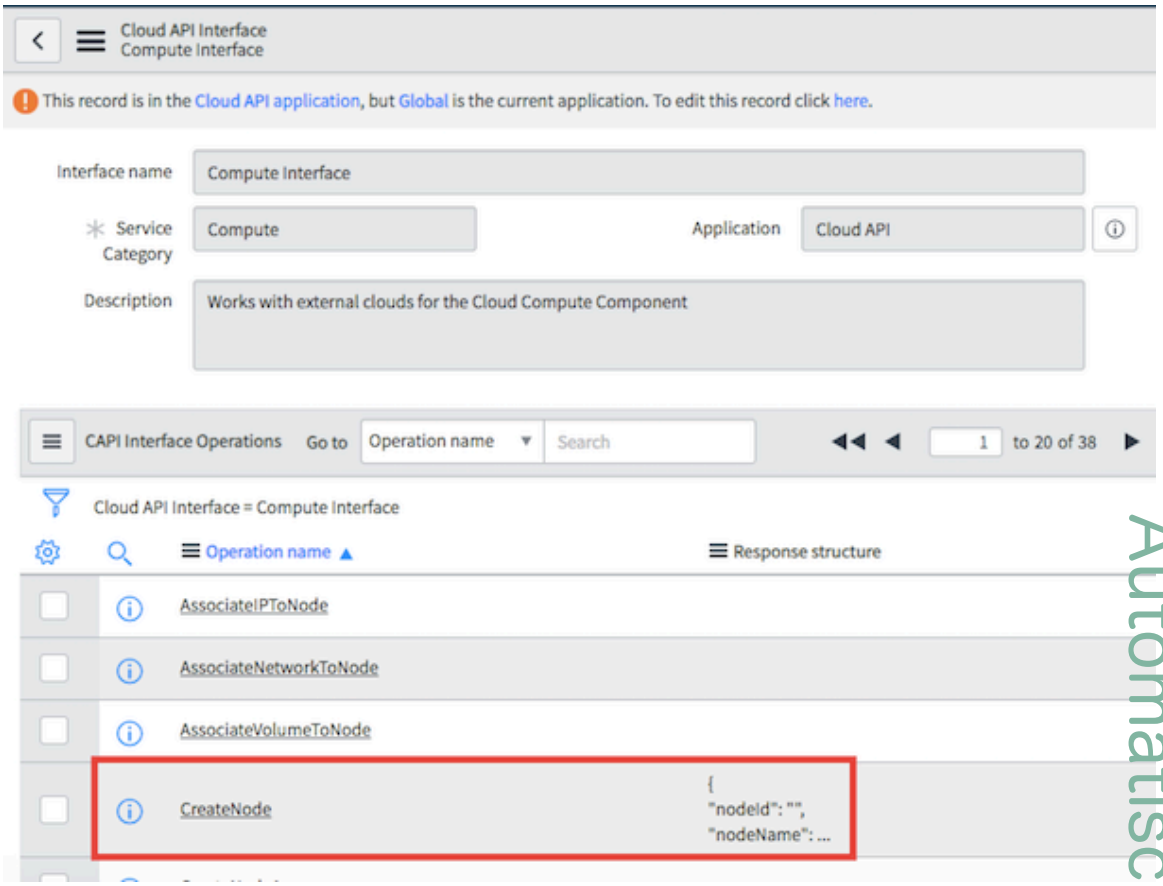
n. Suchen Sie nach **Compute Interface** (Compute-Schnittstelle) und öffnen Sie diese.

o. Überprüfen Sie den Inhalt der Schnittstelle.

Beachten Sie, dass die Schnittstelle REST-Antwortstrukturen für Methoden wie *`CreateNode`* bereitstellt. In der Regel müssen vorhandene Schnittstellen nicht geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie die Servicekategorie und die Vorgänge:

Feld oder zugehörige Liste	Beschreibung
Servicekategorie	Die Servicekategorie klassifiziert die Schnittstelle. Die Kategorie für die Compute-Schnittstelle ist ebenfalls **Compute**.
CAPI-Schnittstellenvorgänge	Die Schnittstellenvorgänge definieren die JSON-Struktur für den REST-Aufruf und die Parameter, die für die Schnittstelle erforderlich sind.

p. Klicken Sie auf den CAPI-Schnittstellenvorgang **CreateNode**.
Über diesen Vorgang wird das Framework für die Erstellung des virtuellen EC2-Servers bereitgestellt.

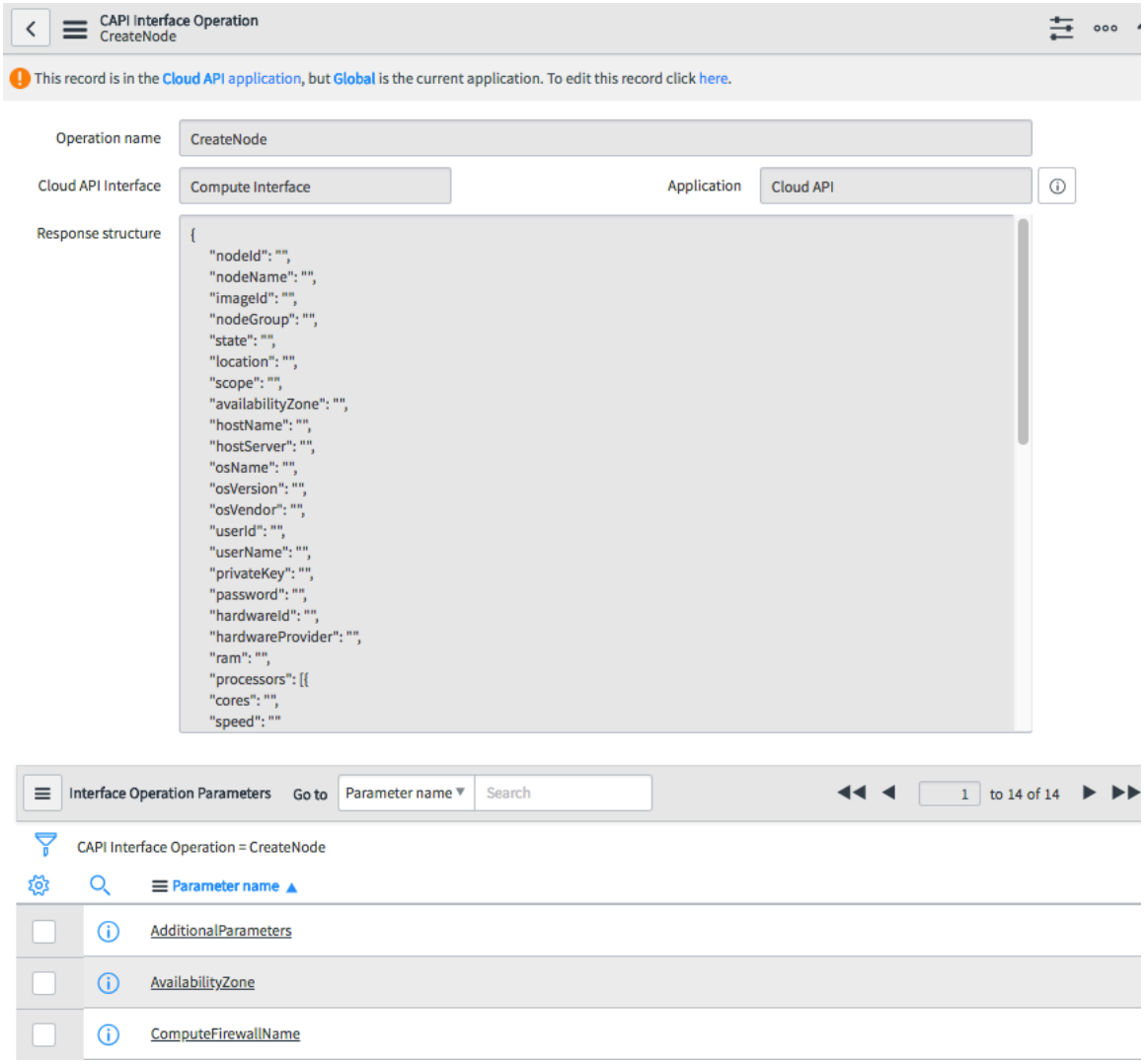
q. Überprüfen Sie die Komponenten des Vorgangs:

Feld oder zugehörige Liste	Beschreibung
Antwortstruktur	Die Antwortstruktur ist das JSON-Framework für den REST API-Aufruf. Diese Struktur bietet eine Liste von Attributen, die der Anbieter zum Erstellen der virtuellen Ressource mit leeren Werten verwenden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld oder zugehörige Liste	Beschreibung
Parameter für Schnittstellenvorgänge	Diese Parameter sind auch die Parameter, die die CAPI-Schnittstelle vom System benötigt, damit sie die Struktur im REST-Aufruf an den Cloud-Anbieter übergeben kann.



r. Navigieren Sie zurück zu **Entwurf** > **Cloud-API** Und klicken Sie dann auf **Anbieter** Registerkarte.

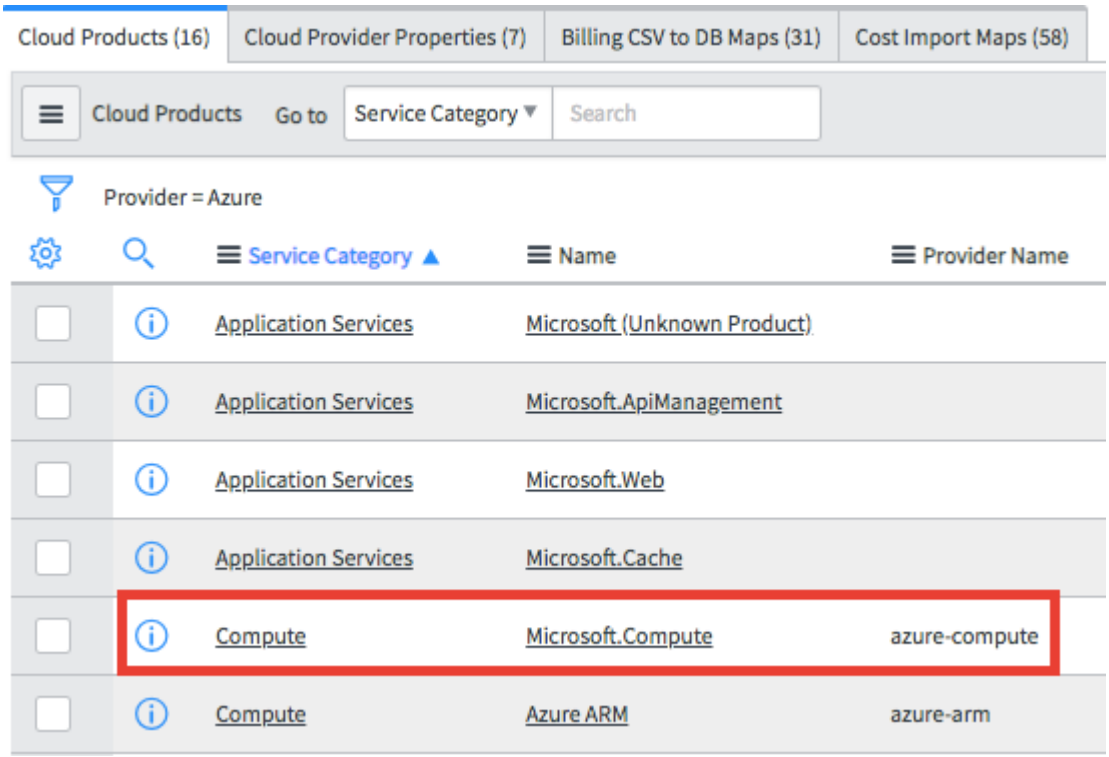
s. Öffnen Sie den Anbieter **Azure**.

Das Formular „Azure Cloud Provider“ (Azure-Cloud-Anbieter) wird geöffnet und zeigt an, dass dieser Anbieter auf einer vorhandenen CMDB-Klasse basiert: **Azure Datacenter [cmdb_ci_azure_datacenter]**.

t. Klicken Sie auf die zugehörige Liste „Cloud Products“ (Cloud-Produkte), und sortieren Sie die Liste nach der Spalte **Name**.

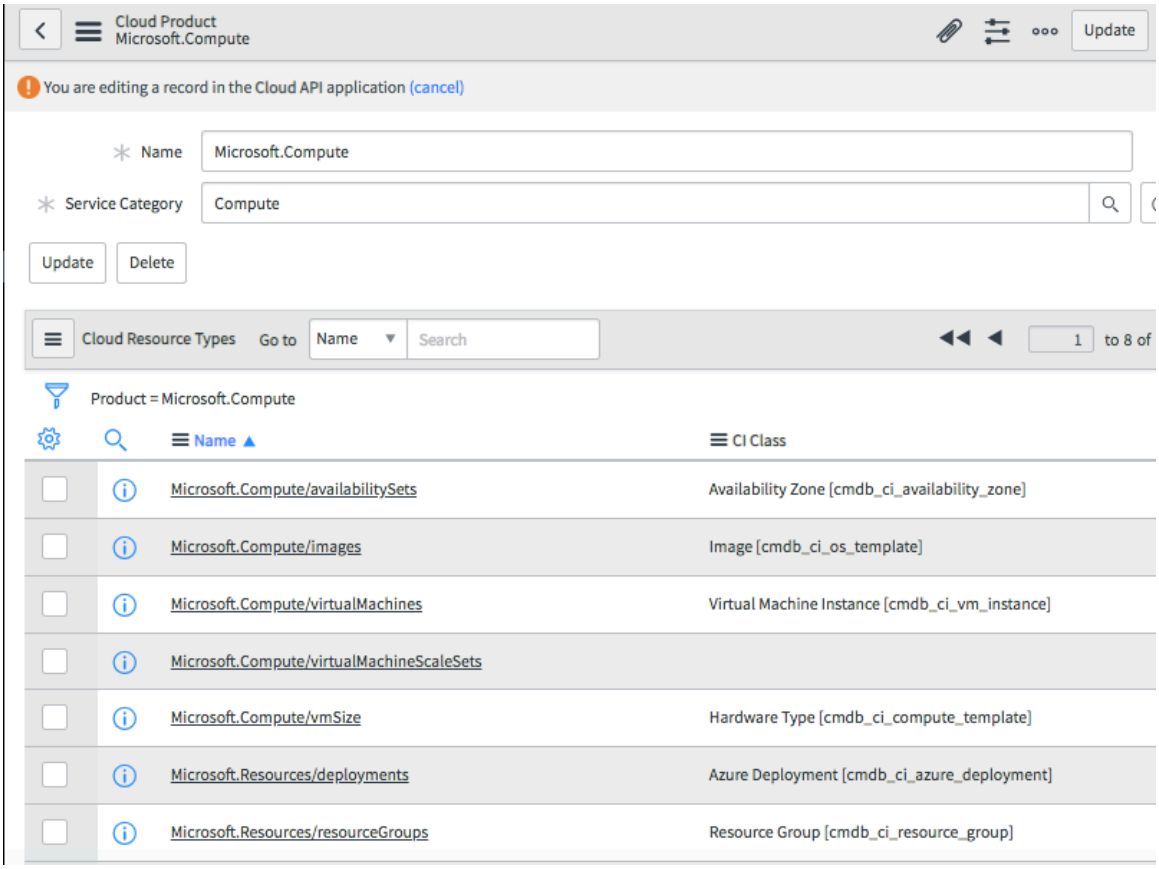
Beachten Sie, dass standardmäßig mehrere Azure-Produkte verfügbar sind. Eines der am häufigsten verwendeten Azure-Produkte, die aus Vorlagen erstellt werden, ist **Microsoft.Compute**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



u. Klicken Sie in der Spalte **Name** auf **Microsoft.Compute**.
Beachten Sie, dass das Produkt viele Ressourcentypen angibt, die jeweils einer CI-Klasse zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

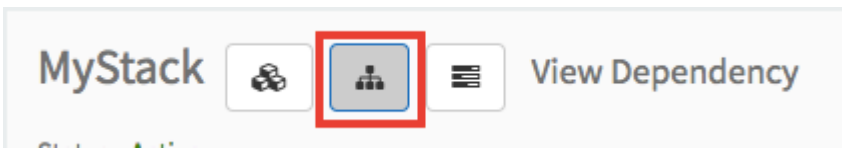


Diese Ressourcentypen geben einige, aber nicht alle CIs an, die sich auf den virtuellen Computer beziehen. Der Antwortprozessor im Ressourcenblock füllt CIs mit Daten aus, wenn der Cloud-Anbieter den virtuellen Computer bereitstellt.

5. So zeigen Sie die wichtigen mit der VM verbundenen CIs an:

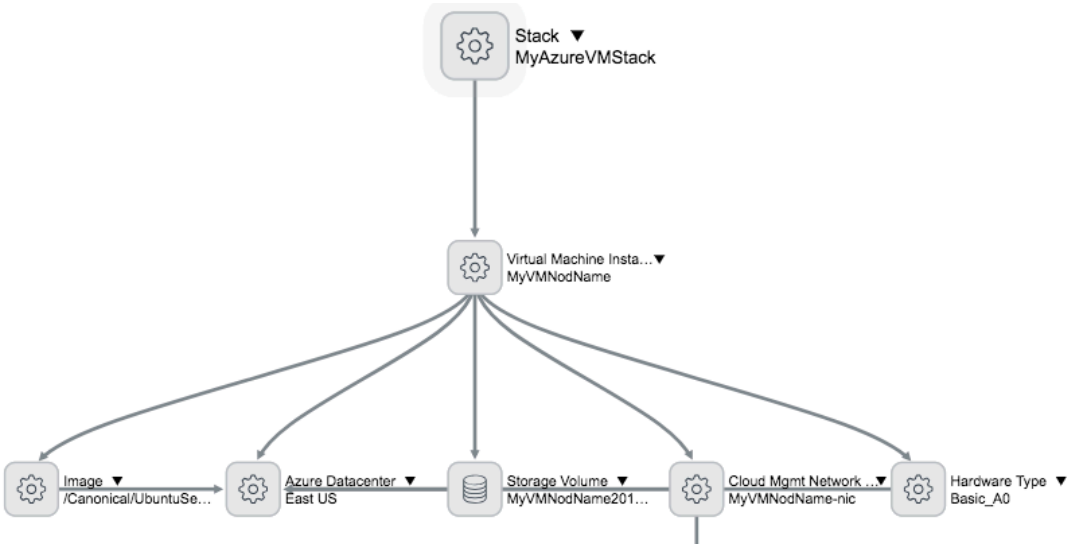
a. Klicken Sie in Cloudbenutzerportal auf **Stapel**, und öffnen Sie dann den Stapel, der die VM enthält.

b. Klicken Sie auf das Symbol **View Dependency** (Abhängigkeit anzeigen).



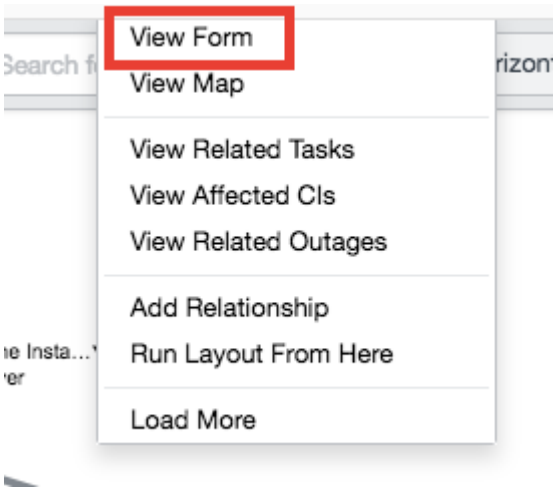
Die Abhängigkeitszuordnung zeigt das Stapel-CI oben, den virtuellen Computer in der Mitte und die verschiedenen zugehörigen CIs unten, z. B. das Bild.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



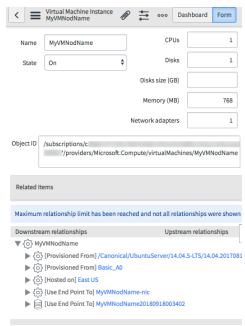
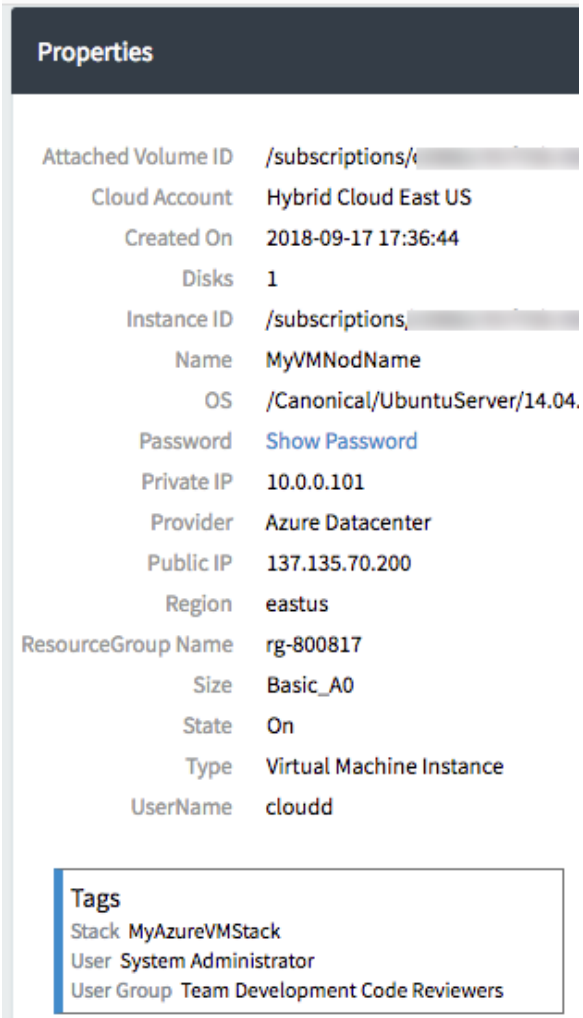
c. Sie rufen das Formular für den virtuellen Computer in der CMDB auf, indem Sie mit der rechten Maustaste auf den Pfeil neben einem CI klicken.

d. Wählen Sie im Menü **View Form** (Formular anzeigen).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das CI-Formular wird geöffnet und zeigt an, dass viele der Informationen bereits auf Cloudbenutzerportal verfügbar sind, wenn Sie die Eigenschaften des virtuellen Computers anzeigen lassen.

VM-CI-Formular	Eigenschaften des virtuellen Computers in Cloudbenutzerportal
	

VM-Bereitstellung bei AWS – Beispiel-Vorstellung

Dieses Beispiel führt Sie durch die Komponenten von Cloud Provisioning and Governance, die während der Bereitstellung eines virtuellen Computers in einem AWS-Rechenzentrum in Betrieb sind. Zu den behandelten Themen gehören Blaupausen, Ressourcenblöcke, die Cloud-API (CAPI) und Skripteinbindungen MID-Server.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Vorstellung beginnt mit einem virtuellen Computer unter Windows, den der Benutzer bereits in AWS bereitgestellt hat. Anschließend werden die Blaupause mit virtuellem Computer, Ressourcenblöcke und in den Ressourcenblöcken angegebene CAPI-Aufrufe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorgestellt. Abschließend zeigt die Vorstellung, wie eine MID-Server-Skripteinbindung die tatsächlichen Aufrufe an die AWS-API durchführt.

In diesem Beispiel werden Standardressourcenblocks und Skript Includes verwendet, die in Ihrer Instanz verfügbar sind. Deshalb können Sie, obwohl Sie möglicherweise keine bereitgestellte VM auf Ihrer Instanz haben, trotzdem diese Schritte befolgen und die in diesem Beispiel verwendeten Komponenten anzeigen, um die Arbeitsweise der Komponenten zu verstehen.

Ein Beispiel für einen virtuellen Computer in Azure finden Sie unter Azure VM-Bereitstellung – exemplarische Vorstellung.

Hinweis: Die Begriffe *virtueller Computer*, *VM* (für „Virtual Machine“) und *virtueller Server* sind in diesem Beispiel synonym.

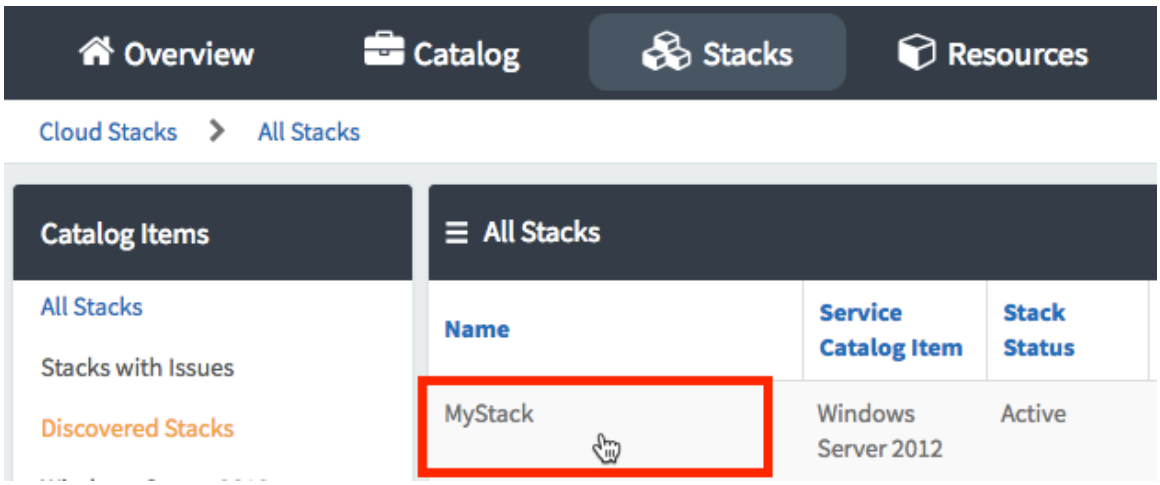
Prozedur

1. Betrachten Sie eine eingerichtete VM im Cloud User Portal und richten Sie den Fokus auf einige Details zur VM:

   a. Öffnen Sie in Ihrer -Instanz Cloudbenutzerportal(Cloud Provisioning and Governance **Cloud-Anwenderportal**) an.

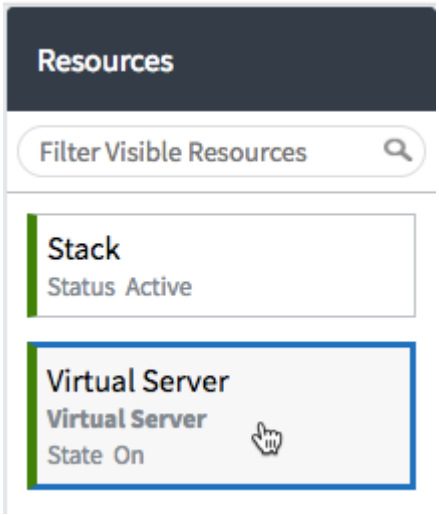
   b. Rufen Sie eine bereitgestellte VM in einem Stapel auf, z. B. diese Windows VM, indem Sie auf **Stapel** und dann auf den Namen des Stapels klicken.

   In diesem Beispiel heißt der Stapel **MyStack**.

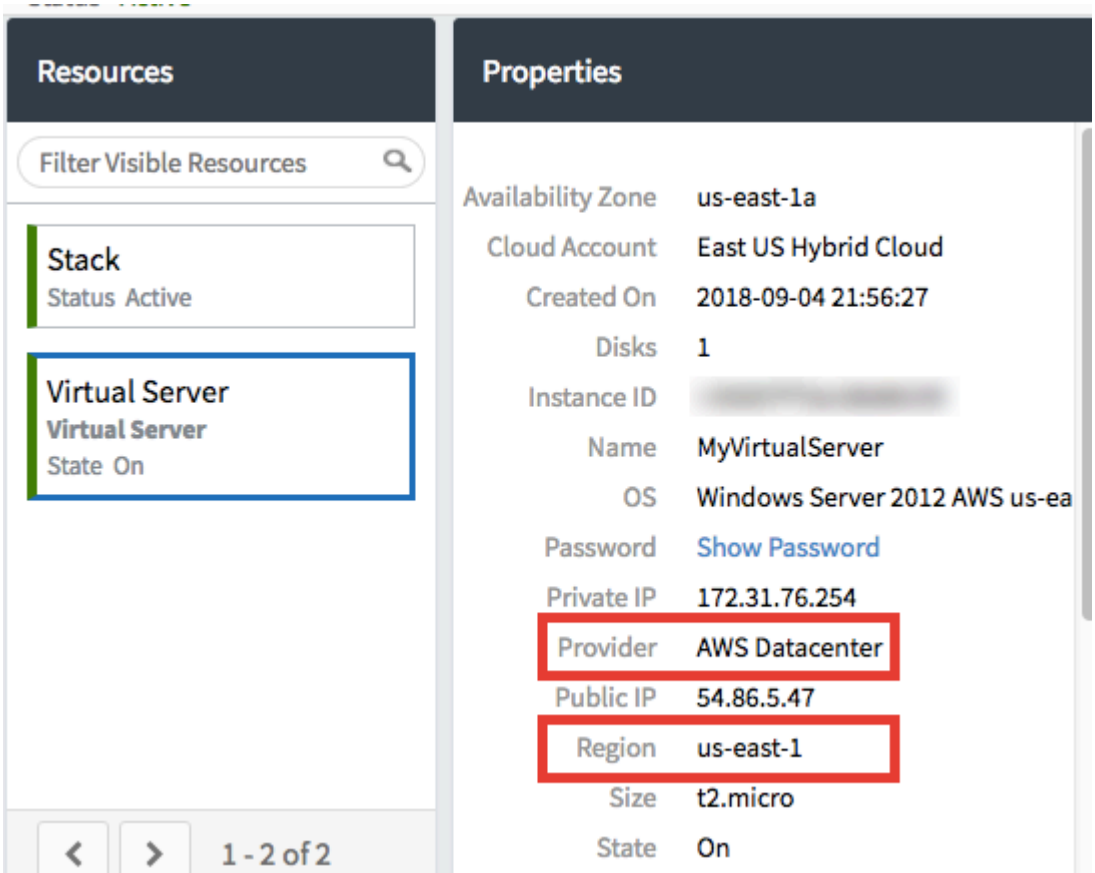


   c. Klicken Sie unter **Resources**(Ressourcen) auf den virtuellen Computer im Stapel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Rufen Sie die Eigenschaften der VM auf; beachten Sie, dass sich die VM in einem AWS-Rechenzentrum in der Region „us-east-1“ befindet.

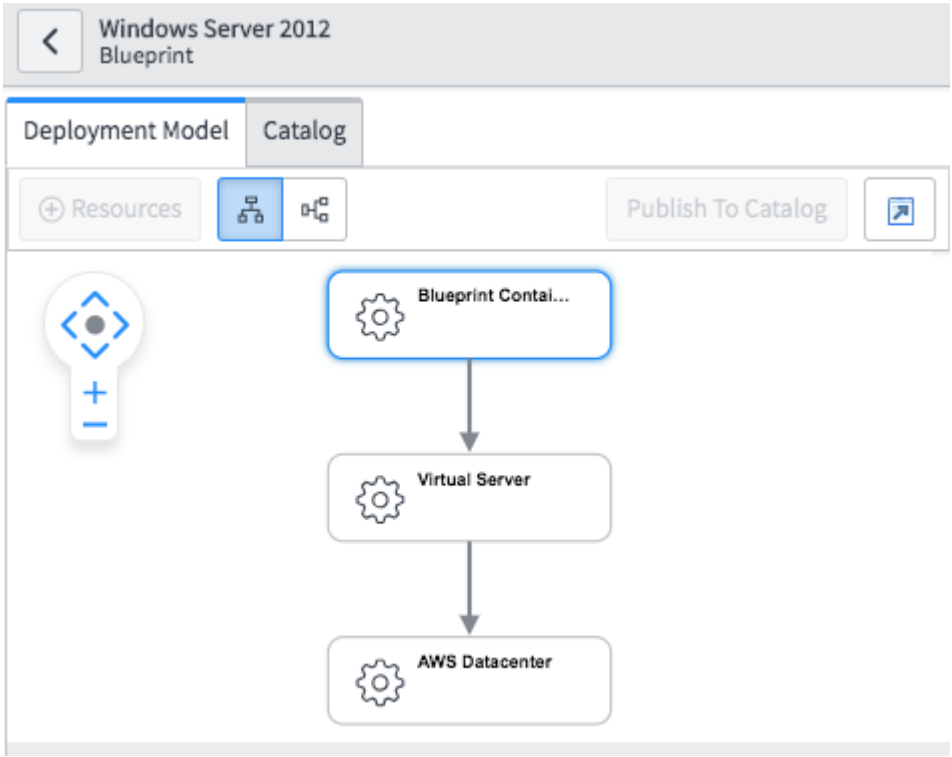


2. Sehen Sie sich die Blaupause an, auf der die VM basiert:

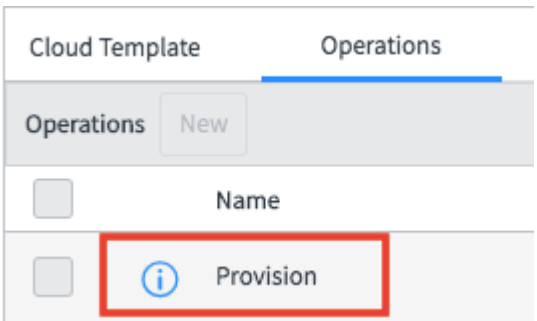
a. Navigieren zu **Entwurf** > **Blueprints**, Und öffnen Sie dann einen Blueprint mit einem virtuellen Server im Azure-Rechenzentrum. Die **Bereitstellungsmodell** Standardmäßig wird die Registerkarte angezeigt, die Ihnen die verschiedenen Komponenten des Blueprints anzeigt.

Diese Beispiel-Blaupause hat drei Komponenten: den Container, den virtuellen Server, der die bereitgestellte VM ist, und das AWS-Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

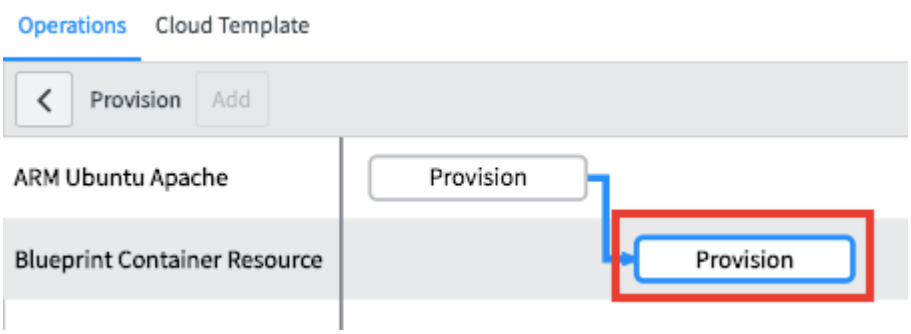


b. Klicken Sie unten auf die Registerkarte **Vorgänge** und dann auf **Bereitstellung**.



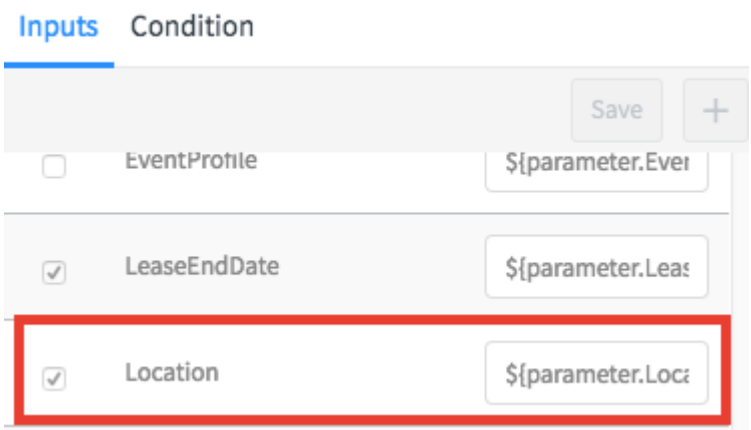
Der Bereitstellungsvorgang ist der Vorgang, den das System beim Erstellen der VM ausgelöst hat. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

c. Klicken Sie auf den Block **Bereitstellung** für die Container-Ressource der Blaupause.



d. Beachten Sie, dass einer der Parameter auf der rechten Seite in der Inputs-Liste „Location“ lautet. Dieser Parameter speichert den Statuswert, der aussagt, wo die VM im Datencenter lebt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

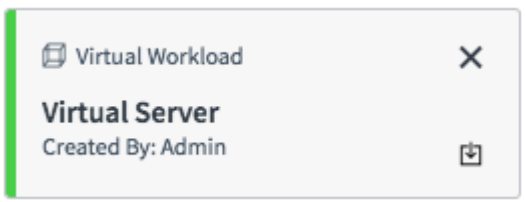


Eingaben können auf Container-Ebene festgelegt werden, wie in diesem Beispiel, oder auf einem beliebigen anderen Ressourcenblock. Standardmäßig ist der *Location*-Parameter bereits für Sie im Blaupause-Container-Ressourcenblock festgelegt, sodass Sie ihn in jeder Blaupause wie dieser verwenden können. Wenn Sie den Status der Blaupause auf **Entwurf** wechseln, können Sie dem Container-Ressourcenblock der Blaupause weitere Parameter hinzufügen. Dem Ressourcenblock des virtuellen Servers können Sie keine Parameter hinzufügen. Für diese Anleitung werden keine weiteren Parameter benötigt.

3. Betrachten Sie die Ressourcenblöcke des virtuellen Servers und des AWS-Rechenzentrums, die in dieser Blaupause verwendet werden:

a. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Ressourcenblöcke**an.

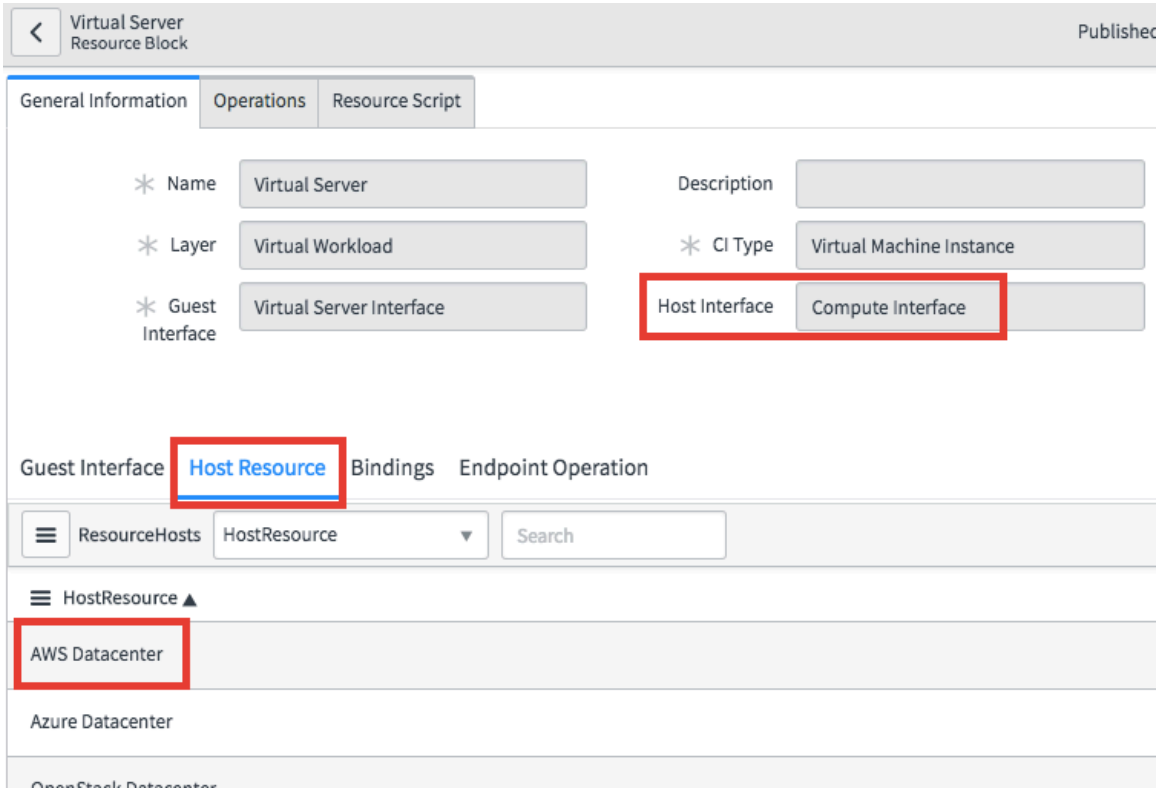
b. Suchen und öffnen Sie den Ressourcenblock **Virtueller Server**, der standardmäßig mit Cloud Provisioning and Governance bereitgestellt wird.



c. Klicken Sie im Ressourcenblock-Formular auf die zugehörige Liste **Hostressource**, um die Liste der unterstützten Host-Ressourcenblöcke anzuzeigen.

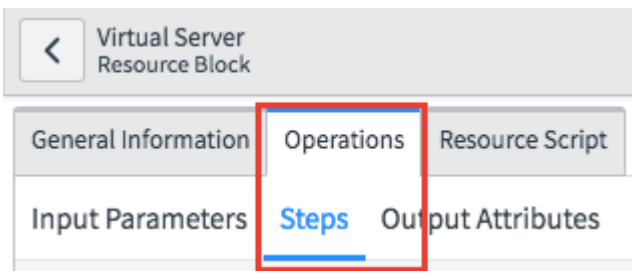
d. Wie Sie erkennen können, wurden Host-Schnittstelle und Host-Ressource bereits angegeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

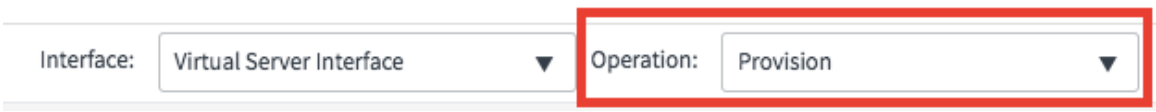


- Das Feld **Host Interface** (Host-Schnittstelle) gibt die Schnittstelle an, die mit der Gastschnittstelle im Ressourcenblock, der den virtuellen Computer hostet, übereinstimmen muss. In diesem Fall ist die Host-Schnittstelle die Compute-Schnittstelle, die auch die Gastschnittstelle auf dem Ressourcenblock des AWS-Rechenzentrums ist. Standardmäßig stellt der Rechenzentrum-Ressourcenblock mehrere Gastschnittstellen bereit, über die sich andere Ressourcenblöcke mit dem Datacenter verbinden können, beispielsweise der virtuelle Speicher.
- Die Spalte **HostResource** in der zugehörigen Liste **Host Resource** (Host-Ressource) gibt bereits **AWS Datacenter** (AWS-Rechenzentrum) an, was bedeutet, dass der Ressourcenblock des AWS-Rechenzentrums ein gültiger Host für diese VM ist.

e. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



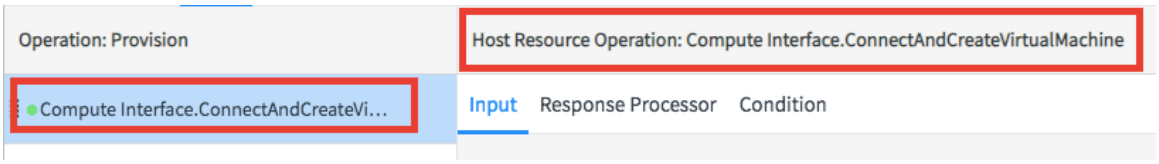
f. Wählen Sie in der Liste **Vorgang** die Option **Bereitstellung** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denken Sie daran, dass es der Bereitstellungsvorgang ist, mit dem das System die VM erstellt. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

g. Beachten Sie den Schritt, der in der Liste angezeigt wird, und die vollständige Schrittbeschreibung, die über den Eingabeparametern angezeigt wird:



(Schritt für Bereitstellung)

- **Host Resource Operation:** (Host-Ressourcenvorgang) gibt an, dass dieser Schritt einen Vorgang für die Host-Ressource (das AWS-Rechenzentrum in diesem Beispiel) aufruft.
- **Compute Interface** (Compute-Schnittstelle) ist die Gastschnittstelle im AWS-Rechenzentrum, die dieser Schritt verwendet.
- **ConnectAndCreateVirtualMachine** ist der Vorgang im AWS-Rechenzentrum, den dieser Schritt aufruft.

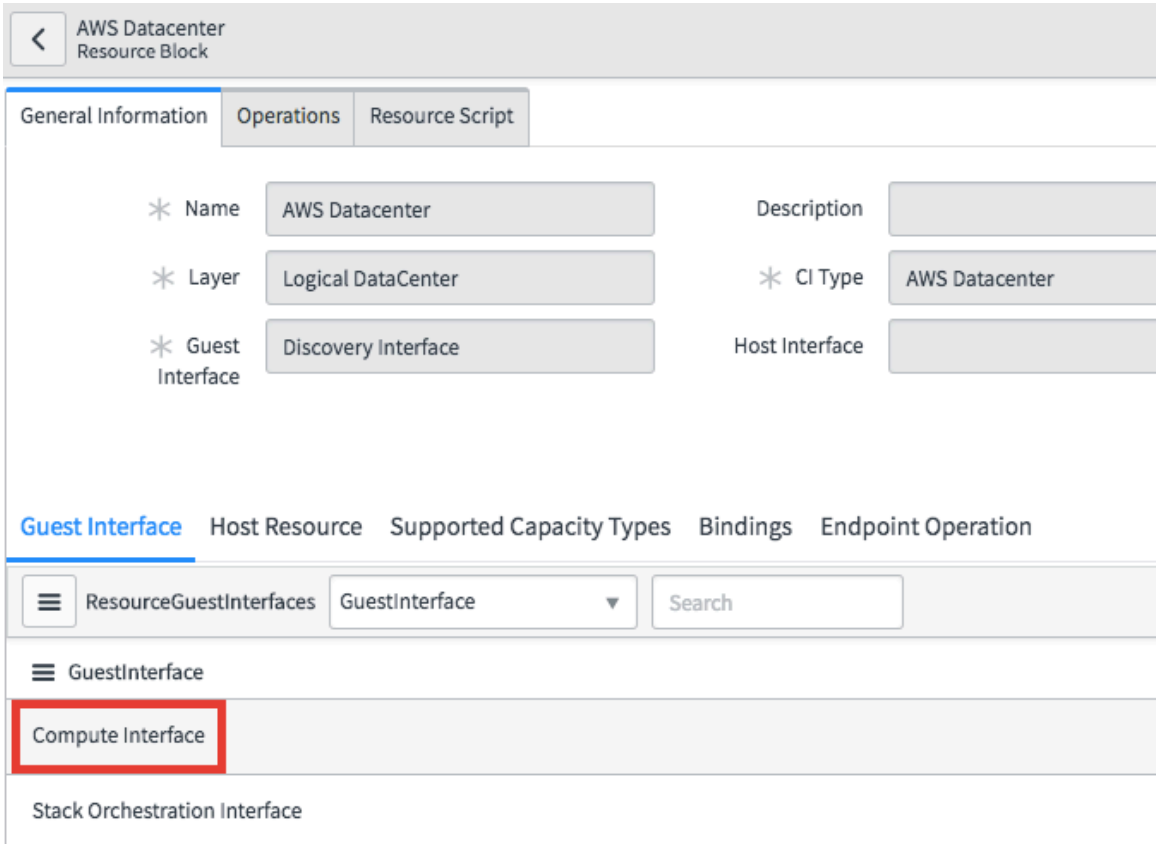
Hinweis: In diesem Fall ruft der Schritt einen Vorgang von einem anderen Ressourcenblock auf: dem AWS-Rechenzentrum. Schritte können CAPI auch direkt aufrufen, und dann kann CAPI REST-Aufrufe an die Cloud-Provider-API ausführen. Das sehen Sie, wenn Sie sich den Ressourcenblock des AWS-Rechenzentrums ansehen.

h. Navigieren Sie zurück zu **Entwurf** > **Ressourcenblöcke**an.

i. Öffnen Sie den Ressourcenblock **AWS Datacenter** (AWS-Rechenzentrum), der den Host-Ressourcenblock darstellt, mit dem der virtuelle Server verbunden ist.

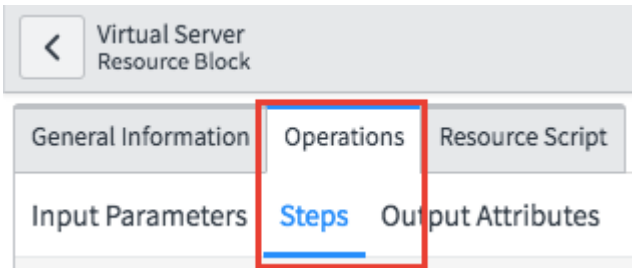
j. Beachten Sie die unterstützten Gastschnittstellen in der zugehörigen Liste **Guest Interface** (Gastschnittstelle):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Gastschnittstellen sind die Schnittstellen, die das AWS-Rechenzentrum anderen Ressourcenblöcken zur Verfügung stellt. Die Option **Compute Interface** (Compute-Schnittstelle) wird bereitgestellt, damit der Ressourcenblock des virtuellen Servers, der die Compute-Schnittstelle als Host-Schnittstelle angibt, eine Verbindung zum Rechenzentrum herstellen kann.

k. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.

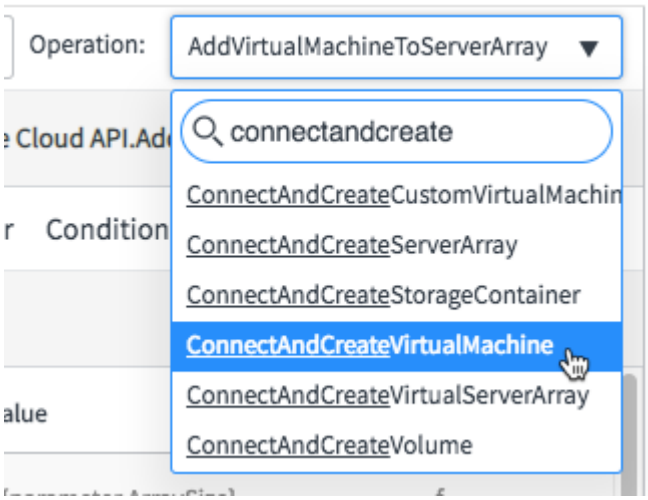


l. Wählen Sie in der Liste **Interface** (Schnittstelle) die Option **Compute Interface** (Compute-Schnittstelle) aus, wenn sie nicht bereits ausgewählt ist.

Denken Sie daran, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

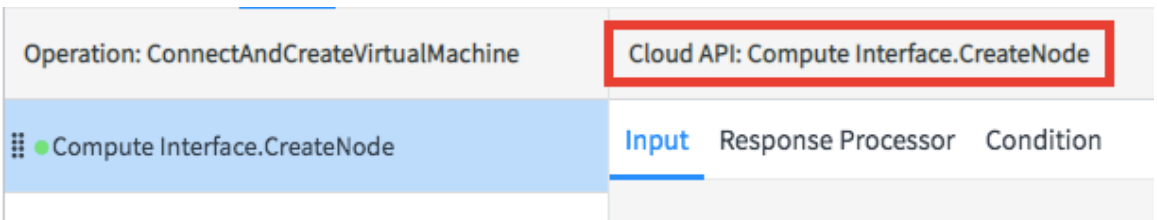
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

m. Suchen Sie in der Liste **Operation** (Vorgang) die Option **ConnectAndCreateVirtualMachine** und wählen Sie sie aus.



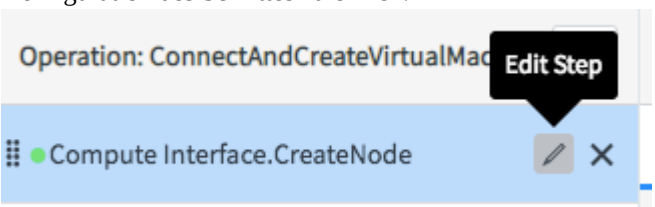
Dabei ist zu berücksichtigen, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

n. Zu beachten ist der CAPI-Aufruf, der im einzigen Schritt für den Vorgang „ConnectAndCreateVirtualMachine“ verwendet wird:



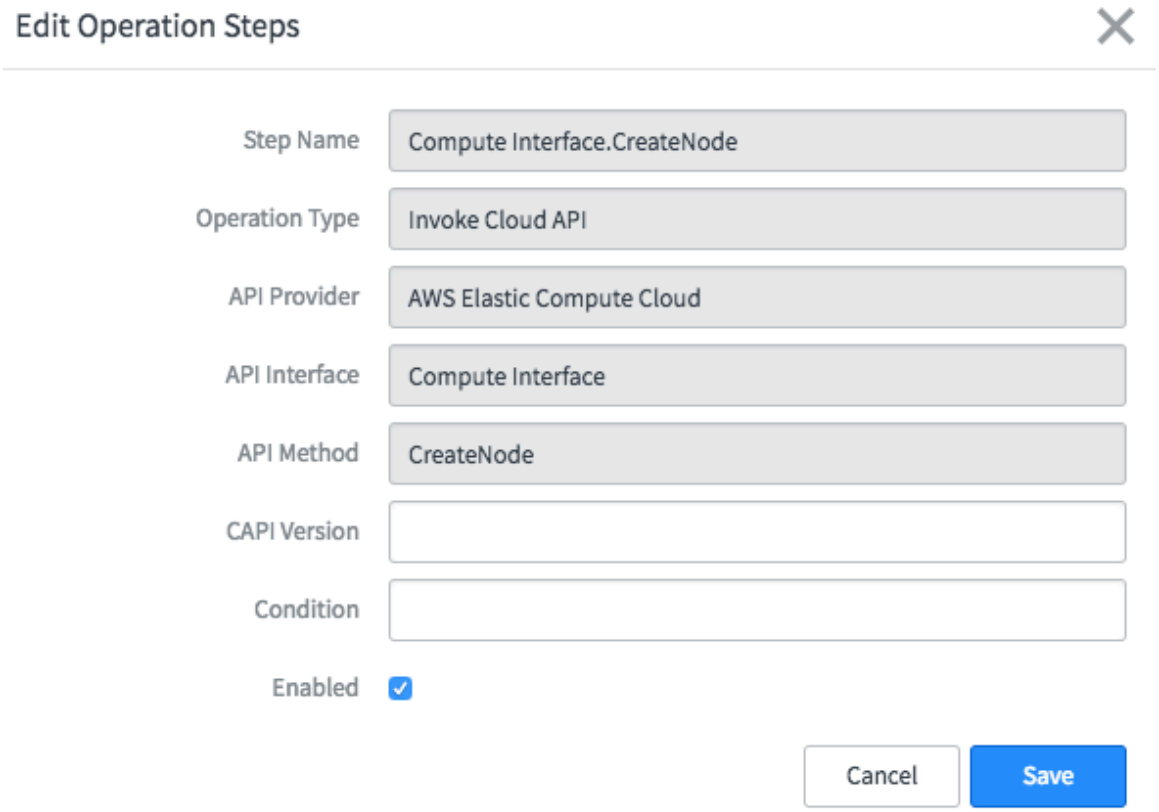
- **Cloud API:** (Cloud-API) Gibt an, dass dieser Schritt CAPI aufruft, sodass CAPI einen REST-Aufruf an den Cloud-Anbieter ausführen kann, der in diesem Fall AWS ist.
- **Compute Interface** (Compute-Schnittstelle) gibt die CAPI-Schnittstelle vor, die von diesem Schritt aufgerufen wird.
- **CreateNode** gibt die Methode an, die ausgeführt wird. Wie der Name schon sagt, weist diese Methode AWS an, den virtuellen Computer zu erstellen.

o. Der Ressourcenblock muss den Status **Draft** (Entwurf) aufweisen. Zeigen Sie dann auf den hervorgehobenen (blauen) Schritt, und klicken Sie auf das Symbol **Edit Step** (Schritt bearbeiten), um die Konfiguration des Schrittes zu öffnen.



p. Sehen Sie sich die Schrittkonfiguration an, und hier insbesondere die Einstellungen, die in CAPI integriert werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



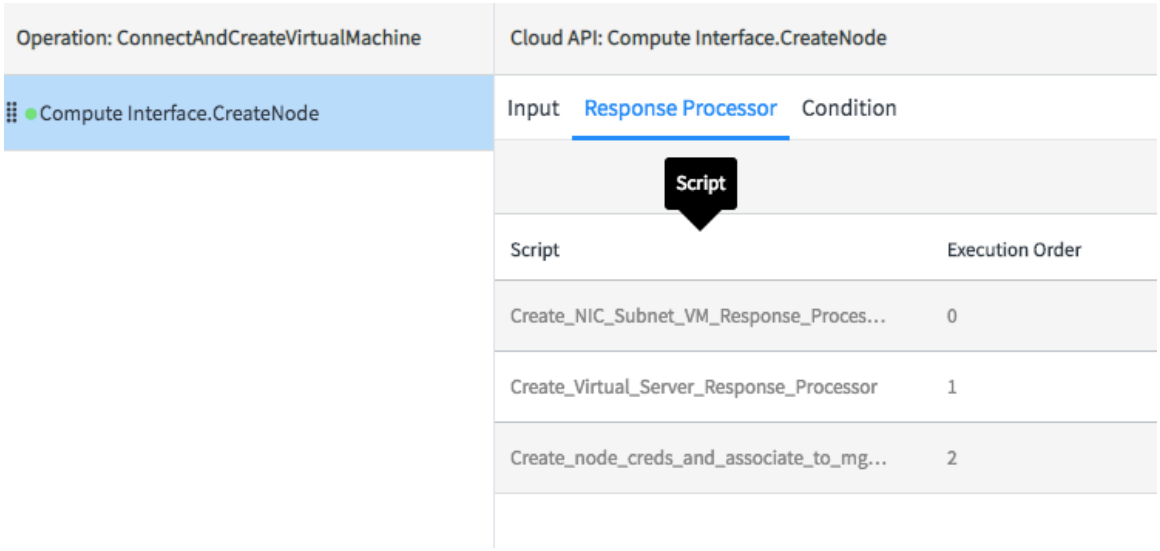
Feld	Beschreibung
Vorgangstyp	**Invoke Cloud API** (Cloud-API aufrufen) gibt an, dass dieser Schritt die CAPI über den angegebenen Anbieter, die angegebene Schnittstelle und die angegebene Methode aufrufen soll.
API-Anbieter	**AWS Elastic Compute Cloud** ist ein Produkt (nicht der tatsächliche Anbieter), das zum AWS-Anbieter gemäß der Definition in CAPI gehört.
API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist ein Produkt, das zum AWS-Anbieter gemäß der Definition in CAPI gehört.
API-Methode	**CreateNode** ist die Methode, die AWS zum Erstellen der VM aufruft.

Hinweis: Die CAPI-API-Definition verbindet den Anbieter (Azure), das Produkt (AWS Elastic Compute Cloud), die Schnittstelle (Compute Interface) und die Methode (CreateNode).

q. Schließen Sie das Fenster.

r. Klicken Sie bei ausgewähltem Schritt **Compute Interface.CreateNode** auf **Response Processor** (Antwortprozessor); beachten Sie dabei das Skript **Create_Virtual_Server_Response_Processor**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Skript ist der Antwortprozessor, der die CMDB in Ihrer Instanz aktualisiert, nachdem der virtuelle Computer in AWS erstellt wurde.

s. Zeigen Sie eine Erklärung des Skripts und das Beispiel an, das Teil des Themas ist Erstellen Sie einen Antwortprozessor .
Wenn Sie die Überprüfung von diesem Themas abgeschlossen haben, kehren Sie zu diesem Thema zurück.

4. Sehen Sie sich die CAPI-Komponenten an, die zusammenarbeiten, um den virtuellen Computer bereitzustellen:

a. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-API**an.

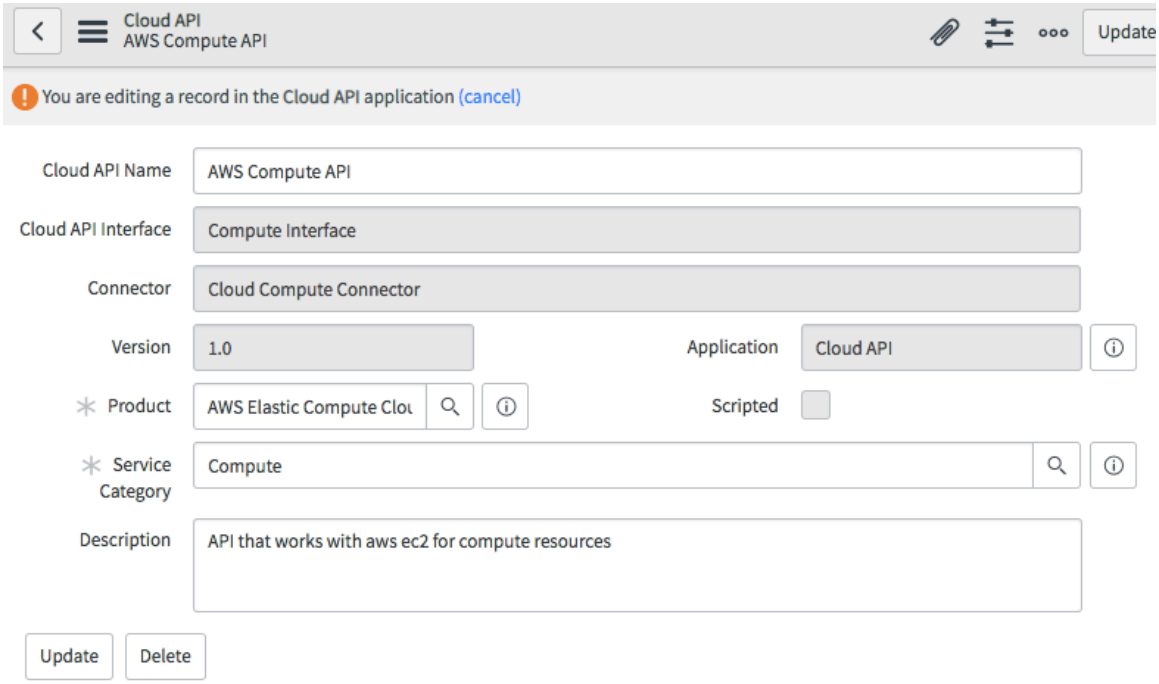
b. Klicken Sie auf die Registerkarte **API**.

c. Suchen Sie nach einer offenen **AWS Compute-API**.

Es gibt zwei AWS Compute-API-Datensätze. Öffnen Sie den ersten in der Liste, der dem Bild im nächsten Schritt entspricht.

d. Sehen Sie sich an, wie diese CAPI-API eine *Schnittstelle* und ein *Produkt* miteinander verknüpft:

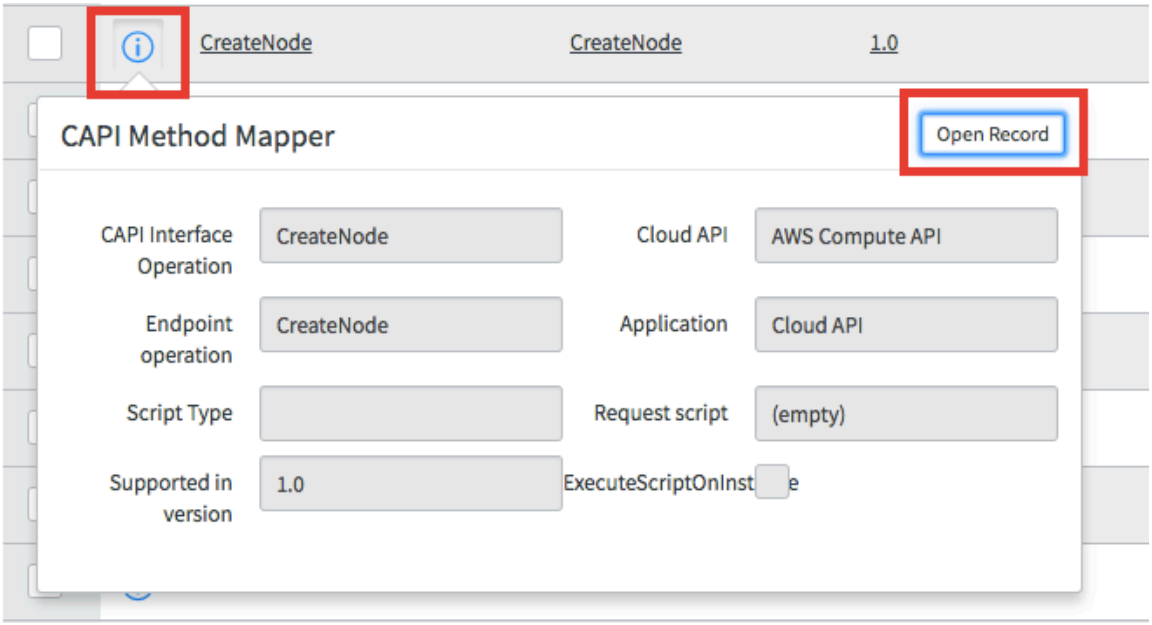
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



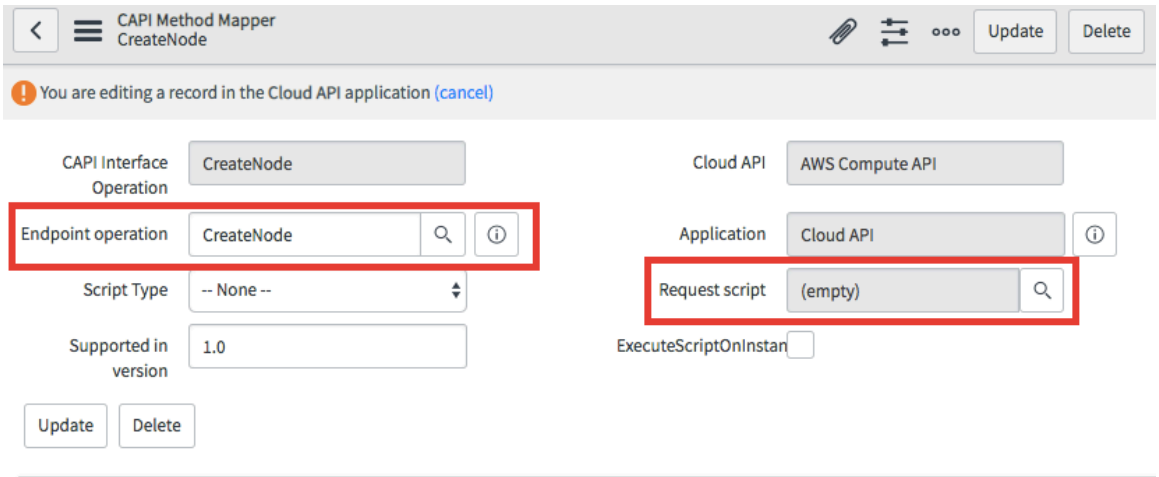
Feld	Beschreibung
Cloud-API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist die gleiche Schnittstelle, die im Ressourcenblock angegeben ist. Die Schnittstelle enthält die Definition für Methoden, einschließlich der Methode `CreateNode`.
Connector	**Cloud Compute Connector** gibt an, dass diese CAPI Java-Aufrufe an das System durchführt, das dann die AWS-API aufruft. Dieser Connector ist nicht geskriptet. Wenn es sich um einen skriptbasierten Connector handeln würde, würde er über eine Skripteinbindung MID-Server verfügen, die die AWS-API aufruft. **Hinweis:** Die meisten AWS-bezogenen APIs, die standardmäßig in der Anwendung Cloud Provisioning and Governance bereitgestellt werden, sind wie diese nicht geskriptet und können nicht geändert werden. Sie können jedoch eigene Skript-APIs erstellen.
Version	**1.0** gibt die Version der API an. Sie können über mehrere Versionen dieser API mit unterschiedlichen Versionsnummern verfügen. Beachten Sie, dass im Schritt im Ressourcenblock für das AWS-Rechenzentrums, den der virtuellen Computer erstellt, ein Versionsfeld bereitgestellt wird. Obwohl dieses Feld im Beispiel leer war, da nur eine Version dieser API vorhanden ist, können Sie eine andere Versionsnummer angeben.
Produkt	**AWS Elastic Compute Cloud** ist das Produkt, das zum AWS-Anbieter in CAPI gehört. Dieses Produkt wird standardmäßig mit Cloud Provisioning and Governance geliefert und ist eines der am häufigsten verwendeten Produkte zum Erstellen virtueller Computer in AWS.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie in der zugehörigen Liste „CAPI Method Mappers“ (CAPI-Methodenzuordnungen) auf das Symbol für die Datensatzvorschau für den Datensatz `CreateNode`, und klicken Sie dann auf **Open Record** (Datensatz öffnen).



f. Sehen Sie sich die Methodenzuordnung für `CreateNode` an:



Beachten Sie, dass der Endpunktvorgang nicht **Execute Script**(Skript ausführen) ist. Dieser Wert gibt an, dass die Methode „CreateNode“ einen Java-Aufruf innerhalb der Anwendung Cloud Provisioning and Governance auf Ihrer Instanz verwendet, um einen REST-Aufruf zur AWS-API durchzuführen. Daher können Sie die Funktionsweise der Methode „CreateNode“ nicht ändern. Wenn der Wert **Execute Script** (Skript ausführen) lauten würde, wäre eine MID-Server-Skripteinbindung im Skriptfeld **Request** (Anforderung) angegeben. Sie können diese Skripteinbindung ändern oder eine neue angeben, um die REST-Aufrufe an den AWS-Provider anzupassen.

g. Scrollen Sie nach unten, und sehen Sie sich Parameter in der zugehörigen Liste der CAPI-Parameterzuordnungen an.
Beachten Sie, dass wichtige Parameter wie **Location** (Standort) angegeben sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Navigieren Sie zurück zum API-Formular von AWS Compute.

i. Klicken Sie auf die zugehörige Liste **API Config Overrides** (API-Konfigurationsüberschreibungen), und überprüfen Sie die für die Authentifizierung erforderlichen Elemente.

Konfigurationsparameter und Überschreibungswert	Beschreibung
AccountAliasName $(CloudCredential.Alias)	Der Alias für das Konto ist ein optionaler Wert, den Sie in Ihrem AWS-Konto erstellen können. Es handelt sich um einen sekundären Namen für Ihre Konto-ID. In der Dokumentation zu AWS finden Sie weitere Informationen.
Berechtigungen $(CloudCredential.secret_key)	Der geheime Schlüssel wird mit dem Zugriffsschlüssel für die Authentifizierung verwendet. Sie haben diesen Wert während der Einrichtung in Ihrem AWS-Anmeldeinformationsdatensatz konfiguriert. Informationen zu diesem Verfahren finden Sie unter Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren.
Endpunkt $(CloudCredential.URL)	Der Endpunkt ist die URL, bei der sich die Benutzer anmelden und authentifizieren müssen. Dazu werden Konto-ID oder Konto-Alias verwendet. In der Dokumentation zu AWS finden Sie weitere Informationen.
Identität $(CloudCredential.access_key)	Der Datensatz „Identify“ (Identifizieren) enthält den AWS-Zugriffsschlüssel, den AWS für die Authentifizierung benötigt.

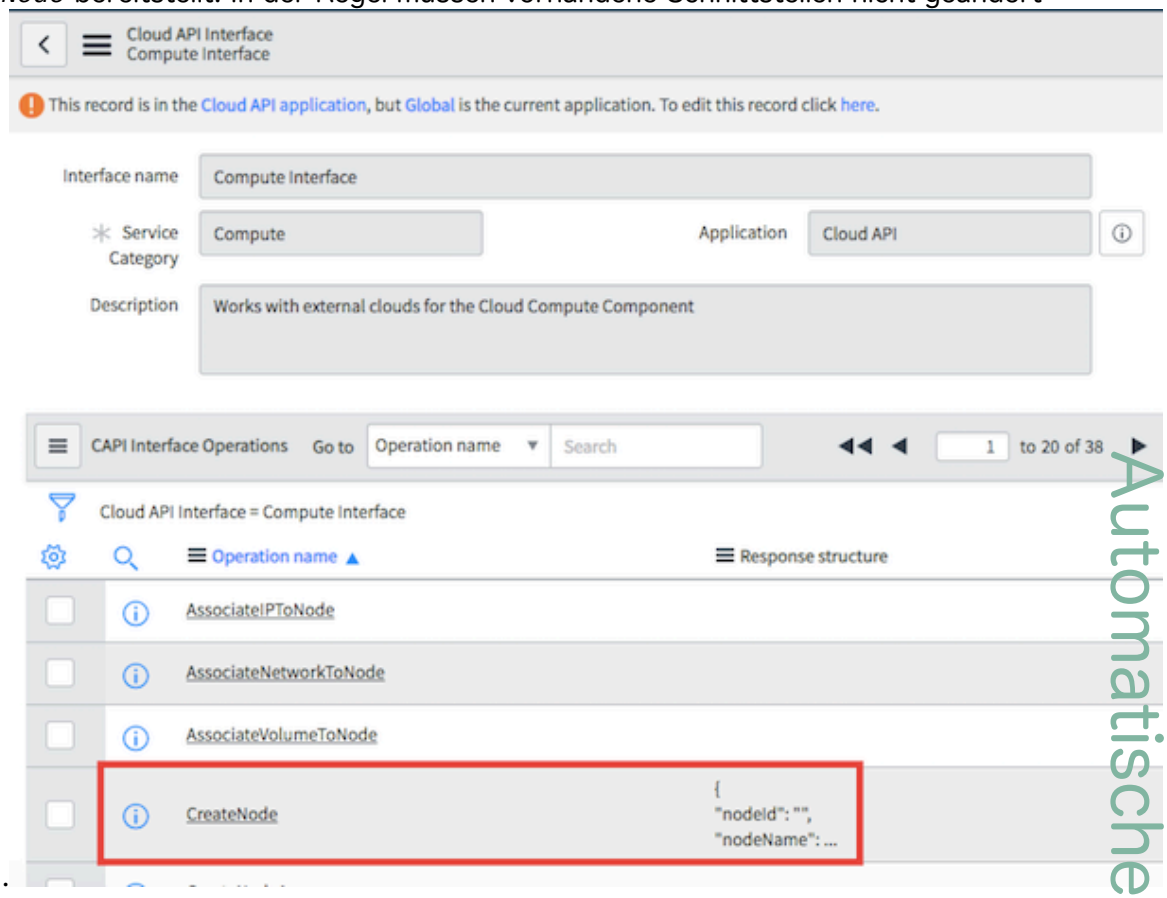
j. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, Und klicken Sie dann auf **Schnittstelle** Registerkarte.

k. Suchen Sie nach **Compute Interface** (Compute-Schnittstelle) und öffnen Sie diese.
Diese Schnittstelle ist die im Ressourcenblock und der CAPI-API unter **AWS Compute-API** angegebene Schnittstelle.

l. Überprüfen Sie den Inhalt der Schnittstelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie, dass die Schnittstelle REST-Antwortstrukturen für Methoden wie `CreateNode` bereitstellt. In der Regel müssen vorhandene Schnittstellen nicht geändert werden.



Beachten Sie die Servicekategorie und die Vorgänge:

Feld oder zugehörige Liste	Beschreibung
Servicekategorie	Die Servicekategorie klassifiziert die Schnittstelle. Die Kategorie für die Compute-Schnittstelle ist ebenfalls **Compute**.
CAPI-Schnittstellenvorgänge	Die Schnittstellenvorgänge definieren die JSON-Struktur für den REST-Aufruf und die Parameter, die für die Schnittstelle erforderlich sind.

m. Klicken Sie auf den CAPI-Schnittstellenvorgang **CreateNode**.
Über diesen Vorgang wird das Framework für die Erstellung des virtuellen EC2-Servers in AWS bereitgestellt.

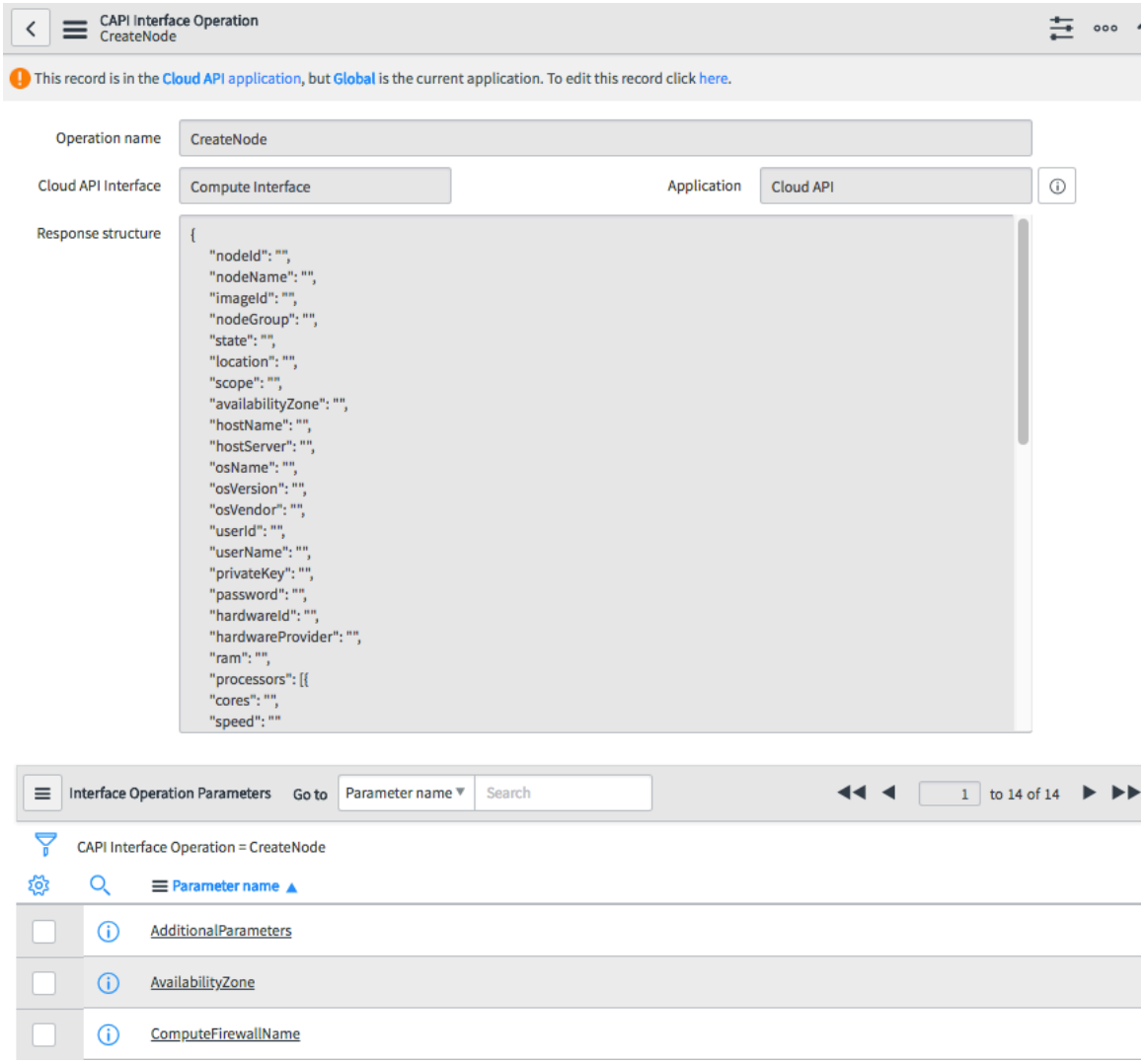
n. Überprüfen Sie die Komponenten des Vorgangs:

Feld oder zugehörige Liste	Beschreibung
Antwortstruktur	Die Antwortstruktur ist das JSON-Framework für den REST API-Aufruf. Diese Struktur bietet eine Liste von Attributen, die AWS zum Erstellen der virtuellen Ressource mit leeren Werten verwenden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld oder zugehörige Liste	Beschreibung
Parameter für Schnittstellenvorgänge	Diese Parameter sind auch die Parameter, die die CAPI-Schnittstelle vom System benötigt, damit sie die Struktur im REST-Aufruf an den Cloud-Anbieter übergeben kann.

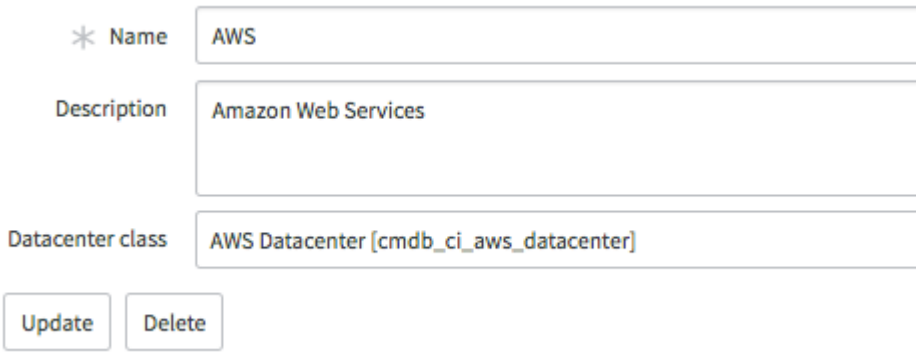


o. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, Und klicken Sie dann auf **Anbieter** Registerkarte.

p. Öffnen Sie den Anbieter **AWS**.

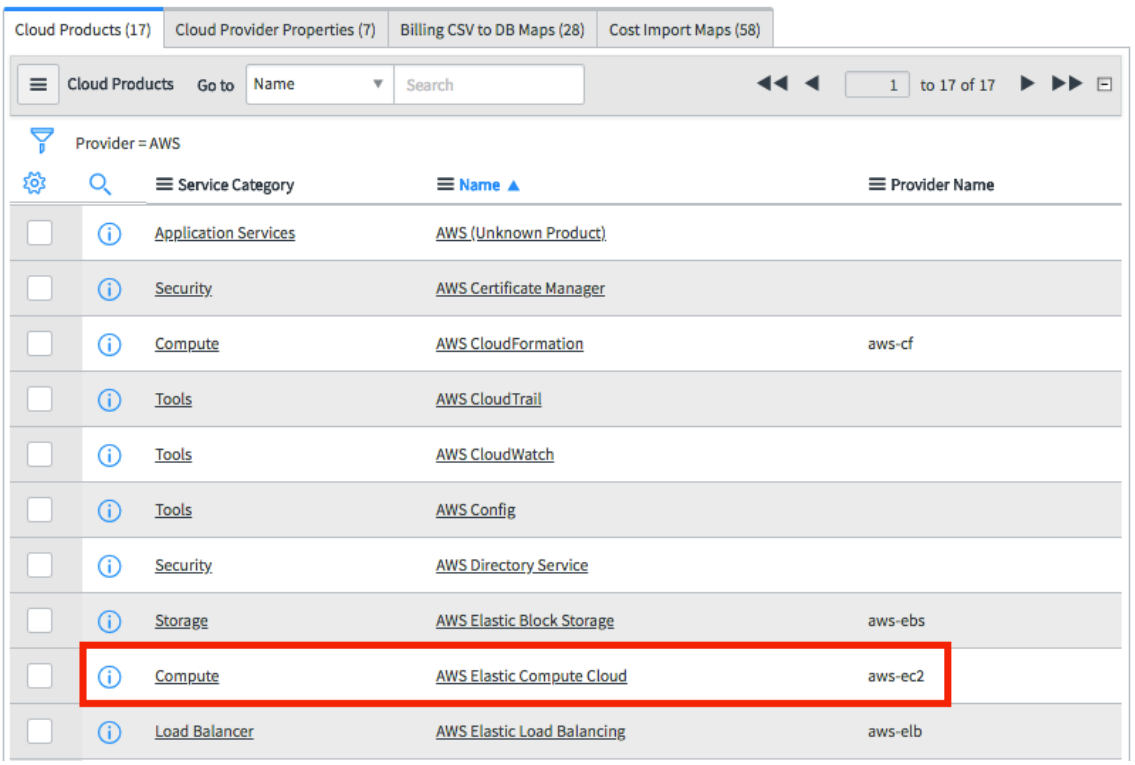
Das Formular „AWS Provider“ (AWS-Anbieter) wird geöffnet und zeigt an, dass dieser Anbieter auf einer vorhandenen CMDB-Klasse basiert: **AWS Datacenter [cmdb_ci_aws_datacenter]**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



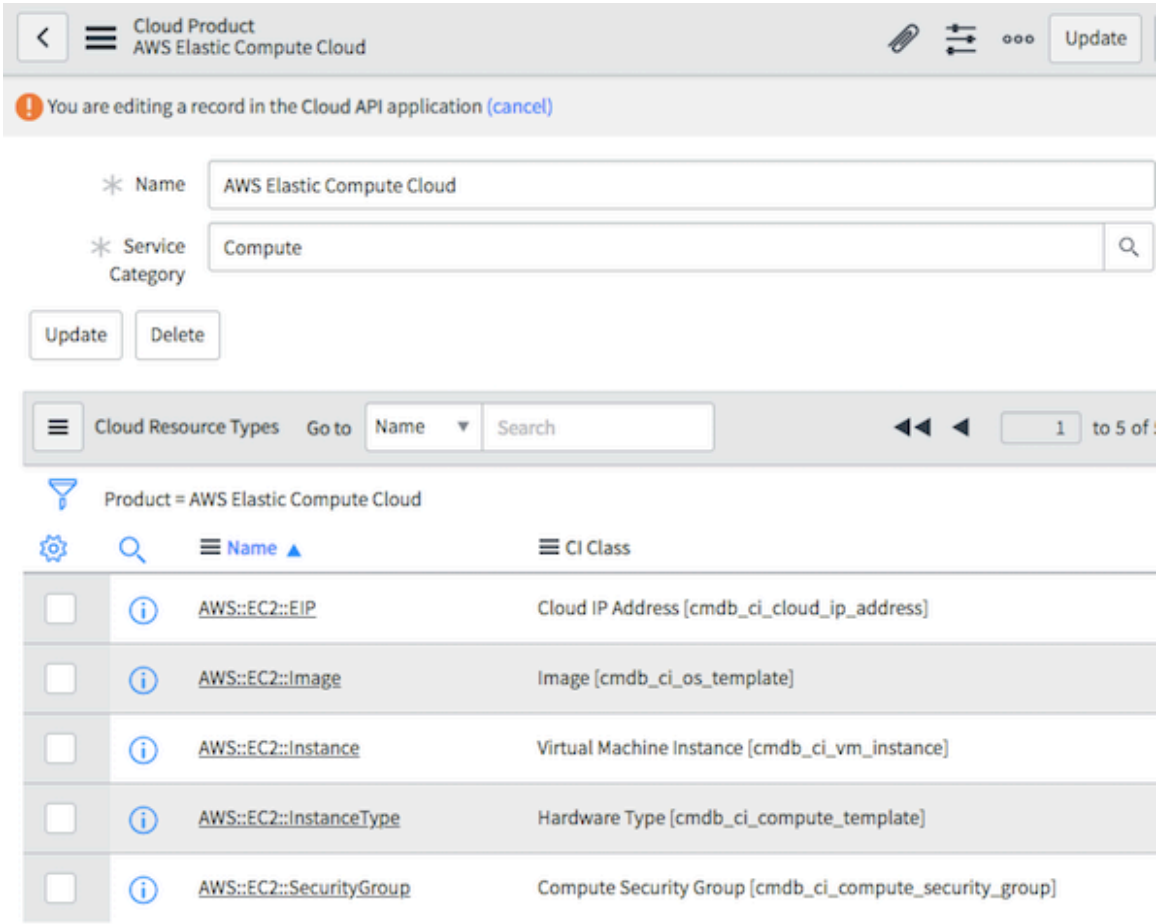
q. Klicken Sie auf die zugehörige Liste „Cloud Products“ (Cloud-Produkte), falls sie noch nicht ausgewählt ist, und sortieren Sie die Liste nach der Spalte **Name**.

Beachten Sie, dass standardmäßig bereits mehrere AWS-Produkte verfügbar sind. Eines der am häufigsten verwendeten AWS-Produkte ist **Elastic Compute Cloud (EC2)**.



r. Klicken Sie in der Spalte **Name** auf **AWS Elastic Compute Cloud**.
Beachten Sie, dass das Produkt viele Ressourcentypen angibt, die jeweils einer CI-Klasse zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

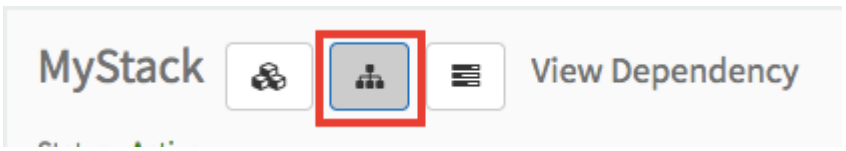


Diese Ressourcentypen geben einige, aber nicht alle CIs an, die sich auf den virtuellen Computer beziehen. Der Antwortprozessor im Ressourcenblock füllt CIs mit Daten aus, wenn AWS den virtuellen Computer bereitstellt.

5. So zeigen Sie die wichtigen mit der VM verbundenen CIs an:

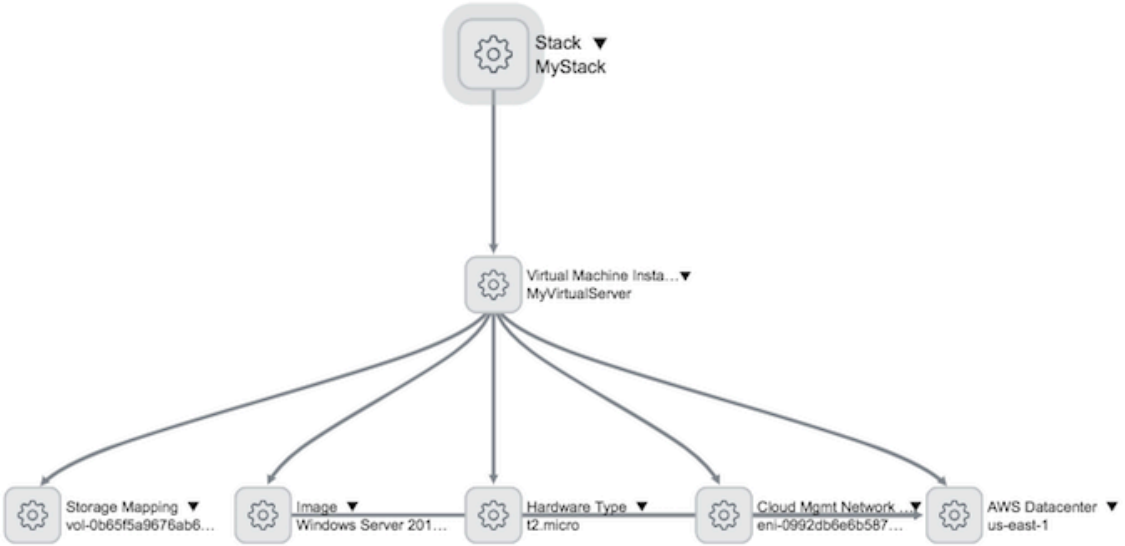
a. Klicken Sie in Cloudbenutzerportal auf **Stapel**, und öffnen Sie dann den Stapel, der die VM enthält.

b. Klicken Sie auf das Symbol View Dependency (Abhängigkeit anzeigen).



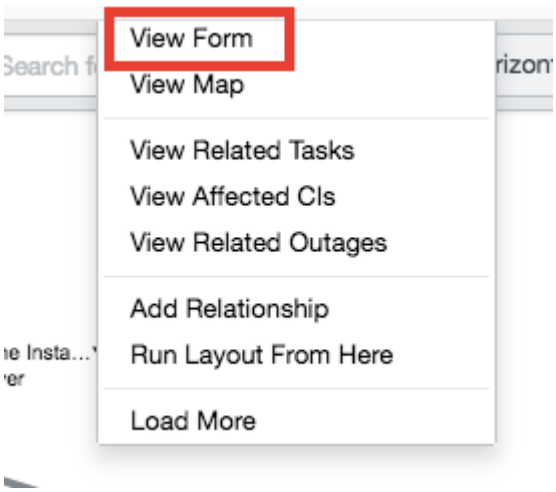
Die Abhängigkeitszuordnung zeigt das Stapel-CI oben, den virtuellen Computer in der Mitte und die verschiedenen zugehörigen CIs unten, z. B. das Bild.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Sie rufen das Formular für den virtuellen Computer in der CMDB auf, indem Sie mit der rechten Maustaste auf den Pfeil neben einem CI, beispielsweise dem virtuellen Computer, klicken.

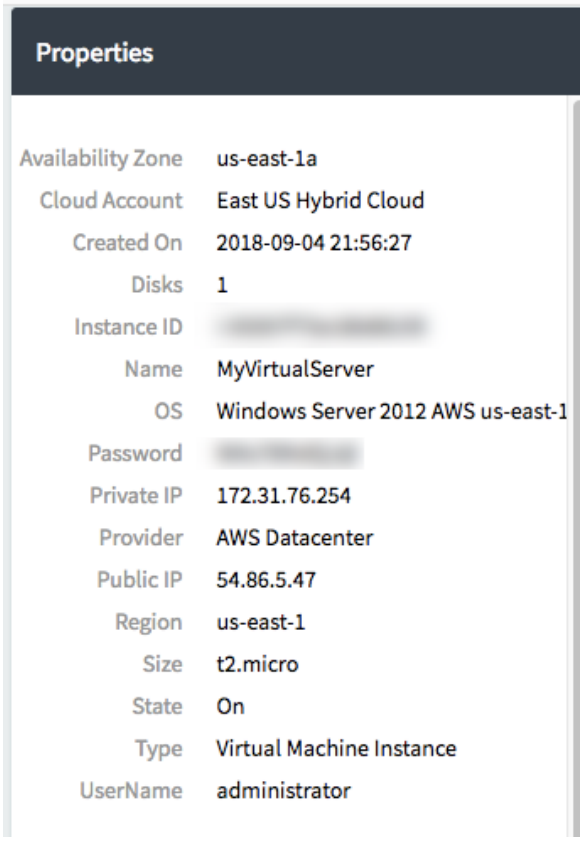
d. Wählen Sie im Menü **View Form** (Formular anzeigen).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das CI-Formular wird geöffnet und zeigt an, dass viele der Informationen bereits auf Cloudbenutzerportal verfügbar sind, wenn Sie die Eigenschaften des virtuellen Computers anzeigen lassen.

Eigenschaften des virtuellen Computers in Cloudbenutzerportal



Einem vorhandenen Provider in CAPI ein Produkt hinzufügen

Die Cloud API (CAPI) Cloud Provisioning and Governance bietet viele Provider wie AWS und Azure und Produkte wie EC2-Instanzen. Sie können jedoch bestehenden Anbietern Produkte für neue Typen von Cloud-Ressourcen hinzufügen.

Vorbereitungen

- Erforderliche Rolle: Administrator
- Überprüfen Sie Standard-CAPI-APIs, und stellen Sie sicher, dass Anbieter und Produkte, die Sie erstellen möchten, nicht bereits angegeben sind.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

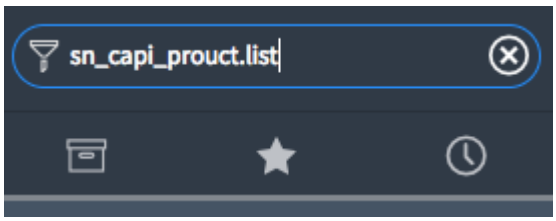
Dieses Thema enthält allgemeine Anweisungen für die Erweiterung eines vorhandenen Cloudanbietes, Produkts und Ressourcentyps.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie in Ihrer Instanz (nicht Portal für Cloud-Admin.), den folgenden Text in den Applikationsfilter ein:

   sn_capi_product.list

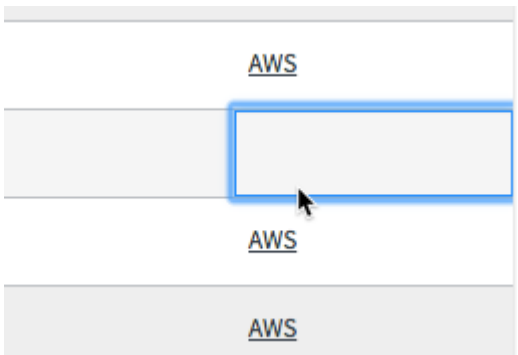
2. Drücken Sie die EINGABETASTE.

   Die Liste der Produkte, die zu allen Anbietern gehören, wird angezeigt. Sie können die Liste filtern, um sicherzustellen, dass das Produkt, das Sie erstellen möchten, nicht bereits bereitgestellt ist.

3. Klicken Sie auf **New** (Neu), geben Sie einen Namen ein und wählen Sie diejenige der vorhandenen Servicekategorien, die am besten geeignet ist.
4. Klicken Sie auf **Absenden**.

   Die Liste der Produkte wird erneut angezeigt.

5. Suchen Sie das von Ihnen erstellte Produkt, und doppelklicken Sie dann auf die leere Zelle in der Spalte **Provider** (Anbieter).

6. Fügen Sie den richtigen Anbieter hinzu.
7. Fügen Sie einen eindeutigen Anbieternamen hinzu: Doppelklicken Sie auf die Zelle im Feld **Provider Name** (Anbietername), und ändern Sie den Namen.

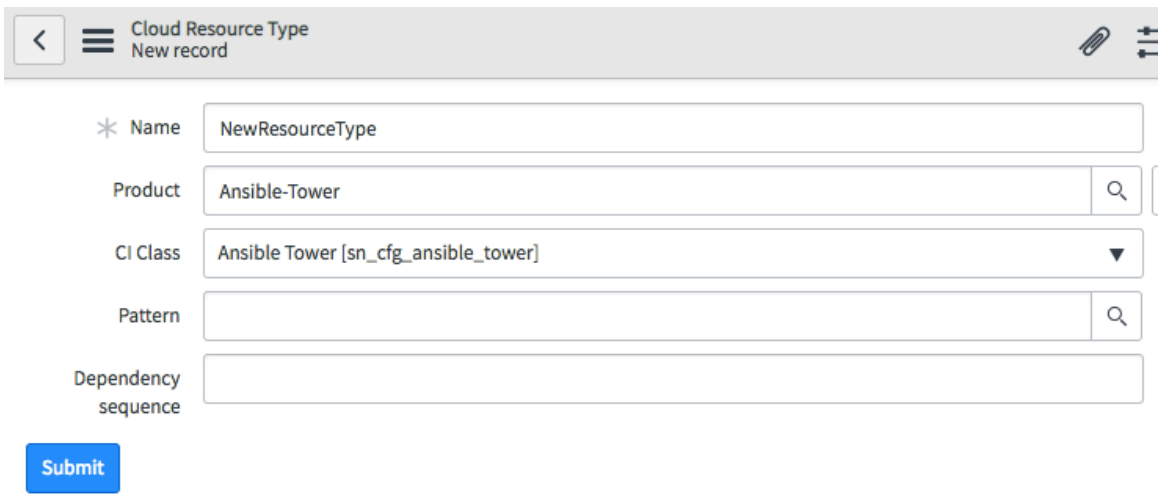
   Das System kann einen Anbieternamen automatisch für Sie generieren, Sie sollten ihn jedoch ändern, um Konflikte mit vorhandenen Anbieternamen zu vermeiden.

8. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-API**an.
9. Klicken Sie auf die Kachel für den Anbieter, dem Sie das neue Produkt hinzugefügt haben.
10. Vergewissern Sie sich, dass sich Ihr Produkt in der zugehörigen Liste **Cloud Products** (Cloud-Produkte) befindet.
11. Klicken Sie auf das Informationssymbol (ⓘ) für das Cloud-Produkt, und klicken Sie dann auf **Open Record** (Datensatz öffnen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Klicken Sie in der zugehörigen Liste „Cloud Resource Types“ (Cloud-Ressourcentypen) auf **New** (Neu), und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger und aussagekräftiger Name.
Produkt	Das Cloud-Produkt, für das Sie den Ressourcentyp erstellen. Wählen Sie aus der Nachschlageliste aus, oder erstellen Sie etwas neu.
CI-Klasse	Eine CMDB-Tabelle, die Sie dem Ressourcentyp zuordnen müssen. Wenn die richtige CMDB-Tabelle nicht angezeigt wird, finden Sie unter Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen Anweisungen dazu, wie Sie eine solche Tabelle erstellen können.
Muster	Das Muster, das zum Erkennen des Ressourcentyps verwendet wird. Wählen Sie aus dem aus Discovery-Muster Suchliste oder Erstellen Sie ein neues Muster .
Abhängigkeitssequenz	Die Reihenfolge, in der der Ressourcentyp bereitgestellt oder erkannt wird. Geben Sie die Reihenfolge basierend auf gegenseitigen Abhängigkeiten von Ressourcen an. Beispiel: Wenn Sie über ein Netzwerk und ein Subnetz verfügen, die erkannt oder erstellt werden sollen, geben Sie einen höheren Rang für das Netzwerk als das Subnetz an, damit die Erkennung oder Erstellung von Ressourcen logisch und sequenziell erfolgt.



13. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen soweit nötig, oder Eine CAPI-Schnittstelle erstellen oder erweitern

Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen

Wenn Basissystem keinen CI-Typ für cloudbasierte virtuelle Ressourcen bereitstellt, können Sie eine CI-Klasse basierend auf der Objektklasse des virtuellen Computers erstellen.

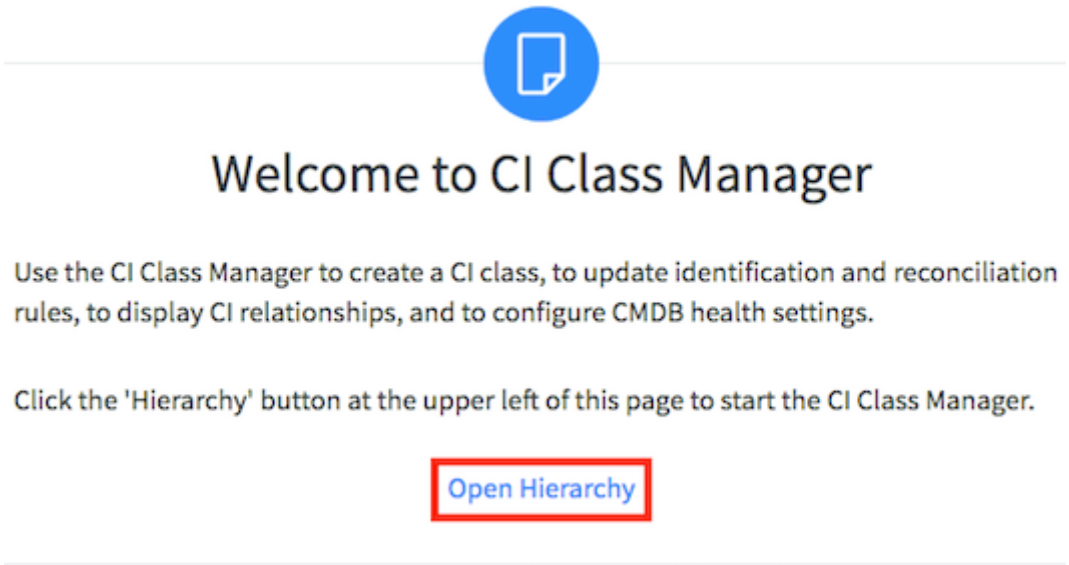
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

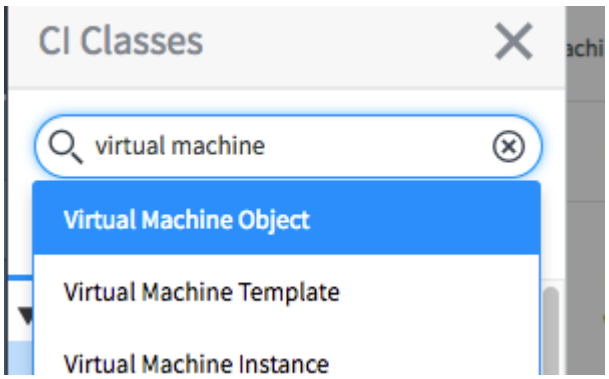
Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Dieses Thema enthält allgemeine Anweisungen für die Erweiterung eines vorhandenen Cloudanbietes, Produkts und Ressourcentyps.

Prozedur
1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**an.
2. Klicken Sie auf **Open Hierarchy** (Hierarchie öffnen).



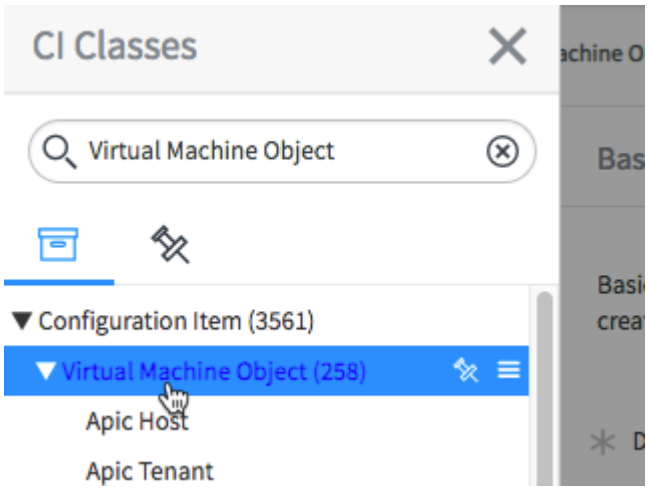
3. Geben Sie im Bereich **CI Classes** (CI-Klassen) im Suchfeld Virtual Machine Object (Objekt d. virtuellen Computers) ein, und wählen Sie dann **Virtual Machine Object**.



4. Klicken Sie auf den Link **Virtual Machine Object** (Objekt d. virtuellen Computers).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Nachfolgeklasse hinzufügen**.
6. Geben Sie im nun eingeblendeten Schritt **Provide Basic Info** (Grundlegende Informationen angeben) einen Namen und eine Beschreibung ein.

   Wenn Sie den Fokus des Cursors aus dem Feld **Display Name** (Anzeigename) entfernen, wird das Feld **Table Name** (Tabellenname) automatisch mit dem gleichen Namen in Kleinbuchstaben ausgefüllt. Bei einer Tabelle in einer bereichsbezogenen Anwendung wird dem Namen ein Namespace-Bezeichner vorangestellt, um anzuzeigen, dass er Teil einer Anwendung ist. Für eine Tabelle in der globalen Anwendung wird dem Namen die Zeichenfolge **u_cmdb_ci** vorangestellt. Sie können das Präfix nicht ändern. Sie können jedoch den Rest des Tabellennamens ändern. Der Name darf nur Kleinbuchstaben, alphanumerische ASCII-Zeichen und Unterstriche (_) enthalten. Die maximale Länge der Zeichenfolge beträgt 80 Zeichen.
7. Klicken Sie auf **Next** (Weiter).
8. Klicken Sie im Schritt **Add Attributes** (Attribute hinzufügen) auf **Derived** (Abgeleitet), und überprüfen Sie dann die Attribute, die von der VM-Objektklasse übernommen wurden.

   Die meisten benötigten Attribute werden bereitgestellt.
9. **Wahlweise:** So fügen Sie ein Attribut hinzu:

   a. Doppelklicken Sie im Feld **Collumn Label** (Spaltenbezeichnung) auf das Feld **Insert a new row** (Neue Zeile einfügen).

   b. Geben Sie einen Namen für die Spalte ein, und klicken Sie auf den grünen Pfeil.

   c. Füllen Sie die restlichen Felder der Zeile aus.
   Siehe Wörterbucheintragsformular Für eine Beschreibung aller Felder.
10. Klicken Sie auf **Next (Weiter)**.
11. Erstellen Sie im Schritt **Set Identification Rule** (Identifizierungsregel festlegen) eine Identifizierungsregel, die eine eindeutige Objekt-ID angibt, die für die Identifizierung erforderlich ist.

> **Wichtig:** Cloud Provisioning and Governance erfordert, dass die Objekt-ID eine Instanz des CI-Klassentyps eindeutig identifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Standardregel unter **Identification Rule** (Identifizierungsregel) auf **Replace** (Ersetzen).

b. Geben Sie einen Namen für die Regel ein, und wählen Sie die Option **Dependent** (Abhängig).

c. Klicken Sie auf **Speichern**.

d. Klicken Sie unter **Bezeichner-Einträge** auf **Hinzufügen**.

e. Verschieben Sie die **Objekt-ID** aus der Spalte **Available** (Verfügbar) in die Spalte **Selected** (Ausgewählt).

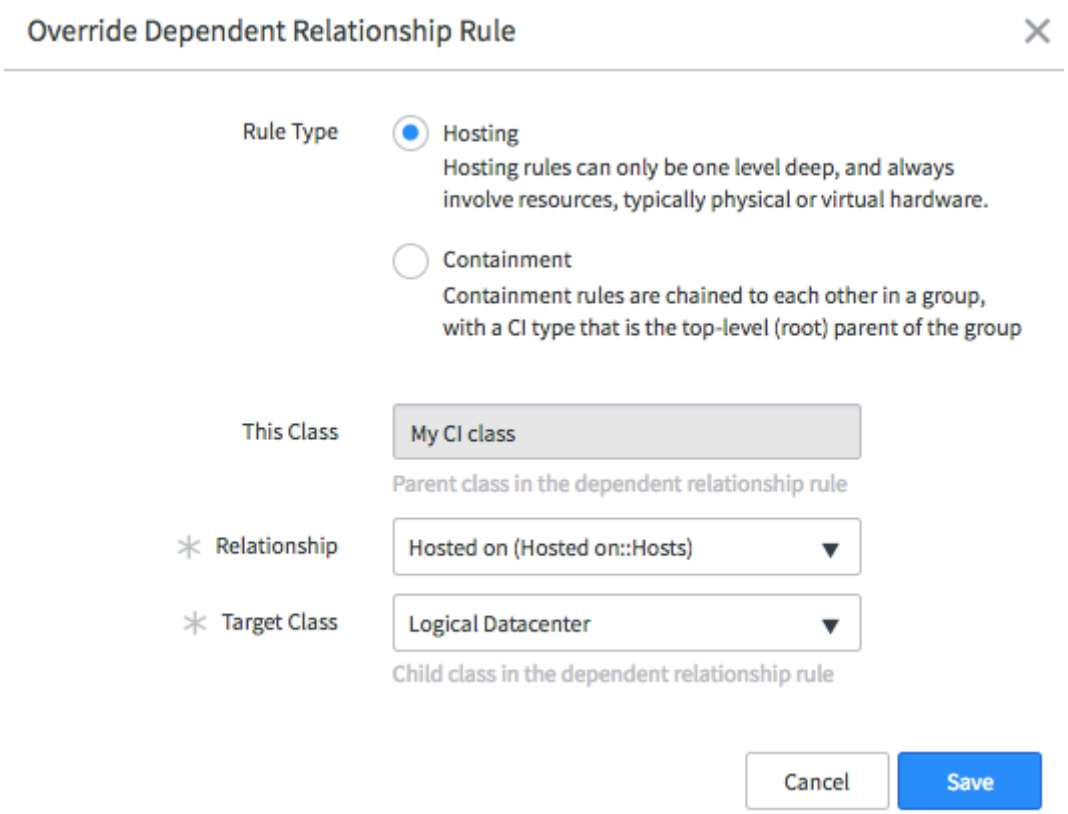
f. Klicken Sie auf **Speichern**.

12. Klicken Sie auf **Next** (Weiter).

13. Klicken Sie im Schritt **Add Dependent Relationships** (Abhängige Beziehungen hinzufügen) auf **Override Dependencies** (Abhängigkeiten überschreiben).

14. Konfigurieren Sie die Beziehung zwischen dieser virtuellen Ressource und dem logischen Rechenzentrum, in dem sie sich befindet:

Feld	Wert
Regeltyp	**Hosting**
Beziehung	**Gehostet auf (Hosted on:Hosts)**
Zielklasse	**Logisches Rechenzentrum**



15. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

16. Klicken Sie auf **Next** (Weiter).
17. Klicken Sie erneut auf **Next** (Weiter), um den Schritt **Add Reconciliation Rules** (Abgleichregeln hinzufügen) zu überspringen, und klicken Sie dann auf **Done** (Fertig), um den Schritt **Add Suggested Relationships** (Vorgeschlagene Beziehungen hinzufügen) zu überspringen.

Nächste Maßnahme

Verwenden Sie die CI-Klasse in einem Ressourcentyp für einen Cloud-Anbieter. Anweisungen dazu finden Sie unter Einem vorhandenen Provider in CAPI ein Produkt hinzufügen.

Ihr Antwortprozessor, der Teil des Ressourcenblocks ist, muss auch die erforderlichen CI-Klassentypen angeben, damit er die CMDB aktualisieren kann. Normalerweise benötigt der Antwortprozessor die Objekt-ID, das spezifische Rechenzentrum und das Cloud-Servicekonto. Unter Beispiel für einen Antwortprozessor für einen virtuellen Server finden Sie Beispiele für Antwortprozessorcode, der CI-Klassen verwendet.

Eine CAPI-Schnittstelle erstellen oder erweitern

Sie können eine neue CAPI-Schnittstelle erstellen oder eine vorhandene erweitern, indem Sie neue Vorgänge hinzufügen.

Vorbereitungen

- Erforderliche Rolle: admin
- Überprüfen Sie Standard-CAPI-APIs und stellen Sie sicher, dass weder Anbieter noch Produkte, die Sie erstellen möchten, bereits vorliegen.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

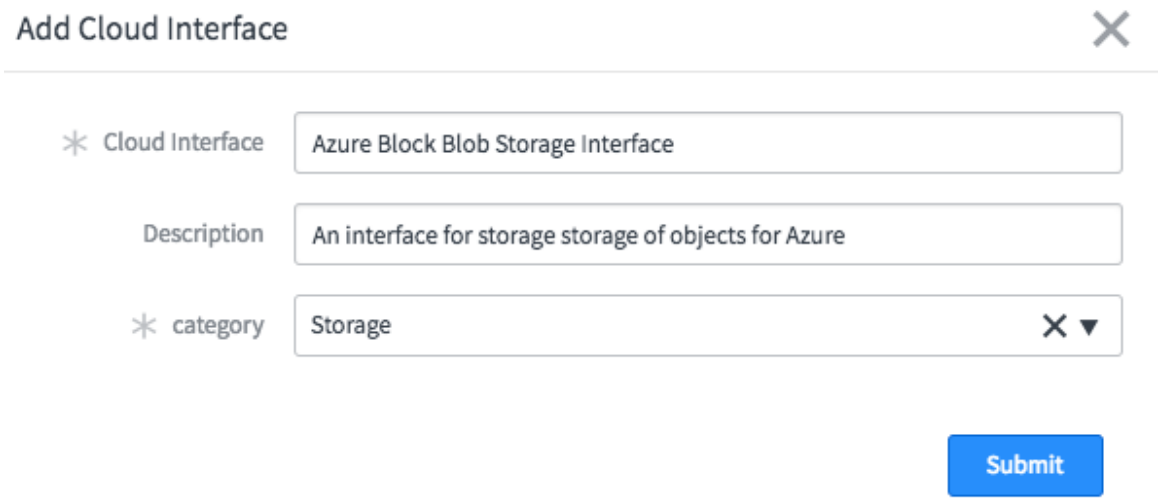
Normalerweise können Sie die Standardschnittstellen verwenden, die in der Anwendung Cloud Provisioning and Governance bereitgestellt werden. Für das Erstellen einer benutzerdefinierten Schnittstelle sollte eine ähnliche, bereits bestehende als Basis verwendet werden.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-API**, Und klicken Sie dann auf **Schnittstelle** Registerkarte.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Fenster „Add Cloud interface“ (Cloudschnittstelle hinzufügen) einen Namen für die Schnittstelle und eine hilfreiche Beschreibung ein, und wählen Sie die relevanteste Kategorie aus, der die API-Schnittstelle angehören soll.

   Dieses Beispiel zeigt eine Schnittstelle für Azure-Speicher:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

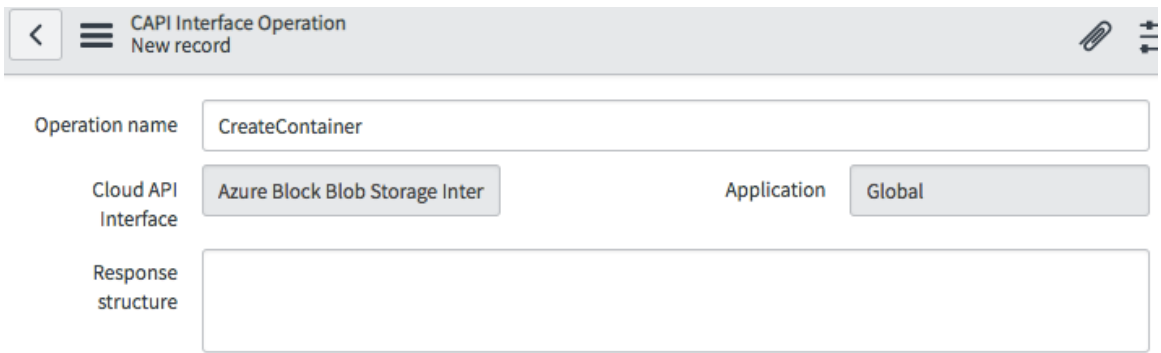


4. Klicken Sie in der zugehörigen Liste für CAPI-Schnittstellenvorgänge auf **New** (Neu).

   Jeder Vorgang, den Sie erstellen, entspricht einem anderen REST API-Aufruf.

5. Geben Sie einen Namen für den Vorgang an, der der API entspricht, die Sie im Anbieter aufrufen möchten.

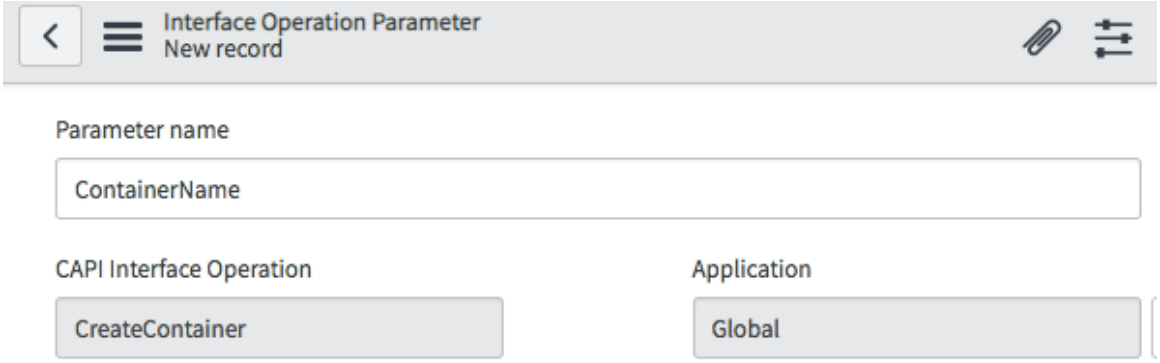
   Beispielsweise können Sie einen Vorgang namens `CreateContainer` erstellen, der dem Vorgang „Create Container“ (Container erstellen) in Azure entspricht.



6. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
7. Klicken Sie in der zugehörigen Liste „Schnittstellen-Vorgangsparameter“ auf **Neu**.
8. Erstellen Sie einen Parameter, den der Vorgang gemäß der Definition der REST API-Dokumentation des Cloud-Anbieters benötigt.

   Wenn Sie die Parameter nicht kennen, schlägt der Vorgang fehl. Im Beispiel mit Azure-Speicher muss der Vorgang `CreateContainer` den Namen des Containers haben, der hier als `ContainerName` bezeichnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Absenden**.
10. Fügen Sie so viele Parameter hinzu, wie Sie für den Vorgang benötigen, und fügen Sie dann alle erforderlichen Vorgänge hinzu.

Nächste Maßnahme

Eine CAPI-API erstellen

Eine CAPI-API erstellen

Wenn die vorhandenen CAPI-APIs nicht in die CAPI-Schnittstelle für einen Anbieter integriert werden, können Sie eine API erstellen. Die Schritte in Ressourcenblöcken können die von Ihnen verwendeten API-Methoden aufrufen, wenn Vorgänge ausgeführt werden.

Vorbereitungen

- Erforderliche Rolle: admin
- Überprüfen Sie Standard-CAPI-APIs und stellen Sie sicher, dass weder Anbieter noch Produkte, die Sie erstellen, bereits vorliegen.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Thema enthält Anweisungen zum Erstellen einer CAPI-API. Sie decken auch die Konfiguration von CAPI, Ressourcenblöcken, Blueprints und Anmeldeinformationszuordnungen ab.

Prozedur

1. In Portal für Cloud-Admin., Navigieren Sie zu **Entwurf** > **Cloud-API**an.
2. Klicken Sie auf die Registerkarte **API**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Cloud-API	Geben Sie einen beschreibenden Namen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schnittstelle	Wählen Sie eine der vorhandenen Schnittstellen aus, die die gewünschten Vorgänge bereitstellen.
Connector	Der **Script Connector** (Skript-Connector) wird in diesem Feld angezeigt, wenn der Connector ein sofort verfügbarer Java-Connector ist, der nicht geändert werden kann. Sie müssen diese Skript-Connectors nicht ändern.
Produkt	Wählen Sie das Produkt aus, das Teil des Anbieters ist. Das Produkt enthält Ressourcentypen in der CMDB.
Version	Geben Sie eine Versionsnummer an, um diese API zu identifizieren. Geben Sie 1.0 ein, wenn diese API die erste Version ist. Sie können mehrere Versionen derselben API erstellen und dann in den Vorgangsschritten der Ressourcenblöcke auf die jeweiligen Versionen verweisen.
Geskriptet	Dieses Feld wird ausgewählt, wenn der Wert von **Interface** (Schnittstelle) **Script Connector** (Script-Connector) lautet.
Skripttyp	Wählen Sie die Sprache für das Skript aus. **Hinweis:** Es empfiehlt sich JavaScript. Die Methodenzuordnungen verwenden in Javascript geschriebene MID-Server-Skripteinbindungen.
ExecuteScriptOnInstance	
Beschreibung	Hier sollte sich die API-Beschreibung befinden.

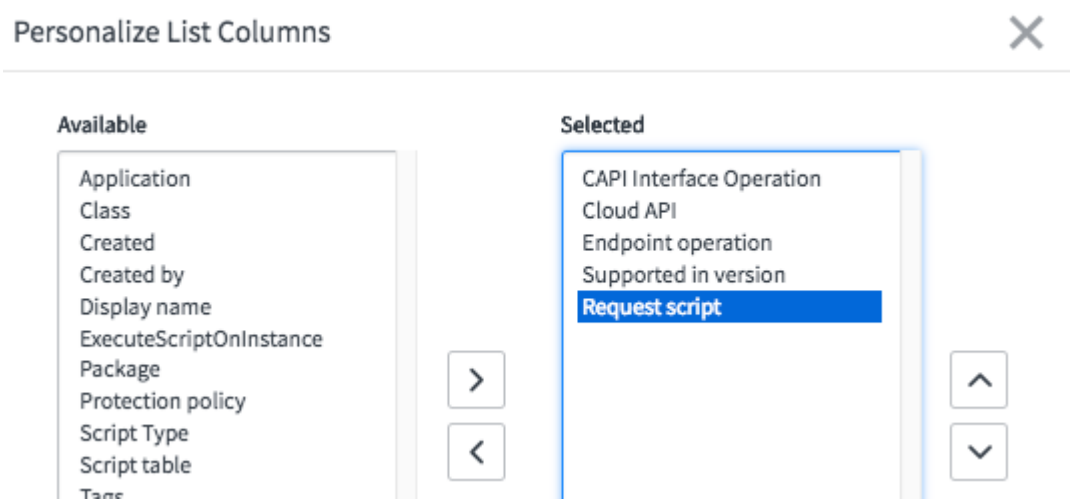
5. Stellen Sie sicher, dass alle erforderlichen Vorgänge in der zugehörigen Liste der **CAPI-Methodenzuordnungen** angezeigt werden.

   Die Vorgänge in der Liste CAPI-Methodenzuordnungen sind in der von Ihnen ausgewählten Schnittstelle die gleichen Vorgänge. Sie sind an diese API gebunden. Für diese Liste sind weder Hinzufügen noch Entfernen von Vorgängen möglich. Einige der Vorgänge, insbesondere Azure-Vorgänge, verwenden MID-Server-Skripteinbindungen, die die tatsächliche Implementierung für die API ausführen. Das Skript enthält einen Aufruf der REST API für den Anbieter, z. B. AWS oder Azure. Sie sollten die API in der Dokumentation des Anbieters finden.

6. So rufen Sie die Skripteinbindung für eine CAPI-Methodenzuordnung auf:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

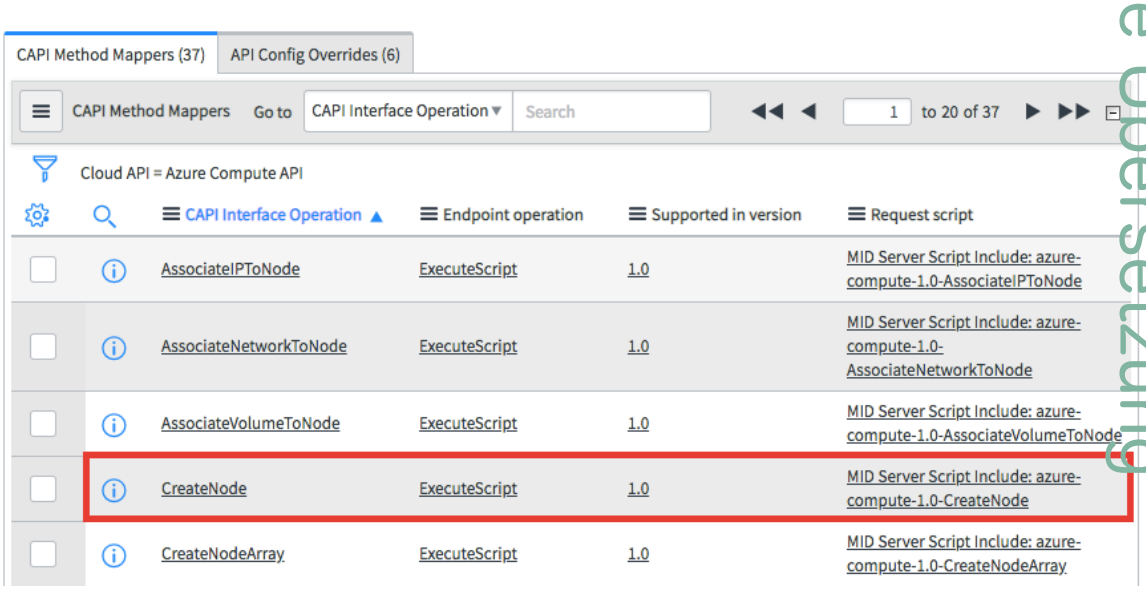
a. Klicken Sie auf das Zahnradsymbol ( ) auf der zugehörigen Liste **CAPI Method Mappers** (CAPI-Methodenzuordnungen), fügen Sie das Feld **Request Script** (Skript anfordern) der **ausgewählten** Spalte hinzu, und klicken Sie dann auf **OK**.



Die Skripteinbindungen von MID-Server werden jetzt in der Liste der Methodenzuordnungen angezeigt.

b. Klicken Sie auf den Namen eines Skripts, um die Skripteinbindung aufzurufen.

In diesem Beispiel verwendet der Vorgang **CreateNode** die Skripteinbindung *azure-compute-1.0-CreateNode*.



Diese Skripteinbindung enthält folgenden Code:

```
createNode();
function createNode(){
  var acp = new AzureComputeVirtualMachine(this.parameters, this.headers);
   //this passes the parameters and headers into the AzureComputeVirtualMachine script
 include.
  var vm = acp.createVirtualMachine();
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  return vm;
}
```

Sie werden bemerken, dass der Code Skripteinbindung `AzureComputeVirtualMachine` aufruft, die standardmäßig mit der Anwendung Cloud Provisioning and Governance verfügbar ist. Sie enthält alle API-Aufrufe bei Azure mit virtuellen Computern.

7. Erstellen Sie eine Überschreibung der API-Konfiguration, um die erforderlichen Anmeldeinformationen an den Cloud-Anbieter zu übergeben.

   Sie müssen auch Header-Informationen übergeben, die für die REST API des Cloud-Anbieters erforderlich sind. API-Konfigurationsüberschreibungen sind erforderlich, da Anmeldeinformationsdaten nicht enthalten sind, wenn die Instanz den REST-Aufruf bei der Cloud-Anbieter-API durchführt.

   Tipp: Wenn Sie nicht wissen, welche API-Konfigurationsüberschreibungen erstellt werden sollen, suchen Sie nach einer ähnlichen API in CAPI, und verwenden Sie dieselben Überschreibungen. Wenn Sie beispielsweise eine API für AWS-Speicher erstellen, suchen Sie nach anderen AWS-APIs wie AWS Block Storage oder AWS Compute.

   a. Klicken Sie in der den API-Konfigurationsüberschreibungen zugehörigen Liste auf **New** (Neu).

   b. Klicken Sie auf das Suchsymbol, und wählen Sie einen vorhandenen Konfigurationsparameter aus. Viele nützliche Parameter werden standardmäßig bereitgestellt, z. B. **Identity** (Identität), **Credentials** (Anmeldeinformationen) usw.

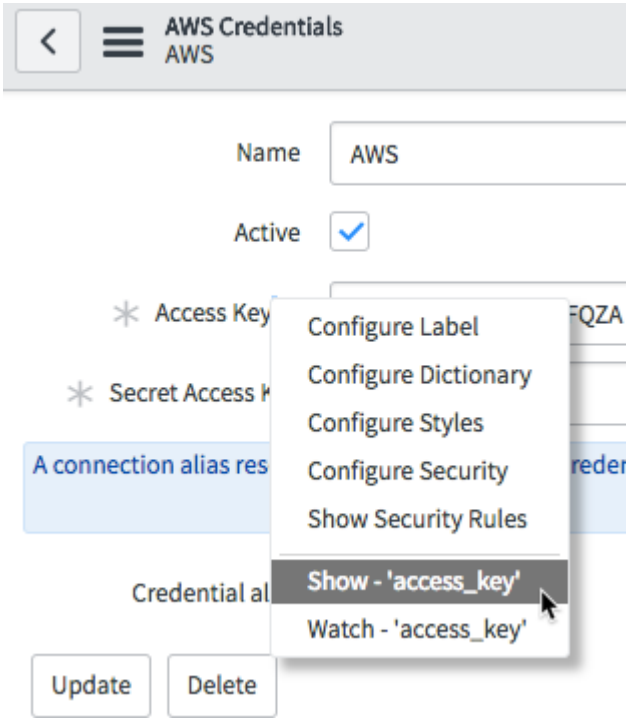
   c. Geben Sie einen **Überschreibungswert** ein.

      Sie können einen statischen Wert festlegen oder einen Wert im Format `$(CloudCredential.attribute_name)` aus dem System verwenden. Die Komponente `CloudCredential` entsperrt den Wert aus dem Anmeldeinformationsspeicher. Die Komponente `attribute_name` ist ein Attribut, das von den konkreten Anmeldeinformationen, Alias- oder Endpunkt-URLs abhängt, die Sie abrufen möchten.

      Wenn Sie zu navigieren **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen** Und öffnen Sie Ihre AWS-Anmeldeinformationen. Sie können mit der rechten Maustaste auf klicken **Zugriffsschlüssel-ID** Und zeigen Sie den Namen der Spalte in der Tabelle „Anmeldeinformationen“ an, in der der Zugriffsschlüssel gespeichert ist. In diesem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall wird der Zugangsschlüssel in der Spalte `access_key` gespeichert. Daher muss der Überschreibungswert `$(CloudCredential.access_key)` sein.



8. Wenn Sie einen Konfigurationsparameter für die API-Konfigurationsüberschreibung erstellen müssen, gehen Sie wie folgt vor:

   a. Klicken Sie im Formular „API Config Override“ (API-Konfigurationsüberschreibung) auf das Suchsymbol im Feld **Config Parameter** (Konfigurationsparameter).

   b. Klicken Sie im Fenster „Config Parameter“ (Konfigurationsparameter) auf **New** (Neu) und füllen Sie das Formular aus.

Feld	Beschreibung
Konfigurationsparametername	Geben Sie einen beschreibenden Namen ein.
Standardwert	Sie können einen optionalen Standardwert festlegen.
Endpunkt	Dieses Feld ist schreibgeschützt.
Beschreibung	Geben Sie eine erläuternde Beschreibung ein.
Konfigurationsdatentypen	Wählen Sie den Datentyp aus: ▪ **Zeichenfolge** ▪ **DateTime** ▪ **Datum** ▪ **Lang** ▪ **Passwort** ▪ **Boolean**
Konfigurationstyp	Wählen Sie den Konfigurationstyp aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Header: Verwenden Sie diesen Wert, um die Überschreibungswerte als Header zu übergeben. Wenn Sie über eine MID-Server-Skripteinbindung als Teil der API verfügen, und diese this.headers als Parameter verwendet, werden die Überschreibungswerte der Anbieter-API übergeben. ▪ Config ▪ URI-Konfiguration

9. Ändern Sie bei Bedarf die Skripteinbindungen, die die Vorgänge für die Cloud-Anbieter-API ausführen:

a. Klicken Sie auf dem Cloud-API-Formular in der zugehörigen Liste der CAPI-Methodenzuordnungen auf das Informationssymbol ( ) neben dem CAPI-Schnittstellenvorgang.
Klicken Sie nicht auf den Namen des CAPI-Schnittstellenvorgangs.

b. Klicken Sie auf **Datensatz öffnen**.

c. Im Vorgangsformular können Sie die folgenden Feldwerte ändern:

Feld	Beschreibung
Endpunktvorgang	Behalten Sie den standardmäßigen Endpunktvorgang **Execute Script** (Skript ausführen) bei.
Unterstützt in Version	Üblicherweise muss dieser Wert nicht geändert werden. Ändern Sie die Version von **Supported in** (Unterstützt in), um die Methodenzuordnung in einer anderen Version der API zu verwenden. Standardmäßig ist für die Methodenzuordnungen dieselbe Versionsnummer festgelegt wie für die zugehörige API.

d. Klicken Sie im Feld **Request Script** (Skript anfordern) auf das Informationssymbol ( ) neben der Platzhalter-Skripteinbindung MID-Server, um Änderungen vorzunehmen.

e. Erstellen Sie mit dem Formular für Skripteinbindungen das gewünschte Skript.

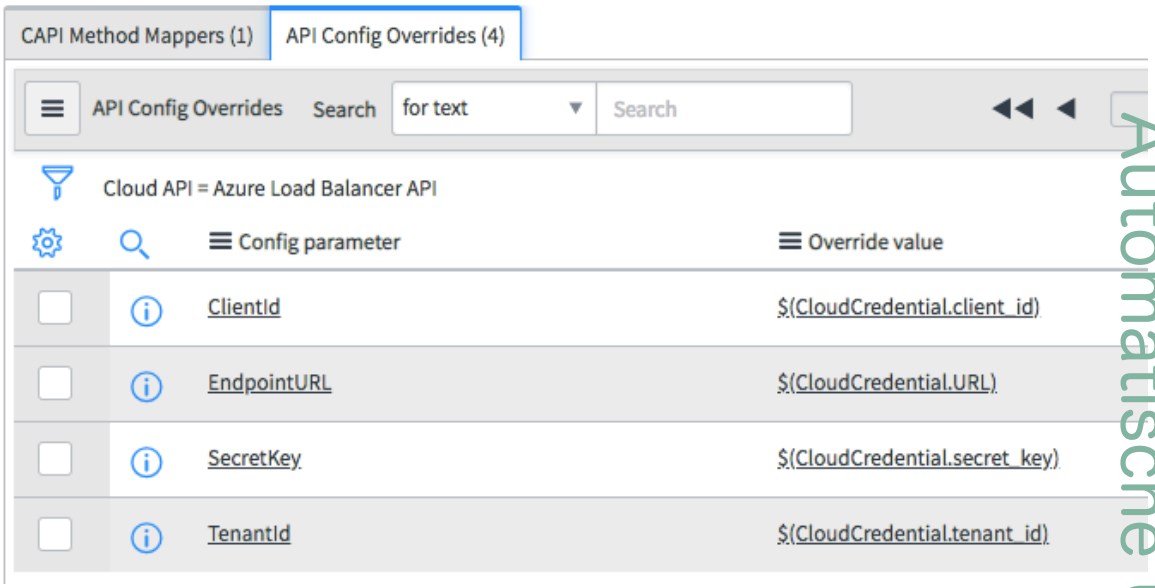
Das folgende Beispiel-JavaScript listet Azure-Lastenausgleichsmodule auf. Beachten Sie die hilfreichen Kommentare:

```
getResourceInfo();

function getResourceInfo() {
 var anpi = new AzureLoadBalancer(this.parameters, this.headers);

    //this calls the 'AzureLoadBalancer' MID-Server script include, which in turn
    //calls the 'AzureCloudAPIBase' script include, both of which
    //are already in your instance by default.
    //The 'AzureCloudBase' script include runs a query for resources of a given type in a
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
//specified region.

var items = anpi.listResourcesByRegionOrIDs();
    //This function is in the 'AzureCloudAPIBase' script include. It calls the Azure API.

return items;
}
```

Die für diesen Vorgang bereitgestellten Überschreibungen sind das, was Azure benötigt, um die Lastenausgleichsmodule zu finden: Client-ID, Mandanten-ID, geheimer Schlüssel und Endpunkt-URL:



Für das Integrationsbeispiel von Google Cloud ist auch eine MID-Server-JAR-Datei erforderlich.

f. Klicken Sie auf **Absenden**.

g. Ändern Sie die Skripteinbindung für jeden Vorgang.

Cloud-Benutzerportal

Das Cloud-Benutzerportal bietet Ihnen direkten Zugriff auf alle täglichen Cloud-Aktivitäten.

Cloud-Benutzerportal

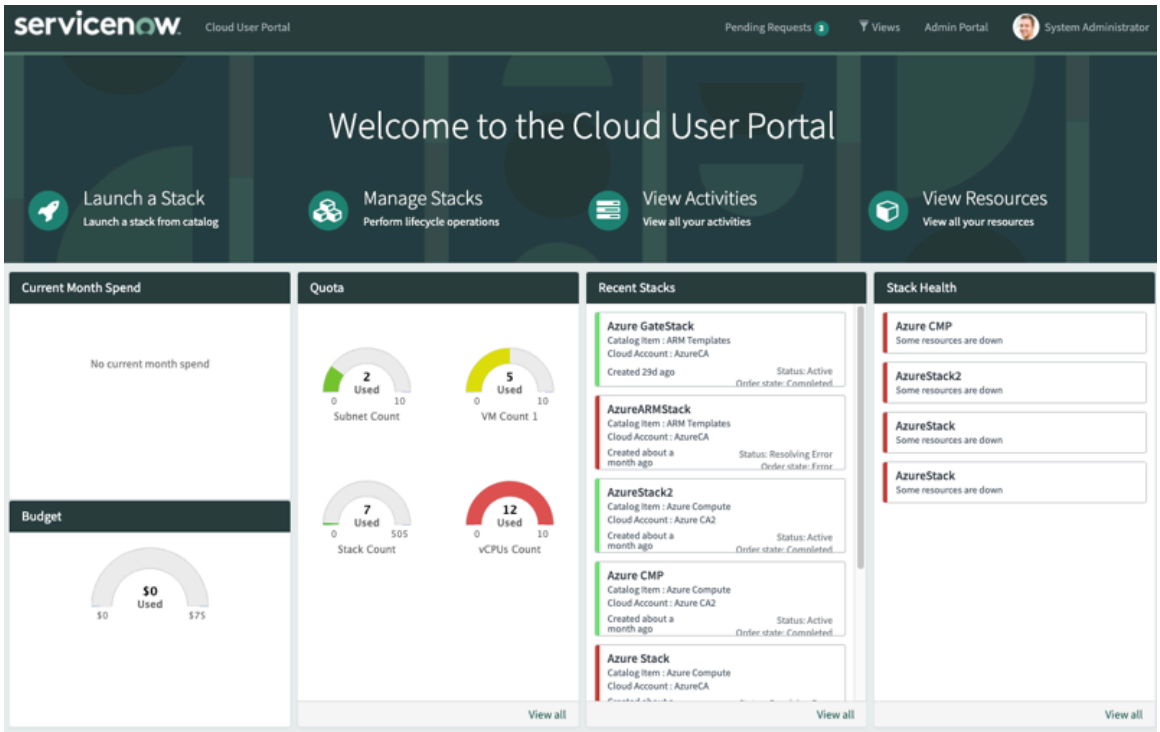
Verwenden Sie das Cloud-Benutzerportal für folgende Vorgänge:

- Kontingente, Kosten, Budgets, Lebenszyklus-Events, Stapelintegrität und Anforderungen überwachen
- Stapel aus dem Servicekatalog anfordern und Anforderungen nachverfolgen.
- Lebenszyklusvorgänge für Stapel und Ressourcen anfordern (z. B. stoppen, starten oder Bereitstellung aufheben)
- Erstellen und Nachverfolgen von Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Overview“ (Übersicht) verwenden



Aufgaben auf der Seite „Overview“ (Übersicht)

Einen Stapel starten	Öffnen Sie den Servicekatalog von Elementen, die Sie anfordern können. Sie fordern ein Element an, und wenn die Anforderung genehmigt wird, startet das System den Stapel. Weitere Informationen finden Sie unter Einen Stapel starten.
Stapel verwalten	Sehen Sie die Ihnen zugewiesenen Stapel an. Weitere Informationen finden Sie unter Einen Stapel verwalten.
Aktivitäten anzeigen	Sehen Sie Aktivitäten für Ihre Stapel und Ressourcen an. Zu den Aktivitäten gehören Stapelanforderungen, Change-Anforderungen, Incidents, Cloud-Ereignisse und SSH-Schlüssel. Vgl. View Activities (Aktivitäten anzeigen).
Ressourcen anzeigen	Öffnet die Seite „Ressourcendetails“ zum Anzeigen von Details und Status einer Ressource. Weitere Informationen finden Sie unter Ressourcen verwalten.
Ausstehende Anforderungen	Wenn Sie eine Anforderung für einen Stapel übermitteln, zeigt die Seite **Acitivities** (Aktivitäten) Fortschritt und Status der Stapelanforderung an, und ein Link und ein Zähler für **Pending Requests** (ausstehende Anforderungen) werden angezeigt. Klicken Sie auf den Link, um eine Zusammenfassung der ausstehenden Stapelanforderungen aufzurufen. Weitere Informationen finden Sie unter Eine Stapel-Anforderung nachverfolgen.

Wichtig: Ab Release Zurich sind die Widgets für aktuelle Monatsausgaben und Budget für nicht domänengetrennte Instanzen veraltet.

Schnellübersicht über Statusberichte auf der Seite „Overview“ (Übersicht)

Ansichten	Ein Filter zum Aufrufen und Verwalten Ihrer Ressourcen sowie der Ressourcen, die der Gruppe zugewiesen sind, der Sie angehören.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnellübersicht über Statusberichte auf der Seite „Overview“ (Übersicht) (Fortsetzung)

Aktuelle Monatsausgaben	Ein Diagramm, das die Kosten für Ihre Cloudressourcen nach Kategorie anzeigt.
Budget	Ein Bogendiagramm, das auf dem verbrauchten des Ihnen zugewiesenen Budgets basiert.
Mengen	In einem Diagramm wird der Kontingentverbrauch für kontingentdefinierte Ressourcentypen wie VM-Anzahl, vCPU-Anzahl, Größe des Speichervolume, Netzwerkanzahl und Stapelanzahl angezeigt. Sie können das von Ihnen verbrauchte Kontingent im Vergleich zu Ihrem maximal zugeteilten Kontingent anzeigen. Weitere Informationen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.
Letzte Stapel	Zehn Stapel, die Sie zuletzt angefordert haben. Jeder Eintrag zeigt **Namen**, angefordertes **Katalogelement**, das zum Anfordern des Stapels verwendete **Cloud-Konto** und den Auftragsstatus des angeforderten Stapels. Klicken Sie auf einen **Namen**, um die Stapeldetails aufzurufen.
Stapelintegrität	Zeigt die letzten 10 Elemente an: Für bereitgestellte Stapel erstellte Incidents oder aktive Stapel mit deaktivierter Ressource. Zeigt auch die Ressourcen an, die nicht verfügbar sind. Klicken Sie auf ein Element, um die Stapeldetails aufzurufen. Farbcodes für Incident-Typ: • Rot: Ausfall. • Orange: Leistungsproblem oder Funktionsstörung. • Grau: Frage oder Anforderung.

Verwenden der Taskleiste

Über die Taskleiste können Sie die folgenden Aktionen ausführen:

Übersicht	Rückkehr zur Homepage des Cloudbenutzerportals.
Katalog	Öffnet den Servicekatalog von Elementen, die Sie anfordern können. Wenn Sie eine **Servicekategorie** auswählen (VM, Compute, Netzwerk, Speicher usw.), werden im Abschnitt **All Items** (Alle Elemente) die Elemente in der ausgewählten Kategorie aufgelistet. Klicken Sie auf **Launch** (Starten), um ein Element anzufordern. Weitere Informationen finden Sie unter Einen Stapel starten.
Stapel	Listet alle Stapel auf, die Ihnen zugewiesen sind. Wählen Sie ein Katalogelement aus, um die vom Element gestarteten Stapel anzeigen zu lassen. Klicken Sie auf einen Stapel, um Details aufzurufen – alle Ressourcen, Ressourceneigenschaften, Aktivitäten und Lebenszyklusvorgänge. Weitere Informationen finden Sie unter Einen Stapel verwalten.
Ressourcen	Listet einzelne Ressourcen der bereitgestellten Stapel auf, die Ihnen zugewiesen sind, unabhängig davon, wer den Stapel angefordert hat. Weitere Informationen finden Sie unter Ressourcen verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivitäten	Stapel-Anforderungen, Change-Anforderungen, Cloud-Lebenszyklus-Events (falls konfiguriert) und Incidents, die Ihren Stapeln und Ressourcen zugeordnet sind. SSH-Schlüssel, die Sie erstellt haben oder die für Sie generiert wurden. Vgl. View Activities (Aktivitäten anzeigen).

Das Cloud-Benutzerportal durchsuchen

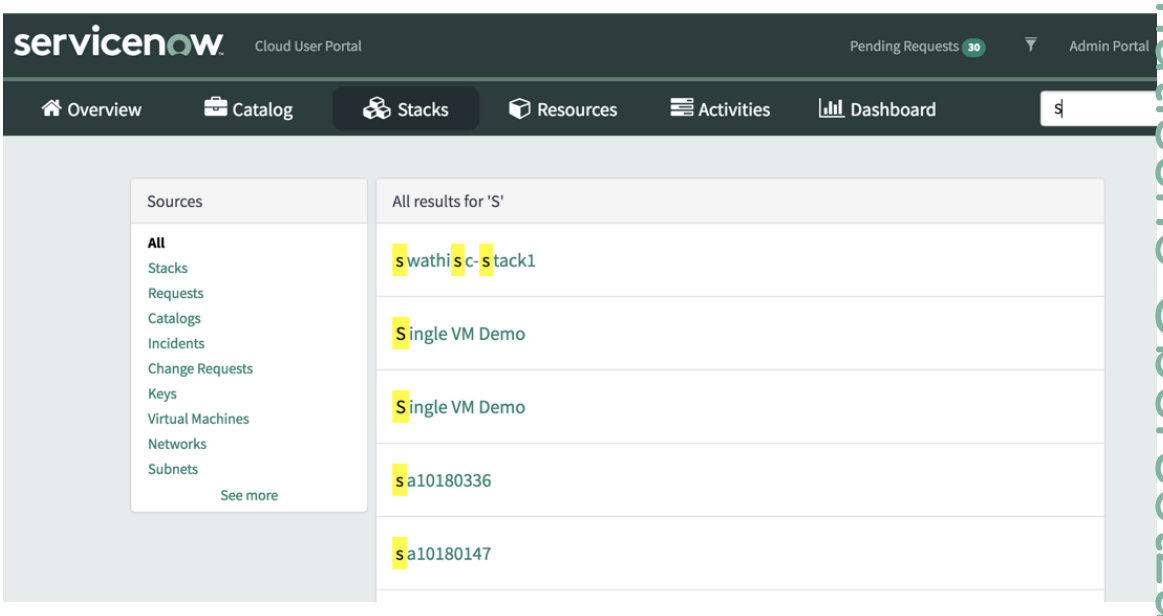
Die Suchseite gibt Suchergebnisse zurück und bietet Filter, mit denen Sie Ergebnisse einschränken können.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Geben Sie auf einer beliebigen Portalseite Text in das Textfeld **Search** (Suchen) ein, und drücken Sie die **Eingabetaste**.
2. Zum Filtern der Suchergebnisse auf der Seite **Cloud Search** (Cloudsuche) klicken Sie auf eine Kategorie. In diesem Beispiel werden nur **Stapel**, die den Suchtext s umfassen, in der Liste **Search Results** (Suchergebnisse) angezeigt:



Einen Stapel starten

Starten Sie einen Stapel von Cloud-Ressourcen, um eine Anforderung für ein Element im Servicekatalog zu übermitteln. Sie können einen Stapel über die Übersichtsseite des Cloud-Benutzerportals starten.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Wenn Sie eine Anforderung für ein Element an den Servicekatalog übermitteln, stellt das System den Stapel in der Regel sofort bereit. Manchmal muss die Anforderung zuerst genehmigt werden.

Wenn für eine Ressource in einem Stapel beim Zugriff über SSH Anmeldeinformationen erforderlich sind, müssen Sie ein SSH-Schlüsselpaar erstellen, bevor Sie den Stapel starten können. Siehe Einen SSH-Schlüssel erstellen und Einen SSH-Schlüssel herunterladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie das Anforderungsformular mit einer der folgenden Methoden:
   - Klicken Sie auf der Übersichtsseite auf **Einen Stapel starten**. Standardmäßig werden alle Katalogelemente in allen Servicekategorien aufgelistet. Wählen Sie eine **Servicekategorie**, und klicken Sie dann auf den **Namen** eines Katalogelements.
   - Öffnen Sie die Seite **Catalog** (Katalog). Standardmäßig werden alle Katalogelemente in allen Servicekategorien aufgelistet. Wählen Sie eine **Servicekategorie**, und klicken Sie dann auf **Launch** (Starten) für ein Katalogelement.
2. Geben Sie in jedem Abschnitt des Formulars die Werte ein, die Ihre Anforderung konfigurieren.

   Die Formularfelder unterscheiden sich für jedes Katalogangebot. Wenden Sie sich an Ihren Administrator für Cloud Provisioning and Governance, wenn Sie Fragen zu den Feldern haben.

   Wichtig: Wenn Sie im Formular eine Benutzergruppe auswählen, werden die Kontingentgrenzen für Sie und die Benutzergruppe (zu der Sie gehören) im Abschnitt „Kontingent“ angezeigt.

   Die folgenden Unterschritte gelten nur, wenn Sie den Terraform-Connector und installierbare Terraform-Konfigurationen verwenden.

   a. Wählen Sie im Abschnitt „Allgemeine Informationen“ für die Option `UseExistingWorkspace` den Eintrag **Ja** aus, um vorhandene Arbeitsbereiche zu verwenden, die bereits erkannt wurden.

   b. Wählen Sie in der Liste **Arbeitsbereich** den Arbeitsbereich aus, in dem sich die installierbare Konfiguration befindet.

   Hinweis: Wenn Sie eine Windows-VM konfigurieren, setzen Sie das Feld **IncludeManagementKey** auf **No** (Nein). Nach der Bereitstellung der VM können Sie den Vorgang des zweiten Tags namens „InfuseKey“ verwenden, um der VM Schlüsselanmeldeinformationen (**UserName** und **Password**) hinzuzufügen.

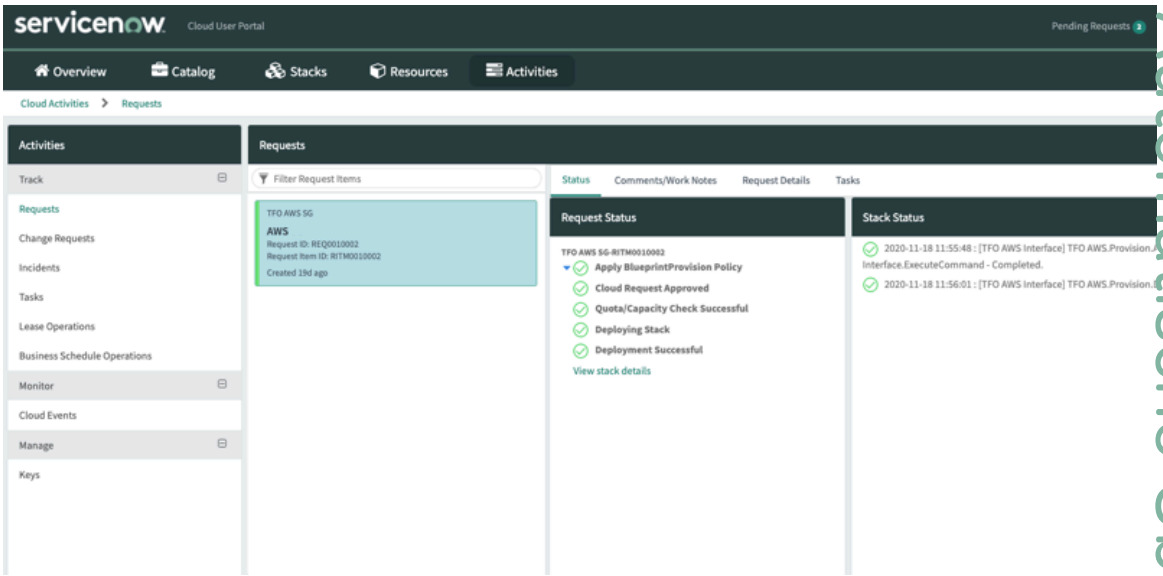
3. **Wahlweise:** Wählen Sie im Abschnitt „Allgemeine Informationen“ den Agent-Pool aus, den Sie in Ihrer Terraform Enterprise-Organisation für die Kommunikation mit einer privaten oder lokalen Infrastruktur erstellt haben.

   Hinweis: Die Auswahl des Agent-Pools betrifft nur Bereitstellungs-Setups für VMware über Terraform Enterprise. Sie müssen in Ihrer Terraform Enterprise-Organisation Agent-Pools erstellt haben und in Ihrem Arbeitsbereich über VMware-Terraform Enterprise-Vorlagen verfügen, damit die Option für Agent-Pools in der GUI angezeigt wird.

4. Klicken Sie auf die Abschnittsüberschrift, um zum nächsten Abschnitt zu wechseln.
   Das verbleibende Kontingent wird basierend auf der von Ihnen ausgewählten Benutzergruppe aktualisiert. Für Pflichtfelder wird standardmäßig das erste Element in der Liste ausgewählt. Sie können dann einen beliebigen Wert auswählen.
5. Klicken Sie auf **Submit** (Absenden), um den Stapel anzufordern.
   - Die **Aktivitäten** Seite wird für geöffnet **Status** Registerkarte im **Titel** > **Anforderungen** Aktivität. Die Registerkarte zeigt den Fortschritt und den Status der Anforderung an. Die folgenden Farbcodes zeigen die Phase der Anforderung an:
   - ▪ Grün: Abgeschlossen oder genehmigt.
     ▪ Orange: Wird verarbeitet.
     ▪ Rot: Abgelehnt, Fehler oder Abgebrochen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine Genehmigung erforderlich ist, startet das System den Stapel, nachdem der Administrator Ihre Anforderung genehmigt hat, und aktualisiert den **Anforderungsstatus**.
- Wenn die Kontingentgrenze für Sie oder Ihre Anwendergruppe überschreitet, wird eine Fehlermeldung angezeigt, oder das System löst eine richtlinienbasierte Genehmigung aus. Weitere Informationen über Kontingentgrenzen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.
- Wählen Sie eine andere Anforderung aus, um deren **Anforderungsstatus** und **Stapelstatus** anzeigen zu lassen.
- Zum Anzeigen einer Zusammenfassung aller ausstehenden Anforderungen können Sie in der Titelleiste jederzeit auf den Link **Pending Requests** (Ausstehende Anforderungen) klicken.



Automatische Übersetzung

Kontingentgrenzen für Ressourcen anzeigen

Zeigen Sie Kontingentgrenzen an, um nachzuvollziehen, wie viele Ressourcen Sie verbraucht haben und wie viele Ressourcen Sie basierend auf den für Sie und Ihre Benutzergruppe festgelegten Kontingentgrenzen bereitstellen können.

Zugeteilte und verbrauchte Kontingentgrenzen

Um das von Ihnen für die Bereitstellung von Ressourcen verbrauchte Kontingent im Vergleich zu dem Ihnen zugeteilten Höchstkontingent anzuzeigen, navigieren Sie zur Seite „Übersicht“. Für die folgenden vordefinierten Ressourcentypen im System sind möglicherweise Kontingentgrenzen für Sie und die Benutzergruppen festgelegt, denen Sie angehören:

- Stapelanzahl
- VM-Anzahl
- vCPU-Anzahl
- Größe des Speichervolume
- Netzwerkanzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

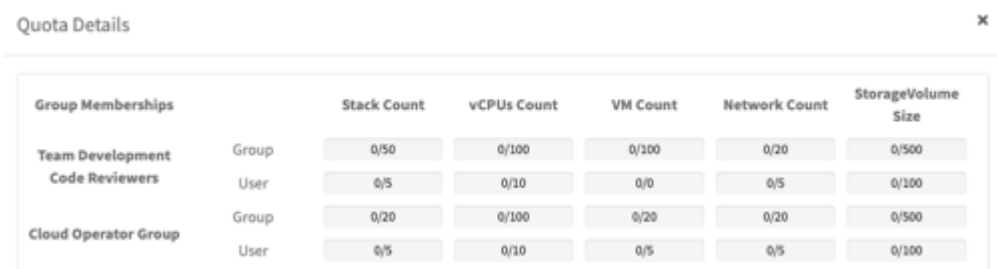
Hinweis: Die Stapelanzahl ist eine im Basissystem bestehende Standardkontingentgrenze, die seit Release Zurich verfügbar ist. Sie wird auf der Seite „Übersicht“ angezeigt, wenn Ihr Cloud Provisioning and Governance-Administrator ein Kontingent für die Stapelanzahl für Sie oder Ihre Benutzergruppe festgelegt hat.

Auf der Seite „Übersicht“ werden im Abschnitt „Kontingent“ die Kontingentgrenzen in einem Diagramm angezeigt.

- Grün zeigt an, dass genügend Ressourcen verfügbar sind.
- Rot zeigt an, dass nicht genügend Ressourcen verfügbar sind.
- Wenn Quotengrenzen überschritten wurden, zeigt das System möglicherweise eine Fehlermeldung an oder löst eine richtlinienbasierte Genehmigung aus, wenn Sie versuchen, einen Stapel bereitzustellen. Weitere Informationen finden Sie unter Stapel auf Basis von Kontingentgrenzen bereitstellen.

Die Kontingentgrenze, die im Abschnitt „Kontingent“ angezeigt wird, ist eine Zusammenfassung aller Benutzergruppen, denen Sie angehören. Um Kontingentgrenzen für Sie und Ihre Benutzergruppen separat anzuzeigen, klicken Sie auf **Alle anzeigen**. Das Popup-Fenster „Kontingentdetails“ wird angezeigt.

Popup-Fenster „Kontingentdetails“



Im Popup-Fenster „Kontingentdetails“ wird Ihr verbrauchtes Kontingent der zugeteilten Kontingentgrenze für jeden Ressourcentyp gegenübergestellt. Zum Beispiel bedeutet „0/5“ für einen Ressourcentyp, dass 0 Ressourcen verbraucht wurden und die zugeteilte Kontingentgrenze 5 Ressourcen beträgt.

Die Kontingentgrenze für einen Ressourcentyp wird entweder als Summe oder als Anzahl angezeigt. Beispielsweise wird die Größe von Speichervolumes als Summe in GB angezeigt, und die VM-Anzahl wird als Zahl angezeigt.

Sie können Kontingentgrenzen auch beim Starten von Stapeln anzeigen. Weitere Informationen finden Sie unter Einen Stapel starten.

Stapel auf Basis von Kontingentgrenzen bereitstellen

Wenn Sie Stapel bereitstellen, berechnet das System das Ihnen und Ihren Benutzergruppen zugeteilte Kontingent. Wenn Quotengrenzen überschritten werden, zeigt das System entweder eine Fehlermeldung an oder löst eine richtlinienbasierte Genehmigung aus.

Um Kontingentgrenzen anzuzeigen, navigieren Sie zur Seite „Übersicht“. Weitere Informationen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.

Kontingentberechnung für vorlagenbasierte Stapel

Die Stapelanzahl ist eine im Basissystem bestehende Standardkontingentgrenze, die seit Release Zurich verfügbar ist. Die Grenze gilt für alle vorlagenbasierten Stapel im Servicekatalog.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

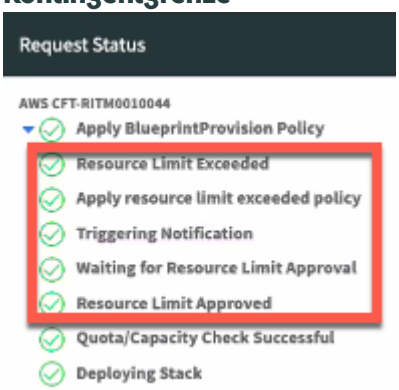
Wenn Ihr Cloud Provisioning and Governance-Administrator für Sie oder Ihre Benutzergruppe ein Stapelanzahl-Kontingent festgelegt hat, berechnet das System die Stapelanzahl, sobald Sie einen Stapel bereitstellen. Nach der Bereitstellung wird die Stapelanzahl des Kontingents für jeden bereitgestellten Stapel um den Wert 1 erhöht.

Stapelbereitstellung nach Überschreiten der Kontingentgrenzen

Wenn die für Sie oder Ihre Benutzergruppe festgelegte Kontingentgrenze überschritten wurde, zeigt das System entweder eine Fehlermeldung an oder löst einen zugeordnete Regel aus, sobald Sie versuchen, einen Stapel bereitzustellen.

- Falls das System eine Fehlermeldung anzeigt, die darauf hinweist, dass die Kontingentgrenze überschritten wurde, können Sie den Stapel nicht bereitstellen. Wenn Sie der Meinung sind, dass die Kontingentgrenze erhöht werden muss, wenden Sie sich an Ihren Cloud Provisioning and Governance-Administrator.
- Ist im System eine Richtlinie für die Überschreitung der Kontingentgrenze definiert, wird diese ausgelöst. Je nach Richtlinie löst das System eine Genehmigungsanforderung oder eine Benachrichtigung zur Erhöhung der Kontingentgrenze aus. Die Anforderung folgt einem vordefinierten Subflow im System zur Genehmigung. Wenn die Anforderung genehmigt wird, stellt das System den Stapel bereit.

Ausgelöste Richtlinie zur Bereitstellung eines Stapels nach Überschreiten der Kontingentgrenze



Eine Stapel-Anforderung nachverfolgen

Das System generiert eine Anforderung, wenn Sie das Formular zum Starten eines Stapels übermitteln.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Wenn keine Genehmigungsrichtlinie definiert ist, werden Anforderungen automatisch genehmigt. Wenn eine Richtlinie definiert ist, muss ein Benutzer auf der Genehmigerliste die Anforderung genehmigen.
Wenn die Kontingentgrenze für Sie oder Ihre Anwendergruppe überschreitet, wird eine Fehlermeldung angezeigt, oder das System löst eine richtlinienbasierte Genehmigung aus. Weitere Informationen über Kontingentgrenzen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.

Prozedur

1. Wechseln Sie zu **Aktivitäten** Seite oder navigieren Sie zu **Übersicht** > **Aktivitäten anzeigen**, Und wählen Sie dann aus **Titel** > **Anforderungen**an.
   Die folgenden Farbcodes zeigen den Status der Anforderung an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Grün: Abgeschlossen oder genehmigt.
- Orange: Wird verarbeitet.
- Rot: Abgelehnt, Fehler oder Abgebrochen.

2. Klicken Sie in der Liste **Requests** (Anforderungen) auf einen Eintrag.

Registerkarte **Status**	
Anforderungsstatus	Für die Anforderung ausgeführte Aktionen. Durch Klicken auf den Abwärtspfeil ( ) wechseln Sie zwischen den folgenden Optionen: ○ Ausführlicher Modus, der jede Aktion und den Status der Aktion beschreibt. ○ Nur-Symbol-Modus, der nur den Status (Erfolg/Misserfolg) einer Aktion anzeigt.
Stapelstatus	Status der einzelnen Stapelanforderungen. Wenn die Bereitstellung fehlschlägt, werden Fehler von der Cloud-Orchestrierung aufgelistet.
Registerkarte **Comments / Work Notes** (Kommentare/Arbeitsnotizen)	
Angefordertes Element und Anforderungsnummer	Protokoll der Kommentare und Notizen, die für die Anforderung erstellt wurden. Die Rolle **itil** ist erforderlich, um einen Kommentar oder eine Arbeitsnotiz hinzuzufügen. So fügen Sie einen Kommentar oder eine Arbeitsnotiz hinzu: **a.** Geben Sie den Text ein. **b.** Wählen Sie das Kontrollkästchen **Work Notes** (Arbeitsnotizen), um eine Arbeitsnotiz hinzuzufügen. **c.** Klicken Sie auf **Senden**.
Registerkarte **Request Details** (Anforderungsdetails)	Werte, die der Anforderer auf dem Stapel-Anforderungsformular übermittelt hat.
Registerkarte **Tasks** (Aufgaben)	Listet alle Katalogaufgaben auf, die für Stapel erstellt wurden, welche nicht bereitgestellt werden konnten. Klicken Sie auf eine Katalogaufgabe, um weitere Details zu dieser Aufgabe anzuzeigen. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.

Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln

Die Anwendung Cloud Provisioning and Governance erstellt eine Nachbesserungs- oder Katalogaufgabe, wenn die Anforderung für einen Stapel nicht bereitgestellt werden kann. Sie können die fehlgeschlagene Anforderung erneut übermitteln oder der Cloud-Operator-Gruppe zuweisen, damit diese sie für Sie bearbeitet.

Vorbereitungen

Erforderliche Rollen: sn_cmp.cloud_service_user und sn_cmp.cloud_operator.

Warum und wann dieser Vorgang ausgeführt wird

Die Aufgabennachbesserung erfasst alle auf eine fehlgeschlagene Anforderung angewendeten Nachbesserungen. Sie können die für eine fehlgeschlagene Anforderung durchgeführte Nachbesserung und alle wichtigen Meilensteine auf der Unterregisterkarte **Comments/Work Notes** (Kommentare/Arbeitsnotizen) in Cloudbenutzerportal anzeigen lassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aufgabennachbesserung ist nur für die neue Bereitstellung von Stapeln und nicht für den Lebenszyklus oder andere Vorgänge verfügbar.

Die Bereitstellung eines Stapels kann aus vielen Gründen fehlschlagen. Ein Stapel schlägt möglicherweise fehl, wenn Sie Ihr Cloud-Kontingent oder die Kapazität Ihres Rechenzentrums überschritten haben oder einen ungültigen Parameter im Anforderungsformular eingegeben haben (z. B. doppelte NICs).

Wenn die Bereitstellung eines Stapels fehlschlägt, wird eine Katalogaufgabe erstellt und Ihnen zugewiesen. Eine Fehlermeldung zur fehlgeschlagenen Anforderung wird auf der Unterregisterkarte **Status** in Cloudbenutzerportal angezeigt.

Prozedur

1. In Cloudbenutzerportal, Navigieren Sie zu **Aktivitäten anzeigen** > **Anforderungen** > **Aufgaben**an.
2. Klicken Sie auf die Katalogaufgabe, die erneut zu übermitteln ist.
3. Wählen Sie eine Aktion nach Ihren Wünschen aus:
   - **Retry** (Wiederholen): Übermittelt die fehlgeschlagene Anforderung erneut. Sie können versuchen, die fehlgeschlagene Anforderung erneut zu übermitteln, indem Sie den Fehler nach Möglichkeit beheben. Wenn der Fehler auf das Überschreiten der Kontingentgrenze zurückzuführen ist, können Sie versuchen, die Bereitstellung einiger Ressourcen aufzuheben, die derzeit nicht verwendet werden, und dann auf **Retry** (Wiederholen) klicken. Wenn Sie auf **Retry** (Wiederholen) klicken, wird die ursprüngliche Anforderung erneut übermittelt. Es wird keine neue Anforderung erstellt.

     Hinweis: Alle Richtlinien, die einem Ressourcenvorgang zugeordnet sind, werden erneut ausgeführt.

   - **Ask for Help** (Um Hilfe bitten): Erstellt eine neue Katalogaufgabe und weist sie der Cloud-Operator-Gruppe zu, um die fehlgeschlagene Anforderung erneut zu übermitteln. Die Gruppe Cloud-Operator-Gruppe kann den Fehler genauer untersuchen und versuchen, ihn für Sie zu beheben. Jedes Mal, wenn die Kommentare oder Arbeitsnotizen in der Katalogaufgabe von der Cloud-Operator-Gruppe aktualisiert werden, werden die Änderungen auf der Unterregisterkarte **Comments/Work Notes** (Kommentare/Arbeitsnotizen) in Cloudbenutzerportal angezeigt. Bei Bedarf kann der Operator die fehlgeschlagene Anforderung abbrechen.
   - **Cancel Order** (Auftrag stornieren): Storniert die fehlgeschlagene Anforderung und hebt die Bereitstellung aller teilweise bereitgestellten Ressourcen auf.

Einen Stapel verwalten

Über die Seite „Stack Details“ (Stapeldetails) können Sie Details und Status für einen Stapel aufrufen und Lebenszyklusvorgänge für einen Stapel durchführen.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

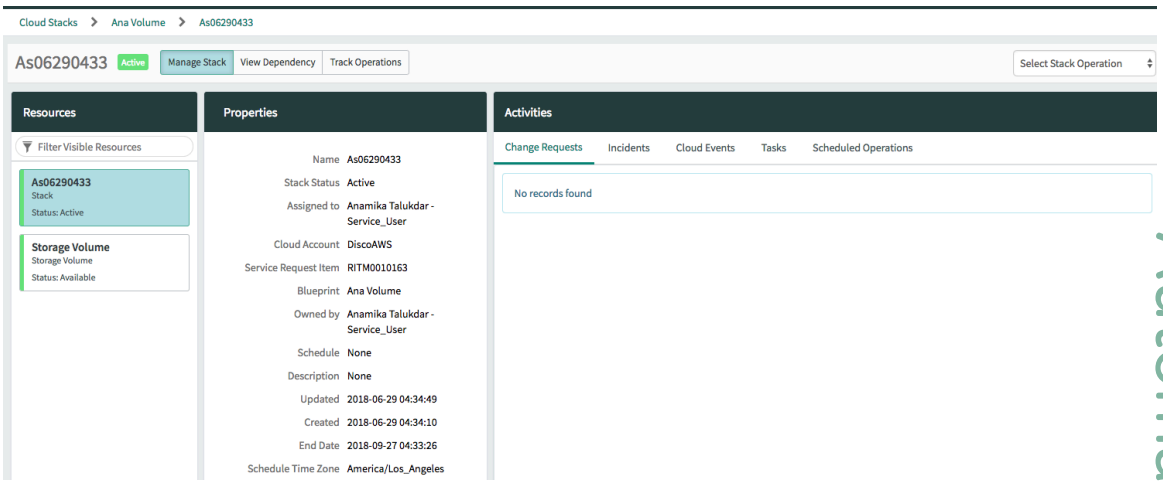
1. Über eine der folgenden Methoden öffnen Sie die Seite **Stack Details** (Stapeldetails):
   - Klicken Sie auf der Symbolleiste auf **Stapel**.
   - Verwenden Sie das Textfeld **Suchen**, um den Stapel zu suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf der Homepage auf einen Stapel im Abschnitt **Letzte Stapel** oder **Stack-Integrität**.
- Klicken Sie auf der Homepage auf **Stapel verwalten**.

Standardmäßig werden alle Stapel in allen Servicekategorien aufgelistet.

2. Wählen Sie in der Liste **Stapel** eine Stapelkategorie, und klicken Sie dann auf den **Namen**eines Stapels.
Auf der Seite **Stack Details** (Stapeldetails) werden die folgenden Informationen angezeigt:



- Breadcrumb-Navigation
- Name des Stapels. Klicken Sie auf **Abhängigkeit anzeigen**, um die Abhängigkeitszuordnung für den Stapel aufzurufen, auf **Stapel verwalten**, um Ressourcen, Eigenschaften und Aktivitäten des Stapels anzuzeigen, und auf **Vorgänge nachverfolgen**, um die Liste der Lebenszyklusvorgänge anzuzeigen, die für den Stapel und seine Ressourcen ausgeführt werden.
- Statusinformationen
- Liste aller Ressourcen im Stapel. Wenn Sie auf eine Ressource klicken, können Sie im Abschnitt **Properties** (Eigenschaften) Details einsehen. Farbcodes zeigen den Status des Stapels an:
  - Grün: Aktiviert/Aktiv.
  - Gelb: Deaktiviert oder Verarbeitung.
  - Rot: Beendet oder Fehler.
- Liste der Stapeleigenschaften. Einige Eigenschaften werden im Stapelanforderungsformular festgelegt, andere werden durch Richtlinien festgelegt.
- Aktivitäten, die dem Stapel zugeordnet sind. Klicken Sie auf eine Registerkarte, um Folgendes anzeigen zu lassen:
  - Change-Anforderungen, die dem Stapel zugeordnet sind. Weitere Informationen finden Sie unter Change-Anforderungen nachverfolgen.
  - Incidents, die für den Stapel ausgelöst wurden. Siehe Übermitteln eines Incidents für einen Stapel und Incidents nachverfolgen.
  - Cloud-Events, die dem Stapel zugeordnet sind. Cloud-Events wird nur angezeigt, wenn eine Ressource ausgewählt ist. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
  - Katalogaufgaben die dem Stapel zugeordnet sind. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bevorstehende Zeitplanvorgänge für Geschäftszeiten, die dem Stapel zugeordnet sind. Sie können einen bevorstehenden Vorgang überspringen oder einen dem Stapel zugeordneten Zeitplan abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.

- Vorgänge, die Sie auf einem Stapel ausführen können. Weitere Informationen finden Sie unter Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen.
- Textfeld, das zum Durchsuchen des Cloud-Benutzerportals nach Stapeln, Ressourcen basierend auf Typen, Stapelanforderungen, Change-Anforderungen, Incidents, Schlüsseln und Katalogelementen verwendet wird.

Stapeleigenschaften

Name	Name, den Sie bei der Anforderung des Stapels angegeben haben.
Stapelstatus	Aktueller Status des Stapels: ○ Aktiv (bereitgestellte Stapel) ○ Beendet (Stapel mit aufgehobener Bereitstellung) ○ Nicht verwaltet (erfasste Stapel) ○ Fehler (fehlerhafte Stapel) ○ Wird verarbeitet (Stapel werden verarbeitet)
Zugewiesen an	Besitzer der Stapelkonfiguration. Dies steuert die Zugriffssteuerungen und Ansichten im Cloud-Portal.
Cloud-Account	Cloud-Konto, dem der Stapel zugeordnet ist.
Serviceanforderungselement	Datensatz, der in der Tabelle „Request Item“ (Anforderungselement) erstellt wurde, als Sie den Katalog bestellt haben, der zu diesem Stapel geführt hat.
Blaupause	Blaupause, der der Stapel zugeordnet ist.
Eigentum von	Benutzername der anfordernden Person.
Besitzergruppe	Name der Gruppe, zu der der Besitzer des Stapels gehört.
Zeitplan	Der Zeitplan ist dem Stapel zugeordnet.
Ausgabe	Spezifische Details für ARM-/CFT-Stapel, z. B. die URL einer Anwendung, Namen oder Standorte aller erstellten Ressourcen.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Stapeldetails.
Erstellt	Datum und Uhrzeit der Anforderung des Stapels.
Enddatum	Datum und Uhrzeit der Beendigung (nicht bereitgestellt) des Stapels.

Ressourcen verwalten

Über die Seite „Resource Details“ (Ressourcendetails) können Sie Details und Status für eine Ressource aufrufen und Lebenszyklusvorgänge für eine Ressource durchführen.

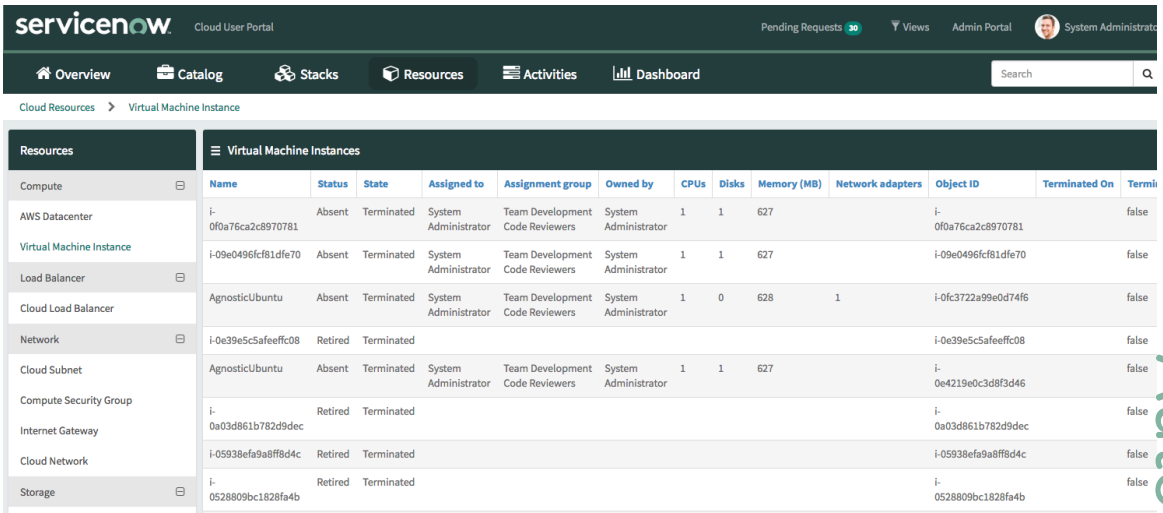
Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

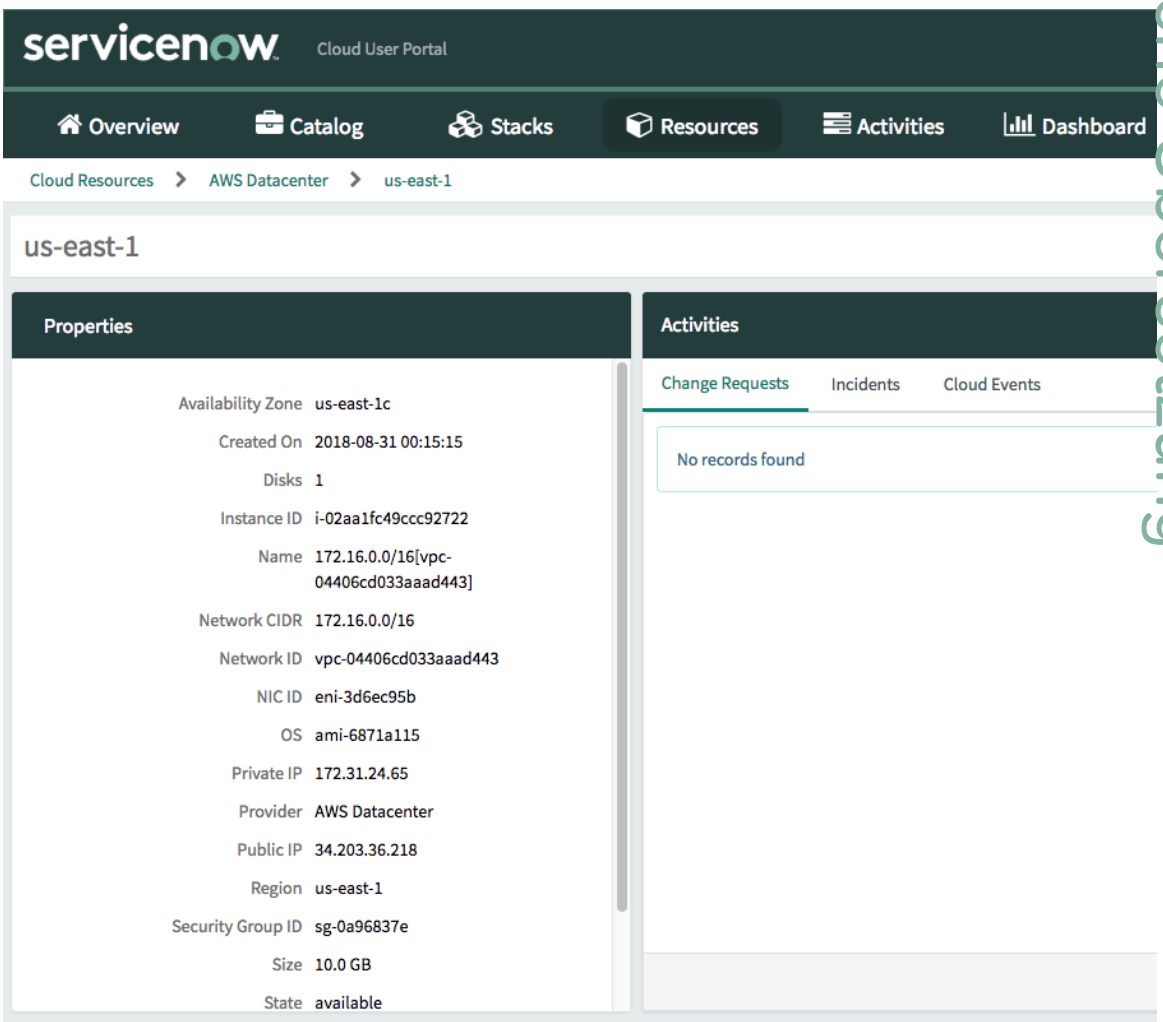
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf der Symbolleiste auf **Resources** (Ressourcen).
   Die Seite **Resources** (Ressourcen) listet alle Ressourcentypen im linken Bereich auf.



2. Navigieren Sie zum entsprechenden Ressourcentyp, um die Liste der Ressourcen aufzurufen, die Sie interessieren, und klicken Sie dann auf einen Ressourcennamen, um spezifische Details zu dieser Ressource anzeigen zu lassen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Ressourcendetailbildschirm enthält folgende Informationen:

- Breadcrumb-Navigation
- Alle für die Ressource spezifischen Eigenschaften
- Aktivitäten, die der Ressource zugeordnet sind. Klicken Sie auf eine Registerkarte, um Folgendes anzeigen zu lassen:
  - Change-Anforderungen, die der Ressource zugeordnet sind. Weitere Informationen finden Sie unter Change-Anforderungen nachverfolgen.
  - Incidents, die für die Ressource ausgelöst wurden. Siehe Übermitteln eines Incidents für einen Stapel und Incidents nachverfolgen.
  - Cloud-Events, die bezüglich der Ressource eingetreten sind. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
- Textfeld, das zum Durchsuchen des Cloud-Benutzerportals nach Stapeln, Ressourcen basierend auf Typen, Stapelanforderungen, Change-Anforderungen, Incidents, Schlüsseln und Katalogelementen verwendet wird.

Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen

Vorgänge wie Start/Stopp, „Aufheben der Bereitstellung“ und „Skript ausführen“ werden *Lebenszyklusvorgänge* oder *Tag-2-Vorgänge* genannt. Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist festgelegt, dass der Change entweder automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss.

Vorbereitungen

Erforderliche Rolle:

Lebenszyklusvorgänge erfordern den Benutzer mit der Rolle `sn_cmp.cloud_service_user`, der die Ressource besitzt. Benutzer mit den Rollen „root_admin“, „admin“ oder `sn_cmp.cloud_admin` können den Vorgang ebenfalls ausführen.

Warum und wann dieser Vorgang ausgeführt wird

- Wie in den Beschreibungen erwähnt, werden nicht alle Vorgänge für alle Anbieter oder für alle Servicekategorien (Ressourcentypen) unterstützt.
- Für alle anderen Anbieter der Konfigurationsverwaltung gilt: Wenn für einen Stapel oder eine Ressource eine Anmeldung erforderlich ist, müssen Sie den zugehörigen SSH-Schlüssel herunterladen, bevor Sie auf die Ressource zugreifen können. Weitere Informationen finden Sie unter Einen SSH-Schlüssel herunterladen.

Prozedur

1. Wählen Sie einen Stapel oder eine Ressource aus.
2. Wählen Sie auf der Seite **Stack Details** (Stapeldetails) den Vorgang aus den Listen **Stapelvorgang auswählen** oder **Ressourcenvorgang auswählen** aus.
   Vollständige Beschreibungen der Vorgänge finden Sie unter Lebenszyklusvorgänge in Cloud Provisioning and Governance.

   Für einige Vorgänge sind Einstellungen erforderlich (z. B. der Name eines Skripts oder neue Zeitplaneinstellungen).
3. Geben Sie die Einstellungen ein, und klicken Sie auf **OK**.
   Das System übermittelt eine Change-Anforderung und die **Aktivitäten** > **Change-Anforderungen** Seite zeigt den Fortschritt und den Status der Anforderung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lebenszyklusvorgänge in Cloud Provisioning and Governance

Vorgänge wie Start/Stopp, „Aufheben der Bereitstellung“ und „Skript ausführen“ werden *Lebenszyklusvorgänge* oder *Tag-2-Vorgänge* genannt. Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist festgelegt, dass der Change entweder automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss.

Um einen Vorgang durchzuführen, wählen Sie einen Stapel oder eine Ressource und klicken Sie dann auf **Stapelvorgang auswählen** oder **Ressourcenvorgang auswählen** aus. Die Liste enthält nur Vorgänge, die für die ausgewählte Ressource oder den ausgewählten Stapel einschlägig sind. Einige Vorgänge werden von Configuration Management Systems wie Ansible oder Terraform bereitgestellt.

Vorgänge in Basissystem

Start

Der Vorgang `Start` startet den ausgewählten virtuellen Computer. Der Ressourcenstatus wechselt auf „On“ (Aktiviert).

Keine Einstellung ist erforderlich.

Stoppen

Der Vorgang `Stop` hält den ausgewählten virtuellen Computer an. Der Ressourcenstatus wechselt auf „Off“ (Deaktiviert).

Keine Einstellung ist erforderlich.

Aufheben der Bereitstellung

Der Vorgang `Deprovision` (Aufheben der Bereitstellung) beendet den ausgewählten Stapel und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

Vorgänge über die Erweiterungsschnittstelle des virtuellen Computers

Nur Google Cloud Platform und IBM Cloud unterstützen Vorgänge über die `Store-Erweiterungsschnittstelle für virtuelle Computer`. Die App Terraform Connector ServiceNow Store stellt die Vorgänge bereit.

Store-Erweiterungsschnittstelle des virtuellen Computers.ExecuteScript

Der Vorgang `ExecuteScript` führt ein Skript auf der ausgewählten Windows- oder Linux-VM aus. Beispielsweise kann ein Skript eine Anwendung auf einer Ressource installieren. Detaillierte Anweisungen finden Sie unter KB0756431 .

> **Hinweis:** Zum Ausführen des Vorgangs `ExecuteScript` muss ein virtueller Computer Anmeldeinformationen enthalten. Virtuelle Computer unter Linux erben bei ihrer Bereitstellung Anmeldeinformationen für den Managementschlüssel. Verwenden Sie für virtuelle Computer unter Windows den Vorgang `InfuseKey`, um dem virtuellen Computer Anmeldeinformationen hinzuzufügen.

Geben Sie im Popup-Fenster Folgendes an:

- **ScriptType**: Shell- und PowerShell-Skripte werden unterstützt.
- **Script**: Name des Skripts.

Store-Erweiterungsschnittstelle des virtuellen Computers.InfuseKey

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Vorgang `InfuseKey` fügt bei virtuellen Computern unter Windows Schlüsselanmeldeinformationen (öffentliche und private Schlüsselpaarwerte) hinzu.

Daher können Sie die Anmeldeinformationen in der Liste „Eigenschaften“ des virtuellen Computers unter Windows einsehen und die Anmeldeinformationen zum Ausführen von VM-Vorgängen verwenden. Anweisungen zum Generieren eines Schlüssels finden Sie unter Einen SSH-Schlüssel erstellen.

So fügen Sie einem virtuellen Computer unter Windows Schlüsselanmeldeinformationen hinzu:

1. Wählen Sie die Windows-VM aus.
2. Wählen Sie in der Liste **Select Resource Operation** (Ressourcenvorgang auswählen) die Option **Virtual Machine Store Extension Interface.InfuseKey**(Store-Erweiterungsschnittstelle des virtuellen Computers.InfuseKey).
3. Geben Sie im Popup-Fenster den zu verwendenden Schlüssel im Feld **UserKey** (Benutzerschlüssel) an, und klicken Sie dann auf **OK**.

Store-Erweiterungsschnittstelle des virtuellen Computers.Execute Job Template

Ansible liefert den Vorgang `Execute Job Template` (Auftragsvorlage ausführen). Mit diesem Vorgang können Sie einen Knoten einem Ansible-Server beifügen und ein Paket für diese VME ausführen. Beispielsweise kann ein Skript eine Anwendung auf einer Ressource installieren. Geben Sie im Popup-Fenster Folgendes an:

WorkloadConfigProviderType	
WorkloadConfigProvider	
Inventar	
HostGroup	Die Liste umfass alle möglichen Anwendungen (in Ansible als *Gruppen* bezeichnet), nicht nur die Anwendungen, die der Konfigurationsmanagement-Anbieter unterstützt. Daher schlägt die Bereitstellung fehl, wenn Benutzer eine nicht unterstützte Anwendung auswählen.
ApplicationProfile	Wählen Sie das Anwendungsprofil aus, das für die ausgewählte Ressource ausgeführt werden soll.

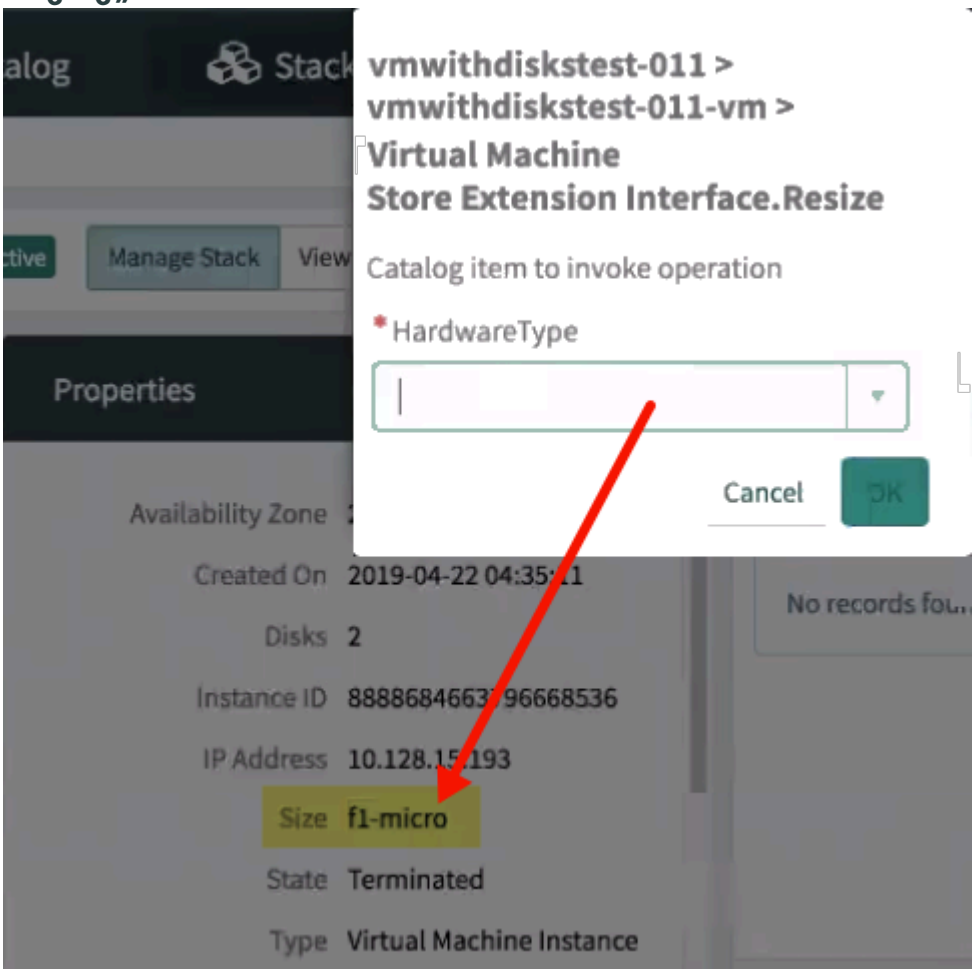
- **ScriptType**: Für Google Cloud Platform wird **Shell** unterstützt.
- **Script**: Name des Skripts.

Store-Erweiterungsschnittstelle des virtuellen Computers.Resize

Der Vorgang `Resize` (Größe ändern) ändert die Einstellung der **Größe** für einen virtuellen Computer (in der CI-Definition als **HardwareType** bezeichnet). Geben Sie im Popup-Fenster im Feld **HardwareType** die neue Größe an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang „Größe ändern“



Vorgänge des Typs „Compute-Sicherheitsgruppe – Store-Erweiterungsschnittstelle“

Die Vorgänge zur *Store-Erweiterungsschnittstelle der Compute-Sicherheitsgruppe* werden nur für IBM Cloud unterstützt. Die App Terraform ServiceNow Store stellt die Vorgänge bereit.

Compute-Sicherheitsgruppe – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet die ausgewählte Compute-Sicherheitsgruppe und sendet eine Benachrichtigung an ihren Besitzer.

Keine Einstellung ist erforderlich.

Der **Status** der Netzwerkschnittstelle wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Lastenausgleichsmodul – Store-Erweiterungsschnittstelle“

Lastenausgleichsmodul – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet das ausgewählte Lastenausgleichsmodul und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der **Status** des Lastenausgleichsmoduls wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Netzwerk – Store-Erweiterungsschnittstelle“

Netzwerk – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *`Deprovision`* (Aufheben der Bereitstellung) beendet das ausgewählte Netzwerk und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

Der **Status** des Netzwerkspeichers wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Speicher-Laufwerk – Store-Erweiterungsschnittstelle“

Die Vorgänge zur *`Store-Erweiterungsschnittstelle des Speicher-Laufwerks`* werden nur für IBM Cloud unterstützt. Die App Terraform ServiceNow Store stellt die Vorgänge bereit.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Create Snapshot

Der Vorgang *`Create Snapshot`* (Snapshot erstellen) generiert eine schreibgeschützte Kopie des angegebenen Laufwerks.

Legen Sie im Popup-Fenster den Parameter **SnapshotName** fest, der als Bezeichnung für den Snapshot verwendet werden soll.

Der Snapshot wird in der Tabelle [cmdbci.ci_storage_vol_snapshot_list] gespeichert.

Wenn keine Genehmigung erforderlich ist, erstellt das System den Snapshot sofort. Wenn eine Genehmigung erforderlich ist, kann es zu Verzögerungen kommen, bis ein Administrator die Änderung genehmigt. Sie erhalten eine E-Mail-Nachricht, wenn der Administrator die Genehmigung erteilt. Kehren Sie nach der Genehmigung durch den Administrator zum VM-Instanzformular zurück, und klicken Sie auf den zugehörigen Link **Proceed with Change** (Mit Änderung fortfahren).

Hinweis: Wenn die VM ausgeführt wird, wird die VM zu Beginn des Snapshot-Prozesses heruntergefahren und dann nach Abschluss des Prozesses neu gestartet. Das System löscht den ältesten Snapshot automatisch, wenn der Grenzwert der **Snapshot-Entfernungsrichtlinie** überschritten wird.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Restore From Snapshot

Der Vorgang *`Restore From Snapshot`* (Aus Snapshot wiederherstellen) stellt das Bild aus dem angegebenen Snapshot wieder her.

Legen Sie den Parameter **SnapshotID** fest, der für die Wiederherstellung des Laufwerks verwendet werden soll.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Delete Snapshot

Der Vorgang *`Delete Snapshot`* (Snapshot löschen) löscht den ausgewählten Snapshot.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Attach

Der Vorgang *`Attach`* (Anfügen) fügt eine VM an das ausgewählte Laufwerk an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wählen Sie das Laufwerk aus, dem etwas angehängt werden soll. Der **Status** des Laufwerks muss **Available** (Verfügbar) sein.
2. Wählen Sie den Vorgang **Storage Volume Store Extension Interface.Attach** (Speicher-Laufwerk –Store-Erweiterungsschnittstelle.Attach).
3. Wählen Sie im Popup-Fenster im Feld **NodeId** die **Instanz-ID** des Servers aus, der an das Laufwerk angefügt werden soll.

   Der Status des Laufwerks ändert sich von „Available“ (Verfügbar) in „In Use“ (In Verwendung).

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Detach

Der Vorgang `Detach` (Trennen) trennt eine VM vom ausgewählten Laufwerk.

1. Wählen Sie das Laufwerk aus, dem etwas angehängt werden soll. Der Status des Laufwerks muss „In Use“ (In Verwendung) sein.
2. Wählen Sie den Vorgang **Storage Volume Store Extension Interface.Detach** (Speicher-Laufwerk –Store-Erweiterungsschnittstelle.Detach).
3. Wählen Sie im Popup-Fenster im Feld **NodeId** die **Instanz-ID** des Hosts aus, der vom Laufwerk getrennt werden soll.

   Wenn diese VM die letzte oder einzige zu trennende VM ist, ändert sich der Status des Laufwerks von „In Use“ (In Verwendung) in „Available“ (Verfügbar).

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang `Deprovision` (Aufheben der Bereitstellung) beendet das ausgewählten Laufwerk und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

- Das Abrechnungselement für die Speicherressource wird entfernt.
- Der **Status** des Laufwerks wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.
- Für IBM Cloud: Das Speicher-Laufwerk ist für längere Zeit in IBM Cloud-Konsole verfügbar, damit der Benutzer es zurückfordern kann.

Übermitteln eines Incidents für einen Stapel

Senden Sie einen Incident für einen Stapel, wenn dieser nicht wie erwartet funktioniert oder Sie Fragen haben. Wenn der Benutzer antwortet oder das Problem behebt, wird der Incident geschlossen.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Incident für einen Stapel oder für eine einzelne Ressource übermitteln.
Sie können auch Incident erstellen Über die Incident-Anwendung. Stellen Sie sicher, dass das Feld **Category** auf den Wert Cloud Provisioning and Governance festgelegt ist. Das Configuration Item muss der Stapelname sein, für den der Incident ausgelöst werden soll, und der Name des Anrufers muss der Name der Person sein, für die der Incident erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Sie können die Seite mit Stapeldetails mit einer der folgenden Methoden anzeigen:
   - Klicken Sie auf der Seite **Stack Details** (Stapeldetails) auf die Registerkarte **Incidents** im Abschnitt **Activities** (Aktivitäten).
   - Auf der **Aktivitäten** Seite klicken Sie auf **Titel** > **Incidents**an.

   Der Abschnitt **Activities** (Aktivitäten) listet alle übermittelten Incidents für den Stapel auf.

Incidents	
Activities # Incidents (Aktivitäten # Incidents)	Lassen Sie Incidents aller Typen für jeden Stapel oder jede Ressource anzeigen, und übermitteln Sie sie.
Stacks # Stack Details # Incidents (Stapel # Stapeldetails # Incidents)	Lassen Sie Incidents für den ausgewählten Stapel anzeigen, und übermitteln Sie sie.
Resources # Resource Details # Incidents (Ressourcen # Ressourcendetails # Incidents)	Lassen Sie Incidents für die ausgewählte Ressource anzeigen, und übermitteln Sie sie.

2. Klicken Sie auf **New Incident** (Neuer Incident) und füllen Sie das Formular aus:

Incident Type (Incident-Typ)	Der Typ, der Ihren Bedürfnissen am ehesten entspricht.
Stack / Resource (Stapel/Ressource) [zusammenhängende Felder]	Stapel und Ressource, für die der Incident gilt. ○ Wählen Sie auf der Seite **Activities** (Aktivitäten) den **Stapel** aus der Liste der aktiven Stapel aus. Lassen Sie das Feld **Resource** (Ressource) leer, wenn das Problem keiner konkreten Ressource zugeordnet ist. ○ Auf der Seite **Stack Details** (Stapeldetails) ist der Wert für **Stapel** der aktuelle Stapel. ○ Auf der Seite **Resources** (Ressourcen) ist der Wert **Resource** (Ressource) die aktuelle Ressource.
Das Problem beschreiben	Beschreiben Sie das aufgetretene Problem, oder geben Sie eine Frage ein. Geben Sie vollständige Informationen zum Verhalten an, das das Problem darstellt.
Was sind die Auswirkungen auf das Geschäft?	Geben Sie an, wie sich der Incident auf Ihre Arbeit und die Arbeit anderer, einschließlich Ihrer Kunden, auswirkt.
Fügen Sie Screenshots, Protokolle usw. an.	Durch Klicken oder Ablegen von Dateien können Problem bzw. Frage besser erläutert werden.

3. Klicken Sie auf **Absenden**.
   Das System generiert den Incident. Die Registerkarte **Incidents** auf der Seite **Activities** (Aktivitäten) zeigt eine Zusammenfassung an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Um eine Liste aller übermittelten Incidents anzuzeigen, navigieren Sie zu **Aktivitäten** > **Incidents**an.

Seite „Activities“ (Aktivitäten) verwenden

Über die Seite „Activities“ (Aktivitäten) können Sie Details Ihrer Cloud-Aktionen anzeigen lassen und verwalten.

Titel	
Anforderungen	Ihre Anforderungen für Katalogelemente (Stapel). Weitere Informationen finden Sie unter Eine Stapel-Anforderung nachverfolgen.
Change-Anforderungen	Change-Anforderungen, die für Stapel oder Ressourcen eingereicht wurden, die Ihnen zugewiesen sind. Das System generiert Change-Anforderungen, wenn Sie Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen. Siehe Change-Anforderungen nachverfolgen und Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen.
Incidents	Incidents für Stapel und die zugehörigen Ressourcen, die Ihnen zugewiesen sind. Weitere Informationen finden Sie unter Incidents nachverfolgen.
Aufgaben	Katalogaufgaben, die erstellt werden, wenn die Bereitstellung einer Anforderung für einen Stapel fehlschlägt. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.
Leasingvorgänge	Lassen Sie eine Liste aller Ihrer Stapel anzeigen, deren Mietenddatum in Kürze ansteht. Sie können das Enddatum einer Miete für alle aufgeführten Stapel verlängern. Weitere Informationen finden Sie unter Die Miete für einen Stapel ändern.
Geschäftsszeitplanvorgänge	Lassen Sie eine Liste aller in Kürze bevorstehenden Vorgängerschaftsrelation anzeigen, die den Stapeln zugewiesen sind. Sie können einen bevorstehenden Vorgang überspringen oder einen einem konkreten Stapel zugeordneten Zeitplan abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.
Überwachen	
Cloud-Events	Liste der Lebenszyklus-Events, die sich auf Ressourcen auswirken, die Ihnen oder einem Benutzer in Ihrer Gruppe zugewiesen sind. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
Verwalten	
Keys	Lassen Sie vorhandene SSH-Schlüssel anzeigen, die Ihnen zugewiesen sind, oder generieren Sie einen Schlüssel. Weitere Informationen finden Sie unter Einen SSH-Schlüssel erstellen.

Change-Anforderungen nachverfolgen

Das System generiert Change-Anforderungen wenn Sie Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird
Jede Change-Anforderung wird entweder standardmäßig genehmigt oder, wenn eine Genehmigungsrichtlinie vorhanden ist, von einem Benutzer genehmigt, der auf der Genehmigerliste steht.

Prozedur
1. Wechseln Sie zu **Aktivitäten** Seite oder navigieren Sie zu **Cloud-Anwenderportal** > **Aktivitäten anzeigen**, Und wählen Sie dann aus **Titel** > **Change-Anforderungen**an.

Anzahl	Eindeutige automatisch generierte Nummer.
Konfigurationselement	Das betroffene CI.
Kategorie	Cloud Provisioning and Governance
Kurzbeschreibung	Text, der vom Anforderer eingegeben wurde.
Genehmigung	Status.

2. Klicken Sie in der Liste der **Change-Anforderungen** auf einen Eintrag, um alle Details aufzurufen.

Incidents nachverfolgen

Bevor ein Incident gelöst und geschlossen wird, können Sie den Status des Incidents anzeigen lassen.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur
1. Sie öffnen die Incidents-Seite mit einer der folgenden Methoden:
   - Auf der **Aktivitäten** Seite klicken Sie auf **Titel** > **Incidents**an.
   - Klicken Sie auf der Seite **Stack Details** (Stapeldetails) auf die Registerkarte **Incidents** im Abschnitt **Activities** (Aktivitäten).

   Der Abschnitt **Activities** (Aktivitäten) listet alle übermittelten Incidents für den Stapel auf.
2. Klicken Sie in der Liste der **Incidents** auf einen Eintrag, um alle Details aufzurufen.

Nummer	Eindeutige automatisch generierte Nummer.
Kategorie	Cloud Provisioning and Governance.
Unterkategorie	○ Leistungsproblem: Das Problem ist der Vorgangsleistung zugeordnet. ○ Anforderung: Anforderung eines Change.
Kurzbeschreibung	Text, den der Übermittler des Incidents eingegeben hat.
Konfigurationselement	CI der Ressource für den Incident.
Auswirkung	○ Dringlichkeit, wie folgt bewertet: ○ **1 - Hoch**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	○ **2 - Mittel** ○ **3 - Niedrig**
Status	○ **New** (Neu): kürzlich erstellter Incident. ○ **Closed** (Geschlossen): Der Benutzer im Feld **Assigned to** (Zugewiesen an) hat auf das Problem reagiert oder es gelöst und den Incident als geschlossen markiert. ○ **Abgebrochen**: Der Benutzer unter „Zugewiesen an“ hat das Problem geprüft, keine Maßnahmen ergriffen und den Incident abgebrochen.
Zugewiesen an	Der Benutzer, der auf den Incident reagieren muss.

Cloud-Events anzeigen

Wenn Ihr Administrator Cloud Provisioning and Governance so konfiguriert hat, dass Events überwacht werden, können Sie die aus Ihren Cloud-Ressourcen generierten Events anzeigen. Alle Events werden auf der Registerkarte „Cloud-Events“ auf der Stapeldetailseite aufgelistet.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Sie öffnen die Cloud-Events-Seite mit einer der folgenden Methoden:
   - Auf der **Aktivitäten** Seite klicken Sie auf **Monitor** > **Cloud-Ereignisse**an.
   - Auf der Seite **Stack-Details** klicken Sie auf die Registerkarte **Cloud-Ereignisse** im Abschnitt **Aktivitäten**.

   Im Abschnitt **Cloud Events** werden alle Events für den Stapel aufgelistet.

Erstellt	Zeitstempel des Eintritts des Events.
Quelle	Quelle des Events: ○ **azure**: Azure-Warnung ○ **aws**: AWS-Konfig ○ **vmware**: VMware-Events
Event-Name	Name, der von Amazon, Azure oder VMware bereitgestellt wird.
Betreff	Text, der das Event beschreibt.
Event-Zeit	Zeitstempel des Events.
Ressourcen-ID	Eindeutige ID der Ressource, die das Event zum Lebenszyklusstatus oder zur Konfigurationsänderung empfangen hat.

2. Klicken Sie auf einen Eintrag, um die vollständigen Details anzeigen zu lassen.

Einen SSH-Schlüssel erstellen

Ein Stapel kann einen virtuellen Computer enthalten, der einen SSH-Schlüssel für den Zugriff erfordert. Zum Anfordern eines solchen Stapels können Sie entweder ein Ihnen zugewiesenes Schlüsselpaar verwenden oder einen anderen Schlüssel generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Klicken Sie unter Cloudbenutzerportal auf **Activities** (Aktivitäten).
2. In **Aktivitäten** Liste, wählen Sie aus **Verwalten** > **Keys**an.
3. Klicken Sie auf der Seite **SSH Key Pair** (SSH-Schlüsselpaar) auf **Generate Key Pair** (Schlüsselpaar generieren), geben Sie einen **Namen** für den Schlüssel an, und klicken Sie dann auf **OK**.

Ergebnis
Das System erzeugt das Schlüsselpaar mit dem **Namen**, den Sie angegeben haben.

Einen SSH-Schlüssel herunterladen

Wenn für eine Ressource auf einem Stapel eine Anmeldung erforderlich ist, müssen Sie den zugehörigen SSH-Schlüssel herunterladen, bevor Sie auf die Ressource zugreifen können.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Klicken Sie im **Cloud-Benutzerportal** auf **Activities** (Aktivitäten).
2. In **Aktivitäten** Liste, wählen Sie aus **Verwalten** > **Keys**an.
3. Klicken Sie in der Liste **SSH Key Pair** (SSH-Schlüsselpaar) auf einen Schlüssel und dann auf **Download Private Key** (Privaten Schlüssel herunterladen) im Abschnitt **SSH Private Key** (Privater SSH-Schlüssel).

Geschäftszeitpläne

Sie können auf allen virtuellen Computern in einem Stapel Geschäftszeitpläne einrichten. Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden.

Zeitpläne können dafür festgelegt werden, wann ein Stapel gestartet, gestoppt und/oder seine Bereitstellung aufgehoben werden soll, indem Parameter wie Geschäftszeiten, Feiertage oder lange Wochenenden definiert werden.

Hinweis: Für den auf Google Deployment Manager (GDM) basierenden Vorlagenkatalog werden Geschäftszeitplanung und Vorgänge auf Stapelebene nicht unterstützt.

Der Administrator kann Zeitplanprofile im **Cloud Admin Portal** (Cloudverwaltungsportal) erstellen. Weitere Informationen finden Sie unter Ressourcenprofile.

Wählen Sie bei der Bereitstellung eines Stapels im Cloud-Benutzerportal mithilfe der Liste **Schedule Profile** (Zeitplanprofil) ein Profil aus, das bereits vom Administrator erstellt wurde. Wählen Sie in der Liste **Zeitzone des Zeitplans** eine Zeitzone aus, die standardmäßig der Zeitzone Ihres Systems entspricht und die Zeitzone angibt, in der die Geschäftszeiten des Zeitplans umgesetzt werden.

Sie können während der Bereitstellung auch den Mietendzeitpunkt für einen Stapel definieren. Der Mietendzeitpunkt für einen Stapel kann jederzeit geändert werden. Weitere Informationen finden Sie unter Die Miete für einen Stapel ändern.

Sobald Sie einen Stapel mit einem Zeitplan und/oder Mietzeitpunkten bereitgestellt haben, erfolgt eine Reihe von Vorgängen (Start, Stopp, Aufhebung der Bereitstellung) zum von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihnen festgelegten Zeitpunkt. Sie können einen Geschäftszeitplanvorgang überspringen oder die einem Zeitplan zugeordneten Geschäftszeitplanvorgänge abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.

Die Miete für einen Stapel ändern

Wenn ein Stapel das Ende seiner Miete erreicht, benachrichtigt das System den Stapel-Besitzer und hebt die Stapel-Bereitstellung auf. Sie können die Miete für einen Stapel ändern, bevor das Enddatum erreicht ist.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Allen bereitgestellten Stapeln wird ein Mietendzeitpunkt zugewiesen. Eine integrierte Richtlinie mit dem Titel *`Lease End ServiceNow`* mit einem Richtlinienauslöser *`on Lease end`* weist Regeln auf, die Benachrichtigungen und Vorgänge definieren, die vor dem Enddatum der Miete, währenddessen und danach ausgeführt werden. Mietzeitpunkte können für aktive Stapel geändert werden. Das System sendet einen Tag vor Ende des Mietzeitraums eine Benachrichtigung an den Stapel-Besitzer. Am Tag, an dem die Miete endet, stoppt das System den Stapel und sendet eine weitere Benachrichtigung. Sieben Tage nach Ende der Miete wird der Stapel beendet und eine endgültige Benachrichtigung an den Stapel-Besitzer gesendet. Sie können die durchgeführten Aktionen und die Zeitpläne dieser Aktionen ändern, indem Sie die Richtlinie *`Lease End ServiceNow`* ändern. Sie können die Standardmietdauer für alle neuen Stapel ändern, indem Sie das zugehörige Aktionsskript in der integrierten Richtlinie *`Scheduling Defaults`* ändern.

Prozedur

1. Navigieren zu **Alle** > **Übersicht** > **Aktivitäten anzeigen**, Und wählen Sie dann aus **Leasingvorgänge**an.
   Eine Liste von Stapeln mit bevorstehenden Mietvorgängen wird angezeigt.
2. Klicken Sie auf die dem Stapel zugeordnete Liste **Select Action** (Aktion auswählen), und wählen Sie dann **Modify Lease** (Miete ändern).
   Die Option **Modify Lease** (Miete ändern) ist auch in der Liste der Stapeldetails unter **Stapel verwalten** verfügbar.
3. Legen Sie ein neues Datum und eine neue Uhrzeit für den Ablauf der Miete fest, und klicken Sie dann auf **OK**.

Geschäftszeitplanvorgänge für einen Stapel ändern

Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Sobald ein Stapel mit einem Geschäftszeitplan eingerichtet wurde, generiert das System eine Reihe von Aufgaben zum Starten und Beenden des Stapels. Sie können diese Aufgaben anzeigen lassen und den Geschäftszeitplan für jeden Stapel ändern.

Prozedur

1. Navigieren zu **Alle** > **Übersicht** > **Aktivitäten anzeigen**, Und wählen Sie dann aus **Geschäftsszeitplanvorgänge**an.
   Eine Liste von Stapeln mit bevorstehenden Geschäftszeitplanvorgängen wird angezeigt.
2. Führen Sie in der dem Stapel zugeordneten Liste **Aktion auswählen** einen der beiden folgenden Vorgänge aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Skip Operation** (Vorgang überspringen) – Klicken Sie hier, um einen einzelnen Geschäftszeitplanvorgang auf einem Stapel zu überspringen. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.
- **Cancel Schedule** (Zeitplan abbrechen) – Klicken Sie hier, um die Geschäftszeitplanung auf einem Stapel abzubrechen. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.

Wenn Sie den Zeitplan eines bestehenden Stapels ändern möchten, navigieren Sie zur Stapeldetailliste unter **Stapel verwalten** und wählen Sie **Modify Schedule** (Zeitplan ändern) aus der Liste **Stapelvorgang auswählen**.

Verwalten persönlicher Ressourcen und Gruppenressourcen

Sie können Ihre Ressourcen aufrufen und verwalten sowie die Ressourcen, die der Gruppe zugewiesen sind, der Sie angehören. Wenn Sie mehreren Gruppen angehören, können Sie alle diesen Gruppen zugewiesenen Ressourcen anzeigen lassen und verwalten.

Vorbereitungen

Erforderliche Rolle: Stammadministrator [sn_CMP.CMP_root_admin] und Systemadministrator [admin].

Warum und wann dieser Vorgang ausgeführt wird

Nur ein Stammadministrator und ein Systemadministrator haben Zugriff auf alle drei Filter: **Mining** , **Meine Gruppen** , Und **Alle** .

Prozedur

1. Auf der Cloudbenutzerportal, Wählen Sie aus **Ansichten** Filter, nach rechts auf dem Banner.
2. Wählen Sie eine Option aus:
   - **Mine** (Meine): Nur Ressourcen anzeigen und verwalten, die Ihnen zugewiesen sind.
   - **My Groups** (Meine Gruppen): Lassen Sie alle Ressourcen anzeigen, die Ihnen und allen Mitgliedern aller Gruppen, denen Sie angehören, zugewiesen sind, und verwalten Sie sie.

Schemata von Cloud Provisioning and Governance-Tabellen

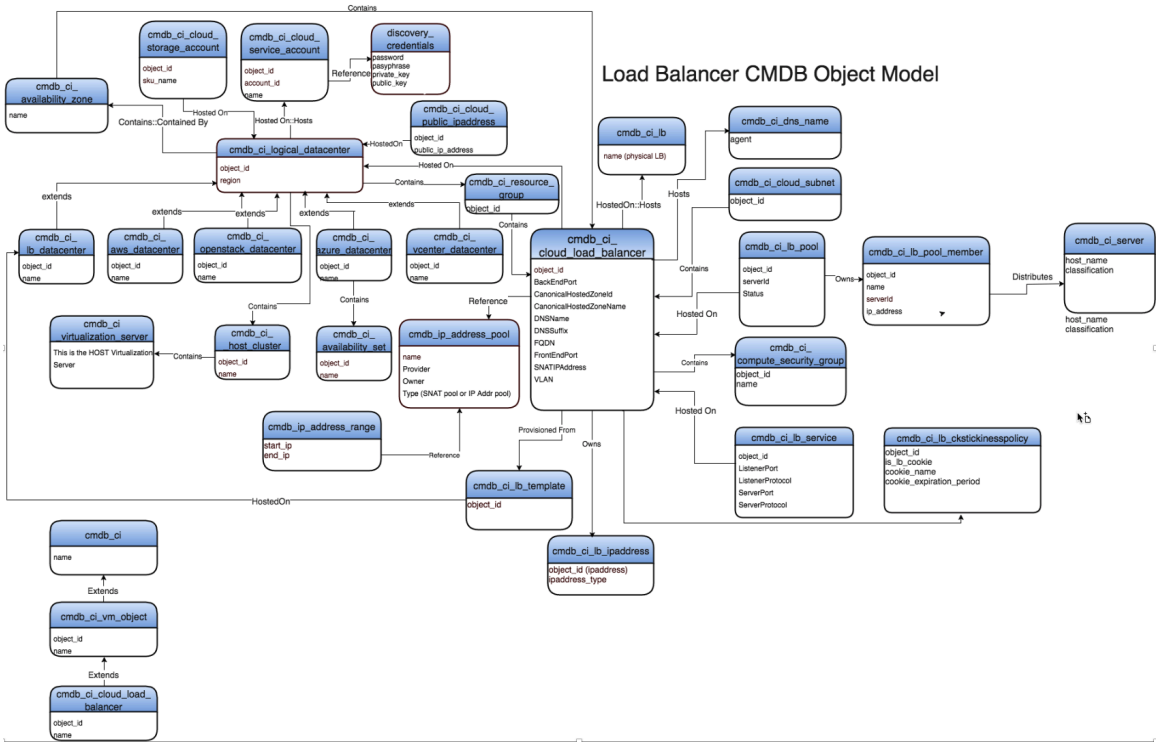
Die Tabellen sind cloudagnostisch und können daher Daten für jeden Cloud-Anbieter enthalten.

Ressourcentabelle Lastenausgleich

Die Lastenausgleichstabelle [cmdb_ci_cloud_load_balancer] baut auf [cmdb_ci_vm_object auf], was auf [cmdb_ci] aufbaut. Klicken Sie, um das Bild zu vergrößern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schema-Lastenausgleichsmodul



Wichtige native Attribute der Tabelle „cmdb_ci_cloud_load_balancer“

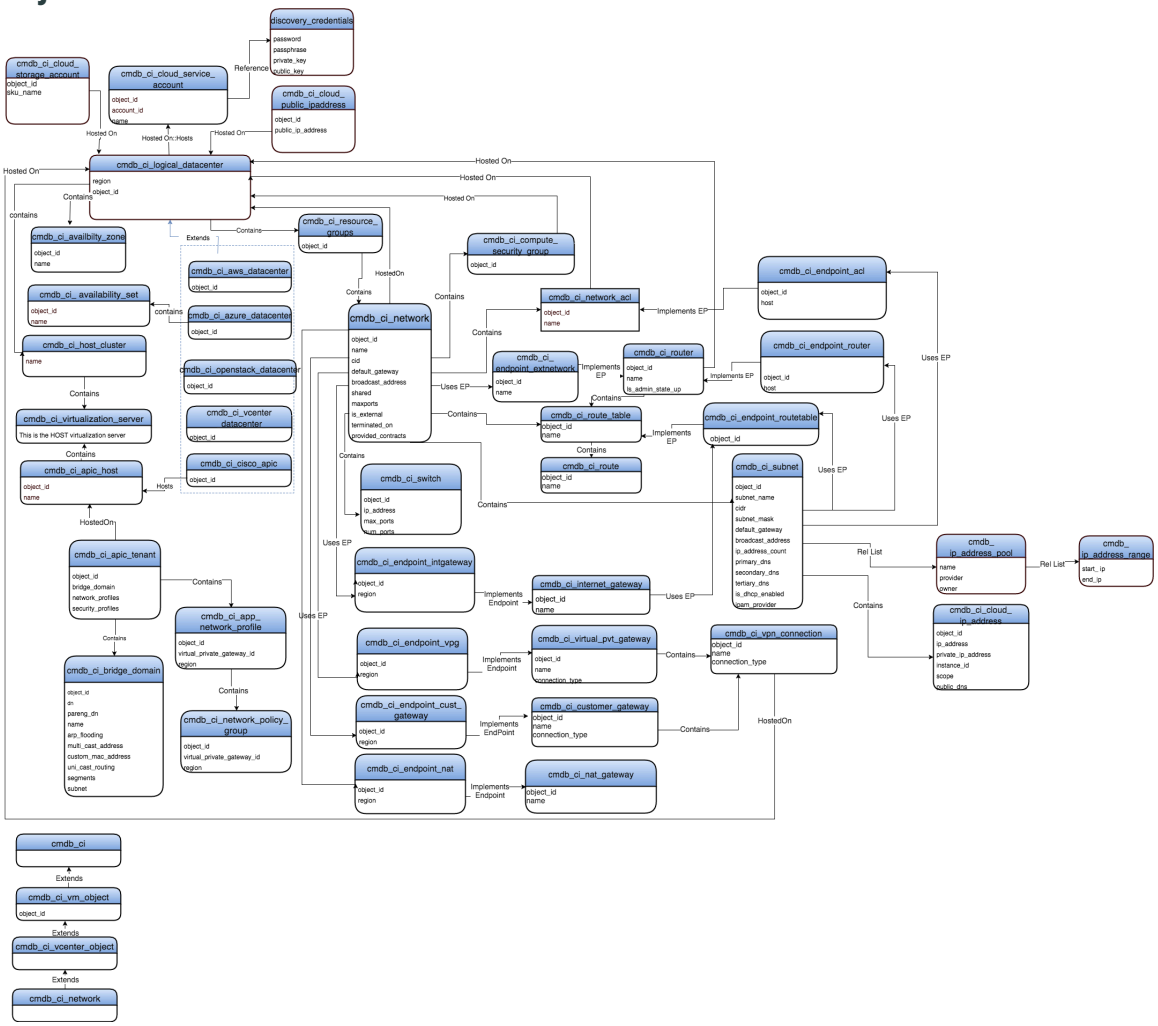
Attribut	Beschreibung
object_id	Bezeichner, der normalerweise den Namen des Lastenausgleichsmoduls als Wert enthält.
canonical_hosted_zone_id	ID der von Amazon Route 53 gehosteten Zone für das Lastenausgleichsmodul.
canonical_hosted_zone_name	DNS-Name des Lastenausgleichmoduls.
dns_name	Öffentlicher DNS-Name des Lastenausgleichmoduls.
fqdn	DNS-Name als vollqualifizierter Domänenname. Kann auch ein CNAME-Datensatz sein, der auf den DNS-Namen verweist.
state	Status des Lastenausgleichmoduls: **available** (verfügbar) oder **terminated** (beendet).

Netzwerkressourcentabelle

Die Netzwerkressourcentabelle [cmdb_ci_network] baut auf [cmdb_ci_vcenter_object] auf, was auf [cmdb_ci_vm_object] aufbaut, und dies wiederum auf [cmdb_ci]. Klicken Sie, um das Bild zu vergrößern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objektmodell – Netzwerktabelle



Wichtige native Attribute der Tabelle „cmdb_ci_network“

Attribut	Beschreibung
object_id	Bezeichner, der normalerweise die Netzwerk-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
name	Name des Netzwerks.
cidr	IP-Adressbereich. Klassenloses Inter-Domain-Routing setzt sich aus einer Reihe von Internetprotokollstandards zusammen, die zum Erstellen eindeutiger Bezeichner für Netzwerke verwendet werden.
default_gateway	Enthält InternetGatewayID, wenn IntenetGateway an das Netzwerk angefügt wird. Ein Standardgateway dient als Zugangspunkt oder IP-Router, über den ein vernetzter Computer Informationen an einen Computer in einem anderen Netzwerk oder Internet sendet. Das angegebene Gateway wird standardmäßig verwendet, es sei denn, eine Anwendung gibt ein anderes Gateway an.
Broadcast_address	IP-Adresse, die zur Übertragung von Nachrichten und Datenpaketen an Netzwerksysteme verwendet wird.
Is_shared	Boolescher Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

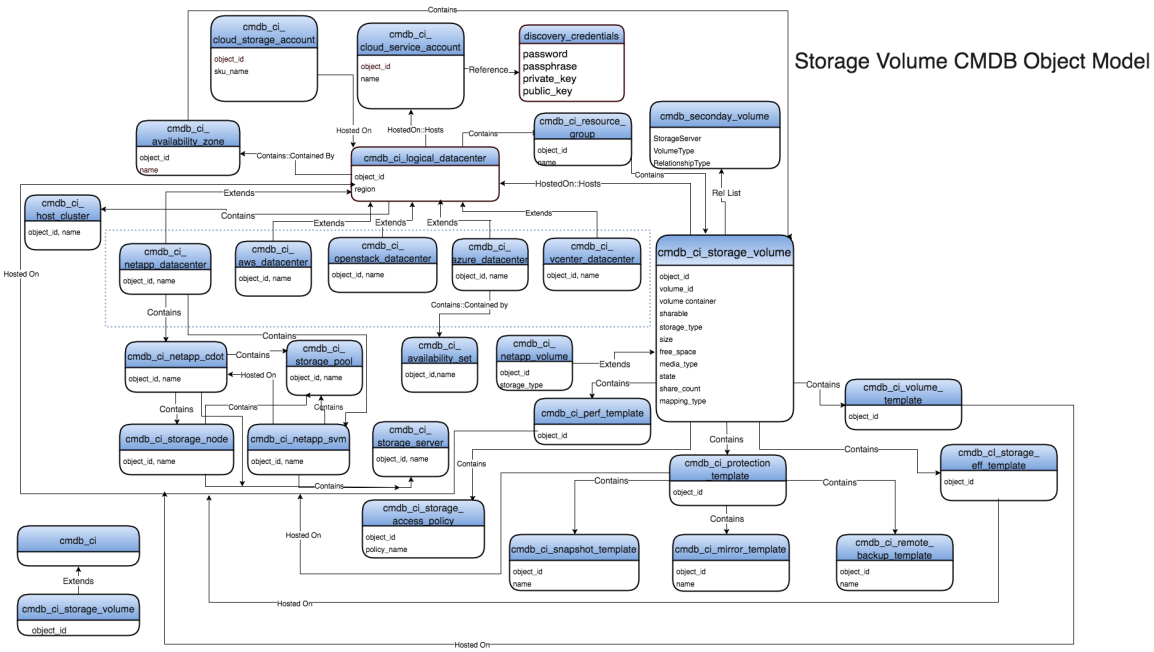
Wichtige native Attribute der Tabelle „cmdb_ci_network“ (Fortsetzung)

Attribut	Beschreibung
	„true“: Netzwerk, das von anderen Projekten gemeinsam verwendet wird. false: Netzwerk, das nicht von anderen Projekten verwendet wird.
max_ports	Maximale Anzahl von Hosts, die mit dem Netzwerk verbunden werden können
is_external	Boolescher Wert. „true“: Netzwerk ist extern. „false“: Netzwerk ist intern.
terminated_on	Zeit, zu der die Bereitstellung des Netzwerks aufgehoben wurde.
state	Status des Netzwerks: **available** (verfügbar) oder **terminated** (beendet).
netmask	CIDR-Typ. 32-Bit-Maske, die eine IP-Adresse in Subnetze unterteilt und die im Netzwerk verfügbaren Hosts angibt.
dhcp_enabled	Boolescher Wert: „true“: Dynamische IP-Adresse wird dem Host zugewiesen „false“: Statische IP-Adresse wird dem Host zugewiesen

Speicher-Laufwerk-Ressourcentabelle

Die Ressourcentabelle [cmdb_ci_storage_volume] des Speicher-Laufwerks baut auf [cmdb_ci] auf. Klicken Sie, um das Bild zu vergrößern.

Schemaspeicher-Volume



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

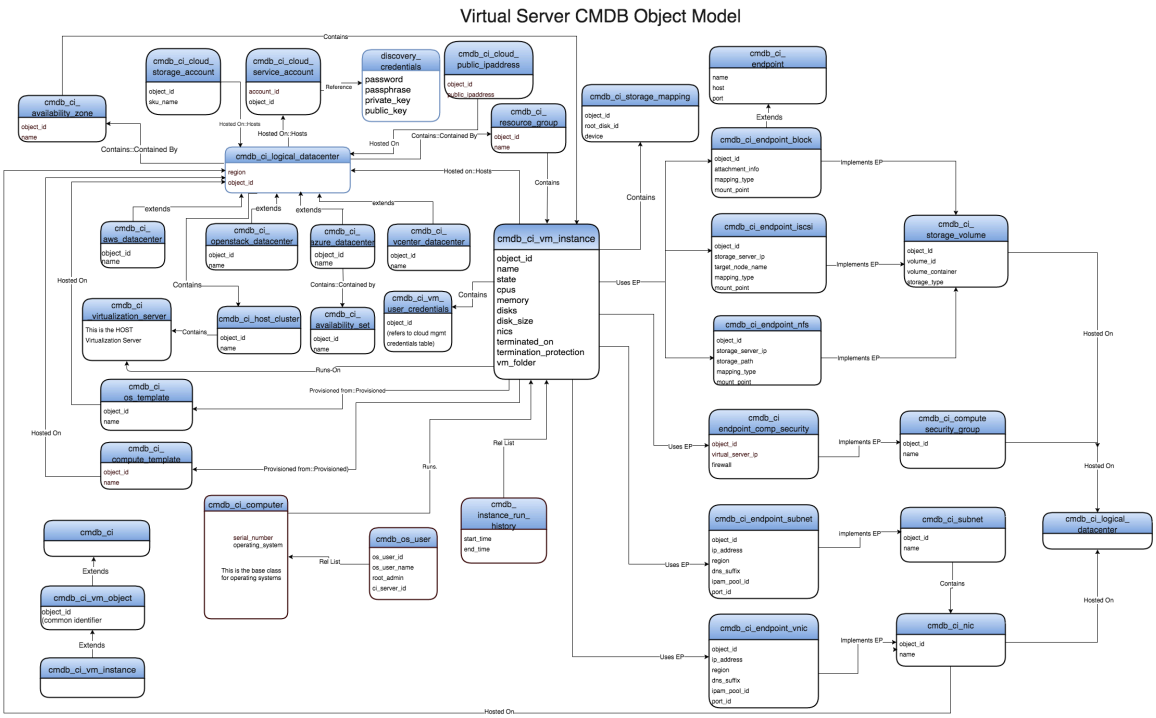
Wichtige native Attribute der Tabelle „cmdb_ci_storage_volume“

Attribut	Beschreibung
object_id	Bezeichner, der üblicherweise die Objekt-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
volume_id	Bezeichner, der üblicherweise die Laufwerk-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
volume_container	Für NetApp Nur wird LUN zum Volume und NetApp Volume wird zum Volume-Container.
sharable	Boolescher Wert. „true“: Laufwerk wird von mehreren VMs gemeinsam verwendet. „false“: Laufwerk wird nicht von mehreren VMs gemeinsam verwendet.
storage_type	Typ des Speichers. • AWS: Block • Azure: PageBlob • vSphere: VMware vdisk
size	Gesamtkapazität des Laufwerks.
free_space	Verfügbarer Speicherplatz des Laufwerks
state	Status des Volumes: **available** (verfügbar) oder **in_use** (in Verwendung).
share_count	Anzahl der VMs, die vom Volume gemeinsam verwendet werden.

Ressourcentabelle des virtuellen Servers

Die Ressourcentabelle des virtuellen Servers [cmdb_ci_vm_instance] baut auf [cmdb_ci_vm_object], was auf [cmdb_ci] aufbaut. Klicken Sie, um das Bild zu vergrößern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wichtige native Attribute der Tabelle „cmdb_ci_vm_instance“

Attribut	Beschreibung
object_id	Bezeichner, der normalerweise die ID der VM-Instanz enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
name	Name der VM
state	Status der VML: **on** (ein), **off** (aus) oder **terminated** (beendet).
cpus	Anzahl an CPUs
memory	Speichergröße in Megabyte
disks	Anzahl der Laufwerke
disk_size	Gesamtgröße der Datenträger in Gigabyte
nics	Anzahl der Netzwerkadapter
terminated_on	Zeit, zu der die Instanz beendet wurde.
termination_protection	Boolescher Wert. Der Standardwert ist „false“. „true“: Kann verhindern, dass die Instanz versehentlich mit Amazon EC2 beendet wird. „false“: Kann nicht verhindern, dass die Instanz versehentlich mit Amazon EC2 beendet wird.

Schnellstarttests für Cloud Provisioning and Governance

Überprüfen Sie, ob Cloud Provisioning and Governance noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. das Anwenden eines Upgrades oder die Entwicklung einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance

Cloud Provisioning and Governance-Schnellstarttests erfordern die Aktivierung der folgenden Cloud Provisioning and Governance-Plugins:

- Cloud Provisioning and Governance (com.snc.cloud.mgmt)
- Plugin „Domain Support – Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer)
- Plugin „Servicekatalog – Domain Separation“ (glideapp.servicecatalog.domain_separation)

Cloud Provisioning and Governance: Azure-Test-Suite

Test	Beschreibung	Release-Version
CMP: Azure-Anmeldeinformationen hinzufügen	Fügt Azure-Anmeldeinformationen hinzu, indem die Felder in die Tabelle „Anmeldeinformationen“ eingefügt werden.	Orlando
CMP: Azure-Serviceaccount	Fügt einen Azure-Serviceaccount hinzu, indem die Felder in die Tabelle „Service-Account“ eingefügt werden.	Orlando
CMP: Rechenzentrumstyp aktualisieren	Aktualisiert das Cloud-Servicekonto mit dem Rechenzentrumstyp.	Orlando
CMP: Ressourcengruppe erstellen	Erstellt eine Ressourcengruppe zum Bereitstellen des Azure-Stack über eine ARM-Vorlage.	Orlando
CMP: Logisches Azure-Rechenzentrum erstellen	Erstellt ein logisches Azure-Rechenzentrum für die Bereitstellung von Ressourcen.	Orlando
CMP: „Contains: Contained by“-Beziehung erstellen	Erstellt eine „Contains: Contained by“-Beziehung zwischen Ressourcengruppe und Azure-Rechenzentrum.	Orlando
CMP: „Gehostet auf“-Beziehung erstellen	Erstellt eine „gehostet auf“-Beziehung zwischen logischem Rechenzentrum und Cloud-Serviceaccount.	Orlando
CMP: Cloudaccount erstellen	Erstellt einen Cloudaccount, indem die Felder in die Cloudaccount-Tabelle eingefügt werden.	Orlando
CMP: Zuordnung zwischen Cloudaccount und logischem Rechenzentrum	Erstellt eine Zuordnung zwischen CMP-Cloud-Konto und logischem Rechenzentrum.	Orlando
CMP: Katalogelement erstellen	Erstellt ein Cloud-Katalogelement mit der ARM-Vorlage.	Orlando
CMP: Vorlagenversion erstellen	Erstellt eine Cloud-Vorlagenversion für das Cloud-Katalogelement.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: Azure-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
CMP: ARM-Vorlagentext	Aktualisiert die Cloud-Vorlagenversionen mit dem ARM-Vorlagentext.	Orlando
CMP: „ServiceNow-Cloud-Vorlagenversionen“ öffnen	Öffnet die GUI-Seite „ServiceNow-Cloud-Vorlagenversionen“.	Orlando
CMP: Cloud-Vorlagenversion aktivieren	Aktiviert die Cloud-Vorlagenversion, um Ressourcenblock, Blueprint und Katalog zu erstellen.	Orlando
CMP: Cloud-Vorlagenversion überprüfen	Validiert, ob der Status „Erfolg“ lautet und ob der Status in der Cloud-Vorlagenversionen nach dem Aktivierungsvorgang aktiv ist.	Orlando
CMP: Cloud-Katalogelement aktivieren	Aktiviert das Cloud-Katalogelement, um dem Cloud-Benutzer das Katalogbestellformular anzuzeigen.	Orlando
CMP: Stapel- und Ressourcengruppennamen in Katalogelement hinzufügen	Legt den Standardwert für Stapelnamen und Ressourcengruppe im Katalogelement fest.	Orlando
CMP: Überprüfen, ob Stapel vorhanden ist	Validiert, ob der Stapel mit dem Namen „ATFARMStack“ verfügbar ist.	Orlando
CMP: Cloud-Katalogelement-Seite öffnen	Öffnet die Seite „Cloud-Katalogelement“ im Serviceportal.	Orlando
CMP: Katalogformular absenden	Sendet das Katalogformular, um die Bereitstellung des ARM-Stacks zu starten.	Orlando
CMP: Überprüfen, oder der Stapelstatus aktiv ist	Validiert den Status eines Stapels nach der Bereitstellung des Stapels.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang stoppen	Validiert, dass sich der Status des Stapels nach dem Stoppvorgang von „Ein“ in „Aus“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang starten	Validiert, dass sich der Status des Stapels nach dem Startvorgang von „Aus“ in „Ein“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang „Aufheben der Bereitstellung“	Validiert, dass sich der Stapelstatus nach dem Vorgang „Aufheben der Bereitstellung“ von „Aus“ in „Beenden“ geändert hat.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: AWS-Test-Suite

Test	Beschreibung	Release-Version
CMP: AWS-Anmeldeinformationen hinzufügen	Fügt AWS-Anmeldeinformationen hinzu, indem die Felder in die Tabelle „Anmeldeinformationen“ eingefügt werden.	Orlando
CMP: Serviceaccount für AWS	Fügt einen Serviceaccount für AWS hinzu, indem die Felder in die Tabelle „Servicekonto“ eingefügt werden.	Orlando
CMP: Rechenzentrumstyp aktualisieren	Aktualisiert das Cloud-Servicekonto mit dem Rechenzentrumstyp.	Orlando
CMP: Logisches Rechenzentrum erstellen	Erstellt ein logisches Rechenzentrum für die Bereitstellung von Ressourcen.	Orlando
CMP: „Gehostet auf“-Beziehung erstellen	Erstellt eine „gehostet auf“-Beziehung zwischen logischem Rechenzentrum und Cloud-Serviceaccount.	Orlando
CMP: Cloudaccount erstellen	Erstellt einen Cloudaccount, indem die Felder in die Cloudaccount-Tabelle eingefügt werden.	Orlando
CMP: Zuordnung zwischen Cloudaccount und logischem Rechenzentrum	Erstellt eine Zuordnung zwischen CMP-Cloud-Konto und logischem Rechenzentrum.	Orlando
CMP: Katalogelement erstellen	Erstellt ein Cloud-Katalogelement mit der CFT-Vorlage.	Orlando
CMP: Vorlagenversion erstellen	Erstellt eine Cloud-Vorlagenversion für das Cloud-Katalogelement.	Orlando
CMP: CFT-Vorlagentext	Aktualisiert die Cloud-Vorlagenversionen mit dem CFT-Vorlagentext.	Orlando
CMP: ServiceNow-Cloud-Vorlagenversionen öffnen	Öffnet die GUI-Seite „ServiceNow-Cloud-Vorlagenversionen“.	Orlando
CMP: Cloud-Vorlagenversion aktivieren	Aktiviert die Cloud-Vorlagenversion, um Ressourcenblock, Blueprint und Katalog zu erstellen.	Orlando
CMP: Cloud-Vorlagenversion überprüfen	Validiert, ob der Status der Cloud-Vorlagenversionen „Erfolg“ lautet und ob der Status nach dem Aktivierungsvorgang aktiv ist.	Orlando
CMP: Cloud-Katalogelement aktivieren	Aktiviert das Cloud-Katalogelement, um	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: AWS-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
	dem Cloud-Benutzer das Katalogbestellformular anzuzeigen.	
CMP: Stapelnamen in Katalogelement hinzufügen	Legt den Standardwert für den Stapelnamen im Katalogelement fest.	Orlando
CMP: Überprüfen, ob Stapel vorhanden ist	Validiert, ob der Stapel mit dem Namen „ATFCFTStack“ verfügbar ist.	Orlando
CMP: Cloud-Katalogelement-Seite öffnen	Öffnet die Seite „Cloud-Katalogelement“ im Serviceportal.	Orlando
CMP: Katalogformular absenden	Sendet das Katalogformular, um die Bereitstellung des CFT-Stacks zu starten.	Orlando
CMP: Überprüfen, oder der Stapelstatus aktiv ist	Validiert den Status des Stapels nach der Bereitstellung des Stapels.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang stoppen	Validiert, dass sich der Status des Stapels nach dem Stoppvorgang von „Ein“ in „Aus“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang starten	Validiert, dass sich der Status des Stapels nach dem Startvorgang von „Aus“ in „Ein“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang „Aufheben der Bereitstellung“	Validiert, dass sich der Stapelstatus nach dem Vorgang „Aufheben der Bereitstellung“ von „Aus“ in „Beenden“ geändert hat.	Orlando

Weitere Informationen zu Cloud Provisioning und Governance finden Sie unter Cloud Provisioning and Governance.

Zugehörige Informationen

Schnellstarttests

Governance für Cloud-Konfigurationen

Verwenden Sie die Anwendung ServiceNow® Governance für Cloud-Konfigurationen, um die Konfigurationseinstellungen von Cloud-Ressourcen in Ihrer Organisation anhand einer Reihe von Richtlinien zu überprüfen und so Verstöße zu identifizieren. Nachdem Sie den Verstoß identifiziert haben, verwenden Sie Fehlerkorrektur-Workflows, um ihn zu minimieren.

Hinweis: Governance für Cloud-Konfigurationen Wird in selbst gehosteten Umgebungen nicht unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen erkunden	• Cloud Configuration Governance installieren • CCG Inhaltspaket installieren • Cloud Configuration Governance für AWS einrichten • Cloud Configuration Governance für Microsoft Azure einrichten	• Richtlinien • Scan-Konfiguration • Fehlerkorrektur

Verwenden	Entwickeln	Problembehandlung und Hilfe
• Scan-Konfiguration ausführen • Dashboard anzeigen • Korrektur ausführen	• Entwicklerschulungen • Entwicklerdokumentation	• Fragen stellen oder beantworten im Governance für Cloud-Konfigurationen-Forum der ServiceNow Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support

Governance für Cloud-Konfigurationen erkunden

Verstehen Sie den typischen Governance für Cloud-Konfigurationen-Workflow und allgemeine Aufgaben.

Um Governance für Cloud-Konfigurationen für die Verwaltung der Konfiguration der Cloud-Ressourcen zu verwenden, führen Sie die folgenden Aufgaben aus:

1. Installieren Sie Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Cloud Configuration Governance installieren.
2. Installieren Sie das CCG-Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte. Weitere Informationen finden Sie unter CCG Inhaltspaket installieren.
3. Weisen Sie Benutzern Governance für Cloud-Konfigurationen-Rollen zu. Weitere Informationen zu den Governance für Cloud-Konfigurationen-Rollen finden Sie unter Cloud Configuration Governance-Rollen und -Systemeigenschaften.
4. Informationen zum Verwalten der Konfiguration der Ressourcen von Amazon Web Services (AWS) über Governance für Cloud-Konfigurationen finden Sie unter Cloud Configuration Governance für AWS einrichten.
5. Informationen zum Verwalten der Konfiguration der Microsoft Azure-Ressourcen über Governance für Cloud-Konfigurationen finden Sie unter Cloud Configuration Governance für Microsoft Azure einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Erstellen Sie eine Scan-Konfiguration, um die Cloud-Ressourcen anhand mindestens eines Richtliniensatzes zu scannen und die Richtlinienverstöße zu identifizieren. Weitere Informationen finden Sie unter Scan-Konfiguration erstellen.
7. Führen Sie die entsprechende Korrekturaktion aus, um die nicht konforme Cloud-Konfiguration zu beheben, die während der Scan-Ausführung identifiziert wurde. Weitere Informationen finden Sie unter Korrektur ausführen.

Nächste Schritte

Siehe Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate Um die Liste der Plugins zu finden, die Sie mit aktivieren Governance für Cloud-Konfigurationen.

Governance für Cloud-Konfigurationen installieren

Sie können die Anwendung Governance für Cloud-Konfigurationen (com.sn.itom.ccg) installieren, wenn Sie über die Administratorrolle verfügen. Die zugehörigen Anwendungsinstallationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Governance für Cloud-Konfigurationen Verwendet ServiceNow® ITOM Cloud Accelerate Abonnement. Wenn Sie diese Anwendung installieren, werden automatisch mehrere Rollen und die Anwendung ServiceNow® Bibliothek von Cloud-Aktionen (sn.itom.cal) installiert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Governance für Cloud-Konfigurationen (com.sn.itom.ccg).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .
3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation” die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden, derzeit installiert sind oder installiert werden müssen. Wenn Plugins oder Anwendungen installiert werden müssen, müssen Sie sie installieren, bevor Sie Governance für Cloud-Konfigurationen installieren können.
4. Wählen Sie **Installieren** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Um auf die Inhalte des Basissystems wie Richtlinien, Konfigurationssammler, Korrekturen usw. zuzugreifen, installieren Sie CCG Inhaltspaket Anwendung. Weitere Informationen finden Sie unter CCG Content Pack installieren.

CCG Inhaltspaket installieren

Sie können installieren CCG Inhaltspaket Anwendung (sn_itom_ccg_cp), wenn Sie die Administratorrolle innehaben.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie die CCG Content Pack -Anwendungsliste im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die CCG Inhaltspaket Stellt die Inhalte des Basissystems bereit, z. B. Richtlinien, Ressourcensammler, Konfigurations-Sammler und Korrekturaktionen für Governance für Cloud-Konfigurationen App.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach CCG Inhaltspaket Anwendung (sn_itom_ccg_cp) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
4. Wählen Sie **Installieren** aus.

Governance für Cloud-Konfigurationen for AWS einrichten

Richten Sie in Governance für Cloud-Konfigurationen Zugriff auf die AWS-Cloud-Konten (Amazon Web Services) ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen. Die Anwendung erfordert Zugriff auf die Cloud-Konten, damit die Cloud-Ressourcen auf nicht konforme Konfigurationen gescannt und nicht konforme Konfigurationen korrigiert werden können.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf zu konfigurieren AWS Accounts:

- Konfigurieren Sie die permanenten Anmeldeinformationen in ServiceNow AI Platform Um eine Verbindung mit dem eigenständigen herzustellen AWS Accounts (diskrete Accounts). Die Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service-account] enthält die Informationen zum Servicekontotyp wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
- Konfigurieren Sie die Mitgliedskonten so, dass sie für den Zugriff auf das Verwaltungskonto zurückgreifen. Konfigurieren Sie die permanenten Anmeldeinformationen des Verwaltungskontos in diesem Fall auf der ServiceNow AI Platform.
- Konfigurieren Sie die Konten so, dass für den Zugriff ein vertrauenswürdiges Konto verwendet wird (lateraler Zugriff innerhalb derselben AWS-Organisation oder über verschiedene AWS-Organisationen hinweg). Konfigurieren Sie die permanenten Anmeldeinformationen des vertrauenswürdigen Kontos in diesem Fall auf der ServiceNow AI Platform.

Hinweis: Governance für Cloud-Konfigurationen Verwendet kein MID-serverbasiertes Übernahmerollen-Setup für den Zugriff auf die vertrauenden Accounts.

Prozedur

1. Erstellen Sie Anmeldeinformationen für die AWS-Servicekonten.
   a. Navigieren zu **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen**an.
   b. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus.
   c. Füllen Sie die Felder des Formulars aus.

Formular für AWS-Anmeldeinformationen

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die Zugriffsschlüssel-ID, die Sie in der AWS-Verwaltungskonsole erstellt haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Zugangsschlüssel	Der geheime Zugriffsschlüssel, den Sie in der AWS-Verwaltungskonsole erstellt haben

d. Wählen Sie **Speichern**.

2. Wählen Sie den Anmeldeinformationsalias **sn_itom_cal.Aws_Creds_Alias** aus, oder erstellen Sie einen Anmeldeinformationsalias.

a. Entsperren Sie den Anmeldeinformationsalias.

b. Suchen Sie nach einem Anmeldeinformationsalias.

c. Wählen Sie **Neu**.

d. Füllen Sie die Felder des Formulars aus.

Formular „Verbindungs- und Anmeldeinformationsalias“

Feld	Beschreibung
Name	Eindeutiger Name des Alias
Typ	Typ des Anmeldeinformationsalias. Wählen Sie in der Dropdown-Liste „Typ“ die Option **Anmeldeinformationen** aus.

e. Wählen Sie **Absenden** aus.

3. Legen Sie das Feld **Authentifizierungsalgorithmus** auf **AWS Authenticator** fest.

4. Wählen Sie **Absenden** aus.

5. Richten Sie ein AWS-Servicekonto ein.

a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**an.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger Name des Servicekontos
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Discovery-Anmeldeinformationen	Die für erforderlichen Anmeldeinformationen ServiceNow Anwendungen für den Zugriff auf den Cloud-Account. Sie können die Discovery-Anmeldeinformationen zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf konfigurieren AWS Accounts. ▪ Wenn Sie ein unabhängiges Servicekonto oder ein Verwaltungskonto einrichten, wählen Sie die zugehörigen AWS-Anmeldeinformationen aus. ▪ Um andere zu verwenden AWS Accounts um auf diesen Account zuzugreifen, lassen Sie das Feld leer. Sie müssen beispielsweise nicht angeben AWS Anmeldeinformationen für Accounts, die IAM-Rollen (Identity and Access Management) annehmen, oder Mitgliedsaccounts, die ihren Verwaltungsaccount für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Lassen Sie dieses Feld leer. **Hinweis:** Verwenden Sie für GovCloud die URL https://ec2.us-gov-west-1.amazonaws.com .
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie **AWS-Rechenzentrum** aus.
Rechenzentrums-Discovery-Status	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die AWS-Organisation darstellt, zu der dieses Mitgliedskonto gehört. Dieses Feld wird angezeigt, wenn Sie „AWS-Rechenzentrum“ auswählen. Wenn der Account zu keinem gehört AWS Organisation, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Dieses Kontrollkästchen wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option „AWS-Rechenzentrum“ auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. Weitere Informationen zu finden AWS Organisation, siehe AWS Dokumentation an.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

d. Wählen Sie **Absenden** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Führen Sie eine der folgenden Aktionen aus.

Option	Beschreibung
Erstellen Sie eine Rollenübernahmekonfiguration für den Verwaltungsaccount	Wenn Sie einen Verwaltungsaccount verwenden möchten, um die Mitgliedsaccounts des zu scannen AWS Organisation: Erstellen Sie eine Rollenübernahmekonfiguration für den Verwaltungsaccount. **a.** Wenn Sie die OrganizationAccountAccessRole nicht für den Zugriff auf den Mitgliedsaccount verwenden möchten, konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen Und Bibliothek von Cloud-Aktionen. **b.** Wiederholen Sie den Schritt 6.aFür alle Mitgliedsaccounts, die ohne Verwendung der OrganizationAccountAccessRole über den Verwaltungsaccount gescannt werden müssen. **c.** Wenn Sie die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, erstellen Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto. Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.
Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen	Wenn Sie einen vertrauenswürdigen Account zum Scannen des vertrauenden Accounts verwenden möchten, konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen. **a.** Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen Und Bibliothek von Cloud-Aktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	b. Wiederholen Sie den Schritt 6.aFür alle vertrauenden Accounts, die über den vertrauenswürdigen Account gescannt werden müssen.

7. Installieren und konfigurieren Sie die MID Servers.
   Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MID-Server .
8. Führen Sie die Rechenzentrumserkennung aus, um die mit den Servicekonten verbundenen Rechenzentren zu identifizieren.
   Weitere Informationen finden Sie unter Rechenzentrumserkennung ausführen.

Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen Und Bibliothek von Cloud-Aktionen

Konfigurieren Sie das vertrauende Konto, auf dessen Ressourcen zugegriffen werden muss, so, dass es über die Identity and Access Management (IAM)-Rolle auf das vertrauenswürdige Konto zurückgreift.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Entscheiden Sie, welcher Amazon Web Services (AWS)-Account der vertrauenswürdige Account sein soll. Sie verwenden den vertrauenswürdigen Account zur Konfiguration temporärer Anmeldeinformationen für Governance für Cloud-Konfigurationen mithilfe von IAM-Rollen. Der vertrauenswürdige Account, den Sie für den Zugriff auf andere Accounts mit IAM-Rollen verwenden, wird als Account eines Zugriffsberechtigten bezeichnet.
- Richten Sie den vertrauenswürdigen und den vertrauenden Account wie in beschrieben ein Governance für Cloud-Konfigurationen for AWS einrichten.

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Prozedur

1. Erstellen Sie eine IAM-Rolle für das vertrauende Konto, und konfigurieren Sie die Vertrauensstellung zwischen dem Benutzer, der diese Rolle übernimmt, und dem vertrauenswürdigen Konto (Account des Zugriffsberechtigten).

   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Account an.

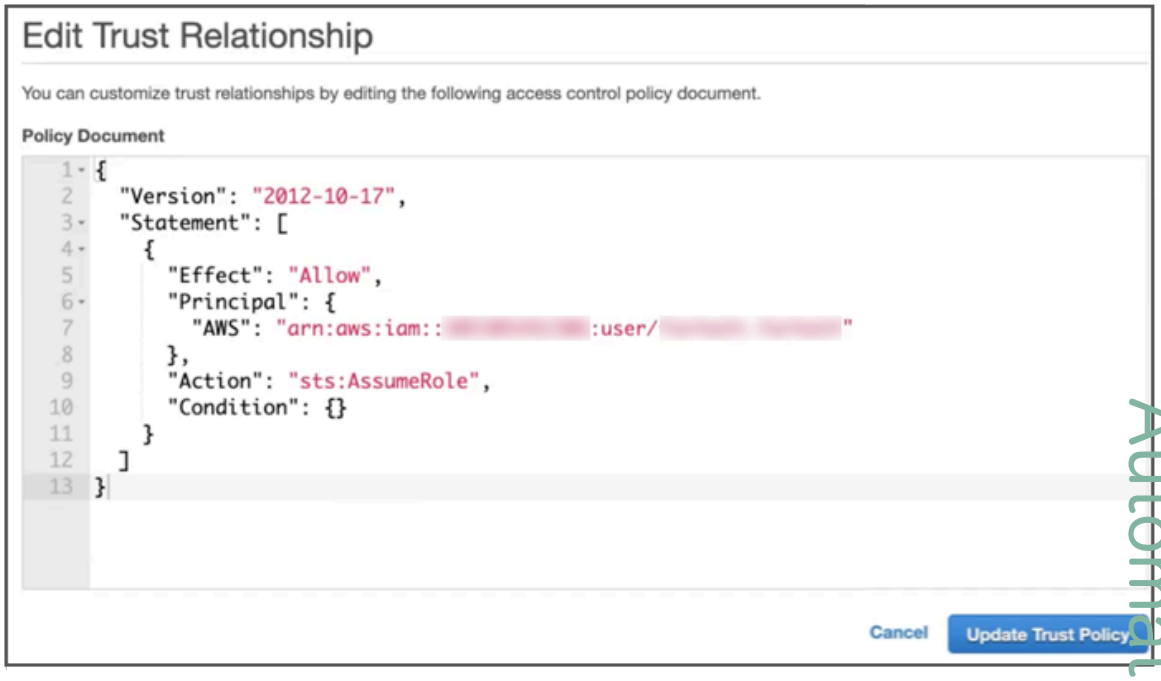
   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des vertrauenswürdigen Kontos (des Accounts des Zugriffsberechtigten) angeben.
   Für Informationen zum Erstellen AWS-Rollen finden Sie unter Amazon Dokumentation an.

   c. Wählen Sie auf der Seite „Zusammenfassung“ für die IAM-Rolle die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten).
   Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Legen Sie den Parameter *AWS* auf den vollständigen Benutzer-ARN des vertrauenswürdigen Accounts (des Zugriffsberechtigten) fest.



f. Verifizieren Sie, ob der `Action`-Wert auf `sts:AssumeRole` festgelegt ist.

g. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Konfigurieren Sie den vertrauenswürdigen Serviceaccount für das vertrauende Konto auf der ServiceNow AI Platform.

a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Service-Konten**

b. Öffnen Sie das vertrauende Konto.

c. Geben Sie im Formular „Cloud-Servicekonto“ den Namen des vertrauenswürdigen Kontos im Feld **Account des Zugriffsberechtigten** ein.

d. Wählen Sie **Aktualisieren**.

3. Erstellen Sie für das vertrauende Konto eine Konfiguration für die Übernahme von Rollen.
Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.

Konfiguration für die Übernahme von Rollen erstellen

Erstellen Sie eine Konfiguration für die Rollenübernahme eines Service-Accounts, um den kontoübergreifenden Zugriff von einem Verwaltungsaccount auf einen Mitgliedsaccount oder von einem vertrauenswürdigen Account auf einen vertrauenswürdigen Account zu einem vertrauenswürdigen Account zu erleichtern.

Vorbereitungen

Stellen Sie sicher, dass die Anmeldeinformationen des Zugriffsberechtigten-Accounts in konfiguriert sind ServiceNow AI Platform.

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn für das Mitgliedskonto keine permanenten Anmeldeinformationen definiert sind, wird von Governance für Cloud-Konfigurationen die Tabelle für die Konfiguration der Rollenübernahme für Cloud-Servicekonten [sn_itom_ccg_service_account_assume_role_config] überprüft, damit die spezielle Konfiguration identifiziert werden kann, die dem Verwaltungskonto zugeordnet ist. Dann werden die Anmeldeinformationen des Verwaltungskontos dazu verwendet, temporäre Anmeldeinformationen für die Mitgliedskonten zu generieren. Wenn die Konfiguration in der Tabelle vorhanden ist, Governance für Cloud-Konfigurationen Verwendet die temporären Anmeldeinformationen, die erworben wurden, indem eine Rolle und ihre Konfiguration in angegeben werden Amazon Web Services(AWS) AssumeRole-Aktion der Sicherheits-Token-Services-API.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Rollenkonfiguration übernehmen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Werte im Formular „Konfiguration der Rollenübernahme für Service-Account“ aus. Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen Formular „Konfiguration der Rollenübernahme für Service-Account“.
4. Wählen Sie **Absenden**.

Governance für Cloud-Konfigurationen for Microsoft Azure einrichten

Richten Sie in Governance für Cloud-Konfigurationen Zugriff auf die Microsoft Azure Cloud-Konten ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen. Die Anwendung erfordert Zugriff auf die Cloud-Konten Ihrer Organisation, damit die Cloud-Ressourcen auf nicht konforme Konfigurationen gescannt und nicht konforme Konfigurationen korrigiert werden können.

Vorbereitungen

Stellen Sie sicher, dass die folgenden Aufgaben abgeschlossen sind:

1. Sie haben von CAPI zu Mustern migriert. Weitere Einzelheiten finden Sie unter Migrieren Sie von CAPI zu Mustern.
2. Die Microsoft Azure Anmeldeinformationen für den Zugriff auf Microsoft Azure Account wurde erstellt. Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.
3. Ihr Azure Service-Accounts wurden konfiguriert. Weitere Informationen finden Sie unter Azure-Servicekonten einrichten.

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Prozedur

1. Erstellen Sie eine IntegrationHub-Verbindung für Microsoft Azure.

   a. Navigieren zu **Prozessautomatisierung** > **Flow Designer**, Und wählen Sie aus **Integrationen** Registerkarte.

   b. Wählen Sie auf der Kachel **Azure Connection** (Azure-Verbindung) die Option **Verbindung hinzufügen** aus.

   c. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Scan-Zeitplan“

Feld	Beschreibung
Verbindungsname	Name der Verbindung
OAuth-Client-ID	Microsoft Azure-Anwendungs-ID
OAuth-Client-Geheimnis	Microsoft Azure-Anwendungsschlüssel
OAuth-Token-URL	Mandanten-ID des Microsoft Azure-Kontos Ersetzen Sie {tenant} durch die Microsoft Azure-Mandanten-ID.

d. Wählen Sie **OAuth-Token erstellen und abrufen** aus.

2. Führen Sie die Rechenzentrumserkennung aus, um die mit den Servicekonten verbundenen Rechenzentren zu identifizieren.
   Weitere Informationen finden Sie unter Rechenzentrumserkennung ausführen.

Domänentrennung und Cloud-Konfigurations-Governance

Domänentrennung wird in nicht unterstützt Governance für Cloud-Konfigurationen . Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Zugehörige Informationen

Domänentrennung für Service Provider

Arbeiten mit Governance für Cloud-Konfigurationen

Governance für Cloud-Konfigurationen bietet eine Reihe von sofort einsatzbereiten Richtlinien. Sie können entweder diese Richtlinien verwenden, um die nicht konformen Cloud-Ressourcenkonfigurationen in Ihrer Cloud-Organisation zu identifizieren, oder benutzerdefinierte Richtlinien erstellen. Nachdem Sie die nicht konformen Cloud-Ressourcenkonfigurationen identifiziert haben, können Sie die Fehlerkorrekturfunktion der Anwendung verwenden, um die Verstöße zu beheben.

Hinweis: Beginnend mit Governance für Cloud-Konfigurationen Version 1,3.7, der Inhalt des Basissystems wird in verschoben CCG Inhaltspaket. Installieren Sie CCG Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte.

Scan-Konfiguration

Die Scan-Konfiguration definiert die verschiedenen Einstellungen für den Governance für Cloud-Konfigurationen-Scan.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine Scan-Konfiguration ausführen, werden von Governance für Cloud-Konfigurationen die Ziel-Cloud-Ressourcentypen aus den Richtliniensätzen identifiziert, die der Scan-Konfiguration angefügt sind. Anschließend werden die entsprechenden Ressourcensammler und Konfigurationssammler aufgerufen, damit die Konfigurationsdaten der Zielressourcentypen importiert werden können. Nach dem Import der Konfigurationsdaten werden die importierten Konfigurationsdaten von Governance für Cloud-Konfigurationen mit den nicht konformen Konfigurationen verglichen, die in den Richtlinien definiert sind. Wird von Governance für Cloud-Konfigurationen eine Übereinstimmung erkannt, wird ein Verstoß im Audit-Verstoßbericht gemeldet.

Sie können die Menge der in das System importierten Konfigurationsdaten reduzieren, indem Sie eine Reihe von Kombinationen aus Servicekonto und Rechenzentrum für die Scan-Konfiguration angeben. Sind solche angegeben, werden von Governance für Cloud-Konfigurationen nur die Daten aus den angegebenen Kombinationen aus Servicekonto und Rechenzentrum importiert. Darüber hinaus können Sie auch Tag-basierte Cloud-Ressourcenfilter verwenden, um die Cloud-Ressourcen zu identifizieren, deren Konfigurationsdaten für den Scan importiert werden müssen.

Weitere Informationen zum Erstellen von Scan-Konfigurationen finden Sie unter Scan-Konfiguration erstellen.

Scan-Konfiguration erstellen

Erstellen Sie in Governance für Cloud-Konfigurationen eine Scan-Konfiguration, um die Cloud-Ressourcen anhand mindestens eines Richtliniensatzes zu scannen und die Richtlinienverstöße zu identifizieren.

Vorbereitungen

- Vergewissern Sie sich, dass ein geeigneter Richtliniensatz für den Scan verfügbar ist. Mit dem Richtliniensatz wird ein bestimmter Sicherheits- oder Organisationsstandard durchgesetzt. Weitere Informationen zum Erstellen des Richtliniensatzes finden Sie unter Richtliniensatz erstellen.
- Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Beginnend mit Governance für Cloud-Konfigurationen Version 1,3.7, der Inhalt des Basissystems wird in verschoben CCG Inhaltspaket. Installieren Sie CCG Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte.

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Konfigurationen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Werte im Formular „Scan Configuration“ (Scan-Konfiguration) aus.
   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans.
4. Wählen Sie **Absenden** aus.
5. Um einen Zeitplan für die Ausführung der Scan-Konfiguration zu erstellen, wählen Sie **Setup Schedule** (Zeitplan einrichten) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. **Wahlweise:** Legen Sie Kriterien zum Abbrechen von Scans fest, die längere Zeit dauern.
Zum Importieren der Konfigurationsdaten der Cloud-Ressourcen verwenden Governance für Cloud-Konfigurationen-Ressourcensammler und -Konfigurationssammler Flow Designer-Subflows. Manchmal schlägt der Subflow fehl, und der Fehler wird nicht gemeldet. In solchen Fällen kann die Scan-Ausführung unbegrenzt ausgeführt werden. Das Festlegen von Abbruchkriterien hilft beim Abbrechen solcher Scans.

Nächste Maßnahme

Führen Sie die Scan-Konfiguration aus, um die Ressourcenkonfiguration der angegebenen Cloud anhand der angegebenen Richtliniensätze auszuwerten und die Richtlinienverstöße zu identifizieren. Weitere Informationen finden Sie unter Scan-Konfiguration ausführen.

Scan-Konfiguration ausführen

Führen Sie eine Scan-Konfiguration aus, um die Ressourcenkonfiguration der angegebenen Cloud anhand der angegebenen Richtliniensätze auszuwerten und die Richtlinienverstöße zu identifizieren. Die identifizierten Richtlinienverstöße werden von Governance für Cloud-Konfigurationen als Audit-Ergebnisse gemeldet.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Konfigurationen**an.
2. Öffnen Sie die Scan-Konfiguration, die Sie ausführen möchten.
3. Wählen Sie **Ausführen** aus.

Scan-Ausführung

Jede Ausführung einer Scan-Konfiguration wird als Scan-Ausführung bezeichnet. Das Modul „Scan Run“ (Scan-Ausführungen) zeigt eine Liste aller Scan-Ausführungen an.

In Governance für Cloud-Konfigurationen werden die folgenden Informationen für jede Scan-Ausführung in einer zugehörigen Liste angezeigt:

- **Scan-Status**: Auf dieser Registerkarte wird der Datenerfassungsstatus auf Servicekonto-Ebene angezeigt. Öffnen Sie den Scan-Ausführungsdatensatz, um den Konfigurationsdaten-Erfassungsstatus für jedes im Scan abgedeckte Rechenzentrum anzuzeigen. Verwenden Sie den Flow-Ausführungskontext, um Probleme bei der Ausführung der Richtlinie zu beheben.
- **Policy Run Status** (Richtlinienausführungsstatus): Auf dieser Registerkarte werden Informationen zu den während der Scan-Ausführung ausgeführten Richtlinien und der Status ihrer Ausführung angezeigt. Verwenden Sie den Flow-Ausführungskontext, um Probleme bei der Ausführung der Richtlinie zu beheben.
- **Run Resource Assocs** (Ressourcenzuordnungen ausführen): Auf dieser Registerkarte werden Informationen zu den Ressourcen und deren Konfigurationsdaten angezeigt, die während der Scan-Ausführung importiert wurden. Sie können eine beliebige Ressource auswählen, um die folgenden Informationen anzuzeigen:
  - Konfigurationseinstellungen der Ressource
  - Ressourcenattribute
  - Audit-Ergebnisse für die Ressource

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte **Scan Run Logs** (Scanausführungsprotokolle): Hier wird die Ablaufverfolgung der Scan-Ausführung angezeigt.

Zugehörige Informationen

Scan-Konfiguration

Governance für Cloud-Konfigurationen-Richtlinien

Eine Governance für Cloud-Konfigurationen-Richtlinie definiert die nicht konformen Konfigurationen für einen bestimmten Cloud-Ressourcentyp.

Jede Governance für Cloud-Konfigurationen-Richtlinie enthält die folgenden Informationen:

- Die Cloud, in der die Ressource bereitgestellt wird
- Den Cloud-Ressourcentyp
- Definition der nicht konformen Konfiguration. Zum Beispiel unverschlüsselte S3-Buckets von Amazon Web Services (AWS) oder unsichere IAM-Konten (Identity and Access Management)
- Definition des Audit-Verstoßberichts (Richtlinienverstoß)

Hinweis: Beginnend mit Governance für Cloud-Konfigurationen Version 1,3.7, der Inhalt des Basissystems wird in verschoben CCG Inhaltspaket. Installieren Sie CCG Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte.

Von Governance für Cloud-Konfigurationen werden mehrere Basissystemrichtlinien bereitgestellt. Sie können entweder diese Richtlinien verwenden oder benutzerdefinierte Richtlinien gemäß den Anforderungen Ihrer Organisation erstellen. Je nach Bedarf und Vertrautheit mit der ServiceNow AI Platform können Sie eine der folgenden Methoden zum Erstellen der Richtlinie verwenden:

- Richtlinie mit dem Bedingungsgenerator erstellen
- Richtlinie mit dem IntegrationHub-Flow erstellen
- Richtlinie per Skript erstellen

Um die Richtlinie zu verwenden, fügen Sie die Richtlinie einem Richtliniensatz hinzu. Jeder Richtliniensatz kann eine oder mehr Richtlinie(n) enthalten. Weitere Informationen zum Erstellen von Richtliniensätzen finden Sie unter Richtliniensatz erstellen.

Basissystemrichtlinien

Name	Typ	Beschreibung
AWS IAM User Activity policy (AWS IAM-Benutzeraktivitätsrichtlinie)	Condition Builder	Richtlinie zur Überprüfung, ob das Passwort für den AWS IAM-Benutzer aktiviert ist. Um diese Richtlinie zu verwenden, stellen Sie sicher, dass das AWS IAM-Benutzerkonto über die folgenden Berechtigungen verfügt: • Iam:GetCredentialReport • Iam:GenerateCredentialReport
AWS S3 Enforce Bucket encryption (AWS-S3-Bucket-Verschlüsselung erzwingen)	Condition Builder	Richtlinie zur Überprüfung, ob die AWS-S3-Buckets verschlüsselt sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basissystemrichtlinien (Fortsetzung)

Name	Typ	Beschreibung
AWS Sample flow policy (Beispiel für eine AWS-Flow-Richtlinie)	IntegrationHub-Flow	Richtlinie zur Veranschaulichung einer IntegrationHub-Flow-basierten Richtlinie
AWS VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den bereitgestellten EC2-VMs nur die genehmigten Hardwaretypen verwendet werden
AWS VM IPAddress	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der EC2-VM mit dem Datensatz der Configuration Management Database (CMDB) übereinstimmt
AWS VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die EC2-VM aktiviert ist
Azure VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den bereitgestellten Azure-VMs nur die genehmigten Hardwaretypen verwendet werden
Azure VM IP Address (Azure-VM-IP-Adresse)	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der Azure-VM mit dem Datensatz der CMDB übereinstimmt
Azure VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die Azure-VM aktiviert ist

- Weitere Informationen zum Erstellen von Richtliniensätzen finden Sie unter Richtliniensatz erstellen.

- Weitere Informationen zu Richtlinien und Richtliniensätzen des Basissystems finden Sie unter AWS-Richtlinien, Azure-Richtlinien, Und Policy sets (Richtliniensätze).

Richtlinie mit dem Bedingungsgenerator erstellen

Verwenden Sie den Bedingungsgenerator, um eine Governance für Cloud-Konfigurationen-Richtlinie zu erstellen, ohne Code zu schreiben. Verwenden Sie diese Option, um die Kriterien für die Identifizierung und Meldung nicht konformer Cloud-Ressourcenkonfigurationen anzugeben.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Richtlinie“ aus.

   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sehen Sie sich eine der Richtlinien, die auf dem Bedingungsgenerator des Basissystems basieren, als Beispiel für die Erstellung der benutzerdefinierten Richtlinie an.

4. Wählen Sie **Absenden** aus.

Nächste Maßnahme

Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

Richtlinie mit IntegrationHub-Subflow erstellen

Verwenden Sie den IntegrationHub-Subflow, um eine Governance für Cloud-Konfigurationen-Richtlinie zu erstellen. In einem IntegrationHub-Subflow werden grafische Codierungsmechanismen dazu verwendet, die Richtlinienbedingungen anzugeben. Der Subflow bietet eine größere Flexibilität in Audit-Verstoßberichten als der Bedingungsgenerator. Das heißt, Sie können dieselbe Richtlinie verwenden, um verschiedene Arten von Problemen zu melden.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Sehen Sie sich die **Sample flow policy** (Beispiel-Flow-Richtlinie) des Basissystems als Beispiel für das Erstellen neuer Richtlinien mit dem IntegrationHub-Subflow an.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für die Richtlinie.

   a. Kopieren Sie den Subflow **CCG – Flow Policy Template** (CCG – Flow-Richtlinienvorlage).
   Weitere Informationen zum Kopieren des Subflows finden Sie unter IntegrationHub-Subflow-Vorlage kopieren.

   b. Um die Konfigurationsdaten zu lesen, fügen Sie die Aktion **CCG – Read Config Setting** (CCG – Konfigurationseinstellung lesen) hinzu.
   Weitere Informationen zur Aktion **CCG – Read Config Setting** (CCG – Konfigurationseinstellung lesen) finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

   c. Wiederholen Sie Schritt 1.b für alle Konfigurationsschlüssel, die Sie in der Richtlinie verwenden möchten.

   d. Fügen Sie die Flow-Logik hinzu.

   e. Weisen Sie Subflow-Ausgaben zu.
   Die Einstellungen der Subflow-Ausgabe definieren, wie Audit-Verstöße von Governance für Cloud-Konfigurationen gemeldet werden. Weitere Informationen zum Zuweisen der Subflow-Ausgabe finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

   f. **Wahlweise:** Wenn Sie die Option **Vorfall melden** im Formular **Subflow-Ausgaben zuweisen** nicht ausgewählt haben, fügen Sie eine Aktion unter der Aktion **Subflow-Ausgaben zuweisen** hinzu und fügen Sie dann die Aktion **Datensatz erstellen** hinzu.
   Weitere Informationen zur Aktion **Datensatz erstellen** finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

   g. Speichern Sie den Subflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**an.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars „Richtlinie“ aus.
   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.
5. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

Richtlinie per Skript erstellen

Verwenden Sie den nativen Skriptmechanismus der ServiceNow-Plattform, um die Richtlinienbedingung zu definieren. Sie können die Entscheidungsfindung für Skripteinbindungen externalisieren und den Code für verschiedene Richtlinien wiederverwenden.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Prozedur
1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Richtlinie“ aus.

   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.

   Sehen Sie sich eine der auf Skripten des Basissystems basierenden Richtlinien als Beispiel für die Erstellung der benutzerdefinierten Richtlinie an.
4. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

Richtlinie testen

Testen Sie die Governance für Cloud-Konfigurationen-Richtlinie anhand der Konfigurationsdaten, die für eine vorherige Scan-Ausführung importiert wurden. Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert.

Vorbereitungen
- Vergewissern Sie sich, dass eine Scan-Ausführung verfügbar ist, die die Konfigurationsdaten enthält, die Sie über die Richtlinie überprüfen möchten.
- Erforderliche Rolle: sn_itom_ccg.governor

Prozedur
1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinie**an.
2. Öffnen Sie die Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Test Policy** (Richtlinie testen) aus.
4. Wählen Sie die entsprechende Scan-Ausführung aus.
5. Wählen Sie **OK** aus.

Konfigurationsschlüssel erstellen

Erstellen Sie einen Konfigurationsschlüssel in Governance für Cloud-Konfigurationen, um ihn in den Richtlinien zu verwenden. Der Konfigurationsschlüssel gibt den Ressourcensammler und den Konfigurationssammler an, die zum Importieren der Konfigurationsdaten aus der Cloud verwendet werden. Er gibt auch den Datentyp des Konfigurationswerts an.

Vorbereitungen

- Vergewissern Sie sich, dass ein Ressourcensammler für den im Konfigurationsschlüssel genannten Ressourcentyp verfügbar ist. Wenn der Ressourcensammler nicht verfügbar ist, können Sie ihn erstellen. Weitere Informationen finden Sie unter Ressourcensammler erstellen.
- Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Konfigurationsschlüssel**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Konfigurationsschlüssel“ aus.
   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Konfigurationsschlüssel“.
4. Wählen Sie **Absenden** aus.

Ressourcensammler erstellen

Erstellen Sie einen Ressourcensammler, um festzulegen, wie von Governance für Cloud-Konfigurationen alle Ressourcen eines bestimmten Typs importiert werden.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Die Cloud-Ressourcen sind unter einem Servicekonto oder einer Kombination aus Servicekonto und Rechenzentrum verfügbar. Vom Ressourcensammler werden IntegrationHub-Subflows dazu verwendet, die Ressourcenliste aus der Cloud zu importieren. Erstellen Sie nur einen Ressourcensammler pro Ressourcentyp.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für den Konfigurationssammler.

   a. Kopieren Sie den Subflow **CCG – Collector Template** (CCG – Sammlervorlage).
   Weitere Informationen zum Kopieren von Subflow-Vorlagen finden Sie unter Kopieren Sie eine IntegrationHub subflow-Vorlagean.

   b. Fügen Sie die entsprechende Bibliothek von Cloud-Aktionen(CAL)-Aktion und die Flow-Logik hinzu, um die Ressourcendaten zu lesen.

   Weitere Informationen zu verfügbaren CAL-Aktionen finden Sie unter Bibliothek von Cloud-Aktionen-Aktionsreferenz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die CAL nicht über die erforderliche Aktion verfügt, können Sie auf eine vorhandene CAL-Aktion verweisen und die IntegrationHub-Datenstromaktion verwenden, um die benutzerdefinierte Aktion zu implementieren. Alternativ dazu können Sie auch den REST-Schritt verwenden. Weitere Informationen finden Sie unter Datenstromaktionen und Paginierung Und REST-Schritt .

c. Fügen Sie die Aktion **CCG – Insert Resource Record** (CCG – Ressourcendatensatz einfügen) hinzu und wählen Sie dann die entsprechenden Eingaben aus, um die Konfigurationsdaten in die Configuration Management Database (CMDB) einzufügen.
Weitere Informationen zur Aktion **CCG – Insert Resource Record** (CCG – Ressourcendatensatz erstellen) finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

d. Wählen Sie **Veröffentlichen** aus.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Ressourcensammler**an.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars aus.
Eine Beschreibung der Feldwerte finden Sie unter Governance für Cloud-Konfigurationen-Formular „Resource collector“ (Ressourcensammler).
5. Wählen Sie **Absenden** aus.

Nächste Maßnahme

- Wenn die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene nicht verfügbar sind, siehe Konfigurationsschlüssel erstellen.
- Wenn Sie in der Anwendung Governance für Cloud-Konfigurationen einen neuen Ressourcentyp erstellt haben, können Sie optional eine CI-Finder-Zuordnung für den neu angelegten Ressourcentyp erstellen. Weitere Informationen finden Sie unter CI-Finder-Zuordnung erstellen.

Konfigurationssammler erstellen

Erstellen Sie einen Konfigurationssammler, um festzulegen, wie die Konfigurationsdaten von Governance für Cloud-Konfigurationen aus der Cloud importiert werden. Vom Konfigurationssammler werden IntegrationHub-Subflows dazu verwendet, die Konfigurationsdaten aus der Cloud zu importieren.

Vorbereitungen

- Vergewissern Sie sich, dass Governance für Cloud-Konfigurationen geeignete Konfigurationsschlüssel für alle Konfigurationswerte enthält, die Sie aus der Cloud importieren möchten. Erstellen Sie einen Konfigurationsschlüssel, wenn er in der Anwendung nicht verfügbar ist. Weitere Informationen finden Sie unter Konfigurationsschlüssel erstellen.

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Für einige Cloud-Ressourcen sind die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene verfügbar. Erstellen Sie deshalb nur dann einen Konfigurationssammler,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wenn die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene nicht verfügbar sind.

Beispielsweise sind die meisten Konfigurationsdaten des Ressourcentyps **VM-Instanz** auf der Cloud-Ressourcenebene verfügbar. Daher ist kein Konfigurationssammler zum Importieren dieser Konfigurationen implementiert.

Sehen Sie sich einen Basissystem-Konfigurationssammler als Beispiel für das Erstellen der Konfigurationssammler an.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für den Konfigurationssammler.

   a. Kopieren Sie den Subflow **CCG – Collector Template** (CCG – Sammlervorlage).
   Weitere Informationen zum Kopieren von Vorlagen finden Sie unter IntegrationHub-Subflow-Vorlage kopieren.

   b. Fügen Sie die Aktion **CCG – Get Resources** (CCG – Ressourcen abrufen) hinzu und füllen Sie die Felder aus.

   c. Fügen Sie die entsprechende Bibliothek von Cloud-Aktionen(CAL)-Aktion und die Flow-Logik hinzu, um die Konfigurationsdaten zu lesen.

   Hinweis:

   Weitere Informationen zu verfügbaren CAL-Aktionen finden Sie unter Bibliothek von Cloud-Aktionen-Aktionsreferenz.

   Wenn die CAL nicht über die erforderliche Aktion verfügt, können Sie auf eine vorhandene CAL-Aktion verweisen und den IntegrationHub-REST-Schritt verwenden, um die benutzerdefinierte Aktion zu implementieren. Weitere Informationen finden Sie unter REST-Schritt .

   d. Fügen Sie die Aktion **CCG – Insert Configuration Settings** (CCG – Konfigurationseinstellungen einfügen) hinzu, um die Konfigurationsdaten in der Configuration Management Database (CMDB) einzufügen.

   e. Wählen Sie **Veröffentlichen** aus.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Konfigurationssammler**an.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Configuration Collector“ (Konfigurationssammler)

Feld	Beschreibung
Provider-Typ	Cloud, in der die über die Richtlinien zu scannenden Ressourcen gehostet werden
Flow	Konfigurationssammler, von dem die Konfigurationsdaten aus der Cloud importiert werden können
Ressourcentyp	Cloud-Ressourcentyp, dessen Konfiguration Sie importieren möchten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Konfigurationssammlers
Beschreibung	Kurzbeschreibung des Konfigurationssammlers

5. Wählen Sie **Absenden** aus.

CI-Finder-Zuordnung erstellen

Verwenden Sie die CI-Suchzuordnung, um die von abgerufenen Ressourcen zu verknüpfen ServiceNow Governance für Cloud-Konfigurationen Scan-Ausführungen mit dem entsprechenden Configuration Management Database (CMDB) Konfigurationselemente (Configuration Items, CIs), falls verfügbar. Nachdem Sie die Zuordnung erstellt haben, können Sie die gemeldeten Konfigurationsverstöße den CIs zuordnen, zu denen sie gehören.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.scheduling_admin oder sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie einen Ressourcentyp in Governance für Cloud-Konfigurationen erstellt haben, können Sie optional eine CI-Finder-Zuordnung für den neuen Ressourcentyp erstellen. Von Cloud Configuration Governance wird das CI-Finder-Zuordnungsskript für alle von den Scan-Ausführungen abgerufenen Ressourcen aufgerufen.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Zuordnungen des CI-Finders**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zuordnungen des CI-Finders“

Feld	Beschreibung
Provider-Typ	Cloud-Service Provider, der die Ressource hostet.
Ressourcentyp	Ressourcentyp der Cloud-Ressource.
Skript	Skript, über das die von der Anwendung Governance für Cloud-Konfigurationen abgerufenen Ressourcen mit dem vorhandenen CI verknüpft werden. Verwenden Sie ein vorhandenes CI-Finder-Zuordnungsskript als Beispiel, um ein Skript für den neuen Ressourcentyp zu erstellen. Governance für Cloud-Konfigurationen bietet mehrere Objekte und Variablen zur Verwendung im Skript. Weitere Informationen finden Sie unter Governance für Cloud-Konfigurationen-Skriptreferenz.

Richtliniensatz erstellen

Erstellen Sie einen Richtliniensatz in Governance für Cloud-Konfigurationen, um Richtlinien zu gruppieren, die einen bestimmten Sicherheits- oder Organisationsstandard durchsetzen. Wenn der Richtliniensatz von der Scan-Konfiguration ausgeführt wird, werden die Cloud-Ressourcen identifiziert, die nicht den festgelegten Standards entsprechen. Ein Richtliniensatz kann eine oder mehrere Richtlinie(n) enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtliniensätze**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Policy Sets“ (Richtliniensätze)

Feld	Beschreibung
Name	Name des Richtliniensatzes
Provider-Typ	Cloud, in der die Ressourcen gehostet werden, die über die dem Richtliniensatz angehängten Richtlinien zu scannen sind
Beschreibung	Kurzbeschreibung des Richtliniensatzes
Richtlinien	Richtlinien, die Sie gruppieren möchten, um einen bestimmten Sicherheits- oder Organisationsstandard durchzusetzen. Der Richtliniensatz kann mehr als eine Richtlinie enthalten.

4. Wählen Sie **Absenden** aus.

IntegrationHub-Subflow-Vorlage kopieren

Kopieren Sie eine IntegrationHub-Subflow-Vorlage, um Subflows für die Anwendung Governance für Cloud-Konfigurationen zu erstellen.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Prozessautomatisierung** > **Flow Designer**an.
2. Wählen Sie **Subflow** aus.
3. Suchen Sie in der Spalte „Name“ nach der erforderlichen Subflow-Vorlage und öffnen Sie sie.
4. Wählen Sie das Symbol weitere Aktionen ( ) Symbol, und wählen Sie dann aus **Subflow kopieren** Aus dem Menü.
5. Geben Sie im Feld **Neuer Subflow-Name** einen eindeutigen und beschreibenden Namen für den kopierten Subflow ein.
6. Wählen Sie **Kopieren**.
   Der neue Subflow wird erstellt und als Registerkarte im Subflow-Designer geöffnet.

Fehlerkorrektur

Verwenden Sie die Korrekturaktionen in Governance für Cloud-Konfigurationen, um damit die nicht konformen Cloud-Ressourcenkonfiguration zu beheben, die während der Scan-Ausführungen identifiziert wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Modul „Remediationen“ zeigt eine Liste aller verfügbaren Korrekturaktionen für den Satz von Verstoßtypen (Verstoßdefinitionen) an. Governance für Cloud-Konfigurationen bietet mehrere Basissystem-Korrekturaktionen. Wenn die Anwendung die erforderliche Korrekturaktion nicht enthält, können Sie benutzerdefinierte Aktionen erstellen. Weitere Informationen finden Sie unter Korrekturkatalogelement erstellen Und Korrekturaktion erstellen.

Da die Korrekturaktionen für die Cloud-Ressourcen von Governance für Cloud-Konfigurationen durchgeführt werden, können Sie optional zusätzliche Genehmigungsanforderungen für die Aktion erzwingen. Immer, wenn der sn_itom_ccg.ccg_operator eine Nachbesserungsanforderung sendet, die eine Genehmigung erfordert, wird von der Anwendung eine Change-Anforderung zum Nachverfolgen der Genehmigung erstellt. Sie können die Liste aller Change-Anforderungen im Modul für Nachbesserungsanforderungen überprüfen.

Hinweis: Beginnend mit Governance für Cloud-Konfigurationen Version 1,3.7, der Inhalt des Basissystems wird in verschoben CCG Inhaltspaket. Installieren Sie CCG Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte.

Korrekturkatalogelement erstellen

Erstellen Sie in ein anwenderdefiniertes Korrekturkatalogelement Governance für Cloud-Konfigurationen Für die Korrekturen, die zusätzliche Eingabeparameter zur Ausführung erfordern.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird
Einige Korrekturaktionen erfordern zusätzliche Betriebsinformationen, z. B. den Hardwaretyp der Ressource, damit sie ausgeführt werden können. Erstellen Sie für solche Fälle ein Korrekturkatalogelement mit benutzerdefinierten Eingabeparametern oder -variablen, und ordnen Sie es der entsprechenden Korrekturaktion und dem Verstoßtyp zu. Nachdem Sie das Korrekturkatalogelement erstellt haben, kann ein Anwender mit der Rolle „sn_itom_ccg.ccg_Operator“ es verwenden, um eine Korrekturanforderung zu stellen.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Nachbesserungskatalog**an.
2. Öffnen Sie den Datensatz „CCG-Fehlerkorrektur – Standardkatalog“.
3. Wählen Sie **Kopieren**, um das Katalogelement zu kopieren.
4. Füllen Sie die Felder des Formulars aus.

Datensatzerstellerformular

Feld	Beschreibung
Name	Name des Governance für Cloud-Konfigurationen-Katalogelements.
Tabellenname	Die Tabelle, in der der Datensatzersteller Datensätze erstellt. Behalten Sie den Standardwert bei.
Besitzer	Besitzer des Katalogelements, der Bearbeitungszugriff darauf hat.
Kurzbeschreibung	Geschäftszweck des Korrekturkatalogelements.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	In Governance für Cloud-Konfigurationen wird dem Benutzer die Kurzbeschreibung angezeigt.
Aktivieren	Status des Katalogelements. Das kopierte Katalogelement ist standardmäßig aktiv.

5. Wählen Sie **Aktualisieren**.
   Der Datensatzersteller erstellt die folgenden Elemente:
   - Eine Flow Designer-Aktion mit dem Namen <Catalog item name>_Action.
   - Einen Flow Designer-Subflow mit dem Namen <Catalog item name>_Subflow.
   - Einen Nachbesserungsdatensatz für das Katalogelement. Der Nachbesserungsdatensatz ist dem Katalogelement und dem <Catalog item name>_Subflow zugeordnet.
6. **Wahlweise:** Definieren Sie Katalogelementvariablen, um zusätzliche Informationen durch das Katalogelementformular zu erfassen.
   a. Wählen Sie in der zugehörigen Liste Variablen die Option aus **Neu** .
   b. Füllen Sie im Formular die Felder aus.
   Weitere Informationen zu Katalogvariablen finden Sie unter Servicekatalog-Variablen .
   c. Speichern Sie das Formular.
7. Ordnen Sie das Korrekturkatalogelement dem Verstoßtyp zu.
   a. Wählen Sie in der zugehörigen Liste „Remediationen“ die Option **Neu** aus.
   b. Doppelklicken Sie auf die Zelle „Violation (Verstoß)“.
   c. Wählen Sie den Verstoßtyp aus.
   d. Wählen Sie das Speichersymbol ( ).
8. Aktualisieren Sie die <Catalog item name>_Action zur Interaktion mit der Cloud-Ressource.
   Von Governance für Cloud-Konfigurationen wird eine IntegrationHub-Aktion dazu verwendet, die Korrektur für die Cloud-Ressource auszuführen. Da geschäftliche Anforderungen die Korrekturlogik vorgeben, wird vom Datensatzersteller nur ein Standardbaustein für die <Catalog item name>_Action erstellt. Sie müssen die <Catalog item name>_Action gemäß den Geschäftsanforderungen implementieren.
   a. Navigieren zu **Alle** > **Flow Designer**an.
   b. Wählen Sie die Registerkarte **Aktionen** aus.
   c. Öffnen Sie die <Catalog item name>_Action.
   d. Lesen Sie in der Dokumentation des Cloud-Anbieters nach, und implementieren Sie die <Catalog item name>_Action gemäß den Geschäftsanforderungen Ihrer Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für weitere Informationen zum Gebäude IntegrationHub Aktionen, siehe Anwenderdefinierte Aktionen werden erstellt .

e. Speichern Sie die aktualisierte <Catalog item name>_Action.

f. Testen Sie die <Catalog item name>_Action.
Weitere Informationen finden Sie unter Testen Sie eine Aktion .

g. Veröffentlichen Sie die <Catalog item name>_Action.

9. Verknüpfen Sie die <Catalog item name>_Action mit dem <Catalog item name>_Subflow.
Von Governance für Cloud-Konfigurationen werden die IntegrationHub-Subflows dazu verwendet, die IntegrationHub-Aktion auszulösen und die zurückgegebenen Daten zu verarbeiten.

a. Navigieren Sie zu Flow Designer Homepage durch Auswahl des Flow Designer-Startsymbols ( ).

b. Wählen Sie die Registerkarte **Subflows** aus.

c. Öffnen Sie den <Catalog item name>_Subflow.

d. Wählen Sie **Aktion, Flow-Logik oder Subflow hinzufügen** aus.

e. Wählen Sie **Aktion** aus.

f. Suchen Sie nach <Catalog item name>_Action, und wählen Sie die Aktion aus.

g. Fügen Sie die entsprechende Flow-Logik hinzu.

h. Weisen Sie die Ausgabe des Subflows der Ausgabevariablen zu.

i. Testen Sie den <Catalog item name>_Subflow.

j. Veröffentlichen Sie den <Catalog item name>_Subflow, um ihn zu aktivieren.

Nächste Maßnahme
Führen Sie die Korrekturaktion aus, um den erkannten Verstoß zu beheben. Weitere Informationen finden Sie unter Korrektur ausführen.

Korrekturaktion erstellen

Erstellen Sie in Governance für Cloud-Konfigurationen eine Korrekturaktion für die Fehlerkorrekturen, für die keine zusätzlichen Eingabeparameter erforderlich sind.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.ccg_governer

Warum und wann dieser Vorgang ausgeführt wird
Von Governance für Cloud-Konfigurationen werden IntegrationHub-Subflows dazu verwendet, Fehlerkorrekturen durchzuführen.

Prozedur
1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Korrekturen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Remediationen“

Feld	Beschreibung
Minimum permission required (Erforderliche Mindestberechtigung)	Zum Ausführen der Fehlerkorrektur mindestens erforderliche Cloud-Berechtigungen. Von Governance für Cloud-Konfigurationen werden die Berechtigungsinformationen aus diesem Feld nicht gelesen. Verwenden Sie dieses Feld, um die Berechtigungsinformationen als zukünftige Referenz zu speichern.
Aktion	Korrektur-Flow, mit dem der ausgewählte Verstoß behoben werden kann
Violation (Verstoß)	Verstoß, den Sie beheben möchten
Genehmigung erforderlich	Option zum Erzwingen der Genehmigung für die Korrekturaktion. Weitere Informationen zu Genehmigungen finden Sie unter Genehmigungen .
Beschreibung	Kurze Beschreibung der Korrekturaktion
Korrekturkatalogelement	Name des Korrekturkatalogelements, das zum Auslösen einer Nachbesserungsanforderung verwendet werden kann. Wählen Sie den CCG-Fehlerkorrektur – Standardkatalog aus.

4. Wählen Sie **Absenden** aus.

Nächste Maßnahme

Führen Sie die Korrekturaktion aus, um den erkannten Verstoß zu beheben. Weitere Informationen finden Sie unter Korrektur ausführen.

Korrektur ausführen

Führen Sie die entsprechende Korrekturaktion aus, um die nicht konforme Cloud-Konfiguration zu beheben, die während der Scan-Ausführung von Governance für Cloud-Konfigurationen identifiziert wurde.

Vorbereitungen

- Die Scan-Ausführung ist abgeschlossen.
- Erforderliche Rolle: sn_itom_ccg.ccg_operator

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Ausführung**an.
2. Öffnen Sie die Scan-Ausführung, in der von **Cloud Configuration Governance** die Audit-Probleme gemeldet wurden.
3. Wählen Sie **Audit-Ergebnisse anzeigen** aus.
4. Wählen Sie den Verstoßtyp aus, den Sie beheben möchten.
   Von Governance für Cloud-Konfigurationen werden die Verstöße nach dem Verstoßtyp gruppiert. Während der Ausführung einer Fehlerkorrektur können Sie nur Verstöße desselben Typs beheben.
5. Wählen Sie mindestens einen Verstoß aus.
6. Wählen Sie **Beheben** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können **Vorerst ignorieren** auswählen, um das Problem zu ignorieren. Wenn Sie ein Problem ignorieren, wird das Problem von Governance für Cloud-Konfigurationen nicht als Verstoß gemeldet und nicht in den Dashboard-Berichten dargestellt.

7. Überprüfen Sie die Liste der für die Fehlerkorrektur ausgewählten Ressourcen.
8. Wählen Sie die Korrekturaktion aus.
9. Wählen Sie **OK** aus.

Ergebnis

Nächste Maßnahme

Wählen Sie in der zugehörigen Liste „Ausführungen der Fehlerkorrektur“ die Change-Anforderung aus, und überprüfen Sie den Status der Fehlerkorrektur. Sie können auch die Liste aller Nachbesserungsanforderungen im Modul für Nachbesserungsanforderungen anzeigen.

Governance für Cloud-Konfigurationen-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Governance für Cloud-Konfigurationen.

Governance für Cloud-Konfigurationen-Dashboard

Governance für Cloud-Konfigurationen ist ein Tool zum Verwalten der Konfiguration der Cloud-Ressourcen gemäß Ihren Organisationsstandards und etablierten Sicherheitsstandards. Verwenden Sie das Dashboard, um die Integritätspunktzahl der Cloud, Statistiken zu Richtlinienverstößen, Trends bei Richtlinienverstößen, Fehlerkorrekturen und mehr zu überprüfen.

Governance für Cloud-Konfigurationen-Dashboard

Erforderliche ServiceNow AI Platform-Rollen

zum Anzeigen des Dashboards und seiner Widgets ist die Rolle sn_itom_ccg.ccg_operator oder sn_itom_ccg.report_viewer erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf das Dashboard von Governance für Cloud-Konfigurationen

Um das Dashboard zu öffnen, wechseln Sie zu: **Governance für Cloud-Konfigurationen** > **Dashboard**an.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_itom_ccg.ccg_operator oder sn_itom_ccg.report_viewer	• Cloud-Integritätspunktzahl überprüfen • Zur Korrektur der identifizierten Richtlinienverstöße eingesetzte Zeit • Den Trend des Richtlinienverstoßes nachvollziehen

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Cloud health score (Cloud-Integritätspunktzahl)	Tachodiagramm	sn_itom_ccg_scan_summary	Prozentsatz der gescannten Cloud-Ressourcen, für die kein Audit-Problem vorliegt
Violating resources (Verstoßende Ressourcen)	Gestapeltes Balkendiagramm	sn_itom_ccg_scan_summary	Schweregrad der erkannten Audit-Probleme pro Cloud-Ressourcentyp
Violations count (Verstoßanzahl)	Ringdiagramm	sn_itom_ccg_violation_stats	Verstoß pro Schweregrad des Audit-Problems
Scanned resources (Gescannte Ressourcen)	Ringdiagramm	sn_itom_ccg_scan_summary	Anzahl der pro Cloud-Ressourcentyp gescannten Cloud-Ressourcen. Verwenden Sie die **CCG-Drilldown-Filter**, um die Daten zu filtern und die gewünschten Daten zu visualisieren.
Probleme	Horizontales Balkendiagramm	sn_itom_ccg_audit_stats	Anzahl der pro Verstoßdefinition gemeldeten Verstöße. Im Diagramm können maximal 10 Balken angezeigt werden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			d. h. einer pro Verstoßdefinitionstyp. Wenn die Daten mehr als 10 Verstoßdefinitionstypen enthalten, werden alle zusätzlichen Verstoßdefinitionstypen im Balken **Sonstige** zusammengeführt. Verwenden Sie die **CCG-Drilldown-Filter**, um die Daten zu filtern und die gewünschten Daten zu visualisieren.
Richtlinien-Compliance	Eingebettete Listen	sn_itom_ccg_policy_compliance_stats	Zeigt die folgenden Informationen für die angegebene Richtlinie an: • Anzahl der konformen Ressourcen • Anzahl der nicht konformen Ressourcen
Policy set compliance (Richtliniensatz-Compliance)	Eingebettete Listen	sn_itom_ccg_policy_set_compliance_stats	Zeigt die folgenden Informationen für den angegebenen Richtliniensatz an: • Anzahl der konformen Ressourcen • Anzahl der nicht konformen Ressourcen
Total issues remediated (Gesamtzahl der korrigierten Probleme)	Halbes Ringdiagramm	sn_itom_ccg_remediation_daily_trend	Anzahl der durchgeführten Korrekturen nach Verstoßdefinitionstyp
Remediations by type (Fehlerkorrekturen nach Typ)	Kreisdiagramm	sn_itom_ccg_remediation_daily_trend	Anzahl der durchgeführten Korrekturen pro Cloud-Ressourcentyp
Remediated on (Korrigiert in)	Halbes Ringdiagramm	sn_itom_ccg_remediation_daily_trend	Zeit, die zum Korrigieren der Verstöße benötigt wurde
Trend	Liniendiagramm	sn_itom_ccg_daily_trend	Trend der Meldung von Verstößen im Zeitverlauf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter

Name	Typ	Beschreibung
CCG-Drilldown-Filter	Auswahlbasierter Filter	Verwenden Sie diesen Filter, um den Cloud Provider, das Cloud-Konto und die Regionen für die Visualisierung der gescannten Ressourcen und Problemdaten auszuwählen.

Governance für Cloud-Konfigurationen-Rollen und -Systemeigenschaften

Benutzer von Governance für Cloud-Konfigurationen benötigen die entsprechenden Rollen und Systemeigenschaften, um verschiedene Aktivitäten auszuführen. Diese Rollen und Systemeigenschaften werden mit der Aktivierung der Anwendung installiert.

Nur Benutzer mit der Rolle user_admin oder admin können Benutzer mit diesen Rollen erstellen:

Governance für Cloud-Konfigurationen-Rollen

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
sn_itom_ccg.scheduling_admin	Ein Planungsadministrator kann die folgenden Aktionen ausführen: • Scan-Zeitpläne erstellen. • CI-Finder-Zuordnungen erstellen.	discovery_admin
sn_itom_ccg.governor	Ein Benutzer mit der Rolle „Kontrolle“ kann die folgenden Aktionen ausführen: • Richtlinien über Bedingungsgenerator, IntegrationHub-Flows oder Skript erstellen • Erstellen Sie einen Richtliniensatz. • Ressourcensammler erstellen • Konfigurationsschlüssel erstellen • Fehlerkorrektur erstellen • CI-Finder-Zuordnungen erstellen.	• flow_designer • action_designer • catalog_admin
sn_itom_ccg.ccg_operator	Ein Operator kann die folgenden Aktionen ausführen: • Audit-Problemberichte anzeigen • Korrektur ausführen • Scan-Konfigurationen ausführen • Dashboard anzeigen	• flow_operator • sn_change_write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen-Rollen (Fortsetzung)

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
sn_itom_ccg.report_viewer	Ein Berichtbetrachter kann folgende Aktionen ausführen: • Audit-Problemberichte anzeigen • Dashboard anzeigen	

Governance für Cloud-Konfigurationen-Systemeigenschaften

Name der Eigenschaft	Beschreibung
snc_af.log_level	Wenn Sie diese Eigenschaft aktivieren, werden die Protokolle von Governance für Cloud-Konfigurationen in das Syslog geschrieben. Die folgenden Protokollebenen werden unterstützt: • DEBUG • INFO • WARN • ERROR • AUS Vergewissern Sie sich, dass der Anwendungsbereich **Global** ist, wenn Sie diese Eigenschaft festlegen oder löschen.

Zugehörige Informationen

Einem Benutzer eine Rolle zuweisen

Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans

Im Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans werden detaillierte Informationen zur Scan-Konfiguration angezeigt.

Feld	Beschreibung
Name	Name, der die Scan-Konfiguration eindeutig identifiziert
Beschreibung	Kurze Beschreibung der Scan-Konfiguration.

Konfigurationsregisterkarte

Legen Sie die Konfigurationseinstellungen fest, z. B. Cloud Provider, Richtliniensätze, Zielservicekonten und Rechenzentren für den Scan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Cloud provider type (Typ des Cloud Providers)	Cloud, die die zu scannenden Ressourcen hostet.
Policy sets (Richtliniensätze)	Richtliniensätze für den Scan. Wählen Sie mindestens einen Richtliniensatz für den Scan aus und speichern Sie das Formular.
Rechenzentrumsfilter	Servicekonto oder Kombination aus Servicekonto und Rechenzentrum für den Scan. **1.** Doppelklicken Sie in der leeren Zeile der Liste „Rechenzentrumsfilter“ auf die Zelle des Servicekontos und wählen Sie dann ein Servicekonto aus. Sie können ein Verwaltungskonto für Amazon Web Services (AWS) auswählen und dann der Scan-Konfiguration alle zugehörigen Mitgliedskonten hinzufügen, sofern die folgenden Bedingungen erfüllt sind: ○ Für das Verwaltungskonto ist eine Konfiguration für die Übernahme von Rollen vorhanden. ○ Von Cloud-Discovery wurde die Rechenzentrumserkennung für die Mitgliedskonten abgeschlossen. Weitere Informationen zum Erstellen von Konfigurationen für die Übernahme von Rollen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren. **2.** Speichern Sie das Formular. **3.** Doppelklicken Sie in der leeren Zeile der Liste „Rechenzentrumsfilter“ auf die Zelle des Rechenzentrums und wählen Sie dann ein Rechenzentrum aus. (Optional) Wenn Sie kein Rechenzentrum auswählen, werden von Governance für Cloud-Konfigurationen alle Rechenzentren gescannt, die dem Servicekonto zugeordnet sind.

Registerkarte „Filter“

(Optional) Geben Sie Kriterien zum Filtern der Cloud-Ressourcen an und importieren Sie dann ihre Konfigurationsdaten aus der Cloud. Wenn angegeben, werden von Governance für Cloud-Konfigurationen ausschließlich die Konfigurationen der Ressourcen abgerufen, die den Filterkriterien entsprechen. Andernfalls werden die Konfigurationen aller Cloud-Ressourcen abgerufen.

Feld	Beschreibung
Tag-Filter	Cloud-Ressourcen-Tags zum Filtern der Cloud-Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Geben Sie den Tag-Namen in das Feld **Name** ein. • Geben Sie den Tag-Wert in das Feld **Wert** ein.
Freihandform	Option zur Angabe einer kommagetrennten Liste von Cloud-Bezeichnern zum Filtern der Cloud-Ressourcen
Ressourcen	Kommagetrennte Liste der Cloud-Bezeichner. Dieses Feld wird nur angezeigt, wenn die Option **Freihandform** ausgewählt ist.

Governance für Cloud-Konfigurationen-Formular „Richtlinie“

Im Governance für Cloud-Konfigurationen-Formular „Richtlinie“ werden detaillierte Informationen zur Richtlinie angezeigt, z. B. Cloud Provider, Ressourcentyp, Richtlinientyp und Einstellungen für die Meldung von Richtlinienverstößen.

Feld	Beschreibung
Richtlinienname	Name, der die Richtlinie eindeutig identifiziert
Beschreibung	Kurzbeschreibung der Richtlinie

Ressourcentyp

Definieren Sie den Ressourcentyp, für den Sie die Richtlinie erstellen möchten.

Feld	Beschreibung
Cloud Provider	Cloud, die die zu scannenden Ressourcen hostet.
Ressourcentyp	Cloud-Ressourcentyp, der über die Richtlinie gescannt werden soll. Wenn der erforderliche Ressourcentyp nicht verfügbar ist, können Sie einen Ressourcentyp erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Ressourcensammler .

Richtlinienbedingung

Definieren Sie den Richtlinientyp und die nicht konforme Ressourcenkonfiguration.

Feld	Beschreibung
Typ	Governance für Cloud-Konfigurationen unterstützt die folgenden Typen: • **Bedingungsgenerator**: Die Methode ohne Code zum Erstellen von Richtlinien. • **IntegrationHub-Flow**: Die Methode mit wenig Code zum Erstellen von Richtlinien. • **Skript**: Die code-basierte Methode zum Erstellen von Richtlinien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie das Symbol zum Anzeigen verfügbarer Schlüssel ( ) aus, um die Liste aller verfügbaren Konfigurationsschlüssel für den ausgewählten Ressourcentyp anzuzeigen. Sie können einen beliebigen Schlüssel in der Richtlinie verwenden.

Bedingung	Bedingungen für die Meldung der nicht konformen Cloud-Ressourcenkonfiguration. Geben Sie immer den Schlüssel und den Wert als Paar an. Verwenden Sie die Operatoren **ODER** und **UND**, um logische Operationen in der Richtlinienbedingung auszuführen.
	Syntax
	`Key is <key_name>`
	`<data_type> Value <condition> <value>`
	Beispiel:
	`Key is AWS:IAM:User:PasswordEnabled`
	`Boolean Value is true`
	Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Bedingungsgenerator** ausgewählt wird.

Konfigurationsschlüssel	Konfigurationsschlüssel für die Richtlinie. Dieses Feld wird nur angezeigt, wenn für das Feld **Typ** die Option **IntegrationHub Flow** ausgewählt wird.
Integration flow (Integrations-Flow)	Der entsprechende IntegrationHub-Flow. Dieses Feld wird nur angezeigt, wenn für das Feld **Typ** die Option **IntegrationHub Flow** ausgewählt wird.
Bedingungsskript	Skript, mit dem die Richtlinienbedingungen zum Identifizieren und melden von Richtlinienverstößen implementiert werden. Governance für Cloud-Konfigurationen enthält mehrere skriptfähige Objekte und Variablen zur Verwendung in den Richtlinienskripts. Weitere Informationen finden Sie unter Skriptreferenz. Sie können Skripteinbindungen erstellen, um die Entscheidungsfindung zu externalisieren und den Code für verschiedene Skripts wiederverwenden. Weitere Informationen zum Erstellen der Skripteinbindungen finden Sie unter Skripteinbindungen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie einen benutzerdefinierten Audit-Ergebnisdatensatz über das Skript erstellen, wird die in der Richtlinie definierte Konfiguration für **Audit Violation Reporting** (Audit-Verstoßberichte) nicht wirksam. Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Skript** ausgewählt wird.

Audit-Verstoßberichte

Definieren Sie, der Richtlinienverstoß von Governance für Cloud-Konfigurationen gemeldet wird.

Feld	Beschreibung
Report violation as (Verstoß melden als)	Verstoßdefinition, die in den Audit-Verstoßbericht aufgenommen werden soll. Von Governance für Cloud-Konfigurationen wird die Verstoßdefinition dazu verwendet, die Nichteinhaltung von Richtlinien zu melden. Wenn keine geeignete Verstoßdefinition verfügbar ist, können Sie wie folgt eine erstellen: **1.** Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) aus. **2.** Wählen Sie **Neu**. **3.** Geben Sie einen Namen ein, der die Verstoßdefinition eindeutig identifiziert. Von Governance für Cloud-Konfigurationen wird der Name der Verstoßdefinition in den Audit-Problembericht aufgenommen. **4.** Wählen Sie den Standardschweregrad für die Verstoßdefinition aus. **5.** (Optional) Geben Sie eine kurze Beschreibung des Verstoßes ein.
Schweregrad	Schweregrad des Verstoßes. Wenn Sie den Schweregrad in der Richtlinie nicht auswählen, verwendet Governance für Cloud-Konfigurationen den in der Verstoßdefinition definierten Standardschweregrad.

Governance für Cloud-Konfigurationen-Formular „Konfigurationsschlüssel“

Das Formular „Konfigurationsschlüssel“ enthält detaillierte Informationen zum Konfigurationsschlüssel.

Formular „Konfigurationsschlüssel“

Name	Beschreibung
Name	Name, der den Konfigurationsschlüssel eindeutig identifiziert.
Beschreibung	Kurze Beschreibung des Konfigurationsschlüssels.
Provider-Typ	Cloud, in der die über die Richtlinien zu scannenden Ressourcen gehostet werden
Ressourcentyp	Cloud-Ressourcentyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfigurationsschlüssel“ (Fortsetzung)

Name	Beschreibung
Werttyp	Datentyp des Konfigurationswerts, der dem Konfigurationsschlüssel zugeordnet ist.
Resource collector (Ressourcensammler)	Ressourcensammler, der die Konfigurationsdaten für den ausgewählten Ressourcentyp erfassen kann.
Configuration collector (Konfigurationssammler)	(Optional) Konfigurationssammler, von dem die Konfigurationsschlüssel importiert werden können. Wenn die erforderlichen Konfigurationsdaten nicht auf Cloud-Ressourcenebene verfügbar sind, wählen Sie den Konfigurationssammler aus, von dem die Konfigurationsschlüssel importiert werden können. Wenn kein geeigneter Konfigurationssammler verfügbar ist, erstellen Sie einen Konfigurationssammler und wählen Sie ihn aus. Weitere Informationen zum Erstellen des Konfigurationssammlers finden Sie unter Konfigurationssammler erstellen.

Governance für Cloud-Konfigurationen-Formular „Resource collector“ (Ressourcensammler)

Das Formular „Ressourcensammler“ (Ressourcensammler) enthält detaillierte Informationen zum Ressourcensammler.

Formular „Resource collector“ (Ressourcensammler)

Feld	Beschreibung
Name	Name, der den Konfigurationsschlüssel eindeutig identifiziert.
Scan mode (Scan-Modus)	Ebene, auf der die Ressource vom Ressourcensammler aus der Cloud importiert wird. Folgende Werte werden unterstützt: • **Run per LDC** (Ausführung pro LRZ): Importieren Sie die Ressource auf Rechenzentrumsebene. Das heißt, einmal aus jedem Rechenzentrum. • **Run per service account** (Ausführung pro Servicekonto): Importieren Sie die Ressource auf Servicekontoebene.
Provider-Typ	Cloud, in der die zu importierenden Ressourcen gehostet werden
Ressourcentyp	Cloud-Ressourcentyp, den Sie über den Ressourcensammler importieren möchten. Wenn Governance für Cloud-Konfigurationen nicht den erforderlichen Ressourcentyp enthält, können Sie ihn wie folgt erstellen: **1.** Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) aus. **2.** Wählen Sie **Neu**. **3.** Geben Sie im Feld **Name** den Cloud-Ressourcentyp ein. **4.** Wählen Sie **Absenden** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Resource collector“ (Ressourcensammler) (Fortsetzung)

Feld	Beschreibung
Flow	Ressourcensammler-Flow, mit dem der angegebene Ressourcentyp importiert werden kann

Governance für Cloud-Konfigurationen Formular „Konfiguration der Rollenübernahme für Service-Account“

Die Governance für Cloud-Konfigurationen Das Formular „Konfiguration der Serviceaccount-Rolle übernehmen“ zeigt detaillierte Informationen zur Konfiguration der Rollenübernahme an, die für den Zugriff auf den vertrauenden Account verwendet wird.

Formular „Konfiguration der Rollenübernahme für Service-Account“

Feld	Beschreibung
Name der Zugriffsrolle	Name der IAM-Rolle (Identity and Access Management), die für den vertrauenswürdigen Account erstellt wurde und dem vertrauenswürdigen Account (Zugriffsberechtigter) den Zugriff auf den vertrauenswürdigen Account ermöglicht. Um die Mitgliedskonten mithilfe des Verwaltungskontos zu scannen, geben Sie in dieses Feld OrganizationAccountAccessRole ein. Wenn Sie die OrganizationAccountAccessRole nicht für den Zugriff auf den Mitgliedsaccount verwenden möchten, geben Sie den Namen der IAM-Rolle ein, die für den Mitgliedsaccount erstellt wurde. Um das vertrauende Konto durch Verwendung des vertrauenswürdigen Kontos zu scannen, geben Sie den Namen der IAM-Rolle ein, die für das vertrauende Konto erstellt wurde.
Service-Account	Name des Service-Accounts, in dem die Übernahmerolle vorhanden ist.
Name der Rollensitzung	Ein Bezeichner für die Sitzung mit übernommener Rolle. Ändern Sie den Standardwert nicht.
Anmeldeinformationsalias	Optional: Anmeldeinformationsalias für AWS Anmeldeinformationen.

Governance für Cloud-Konfigurationen-Skriptreferenz

Von Governance für Cloud-Konfigurationen werden mehrere Objekte und Variablen bereitgestellt, mit denen Sie skriptbasierte Richtlinien und CI-Finder-Zuordnungsskripts erstellen können.

Skriptingreferenz für die Governance für Cloud-Konfigurationen-Richtlinien

Governance für Cloud-Konfigurationen-Objekte

Name	Beschreibung	Schema
configSettings	Stellt die aus der Cloud importierten Konfigurationsdaten dar.	[{ "config_key":"configuration_key", "type":"data_type",

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen-Objekte (Fortsetzung)

Name	Beschreibung	Schema

		<pre>"value":"configuration_value"
		},
		...
		]</pre>

current	Stellt das aktuelle Glide-Datensatzobjekt für den ausgewählten Ressourcentyp dar.	Es enthält die folgenden Felder: • Name: Name der Ressource • Typ: Ressourcentyp • Bezeichner: Eindeutiger Bezeichner der Cloud-Ressource • Details: cloudressourcenspezifische Details

resourceInformation	Ressourcendatensatz und seine Attribute.	<pre>[
		{
		"attribute": "Attribute name",
		"tableName" : "Referenced table",
		"documentId": "Referenced record",
		},
		...
		]</pre>

auditResult	Audit-Details, die in die Configuration Management Database (CMDB) geschrieben werden müssen.	<pre>{
		"details": "Violation definition "'
		"severity": "severity of the violation",
		"auditViolationName": "Violation name"
		};</pre>

Governance für Cloud-Konfigurationen-Variablen

Name	Datentyp	Beschreibung
answer	Boolescher Wert	Mit dieser Variablen wird angegeben, ob gemäß der Richtlinie der Verstoß gemeldet wird oder nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen-Variablen (Fortsetzung)

Name	Datentyp	Beschreibung
		• true: Verstoß melden. Erstellen Sie das Objekt auditResult, um einen benutzerdefinierten Audit-Ergebnisdatensatz in der CMDB zu erstellen. Wenn Sie kein Audit-Ergebnisobjekt erstellen, wird der Verstoß gemäß der in der Richtlinie angegebenen Verstoßdefinition von Governance für Cloud-Konfigurationen gemeldet. • false: Verstoß nicht melden.

violatingConfigSettings	JSON	Grund des Richtlinienverstoßes.
		Syntax
		{
		"config_key": "value"
		};

Skriptingreferenz für das CI-Finder-Zuordnungsskript

Governance für Cloud-Konfigurationen-Objekte

Name	Beschreibung	Schema

attributes	Eine Zuordnung, die den Ressourcenattributschlüssel und den Attributwert aus der Ressourcenattributtabelle für die angegebene Ressource enthält.	{
		"LogicalDatacenter":
		"Referenced record",
		"ServiceAccount":
		"Referenced record"
		}

Governance für Cloud-Konfigurationen-Variablen

Name	Datentyp	Beschreibung
Name	Zeichenfolge	Name der Ressource
Kennung	Ressourcendatensatz	Bezeichner des Governance für Cloud-Konfigurationen-Ressourcendatensatzes.
type	Ressourcendatensatz	Ressourcentyp der Governance für Cloud-Konfigurationen-Ressource.
answer	JSON	CI-Klasse, der die Ressource zugeordnet werden muss. Die Antwort enthält die folgenden Informationen: • sysId der CI-Klasse. • tableName der CI-Klasse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen-Variablen (Fortsetzung)

Name	Datentyp	Beschreibung
		Wenn die CI-Klasse mithilfe der CI-Finder-Zuordnung nicht identifiziert wird, legen Sie diese Variable auf null fest. **Syntax** `{ sysId: "value", tableName: "value" }`

Governance für Cloud-Konfigurationen-Aktionsreferenz

Von Governance für Cloud-Konfigurationen (CCG) werden IntegrationHub-Subflows dazu verwendet, mit der Cloud zu interagieren und die Konfigurationsdaten in der Configuration Management Database (CMDB) zu aktualisieren.

CCG – Read Config Setting (CCG – Konfigurationseinstellung lesen)

Verwenden Sie diese Aktion, um die Konfigurationsdaten der Ressource zu lesen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **Governance für Cloud-Konfigurationen** > **Dienstprogramme** > **CCG – Read Config Setting (CCG – Konfigurationseinstellung lesen)**an.

Aktion „CCG – Read Config Setting“ (CCG – Konfigurationseinstellung lesen)

Feld	Beschreibung
Ressource [Ressource]	Ressourcendatensatz, der die Konfigurationsdaten enthält.
Konfigurationsschlüssel [Konfigurationsschlüssel]	Konfigurationsschlüssel, den Sie lesen möchten.

Unterablauf-Ausgaben zuweisen

Formular „Subflow-Ausgaben zuweisen“

Feld	Beschreibung
Vorfall melden	Option, mit der der Audit-Verstoß über den Subflow gemeldet werden kann. Wählen Sie die Option **Vorfall melden** in der Spalte „Daten“ aus oder deaktivieren Sie dieses Kontrollkästchen, um dieses Feld festzulegen oder zu löschen. • Ausgewählt: Meldet das Problem gemäß der im Feld **Audit Violation Reporting** (Audit-Verstoßberichte) der Richtlinie ausgewählten Verstoßdefinition. • Deaktiviert: Der Verstoß wird von Governance für Cloud-Konfigurationen nicht gemeldet. Erstellen Sie einen benutzerdefinierten Datensatz für den Audit-Verstoß. Sie können Bedingungen angeben, um die Erstellung des Audit-Verstoßdatensatzes zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Subflow-Ausgaben zuweisen“ (Fortsetzung)

Feld	Beschreibung
Details	Verstoßdefinition, die Sie für den Verstoß melden möchten. Geben Sie die Definition des Verstoßes in der Spalte „Daten“ in das Feld **Details** ein. Dieses Feld ist erforderlich, wenn Sie die Option **Vorfall melden** ausgewählt haben.

Datensatz erstellen

Verwenden Sie diese Aktion, um einen Datensatz in der CMDB zu erstellen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **ServiceNow Core** > **Standard** > **Datensatz erstellen**an.

Aktion „Datensatz erstellen“

Feld	Beschreibung
Tabelle	Name der Configuration Management Database (CMDB)-Tabelle, in der das Audit-Ergebnis gespeichert wird. Legen Sie dieses Feld auf „Audit-Ergebnis“ [sn_itom_ccg_audit_result] fest.
Felder	Details des Datensatzes, den Sie in der Configuration Management Database (CMDB) erstellen möchten. Fügen Sie die folgenden Felder hinzu und konfigurieren Sie die Eingabe für sie: • **Scan Run** (Scan-Ausführung): Scan-Ausführung, bei der das Audit-Problem von Governance für Cloud-Konfigurationen identifiziert wurde. • **Ist Testausführung**: Gibt an, ob das Audit-Problem während einer Testausführung von Governance für Cloud-Konfigurationen gemeldet wurde. • **Details**: Details des Verstoßes. • **Violation Definition** (Verstoßdefinition): Verstoßdefinition des Audit-Problems. • **Ressource**: Cloud-Ressource, für die das Audit-Problem von Governance für Cloud-Konfigurationen ausgelöst wurde. • **Schweregrad**: Schweregrad des Audit-Problems.

CCG – Insert Resource Record (CCG – Ressourcendatensatz einfügen)

Verwenden Sie diese Aktion, um einen Ressourcendatensatz in die Configuration Management Database (CMDB) einzufügen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **Governance für Cloud-Konfigurationen** > **Dienstprogramme** > **CCG – Insert Resource Record (CCG – Ressourcendatensatz einfügen)**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion „CCG – Insert Resource Record“ (CCG – Ressourcendatensatz einfügen)

Feld	Beschreibung
Scan-Ausführung	Scanausführung, für die der Ressourcendatensatz vom Subflow erstellt werden muss.
Servicekonto	Servicekonto, an das die Ressource angehängt ist.
Logisches Rechenzentrum	Logisches Rechenzentrum, an das die Ressource angehängt ist.
Bezeichner	Bezeichner des Ressourcendatensatzes.
Name	Name der Ressource
Typ	Ressourcentyp
Anbieter	Cloud Provider, der die Ressource hostet.
Details	Details des Objekts, das Sie im Ressourcendatensatz speichern möchten.
Attribute	Jedes zusätzliche Ressourcenattribut, das Sie in die CMDB importieren möchten.

Bibliothek von Cloud-Aktionen-Aktionsreferenz

Bibliothek von Cloud-Aktionen (CAL) bietet verschiedene Aktionen, mit denen Sie die IntegrationHub-Subflows für Governance für Cloud-Konfigurationen erstellen können.

Bibliothek von Cloud-Aktionen bietet die folgenden Aktionen:

- CAL – AWS generate credential report (CAL – AWS-Anmeldeinformationsbericht generieren)
- CAL – AWS S3 get encryption (CAL – AWS S3-Verschlüsselung abrufen)
- CAL – Azure VM monitoring metric data (CAL – Metrikdaten für Azure-VM-Monitoring)
- AWS turn off EC2 instance (AWS EC2-Instanz deaktivieren)
- CAL – AWS list VMs (CAL – VMs auflisten)
- CAL – AWS list S3 buckets (CAL – AWS S3-Buckets auflisten)
- AWS put S3 bucket encryption (AWS S3-Bucket-Verschlüsselung platzieren)
- AWS enable EC2 instance monitoring (AWS EC2-Instanz-Monitoring aktivieren)
- CAL – Azure VM IP metric (CAL – Azure-VM-IP-Metrik)
- Azure turn off virtual machine (Azure-VM ausschalten)
- AWS get IAM login profile (AWS IAM-Anmeldeprofil abrufen)
- Disable AWS IAM user (AWS IAM-Benutzer deaktivieren)
- AWS list images (AWS-Images auflisten)
- CAL – Azure list VMs (CAL – VMs auflisten)

Die Aktionen von Bibliothek von Cloud-Aktionen sind in den Kategorien **Standard** und **Extern** verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Berechtigungen, die zum Erfassen der Konfigurationsschlüssel des Governance für Cloud-Konfigurationen-Basissystems erforderlich sind

Governance für Cloud-Konfigurationen erfordert geeignete Cloud-Berechtigungen zum Erfassen der Konfigurationsschlüssel des Basissystems aus der Cloud. Daher müssen Sie die entsprechenden Berechtigungen in der Cloud entsprechend den Anforderungen Ihrer Organisation festlegen.

Hinweis: Beginnend mit Governance für Cloud-Konfigurationen Version 1,3.7, der Inhalt des Basissystems wird in verschoben CCG Inhaltspaket. Installieren Sie CCG Inhaltspaket Um auf das Basissystem zuzugreifen Governance für Cloud-Konfigurationen Inhalte.

Amazon Web Services (AWS)-Rechenzentrum

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um den Konfigurationsschlüssel für die Konfigurationsschlüssel des AWS-Rechenzentrums zu erfassen:

- Ressourcensammler: Cloud-Servicekonto
- Verwendete Cloud-API: Aktion: *`DescribeRegions`*
- Cloud-Berechtigungen: *`ec2: DescribeRegions`*

Konfigurationsschlüssel für AWS-Rechenzentrum

Konfigurationsschlüssel	Datentyp
`AWS:EC2:VM:DescribeRegions`	*`String`*

AWS Identity and Access Management (IAM)-Benutzer

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel für AWS IAM-Benutzer zu erfassen:

- Ressourcensammler: AWS IAM User Data Collector
- Verwendete Cloud-API:
  - Aktion: *`GetCredentialReport`* und *`GenerateCredentialReport`*
  - Service: *`AWS IAM service`*
- Cloud-Berechtigungen: *`Iam:GetCredentialReport`* und *`Iam:GenerateCredentialReport`*

Konfigurationsschlüssel für AWS IAM-Benutzer

Konfigurationsschlüssel	Datentyp
`AWS:IAM:Policy:ARN`	*`String`*
`AWS:IAM:Policy:AttachmentCount`	*`String`*
`AWS:IAM:Policy:CreateDate`	*`String`*
`AWS:IAM:Policy:PolicyName`	*`String`*
`AWS:IAM:Policy:UpdateDate`	*`String`*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschlüssel für AWS IAM-Benutzer (Fortsetzung)

Konfigurationsschlüssel	Datentyp
AWS:IAM:User:AccessKey1.active	*Boolean*
AWS:IAM:User:AccessKey1.lastRotated	*Date*
AWS:IAM:User:AccessKey1.lastUsedDate	*Date*
AWS:IAM:User:AccessKey1.lastUsedRegion	*String*
AWS:IAM:User:AccessKey1.lastUsedService	*String*
AWS:IAM:User:AccessKey2.active	*Boolean*
AWS:IAM:User:AccessKey2.lastRotated	*Date*
AWS:IAM:User:AccessKey2.lastUsedDate	*Date*
AWS:IAM:User:AccessKey2.lastUsedRegion	*String*
AWS:IAM:User:AccessKey2.lastUsedService	*String*
AWS:IAM:User:Certificate1.active	*Boolean*
AWS:IAM:User:Certificate1.lastRotated	*Date*
AWS:IAM:User:Certificate2.active	*Boolean*
AWS:IAM:User:Certificate2.lastRotated	*Date*
AWS:IAM:User:CreationTime	*Date*
AWS:IAM:User:LoginProfile.active	*Boolean*
AWS:IAM:User:MfaEnabled	*Boolean*
AWS:IAM:User:PasswordEnabled	*Boolean*
AWS:IAM:User:PasswordLastChanged	*String*
AWS:IAM:User:PasswordLastUsed	*Date*
AWS:IAM:User:PasswordNextRotation	*String*

AWS-Objektspeicher

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel für AWS IAM-Benutzer zu erfassen:

- Konfigurationssammler: AWS S3 Encryption Metric Collector
- Ressourcensammler: AWS S3 Resource Collector
- Verwendete Cloud-API: Aktion: `ListBuckets` und `GetBucketEncryption` im S3-Service
- Cloud-Berechtigungen: *s3:ListBucket* und *s3:GetEncryptionConfiguration*

Konfigurationsschlüssel für AWS-Objektspeicher

Konfigurationsschlüssel	Datentyp
AWS:S3:Encryption:BucketKeyEnabled	*Boolean*
AWS:S3:Encryption:KMSMasterKeyID	*String*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsschlüssel für AWS-Objektspeicher (Fortsetzung)

Konfigurationsschlüssel	Datentyp
AWS:S3:Encryption:ServerSideEncryptionEnabled	*Boolean*
AWS:S3:Encryption:SSEAlgorithm	*String*

- Konfigurationssammler: AWS S3 ACL Permission Metric Collector
- Ressourcensammler: AWS S3 Resource Collector
- Verwendete Cloud-API: Aktion: *GetBucketAcl*
- Cloud-Berechtigungen: *s3:GetBucketAcl*

Konfigurationsschlüssel für AWS-Objektspeicher

Konfigurationsschlüssel	Datentyp
AWS:S3:ACL:AuthnUsersListing	*Boolean*
AWS:S3:ACL:AuthnUsersReadACL	*Boolean*
AWS:S3:ACL:AuthnUsersWrite	*Boolean*
AWS:S3:ACL:AuthnUsersWriteACL	*Boolean*
AWS:S3:ACL:OwnerFullControl	*Boolean*
AWS:S3:ACL:OwnerId	*String*
AWS:S3:ACL:OwnerListing	*Boolean*
AWS:S3:ACL:OwnerName	*String*
AWS:S3:ACL:OwnerReadACL	*Boolean*
AWS:S3:ACL:OwnerWrite	*Boolean*
AWS:S3:ACL:OwnerWriteACL	*Boolean*
AWS:S3:ACL:PublicListing	*Boolean*
AWS:S3:ACL:PublicReadACL	*Boolean*
AWS:S3:ACL:PublicWrite	*Boolean*
AWS:S3:ACL:PublicWriteACL	*Boolean*

AWS-VM-Instanz

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel der AWS-VM-Instanz zu erfassen:

- Ressourcensammler: AWS VM Data Collector
- Verwendete Cloud-API: Aktion: *DescribeInstances* and *AWS EC2 resource*
- Cloud-Berechtigungen: *ec2:DescribeInstances*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
AWS:EC2:VM:CapacityReservationPreference	*String*
AWS:EC2:VM:CpuOptionsCoreCount	*Numeric*
AWS:EC2:VM:CpuOptionsThreadsPerCore	*Numeric*
AWS:EC2:VM:EbsOptimized	*Boolean*
AWS:EC2:VM:HardwareType	*String*
AWS:EC2:VM:ImageId	*String*
AWS:EC2:VM:InstanceState	*String*
AWS:EC2:VM:KeyName	*String*
AWS:EC2:VM:LaunchTime	*Date*
AWS:EC2:VM:MonitoringState	*String*
AWS:EC2:VM:Platform	*String*
AWS:EC2:VM:PrivateDnsName	*String*
AWS:EC2:VM:PrivateIpAddress	*String*
AWS:EC2:VM:PublicDnsName	*String*
AWS:EC2:VM:PublicIPAddress	*String*
AWS:EC2:VM:SecurityGroups	*String*
AWS:EC2:VM:SubnetId	*String*
AWS:EC2:VM:Tags	*Map*
AWS:EC2:VM:UsageOperation	*String*
AWS:EC2:VM:VpcId	*String*

AWS-Profil mit minimalen Berechtigungen

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "iam:GenerateCredentialReport",
            "s3:GetEncryptionConfiguration",
            "ec2:DescribeInstances",
            "s3:ListBucketVersions",
            "ec2:DescribeRegions",
            "s3:ListBucket",
            "iam:GetCredentialReport"
         ],
         "Resource": "*"
      }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  ]
}
```

Microsoft Azure-VM-Instanz

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel der Azure-VM-Instanz zu erfassen:

- Ressourcensammler: Azure VM Data Collector
- Verwendete Cloud-API: `Microsoft.ResourceGraph/resources`
- Cloud-Berechtigungen: `Microsoft.ResourceGraph/resources`

Azure-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:HardwareType	*String*
Azure:VM:NICID	*String*
Azure:VM:OSDiskCaching	*String*
Azure:VM:OSDiskCreateoption	*String*
Azure:VM:OSDiskDeleteoption	*String*
Azure:VM:OSDiskId	*String*
Azure:VM:OSDiskName	*String*
Azure:VM:OSDiskOSType	*String*
Azure:VM:OSDiskSizeGB	*String*
Azure:VM:OSProfileAllowExtensionOperations	*Boolean*
Azure:VM:OSProfileComputerName	*String*
Azure:VM:OSProfileLinuxConfigurationDisablePasswordAuthentication	*Boolean*
Azure:VM:OSProfileLinuxConfigurationPatchSettingsAssessmentMode	*String*
Azure:VM:OSProfileLinuxConfigurationPatchSettingsPatchMode	*String*
Azure:VM:OSProfileLinuxConfigurationProvisionVmAgent	*Boolean*
Azure:VM:OSProfileLinuxConfigurationSSHKeyData	*Map*
Azure:VM:OSProfileLinuxConfigurationSSHPath	*Map*
Azure:VM:OSProfileRequireGuestProvisionSignal	*Boolean*
Azure:VM:OSWindowsConfigurationEnableAutomaticUpdates	*Boolean*
Azure:VM:OSWindowsConfigurationPatchSettingsAssessmentMode	*String*
Azure:VM:OSWindowsConfigurationPatchSettingsEnableHotpatching	*Boolean*
Azure:VM:OSWindowsConfigurationPatchSettingsPatchMode	*String*
Azure:VM:OSWindowsConfigurationProvisionVMAgent	*Boolean*
Azure:VM:PowerState	*String*
Azure:VM:ProvisioningState	*String*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Konfigurationsschlüssel für VM-Instanz (Fortsetzung)

Konfigurationsschlüssel	Datentyp
Azure:VM:ResourceGroup	*String*
Azure:VM:StorageProfileDataDisksCaching	*String*
Azure:VM:StorageProfileDataDisksCreateOption	*String*
Azure:VM:StorageProfileDataDisksDeleteOption	*String*
Azure:VM:StorageProfileDataDisksDetachOption	*String*
Azure:VM:StorageProfileDataDisksDiskIopsReadWrite	*String*
Azure:VM:StorageProfileDataDisksDiskMBpsReadWrite	*String*
Azure:VM:StorageProfileDataDisksDiskSizeGb	*Numeric*
Azure:VM:StorageProfileDataDisksImage	*String*
Azure:VM:StorageProfileDataDisksLun	*Numeric*
Azure:VM:StorageProfileDataDisksManagedDiskDiskEncryptionSet	*String*
Azure:VM:StorageProfileDataDisksManagedDiskId	*String*
Azure:VM:StorageProfileDataDisksManagedDiskResourceGroup	*String*
Azure:VM:StorageProfileDataDisksManagedDiskStorageAccountType	*String*
Azure:VM:StorageProfileDataDisksManagedStorageAccountType	*String*
Azure:VM:StorageProfileDataDisksName	*String*
Azure:VM:StorageProfileDataDisksToBeDetached	*Boolean*
Azure:VM:StorageProfileDataDisksVhd	*String*
Azure:VM:StorageProfileDataDisksWriteAcceleratorEnabled	*Boolean*
Azure:VM:StorageProfileImageReferenceExactVersion	*String*
Azure:VM:StorageProfileImageReferenceId	*String*
Azure:VM:StorageProfileImageReferenceOffer	*String*
Azure:VM:StorageProfileImageReferencePublisher	*String*
Azure:VM:StorageProfileImageReferenceSharedGalleryImageId	*String*
Azure:VM:StorageProfileImageReferenceSku	*String*
Azure:VM:StorageProfileImageReferenceVersion	*String*
Azure:VM:Tags	*Map*
Azure:VM:VMId	*String*

- Ressourcensammler: Azure VM Data Collector
- Configuration collector (Konfigurationssammler): Azure VM Metric Collector
- Verwendete Cloud-API: `Microsoft.ResourceGraph/resources`
- Cloud-Berechtigungen: `Microsoft.ResourceGraph/resources`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:PublicIPAddress	*String*
Azure:VM:PublicIPId	*String*

- Ressourcensammler: Azure VM Data Collector
- Configuration collector (Konfigurationssammler): Azure VM Monitoring Metric Collector
- Verwendete Cloud-API: *Microsoft.Compute/virtualMachines/{vmName}/instanceView*
- Cloud-Berechtigungen: *Microsoft.Compute/virtualMachines/{vmName}/instanceView*

Konfigurationsschlüssel für Azure-VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:MonitoringState	*String*

Hinweis: Verwenden Sie *scope=https://graph.microsoft.com/.default* und *scope=https://management.azure.com/.default*, um das oAuth-Token für Azure-Ressourcen abzurufen.

Azure-Profil mit minimalen Berechtigungen

```
{
   "properties": {
      "roleName": "CCGAzureMinimalPermission",
      "description": "Grants access to scan compute resources from azure subscription",
      "assignableScopes": [
         "/subscriptions/${subscription_id}"
      ],
      "permissions": [
         {
            "actions": [
               "Microsoft.ResourceGraph/resources/read",
               "Microsoft.Compute/virtualMachines/instanceView/read"
            ],
            "notActions": [],
            "dataActions": [],
            "notDataActions": []
         }
      ]
   }
}
```

AWS-Richtlinien

Die Governance für Cloud-Konfigurationen AWS-Richtlinien werden zu Ihrer Referenz aufgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
	AWS IAM User Activity policy (AWS IAM-Benutzeraktivitätsrichtlinie)	Condition Builder	Richtlinie zur Überprüfung, ob das Passwort für den AWS IAM-Benutzer aktiviert ist. Um diese Richtlinie zu verwenden, stellen Sie sicher, dass das AWS IAM-Benutzerkonto über die folgenden Berechtigungen verfügt: • Iam:GetCredentialReport • Iam:GenerateCredentialReport
	AWS S3 Enforce Bucket encryption (AWS-S3-Bucket-Verschlüsselung erzwingen)	Condition Builder	Richtlinie zur Überprüfung, ob die AWS-S3-Buckets verschlüsselt sind
	AWS Sample flow policy (Beispiel für eine AWS-Flow-Richtlinie)	IntegrationHub-Flow	Richtlinie zur Veranschaulichung einer IntegrationHub-Flow-basierten Richtlinie
	AWS VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den bereitgestellten EC2-VMs nur die genehmigten Hardwaretypen verwendet werden
	AWS VM IPAddress	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der EC2-VM mit dem Datensatz der Configuration Management Database (CMDB) übereinstimmt
	AWS VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die EC2-VM aktiviert ist
AWS: IAM-Sicherheit	Stellen Sie sicher, dass die Multifaktor-Authentifizierung (MFA) für alle IAM-Anwender aktiviert ist, die ein	IAM-Anwender	Multifaktor-Authentifizierung (MFA) fügt eine zusätzliche Ebene der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
	Konsolenpasswort haben (automatisiert).		Authentifizierungssicherung über herkömmliche Anmeldeinformationen hinaus hinzu. Wenn MFA aktiviert ist, wird ein Anwender, der sich bei der AWS-Konsole anmeldet, zur Eingabe seines Anwendernamens und Passworts sowie eines Authentifizierungscodes aus seinem physischen oder virtuellen MFA-Token aufgefordert. Es wird empfohlen, MFA für alle Accounts zu aktivieren, die über ein Konsolenpasswort verfügen. Das Aktivieren von MFA bietet erhöhte Sicherheit für den Konsolenzugriff, da der authentifizierende Prinzipal über ein Gerät verfügen muss, das einen zeitkritischen Schlüssel anzeigt und über Anmeldeinformationen verfügt.
	Stellen Sie sicher, dass Anmeldeinformationen, die 45 Tage oder länger nicht verwendet wurden, deaktiviert sind (automatisiert)	IAM-Anwender	AWS IAM-Anwender können mit verschiedenen Arten von Anmeldeinformationen, z. B. Passwörtern oder Zugriffsschlüsseln, auf AWS-Ressourcen zugreifen. Es wird empfohlen, alle Anmeldeinformationen,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			die seit 45 oder mehr Tagen nicht verwendet wurden, zu deaktivieren oder zu entfernen Das Deaktivieren oder Entfernen unnötiger Anmeldeinformationen reduziert das Zeitfenster für die Verwendung von Anmeldeinformationen, die einem gefährdeten oder verworfenen Account zugeordnet sind.
	Stellen Sie sicher, dass nur ein aktiver Zugriffsschlüssel für einen einzelnen IAM-Anwender verfügbar ist (automatisiert)	IAM-Anwender	Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Anwender oder den AWS-Account-Stammanwender. Sie können Zugriffsschlüssel verwenden, um programmgesteuerte Anforderungen an die AWS CLI oder AWS API zu signieren (direkt oder mit AWS SDK) Zugriffsschlüssel sind langfristige Anmeldeinformationen für einen IAM-Anwender oder den AWS-Account-Stammanwender. Sie können Zugriffsschlüssel verwenden, um programmgesteuerte Anforderungen an AWS CLI oder AWS API zu signieren. Eine der besten Möglichkeiten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			zum Schutz Ihres Accounts besteht darin, Anwendern nicht zu erlauben, mehrere Zugriffsschlüssel zu haben.
	Sicherstellen, dass Zugriffsschlüssel alle 90 Tage oder weniger rotiert werden (automatisiert)	IAM-Anwender	Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel, die zum Signieren programmatischer Anforderungen verwendet werden, die Sie an AWS stellen. AWS-Anwender benötigen eigene Zugriffsschlüssel, um programmgesteuerte Aufrufe an AWS über die AWS Command Line Interface (AWS CLI), Tools für Windows PowerShell, AWS SDKs oder direkte HTTP-Aufrufe über die APIs für einzelne AWS-Services zu tätigen.es wird empfohlen, alle Zugriffsschlüssel regelmäßig zu rotieren. Durch das Drehen von Zugriffsschlüsseln wird das Zeitfenster für die Verwendung eines Zugriffsschlüssels, der einem gefährdeten oder gekündigten Account zugeordnet ist, reduziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Zugriffsschlüssel sollten rotiert werden, um sicherzustellen, dass mit einem alten Schlüssel, der verloren gegangen, kaputt oder gestohlen wurde, nicht auf Daten zugegriffen werden kann.
	Sicherstellen, dass IAM-Anwender Berechtigungen nur über Gruppen erhalten (automatisiert)	IAM-Anwender	IAM-Anwendern wird über IAM-Richtlinien Zugriff auf Services, Funktionen und Daten gewährt. Es gibt drei Möglichkeiten, Richtlinien für einen Anwender zu definieren: **1.** Bearbeiten Sie die Anwenderrichtlinie direkt, d. h. eine Inline-, Anwender-, Richtlinie. **2.** Hängen Sie eine Richtlinie direkt an einen Anwender an. **3.** Fügen Sie den Anwender einer IAM-Gruppe hinzu, die über eine angehängte Richtlinie verfügt. Nur die dritte Implementierung wird empfohlen. Durch die Zuweisung der IAM-Richtlinie nur über Gruppen wird die Berechtigungsverwaltung auf einer einzigen, flexiblen Ebene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			zusammengefasst, die den funktionalen Rollen der Organisation entspricht. Durch die Vereinheitlichung der Berechtigungsverwaltung wird die Wahrscheinlichkeit übermäßiger Berechtigungen reduziert.
	Stellen Sie sicher, dass IAM-Richtlinien, die vollständige Administratorrechte „*:*“ zulassen, nicht angehängt sind (automatisiert)	IAM-Anwender	IAM-Richtlinien sind das Mittel, mit dem Anwendern, Gruppen oder Rollen Berechtigungen gewährt werden. Es wird empfohlen und als Standardsicherheitsempfehlung betrachtet, die geringste Berechtigung zu gewähren, d. h. nur die Berechtigungen zu gewähren, die zum Ausführen einer Aufgabe erforderlich sind. Bestimmen Sie, was Anwender tun müssen, und erstellen Sie dann Richtlinien für sie, die es den Anwendern ermöglichen, nur diese Aufgaben auszuführen, anstatt vollständige Administratorrechte zu gewähren. Es ist sicherer, mit einem Mindestsatz von Berechtigungen zu beginnen und bei Bedarf zusätzliche Berechtigungen zu gewähren, anstatt mit zu milden Berechtigungen zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			beginnen und später zu versuchen, sie zu straffen. Durch die Bereitstellung vollständiger Administratorrechte anstatt auf den Mindestsatz von Berechtigungen zu beschränken, die der Anwender ausführen muss, werden die Ressourcen potenziell unerwünschten Aktionen ausgesetzt. IAM-Richtlinien, die eine Anweisung mit „Wirkung“ haben: „Zulassen“ mit „Aktion“: „ *„ Über „Ressource“: „* „ Muss entfernt werden.
	Stellen Sie sicher, dass eine Supportrolle erstellt wurde, um Incidents mit AWS-Support (automatisiert) zu verwalten.	IAM-Anwender	AWS bietet ein Supportcenter, das für die Benachrichtigung und Reaktion auf Incidents sowie für technischen Support und Kundenservices verwendet werden kann. Erstellen Sie eine IAM-Rolle, damit autorisierte Anwender Incidents mit AWS-Support verwalten können. Durch die Implementierung der geringsten Berechtigung für die Zugriffssteuerung erfordert eine IAM-Rolle eine entsprechende IAM-Richtlinie,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			um Support Center-Zugriff zu ermöglichen, um Incidents mit AWS-Support zu verwalten.
	Stellen Sie sicher, dass alle abgelaufenen SSL-/TLS-Zertifikate, die in AWS IAM gespeichert sind, entfernt werden (automatisiert).	IAM-Anwender	Um HTTPS-Verbindungen mit Ihrer Website oder Anwendung in AWS zu aktivieren, benötigen Sie ein SSL/TLS-Serverzertifikat. Sie können ACM oder IAM verwenden, um Serverzertifikate zu speichern und bereitzustellen. Verwenden Sie IAM nur als Zertifikatmanager, wenn Sie HTTPS-Verbindungen in einer Region unterstützen müssen, die von ACM nicht unterstützt wird. IAM verschlüsselt Ihre privaten Schlüssel sicher und speichert die verschlüsselte Version im IAM-SSL-Zertifikatspeicher. IAM unterstützt die Bereitstellung von Serverzertifikaten in allen Regionen, Sie müssen Ihr Zertifikat jedoch von einem externen Anbieter zur Verwendung mit AWS erhalten. Sie können kein ACM-Zertifikat in IAM hochladen. Darüber hinaus können Sie Ihre Zertifikate nicht über die IAM-Konsole verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Durch das Entfernen abgelaufener SSL-/TLS-Zertifikate wird das Risiko eliminiert, dass versehentlich ein ungültiges Zertifikat in einer Ressource wie AWS Elastic Load Balancer (ELB) bereitgestellt wird, was die Glaubwürdigkeit der Anwendung/Website hinter dem ELB beeinträchtigen kann. Als Best Practice wird empfohlen, abgelaufene Zertifikate zu löschen.
	Stellen Sie sicher, dass die IAM-Zugriffsanalyse für alle Regionen aktiviert ist (automatisiert)	AWS::AccessAnalyzer::Analyzer	Aktivieren Sie die IAM-Zugriffsanalyse für IAM-Richtlinien zu allen Ressourcen in jeder Region. IAM Access Analyzer ist eine Technologie, die bei AWS Reinvent 2019 eingeführt wurde. Nachdem die Analyse in IAM aktiviert wurde, werden Scan-Ergebnisse in der Konsole mit den verfügbaren Ressourcen angezeigt. Scans zeigen Ressourcen an, auf die andere Accounts und Verbundanwender zugreifen können, z. B. KMS-Schlüssel und IAM-Rollen. Mit den Ergebnissen können Sie also bestimmen, ob ein unbeabsichtigter Anwender zulässig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			ist, sodass Administratoren den Zugriff mit geringsten Berechtigungen leichter überwachen können. Die Zugriffsanalyse analysiert nur Richtlinien, die auf Ressourcen in derselben AWS-Region angewendet werden. AWS IAM-Zugriffsanalyse hilft Ihnen, die Ressourcen in Ihrer Organisation und Ihren Accounts zu identifizieren, z. B. Amazon S3-Buckets oder IAM-Rollen, die für eine externe Entität freigegeben sind. Auf diese Weise können Sie unbeabsichtigten Zugriff auf Ihre Ressourcen und Daten identifizieren. Die Zugriffsanalyse identifiziert Ressourcen, die für externe Prinzipale freigegeben werden, indem sie logikbasierte Gründe verwendet, um die ressourcenbasierten Richtlinien in Ihrer AWS-Umgebung zu analysieren. Die IAM-Zugriffsanalyse überwacht kontinuierlich alle Richtlinien für S3-Bucket, IAM-Rollen, KMS-Schlüssel (Key Management Service), AWS Lambda-Funktionen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			und Amazon SQS-Warteschlangen (Simple Queue Service).
	Stellen Sie sicher, dass kein Zugriffsschlüssel für den Stammanwenderaccount vorhanden ist (automatisiert)	IAM-Anwender	Der Stamm-Anwenderaccount ist der privilegierte Anwender in einem AWS-Account. AWS-Zugriffsschlüssel bieten programmgesteuerten Zugriff auf einen bestimmten AWS-Account. Es wird empfohlen, alle Zugriffsschlüssel zu entfernen, die dem Stamm-Anwenderaccount zugeordnet sind. Das Entfernen von Zugriffsschlüsseln, die dem Stamm-Anwenderaccount zugeordnet sind, begrenzt die Vektoren, durch die der Account gefährdet werden kann. Darüber hinaus fördert das Entfernen der Stammzugriffsschlüssel die Erstellung und Verwendung rollenbasierter Accounts mit den geringsten Berechtigungen.
	Stellen Sie sicher, dass MFA für den Stamm-Anwenderaccount aktiviert ist (automatisiert)	IAM-Anwender	Der Stamm-Anwenderaccount ist der privilegierte Anwender in einem AWS-Account. Die Multifaktor-Authentifizierung (MFA) fügt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			eine zusätzliche Schutzebene zusätzlich zu einem Anwendernamen und Passwort hinzu. Wenn MFA aktiviert ist, wird ein Anwender, der sich bei einer AWS-Website anmeldet, zur Eingabe seines Anwendernamens und Passworts sowie eines Authentifizierungscodes von seinem AWS MFA-Gerät aufgefordert. Das Aktivieren von MFA bietet erhöhte Sicherheit für den Konsolenzugriff, da der authentifizierende Prinzipal über ein Gerät verfügen muss, das einen zeitkritischen Schlüssel ausgibt und über Anmeldeinformationen verfügt.
	Stellen Sie sicher, dass Hardware-MFA für den Stamm-Anwenderaccount aktiviert ist (automatisiert)	IAM-Anwender	Der Stamm-Anwenderaccount ist der privilegierte Anwender in einem AWS-Account. MFA fügt neben einem Anwendernamen und Passwort eine zusätzliche Schutzebene hinzu. Wenn MFA aktiviert ist, wird ein Anwender, der sich bei einer AWS-Website anmeldet, zur Eingabe seines Anwendernamens und Passworts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			sowie eines Authentifizierungscodes von seinem AWS MFA-Gerät aufgefordert. Für Ebene 2 wird empfohlen, den Stamm-Anwenderaccount mit einer Hardware-MFA zu schützen. Eine Hardware-MFA hat eine kleinere Angriffsfläche als eine virtuelle MFA. Beispielsweise leidet eine Hardware-MFA nicht unter der Angriffsfläche, die vom mobilen Smartphone eingeführt wird, auf dem sich eine virtuelle MFA befindet.
	Eliminieren Sie die Verwendung des Stammanwenders für administrative und tägliche Aufgaben (automatisiert)	IAM-Anwender	Mit der Erstellung eines AWS-Accounts wird ein „Stammanwender“ erstellt, der nicht deaktiviert oder gelöscht werden kann. Dieser Anwender hat uneingeschränkten Zugriff auf und Kontrolle über alle Ressourcen im AWS-Account. Es wird dringend empfohlen, die Verwendung dieses Accounts für tägliche Aufgaben zu vermeiden. Der „Stammanwender“ hat uneingeschränkten Zugriff auf und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Kontrolle über alle Account-Ressourcen. Die Verwendung von ist nicht mit den Grundsätzen der geringsten Berechtigungen und der Aufgabentrennung vereinbar und kann aufgrund von Fehlern oder Account-Kompromittierungen zu unnötigen Schäden führen.
	Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert (automatisiert)	IAM-Anwender	Passwortrichtlinien werden teilweise verwendet, um Anforderungen an die Passwortkomplexität zu erzwingen. IAM-Passwortrichtlinien können verwendet werden, um sicherzustellen, dass Passwörter mindestens eine bestimmte Länge haben. Es wird empfohlen, dass die Passwortrichtlinie eine Mindestpasswortlänge 14 erfordert. Das Festlegen einer Richtlinie zur Passwortkomplexität erhöht die Account-Resilienz gegenüber Brute-Force-Anmeldeversuchen.
	Sicherstellen, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert (automatisiert)	IAM-Anwender	IAM-Passwortrichtlinien können die Wiederverwendung eines bestimmten Passworts durch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			denselben Anwender verhindern. Es wird empfohlen, dass die Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert. Die Verhinderung der Wiederverwendung von Passwörtern erhöht die Account-Resilienz gegenüber Brute-Force-Anmeldeversuchen.
AWS: Datensicherheit	Stellen Sie sicher, dass S3-Buckets mit „öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind.	AWS::S3::Bucket	Amazon S3 bietet öffentlichen Zugriff blockieren (Bucket-Einstellungen) und öffentlichen Zugriff blockieren (Accounteinstellungen), um Sie bei der Verwaltung des öffentlichen Zugriffs auf Amazon S3-Ressourcen zu unterstützen. Standardmäßig werden S3-Buckets und -Objekte neu erstellt, wenn der öffentliche Zugriff deaktiviert ist. Ein IAM-Prinzipal mit ausreichenden S3-Berechtigungen kann jedoch öffentlichen Zugriff auf Bucket- und/oder Objektebene ermöglichen. Wenn diese Option aktiviert ist, verhindert das Blockieren des öffentlichen Zugriffs (Bucket-Einstellungen), dass ein einzelner Bucket und seine containedObjects

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			öffentlich zugänglich werden. Gleichermaßen verhindert das Blockieren des öffentlichen Zugriffs (Accounteinstellungen), dass alle Buckets und enthaltenen Objekte im gesamten Account öffentlich zugänglich werden. Amazon S3 – öffentlichen Zugriff blockieren (Bucket-Einstellungen) verhindert die versehentliche oder böswillige öffentliche Offenlegung von Daten, die in den jeweiligen Buckets enthalten sind. Amazon S3: Öffentlichen Zugriff blockieren (Account-Einstellungen) verhindert die versehentliche oder böswillige öffentliche Offenlegung von Daten, die in allen Buckets des jeweiligen AWS-Accounts enthalten sind. Ob das Blockieren des öffentlichen Zugriffs auf alle oder einige Buckets eine Organisationsentscheidung ist, die auf Datensensibilität, geringsten Berechtigungen und Anwendungsfällen basieren sollte.
AWS: CloudTrail-Protokollierung	Stellen Sie sicher, dass die Protokollierung auf	AWS::S3::Bucket	S3-API-Vorgänge auf Objektebene

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
	Objektebene für Schreib-Ereignisse für S3-Bucket (automatisiert) aktiviert ist.		wie GetObject, DeleteObject und PutObject werden als Datenereignisse bezeichnet. Standardmäßig protokollieren CloudTrail-Trails keine Datenereignisse, daher wird empfohlen Aktivieren Sie die Protokollierung auf Objektebene für S3-Buckets. Begründung: Durch Aktivieren der Protokollierung auf Objektebene können Sie die Compliance-Anforderungen für Daten in Ihrer Organisation erfüllen, umfassende Sicherheitsanalysen durchführen und bestimmte Muster von Anwendern überwachen Verhalten in Ihrem AWS-Account oder sofortige Aktionen für API-Aktivitäten auf Objektebene in Ihren S3-Buckets mithilfe von Amazon CloudWatch-Ereignissen.
AWS: CloudTrail-Protokollierung	Stellen Sie sicher, dass die Protokollierung auf Objektebene für Lese-Ereignisse für den S3-Bucket (automatisiert) aktiviert ist.	AWS::S3::Bucket	S3-API-Vorgänge auf Objektebene wie GetObject, DeleteObject und PutObject werden als Datenereignisse bezeichnet. Standardmäßig protokollieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			CloudTrail-Trails keine Datenereignisse, daher wird empfohlen Aktivieren Sie die Protokollierung auf Objektebene für S3-Buckets. Begründung: Durch Aktivieren der Protokollierung auf Objektebene können Sie die Compliance-Anforderungen für Daten in Ihrer Organisation erfüllen, umfassende Sicherheitsanalysen durchführen und bestimmte Muster von Anwendern überwachen Verhalten in Ihrem AWS-Account oder sofortige Aktionen für API-Aktivitäten auf Objektebene mithilfe von Amazon CloudWatch-Ereignissen.
AWS: Netzwerksicherheit	Stellen Sie sicher, dass keine Netzwerk-ACLs das Eingreifen von 0,0.0.0/0 an Remote-Server-Verwaltungsports zulassen (automatisiert)	AWS::EC2::NetworkAcl	Die Funktion Network Access Control List (NACL) ermöglicht eine statuslose Filterung von eingehendem und ausgehendem Netzwerkverkehr an AWS-Ressourcen. Es wird empfohlen, dass keine NACL uneingeschränkten Eingangszugriff auf Remote-Server-Verwaltungsports zulässt, z. B. SSH

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen AWS-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			auf Port 22 und RDP auf Port 3389. Öffentlicher Zugriff auf Remote-Serververwaltungsports wie 22 und 3389 erhöht die Ressourcenangriffsfläche und erhöht unnötig das Risiko einer Ressourcengefährdung.
AWS: Netzwerksicherheit	Stellen Sie sicher, dass keine Sicherheitsgruppen das Eindringen von 0,0.0.0/0 an Remote-Serververwaltungsports zulassen (automatisiert)	AWS::EC2::SecurityGroup	Sicherheitsgruppen bieten eine statusbehaftete Filterung des eingehenden und ausgehenden Netzwerkverkehrs an AWS-Ressourcen. Es wird empfohlen, dass keine Sicherheitsgruppe uneingeschränkten Eingangszugriff auf Verwaltungsports des Remote-Servers zulässt, z. B. SSH zu Port 22 und RDP zu Port 3389 Öffentlicher Zugriff auf Remote-Serververwaltungsports wie 22 und 3389 erhöht die Ressourcenangriffsfläche und erhöht unnötig das Risiko einer Ressourcengefährdung.

Automatische Übersetzung

Azure-Richtlinien

Die Governance für Cloud-Konfigurationen AWS-Richtlinien werden zu Ihrer Referenz aufgeführt.

Governance für Cloud-Konfigurationen Azure-Richtlinien

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
	Azure VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			bereitgestellten Azure-VMs nur die genehmigten Hardwaretypen verwendet werden
	Azure VM IP Address (Azure-VM-IP-Adresse)	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der Azure-VM mit dem Datensatz der CMDB übereinstimmt
	Azure VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die Azure-VM aktiviert ist
Azure: Sicherheitscenter-Konfiguration	Stellen Sie sicher, dass die automatische Bereitstellung von „Log Analytics Agent für“ aktiviert ist Azure VMs ist auf „ein“ festgelegt (automatisiert)	Azure-Abonnement	Aktivieren Sie die automatische Bereitstellung des Überwachungs-Agents, um Sicherheitsdaten zu erfassen. Wenn „Log Analytics Agent für Azure VMs“ aktiviert ist, stellt Microsoft Defender for Cloud den Microsoft Monitoring Agent auf allen vorhandenen unterstützten virtuellen Azure-Computern und allen neuen, die erstellt werden, bereit. Der Microsoft Monitoring Agent scannt nach verschiedenen sicherheitsbezogenen Konfigurationen und Ereignissen, z. B. Systemupdates, BS-Schwachstellen, Endpunktschutz, und stellt Warnungen bereit.
Azure: Sicherheitscenter-Konfiguration	Stellen Sie sicher, dass „zusätzliche E-Mail-Adressen“ mit einer	Azure-Abonnement	Microsoft Defender for Cloud sendet eine E-Mail an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
	Sicherheitskontakt-E-Mail (automatisiert) konfiguriert ist.		Abonnementbesitzer, wenn eine Warnung mit hohem Schweregrad für ihr Abonnement ausgelöst wird. Geben Sie als zusätzliche E-Mail-Adresse eine Sicherheitskontakt-E-Mail-Adresse an. Microsoft Defender for Cloud sendet eine E-Mail an den Abonnementbesitzer, um ihn über Sicherheitswarnungen zu benachrichtigen. Durch das Hinzufügen der E-Mail-Adresse Ihres Sicherheitskontakts zum Feld „zusätzliche E-Mail-Adressen“ wird sichergestellt, dass das Sicherheitsteam Ihrer Organisation in diesen Warnungen enthalten ist. Dadurch wird sichergestellt, dass die richtigen Personen über potenzielle Kompromisse informiert sind, um das Risiko rechtzeitig zu mindern.
Azure: Sicherheitscenter-Konfiguration	Stellen Sie sicher, dass „über Warnungen mit dem folgenden Schweregrad benachrichtigen“ auf „hoch“ festgelegt ist (automatisiert).	Azure-Abonnement	Aktiviert das E-Mail-Senden von Sicherheitswarnungen an den Abonnementbesitzer oder einen anderen festgelegten Sicherheitskontakt. Durch Aktivieren von E-Mails für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Sicherheitswarnungen wird sichergestellt, dass Sicherheitswarnungs-E-Mails von Microsoft empfangen werden. Dadurch wird sichergestellt, dass die richtigen Personen über potenzielle Sicherheitsprobleme informiert sind und das Risiko mindern können.
Azure: Sicherheitscenter-Konfiguration	Stellen Sie sicher, dass „alle Anwender mit den folgenden Rollen“ auf „Besitzer“ festgelegt ist (automatisiert).	Azure-Abonnement	Aktivieren Sie Sicherheitswarnungs-E-Mails für Abonnementbesitzer. Durch Aktivieren von Sicherheitswarnungs-E-Mails für Abonnementbesitzer wird sichergestellt, dass sie Sicherheitswarnungs-E-Mails von Microsoft erhalten. Dadurch wird sichergestellt, dass sie sich aller potenziellen Sicherheitsprobleme bewusst sind und das Risiko rechtzeitig mindern können.
Azure: Speichersicherheit	Stellen Sie sicher, dass die Speicherprotokollierung für den Blob-Service für Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert)	Microsoft.Speicher/StorageAccounts	Der Storage Blob-Service bietet skalierbaren, kosteneffizienten Zielspeicher in der Cloud. Die Speicherprotokollierung erfolgt serverseitig und ermöglicht die Aufzeichnung von Details für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			erfolgreiche und fehlgeschlagene Anforderungen im Speicher-Account. Mit diesen Protokollen können Anwender Details zu Lese-, Schreib- und Löschvorgängen für die Blobs anzeigen. Speicherprotokollierungsprotokolleint enthalten die folgenden Informationen zu einzelnen Anforderungen: Zeitinformationen wie Startzeit, End-to-End-Latenz und Serverlatenz, Authentifizierungsdetails, Informationen zur Gleichzeitigkeit und die Größen der Anforderungs- und Antwortnachrichten. Storage Analytics-Protokolle enthalten detaillierte Informationen zu erfolgreichen und fehlgeschlagenen Anforderungen an einen Speicherservice. Diese Informationen können verwendet werden, um jede einzelne Anforderung an einen Speicherservice zu überwachen, um die Sicherheit oder Diagnose zu erhöhen. Anforderungen werden nach bestem Bemühen protokolliert. Die Storage Analytics-Protokollierung ist für Ihren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Speicher-Account standardmäßig nicht aktiviert.
Azure: Speichersicherheit	Stellen Sie sicher, dass die Speicherprotokollierung für den Tabellenservice für die Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert)	Microsoft.Speicher/ StorageAccounts	Der Speicher der Speichertabelle ist ein Service, der Strukturdaten in NoSQL in der Cloud speichert und einen Schlüssel-/ Attributspeicher mit einem Design ohne Schema bereitstellt. Die Speicherprotokollierung erfolgt serverseitig und ermöglicht die Aufzeichnung von Details für erfolgreiche und fehlgeschlagene Anforderungen im Speicher-Account. Mit diesen Protokollen können Anwender Details zu Lese-, Schreib- und Löschvorgängen für die Tabellen anzeigen. Speicherprotokollierungsprotokolleint enthalten die folgenden Informationen zu einzelnen Anforderungen: Zeitinformationen wie Startzeit, End-to-End-Latenz und Serverlatenz, Authentifizierungsdetails, Informationen zur Gleichzeitigkeit und die Größen der Anforderungs- und Antwortnachrichten. Storage Analytics-Protokolle enthalten detaillierte Informationen zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			erfolgreichen und fehlgeschlagenen Anforderungen an einen Speicherservice. Diese Informationen können verwendet werden, um jede einzelne Anforderung an einen Speicherservice zu überwachen, um die Sicherheit oder Diagnose zu erhöhen. Anforderungen werden nach bestem Bemühen protokolliert. Die Storage Analytics-Protokollierung ist für Ihren Speicher-Account standardmäßig nicht aktiviert.
Azure: Speichersicherheit	Stellen Sie sicher, dass die Speicherprotokollierung für Warteschlangenservice für Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert)	Microsoft.Speicher/ StorageAccounts	Der Service „Speicherwarteschlange“ speichert Nachrichten, die von jedem Client gelesen werden können, der Zugriff auf das Speicherkonto hat. Eine Warteschlange kann eine unbegrenzte Anzahl von Nachrichten enthalten, von denen jede mit Version 2011-08-18 oder höher bis zu 64 KB groß sein kann. Die Speicherprotokollierung erfolgt serverseitig und ermöglicht die Aufzeichnung von Details für erfolgreiche und fehlgeschlagene Anforderungen im Speicher-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Account. Mit diesen Protokollen können Anwender Details zu Lese-, Schreib- und Löschvorgängen für die Warteschlangen anzeigen. Speicherprotokollierungsprotokolleint enthalten die folgenden Informationen zu einzelnen Anforderungen: Zeitinformationen wie Startzeit, End-to-End-Latenz und Serverlatenz, Authentifizierungsdetails, Informationen zur Gleichzeitigkeit und die Größen der Anforderungs- und Antwortnachrichten. Storage Analytics-Protokolle enthalten detaillierte Informationen zu erfolgreichen und fehlgeschlagenen Anforderungen an einen Speicherservice. Diese Informationen können verwendet werden, um einzelne Anforderungen zu überwachen und Probleme mit einem Speicherservice zu diagnostizieren. Anforderungen werden nach bestem Aufwand protokolliert.die Storage Analytics-Protokollierung ist für Ihren Speicher-Account standardmäßig nicht aktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
Azure: SQL-Sicherheit	Stellen Sie sicher, dass Vulnerability Assessment (VA) auf einem SQL-Server aktiviert ist, indem Sie ein Speicherkonto (automatisiert) festlegen.	Microsoft.Sql/servers	Aktivieren Sie Vulnerability Assessment (VA)-Servicescans für kritische SQL-Server und entsprechende SQL-Datenbanken.
Azure: SQL-Sicherheit	Stellen Sie sicher, dass VA „regelmäßige wiederkehrende Scans“ für jeden SQL-Server auf „ein“ setzt (automatisiert)	Microsoft.Sql/servers	Aktivieren Sie periodische wiederkehrende Scans der Schwachstellenbewertung (VA) für kritische SQL-Server und entsprechende SQL-Datenbanken.
Azure: SQL-Sicherheit	Stellen Sie sicher, dass die VA-Einstellung „Scanberichte senden an“ für einen SQL-Server (automatisiert) konfiguriert ist.	Microsoft.Sql/servers	Konfigurieren Sie „Scan-Berichte senden an“ mit E-Mail-IDs betroffener Datenbesitzer/ Stakeholder für kritische SQL-Server.
Azure: SQL-Sicherheit	Stellen Sie sicher, dass die Schwachstellenbewertungseinstellung „auch E-Mail-Benachrichtigungen an Administratoren und Abonnementbesitzer senden“ für festgelegt ist	Microsoft.Sql/servers	Aktivieren Sie die Einstellung „Vulnerability Assessment (VA)“ „auch E-Mail-Benachrichtigungen an Administratoren und Abonnementbesitzer senden“.
Azure: SQL-Sicherheit	Stellen Sie sicher Azure Active Directory-Administrator ist konfiguriert (automatisiert)	Microsoft.Sql/servers	Verwenden Sie die Azure Active Directory-Authentifizierung für die Authentifizierung mit SQL Database, um Anmeldeinformationen an einem zentralen Ort zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
Azure: SQL-Sicherheit	Stellen Sie sicher, dass der TDE-Schutz von SQL Server mit dem vom Anwender verwalteten Schlüssel (automatisiert) verschlüsselt ist.	Microsoft.Sql/servers	TDE mit vom Kunden verwaltetem Schlüsselsupport bietet mehr Transparenz und Kontrolle über den TDE-Schutz, erhöhte Sicherheit durch einen HSM-gestützten externen Service und Förderung der Aufgabentrennung. Mit TDE werden Daten im Ruhezustand mit einem symmetrischen Schlüssel (Datenbankverschlüsselungsschlüssel verschlüsselt, der in der Datenbank- oder Data Warehouse-Verteilung gespeichert ist. Zum Schutz dieses Datenverschlüsselungsschlüssels (Data Encryption Key, DEK) in der Vergangenheit konnte nur ein Zertifikat verwendet werden, das vom Azure SQL-Service verwaltet wird. Mit der vom Kunden verwalteten Schlüsselunterstützung für TDE kann die DEK jetzt mit einem asymmetrischen Schlüssel geschützt werden, der im Key Vault gespeichert ist. Key Vault ist ein hochverfügbarer und skalierbarer Cloud-basierter Schlüsselspeicher, der zentrale Schlüsselverwaltung bietet, FIPS 140-2

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Level 2 validierte Hardwaresicherheitsmodule (HSMs) nutzt und die Trennung der Verwaltung von Schlüsseln und Daten für zusätzliche Sicherheit ermöglicht. Basierend auf den Geschäftsanforderungen oder der Relevanz von Daten/ Datenbanken, die auf einem SQL-Server gehostet werden, wird empfohlen, den TDE-Schutz mit einem Schlüssel zu verschlüsseln, der vom Datenbesitzer verwaltet wird (vom Kunden verwalteter Schlüssel).
Azure: Protokollierung und Überwachung	Sicherstellen, dass die Diagnoseeinstellung die entsprechenden Kategorien erfasst (automatisiert)	Azure-Abonnement	Die Diagnoseeinstellung sollte so konfiguriert werden, dass die entsprechenden Aktivitäten von der Steuerungs-/ Verwaltungsebene protokolliert werden. Eine Diagnoseeinstellung steuert, wie das Diagnoseprotokoll exportiert wird. Das Erfassen der Diagnoseeinstellungskategorien für die entsprechenden Aktivitäten der Steuerungs-/ Verwaltungsebene ermöglicht richtige Warnungen Eine Diagnoseeinstellung steuert, wie das

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Diagnoseprotokoll exportiert wird. Das Erfassen der Diagnoseeinstellungskategorien für die entsprechenden Aktivitäten der Steuerungs-/ Verwaltungsebene ermöglicht richtige Warnungen.
Azure: Protokollierung und Überwachung	Stellen Sie sicher, dass die Protokollierung für Azure KeyVault „aktiviert“ ist (automatisiert).	Microsoft.KeyVault	Aktivieren Sie die AuditEvent-Protokollierung für SchlüsselVault-Instanzen, um sicherzustellen, dass Interaktionen mit SchlüsselTresoren protokolliert und verfügbar sind. Überwachung, wie und wann auf SchlüsselTresore zugegriffen wird und wer einen Audit-Pfad von Interaktionen mit vertraulichen Informationen, Schlüsseln und Zertifikaten ermöglicht, die von Azure KeyVault verwaltet werden. Durch Aktivieren der Protokollierung für Key Vault werden Informationen in einem Azure-Speicher-Account gespeichert, den der Anwender bereitstellt. Dadurch wird automatisch ein neuer Container mit dem Namen Insights-logs-auditevent für den angegebenen Speicher-Account erstellt, und derselbe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Speicher-Account kann zum Sammeln von Protokollen für mehrere Schlüsselspeicher verwendet werden.
Azure: Datensicherheit	Stellen Sie sicher, dass „nicht angehängte Datenträger“ mit CMK (automatisiert) verschlüsselt sind.	Microsoft.Compute/disks	Stellen Sie sicher, dass nicht angehängte Datenträger in einem Abonnement mit einem vom Kunden verwalteten Schlüssel (CMK) verschlüsselt sind. Verwaltete Datenträger werden standardmäßig mit von der Plattform verwalteten Schlüsseln verschlüsselt. Die Verwendung von anwenderverwalteten Schlüsseln kann ein zusätzliches Sicherheitsniveau bieten oder die regulatorischen Anforderungen einer Organisation erfüllen. Die Verschlüsselung verwalteter Datenträger stellt sicher, dass der gesamte Inhalt ohne Schlüssel vollständig nicht wiederhergestellt werden kann, und schützt das Volume somit vor unberechtigten Lesezugriffen. Auch wenn der Datenträger nicht an einen der VMs angehängt ist,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			besteht immer das Risiko, dass ein gefährdeter Anwenderaccount mit Administratorzugriff auf den VM-Service diese Datenträger bereitstellen/ anhängen kann, was zur Offenlegung und Manipulation vertraulicher Informationen führen kann.
Azure: Zugriffssteuerung	Stellen Sie sicher, dass der Schlüsselspeicher wiederhergestellt werden kann (automatisiert)	Microsoft.KeyVault	Der Schlüsselspeicher enthält Objektschlüssel, Geheimnisse und Zertifikate. Die versehentliche Nichtverfügbarkeit eines SchlüsselVault kann zu sofortigem Datenverlust oder Verlust von Sicherheitsfunktionen (Authentifizierung, Validierung, Verifizierung, Nichtwiderlegung usw.) führen, die von den SchlüsselVault-Objekten unterstützt werden. Es wird empfohlen, den Schlüsselspeicher wiederherstellbar zu machen, indem die Funktionen „nicht löschen“ und „Soft Delete“ aktiviert werden. Dies dient dazu, den Verlust verschlüsselter Daten zu verhindern, einschließlich Speicherkonten,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			SQL-Datenbanken und/oder abhängiger Services, die von SchlüsselVault-Objekten (Schlüssel, Geheimnisse, Zertifikate) usw. bereitgestellt werden, wie dies im Falle einer versehentlichen Löschung durch einen Anwender oder durch störende Aktivitäten durch einen böswilligen Anwender geschehen kann. Es kann Szenarien geben, in denen Anwender versehentlich das Löschen/Löschen eines Befehls für den Schlüsselspeicher ausführen oder Angreifer/böswillige Anwender dies absichtlich tun, um eine Unterbrechung zu verursachen. Das Löschen oder Löschen eines SchlüsselTresors führt zu sofortigem Datenverlust, da Schlüssel, die Daten und Geheimnisse/ Zertifikate verschlüsseln, die Zugriff/Services ermöglichen, nicht zugänglich werden. Es gibt 2 SchlüsselVault-Eigenschaften, die bei der dauerhaften Nichtverfügbarkeit eines SchlüsselTresors eine Rolle spielen.1.enableSoftDelete:wenn

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Sie diesen Parameter für einen SchlüsselTresor auf „wahr“ setzen, wird sichergestellt, dass der SchlüsselTresor selbst oder seine Objekte für die nächsten 90 Tage wiederhergestellt werden können, auch wenn der SchlüsselTresor gelöscht wird. In diesem Zeitraum von 90 Tagen können Schlüsseltresor/ Schlüsselobjekte wiederhergestellt oder gelöscht werden (dauerhafte Löschung). Wenn keine Aktion ausgeführt wird, werden der Schlüsseltresor und seine Objekte nach 90 Tagen gelöscht.2.enablePurgeProtection:ena stellt nur sicher, dass der Schlüsseltresor nicht dauerhaft gelöscht wird und 90 Tage ab dem Löschdatum wiederhergestellt werden kann. Es besteht jedoch die Wahrscheinlichkeit, dass der Schlüsselspeicher und/oder seine Objekte versehentlich gelöscht werden und daher nicht wiederhergestellt werden können. Wenn Sie „enablePurgeProtection“ auf „wahr“ festlegen, wird sichergestellt, dass der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			Schlüsselspeicher und seine Objekte nicht gelöscht werden können.durch Aktivieren beider Parameter in SchlüsselTresoren wird sichergestellt, dass SchlüsselTresore und ihre Objekte nicht dauerhaft gelöscht/ gelöscht werden können.
Azure: App-Servicesicherheit	Stellen Sie sicher, dass die Web-App den gesamten HTTP-Datenverkehr in Azure App Service an HTTPS umleitet (automatisiert)	Microsoft.Web/sites	Mit Azure Web Apps können Sites standardmäßig sowohl unter HTTP als auch unter HTTPS ausgeführt werden. Standardmäßig kann jeder über nicht sichere HTTP-Links auf Web-Apps zugreifen. Nicht sichere HTTP-Anforderungen können eingeschränkt werden, und alle HTTP-Anforderungen können an den sicheren HTTPS-Port weitergeleitet werden. Es wird empfohlen, nur HTTPS-Datenverkehr zu erzwingen. Durch Aktivieren des nur HTTPS-Datenverkehrs werden alle nicht sicheren HTTP-Anforderungen an HTTPS-Ports weitergeleitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Azure-Richtlinien (Fortsetzung)

Richtliniensatz	Richtlinienname	Ressourcentyp	Beschreibung
			HTTPS verwendet das TLS/SSL-Protokoll, um eine sichere Verbindung bereitzustellen, die sowohl verschlüsselt als auch authentifiziert ist. Daher ist es wichtig, HTTPS für die Sicherheitsvorteile zu unterstützen.
Azure: App-Servicesicherheit	Stellen Sie sicher, dass die Web-App die neueste Version der TLS-Verschlüsselung (automatisiert) verwendet.	Microsoft.Web/sites	Das TLS-Protokoll (Transport Layer Security) sichert die Übertragung von Daten über das Internet mit standardmäßiger Verschlüsselungstechnologie. Die Verschlüsselung muss mit der neuesten Version von TLS festgelegt werden. Der App-Service ermöglicht standardmäßig TLS 1,2, was nach Branchenstandards wie PCI DSS die empfohlene TLS-Stufe ist. Mit dem App-Service kann die Web-App derzeit TLS-Versionen 1,0, 1,1 und 1,2 festlegen. Es wird dringend empfohlen, die neueste TLS 1,2-Version für sichere Verbindungen der Web-App zu verwenden.

Automatische Übersetzung

Policy sets (Richtliniensätze)

Die Governance für Cloud-Konfigurationen Richtliniensätze und ihre Richtlinien werden zu Ihrer Referenz aufgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Richtliniensätze

Name Des Richtliniensatzes	Richtlinien	Beschreibung
AWS 1.4.0	Sicherstellen, dass IAM-Anwender Berechtigungen nur über Gruppen erhalten (automatisiert) Stellen Sie sicher, dass keine Netzwerk-ACLs das Eingreifen von 0,0.0.0/0 an Remote-Server-Verwaltungsports zulassen (automatisiert) Stellen Sie sicher, dass die IAM-Passwortrichtlinie eine Mindestlänge von 14 oder mehr erfordert (automatisiert) Stellen Sie sicher, dass eine Supportrolle erstellt wurde, um Incidents mit AWS-Support (automatisiert) zu verwalten. Eliminieren Sie die Verwendung des Stammanwenders für administrative und tägliche Aufgaben (automatisiert) Stellen Sie sicher, dass Hardware-MFA für den Stamm-Anwenderaccount aktiviert ist (automatisiert) Stellen Sie sicher, dass die Protokollierung auf Objektebene für Schreib-Ereignisse für S3-Bucket (automatisiert) aktiviert ist. Sicherstellen, dass Zugriffsschlüssel alle 90 Tage oder weniger rotiert werden (automatisiert) Stellen Sie sicher, dass nur ein aktiver Zugriffsschlüssel für einen einzelnen IAM-Anwender verfügbar ist (automatisiert) Stellen Sie sicher, dass IAM-Richtlinien, die vollständige Administratorrechte „*:*“ zulassen, nicht angehängt sind (automatisiert) Stellen Sie sicher, dass alle abgelaufenen SSL-/TLS-Zertifikate, die in AWS IAM gespeichert sind, entfernt werden (automatisiert). Sicherstellen, dass die IAM-Passwortrichtlinie die Wiederverwendung von Passwörtern verhindert (automatisiert) Stellen Sie sicher, dass die IAM-Zugriffsanalyse für alle Regionen aktiviert ist (automatisiert) Stellen Sie sicher, dass die Multifaktor-Authentifizierung (MFA) für alle IAM-Anwender aktiviert ist, die ein Konsolenpasswort haben (automatisiert). Stellen Sie sicher, dass Anmeldeinformationen, die 45 Tage oder länger nicht verwendet wurden, deaktiviert sind (automatisiert)	Amazon Web Services Fundamentations-Benchmark (automatisiert) v1.4.0 - 05-28-2021

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Richtliniensätze (Fortsetzung)

Name Des Richtliniensatzes	Richtlinien	Beschreibung
	Stellen Sie sicher, dass S3-Buckets mit „öffentlichen Zugriff blockieren (Bucket-Einstellungen)“ konfiguriert sind. Stellen Sie sicher, dass keine Sicherheitsgruppen das Eindringen von 0,0.0.0/0 an Remote-Serververwaltungsports zulassen (automatisiert) Stellen Sie sicher, dass kein Zugriffsschlüssel für den Stammanwenderaccount vorhanden ist (automatisiert) Stellen Sie sicher, dass MFA für den Stamm-Anwenderaccount aktiviert ist (automatisiert) Stellen Sie sicher, dass die Protokollierung auf Objektebene für Lese-Ereignisse für den S3-Bucket (automatisiert) aktiviert ist.	
Azure 1.4.0	Stellen Sie sicher, dass die Protokollierung für Azure KeyVault „aktiviert“ ist (automatisiert). Stellen Sie sicher, dass die Web-App die neueste Version der TLS-Verschlüsselung (automatisiert) verwendet. Stellen Sie sicher, dass Vulnerability Assessment (VA) auf einem SQL-Server aktiviert ist, indem Sie ein Speicherkonto (automatisiert) festlegen. Stellen Sie sicher, dass die Speicherprotokollierung für den Blob-Service für Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert) Sicherstellen, dass die Diagnoseeinstellung die entsprechenden Kategorien erfasst (automatisiert) Stellen Sie sicher, dass die VA-Einstellung „Scanberichte senden an“ für einen SQL-Server (automatisiert) konfiguriert ist. Stellen Sie sicher, dass „über Warnungen mit dem folgenden Schweregrad benachrichtigen“ auf „hoch“ festgelegt ist (automatisiert). Stellen Sie sicher, dass „zusätzliche E-Mail-Adressen“ mit einer Sicherheitskontakt-E-Mail (automatisiert) konfiguriert ist. Stellen Sie sicher, dass die Web-App den gesamten HTTP-Datenverkehr in Azure App Service an HTTPS umleitet (automatisiert) Stellen Sie sicher, dass „alle Anwender mit den folgenden Rollen“ auf „Besitzer“ festgelegt ist (automatisiert).	Microsoft Azure Fundamentations-Benchmark v1.4.0 - 11-26-2021

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Governance für Cloud-Konfigurationen Richtliniensätze (Fortsetzung)

Name Des Richtliniensatzes	Richtlinien	Beschreibung
	Stellen Sie sicher, dass die Speicherprotokollierung für den Tabellenservice für die Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert) Stellen Sie sicher, dass die Speicherprotokollierung für Warteschlangenservice für Anforderungen „Lesen“, „Schreiben“ und „Löschen“ aktiviert ist (automatisiert) Stellen Sie sicher, dass „nicht angehängte Datenträger“ mit CMK (automatisiert) verschlüsselt sind. Stellen Sie sicher, dass VA „regelmäßige wiederkehrende Scans“ für jeden SQL-Server auf „ein“ setzt (automatisiert) Stellen Sie sicher, dass der TDE-Schutz von SQL Server mit dem vom Anwender verwalteten Schlüssel (automatisiert) verschlüsselt ist. Stellen Sie sicher, dass der Schlüsselspeicher wiederhergestellt werden kann (automatisiert)	

Bibliothek von Cloud-Aktionen

Verwenden Sie die einsatzbereiten Aktionen und Subflows der Anwendung ServiceNow® Bibliothek von Cloud-Aktionen, um mit den Cloud-Ressourcen der Organisation zu interagieren. Von ServiceNow® ITOM Cloud Accelerate-Funktionen wie Governance für Cloud-Konfigurationen werden diese Aktionen für den Betrieb verwendet.

Erkunden	Einrichten	Entwickeln
Untersuchen Bibliothek von Cloud-Aktionen	• Installieren Bibliothek von Cloud-Aktionen • Einrichten Bibliothek von Cloud-Aktionen für Amazon Web Services (AWS) • Einrichten Bibliothek von Cloud-Aktionen für Microsoft Azure	• Entwicklerschulungen • Entwicklerdokumentation • Bibliothek von Cloud-Aktionen Referenz

Problembehandlung und Hilfe

- Fragen stellen oder beantworten im Bibliothek von Cloud-Aktionen-Forum der ServiceNow Community

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Bibliothek von Cloud-Aktionen erkunden

Machen Sie sich mit dem typischen Bibliothek von Cloud-Aktionen-Workflow und allgemeinen Aufgaben vertraut.

Führen Sie die folgenden Aufgaben aus, um die Bibliothek von Cloud-Aktionen-Aktionen und -Workflows für die Interaktion mit den Cloud-Ressourcen zu verwenden:

1. Installieren Sie Bibliothek von Cloud-Aktionen. Weitere Informationen finden Sie unter Installieren Bibliothek von Cloud-Aktionenan.
2. Zu verwenden Bibliothek von Cloud-Aktionen Für Interaktionen mit Amazon Web Services(AWS) Ressourcen, siehe Einrichten Bibliothek von Cloud-Aktionen für AWSan.
3. Zu verwenden Bibliothek von Cloud-Aktionen Für Interaktionen mit Microsoft Azure Ressourcen, siehe Einrichten Bibliothek von Cloud-Aktionen für Microsoft Azurean.

Bibliothek von Cloud-Aktionen installieren

Sie können die Anwendung Bibliothek von Cloud-Aktionen (sn.itom.cal) installieren, wenn Sie über die Administratorrolle verfügen. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfung des folgenden Elements: Bibliothek von Cloud-Aktionen Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Mit der Anwendung Bibliothek von Cloud-Aktionen werden mehrere Plugins installiert. Weitere Informationen finden Sie unter Bibliothek von Cloud-Aktionen an.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Bibliothek von Cloud-Aktionen (sn.itom.cal).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.

5. Wählen Sie **Installieren** aus.

Bibliothek von Cloud-Aktionen for AWS einrichten

Richten Sie in Bibliothek von Cloud-Aktionen Zugriff auf die AWS-Cloud-Konten (Amazon Web Services) ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf zu konfigurieren AWS Accounts:

- Konfigurieren Sie die permanenten Anmeldeinformationen in ServiceNow AI Platform Um eine Verbindung mit dem eigenständigen herzustellen AWS Accounts (diskrete Accounts). Die Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service-account] enthält die Informationen zum Servicekontotyp wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
- Konfigurieren Sie die Mitgliedskonten so, dass sie für den Zugriff auf das Verwaltungskonto zurückgreifen. Konfigurieren Sie die permanenten Anmeldeinformationen des Verwaltungskontos in diesem Fall auf der ServiceNow AI Platform.
- Konfigurieren Sie die Konten so, dass für den Zugriff ein vertrauenswürdiges Konto verwendet wird (lateraler Zugriff innerhalb derselben AWS-Organisation oder über verschiedene AWS-Organisationen hinweg). Konfigurieren Sie die permanenten Anmeldeinformationen des vertrauenswürdigen Kontos in diesem Fall auf der ServiceNow AI Platform.

Hinweis: Bibliothek von Cloud-Aktionen Verwendet kein MID-serverbasiertes Übernahmerollen-Setup für den Zugriff auf die vertrauenden Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie Anmeldeinformationen für die AWS-Servicekonten.
   a. Navigieren zu **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen**an.
   b. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus.
   c. Füllen Sie die Felder des Formulars aus.

Formular für AWS-Anmeldeinformationen

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die Zugriffsschlüssel-ID, die Sie in der AWS-Verwaltungskonsole erstellt haben
Geheimer Zugangsschlüssel	Der geheime Zugriffsschlüssel, den Sie in der AWS-Verwaltungskonsole erstellt haben

   d. Wählen Sie **Speichern**.

2. Wählen Sie den Anmeldeinformationsalias **sn_itom_cal.Aws_Creds_Alias** aus, oder erstellen Sie einen Anmeldeinformationsalias.
   a. Entsperren Sie den Anmeldeinformationsalias.
   b. Suchen Sie nach einem Anmeldeinformationsalias.
   c. Wählen Sie **Neu**.
   d. Füllen Sie die Felder des Formulars aus.

Formular „Verbindungs- und Anmeldeinformationsalias“

Feld	Beschreibung
Name	Eindeutiger Name des Alias
Typ	Typ des Anmeldeinformationsalias. Wählen Sie in der Dropdown-Liste „Typ“ die Option **Anmeldeinformationen** aus.

   e. Wählen Sie **Absenden** aus.

3. Legen Sie das Feld **Authentifizierungsalgorithmus** auf **AWS Authenticator** fest.
4. Wählen Sie **Absenden** aus.
5. Richten Sie ein AWS-Servicekonto ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**an.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger Name des Servicekontos
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.
Discovery-Anmeldeinformationen	Die für erforderlichen Anmeldeinformationen ServiceNow Anwendungen für den Zugriff auf den Cloud-Account. Sie können die Discovery-Anmeldeinformationen zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf konfigurieren AWS Accounts. ▪ Wenn Sie ein unabhängiges Servicekonto oder ein Verwaltungskonto einrichten, wählen Sie die zugehörigen AWS-Anmeldeinformationen aus. ▪ Um andere zu verwenden AWS Accounts um auf diesen Account zuzugreifen, lassen Sie das Feld leer. Sie müssen beispielsweise nicht angeben AWS Anmeldeinformationen für Accounts, die IAM-Rollen (Identity and Access Management) annehmen, oder Mitgliedsaccounts, die ihren Verwaltungsaccount für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Lassen Sie dieses Feld leer. **Hinweis:** Verwenden Sie für GovCloud die URL https://ec2.us-gov-west-1.amazonaws.com .
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie **AWS-Rechenzentrum** aus.
Rechenzentrums-Discovery-Status	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die AWS-Organisation darstellt, zu der dieses Mitgliedskonto gehört. Dieses Feld wird angezeigt, wenn Sie „AWS-Rechenzentrum“ auswählen. Wenn der Account zu keinem gehört AWS Organisation, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Kontrollkästchen wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option „AWS-Rechenzentrum“ auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. Weitere Informationen zu finden AWS Organisation, siehe AWS Dokumentation an.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

d. Wählen Sie **Absenden** aus.

6. **Wahlweise:** Um ein Verwaltungskonto zum Scannen der Mitgliedskonten der AWS-Organisation zu verwenden, erstellen Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto.

   a. Wahlweise: Wenn Sie nicht die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, konfigurieren Sie ein vertrauendes Konto für Bibliothek von Cloud-Aktionen. Weitere Informationen finden Sie unter Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen Und Bibliothek von Cloud-Aktionen.

   b. Wahlweise: Wiederholen Sie Schritt 6.a für jedes Mitgliedskonto, das über das Verwaltungskonto gescannt werden muss, ohne die OrganizationAccountAccessRole zu verwenden.

   c. Wahlweise: Wenn Sie die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, erstellen Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto.
   Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.

7. **Wahlweise:** Um ein vertrauenswürdiges Konto zum Scannen des vertrauenden Kontos zu verwenden, konfigurieren Sie das vertrauende Konto für Bibliothek von Cloud-Aktionen.
   Das vertrauenswürdige Konto und das vertrauende Konto können sich in verschiedenen AWS-Organisationen, aber auch in derselben AWS-Organisation befinden.

   a. Konfigurieren Sie ein vertrauendes Konto für Governance für Cloud-Konfigurationen.
   Weitere Informationen finden Sie unter Konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen Und Bibliothek von Cloud-Aktionen.

   b. Wiederholen Sie Schritt 7.a für jedes vertrauende Konto, das über das vertrauenswürdige Konto gescannt werden muss.

Bibliothek von Cloud-Aktionen for Microsoft Azure einrichten

Richten Sie in Bibliothek von Cloud-Aktionen Zugriff auf die Microsoft Azure Cloud-Konten ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie Microsoft Azure-Anmeldeinformationen für den Zugriff auf das Microsoft Azure-Konto. Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.
2. Erstellen Sie eine IntegrationHub-Verbindung für Microsoft Azure.
   a. Navigieren zu **Prozessautomatisierung** > **Flow Designer**, Und wählen Sie aus **Integrationen** Registerkarte.
   b. Wählen Sie auf der Kachel **Azure Connection** (Azure-Verbindung) die Option **Verbindung hinzufügen** aus.
   c. Füllen Sie die Felder des Formulars aus.

Formular „Scan-Zeitplan“

Feld	Beschreibung
Verbindungsname	Name der Verbindung
OAuth-Client-ID	Microsoft Azure-Anwendungs-ID
OAuth-Client-Geheimnis	Microsoft Azure-Anwendungsschlüssel
OAuth-Token-URL	Mandanten-ID des Microsoft Azure-Kontos Ersetzen Sie {tenant} durch die Microsoft Azure-Mandanten-ID.

   d. Wählen Sie **OAuth-Token erstellen und abrufen** aus.

Domänentrennung und Cloud-Aktionsbibliothek

Domänentrennung wird in nicht unterstützt Bibliothek von Cloud-Aktionen . Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Zugehörige Informationen

Domänentrennung für Service Provider

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bibliothek von Cloud-Aktionen-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Bibliothek von Cloud-Aktionen.

AWS Aktivieren Sie die EC2-Instanzüberwachungsaktion

Aktion, mit der die Überwachung für die ausgewählte VM-Instanz von Amazon Web Services (AWS) aktiviert wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *`ec2:MonitorInstances`* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Instanzen

Datentyp: *`String`*

AWS-Instanz-ID. Geben Sie die durch Kommata getrennte Liste von AWS-Instanz-IDs ein.

Beispiel: i-1234567890abcdef0, i-1234567761abcdek1

Anmeldeinformationsalias

Datentyp: *`Record`*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *`String`*

Name des Rechenzentrums

MID verwenden

Datentyp: *`True/False`*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *`Record`*

MID-Server für die ausgehenden Anrufe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

AWS Aktion „IAM-Anmeldeprofil abrufen“

Aktion, durch die der Benutzername für den angegebenen Identity Access Management-Benutzer (IAM) von Amazon Web Services (AWS) abgerufen wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *iam:GetLoginProfile* verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

IAM-Account

Datentyp: *String*

AWS IAM-Benutzername.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

AWS Aktion „Bilder auflisten“

Aktion, die die angegebenen Images (AMIs, AKIs und ARIs), die für Sie verfügbar sind, oder alle für Sie verfügbaren Images beschreibt.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:DescribeImages* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Version

Datentyp: *String*

Version der AWS-API.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den Images enthält.

AWS S3-Bucket-Verschlüsselungsaktion platzieren

Aktion, mit der die Standardverschlüsselung und der S3-Bucket-Schlüssel von Amazon Web Services (AWS) für einen vorhandenen Bucket konfiguriert werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *s3:PutEncryptionConfiguration* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Bucket-Name

Datentyp: *String*

Name des AWS S3-Bucket.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *String*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Bucket-Region

Datentyp: *String*

Rechenzentrum, in dem der angegebene AWS S3-Bucket gehostet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Weitergeleitet

Datentyp: *String*

Wenn der AWS S3-Bucket im angegebenen Rechenzentrum nicht verfügbar ist, gibt die Variable *Bucket Region* das Rechenzentrum des AWS S3-Bucket an.

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

AWS Deaktivieren Sie die EC2-Instanzaktion

Aktion, durch die der angegebene virtuelle AWS-Computer (Amazon Web Services) angehalten wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:StopInstances* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Instanzen

Datentyp: *String*

AWS-Instanz-ID. Geben Sie die durch Kommata getrennte Liste von AWS-Instanz-IDs ein.

Beispiel: i-1234567890abcdef0, i-1234567761abcdek1

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False* Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Azure Aktion „virtuelle Maschine deaktivieren“

Aktion, durch die der angegebene virtuelle Microsoft Azure-Computer angehalten wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.Compute/virtualMachines/*/powerOff* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

VM-Bezeichner

Datentyp: *String*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

CAL – AWS S3-Buckets auflisten – Aktion

Aktion, mit der eine Liste aller AWS-Buckets (Amazon Web Services) zurückgegeben wird, die dem authentifizierten Absender der Anforderung gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung `s3:ListBucket` verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den Images enthält, die dem authentifizierten Absender der Anforderung gehören.

CAL – AWS-Liste der VMs – Aktion

Aktion, mit der eine Liste aller virtuellen AWS-Computer (Amazon Web Services) zurückgegeben wird, die zum angegebenen logischen Rechenzentrum gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:DescribeInstances* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Version

Datentyp: *String*

Version der AWS-API.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den VMs enthält, die im angegebenen logischen Rechenzentrum gehostet werden.

CAL – Azure-Liste der VMs – Aktion

Aktion, mit der die Liste der virtuellen Microsoft Azure-Computer zurückgegeben wird, die zum angegebenen logischen Rechenzentrum gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.ResourceGraph/resources* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

Name des Rechenzentrums

Version

Datentyp: *String*

Version der Microsoft Azure-API.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

Konto-ID

Datentyp: *String*

Microsoft Azure-Konto-ID.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den VMs enthält, die im angegebenen logischen Rechenzentrum gehostet werden.

CAL – Azure-VM-IP-Metrik – Aktion

Aktion, mit der die Details der IP-Adresse des angegebenen virtuellen Microsoft Azure-Computers zurückgegeben werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.ResourceGraph/resources* verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Version

Datentyp: *String*

Version der Microsoft Azure-API.

VM

Datentyp: *Array.Object*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das die IP-Adressdetails der angegebenen Microsoft Azure-VM enthält.

CAL – Metrikdaten für Azure-VM-Monitoring – Aktion

Aktion, mit der Überwachungsinformationen für den angegebenen virtuellen Microsoft Azure-Computer zurückgegeben werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.Compute/virtualMachines/{vmName}/instanceView* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Version

Datentyp: *String*

Version der Microsoft Azure-API.

VM

Datentyp: *Object.Array*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *String*

Die Ergebnisvariable enthält die Überwachungsinformationen für die angegebene Microsoft Azure-VM.

CAL – Ganzzahlstrom – Aktion

Aktion, mit der ein Array von Ganzzahlen im angegebenen Bereich zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Start

Datentyp: *Integer*

Eine Ganzzahl, die angibt, an welcher Position begonnen werden soll.

end

Datentyp: *Integer*

Eine Ganzzahl, die angibt, an welcher Stelle gestoppt werden soll. Der zurückgegebene Ganzzahl-Stream enthält nicht die End-Ganzzahl.

step

Datentyp: *Integer*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Ganzzahl, die das Inkrementintervall für den Ganzzahl-Stream angibt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ganzzahlstrom

Datentyp: *Array.Integer*

Ein Array von Ganzzahlen.

AWS IAM-Benutzer deaktivieren – Aktion

Aktion, mit der das Passwort für den angegebenen IAM-Benutzer gelöscht wird, wodurch der Zugriff des Benutzers auf AWS-Services (Amazon Web Services) über die AWS-Managementkonsole beendet wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *iam:DeleteLoginProfile* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentyp: *True/False*

Nicht unterstützt.

IAM-Account

Datentyp: *String*

AWS IAM-Benutzername.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *String*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

error_code

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

error_message

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

CAL – AWS-Bericht zu Anmeldeinformationen erstellen – Subflow

Subflow, mit dem alle Benutzer in Ihrem Konto und der Status ihrer verschiedenen Anmeldeinformationen aufgelistet werden, einschließlich der Passwörter, Zugriffsschlüssel und MFA-Geräte.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigungen `Iam:GetCredentialReport` und `Iam:GenerateCredentialReport` verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: `Record`

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

MID verwenden

Datentyp: `True/False`

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: `Record`

MID-Server für die ausgehenden Anrufe.

API-Version

Datentyp: `String`

Version der AWS-API.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Fehler

Datentyp: `String`

Beschreibung des vom AWS-Endpunkt zurückgegebenen Fehlers.

credential_report_list

Datentyp: `Array.Object`

Komplexes Objekt, das alle Felder des Anmeldeinformationsberichts enthält.

CAL – AWS S3-Verschlüsselung abrufen – Subflow

Subflow, mit dem die Konfiguration der Standardverschlüsselung für einen S3-Bucket von Amazon Web Services (AWS) zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigung `s3:GetEncryptionConfiguration` verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Bucket-Name

Datentyp: *String*

Name des AWS S3-Bucket.

Anmeldeinformationsalias

Datentyp: *String*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Ist verschlüsselt

Datentyp: *True/False*

Verschlüsselungsstatus der AWS-Ressource.

Bucket-Region

Datentyp: *String*

Rechenzentrum des AWS S3-Buckets.

KMS-Master-Schlüssel-ID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentyp: *String*

Kundenseitige Schlüssel-ID des AWS Key Management Service (KMS), die für die Standardverschlüsselung verwendet wird.

Verschlüsselungsalgorithmus

Datentyp: *String*

Serverseitiger Verschlüsselungsalgorithmus, der für die Standardverschlüsselung verwendet wird.

Bucket-Schlüssel aktiviert

Datentyp: *String*

Gibt an, ob von Amazon S3 ein S3-Bucket-Schlüssel mit serverseitiger Verschlüsselung mittels KMS (SSE-KMS) für neue Objekte im Bucket verwendet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

CAL – Anmeldeinformationsalias auflösen – Subflow

Subflow, mit dem der Anmeldeinformationsalias für die genannten Anmeldeinformationen zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Service-Account

Datentyp: *Record*

Servicekonto, für das ein geeigneter Anmeldeinformationsalias gesucht wird.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Anmeldeinformationsalias

Datentyp: *Record*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Fehler

Datentyp: *String*

Wenn von der zugrunde liegenden CAL-Aktion (Bibliothek von Cloud-Aktionen) kein Anmeldeinformationsalias zurückgegeben wird, wird eine Fehlermeldung zurückgegeben, in der der Grund für den Fehler erläutert wird. Die Fehlervariable enthält die Fehlermeldung, die von der zugrunde liegenden CAL-Aktion zurückgegeben wird.

CAL – MID auflösen – Subflow

Subflow, mit dem basierend auf den angegebenen MID-Server-Auswahlkriterien ein geeigneter MID-Server zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Service-Account

Datentyp: *Record*

Servicekonto, für das ein geeigneter MID-Server gesucht wird.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

MID-Server

Datentyp: *Record*

Aufgelöster MID-Server.

Fehler

Datentyp: *String*

Fehler, der bei der Identifizierung des MID-Server s aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAL – AWS S3 ACL abrufen – Subflow

Subflow, mit dem die Details der Zugriffssteuerungsliste (Access Control List, ACL) für den angegebenen S3-Bucket von Amazon Web Services (AWS) abgerufen werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub Anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Anwenderzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigung `s3:GetBucketAcl` verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Bucket-Name

Datentyp: `String`

Name des AWS S3-Bucket.

MID verwenden

Datentyp: `True/False`

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: `Record`

MID-Server für die ausgehenden Anrufe.

Anmeldeinformationsalias

Datentyp: `Record`

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: `True/False`

Serverautorisierungsstatus des Anrufs.

- `True`: Anruf wurde vom Server autorisiert
- `False`: Anruf wurde vom Server nicht autorisiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bucket-Region

Datentyp: *String*

Rechenzentrum, in dem der angegebene AWS S3-Bucket gehostet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Besitzer Schreiben

Datentyp: *True/False*

Der Bucket-Besitzer kann in den Bucket schreiben.

Bucket-Besitzer Vollzugriff

Datentyp: *True/False*

Der Besitzer hat alle Berechtigungen für den Bucket.

Besitzerliste

Datentyp: *True/False*

Der Bucket-Besitzer kann den Inhalt des Buckets auflisten.

Öffentlicher Schreibzugriff

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann in den Bucket schreiben.

Öffentliche Auflistung

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann den Inhalt des Buckets auflisten.

Öffentliche vollständige Kontrolle

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) verfügt über alle Berechtigungen.

Authentifizierte Anwender für Schreiben

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können in den Bucket schreiben.

Anwender mit vollem Zugriff authentifizieren

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) verfügen über alle Berechtigungen für den Bucket.

Besitzer-Lese-ACL

Datentyp: *True/False*

Der Besitzer des Buckets kann die Bucket-ACL lesen.

Besitzer-Schreib-ACL

Datentyp: *True/False*

Der Besitzer des Buckets kann die Bucket-ACL schreiben oder aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffentlicher Lesezugriff ACL

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann die Bucket-ACL lesen.

Öffentlicher Schreibzugriff ACL

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann die Bucket-ACL schreiben oder aktualisieren.

Authentifizierte Benutzer für ACL Lesen

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können die Bucket-ACL lesen.

Authentifizierte Anwender für ACL Schreiben

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können die Bucket-ACL schreiben oder aktualisieren.

Anwenderliste authentifizieren

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können den Inhalt des Buckets auflisten.

Verantwortlichen-ID

Datentyp: *String*

Kanonische Benutzer-ID des AWS-Kontos.

Anzeigename des Besitzers

Datentyp: *String*

Anzeigename des Ressourcenbesitzers.

Bei der Verbundanmeldung wird vom Subflow kein Anzeigename des Besitzers zurückgegeben.

Cloud-Profile mit minimalen Berechtigungen für Bibliothek von Cloud-Aktionen-Aktionen und -Subflows

Sie benötigen entsprechende Cloud-Berechtigungen, um die Bibliothek von Cloud-Aktionen-Aktionen und -Subflows ausführen zu können. Bearbeiten Sie die JSON-Datei des Cloud-Berechtigungsprofils entsprechend den Anforderungen Ihrer Organisation.

AWS-Profil (Amazon Web Services) mit minimalen Berechtigungen

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
   "iam:GenerateCredentialReport",
   "s3:GetEncryptionConfiguration",
```

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "ec2:DescribeInstances",
  "s3:ListBucketVersions",
  "ec2:DescribeRegions",
  "s3:ListBucket",
  "iam:GetCredentialReport",
  "iam:DeleteLoginProfile",
  "ec2:MonitorInstances",
  "iam:GetLoginProfile",
  "ec2:DescribeImages",
  "s3:PutEncryptionConfiguration",
  "ec2:StopInstances",
  "s3:GetBucketAcl"
 ],
 "Resource": "*"
}]
}
```

Microsoft Azure-Profil mit minimalen Berechtigungen

```
{
 "properties": {
  "roleName": "CCGAzureMinimalPermission",
  "description": "Grants access to scan compute resources from the Azure subscription",
  "assignableScopes": [
   "/subscriptions/${subscription_id}"
  ],
  "permissions": [{
   "actions": [
    "Microsoft.ResourceGraph/resources/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/*/powerOff"
   ],
   "notActions": [],
   "dataActions": [],
   "notDataActions": []
  }]
 }
}
```

ITOM Cloud Accelerate-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von ITOM Cloud Accelerate.

Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate

Tabellen, die die mit installierten Plugins oder Anwendungen auflisten ITOM Cloud Accelerate Anwendungen. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Cloud-Services-Katalog

Die CSK Das Inhaltspaket-Plugin (sn_itom_csc_cp) stellt den erforderlichen vordefinierten Inhalt für bereit Cloud-Services-Katalog Anwendung. Dieser Inhalt enthält Governance-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinien und -Aktionen zur Bereitstellung eines End-to-End-gesteuerten Bereitstellungs-Workflows.

Mit installierte Plugins oder Anwendungen Cloud-Services-Katalog(sn_itom_csc)

Plugin- oder Anwendungsname	Beschreibung
Cloud Provisioning and Governance: Terraform Connector (sn_CMP_terraform)	Integriert Terraform Open Source, Terraform Enterprise, Und Terraform Cloud Mit ITOM Cloud Provisioning and Governance(CPG), mit der Sie Services in mehreren Clouds bereitstellen und verwalten können AWS, Azure, GCP, Und VMware. Die Terraform Vorlagen sind als Cloud-Vorlagenkataloge codiert, die Sie zur Bereitstellung von Cloud-Ressourcen verwenden können.
Cloud Operations Workspace (sn_Cloud_OPS_WS)	Bietet eine umfassende Lösung zur Verwaltung der Cloud-Vorgänge Ihrer Organisation.
Cloud Provisioning and Governance (com.snc.cloud.mgmt)	Bietet eine einzige Schnittstelle für den Zugriff auf Cloud-Ressourcen, die Veröffentlichung von Cloud-Angeboten in einem Katalog und die Verwaltung der Verwendung dieser Ressourcen.
Geführtes Setup (sn_ads_Setup)	Ermöglicht Ihnen, die anfängliche Konfiguration eines Produkts oder einer Anwendung zu durchlaufen, die eine bereitstellt Geführtes Setup Modul. Geführtes Setup Unterstützt Sie bei der Planung des Rollouts eines Produkts und der Durchführung der Basiskonfiguration, die für den Go-Live erforderlich ist.
ITOM/OT SU-Lizenzierung (sn_itom_Lizenzierung)	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.

Mit installierte Plugins oder Anwendungen CSK Inhaltspaket (sn_itom_csc_cp)

Plugin- oder Anwendungsname	Beschreibung
Cloud-Services-Katalog (sn_itom_csc)	Bietet eine vereinfachte Schnittstelle zur Automatisierung des Cloud-Managements und zum Zugriff auf Cloud-Ressourcen. Mit der Anwendung können Sie Cloud-Angebote in einem Katalog veröffentlichen und die Nutzung und den Lebenszyklus dieser Ressourcen verwalten.
ServiceNow IntegrationHub-Aktionsschritt – SSH (com.Glide.Hub.action_step.ssh)	Der SSH-Schritt führt über einen ServiceNow® MID-Server SSH-Befehle für ein externes *nix-System aus. Der Schritt speichert auch Skripts und Befehle für die *nix-Systeme.
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CCG Inhaltspaket (sn_itom_ccg_cp)	Stellt optional vor bereit Definierter Inhalt für Governance für Cloud-Konfigurationen Anwendung Z. B. Richtlinien, Ressourcensammler, Konfigurations-Sammler und Korrekturaktionen.
Flow Designer-Aktionsschritt – E-Mail (com.Glide.Hub.action_STEP.email)	Stellt den Schritt „E-Mail senden“ bereit, um eine E-Mail an angegebene Anwender oder Gruppen als Aktion in einem Flow zu senden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertung der Cloud-Migration

Mit installierte Plugins oder Anwendungen Bewertung der Cloud-Migration(sn_Cloud_Migration)

Plugin- oder Anwendungsname	Beschreibung
ITOM/OT SU-Lizenzierung (sn_itom_Lizenzierung)	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Cloud-Migrationsbasis (com.sn_Cloud_mig_Base)	Ein Basis-Plugin zur Unterstützung von Bewertung der Cloud-Migration Anwendung.

Governance für Cloud-Konfigurationen

Die CCG Inhaltspaket Plugin (sn_itom_ccg_cp) bietet optional Pre Definierter Inhalt für Governance für Cloud-Konfigurationen Anwendung wie Richtlinien, Ressourcensammler, Konfigurationssammler und Korrekturaktionen.

Mit installierte Plugins oder Anwendungen Governance für Cloud-Konfigurationen(sn_itom_ccg)

Plugin- oder Anwendungsname	Beschreibung
Bibliothek von Cloud-Aktionen (sn_itom_CAL)	Stellt vordefinierte Aktionen und Sublows bereit, um die Interaktion mit den Cloud-Ressourcen Ihrer Organisation zu ermöglichen. ServiceNow® ITOM Cloud Accelerate Funktionen wie Governance für Cloud-Konfigurationen Verwenden Sie diese Aktionen, um zu arbeiten.

Mit installierte Plugins oder Anwendungen CCG Inhaltspaket(sn_itom_ccg_cp)

Plugin- oder Anwendungsname	Beschreibung
Governance für Cloud-Konfigurationen (sn_itom_ccg)	Überprüft die Konfigurationseinstellungen von Cloud-Ressourcen in Ihrer Organisation anhand einer Reihe von Richtlinien, um Verstöße zu identifizieren. Nachdem der Verstoß identifiziert wurde, können Sie ihn mithilfe von Korrekturworkflows verringern.

Bibliothek von Cloud-Aktionen

Mit installierte Plugins oder Anwendungen Bibliothek von Cloud-Aktionen(sn_itom_CAL)

Plugin- oder Anwendungsname	Beschreibung
ITOM/OT SU-Lizenzierung (sn_itom_Lizenzierung)	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Bibliothek von Cloud-Aktionen(sn_itom_CAL) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Flow Designer-Aktionsschritt – Payload Builder (com.Glide.Hub.action_STEP.Payload)	Ermöglichen Sie Aktionsdesignern, Name-/Wert-Paare mit dynamischen Daten einfach in JSON- und XML-Nutzlasten zu erstellen.
ServiceNow IntegrationHub-Aktionsschritt – Verbindungsinformationen abrufen (com.Glide.Hub.action_STEP.get_connection_info)	Stellt Details zu Verbindung und Anmeldeinformationen von einem anderen Schritt wie einem REST-Schritt (Representational State Transfer) zu anderen Schritten in Ihrer Aktion bereit.
ServiceNow IntegrationHub-Aktionsschritt – XML-Parser (com.Glide.Hub.action_STEP.xmlparser)	Aktiviert den XML-Parser-Aktionsschritt in Flow Designer.
ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime)	Ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows.
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Flow Designer-Aktionsschritt – Skript auf MID (com.glide.hub.action_step.script_mid)	Stellt einen Aktionsschritt zum Ausführen von anwenderdefiniertem JavaScript innerhalb einer wiederverwendbaren Aktion für einen MID-Server bereit.
ServiceNow IntegrationHub-Aktionsschritt – REST (com.Glide.Hub.action_STEP.Rest)	Aktiviert den REST-Aktionsschritt in Flow Designer.
ServiceNow IntegrationHub-Aktionsvorlage – Datenstrom (com.Glide.Hub.action_type.datastream)	Senden Sie REST-, SOAP- oder JDBC- Anforderungen von Flow Designer an APIs, die einen Stream von Antwortdaten größer als 10 MB oder paginierte Ergebnisse zurückgeben. Parsen Sie Streamdaten in eine Reihe komplexer Objektausgaben, und verwenden Sie die Datenpillen in anderen Aktionen in einem Flow.

Cloud Account Management

Mit installierte Plugins oder Anwendungen Cloud Account Management(sn_Cloud_acct_mgt)

Plugin- oder Anwendungsname	Beschreibung
Muster für Discovery und Service-Mapping (sn_itom_pattern)	Stellt die neuesten im ServiceNow Store veröffentlichten Versionen von Muster für Discovery und Service-Mapping bereit. ServiceNow veröffentlicht im ServiceNow® Store jeden Monat neue Muster, damit Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann.
ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime)	Ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Cloud Account Management(sn_Cloud_acct_mgt) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
ServiceNow IntegrationHub-Aktionsschritt – Verbindungsinformationen abrufen (com.Glide.Hub.action_STEP.get_connection_info)	Stellt Details zu Verbindung und Anmeldeinformationen von einem anderen Schritt wie einem REST-Schritt (Representational State Transfer) zu anderen Schritten in Ihrer Aktion bereit.
ServiceNow IntegrationHub-Aktionsvorlage – Datenstrom (com.Glide.Hub.action_type.datastream)	Senden Sie REST-, SOAP- oder JDBC- Anforderungen von Flow Designer an APIs, die einen Stream von Antwortdaten größer als 10 MB oder paginierte Ergebnisse zurückgeben. Parsen Sie Streamdaten in eine Reihe komplexer Objektausgaben, und verwenden Sie die Datenpillen in anderen Aktionen in einem Flow.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.
Flow Designer-Aktionsschritt – Payload Builder (com.Glide.Hub.action_STEP.Payload)	Ermöglichen Sie Aktionsdesignern, Name-/Wert-Paare mit dynamischen Daten einfach in JSON- und XML-Nutzlasten zu erstellen.
ServiceNow IntegrationHub-Aktionsschritt – REST (com.Glide.Hub.action_STEP.Rest)	Aktiviert den REST-Aktionsschritt in Flow Designer.
ServiceNow IntegrationHub-Aktionsschritt – JSON Parser (com.Glide.Hub.action_STEP.jsonparser)	Identifizieren Sie strukturierte Daten aus einer JSON-Nutzlast, ohne ein Skript schreiben zu müssen. Ordnen Sie eingehenden JSON-Inhalt einer komplexen Objektausgabe zu, die Sie in anderen Schritten oder Aktionen verwenden können. Zur Laufzeit füllen Werte aus einer JSON-Nutzlast die komplexe Objektausgabe.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit aktivierte Plugins ITOM-Optimierung
- Mit Now Assist für ITOM installierte Anwendungen

ITOM-Optimierung

Die Anwendung IT Operations Management (ITOM) Optimization bietet Automatisierung für die Cloud-Workflows, die während ihres gesamten Lebenszyklus zur Verwaltung der Cloud-Ressourcen verwendet werden. Sie ermöglicht eine zertifizierte und unternehmenskonforme Cloud-Bereitstellung, Kostentransparenz und andere Cloud-Managementprozesse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen von ITOM-Optimierung

Die Funktionen von ITOM-Optimierung bieten einen integrierten, serviceorientierten Ansatz, der die Qualität von Business Services maximiert, effiziente Prozesse fördert und eine robuste Governance gewährleistet.

Cloud Provisioning and Governance

Die ServiceNow® Cloud Provisioning and Governance (CPG) dient als einheitliche Schnittstelle für den Zugriff auf Cloud-Ressourcen, die Bereitstellung von Cloud-Angeboten für einen Katalog und die Überwachung der Ressourcennutzung. Diese Anwendung wird in die Anwendung Cloud-Services-Katalog umgewandelt, die eine verfeinerte und optimierte Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen bietet.

ITOM-Optimierung Lizenzierung

Bei der für ServiceNow AI Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Optimierung Anwendungen. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Guided Setup zum Implementieren der IT Operations Management-Anwendungen

Das Guided Setup von IT Operations Management bietet eine Reihe von Aufgaben, die Sie beim Konfigurieren von IT Operations Management-Anwendungen in Ihrer ServiceNow-Instanz unterstützen. Zum Öffnen IT Operations Management Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Nächste Schritte

- Um die Liste der Plugins zu finden, die Sie mit aktivieren IT Operations Management, Siehe Mit aktivierte Plugins ITOM-Optimierung.
- Ausführliche Informationen zu Cloud Provisioning and Governance finden Sie unter Cloud Provisioning and Governance.

ITOM-Optimierung – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von ITOM-Optimierung.

Mit aktivierte Plugins ITOM-Optimierung

Tabelle, die die Plugins auflistet, die mit aktiviert sind ITOM-Optimierung Anwendung Cloud Provisioning and Governance. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit aktivierte Plugins Cloud Provisioning and Governance(Com.snc.Cloud.mgmt)

Plugin-Name	Beschreibung
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Verwaltung der Cloud-Konfiguration (com.snc.config.mgmt)	Ein Konfigurationsmanagement-Framework, das API-Implementierungen zur Integration mit Konfigurationsmanagement-Lieferanten bereitstellt.
Orchestration (com.snc.runbook_automation)	Automatisiert häufig wiederholte manuelle Vorgänge wie Bereitstellungen, Konfigurationen und Informationserfassung. Orchestration Verwendet Workflow und MID-Server Technologien, mit denen Aktivitäten Befehle auf Systemen in Ihrem Unternehmensnetzwerk ausführen können.
Serviceportal – Kern (com.glide.service-portal)	Ein Portal-Framework, mit dem Administratoren eine mobile Selfservice-Experience für Anwender erstellen können.
ITOM-Optimierung Lizenzierung (com.sn_itom_opt_Lizenzierung)	Eine Proxy-Anwendung, mit der Sie alle Anwendungen im Zusammenhang mit der Optimierung installieren können. Sobald Sie die Optimierungslizenz erworben haben, können Sie diese Proxy-Anwendung installieren, mit der Sie jede Anwendung installieren können, die Teil der Optimierungslizenz ist.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit Now Assist für ITOM installierte Anwendungen

MID-Server-Konfiguration und Ausnahmebehandlung

Sie können einen MID-Server mit zusätzlichen Konfigurationsparametern konfigurieren oder eine neue MID-Server-Eigenschaft erstellen, um das Standardverhalten zu ändern.

Mit einer Systemeigenschaft „mid.property.probe.api.timeout.minutes' können Sie entscheiden, wie lange der MID-Server warten soll, bevor bei der Bereitstellung ein Zeitüberschreitungsfehler ausgelöst wird.

Dies Cloud Provisioning and Governance Die MID-Server-Eigenschaft mit den Parametern „Name“ und „Wert“ behandelt die Zeitüberschreitungsausnahme.

Siehe MID Server-Eigenschaften Weitere Informationen zum Erstellen einer MID-Server-Eigenschaft.

ITOM-Transparenz

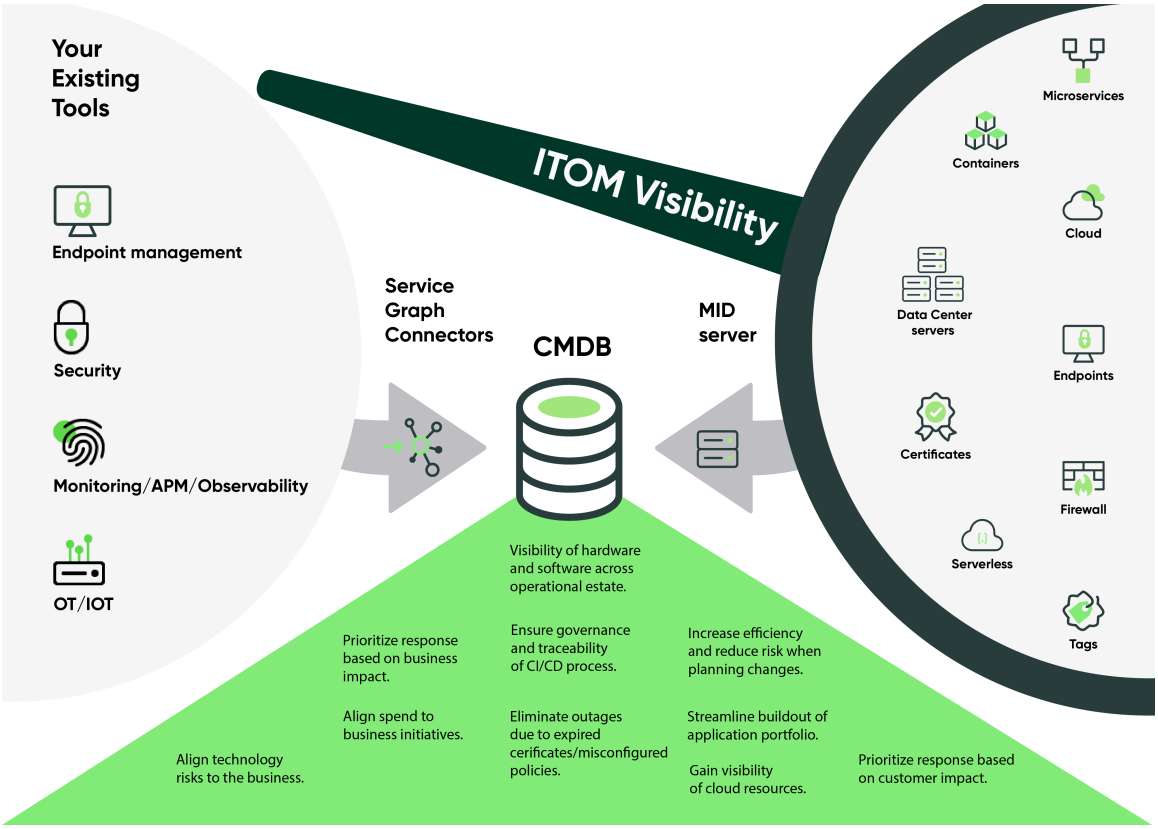
Das ProduktServiceNow® ITOM-Transparenz besteht aus ServiceNow® Discovery, ServiceNow® Service-Mapping, Zertifikatsbestand-Management, Service Graph Connectors, CMDB mit mehreren Quellen sowie Firewall-Audits und Reporting. Discovery und Service-Mapping vermitteln Ihnen zusammen eine einheitliche, verbundene Ansicht Ihres gesamten IT-Netzwerks und der von ihm unterstützten Services.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM-Transparenz – Benutzer

ITOM-Transparenz versetzt IT-Abteilungen von Unternehmen und Cloud-Unternehmen, die Platform-as-a-Service anbieten, in die Lage, ihre IT-Ressourcen zu erkennen.

ServiceNow® Configuration Management Database (CMDB) ist nicht nur einfach ein operatives Tool, sondern in der heutigen IT-Landschaft eine strategische Notwendigkeit. Die Gewährleistung einer genauen und vollständigen CMDB stellt die Grundlage zur Durchführung kritischer Services dar und bietet IT-Abteilungen eine Reihe von wichtigen Ergebnissen.



Die von ITOM-Transparenz erfassten Daten bilden die Grundlage für den Betrieb der folgenden Geschäftsbereiche und Produkte der ServiceNow AI Platform:

ITOM-Integrität

Verwenden Sie ITOM-Integrität, um die Integrität von Services in Ihrer Organisation nachzuverfolgen und zu verwalten. Von ITOM-Integrität werden Warnmeldungen zu Infrastruktur-Events gesammelt, die von Überwachungs-Tools von Drittanbietern erfasst wurden. Anschließend nutzt das Tool von Discovery gesammelte IT-bezogene Informationen, um Konfigurationselementen Warnungen zuzuordnen. Basierend auf den erfassten Informationen stellt ITOM-Integrität Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen. Sie können ITOM-Integrität auch verwenden, um Ihre IT-Infrastruktur proaktiv zu analysieren und so Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von ausgereiftem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur werden von der Anwendung automatisch dynamische Schwellenwerte ermittelt und Anomalien identifiziert, die auf potenzielle Serviceausfälle hindeuten.

ITOM-Optimierung

ITOM-Optimierung erhalten Sie Tools für die Bereitstellung von Private und Public Cloud-Infrastrukturen und -Services sowie für eine konsistente Verwaltung und Kostentransparenz. Die Anwendung Cloud-Einblicke , die im ServiceNow Store verfügbar ist, hilft Ihnen bei der Analyse des gesamten Spektrums der mit Cloud-Assets zusammenhängenden Kosten, sodass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie Möglichkeiten zur Kosteneinsparung und Betriebsoptimierung erkennen und entsprechende Maßnahmen ergreifen können.

Software Asset Management

Verschaffen Sie sich einen Überblick über die in Ihrer IT-Umgebung ausgeführten Software. Software Asset Management funktioniert zusammen mit der durch ITOM-Transparenz unterstützten CMDB. Verwenden Sie Software Asset Management, um Konfigurationen nachzuverfolgen, die sich auf die Nutzung von Softwarelizenzen in Ihren IT-Umgebungen und im Rechenzentrum auswirken.

Kundenservice-Management

Diagnostizieren Sie Probleme im Zusammenhang mit der IT-Infrastruktur, und beheben Sie sie auf effiziente Weise mit mithilfe von von ITOM-Transparenz bereitgestellten Echtzeitdaten.

IT Service Management

Verlassen Sie sich auf die von ITOM-Transparenz erkannte IT-Infrastruktur, um Services für Ihre Benutzer zu verwalten und bereitzustellen. Zeigen Sie Changes und Incidents an, die durch IT Service Management-Anwendungen in ITOM-Transparenz-Servicezuordnungen erstellt und verwaltet werden.

Strategisches Portfoliomanagement

Verwenden Sie die durch ITOM-Transparenz erfassten Daten, um umfassende Kenntnisse über die in Ihrem Unternehmen verwendeten Anwendungen zu erlangen.

Security Operations

Zeigen Sie Security Incidents im Kontext von ITOM-Transparenz an, um herauszufinden, welche Anwendungsservices gefährdet sind. Nutzen Sie diese Informationen, um Bedrohungen je nach Auswirkungen auf Ihr Unternehmen zu priorisieren und zu beheben.

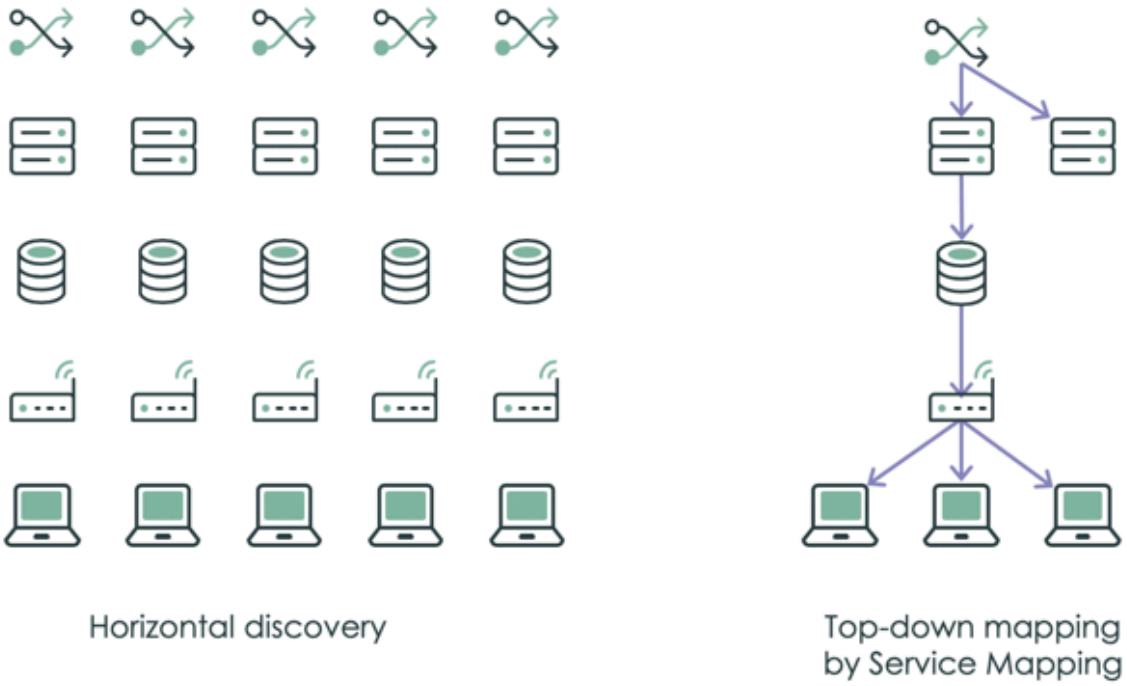
ITOM-Transparenz – Verwendung

Die Discovery-Funktion bietet eine replizierbare und zuverlässige Methode zur Identifizierung der IT-Infrastruktur von Unternehmen. Discovery kann Computer, Server, Software, Drucker, Router und Switches erkennen. Außerdem werden IP-fähige Geräte und die darauf ausgeführten Anwendungen sowie Ressourcen verschiedener Cloud-Anbieter und TLS-Zertifikate gefunden. Diese Methode wird in der Regel als horizontale Erkennung bezeichnet. Bei der horizontalen Erkennung werden keine Verbindungen zwischen Geräten und Anwendungen berücksichtigt.

Die Service-Mapping-Funktion ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Mithilfe der Zuordnung von oben nach unten können Sie sofort die Auswirkungen eines problematischen Objekts auf den Rest des Anwendungsservicevorgangs erkennen. Anwendungsservicezuordnungen zeigen Infrastrukturobjekte und semantische Verbindungen zwischen ihnen. Service-Mapping generiert Anwendungsservicezuordnungen regelmäßig neu, damit sie jederzeit aktuell und relevant sind. Alle fehlerhaften Objekte werden zusammen mit den betroffenen Geräten und Anwendungen angezeigt und geben so einen visuellen Überblick über den Status des Anwendungsservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Horizontale Erkennung und Erkennung von oben nach unten – Ergebnisse im Vergleich



Funktionsweise von ITOM-Transparenz

Discovery Kann Skripts verwenden, um Daten auf einem Host zu erfassen und zu verarbeiten und dann zu aktualisieren CMDB. Skripts, die CIs in Ihrem Netzwerk erkunden oder untersuchen, werden als Probes bezeichnet. Sensoren entsprechen den Skripts, die die von den Probes zurückgegebenen Daten analysieren. Darüber hinaus setzt Discovery Erkennungsmuster ein. Ein Muster entspricht einer Folge von Vorgängen, die zum Erkennen von Attributen von Geräten sowie von Anwendungen und (bei Verwendung von Service-Mapping) deren ausgehenden Verbindungen dienen.

Service-Mapping kann unterschiedliche Methoden zum Erstellen von Anwendungsservices bereitstellen. Erkennungsmuster sind die von Service-Mapping hauptsächlich verwendete Methode. Sie können jedoch auch Anwendungsservices mithilfe von Tags sowie Datenverkehrverbindungen zwischen Geräten und Anwendungen zuordnen. Weitere Informationen finden Sie unter Richtige Methode zur Zuordnung von Anwendungsservices auswählen.

ITOM-Transparenz Lizenzierung

Bei der für ServiceNow AI Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Transparenz Anwendungen. Lizenzierungsoptionen können je nach Vereinbarung Ihrer Organisation variieren. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Was Sie wissen sollten, bevor Sie beginnen

ITOM-Transparenz ist verfügbar durch die Aktivierung des Plugins „Discovery“ (com.snc.discovery) und des Plugins „Service-Mapping“ (com.snc.service-mapping), die ein ITOM-Transparenz-Abonnement erfordern. Nähere Einzelheiten erfahren Sie unter Discovery anfordern und Service-Mapping anfordern. Für „vollständig“ ITOM-Transparenz Funktionalität installieren Sie die neueste ITOM-Transparenz Anwendungen aus dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Store. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den „Release-Informationen zum Versionsverlauf“ im ServiceNow Store.

Definieren Sie Benutzer, und konfigurieren Sie Anmeldeinformationen, um ITOM-Transparenz Zugriff auf Anwendungen und Geräte in Ihrem Unternehmensnetzwerk zu ermöglichen. Details finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Discovery

ServiceNow Discovery Ist ein automatisierter Prozess, der alle Komponenten in der IT-Infrastruktur kontinuierlich scannt und identifiziert. Es spielt eine entscheidende Rolle bei der Aufrechterhaltung einer genauen und aktuellen CMDB mit mehreren Quellen Mit den gefundenen Informationen.

https://player.vimeo.com/video/1092921849?h=0dcb800150&badge=0&autopause=0&player_id=0&app_id=58479

DiscoveryIst als separates Abonnement vom Rest des verfügbar ServiceNow AI Platform. Details siehe Discovery anfordern.

Discovery Unterstützt Datenbankverschlüsselung und Datenträgerverschlüsselung. Details siehe Datenbankverschlüsselung .

Erste Schritte

Einführung

- Zurich
- Discovery erkunden

Einrichten

- Discovery anfordern
- Discovery einrichten
- MID Server-Installation
- Anmeldeinformationen erstellen und testen
- Migrieren Sie von CAPI zu Mustern

konfigurieren

- Discovery konfigurieren
- Discovery-Eigenschaften
- Discovery-Verhalten erstellen
- Discovery-CI-Klassifizierung erstellen
- Discovery-Prozessklassifizierung erstellen

Verwenden

- Horizontale Erkennung planen
- Schnell-Discovery ausführen
- Discovery-Status
- Erkennungsergebnisse validieren

Integrieren und entwickeln

- Aktivieren Sie geplante SCCM Asset Intelligence-Importe
- Discovery-APIs auf der ServiceNow® Developer Site

Problembehandlung und Hilfe

- Monitoring von Erkennungen und Problemlösung
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Fragen im ITOM-Forum stellen oder beantworten
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cloud-Discovery erkunden
- Zertifikatsbestand-Management

Discovery erkunden

Discovery Sucht nach Computern, Servern, Druckern, einer Vielzahl von IP-fähigen Geräten und den darauf ausgeführten Anwendungen. Es kann dann die CIs in Ihrer CMDB mit den gesammelten Daten aktualisieren.

Horizontale Erkennung und Erkennung von oben nach unten

Es gibt zwei Arten von Erkennung:

Horizontale Erkennung

Die horizontale Erkennung ist eine Technik, die Discovery verwendet, um Ihr Netzwerk zu scannen, Computer und Geräte zu erkennen und dann die CMDB mit den gefundenen CIs zu füllen. Bei der horizontalen Erkennung werden direkte Beziehungen zwischen CIs erstellt, zum Beispiel eine Beziehung vom Typ Wird ausgeführt auf zwischen dem CI einer Anwendung und dem CI des tatsächlichen Computers, auf dem die Anwendung ausgeführt wird. Die horizontale Erkennung erkennt keine Business Services und erstellt keine Beziehungen zwischen CIs basierend auf dem Business Service, in dem sie sich befinden.

Erkennung von oben nach unten

Die Erkennung von oben nach unten ist eine Technik, die von Service Mapping verwendet wird, um CIs zu finden und zuzuordnen, die Teil von Business Services wie einem E-Mail-Service sind. Beispielsweise kann die Erkennung von oben nach unten einen Business Service für Websites zuordnen, indem die Beziehungen zwischen einem Apache Tomcat-Webserverdienst, einem Windows-Server und der MSSQL-Datenbank angezeigt werden, in der die Daten für den Business Service gespeichert werden.

Normalerweise arbeiten Service-Mapping und Discovery zusammen und führen zuerst die horizontale Erkennung durch, um CIs zu finden, und anschließend die Erkennung von oben nach unten, um die Beziehungen zwischen Business Services herzustellen, die Sie kennen müssen.

Probes, Sensoren und Muster

Discovery verwendet die folgenden Komponenten für die Suche nach CIs:

Sonden und Sensoren

Probes und Sensoren sind Skripts, die Daten auf einem Host erfassen und verarbeiten und anschließend die CMDB aktualisieren. Genauer gesagt: Probes untersuchen die CIs in Ihrem Netzwerk, und Sensoren analysieren die Daten, die von den Probes zurückgegeben werden. Standardmäßig werden mehrere Probes und Sensoren bereitgestellt, die von Ihnen angepasst werden können, um nach anderen Informationen zu suchen. Sie können Probes und Sensoren aber auch selbst erstellen. Sie können auch mehrere Parameter konfigurieren, um das Verhalten einer bestimmten Probe bei jeder Auslösung zu steuern.

Muster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster entsprechen wie Probes und Sensoren einer Reihe von Vorgängen, die Daten auf einem Host erfassen, verarbeiten und die CMDB aktualisieren. Muster unterscheiden sich von Probes und Sensoren dadurch, dass sie in NDL (Neebula Discovery Language) anstatt in JavaScript geschrieben sind und in den späteren Phasen des horizontalen Erkennungsprozesses in Aktion treten. Es werden Standardmuster bereitgestellt, Sie können Muster jedoch auch mit dem Musterdesigner anpassen oder erstellen.

Phasen der horizontalen Erkennung

Die Phasen der horizontalen Erkennung lauten:

Discovery Folgt diesen Phasen:

Scanvorgang

DiscoverySendet eine Probe namens *Shazzam* An das Netzwerk, um zu sehen, ob häufig verwendete Ports offen sind und ob diese Ports auf Abfragen reagieren können. Wenn Shazzam beispielsweise ein Gerät findet, das auf Port 135 antwortet, DiscoveryWeiß, dass es sich um einen Windows-Server handelt.

Klassifizierung

Wenn DiscoveryFindet Geräte oder Computer und sendet zusätzliche Probes, um den Gerätetyp oder das Betriebssystem auf dem Gerät zu finden. Beispiel: DiscoverySendet die WMI-Probe an einen Windows-Computer, um das Windows 2012-Betriebssystem zu erkennen. Dann DiscoveryVerwendet aufgerufene Datensätze *Klassifizierer* , Die die Auslöserprobe oder Probes angeben, die in den nächsten zwei Phasen ausgeführt werden. Wenn Sie Muster verwenden, gibt der Klassifizierer eine Auslöserprobe an, die wiederum ein Muster startet.

Identifizierung

DiscoveryVersucht, weitere Informationen über das Gerät zu sammeln und dann zu bestimmen, ob ein CI für das Gerät in der CMDB vorhanden ist. DiscoveryVerwendet dann zusätzliche Probes, Sensoren und Bezeichner, um vorhandene CIs in der CMDB zu aktualisieren oder neue zu erstellen. *Kennungen*, auch als Identifikationsregeln bezeichnet, geben die Attribute an, die die Sonden beim Abgleichen von Daten mit den CIs in der CMDB betrachten. Wenn Sie Muster verwenden, DiscoveryVerwendet die entsprechende Identifizierungsregel für den im Muster angegebenen CI-Typ.

Durchsuchen

Der Bezeichner startet zusätzliche im Klassifizierer konfigurierte Sonden. Diese Probes sind speziell als Explorationsprobes konzipiert, um zusätzliche Informationen über das Gerät zu sammeln, z. B. die Anwendungen, die es ausführen, und zusätzliche Attribute wie Arbeitsspeicher, Netzwerkkarten und Treiber. DiscoveryErstellt dann Beziehungen zwischen Anwendungen und Geräten und zwischen Anwendungen. Wenn Sie Muster verwenden, führen die Vorgänge im Muster die Untersuchung des CI durch.

Kommunikation während der Erkennung über MID Server

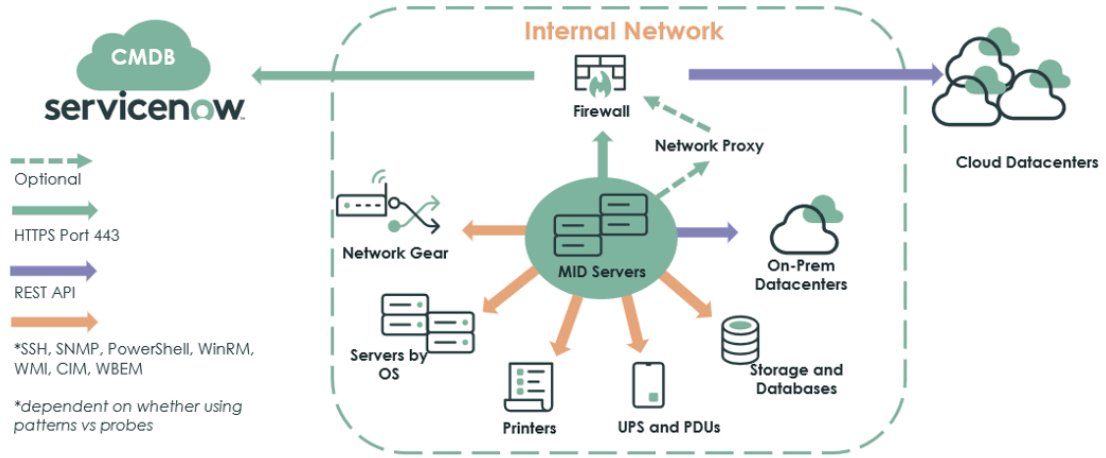
Ein MID Server , der eine Instanz ständig nach auszuführenden Probes abfragt, führt die Anweisungen in der Probe oder in dem von der Probe angegebenen Muster aus. Der MID Server gibt dann die Ergebnisse an die Instanz zurück, wo sie von Sensoren verarbeitet werden. Der MID Server speichert keine Erkennungsinformationen.

Der MID Server startet die gesamte Kommunikation über SOAP auf HTTPS. Dies bedeutet, dass die gesamte Kommunikation sicher ist und alle Kommunikationen innerhalb der Firewall des Unternehmens initiiert werden. Es sind keine speziellen Firewall-Regeln oder VPNs erforderlich.

Discovery wird ohne Agents ausgeführt. Das bedeutet, dass zur Erkennung keine permanente Software auf einem Computer oder Gerät installiert werden muss. Daher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nutzt der MID Server verschiedene Methoden, um Geräte ohne Agents zu erkennen. Beispielsweise stellt der MID Server mithilfe von SSH eine Verbindung zu einem Unix- oder Linux-Computer her und kann dann den in der Probe angegebenen Standardbefehl ausführen, um Informationen zu erfassen. Ebenso wird SNMP (Simple Network Management Protocol) verwendet, um Informationen von einem Netzwerk-Switch oder Netzwerkdrucker zu erfassen.



Arten der Erkennung

Die folgende Tabelle enthält die Arten der horizontalen Erkennung, die Discovery ausführen kann:

Typ	Beschreibung
Netzwerk-Discovery	Führen Sie diese Art der Erkennung aus, um die internen IP-Netzwerke in Ihrem Unternehmen zu erkennen. Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung nicht erforderlich.
CI-Erkennung	Führen Sie diese Art der Erkennung aus, um die Geräte, Computer und Anwendungen in Ihrem Netzwerk zu ermitteln. Das ist im Prinzip der Standardtyp der Erkennung, die am häufigsten ausgeführt wird.
Cloud Discovery	Führen Sie diese Art der Erkennung aus, um AWS- und Azure-Ressourcen in der Cloud Ihres Unternehmens zu ermitteln.
Serverlose Erkennung	Führen Sie diese Art der Erkennung aus, um Anwendungen auf Hostcomputern zu ermitteln, ohne den Host zuerst erkennen zu müssen. Die serverlose Erkennung basiert auf Mustern zum Untersuchen von CIs auf einem Host.

IP-Serviceaffinität

IP-Serviceaffinität bedeutet, dass die IP-Serviceinformationen, die zur erfolgreichen Erkennung eines Geräts benötigt werden, gespeichert und der IP-Adresse des Geräts zugeordnet werden. Mit diesen Informationen kann Discovery in nachfolgenden Ausführungen anhand des genauen Protokolls das Gerät anvisieren. Discovery zeichnet den IP-Service zusammen mit der IP-Adresse auf. Discovery kann die erfolgreichen IP-Serviceinformationen in der Tabelle „IP-Serviceaffinität“ [ip_service_affinity] speichern.

Beispiel: Auf einem Netzwerkgerät sind sowohl ein SSH-Port als auch ein SNMP-Port geöffnet. Aufgrund des Agent-losen Designs versucht Discovery es zuerst mit SSH.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkgeräte müssen jedoch über SNMP erkannt werden. Daher schlägt die von Discovery zuerst versuchte SSH-Probe fehl. Dadurch wird die SNMP-Probe ausgelöst, der erfolgreich ist. Durch die Zuordnung von IP-Adressen zu IP-Services verwenden nachfolgende Erkennungsläufe, die auf diese IP-Adresse abzielen, zuerst SNMP, da dies die erfolgreiche Probe war.

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren

Der horizontale Erkennungsprozess durchläuft die vier Erkennungsphasen mit Probes, die Informationen auf dem Zielcomputer erfassen, und dann mit Sensoren, mit deren Hilfe Discovery ermittelt, was mit diesen Informationen geschehen soll.

Discovery starten

Ein Benutzer löst die horizontale Erkennung aus, indem er einen Discovery-Zeitplan konfiguriert oder eine On-Demand-Discovery mit Discover now oder Quick Discovery startet. Der Zeitplan gibt eine oder mehrere IP-Adressen oder einen Bereich von IP-Adressen an.

Scanphase

1. Discovery nimmt zuerst die Shazzam-Sonde (und dann die Port-Sonden) und platziert sie in einer Anforderung in der Queue des externen Kommunikationskanals (ECC).
2. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab, führt die Tests im Abgleich mit dem Host aus und erkennt offene Ports.
3. Die Port-Tests prüfen gängige Ports mit verschiedenen Protokollen wie WMI, HTTP, SSH und SNMP.
4. Wenn ein oder mehrere Ports antworten, sendet die Shazzam-Sonde Informationen zum Port über den MID Server zurück an die ECC-Warteschlange.
5. Discovery überprüft die ECC-Warteschlange, um herauszufinden, welche Ports geantwortet haben, wodurch der Maschinentyp identifiziert wird. Wenn beispielsweise Shazzam feststellt, dass der Computer an Port 22 empfangsbereit ist, behandelt Discovery den Computer als UNIX- oder Linux-Computer.

Klassifizierungsphase

1. Die Discovery-Anwendung bestimmt, welche Klassifizierungsprüfung an das neu erkannte Gerät gesendet werden soll, indem sie die Informationen im Datensatz der Portprüfung verwendet, die erfolgreich geantwortet haben.
2. Discovery versetzt die Klassifizierungsprüfung in die ECC-Warteschlange.
3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Klassifizierungsprüfung aus.
4. Die Klassifizierungsprüfung ruft zusätzliche Informationen ab, z. B. welche Version des Betriebssystems auf einem Computer ausgeführt wird. Diese Informationen bestimmen die Klasse des von der Discovery gefundenen CIs. Pro erkanntem Gerät gibt es nur eine Klassifizierungssonde.
5. Die Klassifizierungsprüfung sendet Informationen über den MID Server an die Instanz-ECC-Warteschlange zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizierungsphase

1. Discovery bestimmt basierend auf der Klasse des CI und den in allen CI-Klassifiziererdatensätzen angegebenen Kriterien, welcher Klassifizierer zu verwenden ist. Der Klassifizierer gibt an, welche Probes für die nächsten beiden Phasen zu verwenden sind.
2. Discovery setzt die Auslöser-Probe für die Identifizierung für den CI-Klassifizierer in die ECC-Warteschlange. Beispiel: A UNIX Computer wird ausgeführt HP-UX Würde erfordern HP-UX Klassifizierung, die angibt, dass die Mehrfachprobe- HP-UX Auslöser-Probe für Identitätsidentifizierung. Diese Probes verwenden Identifizierungsregeln, um zu bestimmen, ob ein CI in die CMDB eingefügt oder darin aktualisiert werden muss.

   Hinweis: Bei der Auslöser-Probe kann es sich auch um die Probe „Horizontal Pattern“ handeln, der Discovery anweist, die Vorgänge im angegebenen Muster zu verfolgen, anstatt zusätzliche Probes zu versenden. Die Vorgänge im Muster decken sowohl die Identifizierungs- als auch die Erkundungsphase ab. Discovery erkennt anhand des CI-Typs, welche Identifizierungsregeln zu verwenden sind, und führt basierend auf diesen Regeln Einfügungen oder Aktualisierungen in der CMDB durch. Probes und Sensoren werden nicht verwendet.

3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Auslöser-Probe für die Identifizierung aus.
4. Die Identifizierungs-Probe erfasst Identifizierungsdaten für jedes Gerät und sendet diese Daten über den MID Server an die Instanz zurück.
5. Discovery verwendet Sensoren für die Identifizierungs-Probe, um die Informationen zu verarbeiten.
6. Discovery führt die Analyse der CMDB mithilfe von CI-Bezeichnern durch. Discovery kann vorhandene CIs in der CMDB aktualisieren oder neue erstellen.

Erkundungsphase

1. Discovery durchsucht die zugehörige Liste „Auslösertests“ (Auslöser-Probes) im Klassifizierer, um die auszuführende Erkundungs-Probes zu ermitteln.
2. Discovery setzt die Auslöser-Probe für die Erkundung in die ECC-Warteschlange.
3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Auslöser-Probe für die Erkundung aus.
4. Die Probes senden Daten über den MID Server an die Instanz zurück, und die Sensoren aktualisieren genau wie in der Identifizierungsphase die CMDB.

Zugehörige Informationen

Muster und horizontale Erkennung

Prozess-Flow der horizontalen Erkennung mit Mustern

Die horizontale Erkennung mit Mustern weist ebenso wie die horizontale Erkennung mit Probes vier Phasen auf. Für die letzten beiden Phasen löst Discovery jedoch keine zusätzlichen Probes-Sätze aus, sondern Vorgänge aus einem Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scanphase

1. Discovery nimmt zuerst die Shazzam-Sonde (und dann die Port-Sonden) und platziert sie in einer Anforderung in der Queue des externen Kommunikationskanals (ECC).
2. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab, führt die Tests im Abgleich mit dem Host aus und erkennt offene Ports.
3. Die Port-Tests prüfen gängige Ports mit verschiedenen Protokollen wie WMI, HTTP, SSH und SNMP.
4. Wenn ein oder mehrere Ports antworten, sendet die Shazzam-Sonde Informationen zum Port über den MID Server zurück an die ECC-Warteschlange.
5. Discovery überprüft die ECC-Warteschlange, um herauszufinden, welche Ports geantwortet haben, wodurch der Maschinentyp identifiziert wird. Wenn beispielsweise Shazzam feststellt, dass der Computer an Port 22 empfangsbereit ist, behandelt Discovery den Computer als UNIX- oder Linux-Computer.

Klassifizierungsphase

1. Die Discovery-Anwendung bestimmt, welche Klassifizierungsprüfung an das neu erkannte Gerät gesendet werden soll, indem sie die Informationen im Datensatz der Portprüfung verwendet, die erfolgreich geantwortet haben.
2. Discovery versetzt die Klassifizierungsprüfung in die ECC-Warteschlange.
3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Klassifizierungsprüfung aus.
4. Die Klassifizierungsprüfung ruft zusätzliche Informationen ab, z. B. welche Version des Betriebssystems auf einem Computer ausgeführt wird. Diese Informationen bestimmen die Klasse des von der Discovery gefundenen CIs. Pro erkanntem Gerät gibt es nur eine Klassifizierungssonde.
5. Die Klassifizierungsprüfung sendet Informationen über den MID Server an die Instanz-ECC-Warteschlange zurück.

Identifizierungs- und Erkundungsphase

Muster vereinheitlichen die Identifizierungs- und Erkundungsphase der Erkennung.

1. Discovery bestimmt basierend auf der Klasse des CI und den in allen CI-Klassifiziererdatensätzen angegebenen Kriterien, welcher Klassifizierer zu verwenden ist. Der Klassifizierer gibt die Probe Horizontal Pattern an, der wiederum das zu startende Muster angibt. Die Probe „Horizontal Pattern“ enthält auch einen Sensor, der die tatsächliche Aktualisierung der CMDB ausführt.

   Hinweis: Muster benötigen Applicative-Anmeldeinformationen, um auf Hostcomputern ausgeführte Anwendungen zu finden. Stellen Sie sicher, dass Sie Applicative-Anmeldeinformationen zusammen mit den für den Zugriff auf den Hostcomputer erforderlichen Anmeldeinformationen konfiguriert haben.

2. Die Vorgänge im Muster geben die Aktionen an, die Discovery für die Identifizierungs- als auch die Erkundungsphase ausführen muss. Discovery weiß, welche Identifizierungsregeln Zur Verwendung basierend auf dem CI-Typ im Muster führt Discovery Einfügungen oder Aktualisierungen in die CMDB basierend auf diesen Regeln durch. Nur der Sensor für die horizontale Erkennung wird verwendet. Andere Probes und Sensoren werden nicht verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Administratorarbeitsbereich

Die Discovery-Administratorarbeitsbereich Dient als zentraler Standort für die Überwachung, Nachverfolgung und den Abschluss von Discovery-bezogenen Aufgaben. Erleben Sie einen optimierten Discovery-Prozess und eine höhere Effizienz durch die Integration von Zeitplänen, Diagnosen, Optimierungen, Anomalieerkennung und mehr in diesem zentralen Arbeitsbereich.

Voraussetzungen

Um auf zuzugreifen Discovery-Administratorarbeitsbereich, Stellen Sie sicher, dass Discovery Plugin ist installiert und aktiv.

Sie müssen auch über die neueste verfügen ServiceNow Store Version der folgenden Anwendungen:

- Discovery-Administratorarbeitsbereich
- Visibility Content
- CMDB-Arbeitsbereich
- (Optional) Muster für Discovery und Service-Mapping

Rollen

Die folgenden Rollen haben Zugriff auf Discovery-Administratorarbeitsbereich:

- discovery_admin
- Administrator

Abhängigkeiten

Für eine Liste von Discovery-Administratorarbeitsbereich Anwendungsabhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Discovery-Administratorarbeitsbereich Startseite

Die Discovery-Administratorarbeitsbereich H die ome-Seite enthält Tools, mit denen Sie die wichtigsten Discovery-Aufgaben identifizieren und bearbeiten können. Greifen Sie auf kritische Informationen und Anwendungen zu, um die Discovery zu bewerten, den Discovery-Prozess zu verwalten und alle zugehörigen Fehler zu beheben.

Um auf zuzugreifen Discovery-Administratorarbeitsbereich, Navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**an.

Schneller Überblick

Zeigen Sie den Status der Discovery mit an Datenanzahlen Und identifizieren Sie alle Unregelmäßigkeiten, die sich auf die Discovery auswirken könnten. Um detaillierte Informationen zu erhalten, wählen Sie die entsprechende Kachel aus.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Die folgenden Datenanzahlen werden im Abschnitt „Schnellübersicht“ angezeigt:

Aktive Zeitpläne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt die Anzahl der aktiven IP-basierten und an Cloud-Discovery Zeitpläne werden bis heute ausgeführt. Wenn Sie diese Zahl auswählen, gelangen Sie zur Seite „Zeitpläne“, auf der Sie alle anzeigen können Discovery Zeitpläne, die konfiguriert sind und für die Ausführung aktiviert sind.

Fehleraufgaben

Zeigt die aktiven an, einschließlich „Ausstehend“ oder „in Bearbeitung“, Discovery Fehleraufgaben, die in einem bestimmten Zeitraum geöffnet wurden. Wenn Sie diese Visualisierungsnummer auswählen, gelangen Sie zur Seite „Fallmanagement“, auf der Sie alle anzeigen können Discovery Fehleraufgaben.

Hinweis: Sie können die Zeitskala konfigurieren, die sich in der angezeigten Anzahl auf der Seite „Einstellungen“ widerspiegelt. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Zeitpläne mit Anomalien

Zeigt die Anzahl von an Discovery Zeitpläne mit über einen bestimmten Zeitraum erkannten Anomalien. Sie können diese Zeitskala auf der Seite „Einstellungen“ konfigurieren. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Wenn Sie diese Nummer auswählen, werden Sie zum weitergeleitet **Anomalieerkennung** Registerkarte, auf der Sie Details zum Typ und Schweregrad von Anomalien anzeigen können.

Wichtig: Diese Anzahl wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Wenn die Anomalieerkennung inaktiv ist, wählen Sie aus **Aktivieren Sie** Um zur Seite „Einstellungen“ umgeleitet zu werden.

Discovery administratoraufgaben

Überprüfen Sie die drei kritischsten Discovery Fehleraufgaben. Wählen Sie aus **Bearbeiten Sie Die Aufgabe** Schaltfläche, um auf die Detailseite zuzugreifen, auf der Sie die Fehleraufgabe zuweisen oder aktualisieren oder Arbeitsnotizen hinzufügen können. Um alle Discovery-Fehleraufgaben anzuzeigen und zu verwalten, wählen Sie aus **Alle anzeigen** Um auf zuzugreifen **Fallmanagement** Seite.

Hinweis: Dieser Abschnitt konzentriert sich ausschließlich auf Discovery Fehler, denen Aufgaben zugeordnet sind und nicht alle Discovery Fehler.

Discovery Optimierungsempfehlung

Feinabstimmung Discovery Und MID-Server Einstellungen mit automatisierten Vorschlägen, die aus Scans Ihrer Instanz abgeleitet sind. Diese Ergebnisse identifizieren potenzielle Probleme in der Reihenfolge ihrer Relevanz. Wenn Sie ein Ergebnis auswählen, gelangen Sie zum **Optimierungsprüfung** Seite für weitere Details.

Schnell-Discovery

Erkennen Sie Geräte in Ihrem Netzwerk außerhalb einer geplanten Discovery. Geben Sie eine einzelne IP-Adresse, mehrere kommagetrennte IP-Adressen oder ein IP-Netzwerk ein, wie in diesem Beispiel gezeigt:

- IP-Netzwerkadresse – 10.0,1.0/24
- IP-Adressbereich: 10.0,2.1-10.0.2.15
- IP-Adressliste – 10.0,3.176,10.0,3.222,2001::100,2600:1bdc::fffe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie ein aus MID-Server, Ein MID-Cluster oder aktivieren Discovery Um auszuwählen MID-Server Automatisch.

ITOM-Transparenz Apps

Verbessern Sie die Funktionalität von Discovery-Administratorarbeitsbereich Durch Integration von zusätzlichen ITOM-Transparenz Anwendungen. Wenn Sie auswählen **Alle anzeigen** , Sie können sowohl die auf Ihrer Instanz installierten Anwendungen als auch andere anzeigen, die zur Installation verfügbar sind. Weitere Informationen finden Sie unter Anzeigen und filtern ITOM-Transparenz Apps, die verwenden Discovery-Administratorarbeitsbereich.

Erkenntnisse

Erhalten Sie Anleitungen zur Verwaltung von Discovery Verarbeiten und lösen Discovery Fehler bei ITOM-Transparenz Knowledge Base. Greifen Sie über auf relevante Artikel zu ServiceNow Knowledge Base, Erkunden Sie Blog-Posts, oder sehen Sie sich Tutorials für Anleitungsvideos an, um weitere Informationen zu erhalten.

Hinweis: Um die Ressourcen in diesem Abschnitt anzuzeigen, bestätigen Sie, dass Sie installiert haben ITOM Content Service Version 1,2.8.

Discovery-Administratorarbeitsbereich Zeitpläne

Die Seite „Zeitpläne“ bietet einen zentralen Ort zur Überwachung Discovery Leistung, effiziente Verwaltung von Zeitplänen und Status und Einrichtung eines neuen IP-basierten oder Cloud-Discovery Zeitpläne.

Um auf zuzugreifen Discovery-Administratorarbeitsbereich Seite „Zeitpläne“ navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Zeitpläne**an.

Schlüsselfunktionen

Registerkarte „Übersicht“

Ermöglicht es Ihnen, datengesteuerte Entscheidungen durch leistungsstarke Visualisierungen zu treffen.

Hinweis: Sie können die Zeitskala auf dieser Seite auf der Seite „Einstellungen“ konfigurieren. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Datenvisualisierungen

Berichtstitel	Typ	Beschreibung
Aktive Zeitpläne	Indikator	Zeigt die Gesamtzahl der IP-basierten und an Cloud-Discovery Zeitpläne, die konfiguriert und für die wiederkehrende Ausführung aktiviert sind. Wählen Sie die Zahl aus, um alle anzuzeigen Discovery Zeitpläne.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen (Fortsetzung)

Berichtstitel	Typ	Beschreibung
Ohne Anomalien abgeschlossene Zeitpläne	Indikator	Zeigt die Anzahl der IP-basierten und an Cloud-Discovery Zeitpläne, die in einem bestimmten Zeitraum ohne Anomalien abgeschlossen wurden. **Wichtig:** Diese Anzahl wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Wenn die Anomalieerkennung deaktiviert ist, wählen Sie aus **Aktivieren Sie** Um zur Seite „Einstellungen“ umgeleitet zu werden.
X-Tage-Zeitplantrends	Liniendiagramm	Wird Angezeigt Discovery Planen Sie Trends für einen bestimmten Zeitraum. Zeitpläne, die nicht ausgeführt werden konnten, sind als kritische Anomalien markiert. Zeitpläne mit einer niedrigen CI-Discovery-Rate werden als schwerwiegende Anomalien markiert. Zeitpläne mit langer Laufzeit oder hoher Fehleranzahl werden als geringfügige Anomalien markiert. Die Zeitleiste zeigt Ereignisse an, die während des Zeitplans aufgetreten sind. Verwenden Sie das Lupensymbol ( ) Oder scrollen Sie, um die Zeitleiste zu vergrößern, und bewegen Sie den Mauszeiger über den Indikator, um Ereignisdetails anzuzeigen. Mit können Sie Ereignisindikatoren ein- und ausschalten **Legende anzeigen** Funktion. Wählen Sie Aus **Zeigen Sie den Discovery-Status an** Dient zum Anzeigen des Status aller geplanten IP-basierten und Cloud-Erkennungen. Wählen Sie Aus **Zeigen Sie Anomalien an** Zum Anzeigen anomaler Zeitpläne.
Zeitpläne nach Ort	Karte	Wird Angezeigt Discovery Zeitpläne nach Standort. Wählen Sie einen Bereich der Karte aus, der angezeigt werden soll Discovery Zeitpläne in der ausgewählten Region.
Zeitpläne mit Anomalien	Balkendiagramm	Wird Angezeigt Discovery Zeitpläne mit Anomalien, die in einem bestimmten Zeitraum erkannt wurden, was darauf hinweist, welche Zeitpläne fehlgeschlagen sind, eine niedrige CI-Discovery-Rate aufwiesen, eine erhöhte Fehleranzahl aufwiesen oder lange Laufzeiten aufwiesen. Wählen Sie die Nummer oder aus **Alle anzeigen** Zum Anzeigen der anomalen Zeitpläne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen (Fortsetzung)

Berichtstitel	Typ	Beschreibung
		Wichtig: Diese Anzahl wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.
Fehler nach Kategorie	Ringdiagramm	Zeigt die Anzahl aller an Discovery Fehler nach Kategorie. Wählen Sie eine Kategorie aus, um sie dem Diagramm hinzuzufügen oder daraus zu entfernen. Wählen Sie Aus **Zeigen Sie Details an** Zum Anzeigen einer Liste aller Fehler aus allen Erkennungen.

Registerkarte „Discovery-Zeitpläne“

Bietet Ihnen schnellen Zugriff auf alle Ihrer Discovery Zeitpläne. Die Indikatoren oben auf der Seite zeigen eine Anzahl für die Discovery-Zeitpläne insgesamt, IP-basierte Zeitpläne und Cloud-Zeitpläne an. Wenn Sie die Zahl auswählen, wird die Tabelle entsprechend gefiltert.

Verwenden Sie **Filtern nach** Optionen zum Anzeigen von Zeitplänen basierend auf Discovery-Typ, Standort und Anbieter.

Wählen Sie ein aus Discovery Planen Sie aus der Tabelle, um umfassende Details anzuzeigen und die Feldparameter des Zeitplans zu aktualisieren. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich Zeitplandetails.

Registerkarte „Discovery-Status“

Zeigt den Status der geplanten Erkennungen an. Sie können auswählen Discovery Statusnummer zum Anzeigen detaillierter Informationen. Weitere Einzelheiten finden Sie unter Discovery-Status.

Option für schnelle Discovery

Ermöglicht es Ihnen, in wenigen Schritten eine IP-basierte Discovery durchzuführen. Sie können einen IP-Bereich auswählen, die MID-Auswahlmethode auswählen und auswählen MID-Server, Und führen Sie die Discovery alle innerhalb einer Schnittstelle aus. Diese Option ist auf jeder Registerkarte auf der Seite „Zeitpläne“ verfügbar.

Neue Discovery-Option

Ermöglicht Ihnen die Auswahl, wie Sie Ihre Ressourcen erkennen möchten, entweder durch IP-basierte Discovery oder Cloud-Discovery. Diese Option ist auf jeder Registerkarte auf der Seite „Zeitpläne“ verfügbar.

Erstellen Sie eine IP-basierte Discovery Zeitplan

Verwenden Sie Discovery-Administratorarbeitsbereich Dashboard zum Erstellen von IP-basiert Discovery Zeitpläne.

Vorbereitungen

Store-Version 1,8.0.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Zeitpläne**an.
2. Wählen Sie Aus **Neue Discovery** Über den Header einer beliebigen Registerkarte auf der Seite „Zeitpläne“.
3. Wählen Sie Aus **IP-basierte Discovery** Und wählen Sie aus **Fahren Sie Fort** .

   Hinweis: Dieser Zeitplan gilt nur für IP-basierte Discovery. Für Cloud-Discovery, Siehe Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

4. Geben Sie einen Namen für ein Discovery Zeitplan.
5. Wählen Sie aus verfügbar aus Discovery Standorte.
6. Wählen Sie IP-Bereiche aus, indem Sie entweder aus vorhandenen Sätzen auswählen oder die Bereiche manuell eingeben.
   - Um aus vorhandenen IP-Bereichssätzen auszuwählen, wählen Sie aus **Vorhandenen IP-Bereichssatz verwenden (empfohlen)** . Siehe Konfiguration der Discovery-IP-Adresse Weitere Informationen zu IP-Bereichssätzen.
   - Um kommagetrennte IPv4-Adressbereiche, IPv4-Netzwerke oder einzelne IPs manuell einzugeben, die die hinzuzufügenden Bereiche beschreiben, wählen Sie aus **Geben Sie neue IP-Bereiche ein** Und geben Sie die IP-Bereiche ein.
7. Wählen Sie Aus **Als Nächstes** .
8. Wählen Sie Ihr aus MID-Server.

Option	Beschreibung
Cluster von MID-Servern	Wählen Sie ein vorhandenes aus MID-Server Oder erstellen Sie eine. Fehler bei der Bereitstellung von Clustern Überschutz und Last Ausgleich zwischen MID-Servern. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren .
MID-Server automatisch auswählen	Ein verfügbar MID-Server Wird automatisch ausgewählt, wenn Discovery Zeitplanausführungen. Weitere Informationen finden Sie unter Automatische MID-Server-Auswahl.
MID-Server verwenden	Wählen Sie ein aus MID-Server Zum Ausführen von Discovery Zeitplan. Alle MID-Server Werden angezeigt, aber nur diejenigen, die aktiv und validiert sind, können erfolgreich ausgeführt werden Discovery Zeitplan.

9. Wählen Sie Aus **Als Nächstes** .
10. Konfigurieren Sie Discovery Zeitplan.

Option	Beschreibung
Bei Bedarf ausführen	Der Zeitplan wird nur ausgeführt, wenn er manuell ausgelöst wird. Der Zeitplan kann durch Auswahl von ausgelöst werden **Beenden und ausführen** Am Ende dieses Setups oder indem Sie in der Tabelle „Zeitpläne“ zum Zeitplan navigieren und auswählen **Entdecken Sie Jetzt** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Zu einem geplanten Zeitpunkt ausführen	Der Zeitplan wird zu einem geplanten Datum und einer geplanten Uhrzeit ausgeführt. Verwenden Sie die Felder, um zu definieren, wann der Zeitplan ausgeführt wird.
Nach Serie ausführen	Der Zeitplan wird nach einem anderen vorhandenen ausgeführt Discovery Der Zeitplan ist abgeschlossen, indem er sie gestaffelt oder verkettet wird. Wenn Sie einen vorhandenen Zeitplan auswählen, wird eine Beziehungszuordnung aller anderen zugeordneten Zeitpläne angezeigt.
Discovery abbrechen, wenn länger als maximale Laufzeit	Wenn der Zeitplan die maximale Laufzeit überschreitet, wird er abgebrochen. Konfigurieren Sie nach dem Umschalten den Laufzeitschwellenwert.
Beenden und ausführen	Nach der Auswahl werden alle bereitgestellten Informationen validiert. Dann A Discovery Der Zeitplan wird im Hintergrund erstellt Discovery Der Status lautet „erstellt“, und der Zeitplan wird ausgeführt. Sie werden zur Seite „Statusdetails“ für den Zeitplan weitergeleitet.
Fertigstellen	Nach der Auswahl werden alle bereitgestellten Informationen validiert. A Discovery Zeitplan wird erstellt, und Sie werden zu seinem Eintrag in der Tabelle „Zeitpläne“ weitergeleitet. Sie können den Zeitplan bearbeiten Informationen, oder führen Sie sie aus, indem Sie auswählen **Entdecken Sie Jetzt** .

Discovery-Administratorarbeitsbereich Zeitplandetails

Discovery-Administratorarbeitsbereich Ermöglicht Ihnen das bequeme Anzeigen, Bearbeiten und Ausführen von IP-basierten und Cloud-basierten Elementen Discovery Zeitpläne bequem in einer einzigen Schnittstelle.

Um auf zuzugreifen Discovery Zeitplandetails in Discovery-Administratorarbeitsbereich, Navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Zeitpläne** > **Discovery-Zeitpläne**an.

Nachdem Sie einen Zeitplannamen aus der Tabelle ausgewählt haben, zeigt der Zeitplanheader wichtige Informationen an, z. B. Discovery Details, MID-Server Details und Anomalieschweregrad.

Wichtig: Anomalieinformationen werden nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Schlüsselfunktionen

Übersicht

Die **Übersicht** Die Registerkarte enthält Visualisierungen, die detaillierte Informationen zu enthalten Discovery Zeitplan. Diese Visualisierungen bieten eine umfassende Ansicht der Leistung und des Status des Zeitplans und zeigen wichtige Metriken wie die Anzahl der abgeschlossenen Erkennungen, die Erfolgsquote und die aufgetretenen Fehler an. Darüber hinaus heben die Visualisierungen Trends im Zeitverlauf hervor, sodass Sie Muster und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

potenzielle Probleme schnell identifizieren können. Eine vollständige Liste der auf dieser Registerkarte verfügbaren Visualisierungen finden Sie unter Discovery-Administratorarbeitsbereich Datenvisualisierungen.

Hinweis: Die auf dieser Seite reflektierte Zeitskala kann auf der Seite „Einstellungen“ konfiguriert werden. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Zeitplandetails

Die **Zeitplandetails** Die Registerkarte enthält detaillierte Informationen zu Discovery Planen Sie und ermöglicht Ihnen, die Informationen direkt in der -Schnittstelle zu aktualisieren.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), um auf zusätzliche Aktionen zum Anpassen und Verwalten der Formularoberfläche zuzugreifen.

Wählen Sie aus, um einen Bereich von zu erkennenden IP-Adressen zu erstellen **Schnellbereiche** . Führen Sie eine Ausführung aus, indem Sie auswählen **Entdecken Sie jetzt** . Weitere Informationen zu finden Discovery Zeitplankonfiguration, siehe Horizontale Erkennung planen.

Ausführungsverlauf

Die **Ausführungsverlauf** Die Registerkarte zeigt den Status der letzten 10 geplanten Erkennungen an, einschließlich Symbolen für die Anomalieerkennung, wenn diese Option aktiviert ist. Wählen Sie ein aus Discovery Statusnummer zum Anzeigen detaillierter Informationen. Weitere Einzelheiten finden Sie unter Discovery-Administratorarbeitsbereich Statusdetails.

Discovery-Administratorarbeitsbereich Statusdetails

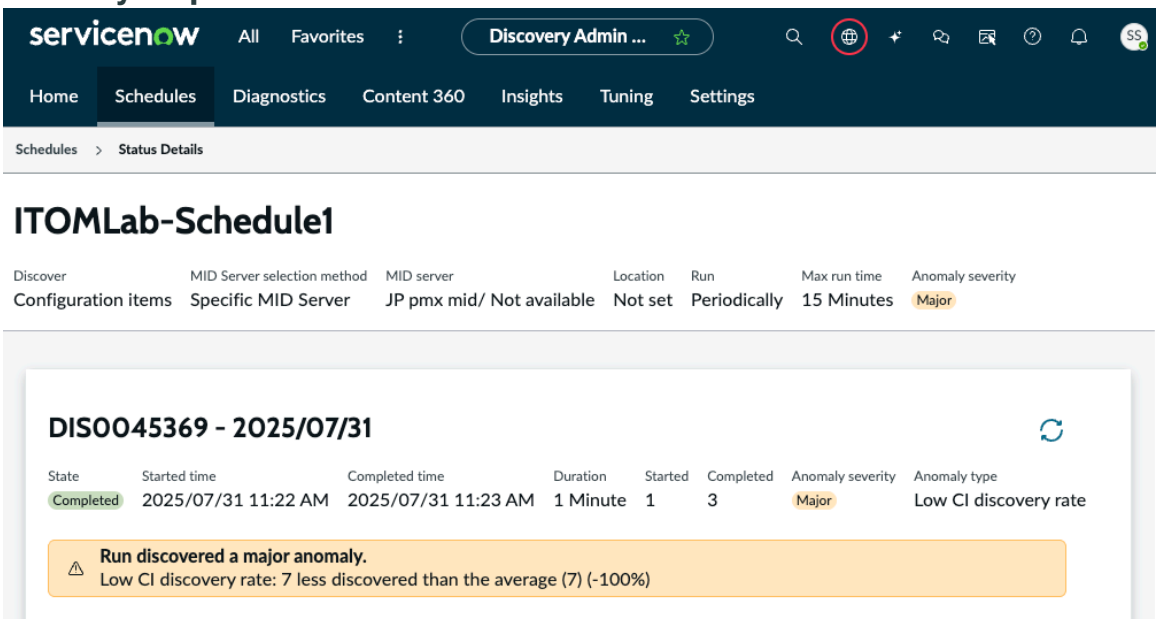
Die Discovery Die Seite „Statusdetails“ enthält eine Zusammenfassung einer Discovery, die über einen Zeitplan initiiert wurde, und enthält die identifizierten Geräte, aufgetretenen Fehler und gefundenen Anomalien.

Um auf zuzugreifen Discovery Statusdetails in Discovery-Administratorarbeitsbereich, Navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Zeitpläne** > **Discovery-Status**an.

Nachdem Sie einen Discovery-Status aus der Tabelle ausgewählt haben, zeigt der Zeitplan-Header wichtige Informationen an, z. B. Discovery Details, MID-Server Details und Anomalieschweregrad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Zeitplan und Status-Header



Hinweis: Ab v1.10.0 zeigt der Zeitplanheader „Quick Discovery“ an, wenn der Zeitplan mit der Quick Discovery-Funktion erstellt wird. Wenn der mit einer Ausführung verknüpfte Zeitplan gelöscht wird, zeigt der Header den Zeitplannamen nicht mehr an.

Der Status-Header zeigt ausführungsbezogene Details an, einschließlich Start- und Endzeiten, Anzahl der ausgelösten und abgeschlossenen Probes und erkannter Anomalien.

Wichtig: Anomalieinformationen werden nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Wenn der Status aktiv oder gestartet ist, wählen Sie aus **Aktualisieren** Symbol ( ) Aktualisiert die Werte „gestartet“ und „Abgeschlossen“ im Header in Echtzeit.

Schlüsselfunktionen

Details

Die **Details** Die Registerkarte enthält Visualisierungen, die detaillierte Informationen zu enthalten Discovery Status. Je nachdem, ob sich der Status auf eine IP- oder Cloud-basierte Discovery bezieht, bieten die Visualisierungen einen detaillierten Überblick über die Leistung des Zeitplans und den aktuellen Status. Sie heben wichtige Metriken hervor, z. B. die Anzahl der erkannten Geräte und IPs, identifizierte Cloud-Ressourcen und alle während der Ausführung aufgetretenen Fehler.

Wählen Sie aus **Weitere Optionen** Symbol ( ), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Datenvisualisierungen der Registerkarte „Details“

Berichtstitel	Discovery-Typ	Beschreibung
Fehler	Sowohl IP- als auch Cloud-basiert	Zeigt die Anzahl der Fehler an, die während der Ausführung erkannt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen der Registerkarte „Details“ (Fortsetzung)

Berichtstitel	Discovery-Typ	Beschreibung
Gesamtanzahl von Geräten	IP-basiert	Zeigt die Anzahl der Geräte an, die während der Ausführung erkannt wurden.
Neue Geräte		Zeigt die Anzahl der neuen Geräte an, die während der Ausführung erkannt wurden.
IPs gesamt		Zeigt die Anzahl der IP-Adressen an, die während der Ausführung erkannt wurden.
Doppelte IPs		Zeigt die Anzahl der doppelten IP-Adressen an, die während der Ausführung erkannt wurden.
Cloud-Ressourcen gesamt	Cloud-basiert	Zeigt die Anzahl der Cloud-Ressourcen an, die während der Ausführung erkannt wurden.

Wenn Sie einen Indikator auswählen, werden zugehörige Informationen in einer Tabelle angezeigt. Standardmäßig werden erkannte Fehler angezeigt, sortiert nach Priorität. Jede Fehlerkarte enthält Details wie den Fehlercode, das Betriebssystem und, falls verfügbar, einen Link zur Begleitdokumentation. Wenn eine Aufgabe erstellt wurde, werden aufgabenbezogene Informationen auf der Karte zusammen mit der Option zum Bearbeiten der Aufgabe angezeigt. Bei Fehlern ohne zugeordnete Aufgabe können Sie entweder eine Aufgabe erstellen oder den Fehler ignorieren. Auswählen von **Fehler Insgesamt** Hyperlink öffnet die Seite „Fehlerstatistiken“, auf der Sie Anweisungen anzeigen und basierend auf dem Fehler Maßnahmen ergreifen können.

Für IP-basierte Zeitpläne **Gesamtanzahl Der Geräte** , **Neue Geräte** , Und **Doppelte IPs** Tabellen enthalten zusätzliche Details wie Quelle, Klassifizierungsprobe und Scan-Status. Auswählen von **Quelle** Hyperlink öffnet eine Seite, auf der Sie weitere Informationen zum Gerät anzeigen, Tags anwenden und auf Details zum Discovery-Protokoll und zur ECC-Warteschlange zugreifen können. Auswählen von **IPs insgesamt** Indikator öffnet die Tabelle „Shazzam-Zusammenfassung“, in der Sie auf Details wie IP-Adressen, IP-Bereich und Netzwerkbereich zugreifen können. Um mehr über ein bestimmtes Element zu erfahren, wählen Sie einfach den zugehörigen Hyperlink in der Tabelle aus.

Wählen Sie für cloudbasierte Zeitpläne aus **Cloud-Ressourcen Insgesamt** Der Indikator zeigt ein Balkendiagramm an, das jede erkannte Cloud-Ressource nach ihrem CI-Typ kategorisiert. Wählen Sie aus **Weitere Optionen** Symbol (⋮), um das Diagramm zu aktualisieren oder zu speichern.

Debugging

Die **Debugging** Die Registerkarte enthält Informationen zu Discovery Protokoll und ECC-Warteschlange.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), um die Daten für jede Visualisierung in diesem Abschnitt zu aktualisieren.

Standardmäßig ist **Discovery-Protokoll** Tabelle zeigt Informationen wie Klassifizierungsfehler, CMDB-Updates und Authentifizierungsfehler an. Ein Discovery-Protokolldatensatz wird für jede Aktion erstellt, die einem Erkennungsstatus zugeordnet ist.

Auswählen von *ECC Queue*Der Indikator zeigt Einträge in an **ECC-Warteschlange** Stellen Sie einen verbundenen Flow von Probe- und Sensoraktivitäten sowie die tatsächliche XML-Nutzlast bereit, die an oder von einer Instanz gesendet wird.

Discovery-Administratorarbeitsbereich Diagnose

Die Seite „Diagnose“ hilft Ihnen, Fehler und Anomalien in IP-basierten und zu priorisieren und zu beheben Cloud-Discovery Zeitpläne. Lösen Sie Probleme, indem Sie Fehleraufgaben erstellen, den Fortschritt nachverfolgen und Support-Tools und -Protokolle verwenden.

Um auf zuzugreifen Discovery-Administratorarbeitsbereich Diagnoseseite navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Diagnosen**an.

Schlüsselfunktionen

Registerkarte „Anomalieerkennung“

Zeigt alle an Discovery Zeitpläne mit in einem bestimmten Zeitraum erkannten Anomalien. Sie können diese Zeitskala auf der Seite „Einstellungen“ konfigurieren. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Wichtig: Diese Registerkarte wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Datenvisualisierungen

Berichtstitel	Typ	Beschreibung
Zeitpläne mit Anomalien	Indikator	Anzahl von Discovery Zeitpläne mit über einen bestimmten Zeitraum erkannten Anomalien. Zeitpläne werden wie folgt kategorisiert: • Kritische Anomalien: Fehler beim Ausführen. • Schwerwiegende Anomalien: Haben eine niedrige CI-Discovery-Rate. • Geringfügige Anomalien: Haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen (Fortsetzung)

Berichtstitel	Typ	Beschreibung
		eine lange Laufzeit oder eine hohe Fehleranzahl.
Fehlgeschlagene Zeitpläne	Indikator	Anzahl von Discovery Zeitpläne, die nicht ausgeführt werden konnten.
Niedrige CI-Erkennungsrate	Indikator	Anzahl von Discovery Zeitpläne mit einer niedrigen CI-Discovery-Rate. **Hinweis:** Der Schwellenwert für die CI-Discovery-Rate kann auf der Seite „Einstellungen“ konfiguriert werden.
Erhöhte Fehleranzahl	Indikator	Anzahl von Discovery Zeitpläne mit einer erhöhten Fehleranzahl. **Hinweis:** Der Schwellenwert für die Fehleranzahl kann auf der Seite „Einstellungen“ konfiguriert werden.
Lange Laufzeit	Indikator	Anzahl von Discovery Zeitpläne mit langer Laufzeit. **Hinweis:** Der Schwellenwert für die Laufzeit kann auf der Seite „Einstellungen“ konfiguriert werden.

Wenn Sie einen der Indikatoren auswählen, wird die Tabelle so gefiltert, dass sie die in der Datenanzahl dargestellten Zeitpläne widerspiegelt. Für jeden Eintrag in der Tabelle können Sie Details zum Typ und Schweregrad von Anomalien anzeigen.

Die **Aktionen** Das Dropdown-Menü bietet eine direkte Verknüpfung zur Seite „Einstellungen“ zum Konfigurieren der Anomalieerkennung. Darüber hinaus enthält das Menü einen **Löschen Sie alle Anomalien** Option, damit Administratoren Datensätze in den Tabellen „Discovery-Zeitplananomalie“ [Discovery_schedule_anomaly] und „Discovery-Zeitplananomaliemetriken“ [Discovery_schedule_anomaly_metrics] schnell entfernen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie **Filtern nach** Optionen zum Priorisieren und Beheben von Anomalien. Filter Discovery Zeitpläne nach Name mithilfe von **Zeitpläne** Dropdown-Menü. Darüber hinaus können Sie die Ergebnisse mit priorisieren **Schweregrad** Dropdown-Menü, das Optionen wie Kritisch, schwerwiegend und gering enthält. Verwenden Sie **Anomalietyp** Dropdown-Menü zum schnellen Anzeigen von Zeitplänen mit derselben Anomalie. Verfügbare Optionen sind fehlgeschlagener Zeitplan, niedrige CI-Discovery-Rate, erhöhte Fehleranzahl und lange Laufzeit.

Registerkarte „Diagnose“

Zeigt alle Fehler aus jeder Discovery an. Für jeden Eintrag in **Discovery-Fehler** Tabelle können Sie entweder eine Fehleraufgabe erstellen oder den Fehler mit ignorieren **Aufgabe erstellen** Und **Ignorieren** Schaltflächen. Wenn für einen Eintrag bereits eine Fehleraufgabe vorhanden ist, wird angezeigt **Bearbeiten Sie die Aufgabe** Schaltfläche zusammen mit dem Namen und der Priorität der Aufgabe.

Verwenden Sie **Filtern nach** Optionen zum Priorisieren und Beheben von Fehlern. Sie können nach filtern Discovery Planen Sie mit **Zeitplan** Dropdown-Menü, oder suchen Sie mit nach dem Namen des Fehlers **Suchen** Balken. Verwenden Sie **Sortieren** Dropdown-Menü zum Organisieren der Ergebnisse nach Code, Priorität und Gesamtfehleranzahl in aufsteigender oder absteigender Reihenfolge.

Die Fehlerdatensätze können auch mit gefiltert werden **Filtern nach** Und **Hat Aufgabe** Dropdown-Menüs. In **Filter** Menü können Sie auswählen, dass nur Fehler im Zusammenhang mit CMDB, Konfiguration, Anmeldeinformationen, Intern oder Netzwerk angezeigt werden. Mehrere Kategorien können gleichzeitig ausgewählt werden. Die **Hat Aufgabe** Das Menü zeigt entweder alle Fehlerdatensätze, Fehlerdatensätze mit einer Aufgabe oder Fehlerdatensätze ohne Aufgabe an.

Für jeden Eintrag in **Discovery-Fehler** Tabelle, die **Fehler Insgesamt** Die Nummer kann ausgewählt werden, um zu zu navigieren **Fehlerstatistikseite** . Auf dieser Seite werden Informationen zum Fehler angezeigt und bereitgestellt **Anweisungen** , Sowie ein zugehöriges Knowledge Base artikel, falls verfügbar. Wenn dem Fehler eine Aufgabe zugeordnet ist, wird die Aufgabennummer im Header angezeigt und kann durch Auswählen der Schaltfläche aufgerufen werden. Die **Aktion** Das Dropdown-Menü enthält vorgeschlagene Aktionen basierend auf dem Fehlertyp. In **Fehler** Tabelle, die **Aktion für ausgewählt** Das Dropdown-Menü kann Fehler für einzelne IP-Adressen ignorieren, ihre Discovery wiederholen, sie der globalen Ausschlussliste hinzufügen oder ihren Shazzam-Portstatus überprüfen.

Registerkarte „Fallmanagement“

Bietet einen Überblick über die Status von Fehleraufgaben. Sie können jede Aufgabe auswählen, um zu ihrem detaillierten Datensatz zu navigieren. Mit können neue Aufgaben erstellt und vorhandenen Fehlern zugeordnet werden **Aufgabe Erstellen** Schaltfläche. Sie können nach filtern Discovery Planen Sie mit **Zeitplan** Dropdown-Menü, oder suchen Sie mit nach dem Namen der Fehleraufgabe **Suchen** Balken. Verwenden Sie **Kanban-Tafelansicht** Und **Listenansicht** Zum Ändern des Anzeigestils.

Support-Tools

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Support-Tools** Die Registerkarte enthält Tools zum Untersuchen und Beheben von Problemen mit Ihrer Instanz. Eine vollständige Liste der auf dieser Registerkarte verfügbaren Tools finden Sie unter Discovery-Administratorarbeitsbereich Support-Tools.

Protokolle

Die **Protokolle** Über die Registerkarte können Sie auf zugreifen **ECC-Warteschlange** Und **Discovery-Protokolle** . Die Überprüfung dieser Protokolle kann bei der Diagnose und Behebung von Fehlern helfen. Sie können einen Eintrag im Protokoll auswählen, um weitere Details anzuzeigen. Darüber hinaus können die Tabellen mithilfe der entsprechenden Schaltflächen gefiltert oder exportiert werden.

Registerkarte „ignorierte Fehler“

Führt einen Datensatz aller Fehler, die in den letzten 30 Tagen ignoriert wurden. Fehler, die älter als 30 Tage sind, werden gelöscht. Sie können dem einen Fehler hinzufügen **Discovery-Fehler** Tabelle mit **Ignorieren rückgängig machen** Schaltfläche.

Virtual Agent-Chat

Ab Version 1.8.0 von Discovery-Administratorarbeitsbereich, Die Seite „Diagnose“ enthält auf jeder Registerkarte einen Virtual Agent-Chatbot. Dieser Chatbot kann helfen, Diagnoseinformationen für die Behebung von Problemen mit abzurufen Discovery. Sie können entweder eine bestimmte Anforderung eingeben oder auswählen **Zeigen Sie mir alles** Zum Anzeigen aller verfügbaren Optionen.

Wichtig: Der Virtual Agent wird nur angezeigt, wenn `sn_disco_workspace.visibility_diagnostic_utility.enabled`Eigenschaft ist auf festgelegt **Wahr** .

Auswählen von **Discovery Und** `MID-Server`**Integritätsvalidierung** Prompt bietet die folgenden Optionen:

- MID-Server Prüfung vor dem Upgrade: Ermöglicht das Ausführen von On-Demand-Tests für MID-Server Vor dem Upgrade. Es identifiziert Probleme, die den Upgradeprozess stoppen könnten, und stellt ein Protokoll bereit, um gefundene Probleme zu beheben.
- MID-Server Statusvalidierung: Validiert, dass MID-Server Der Anwender ist aktiv und Teil der Gruppe „MID_Server“ und prüft auf Fehler bei der Standardauthentifizierung des Anwenders.
- MID-Server Gegenseitige Authentifizierung: Ermöglicht es Ihnen, einen bestimmten Anwender auszuwählen und zu überprüfen, ob der Anwender über ein aktives, nicht abgelaufenes Zertifikat verfügt.
- Validierung der Mustersynchronisierung: Überprüft, ob ein Muster und die zugehörigen Bibliotheken mit dem angegebenen synchronisiert sind MID-Server Und bestimmt, ob sie anwenderdefiniert sind.

Auswählen von **Abrufen der MID-Server-Einstellungen** Mit der Eingabeaufforderung können Sie Einstellungen aus der verfügbaren abrufen MID Servers. Wenn mehrere vorhanden sind MID-Server, Der Service Desk-Mitarbeiter stellt eine Liste von bereit MID Servers Zur Auswahl. Anschließend können Sie die Konfigurationsdatei herunterladen und die Konfigurationswerte für die ausgewählte analysieren MID-Server.

Hinweis: Diese Option ist ab Version 1.10.0 von verfügbar Discovery-Administratorarbeitsbereich.

Auswählen von **Discovery-Leistungsmetriken** Prompt untersucht die ECC-Warteschlange, um Leistungsmetriken für einen Discovery-Status zu erfassen, und stellt die folgenden Informationen bereit:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Durchschnittliche Wartezeiten für die Verarbeitung von ECC-Warteschlangeneingaben.
- Durchschnittliche Wartezeiten für MID-Server Dient zur Verarbeitung von ECC-Warteschlangenausgaben.
- Informationen zu den Probes oder Sensoren, die die längste Zeit in Anspruch genommen haben, um ihre Aufgaben abzuschließen.

Auswählen von **Protokolle Abrufen** Mit der Eingabeaufforderung können Sie auf Musterprotokolle, Discovery-Protokolle oder Knotenprotokolle zugreifen. Musterprotokolle können mithilfe der ECC-Warteschlangenausgabe-ID oder der verwalteten IP-Adresse und des Musternamens abgerufen werden. Auf Discovery-Protokolle kann über Protokollstatus oder ECC-Warteschlangeneingabe zugegriffen werden, Knotenprotokolle nach Transaktions-ID oder ECC-Warteschlangeneingabe.

Discovery-Administratorarbeitsbereich Inhalt 360

Auf der Seite „Inhalt 360 können Sie Anwendungen erkennen und Anwendungsvorschläge basierend auf maschinellem Lernen oder Crowd-Sourcing-Ressourcen bewerten. Erstellen Sie dann Konfigurationselemente mit einem einzigen Klick.

Content 360 verwendet Datenvisualisierungen, um umfassende Transparenz der Anwendungen Ihrer Infrastruktur und der Ressourcen zu bieten, die zum Erstellen von Anwendungskonfigurationselementen (CIs) verfügbar sind. Sie bietet auch Zugriff auf eine Liste von Klassifizierern, die der Discovery hinzugefügt werden sollen. Aktualisieren Sie die Seite, um die aktuellsten Visualisierungen anzuzeigen.

Um auf zuzugreifen Discovery-Administratorarbeitsbereich Inhalt 360 Seite, navigieren Sie zu **Arbeitsbereiche** > *`Discovery-Administratorarbeitsbereich`* > **Content 360**an.

Schlüsselfunktionen

VON KI vorgeschlagene Anwendungsfingerabdrücke

Zeigen Sie eine Liste der vorgeschlagenen Anwendungen mit Fingerabdrücken an, die Sie dem Discovery-Prozess über die Funktion „KI-vorgeschlagene Anwendungsfingerabdrücke“ hinzufügen können. Sie können dann einen Gruppennamen auswählen, um ausführliche Details zu einer Anwendung anzuzeigen.

- Ändern Sie bestimmte Details, z. B. den Namen des Discovery-Musters oder den vorgeschlagenen CMDB Klasse.
- Zeigen Sie zusätzliche Informationen zu Prozessbeispielen und zugehörigen Servern an.
- Wählen Sie diese Option aus, um angezeigte Vorschläge beim nächsten Mal zu ignorieren Discovery Wird ausgeführt.
- Fügen Sie Vorschläge zu hinzu Configuration Management Database (CMDB) Das nächste Mal, wenn Discovery ausgeführt wird.

Das Widget „Fingerabdrücke der von KI vorgeschlagenen Anwendung“ wird nicht automatisch aktualisiert. Um sicherzustellen, dass Sie die neuesten Informationen anzeigen, aktualisieren Sie die Seite manuell.

Weitere Informationen zur Discovery basierend auf Anwendungsfingerabdrücken finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.

Anwendungs-CIs erkannt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie Informationen zu Anwendungs-CIs, die basierend auf Anwendungsfingerabdrücken oder erkannt wurden ITOM Content Service Vorschläge über Discovery-Administratorarbeitsbereich. Ein Kreisbericht veranschaulicht die Gesamtzahl der erkannten anwenderdefinierten Anwendungs-CIs, während ein Balkenbericht die fünf wichtigsten erkannten, innerhalb der letzten zwei Tage erstellten und nach Klasse gruppierten Anwendungs-CIs anzeigt.

ITOM Content Service

ITOM Content Service Erfasst nicht erkannte Anwendungsfingerabdrücke aus verschiedenen Umgebungen. KI-Bibliothekare analysieren diese Fingerabdrücke und erstellen dedizierte Klassifizierer, die wöchentlich aktualisiert und an Sie gesendet werden. Die neueste Version von Discovery-Administratorarbeitsbereich Ermöglicht Ihnen, die Inhaltsservicevorschläge manuell zu aktualisieren, bevor Sie sie überprüfen. Da neue IT-Produkte schnell auf den Markt gebracht werden, gewährt diese Funktion Ihnen eine schnelle Aktualisierung der Transparenz und bietet die folgenden Vorteile:

- Sie überprüft die Produkte, die Sie derzeit jede Woche verwenden, und liefert neue Fingerabdrücke der Anwendung.
- Identifiziert irrelevante Prozesse, die keine geeigneten Kandidaten für CIs sind.
- Basierend auf KI hilft es Ihnen, Fingerabdrücke laufender Prozesse und SNMP-Objektbezeichner (Simple Network Management Protocol, SNMP) zu identifizieren und die CIs zu erstellen, die Sie für die Überwachung Ihrer Infrastruktur benötigen.
- Erkennt eine höhere Anzahl von Produkten mithilfe von KI-Fähigkeiten, die laufende Anwendungsprozesse gruppieren und klassifizieren.

Auf der neuesten Version von Discovery-Administratorarbeitsbereich, Beginnend ab Xanadu Instanzen wird das Widget „Inhaltsservicevorschläge“ automatisch aktualisiert und zeigt die aktuellsten Informationen an. Dies wird durch das Echtzeitsymbol ( ), das neben dem Widget-Namen angezeigt wird.

Weitere Informationen zu ITOM Content Service finden Sie unter ITOM Content Service .

Daten werden für freigegeben *`ITOM Content Service`*

Das Continuance Delivery System (CDS), A ServiceNow® Technologie, synchronisiert Daten zwischen der Datenserviceinstanz, die Daten speichert und verteilt, und den Kundeninstanzen, wobei nur die Prozesse und SNMP-OIDS-Daten verwendet werden. Mit ITOM Content Service Funktion über das CDS können Sie sich anmelden, um Prozessdaten für Fingerabdrücke von Anwendungen freizugeben. Diese Daten können von KI-Bibliothekaren gekennzeichnet und klassifiziert werden, wodurch aktiviert wird ITOM Content Service Um jede Woche neue CIs bereitzustellen. Ihre Daten werden für freigegeben ServiceNow® Instanz in einer sicheren Umgebung. Sie haben die Gewissheit, dass keine personenbezogenen Daten offengelegt werden und alle Informationen anonym gehalten werden. Die Teilnahme ist optional, und Sie können sich jederzeit abwählen. Weitere Informationen finden Sie unter Geben Sie Daten für frei ITOM Content Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Für erforderliche Plugins ITOM Content Service:

- Discovery
- Normalisierungsdatenservices

Erkennen Sie Anwendungen mithilfe von Anwendungsfingerabdrücken oder ITOM Content Service

Erkennen Sie Anwendungen mithilfe von Vorschlägen basierend auf ServiceNow Predictive Intelligence Oder ServiceNow ITOM Content Service Zum Erstellen von Konfigurationselementen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Überprüfen Sie Anwendungsvorschläge basierend auf Fingerabdrücken der Anwendung oder ITOM Content Service Und fügen Sie sie der Discovery hinzu.

- Die auf Fingerabdrücken basierte Erkennung nutzt Algorithmen, um laufende Prozesse zu identifizieren und in Gruppen zu organisieren. Diese Prozessgruppen werden zu vorgeschlagenen Anwendungen oder Kandidaten. Sie überprüfen vorgeschlagene Anwendungen und wählen aus, welche erkannt werden sollen. Die Liste der vorgeschlagenen Anwendungen wird stündlich aktualisiert.Weitere Informationen finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.
- ITOM Content Service Identifiziert die Produkte, die Sie derzeit verwenden, und stellt jede Woche neue Produktvorschläge bereit. Weitere Informationen finden Sie unter ITOM Content Service.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Content 360**an.
2. Wählen Sie einen Anwendungsvorschlag aus, der der Discovery hinzugefügt werden soll, basierend auf den Fingerabdrücken der Anwendung oder ITOM Content Service.

Vorschlagsquelle	Aktionen
Fingerabdrücke der Anwendung	**a.** Wählen Sie aus **VON KI vorgeschlagene Anwendungsfingerabdrücke** Widget. **b.** Wählen Sie den Vorschlag unter aus **Vorgeschlagener Gruppenname** . **c.** Überprüfen Sie die Informationen im angezeigten Formular „Vorschlag für Fingerabdrücke der Anwendung“. Informationen zu den Formularfeldern finden Sie unter Formular „Vorschlag für Fingerabdruck der Anwendung“. **d.** Legen Sie fest, ob der Vorschlag der Discovery hinzugefügt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorschlagsquelle	Aktionen
	▪ Wenn der Vorschlag nicht relevant ist und Sie ihn nicht hinzufügen möchten, wählen Sie aus **Ignorieren** . ▪ Wenn Sie es hinzufügen möchten, wählen Sie aus **Zu Discovery hinzufügen** .
ITOM Content Service	**a.** Bestätigen Sie, dass Sie sich für angemeldet haben ITOM Content Service. **Hinweis:** Wenn **Aktivieren** Option wird angezeigt, Sie haben sich noch nicht angemeldet. Weitere Informationen finden Sie unter Geben Sie Daten für frei ITOM Content Service. **b.** Wählen Sie aus **Inhaltsservicevorschläge** Widget. **c.** Synchronisieren Sie manuell mit Vorschlägen aus Ihrem System, indem Sie auswählen **Kandidaten synchronisieren** . **Hinweis:** Wenn eine Meldung zum Anwendungsbereich angezeigt wird, wählen Sie aus **OK** Zum Beenden der Nachricht. Ändern Sie dann den Umfang, indem Sie das Symbol für den Anwendungsbereich ( ) Und auswählen **Global** . **d.** Wählen Sie im Bestätigungsfenster für Synchronisierungskandidaten die Option aus **Ja** . **e.** Überprüfen Sie die Liste, und wählen Sie den Namen des relevanten Vorschlags aus, um detailliertere Informationen anzuzeigen. **Hinweis:** Sie können mehrere Vorschläge auswählen, die gleichzeitig der Discovery hinzugefügt werden sollen. Aktivieren Sie das Kontrollkästchen neben jedem Vorschlag, und wählen Sie dann aus **Aktivieren** . **f.** Legen Sie fest, ob der Vorschlag der Discovery hinzugefügt werden soll. ▪ Wenn der Vorschlag nicht relevant ist und Sie ihn nicht hinzufügen möchten, kehren Sie zur Liste der vorgeschlagenen Anwendungen zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorschlagsquelle	Aktionen
	▪ Wenn Sie Änderungen am Vorschlag vorgenommen haben, ihn aber nicht der Discovery hinzufügen möchten, wählen Sie aus **Speichern** . ▪ Um den Vorschlag zur Discovery hin–zuzufügen, wählen Sie aus **Aktivieren** .

Discovery-Administratorarbeitsbereich Einblicke

Die Seite „Einblicke“ bietet Zugriff auf spezialisierte Widgets, Dashboards und Berichte, um das IT-Betriebsmanagement und die Infrastrukturüberwachung Ihrer Organisation zu nutzen und die Funktionen von Discovery für eine verbesserte operative Transparenz und die Integrität der Infrastruktur zu nutzen.

Informationen, auf die über die Seite „Einblicke“ zugegriffen wird

Auf der Seite „Einblicke“ können Sie auf die folgenden Informationen zugreifen:

- Oracle Global License Advisory Services (GLAS) – Datenerfassung anhand von Mustern
- Kubernetes Explorer
- Nutanix-Dashboard
- MID-Server-Dashboard
- Dashboard „Agent-Integrität“
- Fehlende Rechenressourcen erkennen
- Shazzam-Einblicke
- VM-Explorer

Fehlende Rechenressourcen erkennen

Verwenden Sie Discovery-Administratorarbeitsbereich Um Rechenressourcen zu identifizieren, die kürzlich nicht erkannt wurden. Führen Sie eine schnelle Discovery aus, um die Daten der Ressource zu aktualisieren. Wenn eine Ressource nicht erkennbar ist, ignorieren Sie die Ressource, und schließen Sie sie aus dem Bericht aus. Dieses Verfahren hilft Ihnen, die Nutzung Ihrer Ressourcen zu maximieren.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig enthält der Bericht die folgenden Informationen:

- Von erkannte Ressourcen ServiceNow® Plattform und ServiceWatch-Suite.
- Ressourcen, die nicht erkannt wurden, seit die vorherige Discovery 14 Tage zuvor ausgeführt wurde, oder die kein Discovery-Datum in haben **Neueste Discovery** Feld.
- Ressourcen, die keine haben **In Bericht ignorieren** Tag.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **Fehlende Rechenressourcen aus Discovery**an.
2. Führen Sie eine schnelle Discovery für eine Ressource aus.
   a. Wählen Sie in der Liste die Ressource aus.
   b. Wählen Sie Aus **Schnelle Discovery** .
   c. Wählen Sie ein aus MID-Server Zum Ausführen der Discovery.
   Die **Geben Sie die IP-Liste ein** Wird automatisch ausgefüllt.
   d. In **MID-Auswahlmethode** Und **MID-Server** Felder wählen Sie die bevorzugten Optionen aus.
   Weitere Informationen finden Sie unter MID-Server-Auswahl .
   e. Wählen Sie Aus **Führen Sie die Discovery aus** .
3. Wenn die Discovery der Ressource fehlgeschlagen ist, ignorieren Sie die Ressource, und schließen Sie sie aus dem Bericht aus.

   Wenn Sie eine Ressource erfolgreich ignorieren, wird ein grünes Banner angezeigt, das darauf hinweist, dass die Ressource im Bericht ignoriert wird. Wenn die Ressource ignoriert wird, wird sie aus entfernt **Fehlende Rechenressourcen** Bericht.

   a. Wählen Sie in der Liste die Ressource aus.
   b. Wählen Sie Aus **In Bericht ignorieren** .
4. **Wahlweise:** Wenn Sie die Discovery für eine zuvor ignorierte Ressource aktivieren möchten, entfernen Sie **Im Bericht ignorieren** Tag.
   a. Navigieren Sie zu **Alle** Und geben Sie den Filter ein `cmdb_ci_Server.list` .
   b. Personalisieren Sie die Liste, um einzubeziehen **Tags** Spalte über die Schaltfläche „Einstellungen“.
   c. Suchen Sie nach dem Ressourcennamen.
   d. In **Tags** Wählen Sie die Entfernungsoption aus.

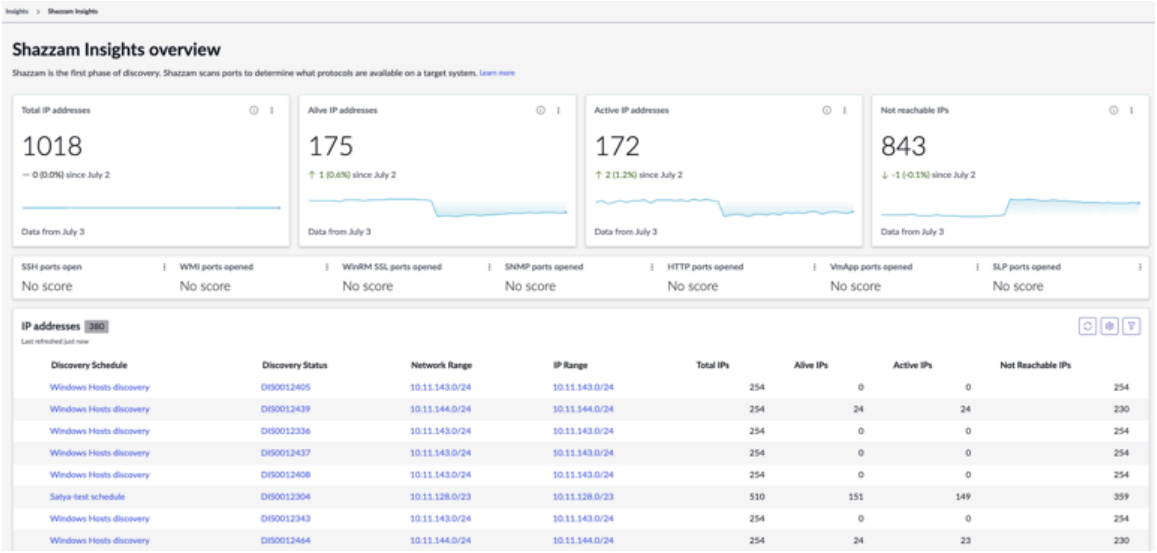
Ergebnis

Wenn die schnelle Discovery erfolgreich war, wird die Instanz zu umgeleitet **Discovery-Status** Dashboard. Wenn die Ressource erkannt wird, wird sie aus entfernt **Fehlende Rechenressourcen** Bericht und wird in der Tabelle „Server“ [cmdb_ci_Server] aufgeführt.

Dashboard „Shazzam-Einblicke“

Die Discovery-Administratorarbeitsbereich Zeigt Informationen zum Port-Scan, die IP-Adressennutzung und an Discovery Zeitpläne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erforderliche ServiceNow AI Platform-Rollen

- discovery_admin
- Administrator

Voraussetzungen

Stellen Sie sicher, dass Sie über den erforderlichen Satz verfügen Aktiv

- Discovery.
- Discovery-Administratorarbeitsbereich 1,3.1. (Store-Release August 2024).
- CMDB-Arbeitsbereich
- Visibility Content

Aktivieren Sie die Datensammlung

Erforderliche Rolle: System_Administrator.

Legen Sie fest *`glide.discovery.shazzaminsights`*Eigenschaft bis **Wahr** .

Führen Sie eine aus Discovery Zeitplan.Weitere Informationen finden Sie unter: Erkennungen im Netzwerk ausführen.

Greifen Sie auf zu Shazzam-Einblicke Dashboard

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **Shazzam-Einblicke**an.

Indikatoren

Gesamtzahl der IP-Adressen

Die Gesamtzahl und der Trend der IP-Adressdaten, die Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus extrahiert Shazzam-Zusammenfassung Tabelle [shazzam_summary].

Aktive IP-Adressen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Nummer und der Trend der reaktionsfähigen und anpingbaren IP-Adresse es Der Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus extrahiert Shazzam-Status Tabelle [shazzam_Status].

Aktive IP-Adressen

Die Nummer und der Trend der verbundenen IP-Adresse es Der Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus extrahiert Shazzam-Status Tabelle [shazzam_Status].

Nicht erreichbare IPs

Die Anzahl und der Trend der nicht reagierenden IP-Adresse es Der Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus extrahiert Shazzam-Zusammenfassung Tabelle [shazzam_summary].

Ports öffnen

- Die Punktzahl der offenen SSH-Ports
- Die Punktzahl der offenen WMI-Ports
- Die Punktzahl der offenen WinRM-SSL-Ports
- Die Punktzahl der offenen SNMP-Ports
- Die Punktzahl der offenen HTTP-Ports
- Die Punktzahl der offenen VmApp-SSL-Ports
- Die Punktzahl der offenen SLP-Ports

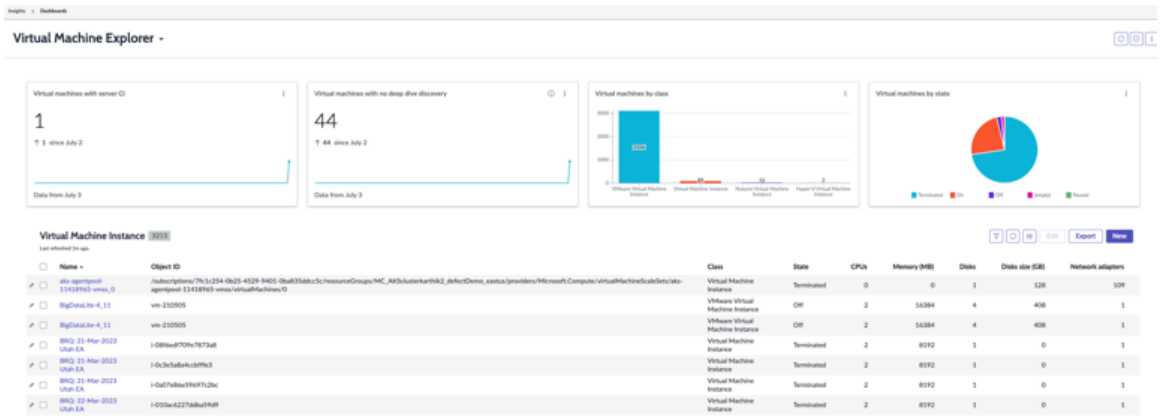
Filter

Name	Typ	Beschreibung
IP-Adressen	Boolean	Mit dem Filter können Sie alle auswählen Discovery Zeitpläne, die Sie überprüfen möchten Nach Kategorie. Die verfügbaren Kategorien Sind: • IP-Bereich • Aktiv • Aktiv

Dashboard „Virtual Machine Explorer“

Die Discovery-Administratorarbeitsbereich Das Dashboard „Virtual Machine Explorer“ zeigt Informationen zur Aktivität und Kapazität Ihrer VM-Instanzen an, wie vom Discovery-Prozess angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um auf das Dashboard zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **VM-Explorer**an.

Schlüsselfunktionen

Mit dem VM Explorer-Dashboard können Sie datengesteuerte Entscheidungen durch leistungsstarke Visualisierungen treffen.

Wählen Sie aus **Weitere Optionen** Symbol (⋮), und wählen Sie dann aus **Aktualisieren** Zum Aktualisieren der Daten für jede Visualisierung in diesem Abschnitt.

Datenvisualisierungen

Berichtstitel	Typ	Beschreibung
Virtuelle Computer mit Server-CI	Indikator und Liniendiagramm	Zeigt die Gesamtzahl und den Trend der VMs an, für die seit einem bestimmten Datum ein Serverkonfigurationselement (CI) erkannt wurde.
Virtuelle Computer ohne Deep Dive-Erkennung	Indikator und Liniendiagramm	Zeigt die Gesamtzahl und den Trend der VMs an, für die seit einem bestimmten Datum keine erstellten CI-Beziehungen erkannt wurden.
Virtuelle Maschine nach Klasse	Balkendiagramm	Zeigt die Anzahl der VMs in Ihrer Infrastruktur nach Klasse sortiert an. VM-Instanzen [cmdb_ci_vm_instance] ist die Quelltabelle für dieses Diagramm.
Virtuelle Maschinen nach Status	Kreisdiagramm	Zeigt den Prozentsatz der VMs an, gruppiert nach den folgenden status: Ein, aus oder andere. VM-Instanzen [cmdb_ci_vm_instance] ist die Quelltabelle für dieses Diagramm.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie nach der Installation zum ersten Mal auf das VM Explorer-Dashboard zugreifen Discovery-Administratorarbeitsbereich, Die virtuellen Computer mit Server-CI und virtuelle Computer ohne Deep-Dive-Discovery-Indikatoren zeigen möglicherweise keine Punktzahlen an. Anweisungen zum Sammeln von Daten für diese Punktzahlen finden Sie unter Führen Sie die Verlaufsdatensammlung für den Virtual Machine Explorer aus.

VM-Instanz

Dieser Abschnitt bietet eine Übersicht über erkannte VM-Instanzen mit wichtigen Informationen wie Objekt-ID, Klasse und Netzwerkadapter. Sie können eine Instanz aus der Tabelle auswählen, um detaillierte Informationen dazu anzuzeigen, oder auf klicken **Formular bearbeiten** Symbol ( ) Zum Bearbeiten von Details und Anzeigen von Aktivitäten. Das Filtersymbol ( ) Ermöglicht es Ihnen, feste Filter anzuwenden oder anwenderdefinierte Filter zu erstellen, die gespeichert und wiederverwendet werden können. Um die Tabelle zu exportieren, wählen Sie aus **Exportieren** Option und wählen Sie Ihr bevorzugtes Format aus: Excel, CSV, JSON oder PDF.

Führen Sie die Verlaufsdatensammlung für den Virtual Machine Explorer aus

Nach der Installation Discovery-Administratorarbeitsbereich, Führen Sie Verlaufsdatensammlungsaufträge aus, um die virtuellen Computer mit Server-CI und virtuelle Computer ohne Deep-Dive-Discovery-Berichte im Dashboard „Virtual Machine Explorer“ auszufüllen.

Vorbereitungen

Der Anwendungsbereich muss auf festgelegt werden **Global** .

Erforderliche Rolle: pa_data_collector oder admin

Prozedur

1. Navigieren zu **Alle** > **Platform Analytics** > **Datenerfasser** > **Aufträge**an.
2. Wählen Sie aus **Filter** Symbol.
3. **[Name] [Enthält]** Historisch **UND [Name][enthält]** VM .
4. Führen Sie den Filter aus, indem Sie auswählen **Ausführen** .
5. Wählen Sie Aus **[PA-VMs mit Links] Verlaufsdatensammlung** Aus der Tabelle.
6. Wählen Sie **Jetzt ausführen**.
   Der Verlaufsdatensammlungsauftrag erfasst Daten für die letzten 60 Tage.
7. Wählen Sie aus **Zurück** Symbol, um zur vorherigen Tabelle zurückzukehren.
8. Wählen Sie Aus **[PA-VMs OHNE Links] Verlaufsdatensammlung** Aus der Tabelle.
9. Wählen Sie **Jetzt ausführen**.
   Der Verlaufsdatensammlungsauftrag erfasst Daten für die letzten 60 Tage.

Nächste Maßnahme

Aktualisieren Sie die Indikatoren im Dashboard „Virtual Machine Explorer“ manuell, um die virtuellen Computer mit Server-CI und virtuellen Computern ohne Deep-Dive-Discovery-Berichte auszufüllen, sodass Sie relevante Daten und Trends anzeigen können. Weitere Informationen finden Sie unter Dashboard „Virtual Machine Explorer“.

Discovery-Administratorarbeitsbereich Optimierung

Auf der Seite „Optimierung“ können Sie Ihre vorhandenen Konfigurationen validieren und Konfigurationsprobleme lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Administratorarbeitsbereich Optimierungs-Homepage

Die Discovery-Administratorarbeitsbereich Die Optimierungs-Homepage bietet Tools zur Bewertung der Instanzintegrität durch konfigurierte Prüfungen und zeigt fehlgeschlagene Prüfungen nach Priorität, Kategorie und Suite an.

Ergebnisse der Optimierungsprüfung

Verwenden Sie die Optimierungstools, um Ihre Instanz nach Konfigurationen zu befragen, die Integritätsprobleme anzeigen und Möglichkeiten zur Behebung von Best Practices identifizieren. Die Optimierung überprüft Ihre vorhandenen Konfigurationen und hilft Ihnen, Probleme zu lösen. Weitere Informationen zum Ausführen von Prüfungen finden Sie unter Führen Sie Optimierungsprüfungen aus.

Führen Sie Optimierungsprüfungen aus

Optimierungsprüfungen sind Scans zur Optimierung von Konfigurationen, die in Suites gruppiert sind, deren spezifische Prüfungen unten aufgeführt sind.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Die konfigurierten Prüfungen sind auf den folgenden Registerkarten aufgeführt:

- Discovery-Suite
- MID-Suite
- Selbstüberwachungs-Suite

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Optimierung**an.
2. Wählen Sie Aus **Prüfungen** .
3. Wählen Sie aus, um manuell eine Prüfung für Discovery-Suite, MID-Suite oder Selbstüberwachungs-Suite auszuführen **Jetzt ausführen** .

   Hinweis:

   Der Instanzscan kann jeweils nur einzeln ausgeführt werden. Warten Sie also, bis der laufende Scan abgeschlossen ist, bevor Sie die Suite erneut ausführen.

4. Um auf weitere Informationen zu einem Problem zuzugreifen, wählen Sie den Namen der Prüfung aus.

   Hinweis:

   - Um das Problem zu verstehen, wählen Sie den Link „Prüfungsbeschreibung anzeigen“ aus.
   - Um weitere Details zum Problem zu erfahren, wählen Sie den Link Dokumentation im Prüfen aus.
   - Um die Definitionsseite anzuzeigen, wählen Sie den Link Definitionsseite überprüfen aus. Informationen zum Bearbeiten eines Schecks finden Sie unter Bearbeiten Sie eine vorhandene Prüfung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeiten Sie eine vorhandene Prüfung

Durch Bearbeiten der Definitionsprüfung können Sie Beschreibung und Skript ändern.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Optimierung**an.
2. Wählen Sie Aus **Überprüfen** .
3. Wählen Sie den Link Definitionsseite überprüfen aus.
4. Um die Prüfung zu bearbeiten, wählen Sie aus **Bereich wechseln** .
5. Aktualisieren Sie alle erforderlichen Details, und wählen Sie aus **Speichern** .

Hinweis: Wenn die Option aktiv aktiviert ist:

- Discovery-Suite wird einmal pro Woche am Sonntag um 8:00 UHR ausgeführt.
- MID-Suite wird einmal pro Woche am Sonntag um 10:00 UHR ausgeführt.
- Die Selbstüberwachungs-Suite wird alle 15 Minuten ausgeführt.

Discovery-Administratorarbeitsbereich-Einstellungen

Auf der Seite „Einstellungen“ können Sie allgemeine anpassen und verwalten Discovery Eigenschaften, sodass sie auf Ihre spezifischen Anforderungen zugeschnitten sind.

Um auf zuzugreifen Discovery-Administratorarbeitsbereich Diagnoseseite navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einstellungen**an.

Discovery -Eigenschaften

Dashboard-Zeitskala

Ermöglicht es Ihnen, die Integrität Ihrer Zeitpläne für die bevorzugte Zeitspanne anzuzeigen.

Verwenden Sie **Zeitskala** Dropdown-Liste zur Auswahl zwischen 7-, 14- und 30-tägigen Zeiträumen. Der Standardzeitraum beträgt 7 Tage. Nachdem Sie sie konfiguriert haben, werden alle relevanten Datenvisualisierungen auf den Seiten „Startseite“, „Zeitpläne“ und „Diagnose“ aktualisiert, um sie über diesen Zeitraum zu messen.

Wichtig: Nachdem diese Einstellungen gespeichert wurden, müssen Sie Ihren Browser aktualisieren, um die Datenvisualisierungen mit der neuen Zeitskala zu aktualisieren.

Sie können diese Einstellung auch konfigurieren, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** > **sn_Disco_Workspace.Discovery_stats_time_scale**an. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Anomalie-Erkennung

Identifiziert ungewöhnliches Verhalten , Wie fehlgeschlagene Ausführungen und erhebliche Abweichungen von den Schwellenwerten für hohe Fehleranzahlen, längere Dauer des Discovery-Status und weniger erkannte Konfigurationselemente (Configuration Items, CIs) oder Cloud-Ressourcen.

Anomalien werden in die folgenden Schweregradstufen kategorisiert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kritisch** : Zeitpläne, die nicht ausgeführt wurden
- **Schwerwiegend** : Zeitpläne mit einer niedrigen CI-Discovery-Rate
- **Geringfügig** : Zeitpläne mit langer Laufzeit oder hoher Fehleranzahl

Die **Aktivieren Sie die Anomalieerkennung** Mit dem Umschalter können Sie die Funktion aktivieren und deaktivieren. Diese Funktion ist standardmäßig aktiviert.

Warnung: Das Deaktivieren dieser Funktion wirkt sich erheblich auf aus Discovery Experience über mehrere Seiten, Diagramme und Tabellen hinweg.

Sie können diese Einstellung auch konfigurieren, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** > **sn_Disco_Workspace.Discovery_schedule_anomaly_Detection_disabled**an. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Erkennungsmethode

Identifiziert Anomalien in Discovery Zeitpläne mit den folgenden Ansätzen:

- **ML-basiert** : Nutzt Algorithmen für maschinelles Lernen (ML), um historische Zeitplandaten zu analysieren, komplexe Muster zu erkennen und Anomalien ohne vordefinierte Regeln zu erkennen.
- **Statistikbasiert** : Stützt sich auf traditionelle mathematische Techniken, z. B. die Berechnung von Standardabweichungen, um Ausreißer basierend auf festen numerischen Schwellenwerten zu identifizieren.

Wählen Sie aus **Erkennungsmethode** Dropdown-Liste, um einen Ansatz auszuwählen. Der ML-basierte Ansatz ist die standardmäßige Erkennungsmethode. Sie können diese Einstellung auch konfigurieren, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** > **sn_Disco_Workspace.Discovery_schedule_anomaly_Detection_method**an. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Sie können auch die Empfindlichkeit der Anomalieerkennung anpassen. Eine niedrigere Empfindlichkeit meldet mehr Anomalien, was zu mehr falsch positiven Ergebnissen führen kann, was bedeutet, dass normale Scans als Anomalien gekennzeichnet werden. Eine höhere Empfindlichkeit meldet weniger Anomalien, was zu mehr falsch negativen Ergebnissen führen kann, was bedeutet, dass tatsächliche Anomalien möglicherweise nicht erkannt werden.

Verwenden Sie **Empfindlichkeit** Dropdown-Liste, um Ihre bevorzugte Erkennungsempfindlichkeit auszuwählen. Auswahlmöglichkeiten: Niedrigste, Niedrig, hoch, höchste. Standardmäßig ist die Anomalieerkennung auf niedrige Empfindlichkeit festgelegt. Sie können diese Einstellung auch konfigurieren, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** > **sn_Disco_Workspace.Discovery_schedule_anomaly_ml_model_sensitivity**an. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Schwellenwerte anpassen

Das Anpassen von Schwellenwerten hilft, falsch positive Ergebnisse zu verhindern und sicherzustellen, dass normale Scans nicht versehentlich als Anomalien gekennzeichnet werden. Wenn die Anomalieerkennungsmethode einen kennzeichnet Discovery Status als Anomalie werden die Statusmetriken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf Abweichungen von den durchschnittlichen Messungen basierend auf den angegebenen Schwellenwerten analysiert.

Scans werden als anomal markiert, wenn die Laufzeit, die Fehleranzahl oder CI-Messungen um einen angegebenen Schwellenwert vom Durchschnitt abweichen. Der Standardschwellenwert beträgt 20 %, Sie können jedoch die Zahl ändern, die diesen Schwellenwert im entsprechenden Textfeld definiert. Auswählen **Zurücksetzen** Setzt den Schwellenwert auf den Standardwert von 20 % zurück.

Sie können diese Einstellung auch konfigurieren, indem Sie zu navigieren **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an. Schwellenwerteigenschaften umfassen: *sn_disco_workspace.discovery_schedule_runtime_anomaly_threshold*, *sn_disco_workspace.discovery_schedule_cis_discovered_anomaly_threshold*, Und *sn_disco_workspace.discovery_schedule_error_anomaly_threshold*. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Hinweis: Es werden keine Änderungen angewendet, bis Sie auswählen **Speichern** .

Anzeigen und filtern ITOM-Transparenz Apps, die verwenden Discovery-Administratorarbeitsbereich

Greifen Sie auf alle zu *ITOM-Transparenz*Apps von einem einzelnen Standort in Discovery-Administratorarbeitsbereich. Zeigen Sie die bereits auf Ihrer Instanz installierten Anwendungen und die zur Installation verfügbaren Anwendungen an, und filtern Sie sie. Verwenden Sie diese Funktion, um Anwendungen zu integrieren und zu verbessern Discovery Experience.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Auf dieser Seite können Sie neue Anwendungen installieren und vorhandene aktualisieren. Zum Aktualisieren von Anwendungen benötigen Sie die Administratorrolle.

Warum und wann dieser Vorgang ausgeführt wird

Sie können zwar auf Details zu den in Ihrer Instanz installierten Apps zugreifen, Informationen zu Preisen und Paketen werden jedoch nicht bereitgestellt, da sie je nach Vertrag variieren. Eine allgemeine Übersicht über Lizenzierungs- und Abonnementdetails finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**an.
2. Wählen Sie Aus **Alle anzeigen** In ITOM-Transparenz Abschnitt „Apps“.
   Die **Sichtbarkeitsanwendungen** Die Seite wird geöffnet und zeigt alle Anwendungen in zwei Kategorien getrennt an: **Installierte Anwendungen** Und **Nicht installierte Anwendungen** .
3. Verwenden Sie die Filter-Dropdown-Liste, um das gewünschte Abonnement für die Anzeige auszuwählen.

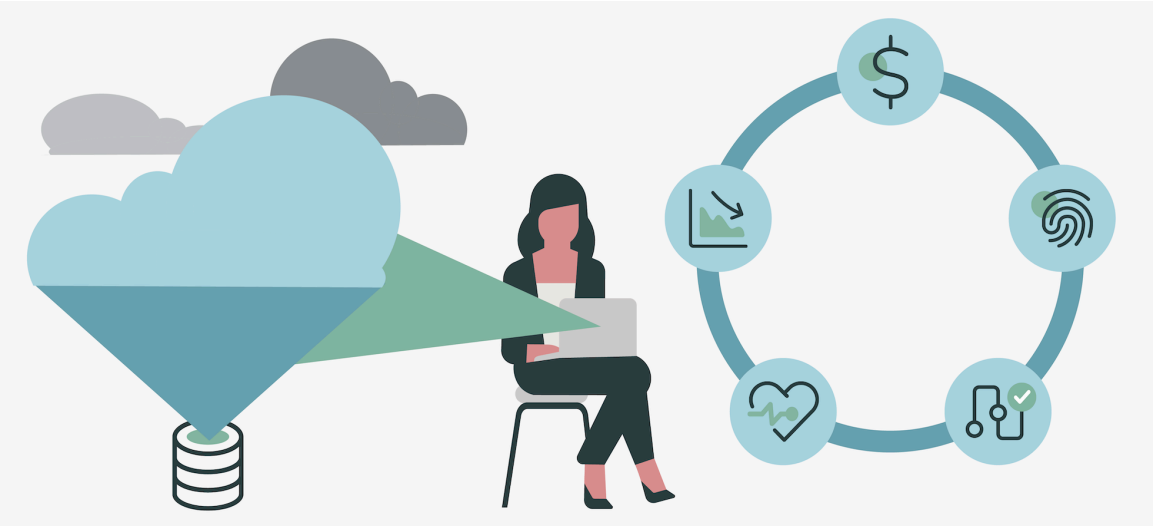
Cloud-Discovery erkunden

Cloud-Discovery ermöglicht IT-Abteilungen von Unternehmen, detaillierte Informationen über ihre cloudbasierte Infrastruktur zu sammeln. Cloud-Discovery findet Ressourcen bei wichtigen Cloud Service Providern.

Einführungsvideo zu Cloud-Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Discovery Sucht Ressourcen in den folgenden Cloud-Anbietern: Amazon AWS Cloud, Microsoft Azure Cloud, Google Cloud Platform (GCP), IBM Cloud Platform, Und Oracle Cloud-Infrastruktur (OCI). Cloud-Discovery Sammelt die logischen Rechenzentren, die dem Account zugeordnet sind, sowie alle Unterkonten. Das Sammeln von Informationen über Ressourcen in der Cloud ist relevant für Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service-Lösungen bereitstellen.



Servicekontobasierte Erkennung

Bei der servicekontobasierten Erkennung werden alle Ressourcen in einem Servicekonto erkannt. Diese Art der Erkennung erfasst Metadaten mithilfe der APIs des Cloud Providers und füllt dann die CMDB-Tabelle der Geräteinstanz mit Basisattributen. Die Service-Account-Discovery bietet Einblick in Tags, was die Datenberichterstellung und die Workflow-Automatisierung unterstützt. Beispielsweise können Cloud-Events verwendet werden, um die Erkennung bei Bedarf für Zielservices auszulösen. Dadurch kann Cloud-Discovery Änderungen erkennen und automatisch die CMDB aktualisieren.

IP-basierte Erkennung

Der andere Typ von Cloud-Discovery, IP-basierte Discovery, verwendet die Metadaten, die aus der Service-Account-basierten Discovery erfasst wurden, um detailliertere Informationen zu sammeln. Dieser Typ stellt Daten über installierte Software, Prozessinformationen, TCP/IP-Verbindungen usw. bereit.

Cloudbasierte Erkennungsmethoden

Cloud-Discovery verwendet Erkennungsmuster, um Geräte und Anwendungen abzufragen und Informationen darüber zu sammeln. Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Mit sind viele Cloud-Muster verfügbar Cloud-Discovery Die die Discovery von unterstützen AWS , Azure , GCP , OCI , IBM , Und OpenStack . Darüber hinaus werden im ServiceNow Store regelmäßig neue Muster verfügbar.

Ihre Instanz kann auch Benachrichtigungen und Warnungen aus der Cloud-Umgebung erkennen. Diese Events werden über eine REST-Verbindung an Ihre Instanz gesendet. Ihre Instanz kann diese Events dann verarbeiten und CIs in CMDB entsprechend aktualisieren.

Hinweis: Ereignisgesteuerte Discovery für Amazon AWS Cloud, Microsoft Azure Cloud, Und Google Cloud Platform Erfordert nicht Cloud Provisioning and Governance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressourcen verwalten

Die Instanz zeigt alle Ergebnisse von Cloud-Discovery auf der Discovery-Homepage an. Sie können Drilldowns zu bestimmten Zeitplänen, erkannten Geräten, Cloud-Ressourcen und Fehlern durchführen. Sortieren Sie diese Ergebnisse, um sie genauer zu betrachten, und zeigen Sie Erkennungstrends für die erkannten Geräte an. Anhand von Fehlermeldungen erhalten Sie konkrete Empfehlungen zur Behebung von Problemen.

Cloud-Discovery auf ServiceNow AI Platform

Cloud-Discovery Verwendet MID-Server Dient zum Zugriff auf externe Geräte und Anwendungen im lokalen Netzwerk eines Unternehmens. Weitere Informationen zu den Fähigkeiten von MID-Server in Bezug auf Cloud-Discovery finden Sie unter MID-Server .

Cloud Provisioning and Governance hängt von den von Cloud-Discovery gefundenen Informationen ab. Cloud Provisioning and Governance bietet eine einzige Oberfläche, über die Sie auf Cloud-Ressourcen zugreifen, Cloud-Angebote in einem Katalog veröffentlichen und die Nutzung dieser Ressourcen verwalten können.

Darüber hinaus verwenden die folgenden Geschäftsbereiche und Produkte von ServiceNow AI Platform die Informationen, die Cloud-Discovery liefert: IT Service Management, Security Incident Response, Hardware Asset Management, Software Asset Management, Governance, Risk und Compliance und Anwendungs-Portfoliomanagement.

Cloud-Discovery Setup mit Discovery-Startseite

Erste Schritte mit Cloud-Discovery Indem Sie Anmeldeinformationen, Service-Accounts, Zeitpläne und konfigurieren MID Servers.

Das Einrichten von Cloud-Discovery ist die erste Stufe der Cloud-Erkennung und der Verwendung von Cloud Provisioning and Governance zur Verwaltung erkannter Cloud-Ressourcen.

Cloud-Discovery ist Teil von ServiceNow AI Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Cloud-Discovery gelten.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Bewerten Sie Ihre Cloud-Bereitstellung, und planen Sie, wie Sie darin eine Erkennung durchführen möchten.
2. Discovery anfordern.
3. Installieren und konfigurieren Sie die MID Server.
4. Richten Sie Servicekonten ein, und konfigurieren Sie den Zugriff darauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wird eingerichtet AWS Service-Accounts
- Servicekonten für Azure erstellen
- Servicekonten für GCP erstellen
- Servicekonten für VMware erstellen

5. Für Amazon AWS Cloud Und Microsoft Azure Cloud, Konfigurieren Sie Benachrichtigungen und Warnungen aus dem Amazon AWS Cloud Und Microsoft Azure Cloud Um die erforderlichen Aktualisierungen an vorzunehmen CMDB Ohne zusätzliches Scannen.
   - Konfigurieren Sie AWS Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz
   - Konfigurieren Sie Microsoft Azure Warnungsservice zum automatischen Aktualisieren von CMDB
   - Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB
   - Konfigurieren Sie VMware-EventsService zum automatischen Aktualisieren von CMDB

   Hinweis: Für die eventgestützte Erkennung ist Cloud Provisioning and Governance nicht erforderlich.

6. Stellen Sie sicher, dass Ihre ServiceNow-Instanz über die relevanten Muster und CI-Klassen (Typen) für Cloud-Ressourcen verfügt. Möglicherweise müssen Sie die neueste Version der folgenden Anwendungen aus dem ServiceNow Store bereitstellen.
   - Discovery and Service Mapping Patterns
   - CMDB CI Class Models
7. Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen.

Cloud-Discovery Setup mit Cloud Operations Workspace

Führen Sie die erforderlichen Verfahren aus, um sich auf die Erkennung von Ressourcen-CIs in der Cloud vorzubereiten.

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

Das Einrichten von Cloud-Discovery ist die erste Stufe der Cloud-Erkennung und der Verwendung von Cloud Provisioning and Governance zur Verwaltung erkannter Cloud-Ressourcen.

Cloud-Discovery ist Teil von ServiceNow AI Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Cloud-Discovery gelten.

Cloud Operations Workspace stellt eine erweiterte Möglichkeit zum Erstellen von Discovery-Zeitplänen bereit. Sie können auch die für die Erkennung von Cloud-Ressourcen erforderlichen Voraussetzungen überprüfen, z. B. Anmeldeinformationen und Servicekonten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Bewerten Sie Ihre Cloud-Bereitstellung, und planen Sie, wie Sie darin eine Erkennung durchführen möchten.
2. Discovery anfordern.
3. Installieren Sie Cloud Discovery Workspace .
4. Installieren und konfigurieren Sie die MID Server.
5. (Für Amazon AWS Cloud und Microsoft Azure Cloud) Konfigurieren Sie Benachrichtigungen und Warnungen von Amazon AWS Cloud und Microsoft Azure Cloud, um die erforderlichen Aktualisierungen an Ihrer CMDB ohne zusätzliches Scannen vorzunehmen.
   - Konfigurieren Sie AWS Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz
   - Konfigurieren Sie Microsoft Azure Warnungsservice zum automatischen Aktualisieren von CMDB
   - Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB
   - Konfigurieren Sie VMware-EventsService zum automatischen Aktualisieren von CMDB

   Hinweis: Für die eventgestützte Erkennung ist Cloud Provisioning and Governance nicht erforderlich.
6. Stellen Sie sicher, dass Ihre ServiceNow-Instanz über die relevanten Muster und CI-Klassen (Typen) für Cloud-Ressourcen verfügt. Möglicherweise müssen Sie die neueste Version der folgenden Anwendungen aus dem ServiceNow Store bereitstellen.
   - Muster für Discovery und Service-Mapping
   - CMDB CI Class Models
7. Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Zugehörige Informationen

Cloud Operations Workspace

Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Erstellen Sie abhängig von der von Ihnen gewählten Cloud Discovery-Methode (Servicekonten oder IP-Bereiche) Zeitpläne für die Erkennung von Cloud-Ressourcen.

Discovery-Manager-Schnittstelle

Verwenden Sie die Schnittstelle zur Cloud-Discovery-Zeitplankonfiguration, um die Informationen einzugeben, die Sie für den Zugriff auf Ihre Servicekonten und Unterkonten benötigen. Sie können die Anmeldeinformationen angeben, um ausgewählte Konten zu validieren. Testen Sie die Verbindungen zu Ihren Konten, und erstellen Sie dann Zeitpläne, um die Cloud-Ressourcen in den ausgewählten Rechenzentren zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Begriff „Unterkonten“ wird allgemein in verwendet Cloud-Discovery Schnittstelle für Zeitplankonfiguration. Ihre Bedeutung variiert je nach Cloud-Anbieter:

- In AWS, Unterkonten beziehen sich auf Mitgliedskonten unter einem Verwaltungs-Account.
- In Microsoft Azure, Das Äquivalent ist ein Abonnement.
- In Google Cloud Platform(GCP), Cloud-Discovery Ziele für Projekte.

Fortschrittsanzeige

Während Sie die einzelnen Konfigurationsphasen abschließen, können Sie den Fortschritt auf den Registerkarten oben im Discovery-Manager nachverfolgen. Abgeschlossene Phasen werden durch ein Häkchen gekennzeichnet. Ein dunkler Unterstrich markiert die aktuelle Phase. Die Registerkarten sind interaktiv, sodass Sie zu einer Phase wechseln können, indem Sie auf die entsprechende Registerkarte klicken.

Discovery-Manager-Bezeichnungen anpassen

Die Tabelle „Feldoptionen für Servicekonten“ [service_account_field_options] enthält Felder zum Ändern der Bezeichnungen im Discovery-Manager. Über diese Felder können Sie den Discovery-Manager für die Verarbeitung neuer Service Provider anpassen oder vorhandene Bezeichnungen ändern, um interne Richtlinien zu erfüllen. Beispielsweise lautet die Bezeichnung für die Microsoft Azure-Konto-ID standardmäßig „Microsoft Azure-Abonnement-GUID“. Sie können sie je nach Bedarf in „Abonnement-ID“, „Konto-ID“ oder in eine beliebige andere Einstellung ändern.

Servicekonto auswählen und Anmeldeinformationen testen

Geben Sie Ihren Cloud-Provider an, und wählen Sie das zu erkennende Servicekonto aus. Sie können ein oder alle verfügbaren Unterkonten in einen Zeitplan aufnehmen. Wählen Sie die Anmeldeinformationen für das Cloud-Servicekonto aus, und testen Sie die Verbindung.

Vorbereitungen

Bevor Sie versuchen, Cloud-Discovery zu konfigurieren, benötigen Sie mindestens einen validierten MID-Server mit dem Status **In Betrieb**. Der MID-Server muss die IP-Bereiche erreichen, auf die sich die Erkennung beziehen soll. Sie können den MID-Server mithilfe des geführten Setups MID-Server verwenden oder durch manuelles Herunterladen und Ausführen des Installationsprogramms installieren. Weitere Informationen können Sie den MID-Server-Installationsanweisungen für Linux und Windows entnehmen. Stellen Sie sicher, dass Sie den für Cloud-Discovery verwendeten MID-Server mit Cloud-Management-Funktionalität konfigurieren.

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow® Cloud-Discovery-Assistent beginnt mit der Kontoauswahl und der Testphase. Verwenden Sie zur Vermeidung langer Wartezeiten oder unerwarteter Zeitüberschreitungen die Systemeigenschaft `cdu.record.watcher.timeout`, um die maximale Wartezeit für diese Cloud-Discovery-Konfigurationsprozesse zu definieren:

- Servicekonto validieren
- Mitgliedskonto-Discovery
- Discovery für logische Rechenzentren

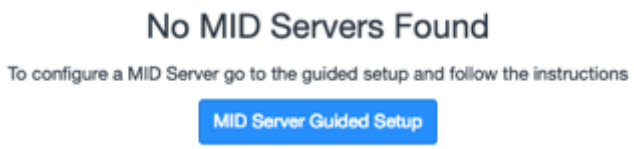
Der Standardwert für die Zeitüberschreitung beträgt 300.000 Millisekunden bzw. 5 Minuten.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**, Und klicken Sie dann auf **Erkennen Sie Cloud-Ressourcen** Im Willkommensbildschirm.

   Hinweis: Der Willkommensbildschirm enthält einen Link zu Discovery Schnellstart. Dieser Assistent wurde entwickelt, um schnell eine grundlegende Discovery einzurichten. Sie können Schnellstart verwenden, um Discovery auszuwerten oder um neue Netzwerkgeräte zu erkunden. Die Anleitung ist jedoch nicht für die Erkennung von Cloud-Ressourcen konzipiert.

   Wenn das System eine entsprechende nicht erkennen kann MID-Server, Sie werden aufgefordert, eine zu installieren und zu konfigurieren MID-Server Mithilfe von Geführtes Setup für MID-Server . Diese Benachrichtigung wird auch angezeigt, wenn ein vorhandener MID-Server aufgrund eines Upgrades nicht verfügbar ist.

2. Wählen Sie im Bereich „Grundlegende Informationen“ des Discovery-Managers im Feld **Provider** den Namen Ihres Cloud-Providers aus, zum Beispiel **AWS** oder **Azure**.
   Im Bereich „MID Servers“ des Assistenten wird die Anzahl der validierten und verfügbaren MID Servers angezeigt.
3. Wenn Sie verwenden AWS, Azure, Oder GCP, Sie können angeben MID-Server Auswahltyp in **MID-Auswahltyp** Feld.

   Hinweis: AWS Und Azure Die Auswahl ist erst nach der Migration zu musterbasiert verfügbar Discovery. Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

   Die folgenden Optionen sind verfügbar:

   - **MID-Server automatisch auswählen**: Der Assistent verwendet automatisch einen geeigneten MID-Server.
   - **Spezifischer MID-Server**: Der Assistent verwendet den im Feld **MID-Server** angegebenen MID-Server. Um MID Servers zu filtern und anzuzeigen, die für die Übernahme einer IAM-Rolle zur Erkennung von Cloud-Ressourcen konfiguriert sind, aktivieren Sie die Option **Discovery ohne Anmeldeinformationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn nicht MID-Server Hat die Cloud-Management-Fähigkeit, klicken Sie auf **Konfigurieren Sie MID-Server** Und konfigurieren Sie eine entsprechend.

   a. Navigieren zu **MID-Server** > **Fähigkeiten**an.

   b. Wählen Sie aus der Liste der MID-Server-Fähigkeiten **Cloud Management** aus.
   Sie können auch **ALLE** auswählen, wodurch Cloud Management standardmäßig eingeschlossen ist.

   c. In MID ServersZugehörige Liste, klicken Sie auf **Bearbeiten** Und fügen Sie dann Ihren hinzu MID Servers Zur Fähigkeit.

   d. Klicken Sie auf **Speichern**.
   Ihre MID Servers sind für die Kommunikation mit Ihren Cloud-Servicekonten bereit.

5. Geben Sie im Feld **Zeitplanname** einen eindeutigen und beschreibenden Namen für den Zeitplan ein.

6. Wählen Sie im Bereich „Servicekonten“ ein vorhandenes Konto für den neu benannten Zeitplan aus.
   Wenn Sie ein vorhandenes Konto auswählen, füllt das System das Formular automatisch mit den verfügbaren Informationen. Wenn Sie ein Konto hinzufügen, müssen Sie die Konto-ID, Anmeldeinformationen und gegebenenfalls die URL angeben. Für VMware müssen Sie die URL angeben.
   - Die AWS-Konto-ID entspricht der Konto-ID.
   - Die Azure-Konto-ID entspricht der Azure-Abonnement-GUID.
   - Die GCP-Konto-ID entspricht der Projekt-ID.
   - Die VMware-Konto-ID entspricht der UUID der VM-Instanz.

   Hinweis: Die VMware-Erkennung kann ohne Servicekonto ausgeführt werden. Um VMware-Ressourcen zu erkennen, konfigurieren Sie den Zeitplan zur Ausführung für die IP-Adresse des vCenter-Servers .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie die Anmeldeinformationen für dieses Cloud-Servicekonto aus, oder fügen Sie neue Anmeldeinformationen hinzu.

   a. Um Anmeldeinformationen hinzuzufügen, klicken Sie auf das Pluszeichen (**+**).

   b. Wählen Sie den entsprechenden Typ der Cloud-Anmeldeinformationen in der Liste aus.

   c. Füllen Sie das Formular aus, und klicken Sie auf **Speichern**.

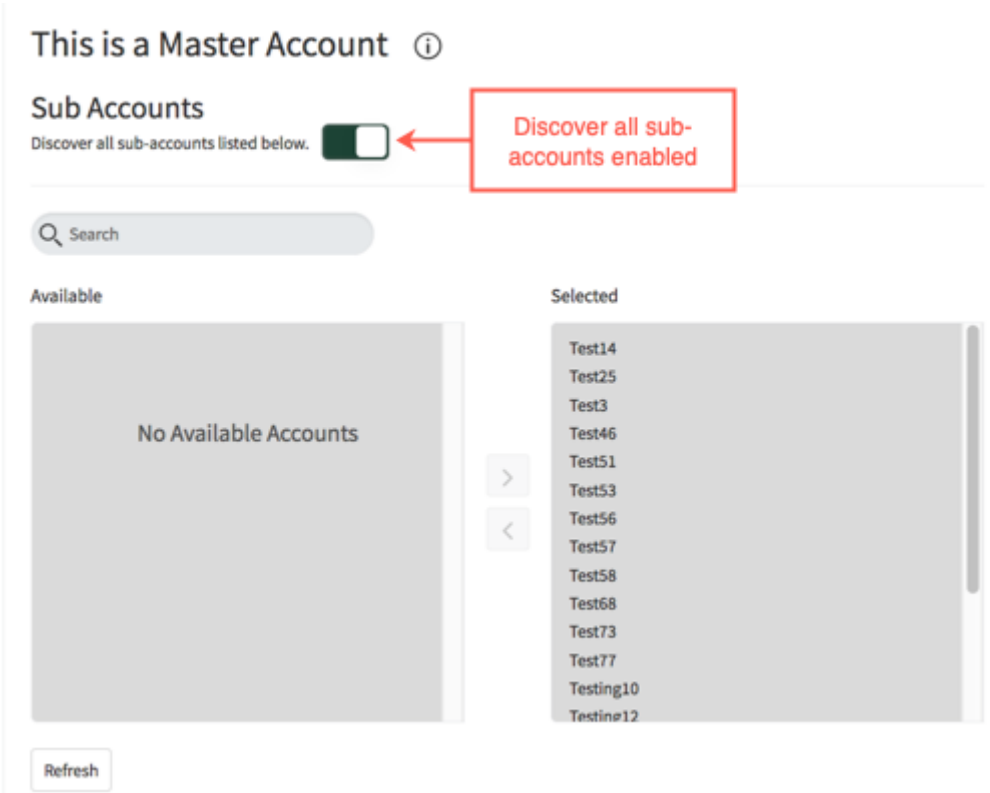
   Hinweis: Sie können AWS so konfigurieren, dass temporäre Anmeldeinformationen für Servicekonten generiert werden. Mit dieser Funktionalität müssen keine Anmeldeinformationen für die Instanz definiert werden. Dadurch erhöht sich die Sicherheit Ihrer Mitgliedskonten (Unterkonten). Details finden Sie unter Zugriff für AWS-Servicekonten einrichten.

8. Klicken Sie auf **Testaccount**, um das Konto mit den angegebenen Details zu validieren.

Nachrichten in der Headerleiste benachrichtigen Sie über die Validierungsergebnisse. Wenn Sie ein Verwaltungskonto angegeben haben und der Verbindungstest erfolgreich war, zeigt der Assistent einen Auswahlbildschirm für alle Mitgliedskonten an, die dem Verwaltungskonto zugeordnet sind. Standardmäßig sind alle aktuellen Mitgliedskonten für den Zeitplan ausgewählt und können nicht in die Liste „Verfügbar“ verschoben werden.

Hinweis:

Wenn der Validierungsprozess keine oder kürzlich hinzugefügte Unterkonten zurückgibt, klicken Sie auf **Mitglieder aktualisieren**, oder führen Sie den Validierungsprozess erneut aus. Wenn bei der Validierung wiederholt Zeitüberschreitungen auftreten, erhöhen Sie das Zeitüberschreitungsintervall in der MID Server-Eigenschaft `cdu.record.watcher.timeout`.

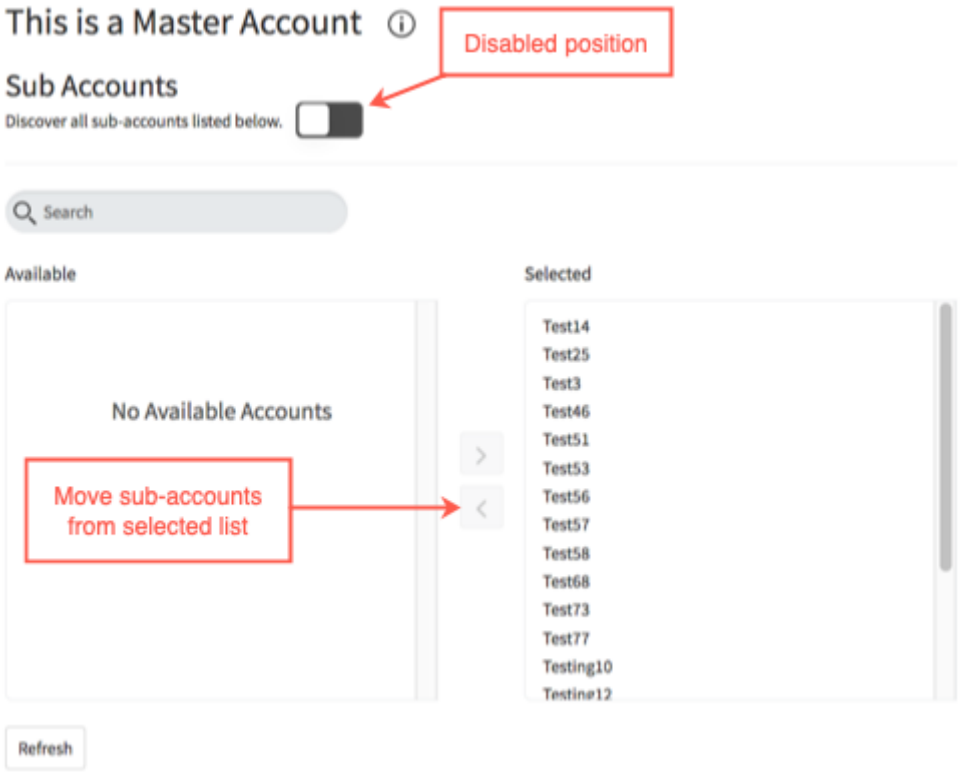


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Um bestimmte Unterkonten für den Zeitplan auszuwählen, deaktivieren Sie die automatische Auswahlfunktion.

   Standardmäßig sind alle Unterkonten ausgewählt. Um die Funktion zu deaktivieren und die Auswahl bestimmter zu erkennender Rechenzentren zuzulassen, schieben Sie den Umschalter nach links.



10. Um ein Unterkonto auszuschließen, ziehen Sie das Unterkonto aus der Liste „Ausgewählt“ in die Liste „Verfügbar“.
11. Klicken Sie auf **Weiter**.

Zu erkennendes Cloud Provider-Rechenzentrum auswählen

Cloud-Discovery Zeigt die Liste der verfügbaren Rechenzentren an, wenn Sie den Service-Account validieren. Geben Sie an, welche Rechenzentren mit diesem Zeitplan erkannt werden sollen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Um die zu erkennenden Rechenzentren auszuwählen, klicken Sie in der Registerkartenleiste des Discovery-Managers auf die Phase **Rechenzentren auswählen**.
   Standardmäßig werden alle dem Servicekonto zugeordneten Rechenzentren für den Cloud-Discovery -Zeitplan ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn keine Rechenzentren angezeigt werden, wählen Sie **Rechenzentren aktualisieren** aus, oder führen Sie die Kontovalidierung erneut aus. Wenn bei der Validierung wiederholt Zeitüberschreitungen auftreten, erhöhen Sie das Zeitüberschreitungsintervall in der Eigenschaft `cdu.record.watcher.timeout` MID-Server.
- Sie können Cloud-Discovery so konfigurieren, dass die Liste der Unterkonten und Rechenzentren vor jeder geplanten Erkennung automatisch aktualisiert wird. Weitere Informationen finden Sie unter Automatische Aktualisierung von Unterkonten und Rechenzentren aktivieren.

2. Um bestimmte Rechenzentren für den Zeitplan auszuwählen, deaktivieren Sie die automatische Auswahlfunktion, indem Sie verschieben **Erkennen Sie alle unten aufgeführten Rechenzentren** Umschalter nach links.
3. Verschieben Sie die Rechenzentren, die Sie erkennen möchten, aus der Liste **Verfügbar** in die Liste **Ausgewählt**.
4. Wählen Sie in der Registerkartenleiste die nächste Phase aus.
   Falls erforderlich, y OE kann IP-Bereiche konfigurieren, um virtuelle Computer (VM) zu erkennen, oder zur Zeitplanphase wechseln und abschließen Cloud-DiscoverySetup.

Erkennung von virtuellen Maschinen aktivieren

Während der Erkennung der Cloud-Ressourcen können Sie virtuelle Maschinen (VMs) erkennen. Cloud-Discovery führt eine umfassende Erkennung der durch den Cloud-Zeitplan identifizierten virtuellen Maschinen (VMs) anhand ihrer IP-Adressen aus.

Vorbereitungen

Alle MID Servers Sie beabsichtigen, für zu verwenden Cloud-Discovery Muss validiert sein, den Status haben **Aktiv** , Und sie können auf die IP-Bereiche im Cloud-Provider-Account zugreifen.

Wichtig: Der Upgradeprozess von Madrid Bis New York Deaktiviert die vorhandene Cloud-Discovery Zeitpläne. Stellen Sie sicher, dass Sie alle Zeitpläne im Discovery Manager erneut aktivieren, die während eines Upgrades von möglicherweise deaktiviert wurden Madrid. Diese Zeitpläne haben einen **Ausführen** Status von **Nicht definiert** In der Tabelle „Discovery-Zeitplan“ [Discovery_schedule].

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Für die mit Cloud-Discovery verwendeten MID Servers müssen Sie keine IP-Bereiche konfigurieren. Cloud-Discovery wählt die IP-Adressen der virtuellen Maschinen automatisch in den Rechenzentren aus, die Sie im Assistenten ausgewählt haben.

Prozedur

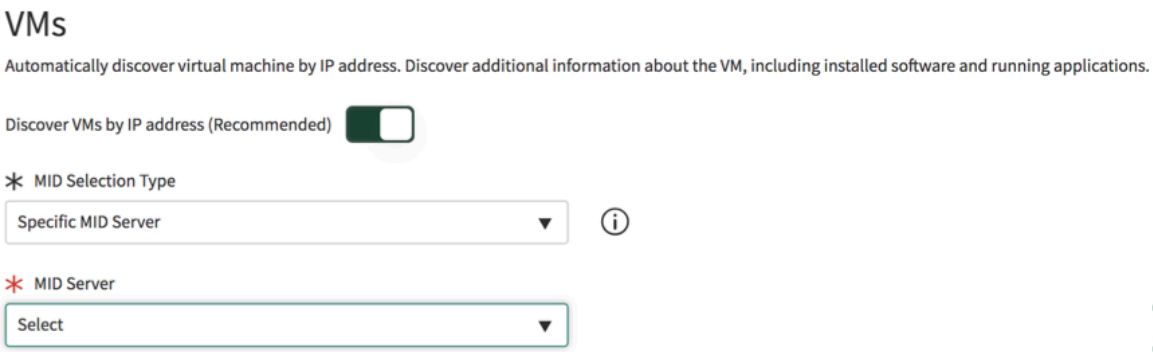
1. Zur Erkennung der VMs, die Teil des aktuellen Zeitplans sind, klicken Sie in der Registerkartenleiste des Discovery-Managers auf die Phase **Virtuelle Computer erkennen (optional)**.

   Die Erkennung von virtuellen Maschinen (VMs) ist standardmäßig aktiv.

   Hinweis: Um mehr über die Funktionsweise von zu erfahren **Virtuelle Computer erkennen (optional)** Informationen zu Cloud-Discovery finden Sie im KB-artikel Wie funktioniert „virtuelle Maschine erkennen“ (optional) in Cloud-Discovery .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie den zu verwendenden MID-Server aus.
   Die folgenden Optionen sind verfügbar:
   - **Automatische Auswahl**: Discovery wählt automatisch einen geeigneten MID-Server aus.
   - **Spezifischer MID Server-Cluster**: Discovery verwendet das genannte MID-Server-Cluster.
   - **Spezifischer MID Server**: Discovery verwendet den genannten MID-Server.



3. Um die VM-Erkennung zu deaktivieren, schieben Sie den Schalter **VMs anhand IP-Adresse erkennen** nach links.
   Das Feld **MID-Auswahltyp** wird ausgeblendet.
4. Wählen Sie aus **Zeitplan Erstellen** Phase in der Registerkartenleiste.

Laufzeit für einen Cloud-Discovery-Zeitplan festlegen

In der letzten Phase des Assistenten für Discovery-Manager wird der Zeitplan erstellt, der die Erkennung der Cloud-Ressourcen auslöst.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch über das Formular „Discovery-Zeitplan“ auf die Zeitplanphase des Discovery-Managers zugreifen. Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und klicken Sie auf **Cloud-Discovery** In der Liste Zeitpläne.

Prozedur
1. Um den Cloud Discovery-Zeitplan zu konfigurieren, wählen Sie in der Registerkartenleiste des Discovery-Managers die Option **Zeitplan erstellen** aus.
   Der Zeitplan ist standardmäßig aktiv.
2. Konfigurieren Sie, wann und wie oft der Zeitplan ausgeführt werden soll, und definieren Sie einen Zeitüberschreitungsschwellenwert, wenn Sie einschränken möchten Cloud-DiscoveryAuf eine bestimmte Dauer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Zum Deaktivieren des Zeitplans verschieben Sie den Schalter **Aktiv** nach links.
4. Schließen Sie ab Cloud-Discovery Zeitplanung Verarbeiten Sie, indem Sie eine der folgenden Optionen auswählen:
   - **Beenden und ausführen** : Ausführungen DiscoverySofort unter Verwendung der aktuellen Konfiguration. Alle nachfolgenden Cloud-Erkennungen werden gemäß dem von Ihnen angegebenen Zeitplan ausgeführt.
   - **Fertigstellen**: Beendet den Assistenten und führt Cloud-Discovery gemäß dem von Ihnen angegebenen Zeitplan aus.

Nächste Maßnahme
Öffnen Sie Discovery-Homepage Und zeigen Sie die Ergebnisse von an Discovery.

Automatische Aktualisierung von Unterkonten und Rechenzentren aktivieren

Konfigurieren Sie die Cloud-Discovery, um die Liste der Unterkonten und Rechenzentren vor jeder geplanten Erkennung automatisch zu aktualisieren. Wenn von Cloud-Discovery neue Unterkonten oder Rechenzentren identifiziert werden, werden sie der Configuration Management Database (CMDB) hinzugefügt und in den Discovery-Zeitplan aufgenommen.

Vorbereitungen
Erforderliche Rolle: Discovery_ Administrator

Warum und wann dieser Vorgang ausgeführt wird
Von Cloud-Discovery kann die Liste der Unterkonten und Rechenzentren, die von einem Discovery-Zeitplan abgedeckt werden, automatisch aktualisiert werden, sofern die folgenden Kriterien erfüllt sind:

- Der Cloud-Provider ist Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform (GCP).
- Die Eigenschaft `glide.discovery.cdu.auto_refresh_sub_accounts_and_ldcs` ist auf `true` festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Cloud-Discovery Zeitplan wird für einen Verwaltungsaccount erstellt.
- Die Cloud-Discovery Der Zeitplan ist so konfiguriert, dass die Ressourcen aller Unterkonten und Rechenzentren des Verwaltungs-Accounts erkannt werden.

Hinweis: Der Begriff „Unterkonten“ wird allgemein in verwendet Cloud-Discovery Schnittstelle für Zeitplankonfiguration. Ihre Bedeutung variiert je nach Cloud-Anbieter:

- In AWS, Unterkonten beziehen sich auf Mitgliedskonten unter einem Verwaltungs-Account.
- In Azure ist das entsprechende Abonnement.
- In Google Cloud Platform(GCP), Cloud-Discovery Ziele für Projekte.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach dem folgenden Systemeigenschaftsdatensatz, und öffnen Sie den Datensatz.

   `glide.discovery.cdu.auto_refresh_sub_accounts_and_ldcs`
3. Ändern Sie im Formular das Feld „Wert“ in `true`.
4. Wählen Sie **Aktualisieren**.

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Erstellen Sie abhängig von der von Ihnen gewählten Discovery-Methode (Servicekonten oder IP-Bereiche) Zeitpläne für die Discovery von Cloud-Ressourcen. Im Discovery-Zeitplan werden die verschiedenen Einstellungen für die Cloud-Discovery definiert.

Vorbereitungen

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

- Überprüfen Sie diese Version 1.7.1 oder höher von Cloud Operations Workspace Anwendung ist auf installiert ServiceNow AI Platform. Weitere Informationen finden Sie unter Cloud Operations Workspace installieren.
- Bevor Sie versuchen, Cloud-Discovery zu konfigurieren, benötigen Sie mindestens einen validierten MID-Server mit dem Status **In Betrieb**. Der MID-Server muss die IP-Bereiche erreichen, auf die sich die Erkennung beziehen soll. Sie können den MID-Server mithilfe des geführten Setups MID-Server verwenden oder durch manuelles Herunterladen und Ausführen des Installationsprogramms installieren. Weitere Informationen können Sie den MID-Server-Installationsanweisungen für Linux und Windows entnehmen. Stellen Sie sicher, dass Sie den für Cloud-Discovery verwendeten MID-Server mit Cloud-Management-Funktionalität konfigurieren.
- Vergewissern Sie sich, dass auf der ServiceNow AI Platform geeignete Anmeldeinformationen verfügbar sind, damit eine Verbindung mit den Servicekonten hergestellt werden kann, für die Sie die Discovery durchführen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Musterbasierte Discovery wird standardmäßig ausgeführt. In Szenarien, in denen die neueste Musteranwendung nicht installiert ist, schlägt die Discovery fehl, und Sie werden aufgefordert, die CAPI-basierte Discovery zu installieren oder zu migrieren. Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow® Cloud-Discovery-Assistent beginnt mit der Kontoauswahl und der Testphase. Verwenden Sie zur Vermeidung langer Wartezeiten oder unerwarteter Zeitüberschreitungen die Systemeigenschaft `cdu.record.watcher.timeout`, um die maximale Wartezeit für diese Cloud-Discovery-Konfigurationsprozesse zu definieren:

- Servicekonto validieren
- Mitgliedskonto-Discovery
- Discovery für logische Rechenzentren

Der Standardwert für die Zeitüberschreitung beträgt 300.000 Millisekunden bzw. 5 Minuten.

Sie können konfigurieren Cloud-Discovery Dient zum automatischen Aktualisieren der Liste der Unterkonten und Rechenzentren vor jeder geplanten Discovery. Weitere Informationen finden Sie unter Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > `Cloud Operations Workspace` > `Cloud-Discovery`an.
2. Wählen Sie **Neuer Discovery-Zeitplan**.
3. Wählen Sie den Cloud Provider aus.
   a. Füllen Sie die Werte im Formular „Choose the provider (Anbieter auswählen)“ aus.
   Eine Beschreibung der Formularfelder finden Sie unter Erstellen Sie einen neuen Discovery-Zeitplan-Formularreferenz.
   b. Wählen Sie **Weiter**.
4. Wählen Sie einen Serviceaccount für den Cloud-Discovery-Zeitplan aus, oder erstellen Sie einen Serviceaccount.

   Beschreibungen der Felder für den Serviceaccount finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars. Wenn Sie ein vorhandenes Konto auswählen, füllt das System das Formular automatisch mit den verfügbaren Informationen.

   Hinweis: Die Discovery für VMware kann ohne Servicekonto ausgeführt werden. Um VMware-Ressourcen zu erkennen, konfigurieren Sie den Zeitplan zur Ausführung für die IP-Adresse des vCenter-Servers.

   a. **Wahlweise:** Um die Verbindung mit dem Servicekonto zu überprüfen, wählen Sie **Testaccount** aus.

   b. **Wahlweise:** Wenn Sie den Discovery-Zeitplan für einen Verwaltungsaccount erstellen, geben Sie an, ob alle Mitgliedsaccounts oder nur bestimmte Mitgliedsaccounts erkannt werden sollen.
   Standardmäßig werden alle vorhandenen Mitgliedsaccounts für den Discovery-Zeitplan ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. **Wahlweise:** Wenn Sie den Discovery-Zeitplan für einen Verwaltungsaccount erstellen und der Validierungsprozess die Unteraccounts nicht zurückgibt, wählen Sie **Aktualisieren**, oder wiederholen Sie die Accountvalidierung.

d. Wählen Sie **Weiter**.

5. Rechenzentren für Discovery-Zeitplan auswählen.
Sie können entweder alle mit dem Servicekonto verbundenen Rechenzentren oder bestimmte Rechenzentren auswählen.

a. **Wahlweise:** Wenn Sie bestimmte Rechenzentren erkennen möchten, wählen Sie die **Rechenzentren** in der Dropdown-Liste „Rechenzentren auswählen“ aus.

b. **Wahlweise:** Wenn keine Rechenzentren angezeigt werden, wählen Sie **Rechenzentren aktualisieren**, oder wiederholen Sie die Accountvalidierung.

c. Wählen Sie **Weiter**.

6. **Wahlweise:** Geben Sie an, ob Sie virtuelle Computer (VM) und ihre Attribute erkennen möchten.

a. **Wahlweise:** Geben Sie an, ob Sie die VM-Discovery mit durchführen möchten AWS Systemmanager.

Hinweis: Diese Option wird nur angezeigt, wenn die Systemeigenschaft verwendet wird `glide.discovery.enable_ssm`Ist aktiviert und **AWS** Ist in Schritt 3 als Cloud-Anbieter ausgewählt.

b. Wählen Sie einen MID-Server oder ein MID-Cluster aus, von dem die VMs erkannt werden können. Wenn Sie sich bei der MID-Auswahl nicht sicher sind, wählen Sie **Automatische Auswahl***MID-Server*.

c. Wählen Sie **Weiter**.

7. Erstellen Sie einen Zeitplan für die Ausführung der Cloud-Discovery.

a. Wählen Sie eine Ausführungshäufigkeit für den Cloud-Discovery-Zeitplan aus.

b. Geben Sie eine Startzeit für die Ausführung der Discovery an.

c. **Wahlweise:** Geben Sie Kriterien zum Abbrechen der Discovery an.

d. Aktivieren Sie den Discovery-Zeitplan.

8. Führen Sie eine der folgenden Aktionen aus.

Option	Beschreibung
Beenden und ausführen	Von Cloud-Discovery wird der Zeitplan gespeichert und ausgeführt.
Fertigstellen	Cloud-Discovery speichert den Zeitplan und führt ihn gemäß der definierten Häufigkeit aus.

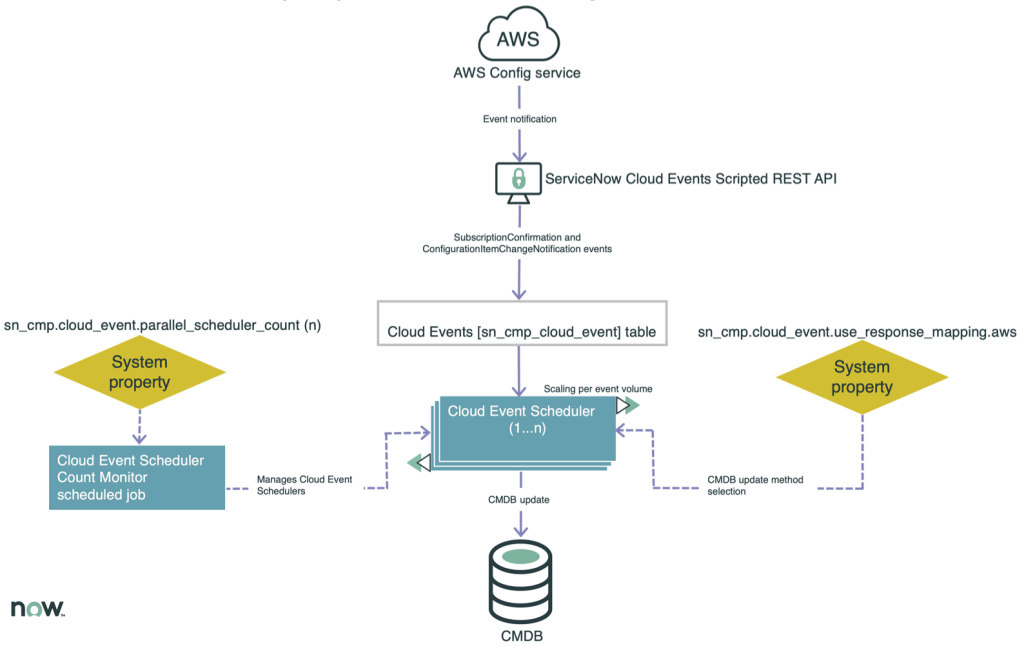
AWS Ereignisgesteuerte Discovery

Die Amazon Web Services(AWS) Der Konfigurationsservice kann Ereignisse für alle Änderungen am Lebenszyklusstatus oder der Konfiguration einer Cloud-Ressource auslösen. Die ServiceNow® Die ereignisgesteuerte Discovery verwendet die Ereignisse,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um die neuesten Ressourceninformationen in automatisch zu aktualisieren Configuration Management Database (CMDB).

Übersicht über AWS Ereignisgesteuerte Discovery



Konfigurieren Sie AWS Konfigurieren Sie den Service, um SNS-Benachrichtigungen (Simple Notification Service) an den zu senden ServiceNow Instanz. Weitere Informationen finden Sie unter Konfigurieren Sie AWS Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz. Nachdem Sie den Service konfiguriert haben, beginnt er mit dem Senden von Ereignisbenachrichtigungen an die ServiceNow REST API für Cloud-Ereignisse. Wenn ein Ereignis eines der folgenden Kriterien erfüllt, schreibt die API es in die Tabelle „Cloud-Ereignisse“ [sn_CMP_Cloud_event]:

- Die *Type*Des Ereignisses ist *`SubscriptionConfirmation`*.
- Die *Type*Des Ereignisses ist *`Notification`*Und *`messageType`*lst *`ConfigurationItemChangeNotification`*.
- Amazon CloudWatch Hat das Ereignis für eine Änderung am Tag ausgelöst, das dem Konfigurationselement (CI) zugeordnet ist.

Der Cloud-Ereignisplaner wählt dann die Ereignisse im Status „bereit“ für die Batch-Verarbeitung aus. Während der Ereignisverarbeitung verwendet die ereignisgesteuerte Discovery Antwortzuordnungen oder -Muster, um die Details der betroffenen Ressource in zu aktualisieren CMDB. Die *`sn_cmp.cloud_event.use_response_mapping_aws`*Die Eigenschaft bestimmt CMDB Methode aktualisieren. Um den Status eines Ereignisses zu verstehen, überprüfen Sie dessen Status in der Tabelle „Cloud-Ereignisse“ [sn_CMP_Cloud_event].

Beginnend mit Zurich Release, die *`sn_cmp.cloud_event.use_response_mapping_aws`*Eigenschaft ist standardmäßig auf „wahr“ festgelegt. Wenn diese Eigenschaft auf „wahr“ festgelegt ist und geeignete Antwortzuordnungen verfügbar sind, verwendet die ereignisgesteuerte Discovery die Antwortzuordnungen, um das CI in zu erstellen oder zu aktualisieren CMDB. Andernfalls löst die ereignisgesteuerte Discovery die entsprechenden Muster aus, um die betroffene Ressource zu erkennen und das CI in zu erstellen oder zu aktualisieren CMDB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beginnend mit Zurich Release, verwenden Sie *sn_cmp.cloud_event.parallel_scheduler_count*Eigenschaft zum Skalieren des Cloud-Ereignisplaners anhand der Ereigniszugangsrate. Die parallele Ausführung mehrerer Cloud-Ereignisplaner trägt dazu bei, die Ereignisverarbeitungsrate der Instanz zu verbessern. Weitere Informationen zur Skalierung der Cloud-Ereignisplaner finden Sie unter Skalieren Sie AWS Cloud-Ereignisplaner.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Konfigurieren Sie AWS Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz

Konfigurieren Sie Amazon Web Services(AWS) Konfigurieren Sie den Service, um Ereignisbenachrichtigungen an zu senden ServiceNow Instanz für alle Änderungen im Lebenszyklusstatus einer Ressource.

Vorbereitungen

- Stellen Sie sicher, dass Discovery Das Plugin „“ (com.snc.Discovery) wird in der Instanz installiert und aktiviert.
- Stellen Sie sicher, dass Sie gültig sind AWS Abonnements (Service-Accounts) und die zugehörigen logischen Rechenzentren werden erkannt.
- Stellen Sie sicher, dass das Passwort des Anwenderaccounts, das zum Abonnieren der Instanz für den Simple Notification Service (SNS) verwendet wird, die Zeichen @ oder # nicht enthält.

Erforderliche Rollen:

- Stellen Sie sicher, dass ein AWS Die Rolle ist verfügbar, die auf die folgenden Services und Ressourcen zugreifen kann:
  - SNS
  - AWS-Konfigurationsservice
  - Ressourcentypen, für die Sie die Konfigurationsänderung nachverfolgen möchten
- ServiceNow-Rollen:
  - discovery_admin
  - sn_CMP.Cloud_event_Integration: Die Zugriffsanmeldeinformationen von ServiceNow Ein Anwender mit der Rolle „sn_CMP.Cloud_event_Integration“ muss die Instanz SNS-Benachrichtigungen abonnieren. Weitere Informationen finden Sie unter Erstellen Sie einen Anwender Und Weisen Sie einem Anwender eine Rolle zu .

Warum und wann dieser Vorgang ausgeführt wird

Die ServiceNow® Die ereignisgesteuerte Discovery verwendet die Ereignisse, um die neuesten Ressourceninformationen in der Configuration Management Database (CMDB) zu aktualisieren. Weitere Informationen finden Sie unter AWS Ereignisgesteuerte Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Viele der Schritte im Thema werden im AWS-Portal ausgeführt. Weitere Informationen finden Sie in der folgenden AWS-Dokumenten.

- Einrichten von Amazon SNS-Benachrichtigungen
- Das AWS Config-Dashboard anzeigen

Hinweis:

Wenn Sie Domänentrennung für Cloud-Discovery verwenden, sind auch die Ereignisse nach Domänen getrennt. Daher können Sie die Details eines verarbeiteten Events nur anzeigen, wenn es zu Ihrer Domäne gehört. Wenn ein Ereignis keinem Service-Account zugeordnet ist, wird es der globalen Domäne zugeordnet.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Prozedur

1. Melden Sie sich bei an AWS Account.
2. Navigieren Sie auf der Seite Services zu **AWS-Services** > **Services Suchen** > **Einfacher Benachrichtigungsservice**an.
3. Erstellen Sie einen Amazon SNS-Thema.
   Die AWS Der Konfigurationsservice verwendet das SNS-Thema, um die Ereignisbenachrichtigungen zu veröffentlichen.
   a. Navigieren Sie im SNS-Dashboard zu **Themen** > **Thema erstellen**an.
   b. Füllen Sie im Formular die Felder aus.

Formular „Thema erstellen“

Feld	Beschreibung
Typ	Benachrichtigungsthema-Typ. Wählen Sie aus **Standard** Thementyp.
Name	Name des SNS-Themas.
Anzeigename: Optional	Anzeigename des SNS-Themas.

   c. Wählen Sie Aus **Thema erstellen** .
4. Abonnieren Sie die Instanz für das SNS-Thema.
   Nachdem Sie das SNS-Thema abonniert haben, kann die Instanz die Ereignisbenachrichtigungen von erhalten AWS Cloud.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie auf der Seite „Themendetails“ die Option aus **Abonnement erstellen** .

b. Füllen Sie im Formular die Felder aus.

Formular „Abonnements erstellen“

Feld	Beschreibung
Protokoll	Zu verwendende Kommunikationsprotokolle. Für das Abonnement, das automatisch aktualisiert CMDB, Wählen Sie HTTPS aus. **Hinweis:** Nach dem Erstellen des HTTPS-Abonnements können Sie ein separates Abonnement erstellen, das E-Mails an eine angegebene Person sendet.
Endpunkt	URL von ServiceNow REST API für Cloud-Ereignisse. Stellen Sie sicher, dass die URL der folgenden Syntax entspricht: `https://<username>:<user_password>@<instance_URL>/api/now/cloud_event`

c. Wählen Sie Aus **Abonnement erstellen** .

5. Aktivieren **AWS** Ereignisaufzeichnung.

a. Navigieren zu **Konfiguration** > **Einstellungen**an.

b. Wählen Sie auf der Seite „Einstellungen“ die Option aus **Bearbeiten** .

c. Wählen Sie aus **Aktivieren Sie** Kontrollkästchen.

d. Wählen Sie im Dialogfeld Aufzeichnung starten die Option aus **Bestätigen** .

e. Füllen Sie die Werte im Formular „Einstellungen bearbeiten“ aus.

Eine Beschreibung der Formularfelder finden Sie unter Formularreferenz für Einstellungen bearbeiten.

f. Wählen Sie **Speichern**.

Nächste Maßnahme

Nachdem einige Events generiert wurden, navigieren Sie zum Cloud-Benutzerportal, um sich die Events anzusehen.

Skalieren Sie AWS Cloud-Ereignisplaner

Skalieren Sie die Cloud-Ereignisplaner, um zu verbessern Amazon Web Services(AWS) Ereignisverarbeitungsrate des ServiceNow Instanz.

Vorbereitungen

Erforderliche Rolle: cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Instanz eine große Anzahl von Ereignissen empfängt und sie nicht innerhalb einer angemessenen Zeit verarbeitet, erstellen Sie zusätzliche Cloud-Ereignisplaner. Die parallele Ausführung mehrerer Cloud-Ereignisplaner trägt dazu bei, die Ereignisverarbeitungsrate der Instanz zu verbessern. Wenn die Ereigniszugangsrate reduziert wird, können Sie einige der Cloud-Ereignisplaner deaktivieren. Weitere Informationen finden Sie unter AWS Ereignisgesteuerte Discovery.

Prozedur

1. Konfigurieren Sie die Anzahl der Cloud-Ereignisplaner, die Sie verwenden möchten.
   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
   b. Suchen Sie in der Spalte Name nach *sn_cmp.cloud_event.parallel_scheduler_count*.
   c. Auf der *sn_cmp.cloud_event.parallel_scheduler_count*Eigenschaftsformular, legen Sie fest **Wert** Feld auf einen entsprechenden Wert.

      Wichtig:
      - Stellen Sie sicher, dass der Wert von *sn_cmp.cloud_event.parallel_scheduler_count*Eigenschaft überschreitet die Anzahl der verfügbaren Worker-Knoten nicht.
      - Wenn Sie mehrere Domänen haben, in denen Cloud-Ereignisse konfiguriert sind, verwenden Sie die *sn_cmp.cloud_event.parallel_scheduler_count*Eigenschaft mit Vorsicht, da jeder Cloud-Ereignisplaner mehrere Iterationen für jede Domäne hat, in der Cloud-Ereignisse aktiv sind.

   d. Wählen Sie **Aktualisieren**.
2. Führen Sie die geplante Aufgabe „Cloud-Ereignisplaner-Zählungsüberwachung“ aus. Die geplante Aufgabe „Cloud-Ereignisplaner-Zählungsüberwachung“ verwaltet die Anzahl der Cloud-Ereignisplaner gemäß dem in angegebenen Wert *sn_cmp.cloud_event.parallel_scheduler_count*Eigenschaft.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
   b. Öffnen Sie die geplante Aufgabe Cloud-Ereignisplaner-Zählungsüberwachung.
   c. Wählen Sie **Jetzt ausführen**.

Erstellen Sie einen Datenbankindex für die Tabelle „Cloud-Ereignisse“

Erstellen Sie einen Datenbankindex aus den angegebenen Spalten der Tabelle „Cloud-Ereignisse“ [sn_CMP_Cloud_event], um die zu verbessern AWS Cloud-Ereignisverarbeitungsleistung.

Vorbereitungen

Stellen Sie sicher, dass der Bereich auf festgelegt ist Cloud Provisioning and Governance.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie nach dem Upgrade von Cloud Provisioning and Governance auf Release Utah einen Datenbankindex aus den angegebenen Spalten der Tabelle „Cloud-Events“ [sn_cmp_cloud_event]. Der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenbankindex hilft, die Leistung der Verarbeitung von AWS-Events (Amazon Web Services) durch die Instanz zu verbessern. Wenn Sie Cloud Provisioning and Governance mit Release Utah verwenden, wird der Datenbankindex bei der Installation der Anwendung automatisch erstellt.

Anstatt den Datenbankindex manuell zu erstellen, können Sie ihn mit einer geplanten Aufgabe erstellen. Weitere Informationen finden Sie unter ServiceNow® Ereignisgesteuerte Discovery: Erstellen Sie einen Datenbankindex für die Tabelle „Cloud-Ereignisse“ (KB1207069).

Sie können auch die Cloud-Ereignisplaner skalieren, um zu verbessern Amazon Web Services(AWS) Ereignisverarbeitungsrate des ServiceNow Instanz. Weitere Informationen finden Sie unter Skalieren Sie AWS Cloud-Ereignisplaner.

Prozedur

1. Navigieren Sie zu https://<instance name>.service-now.com/sn_cmp_cloud_event_list.do
2. Auswahlvorgang **Spaltenoptionen** > **Konfigurieren** > **Tabelle**an.
3. Wählen Sie aus **Datenbankverzeichnisse** Zugehörige Liste.
4. Wählen Sie **Neu**.
5. Wählen Sie in der Liste Verfügbare Spalten die folgenden Spalten in der angegebenen Reihenfolge aus.
   a. **Status**
   b. **Prozess-ID**
   c. **Ressourcen-ID**
6. Wählen Sie Aus **Index Erstellen** .
7. **Wahlweise:** Wählen Sie eine Option aus, um anzugeben, ob Sie eine Benachrichtigung zur Indexerstellung erhalten möchten.
8. Wählen Sie **OK**.
9. Benennen Sie den neuen Index um, um die Identifizierung zu erleichtern.

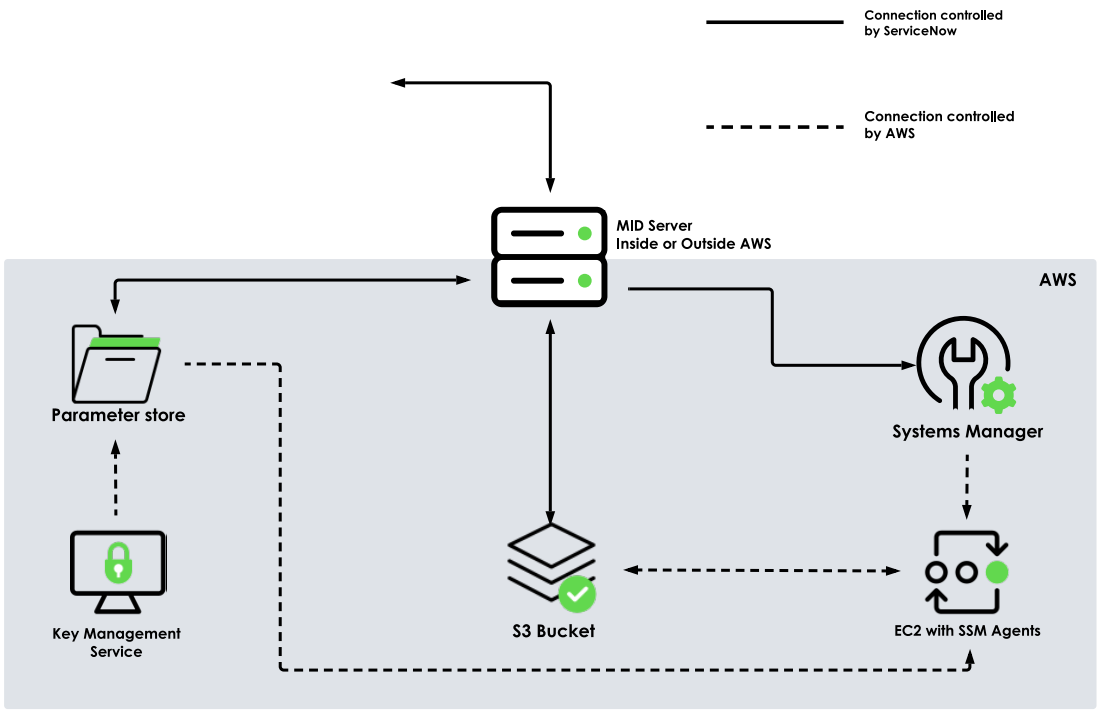
AWS SSM-Discovery

AWS Die Agent-Discovery von Systems Manager (SSM) führt einen optimierten, Agent-basierten Ansatz für die Erkennung ein Amazon Elastic Compute Cloud (EC2) mit AWS SSM. Diese Integration verbessert sich Discovery Durch Nutzung von SSM-Service Desk-Mitarbeitern, um die Abhängigkeit von herkömmlichen Produkten zu reduzieren MID-Server Konfigurationen, vereinfachen die Anmeldeinformationsverwaltung und verbessern die Skalierbarkeit in Umgebungen mit mehreren Regionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow

AWS SSM-Discovery-Workflow



Der Gesamtprozess auf allgemeiner Ebene lautet wie folgt:

1. Die ServiceNow AI Platform® Sendet Discovery-Befehle an MID-Server.
2. Der MID interagiert mit AWS Services (SSM, Simple Storage Service (S3), Parameterspeicher) zum Ausführen von Befehlen auf Zielgeräten.
3. Die SSM-Agents führen die Befehle aus und geben Ergebnisse an S3 zurück.
4. Der MID ruft Ergebnisse ab und verarbeitet sie.
5. Der MID sendet die Ergebnisse zurück an ServiceNow AI Platform®Über die ecc_Queue, die die CMDB aktualisiert.

Vorteile und Nutzung

Die folgenden Beispiele heben die primären Vorteile und praktischen Verwendungen von hervor AWS SSM-Agent-Discovery:

- Führen Sie die Discovery aus, ohne dass zusätzliche Anmeldeinformationen lokal für das Betriebssystem erforderlich sind.
- Vereinfachen Sie die Bereitstellung, ohne dass erforderlich ist Agent Client Collector(ACC) oder Virtual Private Cloud (VPC)-Zugriff.
- Minimieren Sie den Bedarf an mehreren MID ServersUnd direkten Netzwerkzugriff auf Zielgeräte.
- Verwalten Sie Anmeldeinformationen und Befehlsausführung mit sicher AWS Services.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen

Bestätigen Sie, dass Sie über die erforderlichen Versionen der folgenden Anwendungen und Plugins verfügen:

- Discovery
- Cloud Operations Workspace Version 1.7.1 oder höher.
- CMDB CI-Klassenmodelle Version 1.74.0 oder höher.
- Muster für Discovery und Service-Mapping Version 1.27.0 oder höher.

Installieren Sie MID-Server. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die MID-Server .

Überprüfen Sie, ob Sie über einen verfügen AWS Anwenderaccount mit Administratorzugriff.

Überprüfen Sie, ob Sie über einen verfügen ServiceNow AI Platform® Anwenderaccount mit der Rolle „Discovery_admin“.

Nicht unterstützte Funktionen

Derzeit werden die folgenden Funktionen nicht unterstützt AWS SSM-Discovery:

- Dateibasierte Discovery
- Zertifikatbasierte Discovery
- Erkennung von oben nach unten
- Erweitertes ADM
- Anwenderschritt in Mustern ändern/ändern rückgängig machen

Hinweis: SSM unterstützt nur sudo für die Ausführung privilegierter Befehle und standardmäßig die sh-Shell, ohne Unterstützung für alternative Befehl- oder Shell-Typen.

AWS Umgebungskonfiguration

Erstellen Sie IAM-Rollen und -Berechtigungen

Definieren Sie die zu unterstützenden Rollen für Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) AWS SSM-Vorgänge, die die erforderlichen Berechtigungen für die Ausführung von Lese-, Schreib- und Listenbefehlen angeben. Weitere Informationen finden Sie unter IAM-Richtlinien

Konfigurieren Sie EC2-Rollen und -Instanzen

Erstellen Sie EC2-Rollen, und weisen Sie diesen Rollen die erforderlichen Berechtigungen zu, um mit SSM zu interagieren. Weitere Informationen zum Einrichten einer EC2-Instanz finden Sie unter EC2-Instanzen .

Erstellen Sie S3-Buckets

Erstellen Sie S3-Buckets, um große Datenübertragungen zu unterstützen, und konfigurieren Sie entsprechende Bucket-Richtlinien und Lebenszyklusregeln. Um das Ausgabelimit von SSM für 24.000-Zeichen zu überwinden, wird die Befehlsausgabe an S3 weitergeleitet, wodurch die vollständige Nutzlasterfassung aktiviert wird. Darüber hinaus erleichtert S3 Dateiübertragungen an EC2-Instanzen. Weitere Informationen zum Erstellen von S3-Buckets finden Sie unter S3-Bucket einrichten .

(Optional) Konfigurieren Sie KMS-Schlüssel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine anwenderdefinierte AWS Key Management Service (KMS)-Schlüssel zum Verschlüsseln vertraulicher Anmeldeinformationen, die als SecureString-Parameter in gespeichert sind AWS Systemmanager-Parameterspeicher. Die Verwendung eines dedizierten Schlüssels erhöht die Sicherheit, indem überprüft wird, ob Anmeldeinformationen zur Laufzeit verschlüsselt und sicher abgerufen werden, ohne sie in nur-Text darzustellen. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Erstellen Sie einen vom Kunden verwalteten AWS-KMS-Schlüssel .

Wichtig: Wenn Sie in anwendbare Anmeldeinformationen verwenden Discovery, Sie müssen einen anwenderdefinierten KMS-Schlüssel erstellen.

Importieren Sie anwenderdefinierte SSM-Dokumente

Die Ausführung des SSM-Befehls hängt von der Verfügbarkeit der erforderlichen Dokumente ab. Stellen Sie vor dem Initiieren der SSM-basierten Discovery sicher, dass alle YAML-Dateien von bereitgestellt wurden ServiceNowWurden erfolgreich für jeden bereitgestellt AWS Region, in der der Discovery-Prozess ausgeführt wird. Weitere Informationen zu diesem Prozess finden Sie unter Importieren Sie anwenderdefinierte AWS-Dokumente . Sie können die YAML-Dateien direkt aus diesem artikel herunterladen.

Weitere Informationen zu finden AWS Konfiguration der Verwaltungskonsole, siehe Amazon SSM Discovery: Setup-Anweisungen für die AWS-Umgebung artikel in Now Support Knowledge Base.

ServiceNow AI Platform® Instanzkonfiguration

Systemeigenschaften konfigurieren

Aktivieren Sie Folgendes Discovery Systemeigenschaften:

- `glide.discovery.enable_ssm`
- `glide.discovery.ssm.enable_windows`

Die AWS SSM-Agent wird mit Stamm ausgeführt (Linux) Oder SYSTEM (Windows) Berechtigungen, d. h. jeder über ihn gesendete Befehl kann mit vollständigem Systemzugriff ausgeführt werden. Aufgrund dieser hohen Zugriffsstufe ist SSM aus Sicherheitsgründen standardmäßig deaktiviert. Weitere Informationen finden Sie unter Aktivieren Sie die AWS SSM-basierte Discovery.

Definieren Sie Stamm- und nicht-Stamm-Anmeldeinformationen

Die `mid.discovery.aws_ssm.linux.fallback_root`Mit der Eigenschaft können EC2-Instanzen standardmäßig der Stammanwender verwendet werden. Standardmäßig ist diese Einstellung **Falsch** , Wenn Sie jedoch keine alternativen Anwenderanmeldeinformationen einrichten möchten, können Sie es aktivieren, dass Befehle als Stamm ausgeführt werden. Wenn Sie diese Einstellung deaktiviert lassen, müssen Sie einen Anmeldeinformationsdatensatz in erstellen AWS Tabelle „SSM-Instanzanwender“ [aws_ssm_instance_user_credentials], in der Sie einfach den Anwendernamen angeben, der zum Ausführen von Befehlen auf der Instanz verwendet werden soll. Weitere Informationen finden Sie unter . Aktivieren Sie den Stamm-Fallback Und Konfigurieren Sie anwenderdefinierte Anwenderanmeldeinformationen.

MID-Server-Eigenschaften konfigurieren

Nachdem Sie KMS-Schlüssel oder S3-Buckets in eingerichtet haben AWS Verwaltungskonsole konfigurieren Sie Folgendes MID-Server Systemeigenschaften auf der ServiceNow AI Platform®:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *mid.discovery.aws_ssm.kms_key_name*
- *mid.discovery.aws_ssm.kms_key_region*
- *mid.discovery.aws_ssm.s3_bucket_name*
- *mid.discovery.aws_ssm.s3_bucket_region*

Weitere Informationen finden Sie unter MID-Server für konfigurieren AWS S3-Zugriff und Konfigurieren MID-Server Für AWS KMS-Zugriff.

Aktivieren Sie die MID-Server-Fähigkeit

Sie müssen die neue aktivieren MID-Server Fähigkeit für AWS SSM so die MID-Server Kann die Ausführung der SSM-Discovery unterstützen. Standardmäßig ist diese Fähigkeit enthalten, wenn Sie verwenden **ALLE** Fähigkeit. Wenn Sie jedoch einzelne Fähigkeiten verwenden, müssen Sie die neue manuell hinzufügen **AWS SSM** Fähigkeit zu Ihrem MID Servers. Informationen zum Hinzufügen einer Fähigkeit finden Sie unter https://docs.servicenow.com/csh?topicname=t_ConfigureCapabilities&version=zurich&pubname=zurich-integrate-applications .

Cloud-Discovery Zeitplankonfiguration

Erstellen Sie einen Cloud-Discovery Zeitplan

Beim Einrichten eines Discovery-Zeitplans in Cloud Operations Workspace, Sie können SSM-Discovery bereitstellen, indem Sie auswählen **Erkennen Sie virtuelle Computer** Und **Verwenden Sie AWS SSM** Schaltet um. Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Aktivieren Sie die AWS SSM-basierte Discovery

Konfigurieren Discovery Zu verwenden AWS Systemmanager (SSM)-Agent.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die AWS SSM-Agent wird mit Stamm ausgeführt (Linux) Oder SYSTEM (Windows) Berechtigungen, d. h. jeder über ihn gesendete Befehl kann mit vollständigem Systemzugriff ausgeführt werden. Aufgrund dieser hohen Zugriffsstufe ist SSM aus Sicherheitsgründen standardmäßig deaktiviert. Ein Linux, Sie können nicht-Stamm-Anmeldeinformationen für die Ausführung konfigurieren Discovery Befehle sicherer. Ein Windows, Discovery Befehle erfordern Zugriff auf SYSTEMEBENE. Daher müssen Sie entscheiden, ob Sie diese Fähigkeit basierend auf Ihren Sicherheitsanforderungen aktivieren möchten. Wird Aktiviert *glide.discovery.enable_ssm*Aktiviert SSM-Discovery nicht automatisch für Windows. Anders Als Linux, Windows Es fehlt Unterstützung für die Verwendung eines nicht-SYSTEMANWENDERS, daher müssen Sie aus Sicherheitsgründen explizit aktivieren *glide.discovery.ssm.enable_windows*Zu verwendende Eigenschaft AWS SSM-Discovery auf Windows Geräte.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. In **Name** Feld eingeben Glide.Discovery.enable_ssm .
3. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
4. Geben Sie Ein Wahr .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Aktivieren Sie das Häkchen (✓)-Symbol.
6. **Wahlweise:** Zum Aktivieren AWS SSM-basierte Discovery auf Windows Computer, wiederholen Sie die Schritte 2-5 für den *glide.discovery.ssm.enable_windows*Eigenschaft.

Nächste Maßnahme

Definieren Sie das Fallback-Stammverhalten mit *mid.discovery.aws_ssm.linux.fallback_root_user*Eigenschaft oder Erstellung von nicht-Stamm-Anmeldeinformationen zur Ausführung Discovery Befehle mit AWS Tabelle „SSM-Instanzanwender“ [aws_ssm_instance_user_credentials]. Weitere Informationen finden Sie unter Aktivieren Sie den Stamm-Fallback und Konfigurieren Sie anwenderdefinierte Anwenderanmeldeinformationen.

MID-Server für konfigurieren AWS S3-Zugriff

Konfigurieren MID-Server Eigenschaften zum Aktivieren des Zugriffs auf S3 (Simple Storage Service) über den ServiceNow AI Platform® Beim Ausführen der Systems Manager (SSM)-Agent-Discovery.

Vorbereitungen

Bestätigen Sie Folgendes:

- Sie haben mindestens einen MID-Server Und in installiert **Aktiv** status. Weitere Informationen finden Sie unter Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.
- Sie haben einen AWS Anmeldeinformationen, die zulassen MID-Server Um auf zuzugreifen und API-Aufrufe in durchzuführen AWS Umgebung. Weitere Informationen finden Sie unter AWS-Zugriff für MID-Server .
- Sie haben einen anwenderdefinierten S3-Bucket mit aktiviertem erforderlichen Zugriff für die IAM-Rollen erstellt. Weitere Informationen finden Sie unter S3-Bucket einrichten Und Richten Sie eine Richtlinie für den Zugriff auf den S3-Bucket ein .

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Da die SSM-Befehlskonsole ein Limit von 000 Zeichen aufweist, müssen Ergebnisse, die diesen Grenzwert überschreiten, in einem S3-Bucket gespeichert und aus diesem abgerufen werden. Für Put-Dateibefehle dient der S3-Bucket auch als Übertragungspunkt zwischen MID-Server Und AWS Umgebung, die die Dateibereitstellung an Zielgeräte über SSM aktiviert. Zum Konfigurieren von MID-Server Um diese S3-basierten Vorgänge zu unterstützen, legen Sie fest *mid.discovery.aws_ssm.s3_bucket_name*Eigenschaft für den Namen des S3-Buckets, der für die SSM-Agent-Discovery verwendet wird. Geben Sie dann die Region des Buckets in an *mid.discovery.aws_ssm.s3_bucket_region*Eigenschaft.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften**an.
2. In **Name** Feld eingeben `Mid.Discovery.aws_ssm.s3_Bucket_Name` .
3. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
4. Geben Sie den Namen des S3-Buckets ein.
5. Aktivieren Sie das Häkchen (✓)-Symbol.
6. In **Name** Feld eingeben `Mid.Discovery.aws_ssm.s3_Bucket_Region` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
8. Geben Sie den Namen der Region ein, in der sich der S3-Bucket befindet.
9. Aktivieren Sie das Häkchen ( ) -Symbol.

Konfigurieren MID-Server Für AWS KMS-Zugriff

Konfigurieren MID-Server Eigenschaften zum Aktivieren des Schlüsselzugriffs des Schlüsselverwaltungsservice (Key Management Service, KMS) über die ServiceNow AI Platform® Beim Ausführen der Systems Manager (SSM)-Agent-Discovery.

Vorbereitungen

Bestätigen Sie Folgendes:

- Sie haben mindestens einen MID-Server Und in installiert **Aktiv** status. Weitere Informationen finden Sie unter Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.
- Sie haben einen AWS Anmeldeinformationen, die zulassen MID-Server Um auf zuzugreifen und API-Aufrufe in durchzuführen AWS Umgebung. Weitere Informationen finden Sie unter AWS-Zugriff für MID-Server .
- Sie haben eine anwenderdefinierte erstellt AWS KMS-Schlüssel zum Verschlüsseln vertraulicher Anmeldeinformationen. Weitere Informationen finden Sie unter Erstellen Sie einen vom Kunden verwalteten AWS-KMS-Schlüssel .

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Verwendung eines dedizierten Schlüssels erhöht die Sicherheit, indem überprüft wird, ob anwendbare Anmeldeinformationen zur Laufzeit verschlüsselt und sicher abgerufen werden, ohne dass sie im nur-Text verfügbar gemacht werden. Dieser Schritt ist optional und nur erforderlich, wenn Sie während der Discovery anwendbare Anmeldeinformationen verwenden möchten. Zum Konfigurieren von MID-Server Um die sichere Verarbeitung von Anmeldeinformationen während der SSM-Agent-Discovery zu unterstützen, legen Sie fest *`mid.discovery.aws_ssm.kms_key_name`*Eigenschaft für den Namen von AWS KMS-Schlüssel. Legen Sie dann fest *`mid.discovery.aws_ssm.kms_key_region`*Eigenschaft für die Region, in der sich der Schlüssel befindet.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften**an.
2. In **Name** Feld eingeben `Mid.Discovery.aws_ssm.KMS_key_Name` .
3. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
4. Geben Sie den Namen des KMS-Schlüssels ein.
5. Aktivieren Sie das Häkchen ( ) -Symbol.
6. In **Name** Feld eingeben `Mid.Discovery.aws_ssm.KMS_key_Region` .
7. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
8. Geben Sie den Namen der Region ein, in der sich der KMS-Schlüssel befindet.
9. Aktivieren Sie das Häkchen ( ) -Symbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie den Stamm-Fallback

Aktivieren Sie die Fallback-Stammanwendereigenschaft, um zuzulassen AWS SSM-Discovery, auf der Befehle als Stamm ausgeführt werden sollen Linux Systeme, wenn keine alternativen Anwenderanmeldeinformationen konfiguriert sind.

Vorbereitungen
Bestätigen Sie das AWS SSM-Agent-Discovery ist aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie die AWS SSM-basierte Discovery.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn *glide.discovery.enable_ssm*Eigenschaft ist aktiviert, AWS SSM Discovery Ein Linux Standardmäßig wird der Stammanwender für die Befehlsausführung verwendet. Wenn Sie keine alternativen Anwenderanmeldeinformationen für Ihre EC2-Instanzen konfigurieren möchten, müssen Sie aktivieren *mid.discovery.aws_ssm.linux.fallback_root_user*Eigenschaft, um Fallback zur Stammausführung zuzulassen. Wenn diese Option aktiviert ist, wird automatisch ein Datensatz in der Tabelle „AWS SSM-Instanzanwender“ [aws_ssm_instance_user_credentials] mit dem Anwendernamen „Stamm“ erstellt. Wenn Sie diese Eigenschaft jedoch auf festgelegt lassen **Falsch** , Sie müssen nicht-Stamm-Anmeldeinformationen für die Ausführung konfigurieren Discovery Befehle. Weitere Informationen finden Sie unter Konfigurieren Sie anwenderdefinierte Anwenderanmeldeinformationen.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. In **Name** Feld eingeben `Mid.Discovery.aws_ssm.linux.Fallback_root_user` .
3. Doppelklicken Sie auf **Wert** Feld für die Inline-Bearbeitung.
4. Geben Sie Ein `Wahr` .
5. Aktivieren Sie das Häkchen ( ) -Symbol.

Ergebnis
Ein neuer Datensatz wird zu hinzugefügt AWS Tabelle „SSM-Instanzanwender“ [aws_ssm_instance_user_credentials] mit dem Anwendernamen „root“.

Konfigurieren Sie anwenderdefinierte Anwenderanmeldeinformationen

Definieren Sie einen nicht-Stammanwender für AWS SSM-Discovery durch Erstellen eines Anmeldeinformationsdatensatzes, der einen Anwendernamen mit ausreichenden Berechtigungen zum Ausführen von Discovery-Befehlen für angibt Linux Ziele.

Vorbereitungen
Bestätigen Sie Folgendes:

- Die Systemeigenschaft *glide.discovery.enable_ssm*lst aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie die AWS SSM-basierte Discovery.
- Der Anwender, den Sie als nicht-Stammanwender zuweisen, hat Zugriff zum Ausführen aller erforderlichen Befehle auf dem Zielserver. Dieser Anwender erfordert denselben Zugriff wie Anmeldeinformationen, die für reguläre Anwendungen verwendet werden Linux Discovery, einschließlich des erforderlichen Zugriffs auf Stammebene für privilegierte Befehle. Weitere Informationen finden Sie unter Für die Hosterkennung erforderliche Anmeldeinformationen Und SSH-Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Anstatt sich auf den Stamm zu verlassen, können Sie einen anwenderdefinierten Anwender mit ausreichenden Berechtigungen definieren, um die erforderliche auszuführen Discovery Befehle. Es wird nur ein Anwendername benötigt – kein Passwort oder Schlüssel – vorausgesetzt, der Anwender hat die gleiche Zugriffsebene wie herkömmliche Linux Discovery Anmeldeinformationen. Dieser Ansatz fördert eingeschränkten Zugriff und eine bessere Ausrichtung an Unternehmenssicherheitsrichtlinien.

Hinweis: Derzeit unterstützt SSM nur sudo für die Ausführung privilegierter Befehle und standardmäßig die sh-Shell, ohne Unterstützung für alternative Befehl- oder Shell-Typen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Aus **AWS SSM-Instanzanwender** .
4. Geben Sie einen eindeutigen Namen für den Anwender ein.
5. Geben Sie den Anwendernamen aus den alternativen Anwenderanmeldeinformationen ein, die Sie in Ihrer EC2-Instanz erstellt haben AWS Verwaltungskonsole.
   Weitere Informationen finden Sie unter Amazon SSM Discovery: Setup-Anweisungen für die AWS-Umgebung artikel in Now Support Knowledge Base.
6. Wählen Sie **Absenden**.

Ergebnis

Ein neuer Datensatz wird zu hinzugefügt AWS Tabelle „SSM-Instanzanwender“ [aws_ssm_instance_user_credentials].

Erkennung von Azure-Clouds

Wenn sich Ihre Cloud-Ressourcen in einer Azure-Cloud befinden, müssen Sie eine Anwenderidentität namens erstellen *Service-Prinzipal* Die Berechtigungen für erteilt MID-ServerUm auf ausgewählte Ressourcen zuzugreifen.

Azure-Verwaltungsgruppen und -Abonnements

Eine Azure-Verwaltungsgruppe enthält andere Verwaltungsgruppen und Abonnements. Die Verwaltungsgruppen in einer Azure Cloud-Umgebung bilden eine Hierarchie, aber Nicht Enthalten Volumes oder virtuelle Computer. Abonnements enthalten Cloud-Ressourcen, zum Beispiel virtuelle Computer. Die Abonnements, die zu Verwaltungsgruppen gehören, werden als Unterkonten bezeichnet.

Die Verwendung von Verwaltungsgruppen hat folgende Vorteile:

Einfaches Füllen von Unterkonten

Nachdem Sie die Verwaltungsgruppe konfiguriert und die erforderlichen Anmeldeinformationen angegeben haben, können Sie das Konto testen. Wenn der Test erfolgreich ist, gibt Discovery eine Liste von Abonnements in dieser Verwaltungsgruppe zurück. Aus dieser Liste können Sie mindestens ein Abonnement-Unterkonto auswählen, das mithilfe der Verwaltungsgruppe in den Erkennungszeitplan aufgenommen wird.Weitere Informationen zur Hierarchie von Verwaltungsgruppen und Abonnements finden Sie unter Organisieren Sie Ihre Ressourcen mit Azure-Verwaltungsgruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

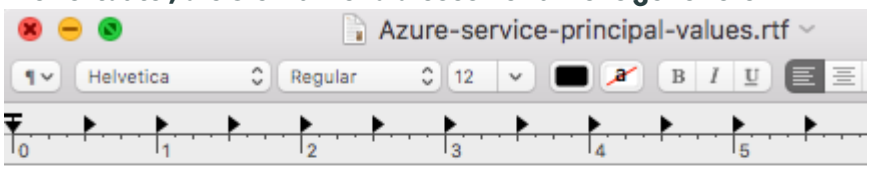
Erkennung von Unterkontoressourcen mithilfe dynamisch bezogener Anmeldeinformationen

Wenn Sie Discovery für Ihre Abonnements ausführen, benötigen Sie keine separaten Anmeldeinformationen für jedes Unterkonto. Discovery erkennt die Anmeldeinformationen für die Verwaltungsgruppe und ordnet sie allen Unterkontos des Abonnements zu. Der Cloud Discovery-Prozess verarbeitet Anmeldeinformationen automatisch, indem temporäre Anmeldeinformationen für jedes Unterkonto über eine Azure-API abgerufen werden. Sie können die Standardkonfiguration verwenden oder den MID Server anpassen, um andere Rollen für zusätzliche Steuerungen und Sicherheitseinstellungen zu übernehmen. Darüber hinaus kann Discovery die Liste der Unterkonten und Rechenzentren, die in einem Discovery-Zeitplan abgedeckt sind, automatisch aktualisieren. Weitere Informationen finden Sie im KB-artikel Rufen Sie neuere Accounts/Unterkonten automatisch über Cloud Discovery ab.

Ein Dienstprinzipal für Azure-Cloud-Services ähnelt einem Microsoft Windows-Servicekonto, über das Windows-Prozesse in einer Active Directory-Domäne miteinander kommunizieren können.

Kopieren Sie zum Erstellen des Azure-Dienstprinzipals in Ihrer ServiceNow-Instanz die Anmeldeinformationen des Dienstprinzipals aus dem Azure-Portal in einen Texteditor und übertragen Sie diese Werte dann in die Instanz.

Die Textdatei, die Sie während dieses Verfahrens generieren



Directory ID: 8bcdd120-9979-491e-8683-d9a4550bdd

Application ID: e6821ea9-e5c5-428a-b50c-7ea62993b2d

Application key: d348050-f893ccb7-hg84yg8-rg200hd

Subscription ID: 4803be48c3ee89-96d2-4fed-bedb-22e49013ee89

Diese Tabelle zeigt den Azure-Serviceprinzipalwert und den Standort in Azure, an dem Sie die Werte finden, die Sie für die Anmeldeinformationen benötigen.

Einstellung für Cloud Provisioning and Governance	**Wert „Azure-Dienstprinzipal“**	**Speicherort des Azure-Werts**
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei	**Azure Active Directory** > **Eigenschaften** > **Verzeichnis-ID**
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei	**Azure Active Directory** > **App-Registrierungen** > **Registrierte App.Anwendungs-ID**
Geheimer Schlüssel	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei	**Azure Active Directory** > **App-Registrierungen** > **Registrierte App** > **Einstellungen** > **Schlüssel (ausgeblendet)**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellung für Cloud Provisioning and Governance	Wert „Azure-Dienstprinzipal“	Speicherort des Azure-Werts
Account-ID	Azure **Abonnement-ID** Der Mandanten-ID zugeordnet.	**Azure Active Directory** > **Abonnements** > **Abonnement-ID**

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

API-Liste für Azure Cloud Discovery

Logisches Rechenzentrum (cmdb_ci_logical_datacenter)

CI-Attribute	Azure-Attribute
object_id	response.name
Name	response.name
region	response.displayName
Status	Installiert

Verfügbarkeitszone (cmdb_ci_av availability_zone)

CI-Attribute	Azure-Attribute
object_id	response.id

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbarkeitszone (cmdb_ci_av availability_zone) (Fortsetzung)

Name	response.name
Status	Installiert/Deaktiviert
Status	

Ressourcengruppe (cmdb_ci_resource_group)

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
Status	available
Status	Installiert/Deaktiviert

Netzwerk (cmdb_ci_network)

CI-Attribute	Azure-Attribute
object_id	id
Status	
Name	Name
cidr	properties.addressSpace.addressPrefixes

Subnetz (cmdb_ci_cloud_subnet)

CI-Attribute	Azure-Attribute
subnetName	response.name
subnetId	response.id
resourceGroup	response.properties.resourceGuid
networkId	response.id.split('/subnets/')
networkName	getNetwork(networkId)
cidrBlock	response.properties.addressSpace.addressPrefixes

Speichervolume (cmdb_ci_storage_volume)

CI-Attribute	Azure-Attribute
Status	properties.provisioningState
storage_type	properties.BlobType
volume_id	id
Name	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume (cmdb_ci_storage_volume) (Fortsetzung)

size_bytes	properties.diskSizeGB * 1024 * 1024 * 1024
object_id	id
size	response.properties.diskSizeGB
"volume_container"	containerName
Status	Installiert/Deaktiviert

Sicherheitsgruppen (cmdb_ci_compute_security_group)

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
Status	properties.provisioningState

Virtueller Server (cmdb_ci_vm_instance)

CI-Attribute	Azure-Attribute
memory	properties.hardwareProfile.vmSize
Status	Die Instanzstatus: • Erfolgreich: Am • Wird ausgeführt: Erfolgreich/wird gestoppt • Aufheben der Zuordnung: Wird gestoppt/gestoppt • Aufgehoben: Aus • Beendet: Fehler
object_id	id
CPUs	properties.hardwareProfile.vmSize
disks	properties.storageProfile.dataDisks
nics	properties.networkProfile.networkInterfaces[].size
vm_inst_id	properties.vmId
Name	Name
Status	Installiert/Deaktiviert

Hardwarevorlage (cmdb_ci_compute_template)

CI-Attribute	Azure-Attribute
Name	Name
object_id	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwarevorlage (cmdb_ci_compute_template) (Fortsetzung)

vcpus	numberOfCores
memory_mb	memoryInMB
local_storage_gb	resourceDiskSizeInMB
cores	numberOfCores

Öffentliche IP-Adresse der Cloud (cmdb_ci_cloud_public_ipaddress)

CI-Attribute	Azure-Attribute
object_id	response.id
Name	response.name
public_dns	properties.dnsSettings.fqdn
public_ip_address	properties.ipAddress

Cloud-LB IP-Adresse (cmdb_ci_Cloud_LB_ipaddress)

CI-Attribute	Azure-Attribute
object_id	"properties.frontendIPConfigurations.properties.privateIPAddress ODER properties.frontendIPConfigurations.properties.publicIPAddress, dann API für öffentliche IP-Adresse aufrufen"
Name	"properties.frontendIPConfigurations.properties.privateIPAddress ODER properties.frontendIPConfigurations.properties.publicIPAddress, dann API für öffentliche IP-Adresse aufrufen"
ipaddress_type	"properties.frontendIPConfigurations.properties.privateIPAddress ==> Private IP-Adresse ODER properties.frontendIPConfigurations.properties.publicIPAddress ==> Öffentliche IP-Adresse"
Status	Installiert

„Cloud-Netzwerkschnittstellen (cmdb_ci_nic)“

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
private_ip	properties.ipConfigurations
public_dns	API für öffentliche IP-Adresse aufrufen – properties.dnsSettings.fqdn
Status	properties.provisioningState
is_static	properties.ipConfigurations
mac_address	properties.macAddress
public_ip	API für öffentliche IP-Adresse aufrufen –

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image (cmdb_ci_os_template)

CI-Attribute	Azure-Attribute
Name	response.id
object_id	response.name
guest_os	properties.storageProfile.osDisk.osType
image_source	id
Status	Installiert/Deaktiviert

Cloud-Speicherkonto (cmdb_ci_cloud_storage_account)

CI-Attribute	Azure-Attribute
Name	Name
object_id	id
sku_name	sku.name
Status	properties.provisioningState

Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]

CI-Attribute	Azure-Attribute
object_id	response.id
Name	response.name
Status	
dns_name	.
fqdn	
canonical_hosted_zone_name	

Anmeldeinformationen für Azure-Cloud erstellen

Wenn sich Ihre Cloud-Ressourcen in einer Azure-Cloud befinden, erstellen Sie Anmeldeinformationen, die auf das Azure-Konto zugreifen können. Dieses Verfahren erfordert die Konfiguration Ihres Azure-Kontos.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Vorbereitungen
Erforderliche Rollen:

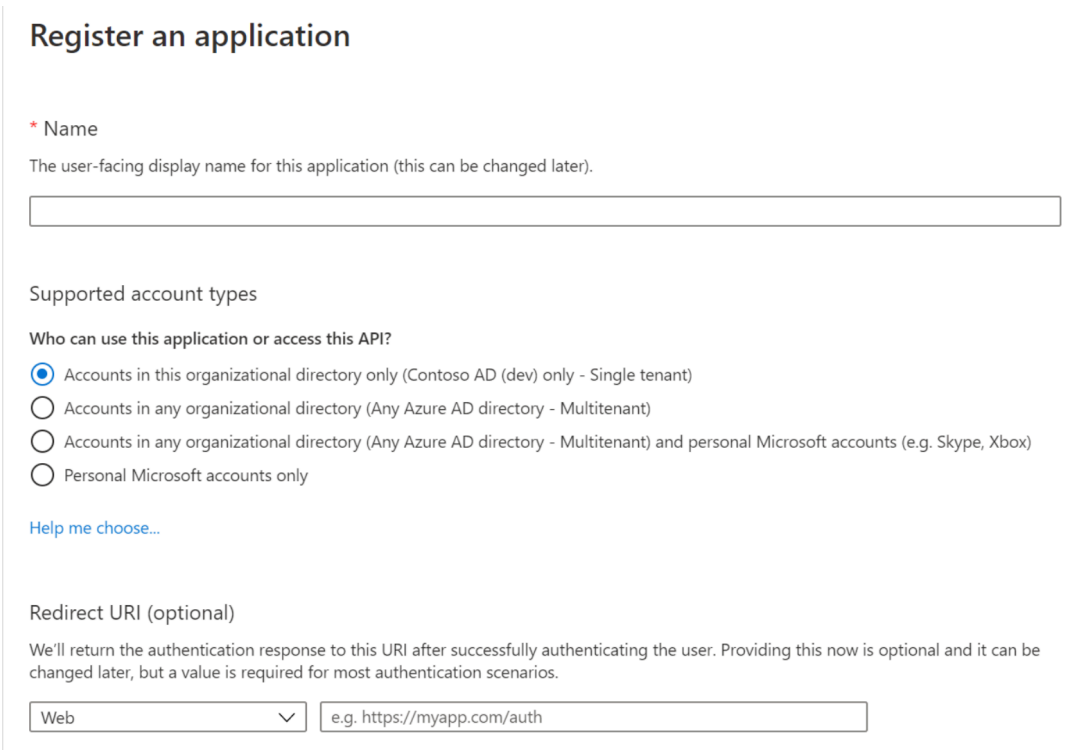
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rollen „Discovery_admin“, „Service_Mapping_admin“, „sn_CMP.Cloud_admin“ in Cloud Provisioning and Governance Oder Rolle sn_Cloud_OPS_WS.Cloud_OPS_admin in Cloud Operations Workspace.
- Vorgänge im Microsoft Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator

  und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Aktivieren Sie die interne Netzwerkverbindung zwischen den MID-Servern und den Azure Cloud API-Endpunkten: `management.azure.com`

Prozedur

1. Melden Sie sich beim Azure-Portal an, und navigieren Sie zu **Azure Active Directory**.
2. Navigieren Sie zu **App-Registrierungen** Abschnitt und wählen Sie aus **Neue Anwendungsregistrierung** .
   Geben Sie für Ihre Anwendung folgende Informationen ein:



Feld	Beschreibung
Name	Eindeutiger Name für die Anwendung und ihre Integrationsanmeldeinformationen. Beispiel: ServiceNow Integration.
Unterstützte Account-Typen	Geben Sie an, wer die Anwendung verwenden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

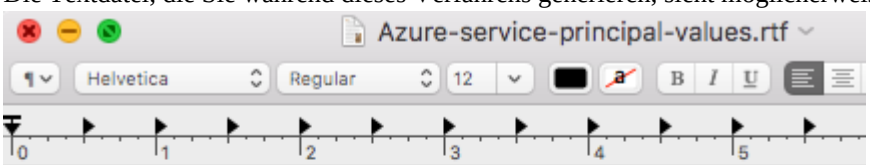
Feld	Beschreibung
Redirect URI (optional, Umleitungs-URI)	URL, die auf Azure zugreift. Normalerweise die URL der ServiceNow-Instanz

3. Wählen Sie **Register** aus, um die Registrierung der App abzuschließen.
4. Wenn die Registrierung abgeschlossen ist, kopieren Sie die Werte für die Anwendungs- (Client-) ID und Verzeichnis (Mandant) ID, und fügen Sie sie in den Texteditor ein.
5. Bezeichnen Sie die Werte **Anwendungs-ID** Und **Verzeichnis-ID** Entsprechend.
6. Navigieren Sie im Azure-Portal zum Abschnitt **Certificates & secrets** (Zertifikate und geheime Schlüssel), und geben Sie dann unter **New client secret** (Neuer Client-Geheimschlüssel) die folgenden Werte an:

Feld	Beschreibung
Schlüsselbeschreibung	Beschreibung für den Schlüssel
Dauer	Ablauf für den Schlüssel. **Hinweis:** Ihre Organisation kann Richtlinien anwenden, um die Gültigkeitsdauer des Schlüssels einzuschränken. Wählen Sie die entsprechende Dauer aus.

7. Wählen Sie **Hinzufügen**.
8. Kopieren Sie den Schlüsselwert, fügen Sie ihn in den Texteditor ein, und beschriften Sie den Wert als **Anwendungsschlüssel**.
9. Damit der Dienstprinzipal mit verschiedenen Azure-Abonnements arbeiten kann, navigieren Sie zu **Abonnements**.
   Zum Verwalten mehrerer Abonnements müssen Sie das folgende Verfahren für jedes Abonnement ausführen:

   a. Fügen Sie die Abonnements-ID in den Texteditor ein, und beschriften Sie sie als **Abonnements-ID**.
   Die Textdatei, die Sie während dieses Verfahrens generieren, sieht möglicherweise wie folgt aus:



Directory ID: 8bcdd120-9979-491e-8683-d9a4550bdd

Application ID: e6821ea9-e5c5-428a-b50c-7ea62993b2d

Application key: d348050-f893ccb7-hg84yg8-rg200hd

Subscription ID: 4803be48c3ee89-96d2-4fed-bedb-22e49013ee89

   b. Navigieren Sie zum Abonnement, und wählen Sie im Menü die Option **Zugriffssteuerung (IAM)** aus.

Automatische Übersetzung

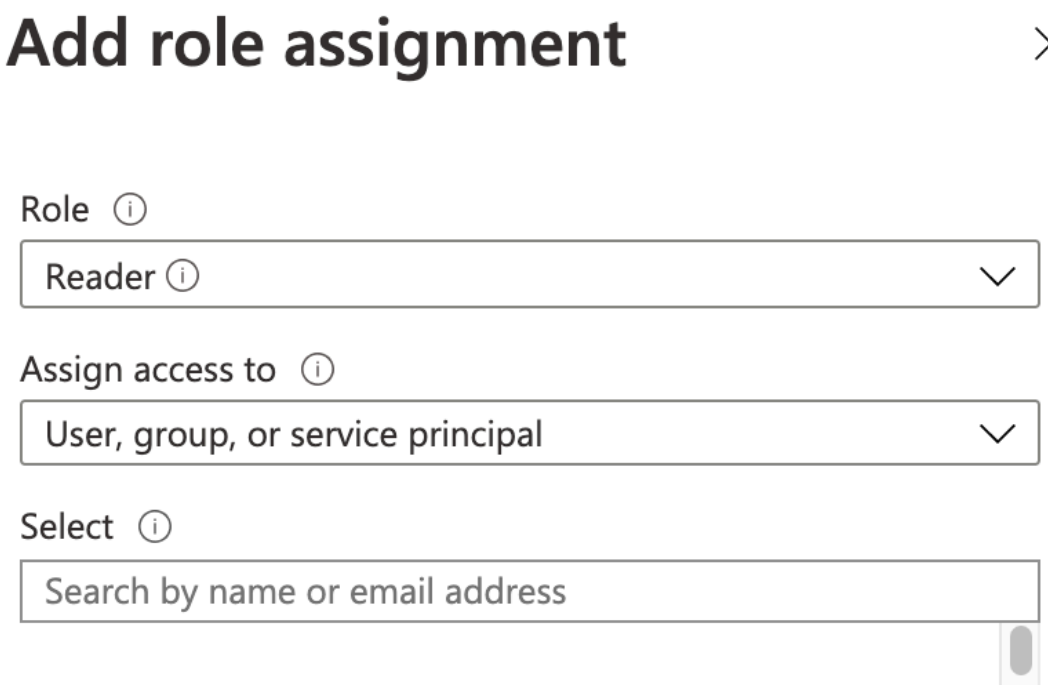
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie Aus **+ Hinzufügen** Oben im Bildschirm dann **Fügen Sie Rollenzuweisung hinzu** .

d. Wählen Sie im Feld **Rolle** den Wert **Leser** aus.
Lassen Sie den Standardwert für **User, group, or service principal** (Benutzer, Gruppe oder Service-Prinzipal) für das Feld **Assign Access to** (Zugriff zuweisen an) unverändert.

Hinweis: Die Rolle **Mitwirkender bei Ressourcenrichtlinien** ist nur für die Bereitstellung erforderlich.

e. Wählen Sie den Namen aus, den Sie in Schritt 2 im erstellt haben **Wählen Sie Aus** Feld und wählen Sie aus **Speichern** .



10. Wählen Sie aus **Azure-Service-Prinzipal** Geben Sie Anmeldeinformationen ein.

a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

b. Wählen Sie **Neu**.

c. Wählen Sie **Azure-Service-Prinzipal** aus.

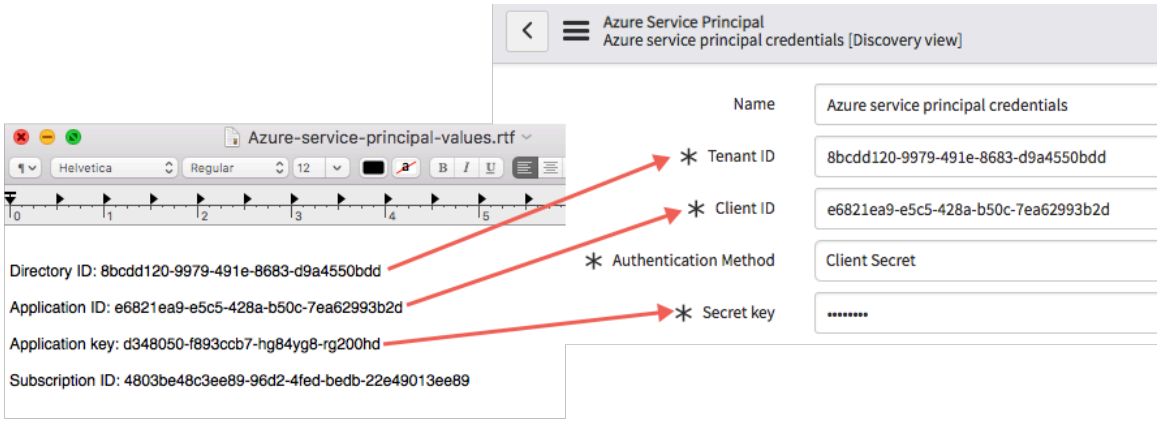
11. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: Azure service principal credentials.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Kopieren Sie die Werte aus der temporären Textdatei, und fügen Sie sie in die verbleibenden Felder ein.



Formularfeld „Anmeldeinformationen“	Wert „Azure-Dienstprinzipal“
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei
Geheimer Key	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei

13. Wählen Sie Aus **Speichern** Zum Erstellen des Azure-Service-Prinzips.

14. Wählen Sie aus **Abonnements Erkennen** Zugehöriger Link, um alle Abonnements für den Azure-Service-Prinzipal zu finden.
Die Instanz erstellt ein Servicekonto für jedes erkannte Abonnement. In der zugehörigen Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.

15. Wählen Sie ein Abonnement aus, um den für das Abonnement erstellten Service-Account anzuzeigen.

16. Wählen Sie ein aus Discovery Statuseintrag in **Discovery-Status Für Anmeldeinformationen** Liste zum Anzeigen von Discovery Protokoll.
Jedes Mal, wenn Sie auswählen **Abonnement Erkennen** , Die Instanz generiert einen neuen Discovery Status und zeigt ihn in an **Discovery-Status Für Anmeldeinformationen** Liste.

Führen Sie Azure Cloud Discovery mithilfe des Service Prinzipals mit SSH-Zertifikaten aus

Erkennen Sie virtuelle Linux-Computer auf Azure mithilfe von Service Principal (SP) mit kurzlebigen SSH-Zertifikaten. Durch die Verwendung dieser Zertifikate wird die Notwendigkeit von Passwörtern oder öffentlichen und privaten Schlüsselpaaren umgangen.

Vorbereitungen

Vor dem Erstellen von Cloud-Discovery-Anmeldeinformationen müssen Serviceprinzipien im Azure-Portal eingerichtet werden. Siehe Microsoft Azure Dokumentationswebsite für weitere Informationen. Überprüfen Sie nach dem Erstellen einer Linux-VM mit aktivierter Azure AD-Anmeldung die Anforderungen für die Anmeldung bei Azure AD mithilfe der OpenSSH-zertifikatbasierten Authentifizierung für Linux-VMs. Konfigurieren Sie geeignete Rollenzuweisungen für das Serviceprinzip und die Ressourcengruppe.

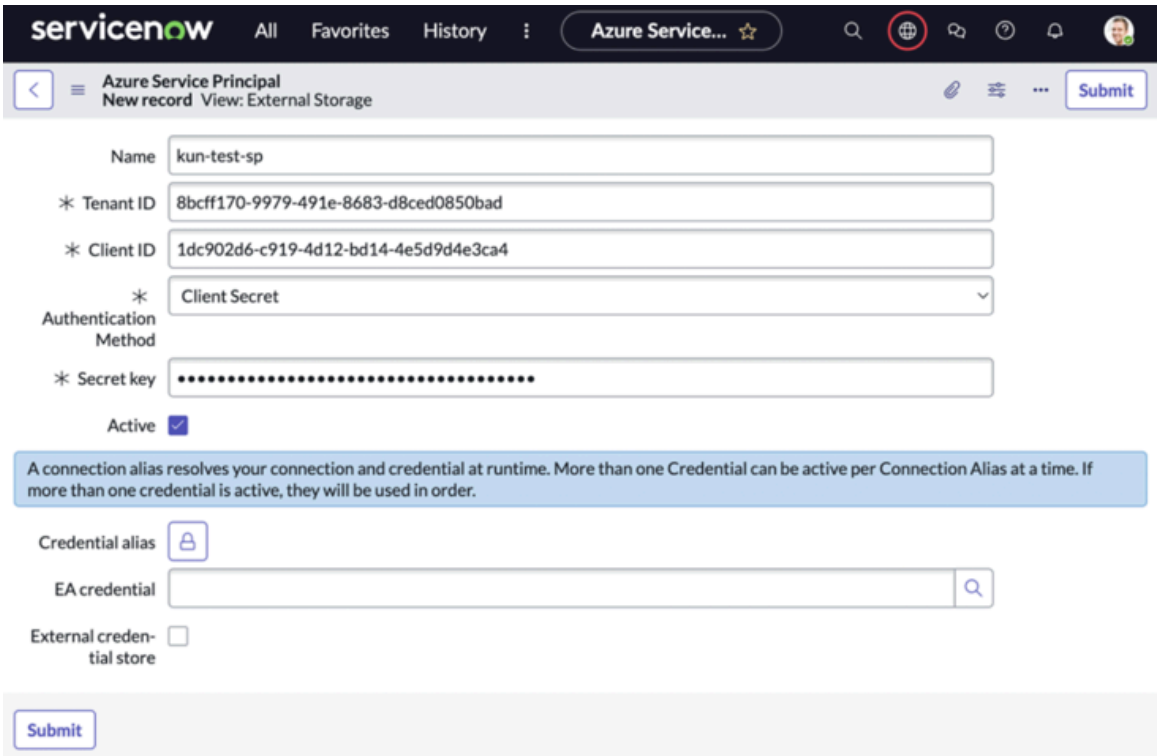
Bevor Sie Anmeldeinformationen erstellen **Externer Anmeldeinformationsspeicher** Plugin ist erforderlich, um Azure VM mithilfe von OpenSSH-Zertifikaten zu verbinden.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

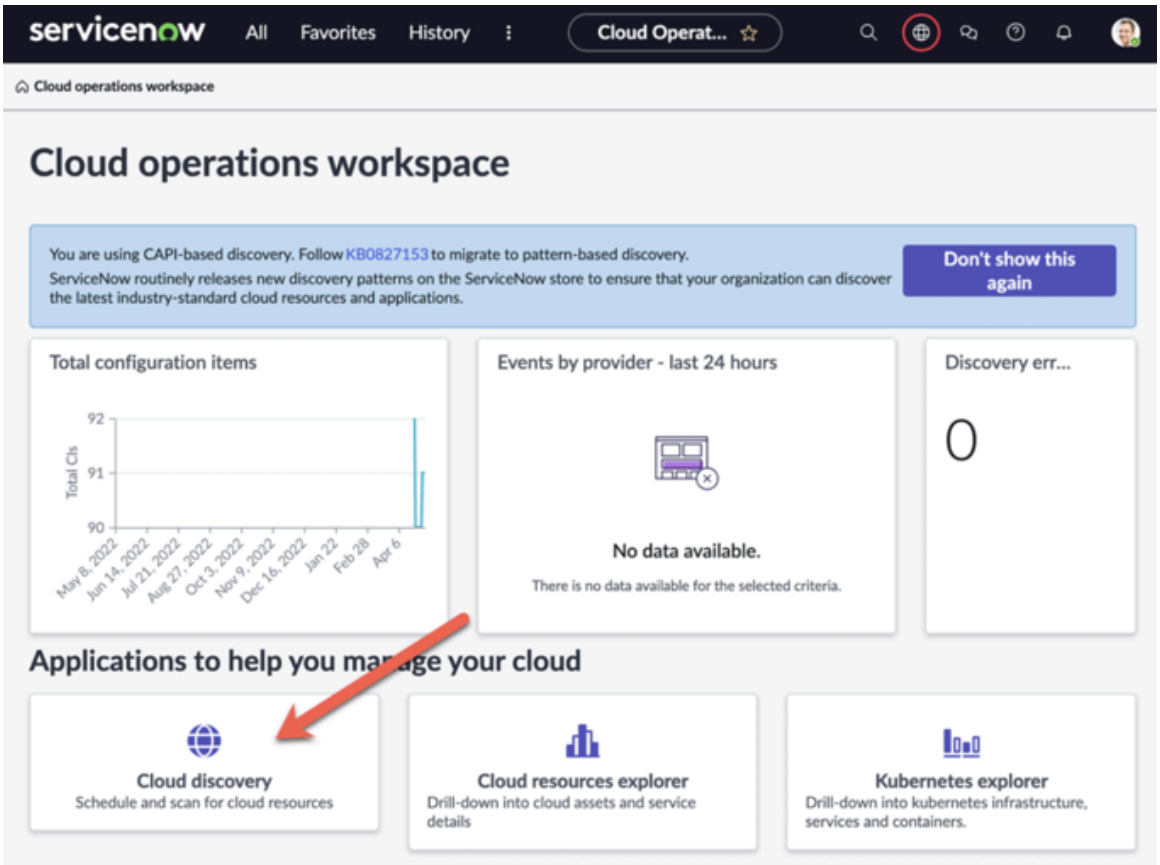
1. Navigieren Sie in der -Instanz zu **Discovery** > **Anmeldeinformationen** Und wählen Sie aus **Neu** .
2. Wählen Sie für den Typ der Anmeldeinformationen aus **Azure-Service-Prinzipal** .
3. Füllen Sie das Formular mit den erforderlichen Informationen aus, und übermitteln Sie es.



4. Navigieren zu **Discovery** > **Anmeldeinformationen** Und wählen Sie aus **Neu** .
5. Wählen Sie für diese Art von Anmeldeinformationen aus **Azure SSH-Zertifikatanmeldeinformationen** .
6. Füllen Sie das Formular mit den erforderlichen Informationen aus, einschließlich der Verknüpfung der in Schritt 3 erstellten Serviceprinzip-Anmeldeinformationen.
   Die Anmeldeinformationen für Azure-Service Provider und SSH-Zertifikat wurden erstellt und verknüpft. Fahren Sie mit dem Verfahren fort, um den Cloud-Discovery-Zeitplan zu erstellen.
7. Navigieren Sie zur Homepage des Cloud Discovery-Arbeitsbereichs, und wählen Sie aus **Cloud-Discovery** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Wählen Sie **Neuer Discovery-Zeitplan**.
9. Geben Sie einen Namen für den Zeitplan an, und wählen Sie aus **Azure** Als Cloud-Anbieter.
10. Erstellen Sie ein neues Abonnement mit **Azure-Service-Prinzipal** In Schritt 3 erstellte Anmeldeinformationen.
11. Wählen Sie Rechenzentren aus.
12. Aktivieren Sie die Option zum Erkennen virtueller Computer.
13. Schließen Sie die Zeitplanerstellung ab, indem Sie auswählen **Beenden und ausführen** .

Ergebnis

Der Discovery-Zeitplan sollte beginnen, und auf der Cloud Operations-Homepage sollte der Ausführungsstatus für den neu erstellten Zeitplan angezeigt werden. Nach einiger Zeit sollte die geplante Discovery abgeschlossen werden, und dann wird ein neuer Zeitplan für die VM-Discovery erstellt und ausgeführt. Der neue VM-Discovery-Zeitplan verwendet den SP, den wir für die Generierung von SSH-zertifikaten erstellt haben, um sich bei den VMs zu authentifizieren. Sie können dies im Abschnitt „Discovery-IP-Affinität“ für die Anmeldeinformationen beobachten.

Über Microsoft Azure-Warnungen gesteuerte Erkennung

Der Microsoft Azure-Warnungsservice kann Warnungen für Änderungen am Lebenszyklusstatus oder an der Konfiguration einer Cloud-Ressource auslösen. Sie können den Service so konfigurieren, dass die neuesten Ressourceninformationen in der Configuration Management Database (CMDB) automatisch aktualisiert werden, ohne auf die Ausführung der nächsten geplanten Cloud-Discovery zu warten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Die Azure Die Change-Verarbeitung bietet im Vergleich zu eine optimale Leistung Microsoft Azure Warnungsgesteuerte Discovery, die eine veraltete Form der Authentifizierung verwendet und nicht mehr verwendet werden sollte. Beginnend mit Muster für Discovery und Service-Mapping App-Version 1,1.0, die Azure Die Change-Verarbeitung hat ersetzt Microsoft Azure Warnungsgesteuerte Discovery. Verwenden Sie den neuen sicheren Webhook, oder migrieren Sie zu Azure Change-Verarbeitung Für zusätzliche Leistungssteigerungen. Weitere Informationen finden Sie unter im sicheren Webhook im Knowledge Base-artikel Der Azure-Warnungsservice zum automatischen Aktualisieren der CMDB verfügt über Webhook-url ohne Anmeldeinformationen im Azure-Portal .

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft `sn_cmp.error_events.default_domain` auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Sie können die Cloud Event Scripted REST API so konfigurieren, dass Warnungen vom Microsoft Azure-Warnungsservice empfangen werden. Für jede Warnung – auch Event genannt – erstellt die API einen Datensatz in der Tabelle „Cloud-Events“ [sn_cmp_cloud_event]. Der Cloud Event Scheduler liest die Events aus der Tabelle [sn_cmp_cloud_event] für die Batch-Verarbeitung. Der Scheduler ruft das Muster auf, um die Events zu verarbeiten, die sich im Status „Bereit“ befinden. Die Muster erkennen die betroffene Ressource und fügen ihre Details in der CMDB hinzu oder aktualisieren sie. Diese Methode hilft beim Aktualisieren von CMDB Konfigurationselementdaten (Configuration Item, CI) und zeigen Sie die neuesten Daten im Cloud-Anwenderportal an.

Wichtig: Wenn Sie Domänentrennung für Cloud-Discovery verwenden, sind auch die Ereignisse nach Domänen getrennt. Daher können Sie die Details eines verarbeiteten Events nur anzeigen, wenn es zu Ihrer Domäne gehört. Wenn ein Ereignis keinem Servicekonto zugeordnet ist, wird es der globalen Domäne zugeordnet.

Für jedes Event speichert die Cloud Event Scripted REST API die folgende Informationen in der Tabelle [sn_cmp_cloud_event]:

- **Quelle**: Dieses Feld ist immer auf `azure activity log` (Azure-Aktivitätsprotokoll) festgelegt.
- **Eventname**: Name des von der Microsoft Azure-Konsole empfangenen Events.
- **Ressourcen-ID**: ID der betroffenen Ressource. Wenn VM-Events vorhanden sind, verwendet Cloud-Discovery diese Informationen, um die VM zu identifizieren.
- **Ressourcentyp**: Ressourcentyp der betroffenen Ressource.

Konfigurieren Sie Microsoft Azure Warnungsservice zum automatischen Aktualisieren von CMDB

Konfigurieren Sie den Microsoft Azure-Warnungsservice so, dass die Configuration Management Database (CMDB) automatisch aktualisiert wird, ohne auf die Ausführung der nächsten geplanten Cloud-Discovery zu warten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Vergewissern Sie sich, dass entweder Discovery oder Cloud Provisioning and Governance in der Instanz aktiviert ist.
- ○ Ein aktiver MID-Server mit Microsoft Azure-Discovery-Funktionalität ist verfügbar.

  Hinweis: Die Warnungskonfiguration pingt weiterhin Warnungen, auch wenn der MID-Server nicht verfügbar ist. Dies führt wiederum zu einer hohen Anzahl von Fehlern in der ECC-Warteschlange. Wenn kein MID-Server verfügbar ist, müssen Sie die Microsoft Azure-Warnungsregel manuell deaktivieren. Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält alle Microsoft Azure-Warnungsregeln.

Erforderliche Rolle:

- ServiceNow-Rolle: sn_cmp.cloud_event_integration
- Microsoft Azure-Rollen:
  - ○ Microsoft Azure-Anmeldeinformationen mit der Leser-Rolle
  - ○ Benutzerdefinierte Microsoft Azure-Rolle mit den folgenden Berechtigungen:

```
"permissions": [
        {
          "actions": [
            "Microsoft.Insights/ActionGroups/Write",
            "Microsoft.Insights/ActionGroups/Delete",
            "Microsoft.Insights/ActionGroups/Read",
            "Microsoft.Insights/ActivityLogAlerts/Write",
            "Microsoft.Insights/ActivityLogAlerts/Delete",
            "Microsoft.Insights/ActivityLogAlerts/Read",
            "Microsoft.Insights/ActivityLogAlerts/Activated/Action",
            "Microsoft.Insights/AlertRules/Write",
            "Microsoft.Insights/AlertRules/Delete",
            "Microsoft.Insights/AlertRules/Read",
            "Microsoft.Resources/deployments/write",
            "Microsoft.Resources/deployments/delete",
            "Microsoft.Resources/deployments/read"
          ],
```

Hinweis: Zum Einrichten der warnungsbasierten Erkennung können Sie einen Microsoft Azure-Dienstprinzipal nur mit der Leserrolle verwenden. Weitere Informationen finden Sie im Community-Artikel Azure alert driven discovery with reader privileges (Auf Azure-Warnungen basierte Erkennung mit Leseberechtigungen).

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie den Warnungsservice konfiguriert haben, erleichtert er die Nachverfolgung des Lebenszyklusstatus und der Konfiguration von Microsoft Azure Cloud-Ressourcen.

Wichtig: Sie können einen sicheren Webhook verwenden, um weiterzuleiten Microsoft Azure Warnungen an den ServiceNow AI Platform. Weitere Informationen finden Sie unter Verwenden Sie einen sicheren Webhook, um weiterzuleiten Microsoft Azure Warnungen an den ServiceNow AI Platform [KB1208357] an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Deaktivieren Sie die Authentifizierung für die Cloud Event Scripted REST API, da die Microsoft Azure-Warnung die Standardauthentifizierung nicht unterstützt.

   a. Navigieren Sie als Administrator zu **Scripted Web Services** > **Scripted REST APIs**an.

   b. Öffnen Sie den Cloud Event-Datensatz.

   c. Öffnen Sie auf der Registerkarte **Ressourcen** den Datensatz zur Option Cloud Config Event Post (Veröffentlichung zu Cloud-Konfigurations-Event).

   d. Setzen Sie den Anwendungsbereich auf **Global**.

   e. Deaktivieren Sie auf der Registerkarte **Sicherheit** das Kontrollkästchen **Erfordert Authentifizierung**.

   > **Wichtig:** In der ServiceNow-Instanz wird eine Webhook-URL für die warnungsbasierte Erkennung verwendet. Die Microsoft Azure-Warnungskonfiguration der ServiceNow-Instanz unterstützt jedoch keine Authentifizierung zum Erstellen des Webhooks. Sie können die Authentifizierung aktivieren, indem Sie den Benutzernamen und das Passwort in der Webhook-URL angeben. Weitere Informationen finden Sie im KB-Artikel KB0963526 .

2. Navigieren zu **Discovery** > **Cloud-Warnungen** > **Azure-Warnmeldungskonfigurationen**an.

   > **Hinweis:** Wenn Sie Discovery in der Instanz aktiviert haben, können Sie direkt zu navigieren **Warnungskonfigurationen** Verwenden Sie Ihre Instanz-URL. Beispiel:
   >
   > `https://{instancename}.service-now.com/sn_cmp_azure_alert_configuration_list.do`

3. Wählen Sie auf der Registerkarte **Azure** die Option **Neu** aus.
4. Füllen Sie die Felder des Formulars aus.

Azure-Warnungskonfiguration – Formular

Feld	Beschreibung
Servicekonto	Microsoft Azure-Servicekonto, für das Sie die Azure-Warnungskonfiguration erstellen möchten. Stellen Sie sicher, dass Cloud-Discovery alle dem Cloud-Konto zugeordneten logischen Rechenzentren (LRZ) erkannt hat.
Ressourcengruppe	Ressourcengruppe, die die Warnungsregeln enthält. Wählen Sie das Microsoft Azure-Servicekonto aus. Weitere Informationen zum Hinzufügen eines Microsoft Azure-Servicekontos finden Sie unter Fügen Sie einen hinzu Azure Servicekonto. Die Warnungsregeln werden von der Instanz für alle innerhalb des Servicekontos verfügbaren Ressourcen erstellt.
Aktivieren	Option zum Angeben des Status der Warnungskonfiguration. Diese Option ist standardmäßig ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwender	Benutzername eines ServiceNow-Benutzers mit der Rolle sn_cmp.cloud_event_integration.
Passwort	Passwort des ServiceNow-Benutzerkontos.

5. Wählen Sie **Absenden** aus.
   Bei erfolgreicher Konfiguration des Microsoft Azure-Warnungsservice ändert sich der Status der Warnungskonfiguration von **Keine** in **Aktiviert**.

Microsoft Azure-Warnungsregel hinzufügen

Aktivieren Sie die warnungsbasierte Erkennung für einen neuen Microsoft Azure-Warnungstyp, indem Sie ihn der Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] hinzufügen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält alle unterstützten Warnungstypen. Weitere Informationen finden Sie unter Unterstützte Microsoft Azure-Warnungstypen. Vom Microsoft Azure-Warnungsservice werden diese Warnungsregeln, die in der Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] gespeichert sind, dazu verwendet, die Warnungen auszulösen. Cloud-Discovery unterstützt auch alle Warnungen, die für die Mitglieder der in der Microsoft Azure-Warnungskonfiguration angegebenen Ressourcengruppe generiert wurden.

Prozedur

1. Navigieren Sie zur Tabelle „Azure-Warnungsregeln“ [azure_alert_rule], indem Sie in die Navigationsleiste des Browsers die folgende URL eingeben:
   https://<instance name>.service-now.com/azure_alert_rule_list.do
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Azure-Warnungsregel – Formular

Feld	Beschreibung
Regelname	Name des Microsoft Azure-Warnungstyps.
Aktion	Microsoft Azure-API-Pfad für Ressourcenvorgänge. Weitere Informationen zu finden Microsoft Azure Ressourcen, für die Sie Warnungen auslösen können, wechseln Sie zu Microsoft Azure Dokumentation und weitere Informationen finden Sie unter „Azure-Ressourcenanbieter-Vorgänge“.
Aktiv	Option zum Angeben des Status des Microsoft Azure-Warnungstyps. Diese Option ist standardmäßig ausgewählt.

4. Wählen Sie **Absenden** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Microsoft Azure-Warnungstypen

Von der Cloud-Discovery des Basissystems wird die warnungsbasierte Erkennung für mehrere Microsoft Azure-Warnungstypen unterstützt. Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält die unterstützten Warnungstypen.

Von der Cloud-Discovery des Basissystems werden folgende Microsoft Azure-Warnungstypen unterstützt:

```
Microsoft.Compute/virtualMachines/deallocate/action
Microsoft.Network/privateDnsZones/delete
Microsoft.Compute/availabilitySets/write
Microsoft.Network/loadBalancers/write
Microsoft.Network/connections/delete
Microsoft.Network/publicIPAddresses/delete
Microsoft.Storage/storageAccounts/write
Microsoft.Network/virtualNetworks/delete
Microsoft.Sql/servers/databases/delete
Microsoft.Network/expressRouteCircuits/write
Microsoft.Network/localnetworkgateways/delete
Microsoft.Network/networkInterfaces/delete
Microsoft.Compute/virtualmachines/write
Microsoft.Network/expressRouteCircuits/delete
Microsoft.Network/natGateways/write
Microsoft.Network/loadBalancers/delete
Microsoft.Compute/virtualMachineScaleSets/delete
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete
Microsoft.Storage/storageAccounts/delete
Microsoft.Compute/availabilitySets/delete
Microsoft.Network/connections/write
Microsoft.Compute/virtualMachines/start/action
Microsoft.Compute/virtualMachines/restart/action
Microsoft.Sql/servers/databases/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Network/networkInterfaces/write
Microsoft.Network/privateDnsZones/write
Microsoft.Network/localnetworkgateways/write
Microsoft.Network/natGateways/delete
Microsoft.Compute/virtualMachines/stop/action
Microsoft.Network/publicIPAddresses/write
Microsoft.Compute/virtualMachineScaleSets/write
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write
Microsoft.Network/virtualNetworks/write
Microsoft.Sql/servers/delete
Microsoft.Sql/servers/write
```

Azure Change-Verarbeitung

Die Azure Die Funktion „Change-Verarbeitung“ erfasst Informationen zu Microsoft Azure Ressourcen, die einer Statusänderung oder Konfigurationsänderung im Lebenszyklus unterzogen wurden Nahezu Echtzeit . Anschließend werden die gesammelten Informationen verwendet, um zu aktualisieren Configuration Management Database (CMDB).

Die Azure Geplante Aufgaben der Change-Verarbeitung fragen ab Azure API und erfassen Sie die Informationen zur Ressourcenänderung. Während jedes Ausführungszyklus erfasst die geplante Aufgabe Informationen zu allen Ressourcen, die sich geändert haben Nach dem letzten Azure-Change-Verarbeitungszyklus.Nach dem Sammeln der Change-Informationen wird die Azure Die Change-Verarbeitung verwendet Antwortzuordnungen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um die Change-Informationen in zu aktualisieren CMDB. Während der nächsten Discovery Cloud-Discovery Löst entsprechende Muster aus, falls verfügbar, und füllt detaillierte Ressourceninformationen in aus CMDB.

Standardmäßig ist Azure Geplante Aufgaben zur Change-Verarbeitung werden alle 5 Minuten ausgeführt. Aktualisieren Sie bei Bedarf die Ausführungshäufigkeit des Zeitplans entsprechend Ihren Anforderungen. Legen Sie die Ausführungshäufigkeit innerhalb des Mindestwerts von einer Minute fest.

Wenn Sie ausführen Azure Change-Verarbeitung zum ersten Mal. Sie kann einige Stunden ausgeführt werden S aufgrund der Verarbeitung von Ressourcenänderungen, die in den letzten vier Stunden aufgetreten sind. Wenn Sie den standardmäßigen Ausführungszeitraum des Zeitplans verlängern möchten, stellen Sie sicher, dass genügend Worker-Knoten zur Ausführung des Zeitplans verfügbar sind.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Hinweis:

Azure Die Change-Verarbeitung kann Ressourcenänderungsinformationen nur aus den Service-Accounts abrufen, die von Discovery_admin oder sn_CMP.Cloud_admin erstellt wurden.

Aktualisieren Sie Ihren Muster für Discovery und Service-Mapping Plugin auf ServiceNow Store Muss mindestens Version 1.21.0 von haben Azure Change-Verarbeitung. Sehen Sie sich das Upgrade-Szenario in an KB1705862

Startet in Muster für Discovery und Service-Mapping Version 1.21.0, die geplanten Aufgaben wurden erweitert und umbenannt:

- Die *Azure Process Changes*Die geplante Aufgabe wurde umbenannt in *ACP Pull Changes*.
- Die *CPG Build Azure Changes IRE Payload*Die geplante Aufgabe wurde umbenannt in *ACP Process Changes*.

ACP-Tabellen

Wird gestartet Muster für Discovery und Service-Mapping Version 1.21.0, Erweiterung der Azure-Change-Verarbeitung führt vier Tabellen ein.

ACP-Ressourcentyp [sn_itom_pattern_acp_supported_resource_types]

Sie können diese Tabelle verwenden, um alle unterstützten Ressourcentypen zu überprüfen, einen Ressourcentyp für die Change-Verarbeitung hinzuzufügen und die Verarbeitung für eine bestimmte Ressource zu deaktivieren oder zu aktivieren.

Weitere Informationen zum Hinzufügen von Support für Azure Ressourcentyp, siehe Fügen Sie Unterstützung für die Change-Verarbeitung für hinzu Azure Ressourcentyp.

Schlüsselfelder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcentyp.
- Abfrage: Die Ressourcendiagrammabfrage, die Änderungen von abruft Azure.
- Aktiv: Gibt an, ob der Ressourcentyp aktiv abgefragt wird.

ACP-Bestellstatus [sn_itom_pattern_acp_order_Status]

Diese Tabelle verfolgt den Status von Azure Ressourcendiagrammabfrage für jeden Ressourcentyp basierend auf den zugehörigen Anmeldeinformationen, die für die Abfrage verwendet werden Azure. Sie können diese Tabelle verwenden, um den Verarbeitungsstatus zu überprüfen. Weitere Informationen zur Abfrage finden Sie unter KB1705862 .

Schlüsselfelder:

- Ressourcentyp.
- Anmeldeinformationen: Die spezifischen Anmeldeinformationen, die zum Abrufen von Changes verwendet werden.
- Zeit der letzten Verarbeitung.
- Status: Verfolgt den Erfolg oder Fehler des Ereignisabrufprozesses. Nach dem nächsten ACP-Abruf-Changes Geplante Aufgabe. Dieser Status wird basierend auf dem CMP-Auftragsstatus aktualisiert.
- CMP-Reihenfolge: Verweis auf das Feld „CMP-Reihenfolge“ [sn_CMP_order], das Details zum aktuellen Auftragsfortschritt und zum aktuellen Ergebnis enthält.

ACP-Ressourcenänderung [sn_itom_pattern_acp_resource_Change]

Diese Tabelle zeichnet Änderungen in auf Azure Ressourcen. Die Tabelle [sn_CMP_resource_Changes_Payload_info], die zum Speichern dieser Informationen vor Version 1.21.0 verwendet wurde, ist nicht mehr verfügbar.

Schlüsselfelder:

- Ressourcen-ID: Der eindeutige Bezeichner für die geänderte Ressource in Azure.
- Change-Nutzlast: Ein Snapshot der Attribute, die für die Ressource von Interesse sind.
- Reihenfolge: Ein Verweis auf das Feld „CMP-Reihenfolge“ [sn_CMP_order], das den Change abgerufen hat.
- Ressourcenstatus: Ein Verweis auf die Tabelle „ACP-Ressourcenstatus“, um den Verarbeitungsstatus des Change nachzuverfolgen.
- Status: Der aktuelle Verarbeitungsstatus des Change. Wenn der Status als „Fehler“ markiert ist, überprüfen Sie den zugehörigen Ressourcenstatusdatensatz auf weitere Details.

ACP-Ressourcenstatus [sn_itom_pattern_acp_resource_Status]

Diese Tabelle verfolgt den Gesamtstatus der Ressourcenverarbeitung.

Schlüsselfelder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressourcen-ID: Der Bezeichner für die zu verarbeitende Ressource.
- Status: Der Verarbeitungsstatus. Die status sind: Bereit, in Bearbeitung, Fehler und Erfolg.
- Fehlermeldung: Wenn die Verarbeitung fehlgeschlagen ist, enthält dieses Feld Details zum Fehler.

Unterstützt Azure Ressourcentypen und Changes

Azure Die Change-Verarbeitung verfolgt eine Reihe von Ressourceneigenschaften für jeden unterstützten Ressourcentyp. Wenn eine Änderung in einer dieser Eigenschaften erkannt wird, Azure Change-Verarbeitung ruft einen aktualisierten Snapshot der Ressource aus ab Azure, Und verarbeitet es in CMDB Um den Change widerzuspiegeln.

Ressourcentyp	Ressourceneigenschaft
Microsoft.Compute/ VirtualMachine	• *CreateOrDeleteVm : properties.changeType in ('Create','Delete')* • *ChangeStatus: (properties.extended.instanceView.powerState.code) in ('PowerState/running', 'PowerState/stopped', 'PowerState/deallocated'))* • *ChangeDisk: properties.storageProfile* • *ChangeTag: tags.** • *ChangeNetworkInterface : properties.networkProfile.networkInterfaces*
Microsoft.Compute/ Datenträger	• *CreateOrDeleteDisk : properties.changeType in ('Create','Delete')* • *ChangeState : properties.diskState* • *ChangeSize : properties.storageProfile* • *ChangeTag : tags.**
Microsoft.Netzwerk/ Netzwerksicherheitsgruppen	• *CreateOrDeleteNsg : properties.changeType in ('Create','Delete')* • *ChangeTag : tags.**
Microsoft.Netzwerk-/ Netzwerkschnittstellen	• *CreateOrDeleteNic : properties.changeType in ('Create','Delete'),* • *changePrimary : properties. properties.primary* • *ChangeIp : properties.ipConfigurations[0]'* • *ChangeTag : tags.**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcentyp	Ressourceneigenschaft
Microsoft.Network/ publicIPAddresses	• `CreateOrDeleteIp : properties.changeType in ('Create','Delete'),` • `ChangeIpAddress : 'properties.ipaddress',` • `ChangeFqdn : properties.dnsSettings.fqdn` • `ChangeIpConfig : properties.ipConfiguration` • `ChangeTag : tags.*`

Vorteile von Azure Change-Verarbeitung

Die Azure Die Change-Verarbeitung bietet gegenüber den folgende Vorteile Microsoft Azure Warnungsgesteuerte Discovery:

- Verbesserte Leistung und verringerte Wahrscheinlichkeit von Azure API-Drosselung
- Einfaches Setup

Verbesserte Leistung und verringerte Wahrscheinlichkeit von Azure API-Drosselung

Die Microsoft Azure Die warnungsgesteuerte Discovery löst eine gezielte Discovery für jede betroffene Ressource aus. Daher wenn ServiceNow AI Platform Erhält eine große Anzahl von Warnungen, die durch die gezielte Discovery verursacht werden kann Azure Zu drosselnde APIs. Infolgedessen wird die Warnungsverarbeitungsleistung von ServiceNow AI Platform Kann ablehnen. Im Gegensatz dazu Azure Die Change-Verarbeitung löst nicht die gezielte Discovery für jede betroffene Ressource aus. Stattdessen werden Antwortzuordnungen verwendet, um die CMDB gemäß den verfügbaren Change-Informationen zu aktualisieren. Während der nächsten Discovery Cloud-Discovery Löst entsprechende Muster aus, falls verfügbar, und füllt detaillierte Ressourceninformationen in aus CMDB. Daher Azure Die Change-Verarbeitung verbessert die Change-Verarbeitungsleistung von ServiceNow AI Platform Und reduziert die Wahrscheinlichkeit von Azure API-Drosselung.

Einfaches Setup

Die Microsoft Azure Die warnungsgesteuerte Discovery verwendet einen Webhook, um die Warnungen an den zu senden ServiceNow AI Platform. Als Azure Cloud generiert Warnungen auf Abonnementebene, der Microsoft Azure Für die warnungsgesteuerte Discovery ist für jedes Abonnement, das Sie überwachen möchten, ein Webhook erforderlich. Im Gegensatz dazu Azure Die Change-Verarbeitung verwendet CAPI und MID-Server Dient zur Interaktion mit Azure API für Ressourcenänderungen. Die API kann Change-Informationen auf Managementgruppenebene bereitstellen. Daher Azure Die Change-Verarbeitung macht Webhooks überflüssig und vereinfacht das Setup.

Sie können Konfigurieren Sie die Azure-Change-Verarbeitung Um Ressourcenänderungsinformationen aus abzurufen Microsoft Azure Cloud und verwenden Sie sie, um zu aktualisieren CMDB.

Wenn Sie verwenden Microsoft Azure Warnungsgesteuerte Discovery, dann können Sie es Zur Azure-Change-Verarbeitung migrieren Dient zur Verbesserung der Change-Verarbeitungsleistung von ServiceNow AI Platform Und nutzen Sie das vereinfachte Setup.

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Microsoft Azure Cloud-Discovery mithilfe von Mustern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Azure Change-Verarbeitung

Konfigurieren Sie Azure Change-Verarbeitung zum Sammeln von Ressourcenänderungsinformationen aus dem Microsoft Azure Cloud und verwenden Sie sie, um zu aktualisieren Configuration Management Database (CMDB).

Vorbereitungen

- Stellen Sie sicher, dass die neueste Version von ist Muster für Discovery und Service-Mapping Store-App ist auf installiert ServiceNow AI Platform.
- Stellen Sie sicher Microsoft Azure Die warnungsgesteuerte Discovery ist auf nicht konfiguriert ServiceNow AI Platform.

Erforderliche Rolle: Discovery_admin oder sn_CMP.Cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Für Informationen zu den von unterstützten Ressourcen Azure Change-Verarbeitung, siehe Azure Change-Verarbeitung.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Konfigurieren** *Azure* **Change-Verarbeitung**an.
2. Wählen Sie die Accounts aus, die Sie synchronisieren möchten Azure Change-Verarbeitung für.
   a. Wählen Sie die Accounts aus dem aus **Service-Accounts Ohne Change-Verarbeitung auf „Pull-Basis“** Liste.
   b. Fügen Sie die ausgewählten Accounts zu hinzu **Service-Accounts Mit Change-Verarbeitung auf „Pull-Basis“** Liste.

   Hinweis: Wenn Sie aktivieren Azure Change-Verarbeitung für Azure Verwaltungsgruppe ist auch für alle Abonnements in der Verwaltungsgruppe aktiviert.
3. Wählen Sie **OK**.

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Migrieren Sie zu Azure Change-Verarbeitung

Migrieren Sie zu Azure Change-Verarbeitung, um die Change-Verarbeitungsleistung von zu verbessern ServiceNow AI Platform Und nutzen Sie das vereinfachte Setup.

Vorbereitungen

- Stellen Sie sicher, dass die neueste Version von ist Muster für Discovery und Service-Mapping Store-App ist auf installiert ServiceNow AI Platform.
- Stellen Sie sicher Microsoft Azure Die warnungsgesteuerte Discovery ist auf konfiguriert ServiceNow AI Platform.
- Stellen Sie sicher, dass die Tabelle „Cloud-Ereignisse“ [sn_CMP_Cloud_event] kein Ereignis im Status „bereit“ enthält.
- Stellen Sie sicher, dass der Bereich auf Global festgelegt ist.
- Stellen Sie sicher, dass mindestens ein aktiv ist MID-Server Ist verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Discovery_admin oder sn_CMP.Cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie verwenden Microsoft Azure Warnungsgesteuerte Discovery und ServiceNow AI Platform Erhält eine große Anzahl von Warnungen von Azure Cloud kann es eine beträchtliche Zeit dauern, bis die Warnungen verarbeitet und aktualisiert werden Configuration Management Database (CMDB). Migrieren Sie zu AzureÄndern Sie die Verarbeitung, um Leistungsprobleme zu überwinden. Weitere Informationen zu finden Azure Change-Verarbeitung, siehe Azure Change-Verarbeitung.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Konfigurieren** *Azure* **Change-Verarbeitung**an.
2. Wählen Sie Abrufen Azure Warnungskonfigurationen zum Abrufen der Liste aller aktiven Azure Warnungskonfigurationen.
3. Wählen Sie Aus **Deaktivieren** *Azure* **Warnungskonfigurationen** .
   Die ServiceNow AI Platform Deaktiviert Azure Warnungskonfigurationen und entfernen S Die Webhooks aus dem Azure Portal.
4. Wählen Sie die Accounts aus, für die Sie konfigurieren möchten Azure Change-Verarbeitung.

   a. Von **Service-Accounts ohne „abrufbasierte“ Change-Verarbeitung** Wählen Sie die Accounts aus, für die Sie konfigurieren möchten Azure Change-Verarbeitung.

   b. Fügen Sie die ausgewählten Accounts zu hinzu **Service-Accounts mit „Pull-based“ Change-Verarbeitung** Liste.

   Hinweis: Wenn Sie aktivieren Azure Change-Verarbeitung für Azure Verwaltungsgruppe ist auch für alle Abonnements in der Verwaltungsgruppe aktiviert.

5. Wählen Sie **OK**.

Ergebnis

Das Migrationsskript markiert Azure Konfigurationsmodul als veraltet. In Cloud-Discovery. Die Azure Die Seite „Warnungskonfigurationen“ ist in ausgeblendet Cloud Operations Workspace.

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Fügen Sie Unterstützung für die Change-Verarbeitung für hinzu Azure Ressourcentyp

Hinzufügen Azure Verarbeitungsunterstützung für ändern Azure Ressourcentyp entsprechend den Anforderungen Ihrer Organisation.

Vorbereitungen

Erforderliche Rolle: Discovery_admin oder Cloud_root_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren gilt nur für Muster für Discovery und Service-Mapping Store-Versionen, die älter als 1.21.0 sind. Ab Version 1.21.0 werden alle unterstützten Ressourcentypen in der Tabelle [sn_itom_pattern_acp_supported_resource_types] aufgeführt.
Alle Ressourcentypen sind standardmäßig aktiviert. Die MID-Server Eigenschaft *mid.cmp.azure.event.supported_resource_types*lst nicht mehr verfügbar. Sie können die Tabelle [sn_itom_pattern_acp_supported_resource_types] verwenden, um einen Eintrag

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für einen Ressourcentyp hinzuzufügen und eine Abfrage hinzuzufügen. Informationen zum Hinzufügen einer Abfrage finden Sie im Abschnitt „Beispiel-VM-Abfrage“ in KB1705862 .

Dient zum Hinzufügen von Unterstützungen für die Change-Verarbeitung für Azure Ressourcentyp In Legacy-Versionen , Fügen Sie die Ressourcentypen zu hinzu `mid.cmp.azure.event.supported_resource_types`Eigenschaft. Als kommagetrennter Wert. Erstellen Sie dann Antwortzuordnungen zwischen den Change-Feldern und den CI-Feldern (Configuration Item). Antwortzuordnungen definieren eine Einzelzuordnung zwischen den Quelldatenfeldern und den CI-Feldern. Azure Bei der Change-Verarbeitung werden die Zuordnungsinformationen verwendet, um Ressourcenänderungsdaten in den entsprechenden CI-Klassenfeldern zu aktualisieren.

Prozedur

1. Navigieren zu **Alle** > *`MID-Server`* > **Eigenschaften**an.
2. Öffnen Sie die Eigenschaft `mid.cmp.azure.event.supported_resource_types`.
3. In **Wert** Feld hinzufügen *`Azure`* Ressourcentyp als kommagetrennter Wert.
4. Wählen Sie **Aktualisieren**.
5. Erstellen Sie Antwortzuordnungen für die Change-Felder, die Sie in aktualisieren möchten Configuration Management Database (CMDB).

   a. Navigieren Sie zur Tabelle Antwortzuordnung [sn_CMP_response_Mapping].
   https://<instance name>.service-now.com/sn_cmp_response_mapping_list.do

   b. Wählen Sie **Neu**.

   c. Füllen Sie im Formular die Felder aus.

   Formular „Antwortzuordnung“

Feld	Beschreibung
CI-Klasse	Name der CI-Klasse, die die Azure-Ressource in darstellt CMDB.
Datenquelle	Name der Eingabedatenquelle. Legen Sie das Feld Datenquelle auf fest Azure Ressourcenänderungen.
CI-Klassenfelder	Name des CI-Klassenfelds, das das logische Äquivalent des Quellfelds ist.
Quellenfeld	Name des Quellfelds, das Sie im angegebenen CI-Klassenfeld aktualisieren möchten.

   Weitere Informationen zur Antwortzuordnung finden Sie unter Antwortzuordnung wird verwendet Thema in ServiceNow Community.

   d. Wählen Sie **Absenden**.

   e. Wiederholen Sie die Schritte 5.bBis 5.dFür alle Change-Felder, die Sie in aktualisieren möchten CMDB.

Erkennung von Google Cloud Platform

Discovery erkennt Google Cloud Platform und die zugehörigen Komponenten. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Für die Google Cloud Platform-Komponenten erkannten Daten bieten Sichtbarkeit für mehrere ServiceNow-Produkte, einschließlich Cloud Provisioning and Governance.

Discovery verwendet mehrere Muster, um GCP-Komponenten zu erkennen.

Sie können globale und regionale Ressourcen erkennen.

Erkennbare globale und regionale GCP-Ressourcen

Global	Regional
Globale statische externe IP-Adressen	Regionale statische externe IP-Adressen
Globale Lastenausgleichsmodule (Globale HTTP-Lastenausgleichsmodule)	Regionale Lastenausgleichsmodule (regionale HTTP-Lastenausgleichsmodule, TCP/UDP-Lastenausgleichsmodule)
Bilder	Subnetze
Snapshots	Regionale verwaltete Instanzgruppen
Instanzvorlagen	Regionale persistente Festplatten
VPC-Netzwerk	
Firewalls	

Anforderungen für GCP Discovery

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping Startversion 1.8.0 (September 2023)
- CMDB CI-Klassenmodelle Startversion 1.49.0 (September 2023)
- Visibility Content Startversion 6.13.0 (September 2023)

Verifizieren Sie MID-Server Anforderungen

- Verwenden Sie zur Cloud-Erkennung einen dedizierten MID-Server. Der MID-Server muss über 16 Kerne und 8 GB mit 4 GB Java Memory Model (JVM)-Speicherzuweisung verfügen. Für Informationen zur Verifizierung MID-Server Spezifikationen siehe KB-artikel KB2156327 .
- Stellen Sie den dedizierten MID-Server mit Internetzugang bereit und stellen Sie die Verbindung her.
- Weitere Informationen zu finden MID-Server Konfigurationen, siehe Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.

Verifizieren Google Cloud BigQuery und Google Cloud-Bigtable-Anforderungen

Um zu erkennen Google Cloud BigQuery und Google Cloud-Bigtable, navigieren Sie zu **Alle** > **Discovery** > **MID-Server** > **Eigenschaften** Und stellen Sie sicher, dass die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*sn_itom_pattern.google_dbservice_table_collection*Eigenschaft ist auf festgelegt **Wahr** .

Überprüfen Sie die Anwenderrolleneinstellungen

Legen Sie die Benutzerberechtigung für das Google Cloud Platform-Mitglied auf **Betrachter** fest:

1. Navigieren Sie in der Google Cloud Platform-Konsole zu **IAM**.
2. Wählen Sie das entsprechende Mitglied aus der Liste aus, und klicken Sie auf das Symbol **Bearbeiten**.
3. Wählen Sie im Fenster „Bearbeitungsberechtigungen“ in der Liste **Rolle** Betrachter aus.
4. Klicken Sie auf **Speichern**.

Konfigurieren Google API-Anmeldeinformationen

Weitere Informationen finden Sie unter Konfigurieren Sie Google API-Anmeldeinformationen für Cloud-Discovery.

Erstellen Sie einen Google Cloud Platform Service-Account

Weitere Informationen finden Sie unter Erstellen GCP Service-Accounts.

Sammeln von Cloud-Protokollierungs-Events aktivieren

Die Google Cloud Platform-Muster können Cloud-Protokollierungs-Events sammeln, die von den nativen Google Cloud-APIs generiert werden. Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Überprüfen Sie, ob ein Discovery Zeitplan ist konfiguriert

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Zugehörige Informationen

Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern

Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB

Sie können den Google Stackdriver Logging-Service aktivieren, um CMDB CI-Daten automatisch zu aktualisieren, wenn Google Cloud Connector oder Ihr Google-Konto bei einer Google Cloud Platform-Ressource eine Änderung des Lebenszyklusstatus oder der Konfiguration durchführt. Die CI-Daten werden dann in der CMDB aktualisiert, ohne dass auf die Ausführung von Discovery gewartet werden muss.

Vorbereitungen

- Aktivieren Sie Discovery and Service Mapping-Muster. Weitere Informationen finden Sie unter Google Cloud Platform Discovery.
- Discovery hat die logischen Rechenzentren des Google-Projekts erfolgreich erkannt. Weitere Informationen finden Sie unter Richten Sie ein Cloud-KontoUnd ServicekontoFür Google Cloud Platform.

  Hinweis: Vergewissern Sie sich, dass Sie auf der Seite „Google-Servicekonto“ das Kontrollkästchen **Sollte Events abrufen** aktiviert haben, bevor Sie Discovery für das Rechenzentrum ausführen.

Erforderliche Rolle:

- discovery_admin für Cloud-Discovery und `sn_cmp.cloud_event_integration`, wenn eine Authentifizierung beim Cloud-Event-Endpunkt erforderlich ist. Diese Rolle ist erforderlich, um eine Warnungsregel in der Instanz einzurichten.
- Google Cloud Platform-Administrator für Konfigurationsschritte in der GCP-Konsole.
- Protokollierungsrolle für den Google Cloud Platform (GCP)-Integrationsbenutzer, die OAuth-Bereiche für Folgendes zulässt:
  - `https://www.googleapis.com/auth/logging.admin`
  - `https://www.googleapis.com/auth/cloud-platform.read-only`
  - `https://www.googleapis.com/auth/cloud-platform`
  - `https://www.googleapis.com/auth/logging.read`

Warum und wann dieser Vorgang ausgeführt wird

Discovery Unterstützt die Überwachungs-API-Warnungen der Vorgangs-Suite von Google Cloud aus einem bestimmten Projekt in Google Cloud Platform. Wenn eine Warnung/ein Event für die Ressourcen in einem Projekt generiert wurde, erfasst Discovery die Warnungsdaten.

Erstellen und verwalten Sie Warnungsrichtlinien mit der Überwachungskonsole der Google Cloud Operations Suite, der Überwachungs-API der Google Cloud Operations Suite und dem Cloud SDK. Jede Richtlinie legt Folgendes fest:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

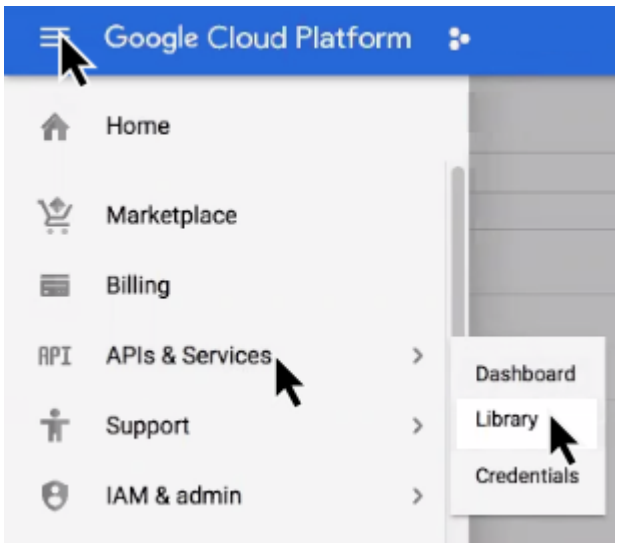
- Bedingungen, die angeben, dass sich eine Ressource oder eine Gruppe von Ressourcen in einem fehlerhaften Zustand befindet.
- Benachrichtigungen, die über E-Mail, SMS oder andere Kanäle gesendet werden, um darauf hinzuweisen, dass ein Ressourcenstatus fehlerhaft ist.
- Dokumentation oder Informationen, die in einige Benachrichtigungstypen aufgenommen werden können, um Ihr Supportteam bei der Lösung des Problems zu unterstützen.

Wenn Ereignisse Bedingungen in einer Ihrer Warnungsrichtlinien auslösen, erstellt die Operations Suite Monitoring von Google Cloud einen Incident und zeigt ihn in der Operations Suite Monitoring-Konsole von Google Cloud an.

Hinweis: Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die in der CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

Prozedur

1. Melden Sie sich bei Ihrem Google Cloud Platform-Konto an.
   Navigieren Sie für Ihr Projekt zu **APIs und Services** > **Bibliothek**an.

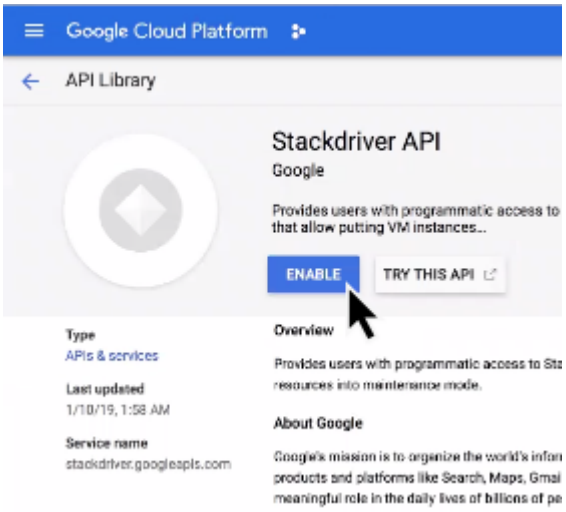


2. Aktivieren Sie sowohl die **Stackdriver API** als auch die **Cloud Logging API**.
   a. Suchen Sie in der Bibliothek nach Stackdriver.
   b. Klicken Sie auf die Karte **Stackdriver API**.

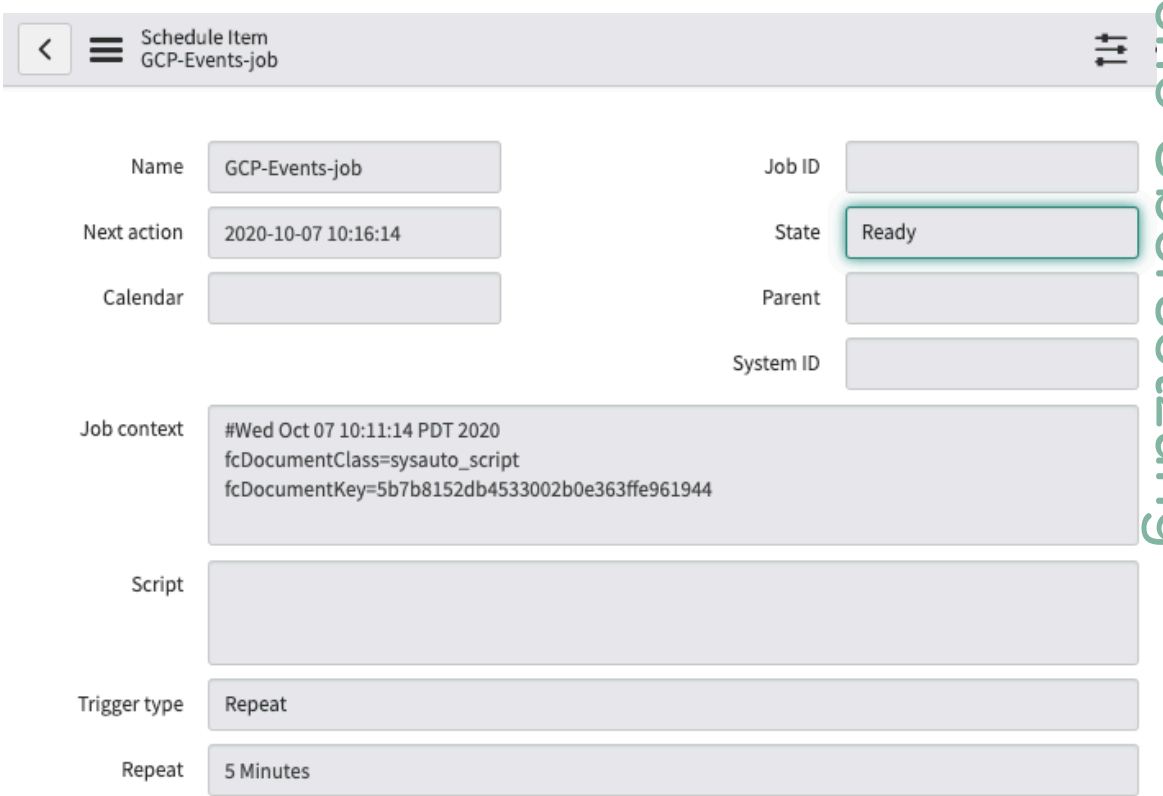
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf der Seite der Stackdriver API auf **Aktivieren**.



3. Wiederholen Sie den vorherigen Schritt für die **Cloud Logging API**.
   Standardmäßig ruft eine regelmäßigen Aufgabe für Ihre Instanz (GCP-Events-job) alle 5 Minuten Aktualisierungen vom Google Stackdriver Logging-Service ab.
4. Um den Zeitplan zu ändern, navigieren Sie zu **Systemzeitplaner** > **Geplante Aufgaben** Und klicken Sie dann auf **GCP-Events-Job** Und aktualisieren Sie dann **Wiederholen** Einstellung nach Bedarf.



5. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

- Sobald die Google Cloud Platform ein Event generiert und Discovery die Eventinformationen empfängt, werden die regelmäßigen Aufgaben „GCP-Events-job“ im Hintergrund ausgeführt.

- Durch den geplanten Auftrag wird die Eventnutzlast an das Modul für Identifizierung und Abgleich (Identification and Reconciliation Engine, IRE) übergeben. Die IRE ergreift dann die erforderlichen Aktionen, um den Status der Ressourcen basierend auf dem Event zu ändern.

Erkennung von IBM-Clouds

Wenn sich Ihre Cloud-Ressourcen in einer IBM-Cloud befinden, erstellen Sie Anmeldeinformationen, die auf das IBM-Konto zugreifen können.

Formular für IBM-Anmeldeinformationen

Feld	Wert
Name	Eindeutiger Name der IBM-Anmeldeinformationen, die bei der Instanz registriert werden sollen
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
SoftLayer-API-Benutzer	Benutzername der Softlayer-Cloud
SoftLayer-API-Schlüssel	Schlüssel der SoftLayer-API
Bluemix-API-Schlüssel	Schlüssel der Bluemix-API

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

API-Liste für IBM Cloud Discovery

Region

CI-Attribute	IBM-Einschränkungen
object_id	Name
dns_domain	domain
Name	alias
short_description	display_name
region	Name

cmdb_ci_availability_zone

CI-Attribute	IBM-Einschränkungen
object_id	id
short_description	longName
Name	Name
install_status	statusId

Standortgruppe (cmdb_ci_cloud_location_group)

CI-Attribute	IBM-Einschränkungen
object_id	id
short_description	Beschreibung
location_group_type_id	locationGroupTypeId
Name	Name
location_group_type	locationGroupType.name

Virtueller Server (cmdb_ci_vm_instance)

CI-Attribute	IBM-Einschränkungen
object_id	id
CPUs	maxCpu/startCpus
memory	maxMemory

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtueller Server (cmdb_ci_vm_instance) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
disks	<nicht zugeordnet>
disks_size	<nicht zugeordnet>
nics	<nicht zugeordnet>
terminated_on	<nicht zugeordnet>
Status	statusId
termination_protection	<nicht zugeordnet>
short_description	notes
Name	hostname
dns_domain	domain
fqdn	fullyQualifiedDomainName

Image (cmdb_ci_os_template)

CI-Attribute	IBM-Einschränkungen
cmdb_ci_os_template	
image_type	
guest_os	
Version	
offer	
OS Status	
root_device_type	
image_source	
Anmeldeinformationen	
infuse_key	
update_host_name	
Name	Name
object_id	id
short_description	Beschreibung

Öffentlichen Schlüssel hinzufügen (cmdb_ci_cloud_key_pair)

CI-Attribute	IBM-Einschränkungen
object_id	id
finger_print	fingerprint
created_date	createDate
key	key

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffentlichen Schlüssel hinzufügen (cmdb_ci_cloud_key_pair) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
Name	Bezeichnung
modify_date	modifyDate
short_description	notes

Speichervolume (cmdb_ci_storage_volume)

CI-Attribute	IBM-Einschränkungen
volume_id	id
size	capacityGb
size_bytes	capacityGb
free_space	<nicht zugeordnet>
free_space_bytes	<nicht zugeordnet>
media_type	<nicht zugeordnet>
file_system	<nicht zugeordnet>
Bezeichnung	serviceResourceName
lun (Logische Einheitsnummer)	<nicht zugeordnet>
volume_container	<nicht zugeordnet>
Status	?
storage_type	storageTypeId
protected_by	<nicht zugeordnet>
share_count	<nicht zugeordnet>
sharable	FALSCH
Gerät	guestId
delete_on_termination	<nicht zugeordnet>
mapping_type	<nicht zugeordnet>
object_id	id
vdisk_id	<nicht zugeordnet>
storage_type	nasType
Name	serviceResourceName

Snapshot des Speichervolume (cmdb_ci_storage_vol_snapshot)

CI-Attribute	IBM-Einschränkungen
object_id	id
Kapazität	capacityGb
is_encrypted	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Snapshot des Speichervolume (cmdb_ci_storage_vol_snapshot) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
volume_name	serviceResourceName
storage_server	
start_time	
Status	
snapshotSizeBytes	snapshotSizeBytes

Netzwerk (cmdb_ci_network)

CI-Attribute	IBM-Einschränkungen
Status	
cidr	<nicht zugeordnet>
is_external	Wahr/Falsch
netmask	<nicht zugeordnet>
broadcast_address	<nicht zugeordnet>
default_gateway	<nicht zugeordnet>
is_shared	<nicht zugeordnet>
is_dhcp_enabled	<nicht zugeordnet>
scope	<nicht zugeordnet>
max_ports	<nicht zugeordnet>
terminated_on	<nicht zugeordnet>
provided_contracts	<nicht zugeordnet>
object_id	id
access_port_vlan	vlanNumber
<nicht zugeordnet>	primarySubnetId
Name	vlanNumber
<nicht zugeordnet>	accountId

Subnetz (cmdb_ci_cloud_subnet)

CI-Attribute	IBM-Einschränkungen
subnet_mask	netmask
cidr	networkIdentifier +'/' + cidr
available_ip_count	usableIpAddressCount
broadcast_address	broadcastAddress
primary_dns	<nicht zugeordnet>
secondary_dns	<nicht zugeordnet>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subnetz (cmdb_ci_cloud_subnet) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
tertiary_dns	<nicht zugeordnet>
is_dhcp_enabled	<nicht zugeordnet>
ipam_provider	<nicht zugeordnet>
domain_name	<nicht zugeordnet>
parent_domain_name	<nicht zugeordnet>
gateway	gateway
route_table_association_id	<nicht zugeordnet>
Status	<nicht zugeordnet>
<nicht zugeordnet>	modifyDate
<nicht zugeordnet>	Version
<nicht zugeordnet>	networkVlanId
<nicht zugeordnet>	isCustomerRoutable
object_id	id
<nicht zugeordnet>	broadcastAddress
<nicht zugeordnet>	isCustomerOwned
<nicht zugeordnet>	sortOrder
<nicht zugeordnet>	networkIdentifier
<nicht zugeordnet>	totalIpAddresses
<nicht zugeordnet>	addressSpace
category	subnetType
Name	networkIdentifier +'/' + cidr

Compute-Sicherheitsgruppe (cmdb_ci_compute_security_group)

CI-Attribute	IBM-Einschränkungen
region	<nicht zugeordnet>
object_id	id
intld	<nicht zugeordnet>
tenant_name	<nicht zugeordnet>
Status	<nicht zugeordnet>
<nicht zugeordnet>	port
<nicht zugeordnet>	Beschreibung
<nicht zugeordnet>	createDate
<nicht zugeordnet>	modifyDate
Name	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compute-Sicherheitsgruppe (cmdb_ci_compute_security_group) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
short_description	Beschreibung

Neues CI (cmdb_ci_compute_security_group_rule)

CI-Attribute	IBM-Einschränkungen
erstellt	createDate
direction	direction
ethertype	ethertype
object_id	id
aktualisiert	modifyDate
portRangeMax	portRangeMax
portRangeMin	portRangeMin
protocol	protocol
remoteGroupId	remoteGroupId
securityGroupId	securityGroupId

Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]

CI-Attribute	IBM-Einschränkungen
Status	"operatingStatus"
canonical_hosted_zone_id	
canonical_hosted_zone_name	
dns_name	address
snat_ip_address	
vlan	
app_code	
component_code	
env_code	
ip_address_pool	
	"accountId"
	"address"
	"createDate"
	"description"
object_id	"id"
	isPublic
	"locationId"

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer] (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
	"modifyDate"
Name	"name"
	"provisioningStatus"
	"useSystemPublicIpPool"
	"uuid"

Lastenausgleichsservice (cmdb_ci_lb_service)

CI-Attribute	IBM-Einschränkungen
cmdb_ci_lb_service	
Pool	
port	protocolPort
last_port	
input_url	
host_name	
back_end_port	
front_end_port	protocolPort
listener_protocol	protocol
server_port	
server_protocol	
traffic_domain	
ssl_certificate_id	
object_id	id
hit_count	

LB-Integritätsservice (cmdb_ci_lb_health_service erweitert cmdb_ci_vm_object)

CI-Attribute	IBM-Einschränkungen
check_interval_sec	interval
max_retries	maxRetries
monitor_type	monitorType
provisioning_status	provisioningStatus
timeout_sec	timeout
object_id	id

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LB Pool (cmdb_ci_lb_pool)

CI-Attribute	IBM-Einschränkungen
	createDate
load_balancing_method	loadBalancingAlgorithm
	modifyDate
	protocol
	protocolPort
pool_status	provisioningStatus
object_id	uuid

LB-Poolmitglied (cmdb_ci_lb_pool_member)

CI-Attribute	IBM-Einschränkungen
server_id	address
object_id	id
	createDate
	modifyDate
	provisioningStatus
	uuid
	weight

Ressourcengruppe (cmdb_ci_resource_group)

CI-Attribute	IBM-Einschränkungen
Name	Name
Nachschauen, was das ist?	quota_id
	tags
object_id	id

Organisation (cmdb_ci_cloud_org)

CI-Attribute	IBM-Einschränkungen
Name	Name
url	url
billing_enabled	billing_enabled
quota_definition_url	quota_definition_url
spaces_url	spaces_url
guid	guid
Status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Organisation (cmdb_ci_cloud_org) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
object_id	metadata.guid

Organisation (cmdb_ci_cloud_space)

CI-Attribute	IBM-Einschränkungen
Name	Name
url	url
object_id	metadata.guid
allow_ssh	allow_ssh
guid	metadata.guid

Erkennung von VMware-Clouds

Anwendungen, mit denen auf VMware-Cloud-Ressourcen zugegriffen wird, benötigen Zugriff auf VMware-Anmeldeinformationen.

Der VMware-Anmeldeinformationstyp ermöglicht es Discovery beispielsweise, VMware vCenter auf einem Windows-Computer zu erkunden, um ESX-Computer, virtuelle Computer und Ressourcenpools zu erkennen. VMware DiscoveryUnd die Automatisierungs-API (vCenter-API) stellt jetzt die global eindeutige Seriennummer für Computer-CIs bereit. CIM-Anmeldeinformationen sind nicht erforderlich, um den Zugriff auf jeden VMware-Host zu ermöglichen.

Hinweis: Windows-Anmeldeinformationen sind für vCenter nicht erforderlich Discovery, Wenn gültige VMware-Anmeldeinformationen verwendet werden.

Formular für VMWare-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für die VMware-Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Anwendername	Geben Sie den Anwendernamen ein, den Sie für Ihren VMware-Account verwenden. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Die VMware-Anmeldeinformationen müssen in vCenter über die Rolle mit Lesezugriff verfügen.
Passwort	Geben Sie das Passwort für das VMware-Konto ein.
Betrifft	Wählen Sie mindestens eine aus MID ServersAus der Liste der verfügbaren MID Servers. Die in diesem Datensatz konfigurierten Anmeldeinformationen sind für verfügbar MID ServersIn dieser Liste. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für VMWare-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Konfigurieren Sie VMware-EventsService zum automatischen Aktualisieren von CMDB

Konfigurieren Sie Events der Cloud-Umgebung so, dass die CMDB ohne zusätzlichen Scanvorgang aktualisiert wird. Der VMware-Events-Service kann CI-Daten in der CMDB automatisch aktualisieren, wenn Cloud Provisioning and Governance bei einer VMware-Ressource eine Änderung des Lebenszyklusstatus oder der Konfiguration durchführt. Die CI-Daten werden dann in der CMDB aktualisiert, ohne dass Discovery vorher ausgeführt werden muss.

Vorbereitungen

Wichtig: Sie können den Service für VMware-Events so konfigurieren, dass die CMDB für eventbasierte Erkennungs- oder Konfigurationsänderungen automatisch aktualisiert wird, auch wenn Sie die Cloud Provisioning and Governance-Plugins nicht abonniert und aktiviert haben.

- Sie müssen über ein Cloud-Konto mit VMware, Servicekonten und zugehörigen logischen Rechenzentren verfügen.
- Die folgenden Cloud Provisioning and Governance-Plugins müssen aktiviert sein (nicht obligatorisch für Cloud Discovery):
  - Cloud Provisioning and Governance (com.snc.cloud.mgmt)
  - Cloud Provisioning and Governance Core (com.snc.cloud.core)
  - Cloud API (com.snc.cloud.api)
  - Verwaltung der Cloud-Konfiguration (com.snc.config.mgmt)
- A MID-Server Muss mit verfügbar sein **Alle** Oder **VMware** Fähigkeiten.
- Die vCenter-Rechenzentren werden erfolgreich erkannt, und die zugehörigen Daten werden ausgefüllt.

Erforderliche Rolle: sn_cmp.cloud_event_integration

Warum und wann dieser Vorgang ausgeführt wird

Wenn VMware-Events ein Update sendet, verarbeitet die Instanz das Event und erstellt oder aktualisiert den CI-Eintrag in der CMDB und die CI-Informationen im Cloud-Anwenderportal. Jedes Event wird als Datensatz in der Tabelle „Events“ auf Ihrer Instanz gespeichert. Konfigurieren Sie alle Event-/Warnungsregeln im vCenter.

So stellen Sie eine Verbindung mit einem anderen MID-Server oder mit vCenter her: Aktualisieren Sie die Einstellungen, und klicken Sie dann auf den zugehörigen Link **Starten**. Der Wert für **Status** ändert sich in **Aktualisierung läuft** und dann in **Gestartet**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Prozedur

1. Navigieren Sie auf eine der folgenden Arten zur VMware-Warnungskonfiguration:
   - Verwenden Sie https://baseURL/ecc_agent_ext_context_vcenter zur direkten Navigation über die URL.
   - Auf der **Cloud-Administratorportal** , Navigieren Sie zu **Verwalten** > **Warnmeldungskonfigurationen**an.
2. Klicken Sie auf der Registerkarte **VMware** auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

vCenter-Ereignissammlungskontext

Feld	Beschreibung
Name	Ein eindeutiger Name für den Datensatz der Event-Sammlung
Kurzbeschreibung	Kurzbeschreibung des Datensatzes
Ausführen auf	Wählen Sie **Spezifischer MID Server** aus.
MID-Server	Wählen Sie einen MID-Server.
vCenter	Wählen Sie das zu überwachende vCenter aus.
Erweiterung [schreibgeschützt]	Die MID-Server-Erweiterung dieses Kontexts. Aktualisiert, wenn die Datenerfassung beginnt.
Status [schreibgeschützt]	Der Status des Datenerfassungsprozesses, z. B. „Wird gestartet“, „Gestartet“ usw.
Ausführung auf [schreibgeschützt]	Der MID-Server, auf dem der Eventsammler ausgeführt wird.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
5. Testen Sie die Verbindung zwischen dem vCenter und dem MID-Server: Klicken Sie auf **Testparameter**. In einem Popup-Fenster wird bei Erfolg **Parameter verifiziert** angezeigt. Das Feld **Status** ändert sich nicht. Zum Aktualisieren eines Parameters (z. B. zum Ändern von MID-Server oder vCenter) ändern Sie die Einstellung und klicken Sie dann auf **Parameter aktualisieren**.
6. Klicken Sie auf den zugehörigen Link **Starten**, um mit dem Sammeln von Events für vCenter zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um zu bestätigen, dass die Instanz Events empfängt, stellen Sie sicher, dass im Feld **Status** der Wert **Gestartet** angezeigt wird.
- Klicken Sie auf **Stoppen**, um die Erfassung von Events für ein bestimmtes vCenter zu beenden.
- Klicken Sie auf **Neu starten**, um die Sammlung von Events neu zu starten.

vCenter-Events werden in Tabelle `sn_cmp_cloud_event` ausgefüllt.

Ergebnis

- Wenn das vCenter Events im Event-Manager aufweist und dieselben Events konfiguriert sind, erfasst Cloud Provisioning and Governance die Events und ergreift entsprechende Maßnahmen für die CIs.
- Die Engine für Identifizierung und Abgleich (Identification and Reconciliation Engine, IRE) ändert den CI-Status basierend auf der empfangenen Eventnutzlast, und die IRE kann nicht angepasst werden.

Cloud-Discovery Berichterstellung

Cloud-Discovery Das Reporting bietet eine anwenderfreundliche Oberfläche zum Navigieren und Analysieren Ihres Cloud-Ressourcenbestands. Es bietet Optionen wie Drilldown- und Slice-and-Dice-Ansichten, um granulare Einblicke in Ihre Cloud-Ressourcenbestände zu erhalten, mit Details, die aus der Discovery abgerufen wurden. Sie bietet eine einfache Möglichkeit, den Status und Standort Ihrer Cloud-Ressourcen schnell zu lokalisieren und zu identifizieren, wodurch Ihre Verwaltungsaufgaben optimiert werden.

Erfahren Sie mehr über Cloud-Discovery Berichterstellung:

- Analytics und Berichte für Cloud Resources
- Dashboard Cloud-Ressourcen
- Cloud-Ressourcenbestand

Hinweis: Um bessere Ergebnisse zu erzielen, verwenden Sie den Cloud-Ressourcen-Explorer anstelle der Platform Analytics-Lösungen, die im Dashboard „Cloud-Ressourcen“ angezeigt werden.

Analytics und Berichte für Cloud Resources

Lösungen für Performance Analytics and Reporting enthalten vorverpackte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen ServiceNow AI Platform-Produkten.

Performance Analytics-Inhaltspaket für Cloud-Ressourcen – Übersicht

Das Performance Analytics Content Pack for Cloud Resources zeigt die zusammengefasste Ansicht all Ihrer Cloud-Ressourcen an. Sie können nach bestimmten Informationen filtern, um weitere Details anzuzeigen. Es gibt auch Analytics-Tabellen und -Ansichten, in denen Tags mit Ressourcen verknüpft werden, sodass Sie eigene benutzerdefinierte Dashboards und Berichte erstellen können.

Das Performance Analytics Content Pack for Cloud Resources funktioniert mit Discovery und Cloud Provisioning and Governance und bietet Unterstützung für die folgenden Cloud-Provider:

- Amazon Web Services
- Microsoft Azure Public Clouds

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- VMware vCenter
- Google Cloud Platform (GCP) (Unterstützt mit Performance Analytics Content Pack for Cloud Resources, Version 1.2.1 und höher).

Die Gesamtanzahl der einzelnen Cloud-Ressourcen und die neuesten Cloud-Discovery-Fehlerprotokolle werden im Dashboard angezeigt. Sie können die Cloud-Ressourcen nach Servicekonten, Rechenzentren oder Ressourcengruppen (nur für Microsoft Azure) unter einem bestimmten Anbieter filtern und die Ressourcenanzahl sowie die Ressourcen entsprechend anzeigen.

Das Performance Analytics Content Pack for Cloud Resources-Dashboard des Basissystems enthält kein Widget für die GCP-Ressourcen. Sie können die Berichte und Widgets erstellen, indem Sie Daten aus den entsprechenden Tabellen verwenden. Weitere Informationen zu den Tabellen, die die GCP-Ressourcendaten enthalten, finden Sie unter Dashboard Cloud-Ressourcen. Alternativ dazu können Sie die Anwendung Cloud Operations Workspace installieren, um die GCP-Berichte und -Widgets anzuzeigen. Weitere Informationen finden Sie unter Cloud Operations Workspace.

Für jeden Cloud-Anbieter wird alle 30 Minuten eine separate regelmäßige Aufgabe ausgelöst. Die aktuellen CI-Daten werden in den Analytics-Tabellen für Cloud-Ressourcen aktualisiert, damit das Dashboard realistischer ist und die aktualisierte Anzahl ausweist. Die Informationen zu den einzelnen regelmäßigen Aufgaben sind in der Tabelle für den Cloud-Dashboard-Aufgabenstatus [sn_disco_cd_cloud_dashboard_job_status] verfügbar. In dieser Tabelle werden die Aufgabendetails einschließlich Anbietertyp, Status, Startzeit, Endzeit und Dauer gespeichert.

Die Berichte für die Cloud-Dashboard-Widgets werden aus den Analytics-Tabellen für Cloud-Ressourcen generiert. Die Analytics-Tabellen werden durch die regelmäßige Aufgabe gefüllt. Die regelmäßige Aufgabe fragt die neuen Datenbankansichten ab. Anschließend werden die Datensätze in die Analytics-Tabellen eingefügt und aktualisiert.

Die maximale Ausführungsdauer der regelmäßigen Aufgabe beträgt 360 Minuten. die maximale Zeitüberschreitung für Aufgaben wird mithilfe der Systemeigenschaft (sn_disco_cd.scheduled_job_time_out_in_mins) festgelegt. Wenn die regelmäßige Aufgabe 360 Minuten oder die in dieser Eigenschaft festgelegte Dauer überschreitet, wird sie abgebrochen.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform-Administrator (admin): Installiert und aktiviert diese Analytics- und Reporting-Lösung und kann alle erforderlichen Änderungen an den Systemeigenschaften vornehmen
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datensammlung ein und startet diese. Gibt die Dashboards für die entsprechenden Stakeholder frei
- Cloud-Dashboard-Benutzer (sn_disco_cd.user): Stellt die Cloud-Ressourcen-Widgets im Cloud-Dashboard zusammen und verfügt über Lesezugriff auf die Analytics-Tabellen für Cloud-Ressourcen und die Dashboard-Berichte
- Cloud-Dashboard-Administrator (sn_disco_cd.admin): Kann Dashboard-Widgets und -Berichte anzeigen, hinzufügen oder bearbeiten und verfügt über Lesezugriff auf die Analytics-Tabellen für Cloud-Ressourcen. Standardmäßig enthält (sn_disco_cd.admin) die Rolle (sn_disco_cd.user), und (discovery_admin) enthält die Rolle (sn_disco_cd.admin).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analytics und Berichte für Cloud Resources aktivieren

Aktivieren Sie das Performance Analytics Content Pack für die ServiceNow Store-Anwendung Cloud Resources für die Analytics- und Reporting-Lösung.

Vorbereitungen

Vergewissern Sie sich, dass das Plugin „Cloud Provisioning and Governance“ (com.snc.cloud.core) installiert und aktiviert ist und dass Sie auf Release Orlando oder höher aktualisiert haben. Cloud Provisioning and Governance Core ist sowohl mit Discovery als auch mit dem Plugin „Cloud Provisioning and Governance Core“ verfügbar.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

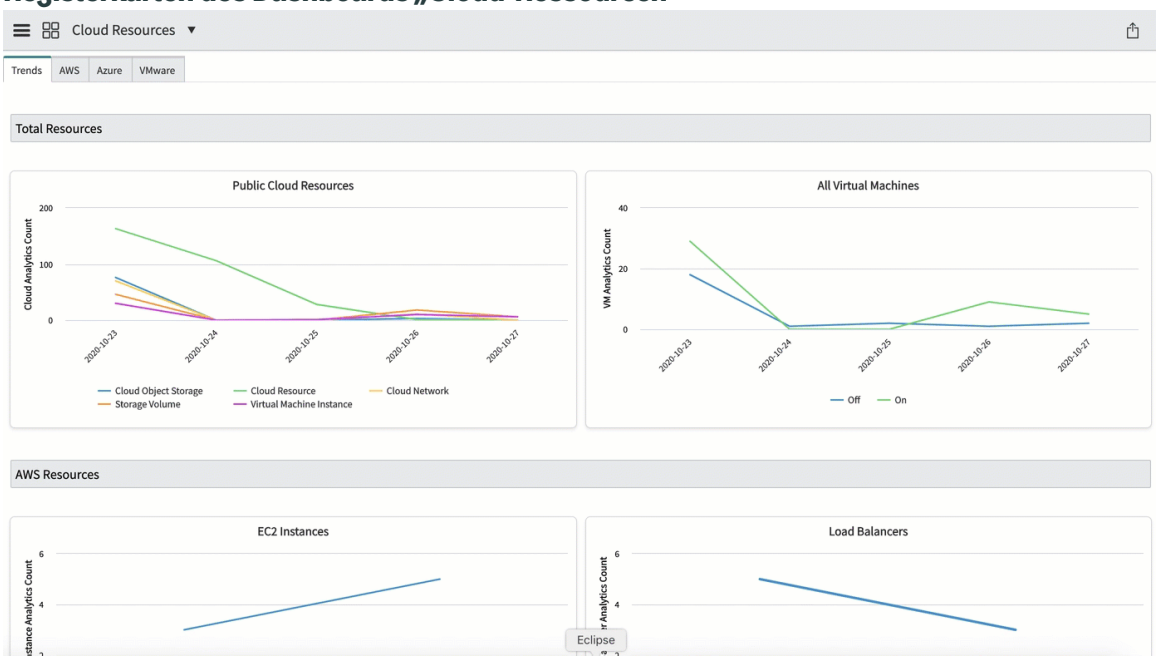
1. Navigieren zu **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**an.
2. Suchen Sie nach Performance Analytics Content Pack for Cloud Resources, und vergewissern Sie sich, dass Sie über die erforderlichen gültigen Berechtigungen verfügen.

   Sie benötigen ein HI-Konto und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen. HI-Konto und Instanz müssen zum selben Unternehmen gehören. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.
3. Installieren Sie die Anwendung Performance Analytics Content Pack for Cloud Resources.

Dashboard Cloud-Ressourcen

Im Dashboard „Cloud-Ressourcen“ werden neben der zusammengefassten Ansicht all Ihrer Cloud-Ressourcen kombinierte Analyseansichten, eine visuelle Zusammenfassung und Details aller Cloud-Ressourcen angezeigt.

Registerkarten des Dashboards „Cloud-Ressourcen“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Die Anwendungsfälle bieten Beispiele dafür, wie Benutzer in Ihrem Unternehmen dieses Dashboard verwenden könnten.

Anwender	Dashboard-Verwendung
Cloud-Benutzer	Discovery-Kunden haben mit Cloud-Discovery eine enorme Anzahl von CIs erkannt, die an einem zentralen Ort angezeigt werden können.
Cloud-Benutzer mit der Rolle sn_disco_cd.admin	Verwenden Sie die verfügbaren Analytics-Tabellen, um benutzerdefinierte Dashboards zu erstellen. Diese Tabellen sind spezifische Baseline-Datenbankansichten mit Ressourcen-Tags. Weitere Informationen finden Sie unter Dashboard „Cloud-Ressourcen“ anpassen.

Datenvisualisierungen

Titel	Typ	Quelltabelle
Cloud-Netzwerke	Liniendiagramm	VMware-Netzwerk-Analytics [sn_disco_cd_vmware_network_analytics]
Cloud-Netzwerke	Einzelne Punktzahl	VMware-Netzwerk-Analytics [sn_disco_cd_vmware_network_analytics]
Public Cloud-Ressourcen	Liniendiagramm	Cloud-Analytics [sn_disco_cd_analytics]
Cluster	Einzelne Punktzahl	Analytics für VMware-Cluster [sn_disco_cd_vmware_cluster_analytics]
Cluster	Liniendiagramm	Analytics für VMware-Cluster [sn_disco_cd_vmware_cluster_analytics]
Compute-Sicherheitsgruppen	Einzelne Punktzahl	Analytics für AWS-Sicherheitsgruppen [sn_disco_cd_aws_sec_group_analytics]
Datenbanken	Einzelne Punktzahl	Azure-Datenbank-Analytics [sn_disco_cd_azure_database_analytics]
Datenbanken	Liniendiagramm	Azure-Datenbank-Analytics [sn_disco_cd_azure_database_analytics]
Datenspeicher-Datenträger	Einzelne Punktzahl	Analytics für VMware-Datenspeicher-Datenträger [sn_disco_cd_vmware_ds_disk_analytics]
Datenspeicher	Einzelne Punktzahl	Analytics für VMware-Datenspeicher [sn_disco_cd_vmware_datastore_analytics]
Datenträger	Liniendiagramm	Analytics für Azure-Datenträger [sn_disco_cd_azure_disk_analytics]
Datenträger	Einzelne Punktzahl	Analytics für Azure-Datenträger [sn_disco_cd_azure_disk_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Verteilte virtuelle Portpruppen	Einzelne Punktzahl	Analytics für verteilte virtuelle VMware-Portgruppen [sn_disco_cd_vmware_dv_port_grp_analytics]
Verteilte virtuelle Switches	Einzelne Punktzahl	Analytics für verteilte virtuelle VMware-Switches [sn_disco_cd_vmware_dvs_analytics]
EC2-Instanzen	Einzelne Punktzahl	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
EC2-Instanzen	Liniendiagramm	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
EC2-Instanzen	Tortendiagramm	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
ESX-Server	Einzelne Punktzahl	ESX-Server-Analytics [sn_disco_cd_vmware_esx_analytics]
ESX-Server	Liniendiagramm	ESX-Server-Analytics [sn_disco_cd_vmware_esx_analytics]
Ordner	Einzelne Punktzahl	Analytics für vCenter-Ordner [sn_disco_cd_vmware_folder_analytics]
Funktionen	Einzelne Punktzahl	Azure-Funktionsanalysen [sn_Disco_cd_Azure_function_Analytics]
Generische Cloud-Ressourcen	Einzelne Punktzahl	Analytics für generische AWS-Cloud-Ressourcen [sn_disco_cd_aws_gen_resource_analytics]
Generische Cloud-Ressourcen	Liniendiagramm	Analytics für generische AWS-Cloud-Ressourcen [sn_disco_cd_aws_gen_resource_analytics]
Generische Cloud-Ressourcen	Einzelne Punktzahl	Analytics für generische Azure-Cloud-Ressourcen [sn_disco_cd_azure_gen_resource_analytics]
Bilder	Einzelne Punktzahl	Analytics für AWS-Images [sn_disco_cd_aws_image_analytics]
Bilder	Einzelne Punktzahl	Analytics für Azure-Images [sn_disco_cd_azure_image_analytics]
Lambdas	Einzelne Punktzahl	Analytics für AWS Lamda [sn_disco_cd_aws_lambda_analytics]
Lastenausgleichsmodule	Liniendiagramm	Analytics für AWS-Lastenausgleichsmodule [sn_disco_cd_aws_loadbalancer_analytics]
Lastenausgleichsmodule	Einzelne Punktzahl	Analytics für AWS-Lastenausgleichsmodule [sn_disco_cd_aws_loadbalancer_analytics]
Lastenausgleichsmodule	Einzelne Punktzahl	Analytics für Azure-Lastenausgleichsmodule [sn_disco_cd_azure_loadbalancer_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Lastenausgleichsmodule	Liniendiagramm	Analytics für Azure-Lastenausgleichsmodule [sn_disco_cd_azure_loadbalancer_analytics]
Netzwerkschnittstellen	Einzelne Punktzahl	Analytics für AWS-Netzwerkschnittstellen [sn_disco_cd_aws_nw_interface_analytics]
Netzwerkschnittstellen	Einzelne Punktzahl	Analytics für Azure-Netzwerkschnittstellen [sn_disco_cd_azure_nw_interface_analytics]
Netzwerksicherheitsgruppen	Einzelne Punktzahl	Analytics für Azure-Netzwerksicherheitsgruppen [sn_disco_cd_azure_nw_sec_group_analytics]
Relational Database Services (RDS)	Liniendiagramm	AWS RDS-Analytics [sn_disco_cd_aws_rds_analytics]
Relational Database Services (RDS)	Einzelne Punktzahl	AWS RDS-Analytics [sn_disco_cd_aws_rds_analytics]
S3-Buckets	Einzelne Punktzahl	Analytics für AWS S3-Buckets [sn_disco_cd_aws_s3_bucket_analytics]
Speicher-Laufwerke	Einzelne Punktzahl	Analytics für AWS-Speichervolumes [sn_disco_cd_aws_storage_volume_analytics]
Speicher-Laufwerke	Liniendiagramm	Analytics für AWS-Speichervolumes [sn_disco_cd_aws_storage_volume_analytics]
Virtuelle Maschinen	Liniendiagramm	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Einzelne Punktzahl	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Tortendiagramm	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Liniendiagramm	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Virtuelle Maschinen	Tortendiagramm	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Virtuelle Maschinen	Einzelne Punktzahl	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Alle virtuellen Computer	Liniendiagramm	VM-Analytics [sn_disco_cd_vm_analytics]
Virtuelle Netzwerke	Einzelne Punktzahl	Analytics für virtuelle Azure-Netzwerke [sn_disco_cd_azure_virtual_nw_analytics]
Virtual Private Clouds (VPC)	Liniendiagramm	AWS-VPC-Analytics [sn_disco_cd_aws_vpc_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Virtual Private Clouds (VPC)	Einzelne Punktzahl	AWS-VPC-Analytics [sn_disco_cd_aws_vpc_analytics]
VM-Vorlagen	Einzelne Punktzahl	Analytics für VMware-VM-Vorlagen [sn_disco_cd_vmware_vm_template_analytics]

Dashboard „Cloud-Ressourcen“ aufrufen

Um auf das Dashboard „Cloud-Ressourcen“ zuzugreifen, navigieren Sie zu **Discovery** > **Cloud-Ressourcen-Dashboard** oder **Cloud Provisioning and Governance** > **Cloud-Ressourcen-Dashboard**an.

Dashboard „Cloud-Ressourcen“ anpassen

Passen Sie das Dashboard auf jeder Cloud-Anbieter-Registerkarte an, indem Sie nach folgenden Attributen filtern:

- Servicekonto: Es werden alle Servicekonten aufgelistet, die für die ausgewählte Cloud-Anbieter-Registerkarte spezifisch sind.
- Rechenzentren: Die Rechenzentren werden basierend auf dem Cloud-Anbieter gefüllt.
- Ressourcengruppe: Mit diesem nur für Microsoft Azure gültigen Filter werden Objekte und Ressourcen auf die ausgewählte Ressourcengruppe beschränkt.

Verwenden Sie diese Datenbankansichten mit Ressourcen-Tags, um Ihr eigenes Dashboard zu erstellen.

AWS-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_aws_api_gateway_analytics_tags_db_view	Analytics für AWS API-Gateways mit Tags
sn_disco_cd_aws_ec2_instance_analytics_tags_db_view	Analytics für AWS EC2-Instanzen mit Tags
sn_disco_cd_aws_gen_resource_analytics_tags_db_view	Analytics für AWS Cloud-Ressourcen mit Tags
sn_disco_cd_aws_image_analytics_tags_db_view	Analytics für AWS-Images mit Tags
sn_disco_cd_aws_lambda_analytics_tags_db_view	AWS Lamda-Analytics mit Tags
sn_disco_cd_aws_loadbalancer_analytics_tags_db_view	Analytics für AWS-Lastenausgleichsmodule mit Tags
sn_disco_cd_aws_nw_interface_analytics_tags_db_view	Analytics für AWS NW-Schnittstellen mit Tags
sn_disco_cd_aws_rds_analytics_tags_db_view	AWS RDS-Analytics mit Tags
sn_disco_cd_aws_s3_bucket_analytics_tags_db_view	Analytics für AWS S3-Bucket mit Tags
sn_disco_cd_aws_sec_group_analytics_tags_db_view	Analytics für AWS-Sicherheitsgruppen mit Tags
sn_disco_cd_aws_storage_volume_analytics_tags_db_view	Analytics für AWS-Speichervolumes mit Tags
sn_disco_cd_aws_vpc_analytics_tags_db_view	AWS VPC-Analytics mit Tags
sn_disco_cd_aws_zone_analytics_tags_db_view	Analytics für AWS-Zonen mit Tags

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_azure_database_analytics_tags_db_view	Analytics für Azure-Datenbanken mit Tags
sn_disco_cd_azure_disk_analytics_tags_db_view	Analytics für Azure-Datenträger mit Tags
sn_disco_cd_azure_function_analytics_tags_db_view	Analytics für Azure-Funktionen mit Tags
sn_disco_cd_azure_gen_resource_analytics_tags_db_view	Analytics für Azure-Cloud-Ressourcen mit Tags
sn_disco_cd_azure_image_analytics_tags_db_view	Analytics für Azure-Images mit Tags
sn_disco_cd_azure_loadbalancer_analytics_tags_db_view	Analytics für Azure-Lastenausgleichsmodule mit Tags
sn_disco_cd_azure_nw_interface_analytics_tags_db_view	Analytics für Azure NW-Schnittstellen mit Tags
sn_disco_cd_azure_nw_sec_group_analytics_tags_db_view	Analytics für Azure-Sicherheitsgruppen mit Tags
sn_disco_cd_azure_virtual_nw_analytics_tags_db_view	Analytics für Azure Virtual NW mit Tags
sn_disco_cd_azure_vm_analytics_tags_db_view	Analytics für Azure-VMs mit Tags
sn_disco_cd_azure_zone_analytics_tags_db_view	Analytics für Azure-Zonen mit Tags

VMware-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_vmware_cluster_analytics_tags_db_view	Analytics für VMware-Cluster mit Tags
sn_disco_cd_vmware_datastore_analytics_tags_db_view	Analytics für VMware-Datenspeicher mit Tags
sn_disco_cd_vmware_ds_disk_analytics_tags_db_view	Analytics für VMware-Datenspeicher-Datenträger mit Tags
sn_disco_cd_vmware_dvs_analytics_tags_db_view	Analytics für VMware DVS mit Tags
sn_disco_cd_vmware_dv_port_grp_analytics_tags_db_view	Analytics für VMware DV-Portgruppen mit Tags
sn_disco_cd_vmware_esx_analytics_tags_db_view	VMware ESX-Analytics mit Tags
sn_disco_cd_vmware_folder_analytics_tags_db_view	Analytics für VMware-Ordner mit Tags
sn_disco_cd_vmware_network_analytics_tags_db_view	Analytics für VMware-Netzwerke mit Tags
sn_disco_cd_vmware_vm_analytics_tags_db_view	Analytics für VMware-VMs mit Tags
sn_disco_cd_vmware_vm_template_analytics_tags_db_view	Analytics für VMware-VM-Vorlagen mit Tags

Die folgenden Ressourcen, die für GCP unterstützt werden, werden von GCPResourcePopulateScheduledJob gefüllt.

Google Cloud Platform (GCP)-Analytics-Tabellen und ihre entsprechenden CI-Ressourcentabellen (Configuration Item) in der Configuration Management Database (CMDB)

Analytics-Tabelle	CMDB-CI-Ressourcen
Analytics für GCP-VMs [sn_disco_cd_gcp_database_analytics]	VM-Instanz [cmdb_ci_vm_instance]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Google Cloud Platform (GCP)-Analytics-Tabellen und ihre entsprechenden CI-Ressourcentabellen (Configuration Item) in der Configuration Management Database (CMDB) (Fortsetzung)

Analytics-Tabelle	CMDB-CI-Ressourcen
Analytics für GCP-Speichervolumes [sn_disco_cd_gcp_storage_volume_analytics]	Speichervolume [cmdb_ci_storage_volume]
Analytics für GCP-Datenbanken [sn_disco_cd_gcp_database_analytics]	Cloud-Datenbank [cmdb_ci_cloud_database]
Analytics für virtuelle GCP-Netzwerke [sn_disco_cd_gcp_virtual_nw_analytics]	Cloud-Netzwerk [cmdb_ci_network]
Analytics für GCP-Lastenausgleichsmodule [sn_disco_cd_gcp_loadbalancer_analytics]	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Analytics für GCP-Images [sn_disco_cd_gcp_image_analytics]	Cloud-Betriebssystem-Images [cmdb_ci_cloud_os_images]
Analytics für generische GCP-Cloud-Ressourcen [sn_disco_cd_gcp_gen_resource_analytics]	Cloud-Ressource [cmdb_ci_cmp_resource]
Analytics für GCP-Netzwerkschnittstellen [sn_disco_cd_gcp_nw_interface_analytics]	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Regelmäßige Aufgaben

Regelmäßige Aufgaben installiert

Auftrag	Beschreibung
GCPResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die GCP-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
AWSResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die AWS-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
AzureResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die Microsoft Azure-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
VMwareResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die VMware-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.

Da für jeden Cloud-Provider alle 30 Minuten eine separate regelmäßige Aufgabe ausgelöst wird, können Sie überprüfen, ob die letzte Aufgabe erfolgreich war. Wenn die geplante Aufgabe nicht erfolgreich war, können Sie die Aufgabe manuell auslösen, indem Sie zu wechseln **Systemdefinition** > **Geplante Aufgaben**an. Wählen Sie die Aufgabe für den betreffenden Cloud-Anbieter aus, und klicken Sie auf **Jetzt ausführen**.

Im Rahmen der alle 30 Minuten stattfindenden Aktualisierungsaufgaben werden Analytics-Tabellen mit Daten gefüllt, und das Datum wird aktualisiert. Sie können diese Häufigkeit steigern, um häufiger aktualisierte Daten zu erhalten.

In folgenden Fällen ist eine Synchronisierung erforderlich:

- Der Ressourcenstatus wurde von **Installiert** auf einen anderen Status (z. B. „Deaktiviert“ oder „Abgebrochen“) aktualisiert.
- Vor Kurzem wurden neue Ressourcen erkannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In folgenden Fällen ist keine Synchronisierung erforderlich:

- Es wurden keine Ressourcen aktualisiert.
- Es sind neue Ressourcen vorhanden, die noch nicht erkannt wurden.

Wichtiger Hinweis:

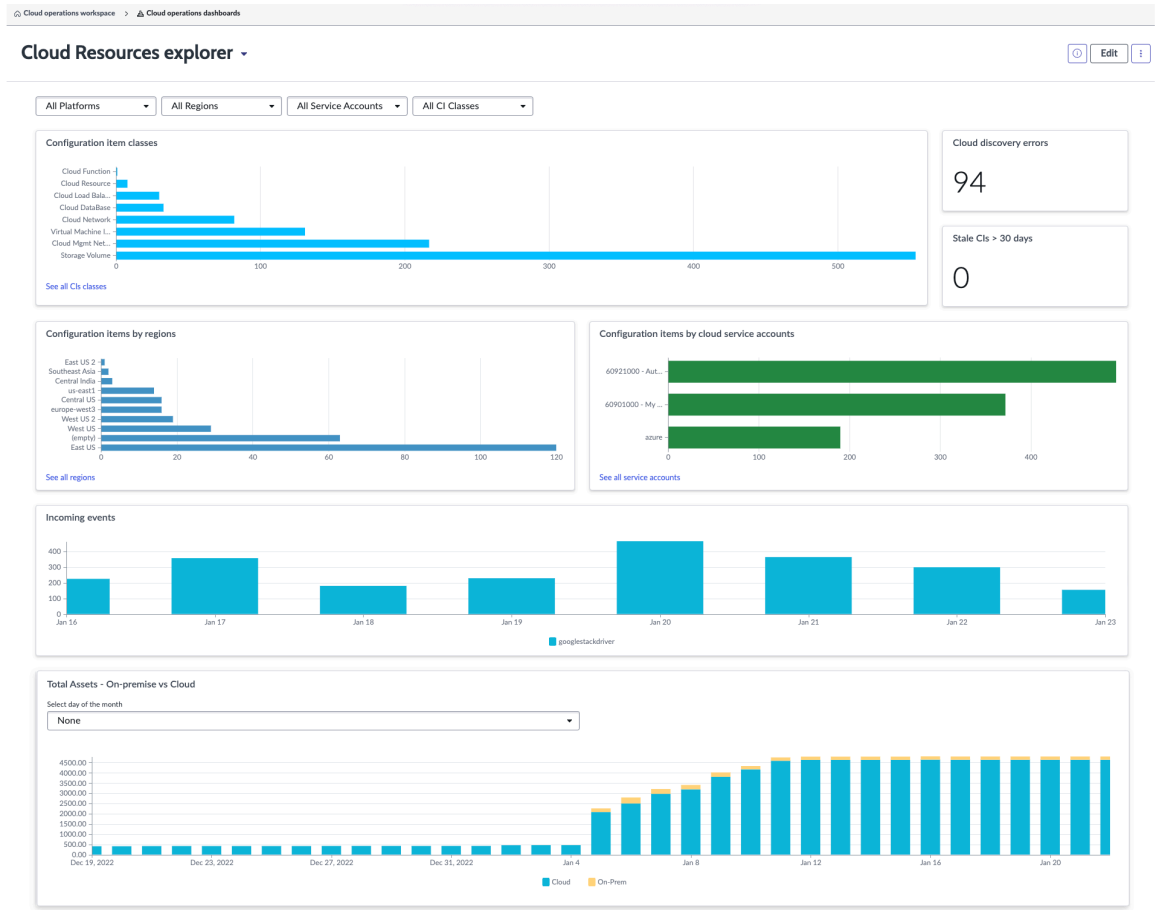
- Es kann jeweils nur eine Aufgabe ausgeführt werden. Wenn beispielsweise bei der Aufgabenausführung bereits eine AWS-Aufgabe ausgeführt wird, können Sie keine weitere AWS-Aufgabe auslösen.
- Wenn die Felder „LRZ“ (logisches Rechenzentrum) und „Servicekonto“ einer CI-Ressource leer sind, kann die Ressource in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] keinem LRZ zugeordnet werden, oder die Ressource ist eine generische Cloud-Ressource vom Typ IAM, und die Felder sind leer.
- Nur die Ressourcen, deren Installationsstatus auf „Installiert“ festgelegt ist, werden gezählt und in den Widgets des Dashboards „Cloudressourcen“ dargestellt.
- Wenn nach Ausführung der regelmäßigen Aufgabe eine neue Ressource erkannt wird, werden von der nächsten regelmäßigen Aufgabe die Ressourcendetails in den Analytics-Tabellen hinzugefügt.
- Wenn eine Aufgabe in der Tabelle „Cloud-Dashboard-Aufgabenstatus“ [sn_disco_cd_cloud_dashboard_job_status] als fehlgeschlagen markiert wird, ist der Grund des Fehlers in den Systemprotokollen verzeichnet. Filtern Sie die Systemprotokolltabelle nach der sys_id der Aufgabe, um die Fehlermeldung abzurufen.
- Wenn IP-basierte Discovery zur vCenter-Erkennung verwendet wird, bleibt das Feld „Servicekonto“ der VMware-Ressource leer.
- Systemadministrator dürfen die Datensätze nicht aus der Analytics-Tabelle löschen, da Datensätze, die aus der Analytics-Tabelle gelöscht wurden, von der regelmäßigen Aufgabe nicht erneut gefüllt werden. Das Löschen von Datensätzen führt zu Dateninkonsistenzen in der Analytics-Tabelle.
- Um eine vollständige Aktualisierung der VMware-Datensätze (einschließlich der Servicekonten) nach Änderung des Mechanismus zur Erkennung von VMware-Ressourcen sicherzustellen, löschen Sie die VMware-Datensätze aus der Tabelle „Cloud-Dashboard-Auftragsstatus“ [sn_disco_cd_cloud_dashboard_job_status], und führen Sie die regelmäßige Aufgabe aus. In der Tabelle „Cloud-Dashboard-Auftragsstatus“ ist das Provider-Feld aller VMware-Ressourcen auf *`vmware`* festgelegt. Sie können entweder die IP-basierte vCenter-Erkennung oder die vCenter-Servicekonto-Erkennung verwenden, um die VMware-Ressourcen zu erkennen.

Cloud-Ressourcenbestand

Verwenden Sie ServiceNow® Cloud-Ressourcenbestand, um die Verteilung der Ressourcen in Ihrer Multi-Cloud-Umgebung zu filtern und zu visualisieren. Erhalten Sie Einblicke in Betriebsinformationen wie veraltete Ressourcen und Zuflussraten von Cloud-Ereignissen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressourcenbestand



Der Cloud-Ressourcenbestand bietet Unterstützung für folgende Cloud-Anbieter:

- Amazon Web Services.
- Microsoft Azure Public Clouds.
- VMware vCenter.
- Google Cloud Platform (GCP) (Unterstützt mit Performance Analytics Content Pack for Cloud Resources, Version 1.2.1 und höher).

Erforderliche ServiceNow AI Platform-Rollen

Die Rolle sn_Cloud_OPS_WS.Cloud_OPS_admin ist erforderlich, um anzuzeigen Cloud-Ressourcenbestand.

Auf Cloud-Ressourcenbestand zugreifen

Um zu öffnen Cloud-Ressourcenbestand, Navigieren Sie zu **Alle** > **Cloud-Discovery-Arbeitsbereich** > **Cloud-Ressourcen-Explorer**an.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Erhalten Sie Einblicke in die Anzahl der Bestände von Cloud-Ressourcen und die aktuelle Größe der Configuration Management Database (CMDB) und darüber, wie viele Objekte sich im Geltungsbereich befinden. • Erhalten Sie Einblicke in fehlerbezogene Informationen wie Cloud-Discovery-Fehler. • Erhalten Sie Einblicke in Betriebsinformationen wie die Zufluss- und die Verarbeitungsrate des Ereignisses. • Erhalten Sie Einblicke in die Integrität der CMDB. • Erhalten Sie Einblicke in die Verteilung von Ressourcen in der lokalen Cloud und in Public Clouds.

Indikatoren

Cloud-Discovery-Fehler

Cloud-Discovery-Fehler insgesamt, die im Laufe der Zeit aufgetreten sind.

Veraltete CIs > 30 Tage

Wenn ein CI in den letzten 30 Tagen nicht aktualisiert wurde, gilt es als veraltetes CI.

Ein veraltetes CI gibt an, dass das CI in der Configuration Management Database (CMDB), aber möglicherweise nicht im Rechenzentrum vorhanden ist. Das Identifizieren der veralteten CIs ist wichtig für die Aufrechterhaltung der Integrität der CMDB.

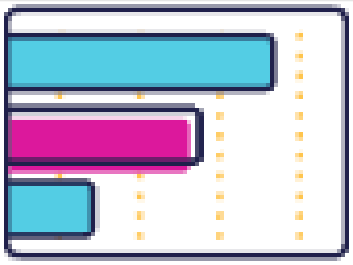
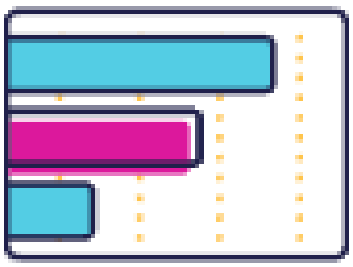
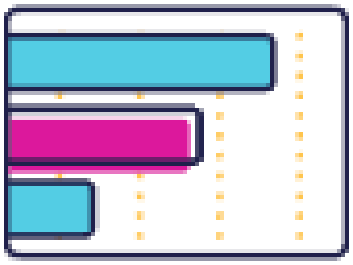
Hier sind einige der Szenarien aufgeführt, die dazu führen, dass veraltete CIs entstehen:

- Die Cloud-Ressource ist nicht vorhanden, ihre Löschung wird jedoch nicht in der CMDB aktualisiert.
- Das Gerät befindet sich möglicherweise noch im Netzwerk, aber im Rahmen der automatisierten Erkennung kann keine Verbindung zum Gerät hergestellt werden, damit es erneut erkannt werden kann.
- Das Gerät ist im Netzwerk vorhanden, und es kann darauf zugegriffen werden, aber es wird im Identifizierungsprozess nicht eindeutig erkannt. Daher wurde von Cloud-Discovery ein doppeltes CI in der CMDB erstellt.

Datenvisualisierungen

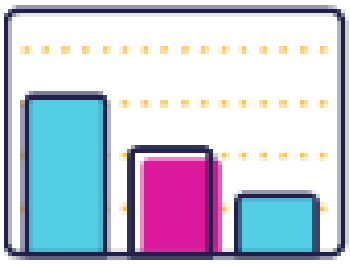
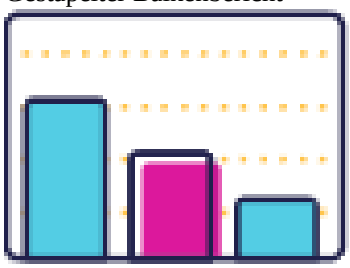
Titel	Typ	Quelltabelle	Beschreibur
Konfigurationselementsklassen	Bericht mit horizontalen Balken	Cloud-Analytics [sn_disco_cd_analytics]	In diesem Be 10 wichtigste die im Zeitve

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibur
			Sie können Berichtsein aus dem Be „Konfigura auswählen, Analysenta auf der der basiert. We bestimmter ausgewählt die Analyse bestimmter Andernfalls übergeordn für diesen Wenn Sie i Ressourcen „Google“ au im Bericht „Speicherv erscheint d Analysenta „Google-Spe Wenn Sie i alle Plattf im Bericht „Speicherv wird die üb Analysenta „Speicherv
Konfigurationselemente nach Regionen	Bericht mit horizontalen Balken 	Cloud-Analytics [sn_disco_cd_analytics]	In diesem Be der CIs pro R angezeigt.
Konfigurationselemente nach Cloud-Servicekonten	Bericht mit horizontalen Balken 	Cloud-Analytics [sn_disco_cd_analytics]	In diesem Be wichtigsten S maximalen A angezeigt.

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibur
Eingehende Events	Balkenbericht 	Cloud-Ereignis [sn_cmp_cloud_event]	In diesem B Trend der i empfangen Ressourcer angezeigt. Um die List einem best empfangen Ereignisse Sie den ent Berichtsein
Lokale Cloud-Ressourcen im Vergleich zu öffentlichen Cloud-Ressourcen insgesamt	Gestapelter Balkenbericht 	Tägliche Ressourcenanzahl nach Anbietern [sn_disco_cd_daily_resource_cnt_by_provider]	In diesem Be Anzahl der R Unternehmen lokale Cloud verteilt sind. Verwenden um die Nut Cloud und virtuellen C Zeitverlauf In diesem B Cloud als lo

Um die Tabelle „Cloud Analytics“ [sn_Disco_cd_Analytics] auszufüllen, die Cloud-Ressourcenbestand Verwendet denselben Satz geplanter Aufgaben wie Performance Analytics Inhaltspaket für Cloud-Ressourcen. Weitere Informationen zu den geplanten Aufgaben finden Sie unter Dashboard „Cloud-Ressourcen“ .

Zum Anzeigen der Details der Betriebssystem-Images, die in den AWS-, Microsoft Azure- und GCP-Clouds erkannt werden, muss die Store-App Discovery and Service-Mapping Patterns, Version 1.0.87 oder höher, in der Instanz installiert sein. Außerdem muss die Eigenschaft *sn_cmdb_ci_class.use_single_cloud_os_image* auf true festgelegt werden.

Filter

Name	Typ	Beschreibung
Cloud-Ressourcenfilter	Auswahlbasierter Filter	Verwenden Sie den Cloud-Ressourcenfilter, um die gewünschten Cloud-Ressourcendaten auszuwählen und zu visualisieren. Standardmäßig werden im Cloud-Ressourcenbestand Daten für alle Cloud-Ressourcen der Cloud-Anbieter Ihrer Organisation angezeigt. Allerdings werden im Cloud-Ressourcenfilter nur die Cloud-Anbieter angezeigt, die Sie auf der Auswahlseite für Cloud-Anbieter der App Cloud Operations Workspace ausgewählt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
		Sie haben die Wahl zwischen den folgenden überlappenden Filtern: • Plattform: Wählen Sie den Cloud-Anbieter mit den Ressourcendaten aus, die Sie visualisieren möchten. • Region: Wählen Sie die Region oder das Rechenzentrum mit den Ressourcendaten aus, die Sie visualisieren möchten. • Service-Account: Wählen Sie den Serviceaccount mit den Ressourcendaten aus, die Sie visualisieren möchten. • CI-Klasse: Wählen Sie die CI-Klasse mit den Ressourcendaten aus, die Sie visualisieren möchten. • Ressourcengruppe: Wählen Sie die Ressourcengruppe mit den Ressourcendaten aus, die Sie visualisieren möchten. Dieses Feld ist nur verfügbar, wenn in der Dropdown-Liste „Plattform“ Azure ausgewählt ist. Sie können den Bericht „Eingehende Ereignisse“ nur basierend auf dem Plattformfilter filtern. Die im Cloud-Discovery-Fehlerindikator angezeigten Daten sind nicht von den im Cloud-Ressourcenfilter ausgewählten Kriterien betroffen.
Tagesnavigator	Auswahlbasierter Filter	Verwenden Sie den Tagesnavigator, um den Bericht „Lokale Cloud-Ressourcen im Vergleich zu öffentlichen Cloud-Ressourcen insgesamt“ in die folgenden Dimensionen zu segmentieren: • Keine: Der Bericht zeigt die im letzten Jahr gesammelten Daten an, falls verfügbar. • Erster Tag des Monats: Der Bericht zeigt die Verlaufsdaten an, die für den ersten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar. • Mitte des Monats: Der Bericht zeigt die Verlaufsdaten an, die für die Monatsmitte des letzten Jahres gesammelt wurden, falls verfügbar. • Letzter Tag des Monats: Der Bericht zeigt die Verlaufsdaten an, die für den letzten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar. • Datum des Monats auswählen: Der Bericht zeigt die Verlaufsdaten an, die für den ausgewählten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar.

Vergleich von Cloud-Discovery-Lösungen

Der Vergleich von Cloud-Discovery-Lösungen bietet Einblicke in die relativen Stärken jeder Lösung. Der Vergleich zeigt die Anzahl der Ressourcentypen, die von den Lösungen unterstützt werden AWS, Azure, Und GCP. Der Vergleich kann Ihnen helfen, die Fähigkeiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

jeder Lösung zu verstehen und besser zu verwalten CMDB Bei Verwendung einer oder mehrerer Methoden.

Muster für Discovery und Service-Mapping Vs. Service Graph Connectors

ITOM-Transparenz Bietet zwei primäre Lösungen zum Erkennen von Cloud-Ressourcen und zum Zuordnen dieser Ressourcen an Configuration Management Database (CMDB): Cloud Muster für Discovery und Service-Mapping Und Cloud Service Graph Connectors.

Muster sind der Kern von ITOM Native Discovery-Fähigkeiten von Transparenz. Sie bieten eine tiefere, dynamischere und ganzheitlichere Ansicht Ihrer Infrastruktur. Muster verwenden eine Vielzahl von Discovery-Methoden: Agentenlos, Agent-basiert und Cloud-nativ, um eine einheitliche, geschäftsorientierte Ansicht Ihrer Services zu erstellen. Durch die Nutzung von maschinellem Lernen ordnen Muster technische Komponenten automatisch ihrem Geschäftskontext zu, wodurch umfassende Beziehungen und ein umfassendes Wissensdiagramm erstellt werden.

Service Graph Connectors hingegen bietet schnelle Point-in-Time-Daten, die aus vorhandenen Systemen erfasst werden. Sie helfen Ihnen, schnell Daten aus bestimmten Quellen wie Public Cloud-Anbietern (zu erfassen AWS, Azure, GCP), Endpunktverwaltungssysteme und Sicherheits- oder Netzwerktools.

Während Service Graph Connectors einen schnellen Datenimport bietet, bieten Muster die Grundlage für laufende, automatisierte Service-Mapping und tiefere operative Einblicke basierend auf regelmäßigen Updates von ServiceNow Store. Dieser Unterschied ist entscheidend für die Lösung komplexer Herausforderungen wie Zertifikatverwaltung, Firewall-Auditing und einer Vielzahl anderer Service- und Betriebsanwendungsfälle.

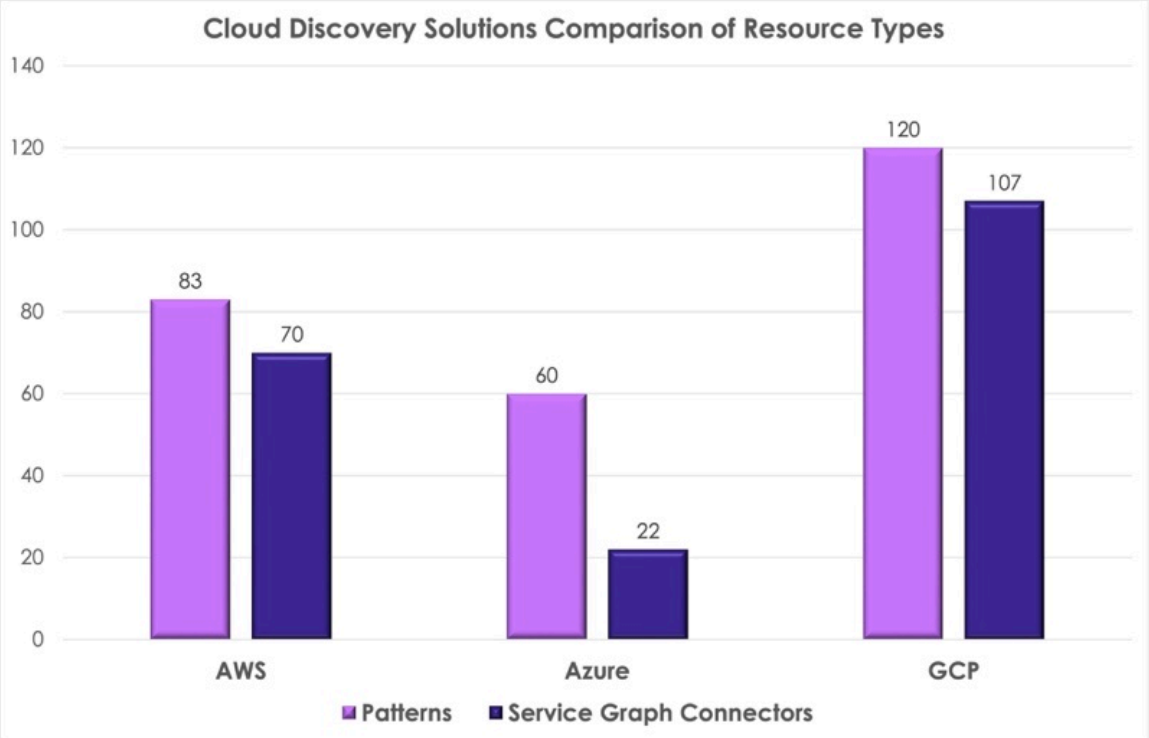
Die Auswahl zwischen Mustern und Connectors wirkt sich auf die Abdeckung, den Detailgrad und die Art und Weise aus, wie Daten in modelliert werden CMDB Und die Häufigkeit der Aktualisierung. Einige Ressourcentypen werden von beiden Lösungen unterstützt, die Daten können jedoch unterschiedlich ausgefüllt werden CMDB CI-Klassen. Das Verständnis dieser Unterschiede hilft Ihnen, eine konsistente und effektive Discovery-Strategie zu planen.

Indem Sie die Abdeckungstabellen für überprüfen AWS, Azure, Und GCP, Können Sie

- Identifizieren Sie, welche Ressourcen von Mustern, Connectors oder beidem unterstützt werden.
- Verstehen Sie, wie derselbe Ressourcentyp unterschiedlich behandelt werden kann (Muster können beispielsweise alle Zonendaten einbeziehen, während Connectors nur Zonen einbeziehen, die an eine Instanz gebunden sind).
- Entscheiden Sie sich für eine Lösung pro Anbieter unter Berücksichtigung der CI-Abdeckung oder des Datenmodells. Beispiel: Verwenden Sie Connectors, um Ihren zu erkennen GCP Ressourcen, aber verwenden Sie Muster für AWS Und Azure.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Und Service Graph Connectors-Vergleich



AWS Discovery-Lösungsvergleich

ITOM-Transparenz Anwendungen erkennen eine Vielzahl von AWS Ressourcen, und füllen Sie die relevanten Konfigurationselementklassen (Configuration Item, CI) in aus Configuration Management Database (CMDB) Mit ihren Attributen.

ITOM-Transparenz Lösungen

ITOM-Transparenz Kann Ihnen einen umfassenden Einblick in die Cloud-Infrastruktur Ihrer Organisation bieten. Jede Anwendung bietet einzigartige Stärken und Fähigkeiten, und durch den Vergleich erhalten Sie ganzheitliche Einblicke in ihre Fähigkeiten und Vorteile.

ITOM-Transparenz Lösungen für die Erkennung AWS

Die Lösung ITOM-Transparenz	Übersicht	Konfiguration
Muster für Discovery und Service-Mapping und Visibility Content	Von ITOM-Transparenz verwendete Erkennungsmuster	• Sie müssen Ihre Store-Apps auf die neueste Release-Version aktualisieren. • Sie müssen angeben ITOM-Transparenz Mit Zugriffsberechtigungen. Weitere Informationen finden Sie unter Wird eingerichtet AWS Service-Accounts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM-Transparenz Lösungen für die Erkennung AWS (Fortsetzung)

Die Lösung ITOM-Transparenz	Übersicht	Konfiguration
Service Graph Connector für AWS	Service Graph Connector für AWS	Konfigurieren Service Graph Connector für AWSMit dem geführten Setup

Hinweis:

Die CI-Klasse gilt in den meisten Fällen für beide Lösungen. Wenn dies nicht für eine der Lösungen gilt, wird die Lösung als „N/V“ markiert.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für AWS

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
AWS::AppSync::API	Ja	Nein	cmdb_aws_appsync_api
AWS::Athena::Workgroup	Ja	Nein	cmdb_aws_athena_Workgroup
AWS::Backup::BackupPlan	Ja	Nein	cmdb_aws_Backup_Backup_Plan
AWS::Sicherung::BackupVault	Ja	Nein	cmdb_aws_Backup_Backup_Vault
AWS::CloudFront::Distribution	Ja	N/V	cmdb_aws_cloudfront_Distribution
AWS::CloudFront::Distribution	N/V	Ja	cmdb_ci_cmp_resource
AWS::CloudWatch::Log	Ja	Nein	cmdb_aws_cloudwatch_log
AWS::CodeDeployment::Bereitstellung	Ja	Nein	cmdb_aws_codedeploy_Deployment
AWS::CodePipeline::Pipeline	Ja	N/V	cmdb_aws_codepipeline_Pipeline
AWS::CodePipeline::Pipeline	N/V	Ja	cmdb_ci_cmp_resource
AWS::DMS::Endpunkt	Ja	Nein	cmdb_aws_dms_Endpoint
AWS::ElasticBeanstalk::Application	Ja	N/V	cmdb_aws_Elastic_beanstalk_Application
AWS::ElasticBeanstalk::Application	N/V	Ja	cmdb_ci_cmp_resource
AWS::EMR::Cluster	Ja	Nein	cmdb_aws_emr_Cluster
AWS::EventBridge::EventBus	Ja	Nein	cmdb_aws_eventbridge_event_Bus
AWS::FSX::Sicherung	Ja	Nein	cmdb_aws_fsx_Backup
AWS::FSX::filesystem	Ja	Nein	cmdb_aws_fsx_FILE_System
AWS::Glue::Database	Ja	Nein	cmdb_aws_Glue_database
AWS::IAM::Richtlinie	Ja	N/V	cmdb_aws_iam_Policy
AWS::IAM::Richtlinie	N/V	Ja	cmdb_ci_cmp_resource
AWS::IAM::role	Ja	N/V	cmdb_aws_iam_role
AWS::IAM::role	N/V	Ja	cmdb_ci_cmp_resource
AWS::IAM::Anwender	Ja	N/V	cmdb_aws_iam_user

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für AWS (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
AWS::IAM::Anwender	N/V	Ja	cmdb_ci_cmp_resource
AWS::KMS::Key	Ja	Nein	cmdb_aws_KMS_key
AWS::MQ::Broker	Ja	Nein	cmdb_aws_mq_Broker
AWS::MQ::Configuration	Ja	Nein	cmdb_aws_mq_Configuration
AWS::S3::GlacierVault	Ja	Nein	cmdb_aws_s3_Glacier_Vault
AWS::SageMaker::NotebookInstance	Ja	Nein	cmdb_aws_sagemaker_Notebook_instance
AWS::SecretsManager::Secret	Ja	Nein	cmdb_aws_Secrets_Manager_Secret
AWS::SimpleEmailService::Identity	Ja	Nein	cmdb_aws_simple_email_Service_Identity
AWS::SQS::Warteschlange	Ja	Nein	cmdb_aws_sqs_Queue
AWS::StepFunctions::StateMachine	Ja	Nein	cmdb_aws_STEP_Functions_State_Machine
AWS::StorageGateway::Gateway	Ja	Nein	cmdb_aws_Storage_Gateway_Gateway
AWS::SystemsManager::Document	Ja	Nein	cmdb_aws_Systems_Manager_document
AWS::SystemsManager::ParameterStore	Ja	Nein	cmdb_aws_Systems_Manager_Parameter_St
AWS::TransferFamily::Server	Ja	Nein	cmdb_aws_Transfer_Family_Server
AWS::VPC::FlowLog	Ja	Nein	cmdb_aws_vpc_Flow_log
AWS::VPC::ManagedPrefixList	Ja	Nein	cmdb_aws_vpc_Managed_prefix_list
AWS::XRay::SamplingRule	Ja	Nein	cmdb_aws_xray_Sampling_rule
ec2: DescribeAvailabilityZones	Ja	Ja	cmdb_ci_availability_zone
ec2: DescribeRegions	Ja	Ja	cmdb_ci_aws_datacenter
AWS::Kinesis::Stream	Ja	Nein	cmdb_ci_aws_Kinesis_Data
AWS::KinesisAnalytics	Ja	Nein	cmdb_ci_aws_Kinesis_Data_Analytics
AWS::KinesisFirehose	Ja	Nein	cmdb_ci_aws_Kinesis_Firehose
AWS::KinesisVideo	Ja	Nein	cmdb_ci_aws_Kinesis_Video
AWS::Redshift::Cluster	Ja	N/V	cmdb_ci_aws_Redshift
AWS::Redshift::Cluster	N/V	Ja	cmdb_ci_cmp_resource
AWS::CertificateManager::Certificate	Ja	Nein	cmdb_ci_certificate
AWS::Cognito::UserPool	Ja	Nein	cmdb_ci_Cloud_Authentication
AWS::RDS::DBInstance	Ja	Ja	cmdb_ci_cloud_database
AWS::ECS::Cluster	Ja	Nein	cmdb_ci_Cloud_ecs_Cluster
AWS::ECS::Service	Ja	Nein	cmdb_ci_Cloud_ecs_Service
AWS::ECS::Aufgabendefinition	Ja	Nein	cmdb_ci_Cloud_ecs_Task_Definition

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für AWS (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
AWS::Lambda::function	Ja	Ja	cmdb_ci_cloud_function
AWS::ApiGateway::RestApi	Ja	Ja	cmdb_ci_cloud_gateway
ec2: DescribeInstanceTypes	Ja	Ja	cmdb_ci_Cloud_Hardware_type
AWS::EC2::Host	Ja	Nein	cmdb_ci_cloud_host
AWS::EC2::Schlüsselpaar	Ja	Nein	cmdb_ci_cloud_key_pair
AWS::ElasticLoadBalancingV2::LoadBalancer	Ja	Ja	cmdb_ci_cloud_load_balancer
Amazon::S3::Bucket	Ja	Ja	cmdb_ci_cloud_object_storage
Organisationen	Ja	Ja	cmdb_ci_Cloud_org oder cmdb_ci_Cloud_Service_Account
Organisationen::AWS-Accounts	Ja	Ja	cmdb_ci_cloud_service_account
AWS::EC2::Subnet	Ja	Ja	cmdb_ci_cloud_subnet
AWS SSM-Agents	Ja	Nein	cmdb_ci_Cloud_System_Management_Agent
AWS::EC2::Subnet	Ja	Nein	cmdb_ci_cloud_subnet
AWS::WAF::WebACL	N/V	Ja	cmdb_ci_cmp_resource
AWS::WAFRegional::WebACL	N/V	Ja	cmdb_ci_cmp_resource
AWS::ACM::Zertifikat	N/V	Ja	cmdb_ci_cmp_resource
AWS::Redshift::EventSubscription	N/V	Ja	cmdb_ci_cmp_resource
AWS::RDS::DBSnapshot	N/V	Ja	cmdb_ci_cmp_resource
AWS::Redshift::ClusterParameterGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::Automatische Skalierung::Startkonfiguration	N/V	Ja	cmdb_ci_cmp_resource
AWS::Redshift::ClusterSnapshot	N/V	Ja	cmdb_ci_cmp_resource
AWS::CloudFormation::Stack	N/V	Ja	cmdb_ci_cmp_resource
AWS::CodeBuild::Project	N/V	Ja	cmdb_ci_cmp_resource
AWS::ElasticBeanstalk::ApplicationVersion	N/V	Ja	cmdb_ci_cmp_resource
AWS::Redshift::ClusterSecurityGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::CloudTrail::Trail	N/V	Ja	cmdb_ci_cmp_resource
AWS::CloudFront::StreamingDistribution	N/V	Ja	cmdb_ci_cmp_resource
AWS::WAF::RuleGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::RDS::DBSecurityGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::RDS::EventSubscription	N/V	Ja	cmdb_ci_cmp_resource

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für AWS (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
AWS::WAF::Rule	N/V	Ja	cmdb_ci_cmp_resource
AWS::Automatische Skalierung::ScheduledAction	N/V	Ja	cmdb_ci_cmp_resource
AWS::ElasticBeanstalk::Environment	N/V	Ja	cmdb_ci_cmp_resource
AWS::Automatische Skalierung::ScalingPolicy	N/V	Ja	cmdb_ci_cmp_resource
AWS::Shield::Protection	N/V	Ja	cmdb_ci_cmp_resource
AWS::CloudWatch::Alarm	N/V	Ja	cmdb_ci_cmp_resource
AWS::XRay::EncryptionConfig	N/V	Ja	cmdb_ci_cmp_resource
AWS::ShieldRegional::Protection	N/V	Ja	cmdb_ci_cmp_resource
AWS::Redshift::ClusterSubnetGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::IAM::Group	N/V	Ja	cmdb_ci_cmp_resource
AWS::WAFRegional::RateBasedRule	N/V	Ja	cmdb_ci_cmp_resource
AWS::WAFRegional::RuleGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::WAF::RateBasedRule	N/V	Ja	cmdb_ci_cmp_resource
AWS::RDS::DBSubnetGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::SSM::AssociationCompliance	N/V	Ja	cmdb_ci_cmp_resource
AWS::EC2::SecurityGroup	Ja	Ja	cmdb_ci_compute_security_group
ec2: DescribeInstanceTypes	Ja	Ja	cmdb_ci_compute_template
AWS::ECR::Repository	Ja	Nein	cmdb_ci_Container_Repository
AWS::EC2::CustomerGateway	Ja	Nein	cmdb_ci_Customer_Gateway
Docker-Container	Ja	Ja	cmdb_ci_docker_container
ecr: DescribeImages	Ja	Nein	cmdb_ci_docker_image
AWS::DynamoDB::GlobalTable	Ja	Ja	cmdb_ci_dynamodb_table
AWS::AutoScaling::AutoScalingGroup	Ja	N/V	cmdb_ci_instance_Scale_Set
AWS::AutoScaling::AutoScalingGroup	N/V	Ja	cmdb_ci_cmp_resource
AWS::EC2::InternetGateway	Ja	Nein	cmdb_ci_Internet_Gateway
AWS::EKS::Cluster	Ja	Ja	cmdb_ci_kubernetes_cluster
WS::ElasticLoadBalancingV2::TargetGroup	Ja	Nein	cmdb_ci_lb_pool
AWS::ElasticLoadBalancingV2::TargetGroup TargetDescription	Ja	Nein	cmdb_ci_lb_pool_member
AWS::ElasticLoadBalancingV2::Listener	Ja	Nein	cmdb_ci_lb_service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für AWS (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
AWS::EC2::NatGateway	Ja	Nein	cmdb_ci_nat_Gateway
AWS::EC2::VPC	Ja	Ja	cmdb_ci_network
AWS::EC2::NetworkAcl	Ja	Nein	cmdb_ci_network_acl
AWS::EC2::NetworkInterface	Ja	Ja	cmdb_ci_nic
AWS::EC2::RouteTable	Ja	Nein	cmdb_ci_route_table
AWS::EC2::VolumeAttachment	Ja	Ja	cmdb_ci_storage_mapping
AWS::EC2::Volume	Ja	Ja	cmdb_ci_storage_volume
AWS::EC2::VPNG	Ja	Nein	cmdb_ci_virtual_pvt_gateway
AWS::EC2::VPNConnection	Ja	Nein	cmdb_ci_vpn_connection
AWS::WAFv2::WebACL	Ja	N/V	cmdb_ci_Web_acl
AWS::WAFv2::WebACL	N/V	Ja	cmdb_ci_cmp_resource
Tags	Ja	Ja	cmdb_key_value
Kubernetes-DaemonSet	Nein	Ja	cmdb_ci_kubernetes_daemonset
Kubernetes-Bereitstellung	Nein	Ja	cmdb_ci_kubernetes_deployment
Kubernetes-Namespace	Nein	Ja	cmdb_ci_kubernetes_namespace
Amazon EKS-Knoten	Nein	Ja	cmdb_ci_kubernetes_node
Amazon EKS-Pod	Nein	Ja	cmdb_ci_kubernetes_pod
Amazon EKS-Service	Nein	Ja	cmdb_ci_kubernetes_service
Kubernetes-Volumen	Nein	Ja	cmdb_ci_kubernetes_volume
AWS::SSM::ManagedInstanceInventory	Nein	Ja	cmdb_ci_spkg

Microsoft Azure Discovery-Lösungsvergleich

ITOM-Transparenz Anwendungen erkennen eine Vielzahl von Microsoft Azure Ressourcen, und füllen Sie die relevanten Konfigurationselementklassen (Configuration Item, CI) in aus Configuration Management Database (CMDB) Mit ihren Attributen.

ITOM-Transparenz Lösungen

ITOM-Transparenz Kann Ihnen einen umfassenden Einblick in die Cloud-Infrastruktur Ihrer Organisation bieten. Jede Anwendung bietet einzigartige Stärken und Fähigkeiten, und durch den Vergleich erhalten Sie ganzheitliche Einblicke in ihre Fähigkeiten und Vorteile.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM-Transparenz Lösungen für die Erkennung Azure

Die Lösung ITOM-Transparenz	Übersicht	Konfiguration
Muster für Discovery und Service-Mapping und Visibility Content	Von ITOM-Transparenz verwendete Erkennungsmuster	• Sie müssen Ihre Store-Apps auf die neueste Release-Version aktualisieren. • Sie müssen angeben ITOM-Transparenz Mit Zugriffsberechtigungen. Weitere Informationen finden Sie unter Azure-Servicekonten einrichten
Service Graph Connector für Microsoft Azure	Service Graph Connector für Microsoft Azure	Konfigurieren Service Graph Connector für Microsoft Azure Mit dem geführten Setup

Hinweis:

Die CI-Klasse gilt in den meisten Fällen für beide Lösungen. Wenn dies nicht für eine der Lösungen gilt, wird die Lösung als „N/V“ markiert.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für Microsoft Azure

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
microsoft.compute/availabilitysets	Ja	N/V	cmdb_ci_Availability_Set
microsoft.compute/availabilitysets	Ja	Ja	cmdb_ci_availability_zone
Microsoft.Management/managementGroups	Ja	Nein	cmdb_ci_Azure_Management_Group
microsoft.KeyVault/Tresore	Ja	Nein	cmdb_ci_certificate
• Microsoft.Sql/servers/databases • Microsoft.DBforMySQL/Server • Microsoft.DocumentDB/databaseAccounts • Microsoft.Cache/Redis	Ja	Nein	cmdb_ci_cloud_database

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für Microsoft Azure (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
• Microsoft.Sql/servers • Microsoft.DBforPostgreSQL/Server	Ja	Ja	cmdb_ci_cloud_database
microsoft.network/expressroutecircuits	Ja	Nein	cmdb_ci_Cloud_direct_Connect
Microsoft.Storage/storageAccounts/fileServices	Ja	Nein	cmdb_ci_Cloud_file_Service
Microsoft.Storage/storageAccounts/fileServices/Shares	Ja	Nein	cmdb_ci_Cloud_file_share
Microsoft.Web/Sites/Funktionen	Ja	Ja	cmdb_ci_cloud_function
VM-Größe	Ja	Nein	cmdb_ci_Cloud_Hardware_type
microsoft.compute/hostgroups/hosts	Ja	Nein	cmdb_ci_cloud_host
microsoft.network/applicationgateways	Ja	Nein	cmdb_ci_cloud_load_balancer
microsoft.network/loadbalancers	Ja	Ja	cmdb_ci_cloud_load_balancer
Microsoft.Storage/storageAccounts/blobService	Ja	Nein	cmdb_ci_Cloud_object_Service
Mandant	Ja	Nein	cmdb_ci_cloud_org
microsoft.network/publicipaddresses	Ja	Ja	cmdb_ci_cloud_public_ipaddress
Microsoft.Storage/storageAccounts/QueueServices	Ja	Nein	cmdb_ci_Cloud_Queue_Service
Microsoft.Resources/Abonnements	Ja	Ja	cmdb_ci_cloud_service_account
Microsoft.Management/managementGroup	Ja	Nein	cmdb_ci_cloud_service_account
microsoft.storage/storageaccounts	Ja	Ja	cmdb_ci_cloud_storage_account
Microsoft.Network/virtualNetworks/subnets	Ja	Nein	cmdb_ci_cloud_subnet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für Microsoft Azure (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
Microsoft.Storage/ storageAccounts/ tableServices	Ja	Nein	cmdb_ci_Cloud_table_Service
microsoft.Web/Sites	Ja	Nein	cmdb_ci_cloud_webserver
microsoft.network/ networksecuritygroups	Ja	Ja	cmdb_ci_compute_security_group
microsoft.network/ privatednszones	Ja	Nein	cmdb_ci_dns_Zone
microsoft.compute/ virtualmachinescalesets	Ja	Ja	cmdb_ci_instance_Scale_Set
microsoft.containerservice/ managedClusters	Ja	Ja	cmdb_ci_kubernetes_cluster
Microsoft.Network/ loadBalancers/ backendAddressPools	Ja	Nein	cmdb_ci_lb_pool
Microsoft.Network/ loadBalancers/ inboundNatRules	Ja	Nein	cmdb_ci_lb_service
microsoft.network/ natgateways	Ja	Nein	cmdb_ci_nat_Gateway
microsoft.network/ virtualnetworks	Ja	Ja	cmdb_ci_network
microsoft.network/ networkinterfaces	Ja	Ja	cmdb_ci_nic
microsoft.compute/ images	Ja	Nein	cmdb_ci_os_template
Microsoft.Resources/ resourceGroups	Ja	Ja	cmdb_ci_resource_group
Microsoft.Network/ routeTables/routes	Ja	Nein	cmdb_ci_route_table
microsoft.network/ routetables	Ja	Nein	cmdb_ci_route_table
microsoft.compute/disks	Ja	Ja	cmdb_ci_storage_volume
microsoft.network/ localnetworkgateways	Ja	Nein	cmdb_ci_virtual_pvt_gateway
microsoft.network/ virtualnetworkgateways	Ja	Nein	cmdb_ci_virtual_pvt_gateway
microsoft.compute/ virtualmachines	Ja	Ja	cmdb_ci_vm_instance

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für Microsoft Azure (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
microsoft.sqlvirtualmachine/sqlvirtualmachines	Ja	Nein	cmdb_ci_vm_instance
Microsoft.Network/virtualNetworks/virtualNetworkPeerings	Ja	Nein	cmdb_ci_vnet_Peering
microsoft.network/connections	Ja	Nein	cmdb_ci_vpc_Gateway_connection
Microsoft.Resources/Tags	Ja	Ja	cmdb_key_value
Microsoft.Compute/virtualMachines	Nein	Ja	cmdb_ci_server
Microsoft.Compute/virtualMachines	Nein	Ja	cmdb_ci_win_server
Microsoft.Network/networkInterfaces	Nein	Ja	cmdb_ci_hardware
Microsoft.Compute/virtualMachines	Nein	Ja	cmdb_ci_linux_server
microsoft.containerservice/managedClusters	Ja	Ja	cmdb_ci_kubernetes_cluster
Microsoft.Compute/virtualmachinescalesets	Nein	Ja	cmdb_ci_vm_instance
Microsoft.ServiceBus/Namespaces/Warteschlangen	Ja	Nein	cmdb_Azure_Service_Bus_Queue
Microsoft.ServiceBus/Namespaces/Themen	Ja	Nein	cmdb_Azure_Service_Bus_topic
microsoft.appConfiguration/ConfigurationStores	Ja	Nein	cmdb_Azure_App_Configuration_Store
microsoft.automation/automationaccounts	Ja	Nein	cmdb_Azure_Automation_Automation_Acco
microsoft.compute/diskencryptionsets	Ja	Nein	cmdb_Azure_Disk_Encryption_Set_Disk_En
microsoft.compute/galleries/images	Ja	Nein	cmdb_Azure_Compute_Gallery_image_Defi
microsoft.compute/snapshots	Ja	Nein	cmdb_Azure_Compute_Snapshot
microsoft.containerregistry/Registrierungen	Ja	Nein	cmdb_Azure_Container_Registry_Registry
microsoft.databricks/Arbeitsbereiche	Ja	Nein	cmdb_Azure_databricks_Workspace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für Microsoft Azure (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
microsoft.datafactory/Fabrics	Ja	Nein	cmdb_Azure_Data_Factory_Data_Factory
microsoft.Datenschutz/Backupvaults	Ja	Nein	cmdb_Azure_Data_Protection_Backup_Vaul
microsoft.eventraster/systemthemen	Ja	Nein	cmdb_Azure_Event_Grid_System_topic
microsoft.eventhub/namespaces	Ja	Nein	cmdb_Azure_Event_Hub_Namespace
microsoft.insights/components	Ja	Nein	cmdb_Azure_Application_Insight_componen

GCP Discovery-Lösungsvergleich

ITOM-Transparenz Anwendungen erkennen eine Vielzahl von Google Cloud Platform (GCP) Ressourcen, und füllen Sie die relevanten Konfigurationselementklassen (Configuration Item, CI) in aus Configuration Management Database (CMDB) Mit ihren Attributen.

ITOM-Transparenz Lösungen

ITOM-Transparenz Kann Ihnen einen umfassenden Einblick in die Cloud-Infrastruktur Ihrer Organisation bieten. Jede Anwendung bietet einzigartige Stärken und Fähigkeiten, und durch den Vergleich erhalten Sie ganzheitliche Einblicke in ihre Fähigkeiten und Vorteile.

ITOM-Transparenz Lösungen für die Erkennung GCP

Die Lösung ITOM-Transparenz	Übersicht	Konfiguration
Muster für Discovery und Service-Mapping und Visibility Content	Von ITOM-Transparenz verwendete Erkennungsmuster	• Sie müssen Ihre Store-Apps auf die neueste Release-Version aktualisieren. • Sie müssen angeben ITOM-Transparenz Mit Zugriffsberechtigungen. Weitere Informationen finden Sie unter Richten Sie Google Cloud Platform-Service-Accounts ein
Service Graph Connector für GCP	Service Graph Connector für GCP	Konfigurieren Service Graph Connector für GCP Mit dem geführten Setup

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Die CI-Klasse gilt in den meisten Fällen für beide Lösungen. Wenn dies nicht für eine der Lösungen gilt, wird die Lösung als „N/V“ markiert.

Wenn ein Eintrag mit einem Sternchen markiert ist, wird der Ressourcentyp von Mustern nur unterstützt, indem verwendet wird **Google-Asset-Bestand** Aufnahmeliste des Musters. Weitere Informationen finden Sie unter Google Cloud Platform (GCP) Asset-Bestandserkennung mit Mustern.

Wenn ein Eintrag mit zwei Sternchen markiert ist, wird der Ressourcentyp von Service Graph Connecters nur unterstützt, indem die Tabelle [sn_cmdb_int_util_Service_Graph_resource_Inclusion_Whitelist] verwendet wird.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
admissionregistration.k8s.io/mutatingwebhookconfiguration	Ja*	Ja**	cmdb_ci_cmp_resource
admissionregistration.k8s.io/validatingwebhookconfiguration	Ja*	Ja**	cmdb_ci_cmp_resource
alloydb.googleapis.com/Cluster	Ja	Nein	cmdb_ci_cloud_db_cluster
apigateway.googleapis.com/api	Ja*	Ja**	cmdb_ci_cmp_resource
apigateway.googleapis.com/apiconfig	Ja*	Ja**	cmdb_ci_cmp_resource
apigee.googleapis.com/instance	Ja*	Ja**	cmdb_ci_cmp_resource
apigee.googleapis.com/organization	Ja*	Ja**	cmdb_ci_cmp_resource
apikeys.googleapis.com/key	Ja*	Ja**	cmdb_ci_cmp_resource
appengine.googleapis.com/application	Ja*	Ja**	cmdb_ci_cmp_resource
apps.k8s.io/daemonset	Ja*	Ja**	cmdb_ci_cmp_resource
apps.k8s.io/Deployment	Ja*	Ja	cmdb_ci_kubernetes_deployment
apps.k8s.io/ReplicaSet	Ja*	Ja	cmdb_ci_kubernetes_replicaset
apps.k8s.io/statefulset	Ja*	Ja**	cmdb_ci_cmp_resource
artifactregistry.googleapis.com/dockerimage	Ja*	Ja**	cmdb_ci_cmp_resource
artifactregistry.googleapis.com/repository	Ja*	Ja**	cmdb_ci_cmp_resource

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
bigquery.googleapis.com/bigquery-public-data/datasets	Ja	Nein	cmdb_ci_Cloud_public_database
bigquery.googleapis.com/bigquery-public-data/datasets/tables	Ja	Nein	cmdb_ci_database
bigquery.googleapis.com/Dataset	Ja	N/V	cmdb_ci_cloud_database
bigquery.googleapis.com/Dataset	N/V	Ja**	cmdb_ci_cmp_resource
bigquery.googleapis.com/Table	Ja	Nein	cmdb_ci_database
bigtableadmin.googleapis.com/Instance	Ja	Ja	cmdb_ci_cloud_database
bigtableadmin.googleapis.com/Table	Ja	Nein	cmdb_ci_database
cloudasset.googleapis.com/feed	Ja*	Ja**	cmdb_ci_cmp_resource
cloudbilling.googleapis.com/billingaccount	Ja*	Ja**	cmdb_ci_cmp_resource
cloudbilling.googleapis.com/projectbillinginfo	Ja*	Ja**	cmdb_ci_cmp_resource
cloudfunctions.googleapis.com/CloudFunction	Ja	Ja	cmdb_ci_cloud_function
cloudresourcemanager.googleapis.com/Folder	Ja	Ja	cmdb_ci_gcp_folder
cloudresourcemanager.googleapis.com/Organization	Ja	Ja	cmdb_ci_cloud_org
cloudresourcemanager.googleapis.com/Project	Ja	Ja	cmdb_ci_gcp_Project
cloudresourcemanager.googleapis.com/tagkey	Ja*	Ja	cmdb_ci_cmp_resource
cloudresourcemanager.googleapis.com/tagvalue	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Address	Ja	Nein	cmdb_ci_cloud_public_ipaddress
compute.googleapis.com/autoscaler	Ja*	Ja**	cmdb_ci_cmp_resource

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
compute.googleapis.com/BackendService	N/V	Ja	cmdb_ci_cloud_load_balancer
compute.googleapis.com/BackendService	Ja	N/V	cmdb_ci_lb_service
compute.googleapis.com/Disk	Ja	Ja	cmdb_ci_storage_volume
compute.googleapis.com/DiskTypes	Ja	Nein	cmdb_ci_disk_type
compute.googleapis.com/Firewall	N/V	Ja	cmdb_ci_compute_security_group
compute.googleapis.com/Firewall	Ja	Ja	cmdb_ci_network_acl_rule
compute.googleapis.com/ForwardingRule	Ja	Ja	cmdb_ci_lb_service
compute.googleapis.com/HttpHealthCheck	Ja	Ja	cmdb_ci_lb_health_service
compute.googleapis.com/Image	Ja	Nein	cmdb_ci_os_template
compute.googleapis.com/Instance	Ja	N,A	cmdb_ci_lb_pool_member
compute.googleapis.com/Instance	N/V	Ja	cmdb_ci_server
compute.googleapis.com/Instance	Ja	Ja	cmdb_ci_vm_instance
compute.googleapis.com/Instance/networkInterfaces	Ja	Nein	cmdb_ci_endpoint_vnic
compute.googleapis.com/Instance/networkInterfaces	Ja	Ja	cmdb_ci_nic
compute.googleapis.com/InstanceGroup	Ja	N/V	cmdb_ci_lb_pool
compute.googleapis.com/InstanceGroup	N/V	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Instancegroupmanager	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Instancesettings	Ja*	Ja**	cmdb_ci_cmp_resource

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
compute.googleapis.com/InstanceTemplate	Ja	Nein	cmdb_ci_instance_template
compute.googleapis.com/Instancetemplate	Nein	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/MachineImage	Nein	Ja	cmdb_ci_os_template
compute.googleapis.com/MachineTypes	Ja	Nein	cmdb_ci_Cloud_Hardware_type
compute.googleapis.com/MachineTypes	Ja	Nein	cmdb_ci_compute_template
compute.googleapis.com/Network	Ja	Ja	cmdb_ci_network
compute.googleapis.com/Networkendpointgroup	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Regions	Ja	Nein	cmdb_ci_google_datacenter
compute.googleapis.com/resourcepolicy	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/router	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Snapshot	Ja	Ja	cmdb_ci_storage_vol_snapshot
compute.googleapis.com/ssh	Ja	Nein	cmdb_ci_cloud_key_pair
compute.googleapis.com/sslcertificate	Ja*	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/Subnetwork	Ja	Ja	cmdb_ci_cloud_subnet
compute.googleapis.com/targetHttpProxy	Ja	N/V	cmdb_ci_lb_service
compute.googleapis.com/targetHttpProxy	Ja	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/TargetPool	Ja	N/V	cmdb_ci_cloud_load_balancer
compute.googleapis.com/TargetPool	N/V	Ja	cmdb_ci_lb_pool
compute.googleapis.com/targetSslProxy	Ja	Nein	cmdb_ci_lb_service

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
compute.googleapis.com/targetTcpProxy	Ja	Nein	cmdb_ci_lb_service
compute.googleapis.com/UrlMap	Ja	N/V	cmdb_ci_cloud_load_balancer
compute.googleapis.com/UrlMap	N/V	Ja**	cmdb_ci_cmp_resource
compute.googleapis.com/zones	Ja	Nein	cmdb_ci_availability_zone
container.googleapis.com/Cluster	Ja	Ja	cmdb_ci_kubernetes_cluster
container.googleapis.com/NodePool	Nein	Ja	cmdb_ci_kubernetes_node_Pool
containerregistry.googleapis.com/image	Ja*	Ja**	cmdb_ci_cmp_resource
dataplex.googleapis.com/entrygroup	Ja*	Ja**	cmdb_ci_cmp_resource
firebase.googleapis.com/firebaseproject	Ja*	Ja**	cmdb_ci_cmp_resource
firebasedatabase.googleapis.com/instances	Ja	Nein	cmdb_ci_cloud_database
firebaserules.googleapis.com/release	Ja*	Ja**	cmdb_ci_cmp_resource
firebaserules.googleapis.com/ruleset	Ja*	Ja**	cmdb_ci_cmp_resource
firestore.googleapis.com/Database	Ja	Ja	cmdb_ci_cloud_database
iam.googleapis.com/role	Ja*	Ja**	cmdb_ci_cmp_resource
iam.googleapis.com/serviceaccount	Ja*	Ja**	cmdb_ci_cmp_resource
iam.googleapis.com/serviceaccountkey	Ja*	Ja**	cmdb_ci_cmp_resource
integrations.googleapis.com/integration	Ja*	Ja**	cmdb_ci_cmp_resource
integrations.googleapis.com/integrationversion	Ja*	Ja**	cmdb_ci_cmp_resource
K8s.io/endpoints	Ja*	Ja**	cmdb_ci_cmp_resource
K8s.io/Namespace	Ja*	Ja	cmdb_ci_kubernetes_namespace
k8s.io/Node	Ja*	Ja	cmdb_ci_kubernetes_node

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
K8s.io/persistentvolume	Ja*	Ja**	cmdb_ci_cmp_resource
k8s.io/ persistentvolumeclaim	Ja*	Ja**	cmdb_ci_cmp_resource
K8s.io/Pod	Ja*	Ja	cmdb_ci_docker_container
K8s.io/Pod	N/V	Ja	cmdb_ci_docker_image
K8s.io/Pod	N/V	Ja	cmdb_ci_kubernetes_pod
K8s.io/Pod	N/V	Ja	cmdb_ci_kubernetes_volume
K8s.io/resourcequota	Ja*	Ja**	cmdb_ci_cmp_resource
k8s.io/Service	Ja*	Ja	cmdb_ci_kubernetes_service
K8s.io/serviceaccount	Ja*	Ja**	cmdb_ci_cmp_resource
Bezeichnungen	Ja	Nein	cmdb_key_value
logging.googleapis.com/ logbucket	Ja*	Ja**	cmdb_ci_cmp_resource
logging.googleapis.com/ logmetric	Ja*	Ja**	cmdb_ci_cmp_resource
logging.googleapis.com/ logsink	Ja*	Ja**	cmdb_ci_cmp_resource
logging.googleapis.com/ recentquery	Ja*	Ja**	cmdb_ci_cmp_resource
memcache.googleapis.com/ Instance	Ja*	Ja	cmdb_ci_cloud_database
monitoring.googleapis.com/ alertpolicy	Ja*	Ja**	cmdb_ci_cmp_resource
monitoring.googleapis.com/ dashboard	Ja*	Ja**	cmdb_ci_cmp_resource
monitoring.googleapis.com/ notificationchannel	Ja*	Ja**	cmdb_ci_cmp_resource
networkmanagement.googleapis.com/ connectivitytest	Ja*	Ja**	cmdb_ci_cmp_resource
orgpolicy.googleapis.com/ policy	Ja*	Ja**	cmdb_ci_cmp_resource
policy.k8s.io/ poddisruptionbudget	Ja*	Ja**	cmdb_ci_cmp_resource
pubsub.googleapis.com/ subscription	Ja*	Ja**	cmdb_ci_cmp_resource
pubsub.googleapis.com/ topic	Ja*	Ja**	cmdb_ci_cmp_resource

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
rbac.authorization.k8s.io/ ClusterRole	Nein	Ja	cmdb_ci_kubernetes_Cluster_role
rbac.authorization.k8s.io/ ClusterRoleBinding	Nein	Ja	cmdb_ci_kubernetes_cluster_role_binding Tabelle
rbac.authorization.k8s.io/ role	Ja*	Ja**	cmdb_ci_cmp_resource
rbac.authorization.k8s.io/ rolebinding	Ja*	Ja**	cmdb_ci_cmp_resource
redis.googleapis.com/ clusters	Ja	Nein	cmdb_ci_cloud_db_cluster
redis.googleapis.com/ Instance	Nein	Ja	cmdb_ci_cloud_database
run.googleapis.com/ revision	Ja*	Ja**	cmdb_ci_cmp_resource
run.googleapis.com/ service	Ja*	Ja**	cmdb_ci_cmp_resource
servicedirectory.googleapis.com/ endpoint	Ja*	Ja**	cmdb_ci_cmp_resource
servicedirectory.googleapis.com/ namespace	Ja*	Ja**	cmdb_ci_cmp_resource
servicedirectory.googleapis.com/ service	Ja*	Ja**	cmdb_ci_cmp_resource
servicemanagement.googleapis.com/ managedservice	Ja*	Ja**	cmdb_ci_cmp_resource
servicenetworking.googleapis.com/ connection	Ja*	Ja**	cmdb_ci_cmp_resource
serviceusage.googleapis.com/ service	Ja*	Ja**	cmdb_ci_cmp_resource
spanner.googleapis.com/ Database	Ja	Nein	cmdb_ci_database
spanner.googleapis.com/ Instance	Ja	Ja	cmdb_ci_cloud_database
sqladmin.googleapis.com/ backup	Ja*	Ja**	cmdb_ci_cmp_resource
sqladmin.googleapis.com/ backuprun	Ja*	Ja**	cmdb_ci_cmp_resource
sqladmin.googleapis.com/ Instance	Ja*	Ja	cmdb_ci_cloud_database

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für Discovery und Service-Mapping Vs Service Graph Connector für GCP (Fortsetzung)

Ressourcentyp	Unterstützt von Cloud-Discovery- und Service-Mapping-Mustern	Unterstützt von Cloud Service Graph Connectors	CI-Klasse
sqladmin.googleapis.com/Instances/databases	Ja*	Nein	cmdb_ci_database
storage.googleapis.com/Bucket	N/V	Ja	cmdb_ci_cloud_object_storage
storage.googleapis.com/Bucket	Ja	N/V	cmdb_ci_cmp_resource
storage.k8s.io/storageclass	Ja*	Ja**	cmdb_ci_cmp_resource

Container-Discovery erkunden

Mit der Container-Discovery können IT-Abteilungen von Unternehmen detaillierte Informationen zu ihren Containerverwaltungstools in der Infrastruktur sammeln. Discovery Sucht Ressourcen in Anbietern wichtiger Container-Management-Services.

Kubernetes Discovery mithilfe von Mustern

Amazon ECS-Ressourcen-Discovery mit Mustern

Erkennung von Pivotal Cloud Foundry

Discovery Lösungen für Performance Analytics and Reporting

Lösungen für Performance Analytics and Reporting enthalten vorkonfigurierte Dashboards. Diese Dashboards enthalten Visualisierungen handlungsrelevanter Daten, mit denen Sie Ihre Geschäftsprozesse und -praktiken optimieren können.

Lösungen für Performance Analytics and Reporting

Platform Analytics Datenvisualisierungen verwenden Performance Analytics *Indikator*Daten, die Ihnen Daten im Zeitverlauf anzeigen, damit Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Lösungen für Performance Analytics and Reporting können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Um das Lösungs-Plugin für zu aktivieren Discovery , Kann ein Administrator zu navigieren **Systemdefinitionen** > **Plugins** Und aktivieren Sie das Plugin „Performance Analytics – Inhaltspaket – Discovery“.

Zugehörige Informationen

Performance Analytics-Abonnement aktivieren

Kubernetes Discovery mithilfe von Mustern

Die ServiceNow ITOM-Transparenz Findet Kubernetes Und OpenShift Komponenten mit Mustern Und erstellt Anwendungsservices, die sie enthalten . Discovery Findet auch Kubernetes Ereignisse und aktualisiert häufig CMDB Um die Dynamik widerzuspiegeln Kubernetes Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Verwendet Kubernetes Muster und seine Erweiterungsabschnitte, die erkannt werden sollen Kubernetes Komponenten für Kubernetes Version 1,21:

- Die *`Collect OpenShift info`* Abschnitt „Erweiterung“ von Kubernetes Muster erkennt OpenShift Komponenten von Kubernetes Bereitstellung. Die OpenShift Der Abschnitt „Build-Konfiguration“ ist ab Store-Version 1,0.53 verfügbar.
- Von der *`Service Mesh`*-Erweiterung werden Servicenetz-Details erkannt. Diese Informationen ermöglichen es dem Muster, Service-zu-Service-Beziehungen zu erstellen, die als Verbunden zu::Verbunden angezeigt werden. Die Service Mesh-Discovery erfordert die Bereitstellung von Istio auf Ihrem K8s-Cluster (Kubernetes). Der Abschnitt „Service Mesh-Erweiterung“ ist in verfügbar Kubernetes-Erweiterungsklassen . Wird auf unterstützt ServiceNow AI Platform Mit Madrid Release oder höher.
- Von *`Collect Container Repository`* und Erweiterungsabschnitt wird nach Container-Registrierungen und Images in diesen Registrierungen gesucht.

Darüber hinaus Discovery Verwendet Kubernetes Ereignismuster, für das Ereignisse erkannt werden sollen Kubernetes Komponenten für Versionen Kubernetes Version 1,21.

Ab Release 1.0.68 auf ServiceNow Store, Service-Mapping Kann CI-Beziehungen verwenden, um hinzuzufügen Kubernetes Komponenten für Anwendungsservices während der Tag-basierten Discovery.

Discovery Verwendet die folgenden Muster, um das gesamte zu erkennen Kubernetes Auf GCP, AWS und Azure bereitgestellte Infrastruktur:

- Google Cloud Platform (GCP) – Abrufen Kubernetes Cluster .
- Amazon AWS – Abrufen Kubernetes Cluster .
- Azure – Abrufen Kubernetes Cluster .

Mit diesen Mustern werden Cloud-Abfragen durchgeführt, Daten zu allen Kubernetes-Clustern gesammelt und Zeitpläne für die serverlose Erkennung für die einzelnen Cluster erstellt. Wenn der Cluster gelöscht wird, wird der Zeitplan als inaktiv markiert. Mithilfe dieser Funktion wird der Mehraufwand für die Erstellung und Verwaltung mehrerer Anmeldeinformationen und Zeitpläne für serverlose Erkennung pro Cluster eliminiert. Die Cloud-Infrastrukturmuster werden durch die standardmäßige Cloud-Erkennung ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Hinweis: Für Voraussetzungen für Kubernetes Cloud-Infrastruktur-Discovery, siehe Unten .

Hinweis: Automatische serverlose Ausführung Kubernetes Zeitpläne ruft das Bearer-Token ab. Das Hinzufügen von Anmeldeinformationen ist nicht erforderlich.

Führen Sie die folgenden Schritte aus, um dies sicherzustellen Discovery Kann verwenden Muster, das erfolgreich gefunden werden soll Kubernetes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Stellen Sie die aktuelle Anwendung Discovery and Service Mapping Patterns aus dem ServiceNow Store bereit.
2. Auf der Kubernetes Plattform: Suchen Sie nach den Parametern, die eingerichtet werden sollen Kubernetes Discovery:

   - Suchen Sie nach der URL des kubeapi-Servers:
     a. Auf der Kubernetes Plattform: Führen Sie den folgenden Befehl aus:

        `kubectl cluster-info`

     b. Suchen Sie in der Ausgabe nach der Zeile, die die URL des kubeapi-Servers angibt. Beispiel: Kubernetes Die Steuerungsebene wird um ausgeführt

        `https://10.154.144.146:443`

   - Suchen Sie den Namespace des Kubeapi-Servers:
     a. Auf der Kubernetes Plattform, führen Sie diesen Befehl aus:

        `kubectl get namespaces`

     b. Suchen Sie in der Ausgabe die Zeile, die die Namespaces angibt. Beispiel: `kube-system`.
   - Suchen Sie nach Kubernetes Anwendername und Passwort:
     a. Auf der Kubernetes Plattform, führen Sie diesen Befehl aus:

        `kubectl config view`

     b. Suchen Sie in der Ausgabe den Benutzernamen und das Passwort.

Hinweis: In einer bestimmten Umgebung `Kubectl-Konfigurationsansicht` Befehl zeigt nicht die erwarteten Details an. Verwenden Sie Unterstützt Befehl von Kubernetes administrator zum Abrufen der Anwendernamen- und Passwortdetails.

   - Suchen Sie das gültige Bearer-Token mit den richtigen Berechtigungen:

     - Wenn Sie den Standard-Token-Namen kennen, verwenden Sie den Befehl im folgenden Format: `Kubectl beschreibt geheime <default-token-token name>` .

       Beispiel: `Kubectl beschreiben Secret default-Token-g6pwc` .

     - Wenn Sie den Standard-Token-Namen nicht kennen, verwenden Sie den folgenden Befehl: `Kubectl-Beschreibungsgeheimnis` .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Stellen Sie sicher, dass der API-Server über erreichbar ist MID-Server Für erfolgreich Kubernetes Discovery.
4. Stellen Sie sicher, dass der Anwender auf konfiguriert ist Kubernetes Plattform hat **ABRUFEN** Berechtigungen zum Ausführen der folgenden /api/v1-Elemente:
   - https://<URL>/api/v1/namespaces/
   - https://<URL>/api/v1/namespaces/<Namespace>
   - https://<URL>/api/v1/namespaces/kube-system/endpoints/kube-controller-manager
   - https://<URL>/api/v1/services
   - https://<URL>/api/v1/pods
   - https://<URL>/api/v1/nodes
   - https://<url>/api/v1/replicationController
   - https://<url>/apis/Networking.k8s.io/v1/eingangs
   - https://<url>/apis/Apps/v1/Bereitstellungen
   - https://<url>/apis/Apps/v1/statefulsets
   - https://<url>/apis/Apps/v1/Daemonsets
   - https://<url>/apis/Apps/v1/replicasets
   - https://<url>/apis/Batch/v1/cronjobs
   - https://<url>/apis/Batch/v1/Jobs
5. Um zu erkennen OpenShift Komponenten von Kubernetes Bereitstellung: Stellen Sie sicher, dass der Anwender auf konfiguriert ist Kubernetes Plattform hat **ABRUFEN** Berechtigungen zum Ausführen der folgenden /api/v1-Elemente:
   - /apis/apps.openshift.io/v1/deploymentconfigs
   - /apis/build.openshift.io/v1/buildconfigs
   - /apis/route.openshift.io/v1/routes
   - /apis/user.openshift.io/v1/groups☒
   - /apis/user.openshift.io/v1/users☒
   - /apis/project.openshift.io/v1/projects
   - /apis/image.openshift.io/v1/images
   - /apis/image.openshift.io/v1/imagestreams

   So erkennen Sie Service-Mesh-Informationen:
   - Stellen Sie Istio auf Ihrem K8s-Cluster bereit.
   - Geben Sie die Prometheus-URL an.
   - Konfigurieren Sie Prometheus, um Metriken aus Istio zu entfernen.
6. Aktivieren **Kubernetes-Konfigurationsdateien Abrufen** Erweiterung auf:
   - Erkennen Sie Konfigurationsdateien.
   - Erstellen Sie nachverfolgte Konfigurationsdateien.
   - Ordnen Sie die Arbeitsauslastungen und Services der Konfigurationsdatei einer Beziehung zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Inhalt der nachverfolgten Dateien liegt im JSON-Format ab Version 1,0.92 vor. Der Inhalt der nachverfolgten Dateien ist ab Version 1.0.91 im YAML-Format.

7. Erstellen Sie Kubernetes Anmeldeinformationen für ServiceNow Plattform:
   a. Auf der ServiceNow AI Platform, Navigieren Sie zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
   b. Wählen Sie **Neu**.
   c. Wählen Sie Aus **Kubernetes-Anmeldeinformationen** .
   d. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen.
Anwendername	Anwendername, der diesen Anmeldeinformationen zugeordnet ist. Führende oder nachfolgende Leerzeichen sollten vermieden werden. Wenn solche erkannt werden, wird eine Warnung angezeigt. Es darf nur eine Authentifizierungsmethode verwendet werden: Entweder ein Anwendername und ein Passwort oder ein Bearer-Token. Verwenden Sie nicht beides.
Passwort	Passwort, das diesen Anmeldeinformationen zugeordnet ist. Es darf nur eine Authentifizierungsmethode verwendet werden: Entweder ein Anwendername und ein Passwort oder ein Bearer-Token. Verwenden Sie nicht beides.
Bearer-Token-Authentifizierung	Diese Option aktiviert die erweiterte Authentifizierung mit einem Bearer-Token. Wenn das Kontrollkästchen aktiviert ist, wird das Feld Bearer-Token angezeigt.
Bearer-Token	Discovery Verwendet das Bearer-Token für die erweiterte Authentifizierung beim Zugriff Kubernetes. Das Bearer-Token muss im BASE64-codierten Format vorliegen und die Zeichensequenz als Token verwenden. Beispiel: 31ada4fd-adec-460c-809a-9e56ceb75269. Es darf nur eine Authentifizierungsmethode verwendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden: Entweder ein Anwendername und ein Passwort oder ein Bearer-Token. Verwenden Sie nicht beides.
Anmeldeinformationsalias	Ein Alias ist für die Verwendung von konfiguriert Kubernetes Anmeldeinformationen für andere Geräte und Anwendungen als Kubernetes. Dieser Alias wird auch beim Definieren eines serverlosen Discovery-Zeitplans für die Erkennung von verwendet Kubernetes Bereitstellung. **i.** Wählen Sie das Vorhängeschloss-Symbol und dann das Suchsymbol. **ii.** Wählen Sie im Formular Aliasse für Verbindungen und Anmeldeinformationen die Option aus **Neu** . **iii.** Geben Sie einen Namen für den Aliasdatensatz für Anmeldeinformationen an. **iv.** Definieren Sie Attribute für den Alias. Legen Sie den *Type* auf Berechtigung fest. **v.** Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** , Und wählen Sie dann aus **Aktualisieren** . **vi.** Wählen Sie im Formular Aliasse für Verbindungen und Anmeldeinformationen den neu hinzugefügten Alias aus. Der Alias wird im Feld „Anmeldeinformationsalias“ angezeigt.

e. Auf der Kubernetes Formular „Anmeldeinformationen“ auswählen **Aktualisieren** .

8. Erstellen Sie einen serverlosen Discovery-Zeitplan für Kubernetes Muster.

Erstellen und definieren Sie das Ausführungsmuster ohne Server wie in der Produktdokumentation beschrieben. Konfigurieren Sie die für erforderlichen Parameter KubernetesMuster wie folgt:

Attribute für Ausführungsmuster konfigurieren

Feld	Beschreibung
URL	Der Bezeichner für den Hostnamen, die IP oder den FQDN und den Port des Kubernetes Apiserver. Verwenden Sie das folgende Format: beispiel_hostname:beispiel_port oder beispiel_ip:beispiel_port. Geben Sie das richtige Protokoll (HTTP oder HTTPS) in der URL an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
namespace	Die Namespaces, die das System in übergibt Kubernetes Discovery-Konfiguration. Geben Sie einen der folgenden Werte ein: ○ Individueller Namespace: Geben Sie den Namespace und dann „kube-System“ ein. Beispiel: dev,kube-System ○ Der Standardwert: Eingabetaste Standard, kube-System ○ Multipile-Namespaces: Geben Sie die Namespaces ein, trennen Sie die Werte durch ein Komma (,), und geben Sie dann „kube-System“ ein. Beispiel: Automatisierung,Anwendung,Test,Kube-System ○ Alle Namespaces: Verwenden Sie ein Sternchen (*), um alle Namespaces einzugeben
Alias für Anmeldeinformationen	Der Alias, der dem zuvor erstellten zugeordnet ist Kubernetes Anmeldeinformationen.
Clustername	Der Name des Kubernetes Cluster im folgenden Format: <serviceaccountid> <space> <clustername>.
Anbieter	Der Cloud-Anbieter: GCP, AWS oder Azure.
cluster_resource_id	Beispiel für Cluster-Ressourcen-ID: ○ Azure Kubernetes Cluster: Ressourcen-ID. ○ AWS: Cluster-ARN. ○ GCP: Globaler Clustername.

9. Erstellen Sie einen serverlosen Discovery-Zeitplan für Kubernetes Ereignismuster. Konfigurieren Sie den Zeitplan so, dass er alle 5 oder 10 Minuten ausgeführt wird.

   Hinweis: Wenn das Muster zum ersten Mal ausgeführt wird, wird ein event_timestamp gespeichert. Später werden nur die Delta-Events basierend auf dem Zeitstempel erfasst. Je häufiger das Muster ausgeführt wird, desto weniger Updates für die CMDB-IRE sind erforderlich.

   Erstellen Sie ein serverloses Ausführungsmuster für den Discovery-Zeitplan, und weisen Sie es dem zu Kubernetes Ereignismuster. Konfigurieren Sie die für erforderlichen Parameter Kubernetes Muster wie in beschrieben Attribute für Ausführungsmuster konfigurieren.

10. Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Voraussetzungen für die Erkennung von Kubernetes-Cloud-Infrastrukturen

Für Google Cloud Platform (GCP)– Abrufen Kubernetes Cluster Muster: Führen Sie Folgendes aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Richten Sie in der ServiceNow-Instanz ein Servicekonto für Google Cloud Platform (GCP) mit gültigen Anmeldeinformationen und Berechtigungen ein.
2. Auf der GCP Infrastruktur, richten Sie die ein MID-Server Mit vollem Zugriff auf alle Cloud-APIs: Legen Sie die Cloud-API-Zugriffsbereiche auf „vollständigen Zugriff auf alle Cloud-APIs zulassen“ fest. Die MID-Server-Instanz kann nur auf die Cluster zugreifen, die für das Projekt spezifisch sind.
3. Navigieren Sie zu `sys_properties.list`, und konfigurieren Sie die folgenden Eigenschaften:
   - *`sn_itom_pattern.k8s_midserver`*: Geben Sie ein gültiges an MID-Server Name.
   - *`sn_itom_pattern.k8s_create_schedule_enabled`*: Legen Sie den Wert auf **true** fest.

     Hinweis: Aktivieren von *`sn_itom_pattern.k8s_create_schedule_enabled`*Die Eigenschaft erstellt automatisch einen serverlosen Zeitplan für Ihre Cloud-Cluster, wodurch keine manuelle Planung erforderlich ist. Wenn Sie einen vorhandenen manuellen Zeitplan haben und ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. Es wird kein zusätzlicher Zeitplan erstellt.

4. Erstellen und ausführen Google Cloud Discovery

   Hinweis:

   Zum Abrufen des Bearer-Tokens während der Ausführung von GKE Kubernetes Planen, verwenden Sie den gcloud-Befehl:

   ```
   Gcloud config-helper --Format="value(credential.Access_Token)"
   ```

   Durch die Konfiguration von gcloud in der MID-Server-Instanz wird Zugriff auf den GKE-Cluster zum Abrufen des Tokens gewährt.

Für Amazon Elastic Kubernetes Service (EKS) Führen Sie die Cluster-Discovery wie folgt aus:

1. Richten Sie in der ServiceNow-Instanz ein Servicekonto für AWS mit gültigen Anmeldeinformationen für das Verwaltungskonto sowie mit gültigen Berechtigungen ein.
   a. Stellen Sie sicher, dass Amazon Elastic Kubernetes Service (EKS) Cluster hat eine Clusterrolle mit schreibgeschütztem Zugriff auf alle Ressourcen.
   b. Erstellen Sie eine Clusterrollenbindung zwischen der Clusterrolle und einem Kubernetes-Benutzer. Beispiel: Schreibgeschützt Anwender.
   c. Erstellen Sie eine AWS-IAM-Rolle mit der Richtlinie EKSReadOnly.
   d. Ordnen Sie die IAM-Rolle dem Kubernetes-Benutzer auf eine der folgenden Arten zu:
      - Bearbeiten Sie im Cluster die aws-auth ConfigMap.
      - Führen Sie den folgenden Befehl aus:

        ```
        eksctl create iamidentitymapping --cluster yourClusterName --
        arnarn:aws:iam::yourAccountID:role/yourIAMRoleName --username read-only-user
        ```

2. Ausführen Amazon Elastic Kubernetes Service (EKS) Cluster-Discovery auf eine von zwei Arten: Mit AWS Befehlszeilenschnittstelle (CLI) oder ohne Verwendung von AWS CLI. Legen Sie zuerst die Systemeigenschaft fest

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*sn_itom_pattern.k8s_aws_cli_to_generate_token*Um das von Ihnen ausgewählte Modell zu verwenden. Diese Systemeigenschaft ist auf festgelegt **Wahr** Standardmäßig.

- Legen Sie diese Systemeigenschaft auf fest **Wahr** Zu verwenden AWS CLI zum Generieren eines Tokens.
- Legen Sie diese Systemeigenschaft auf fest **Falsch** Dient zur Verwendung von „Rollen übernehmen“ zum Generieren eines Tokens.

a. Ausführen Amazon Elastic Kubernetes Service (EKS) Cluster-Discovery mit AWS CLI:

i. Richten Sie ein MID-Server Mit AWS CLI konfiguriert. Wird Konfiguriert AWS CLI-Anmeldeinformationen gewähren Zugriff auf Amazon Elastic Kubernetes Service (EKS) Cluster.

Hinweis: Der beim System angemeldete Anwender muss mit identisch sein MID-Server Anwender.

ii. Dient zum Generieren des Bearer-Tokens während der Ausführung von Amazon Elastic Kubernetes Service (EKS) Planen, verwenden Sie AWS CLI-Befehl: `aws eks GET-Token --Cluster-Name <cluster_name>` .

Konfigurieren von AWS CLI-Anwender/-Rolle in MID-Server Instanz gewährt Zugriff auf Amazon Elastic Kubernetes Service (EKS) Cluster zum Generieren des Tokens.

b. Ausführen Amazon Elastic Kubernetes Service (EKS) Cluster-Discovery ohne Verwendung AWS CLI:

Hinweis:

Diese Funktion wird von unterstützt Muster für Discovery und Service-Mapping Version 1.0.96 – Dezember 2022.

Detaillierte Anweisungen finden Sie in der folgenden KB: KB1182188: EKS-Cluster-Discovery mit STS AssumeRoles (ohne AWS CLI)

3. Navigieren Sie zu `sys_properties.list`, und konfigurieren Sie die folgenden Eigenschaften:

- *sn_itom_pattern.k8s_midserver*: Geben Sie ein gültiges an MID-Server Name.
- *sn_itom_pattern.k8s_create_schedule_enabled*: Legen Sie den Wert auf **true** fest.

Hinweis: Aktivieren von *sn_itom_pattern.k8s_create_schedule_enabled*Die Eigenschaft erstellt automatisch einen serverlosen Zeitplan für Ihre Cloud-Cluster, wodurch keine manuelle Planung erforderlich ist. Wenn Sie einen vorhandenen manuellen Zeitplan haben und ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. Es wird kein zusätzlicher Zeitplan erstellt.

4. Erstellen Sie den AWS Cloud Discovery-Zeitplan, und führen Sie diesen aus.

Für Microsoft Azure Kubernetes Services (AKS) – Kubernetes Führen Sie die Cluster-Discovery wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktualisieren Sie auf den neuesten Muster für Discovery und Service-Mapping Version.
2. In ServiceNow-Instanz konfigurieren Azure Service-Account mit gültig Azure Anmeldeinformationen und Berechtigung.
3. Navigieren Sie zu sys_properties.list, und konfigurieren Sie die folgenden Eigenschaften:
   - *sn_itom_pattern.k8s_midserver*: Geben Sie ein gültiges an MID-Server Name.
   - *sn_itom_pattern.k8s_create_schedule_enabled*: Legen Sie den Wert auf **true** fest.

     Hinweis: Aktivieren von *sn_itom_pattern.k8s_create_schedule_enabled*Die Eigenschaft erstellt automatisch einen serverlosen Zeitplan für Ihre Cloud-Cluster, wodurch keine manuelle Planung erforderlich ist. Wenn Sie einen vorhandenen manuellen Zeitplan haben und ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. Es wird kein zusätzlicher Zeitplan erstellt.

   an.
4. Wenn Sie keine lokalen Accounts bei haben Kubernetes RBAC und um die Mustereffizienz zu verbessern, navigieren Sie zu **MID-Server** > **Eigenschaften** Und legen Sie fest *sn_itom_pattern.aks_fetch_local_ad_token*Eigenschaft bis **Falsch** .
5. Führen Sie einen aus Azure Cloud-Discovery-Zeitplan.
6. Konfigurieren Sie MID-Server In Discovery Plant entsprechend dem Cluster-Account-Typ. Wenn Sie keine lokalen Accounts bei RBAC haben, können Sie diesen Schritt ignorieren.

Cluster-Account-Typ	Discovery Zeitplan MID-Server
Ms Entra ID-Authentifizierung mit Kubernetes RBAC.	Beliebig MID-Server.
Ms Entra ID-Authentifizierung mit Azure RBAC.	Beliebig MID-Server.
Lokale Accounts mit Kubernetes RBAC.	Wählen Sie aus MID-Server Mit Azure Befehlszeilenschnittstelle (CLI) konfiguriert. Konfigurieren von Azure CLI-Anmeldeinformationen gewähren Zugriff auf den AKS-Cluster. Zum Abrufen des Bearer-Tokens während der Ausführung von AKS Kubernetes Planen, verwenden Sie Azure CLI-Befehl: az AES get-credentials --Name <cluster_name>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cluster-Account-Typ	Discovery Zeitplan MID-Server
	`--overwrite-existing --resource-Group <resourceGroup_name> --file -` .

Hinweis:

- Der beim System angemeldete Anwender muss mit identisch sein MID-Server Anwender.
- Detaillierte Informationen zur Konfiguration der AKS-Cluster-Discovery finden Sie unter Konfigurationsdetails für AKS-Cluster-Discovery [KB1220553] artikel in Now Support Knowledge Base.

Andere unterstützte Systemkonfiguration

	Eigenschaftsname	Eigenschaftsbeschr	Typ	Standardwert
	sn_itom_pattern.manifest_digest_image_ID		Boolean	falsch **Hinweis:** Bevor Sie diese Eigenschaft auf festlegen **Wahr** Und Discovery wird ausgeführt: Verhindern Sie, dass doppelte Datensätze erstellt werden, indem Sie alle löschen Docker Bilddatensätze.
	sn_itom_pattern.k8s_create_schedule_enabled	Die Funktionskennzeichnung, die unter den Systemeigenschaften aktiviert/ deaktiviert werden kann, die für die Steuerung der Musterausführung verantwortlich ist. Wenn diese Option aktiviert ist, werden Discovery-Zeitpläne trotz	Boolean	falsch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschr	Typ	Standardwert
		des neuen Eigenschaftswerts erstellt.		
	sn_itom_k8s_Run_Cloud_Discovery	Wenn diese Eigenschaft aktiviert ist, werden Cloud-k8s-Muster ausgeführt, die k8s-Cluster erkennen, ohne automatische Zeitpläne zu erstellen.	Boolean	falsch
MID-Server	sn_itom_pattern.k8s_cred_alias	[Standard] Beispiel: Gültiger MID-Servername	Zeichenfolge	
	sn_itom_pattern.k8s_cred_alias_MID-Server	[Basierend auf Service-Account-Ebene] Beispiel: Gültiger MID-Servername	Zeichenfolge <service_account_id>_MID-	
	sn_itom_pattern.k8s_cred_alias_MID-Server	[Basierend auf Clustername] Beispiel: Gültiger MID-Servername	Zeichenfolge <service_account_id>_<clustername>_MID-	
	sn_itom_pattern.kubernetes_Collect_Volume	Wenn die Eigenschaft auf festgelegt ist **Wahr** , Die Daten für das Kubernetes-Volume [cmdb_ci_kubernetes_Volume] werden ausgefüllt.	Zeichenfolge	falsch
Anmeldeinformationsalias	sn_itom_pattern.k8s_cred_alias	[Standard]	Zeichenfolge	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschr	Typ	Standardwert
		Beispiel: Aliasname für Anmeldeinformationen		
	sn_itom_pattern.k8s_service_account_id>_alias	[Basierend auf Service-Account-Ebene] Beispiel: Gültiger Aliasname für Anmeldeinformationen.	Zeichenfolge	
	sn_itom_pattern.k8s_service_account_id>_<clustername>_alias	[Basierend auf Clustername] Beispiel: Gültiger Aliasname für Anmeldeinformationen.	Zeichenfolge	
Prometheus-Url	sn_itom_pattern.k8s_prometheusUrl	[Standard] Beispiel: Gültige Prometheus-Url	Zeichenfolge	
	sn_itom_pattern.k8s_service_account_id>_prometheusUrl	[Basierend auf Service-Account-Ebene] Beispiel: Gültige Prometheus-Url	Zeichenfolge	
	sn_itom_pattern.k8s_service_account_id>_<clustername>_prometheusUrl	[Basierend auf Clustername] Beispiel: Gültige Prometheus-URL	Zeichenfolge	
	sn_itom_pattern.k8s_ausführen	[Ausführung des unterstützten Discovery-Zeitplans – täglich, bei Bedarf, Wochentage, Wochenenden, Monat letzter Tag, Kalenderquartalsende]	Zeichenfolge	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschr	Typ	Standardwert
		Beispiel: Täglich		
	sn_itom_pattern.kas_batch_count	[Verbraucht auf die Anzahl der Zeitpläne, die im Batch ausgeführt werden sollen – Standard auf 5 festgelegt] Beispiel – 5 (Anzahl der Zeitpläne, in denen im Batch ausgeführt werden soll)	Ganzzahl	5
	sn_itom_pattern.kas_batch_delay	[Verbraucht die Zeitdifferenz zwischen zwei Batches, die der Wert enthält, in Sekunden] Beispiel: 300 (in Sekunden)	Ganzzahl	
	sn_itom_pattern.kas_run_time	[Verbraucht die aktuelle Zeit für einen Batch nach] Wenn diese Eigenschaft festgelegt ist, können Sie dieselbe verwenden oder unser dynamisches Timing verwenden, das 5 ist Min. Nach dem aktuellen Systemzeitpunkt. Werte enthalten im Format HH:MM:SS	Zeichenfolge	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschr	Typ	Standardwert
		BEISPIEL – 10:11:12 (HH:MM:SS)		

Hinweis: `<service_account_id>` Ist der Name der Account-ID unter Cloud-Service-Accounts. Weitere Informationen finden Sie unter: Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Kubernetes Discovery ohne Anmeldeinformationen oder MID-in-Cluster

Voraussetzungen für Kubernetes Discovery ohne Anmeldeinformationen:

Stellen Sie das containerisiert bereit MID-Server Zu Kubernetes Cluster. Wird Konfiguriert Kubernetes Anmeldeinformationen sind seit unnötig MID-Server In Kubernetes Cluster erkennt den API-Server automatisch und authentifiziert sich.

Konfigurieren von Ausführungsmusterattributen für die Discovery ohne Anmeldeinformationen

Feld	Beschreibung
URL	Geben Sie einen beliebigen der folgenden Werte in das URL-Feld ein: https://cluster Oder https://kubernetes.default.svc
namespace	Die Namespaces, die das System in übergibt Kubernetes Discovery-Konfiguration. Geben Sie einen der folgenden Werte ein: • Individueller Namespace: Geben Sie den Namespace und dann „kube-System“ ein. Beispiel: `dev,kube-System` • Der Standardwert. Eingabe: `Standard,kube-System` • Multipile-Namespaces: Geben Sie die Namespaces ein, trennen Sie die Werte durch ein Komma (,), und geben Sie dann „kube-System“ ein. Beispiel: `Automatisierung,Anwendung,Test,Kube-System` • Alle Namespaces: Verwenden Sie ein Sternchen (*), um alle Namespaces einzugeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren von Ausführungsmusterattributen für die Discovery ohne Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
cluster_name	Geben Sie einen eindeutigen Namen ein.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]	
Name	Der Name des kube-Controller-Manager-Leader
K8s_uid	Die Kube-System-Namespace-UID [unterstützte Versionen: 1.0.92 und höher]
ip_address	Der Bezeichner für Host_ip des Kubernetes Apiserver.
port	Der Bezeichner für Kubernetes Apiserver-Port.
namespace	Dieser Wert zeigt die Namespaces an, die das System in übergeben hat Kubernetes Discovery-Konfiguration.
event_timestamp	Der Zeitstempel des letzten Ereignisses, das für erstellt wurde Kubernetes Cluster zum Zeitpunkt der Discovery.
Kubernetes Knoten [cmdb_ci_kubernetes_node]	Der virtuelle Aspekt von Kubernetes Knoten. Daten, die sich auf den physischen Aspekt von beziehen Kubernetes Knoten wird unter gespeichert Linux Server.
name	Der Name des Kubernetes Knoten. Das Format kann nur der Name des Computers oder der vollständige Name sein, der aus dem Namen und dem Hostnamen besteht: <name>.<hostname>.
k8s_uid	Der Bezeichner für Kubernetes Knoten-UUID.
Cluster	Der Name des Clusters, der diese Ressource enthält.
operational_status	Der Betriebsstatus des Kubernetes Knoten.
Kubernetes Service [cmdb_ci_kubernetes_Service]	
name	Der Name des Kubernetes Service.
Auswahl	Eine kommagetrennte Liste der in angegebenen Bezeichnungsauswahlen Kubernetes Konfiguration, die zum Auswählen von Ziel-Pods verwendet wird.
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Service gehört.
k8s_uid	Die Kubernetes Service-UUID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Cluster	Der Name des Clusters, der diese Ressource enthält.
Kubernetes Pod [cmdb_ci_kubernetes_Pod]	
name	Der Name des Kubernetes Pod.
k8s_uid	Die Kubernetes Pod-UUID.
resourceVersion	Die Ressourcenversion von Kubernetes Pod.
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Pod gehört.
Cluster	Der Name des Clusters, der diese Ressource enthält.
Status	Die Kubernetes Pod-Status: Ausstehend, wird ausgeführt, erfolgreich, Fehlgeschlagen, und Unbekannt.
Kubernetes Cronjob [cmdb_ci_kubernetes_cronjob]	
name	Der Name des Kubernetes Cronjob
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Pod gehört.
k8s_uid	Die Kubernetes Cronjob-UUID.
Cluster	Der Name des Clusters, der diese Ressource enthält.
Kubernetes Auftrag [cmdb_ci_kubernetes_Job]	
name	Der Name des Kubernetes Auftrag
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Auftrag gehört.
k8s_uid	Die Kubernetes Auftrags-UUID
Cluster	Der Name des Clusters, der enthält Kubernetes Auftrag.
Kubernetes Daemonset [cmdb_ci_kubernetes_Daemonset]	
name	Der Name des Kubernetes Daemonset.
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Daemonset gehört.
k8s_uid	Die Kubernetes Daemonset-UUID.
Cluster	Der Name des Clusters, der diese Ressource enthält.
Pods_Avail	Die Anzahl der verfügbaren Pods.
Pods_failed	Die Anzahl der Pods in der fehlgeschlagenen Phase.
Pods_Running	Die Anzahl der Pods in der laufenden Phase.
Pods_successful	Die Anzahl der Pods in der erfolgreichen Phase.
Pods_Warten	Die Anzahl der Pods in der Wartephase.
Kubernetes Eingangsspannung [cmdb_ci_kubernetes_ingress]	
name	Der Name des Kubernetes Eingehend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Eingang gehört.
k8s_uid	Die Kubernetes Eingehende UID
Cluster	Der Name des Clusters, der diese Ressource enthält.
Kubernetes Bereitstellung [cmdb_ci_kubernetes_Deployment] Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset] Kubernetes Replikations-Controller [cmdb_ci_kubernetes_replicationController] Kubernetes Statussatz [cmdb_ci_kubernetes_statefulset]	
name	Der Name dieser Ressource
namespace	Die Kubernetes Namespace, zu dem diese Ressource gehört.
K8s_uid	Die Kubernetes UID dieser Ressource
Cluster	Der Name des Clusters, der diese Ressource enthält.
total_replicas	Anzahl der Replikate in dieser Ressource
desired_replicas	Die Anzahl der Replikate in der gewünschten Phase
available_replicas	Anzahl der verfügbaren Replikate
unavailable_replicas	Anzahl der Replikate in nicht verfügbarer Phase
updated_replicas	Anzahl der aktualisierten Replikate
Docker-Container [cmdb_ci_docker_container]	Die Komponente, die das Docker-Image ausführt
container_id	Der eindeutige Bezeichner für Kubernetes docker-Container In Fällen, in denen doppelte Datensätze erstellt werden, werden Deduplizierungsaufgaben angezeigt, sobald die Discovery ausgeführt wird. Informationen zur Lösung dieser Aufgaben finden Sie unter Docker-Container-Bezeichner unabhängig machen [KB1443042] artikel in ServiceNow® Knowledge Base.
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes docker-Container gehört
Docker-Image [cmdb_ci_docker_image]	Ein ausführbares Paket einer Anwendung und der zugehörigen Software, das von einem Docker-Container instanziiert werden kann
image_id	Der Bezeichner für Kubernetes docker-Image
name	Der Name des Kubernetes docker-Image.
image_url	Die URL für das Herunterladen des Docker-Image.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes docker-Image gehört.
Linux-Server [cmdb_ci_linux_server]	Der Server, der hostet Kubernetes Knoten.
name	Der Name des Linux-Servers, auf dem die ausgeführt wird Kubernetes Knoten.
hostname	Der Hostname des Linux-Servers
os	Das auf diesem Linux-Server bereitgestellte Betriebssystem
kernel_release	Die Version des auf diesem Linux-Server bereitgestellten Linux-Kernel-Betriebssystems.
ram	Die Größe des auf diesem Linux-Server installierte RAM.
ip_address	Die IP-Adresse des Linux-Servers
Schlüsselwert [cmdb_key_value]	Dieses Konfigurationselement enthält Kubernetes Bezeichnungen. Bezeichnungen sind Schlüssel/Wert-Paare, die an Objekte wie Pods angehängt werden.
key	Der Schlüssel von Kubernetes Pod oder Kubernetes Service `Key Value`Parameter.
Wert	Der Wert von Kubernetes Pod oder Kubernetes Service `Key Value`Parameter.
Kubernetes Volume [cmdb_ci_kubernetes_Volume]	
k8s_uid	Die Kubernetes Volume-UUID.
mount_path	Der Pfad für den Zugriff darauf Kubernetes Volume.
name	Der Name des Kubernetes Volume.
namespace	Die Kubernetes Namespace, für den dies gilt Kubernetes Volume gehört.
Cluster	Der Name des Clusters, der diese Ressource enthält.
volume_id	Die ID des Kubernetes Volume.
OpenShift Bereitgestellte Konfiguration [cmdb_ci_openshift_dep_conf]	
name	Der Name des OpenShift Bereitstellungskonfiguration.
namespace	Der Name des Namespace, der die Bereitstellungskonfiguration enthält
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Bereitgestellte Konfiguration, nur verfügbar für Kubernetes Versionen vor 1,16.
OpenShift Build-Konfiguration [cmdb_ci_openshift_build_conf]	
name	Der Name des OpenShift Build-Konfiguration.
namespace	Der Name des OpenShift Namespace, der die Build-Konfiguration enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
k8s	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Build-Konfiguration, nur verfügbar für Kubernetes Versionen vor 1,16.
OpenShift Source2Image [cmdb_ci_openshift_Source_2_image]	
name	Der Name des OpenShift-Quell-Image
bis	Zugehöriges Image
parent_id	Die ID des OpenShift Quellbild.
OpenShift Route [cmdb_ci_openshift_Route]	
name	Der Name des OpenShift Route.
namespace	Der Name des Namespace, der den enthält OpenShift Route.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Route, nur verfügbar für Kubernetes Versionen vor 1,16.
host	Der Zielhost von OpenShift Route.
port	Der Zielport des OpenShift Route.
OpenShift Gruppe [cmdb_ci_openshift_Group]	
name	Der Name des OpenShift Gruppe.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Gruppe, nur verfügbar für Kubernetes Versionen vor 1,16.
OpenShift Anwender [cmdb_ci_openshift_user]	
name	Der Name des OpenShift Anwender.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Anwender, nur verfügbar für Kubernetes Versionen vor 1,16.
full_name	Der vollständige Name des OpenShift Anwender.
OpenShift Projekt [cmdb_ci_openshift_project]	
name	Der Name des OpenShift Projekt.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Projekt, nur verfügbar für Kubernetes Versionen vor 1,16.
OpenShift Bild [cmdb_ci_openshift_images]	
name	Der Name des OpenShift Bild.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Bild, nur verfügbar für Kubernetes Versionen vor 1,16.
docker_image_metadata_id	Die ID des Docker-Image

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
docker_image_metadata_parent_id	Die ID der übergeordneten ID des Image
arch	Architektur des Image
size	Die Image-Größe
hostname	Der dem Image zugeordnete Host-Name
OpenShift Image-Stream [cmdb_ci_openshift_images_Stream]	
name	Der Name des OpenShift Image-Stream.
k8s_uid	Die Kubernetes Volume-UUID.
URL	Die URL des OpenShift Image-Stream, nur verfügbar für Kubernetes Versionen vor 1,16.
namespace	Der Name des Namespace, der den enthält OpenShift Image-Stream.
OpenShift Docker-Image-Repository [cmdb_ci_openshift_Docker_images_Repository]	
name	Der Name des OpenShift docker-Image-Repository.
parent_ID	Die ID des übergeordneten Systems
Namespace [cmdb_ci_kubernetes_Namespace]	
name	Der Name des Kubernetes Namespace.
Status	Die Kubernetes Namespace-Phasen: Aktiv oder wird beendet.

Diese Daten werden vom Erweiterungsabschnitt *`Collect Container Repository`* erfasst.

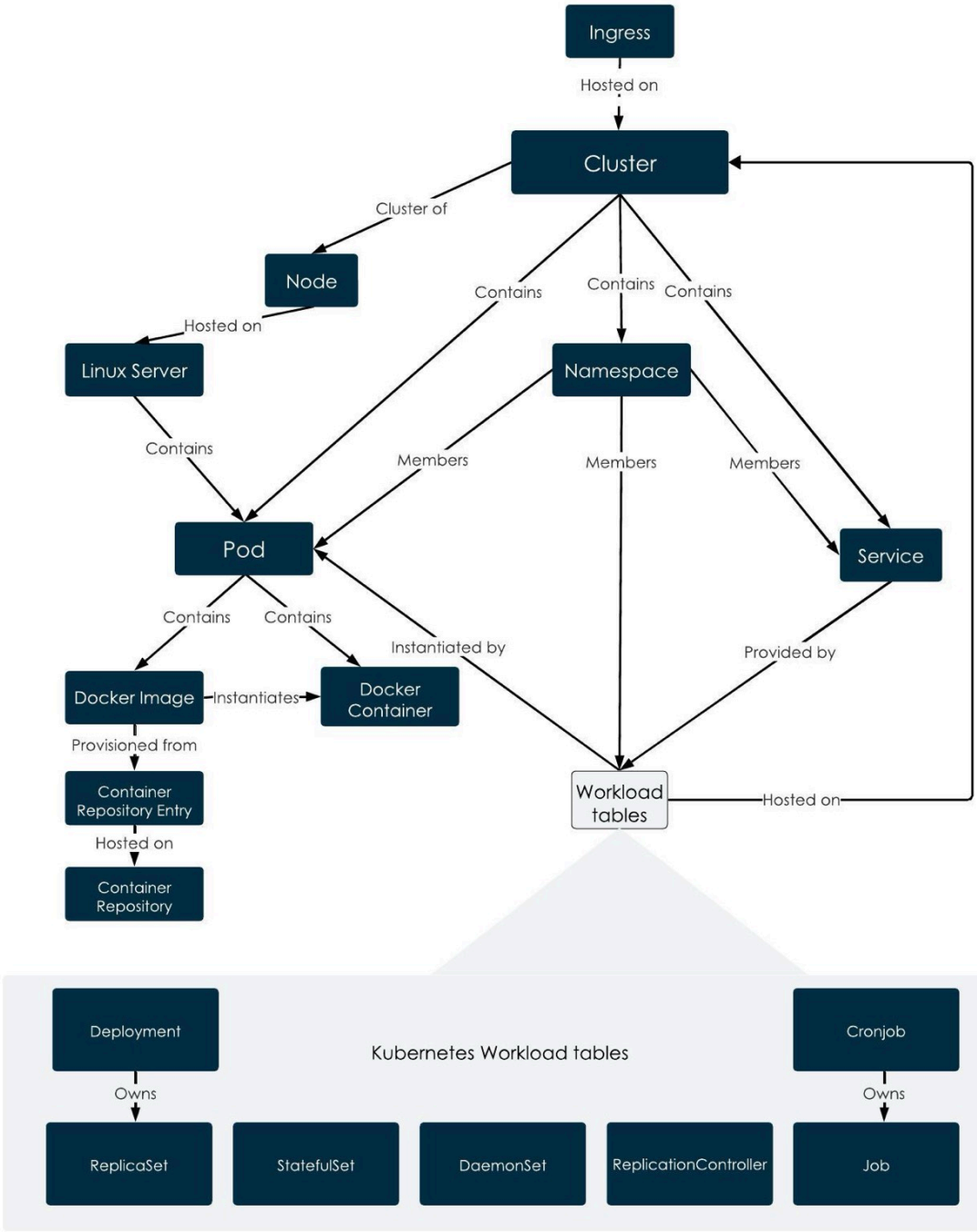
Tabelle und Feld	Beschreibung
Container-Repository [cmdb_ci_container_repository]	
Name [name]	Der Name des Container-Repositorys.
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	
Name [name]	Der Name des Container-Repository-Eintrags.
Kategorie [category]	Die Kategorie des Container-Repository-Eintrags.

Die Grafik zeigt CIs, die Teil von sind Kubernetes Discovery.

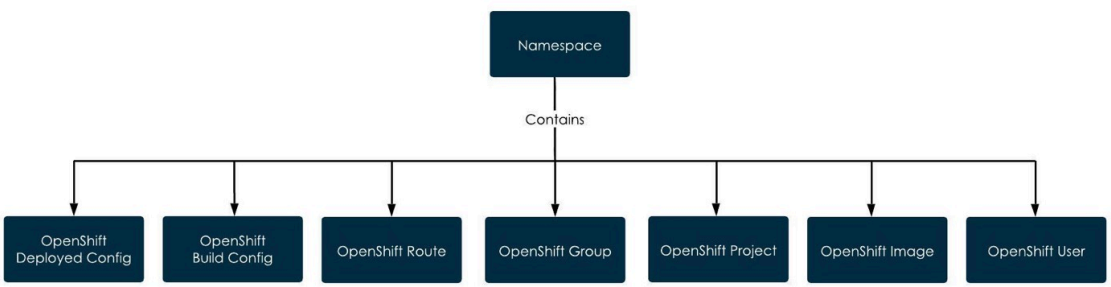
Hinweis: Diese Abhängigkeitsansichten-Zuordnung wurde der Übersichtlichkeit halber vereinfacht. Ihr Kubernetes Bereitstellungen können viele weitere CIs enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten von Kubernetes Bereitstellung



Komponenten von Kubernetes Bereitstellung einschließlich OpenShift



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom Muster „Kubernetes“ erfasste CI-Beziehungen

Diese Beziehungen werden von erstellt Kubernetes Muster :

CI	Beziehung	CI
Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]	Enthält::Enthalten in	Kubernetes Service [cmdb_ci_kubernetes_Service]
	Enthält::Enthalten in	Kubernetes Pod [cmdb_ci_kubernetes_Pod]
	Enthält::Enthalten in	Kubernetes Eingangsspannung [cmdb_ci_kubernetes_ingress]
	Enthält::Enthalten in	Kubernetes Namespace [cmdb_ci_kubernetes_Namespace]
	Enthält::Enthalten in	[cmdb_ci_openshift_source_2_image]
	Enthält::Enthalten in	OpenShift Gruppe [cmdb_ci_openshift_Group]
	Enthält::Enthalten in	OpenShift Anwender [cmdb_ci_openshift_user]
	Enthält::Enthalten in	OpenShift Projekt [cmdb_ci_openshift_project]
	Enthält::Enthalten in	OpenShift Bild [cmdb_ci_openshift_images]
	Enthält::Enthalten in	OpenShift Docker-Image-Repository [cmdb_ci_openshift_Docker_images_Repository]
	Cluster von::Cluster	Kubernetes Knoten [cmdb_ci_kubernetes_node]
	Verwaltet::Verwaltet von	Linux-Server [cmdb_ci_linux_server]
	Enthalten in::Enthält	Ressourcengruppe [cmdb_ci_resource_group]
Kubernetes Pod [cmdb_ci_kubernetes_Pod]	Enthält::Enthalten in	Docker-Container [cmdb_ci_docker_container]
	Enthält::Enthalten in	Docker-Image [cmdb_ci_docker_image]
	Enthält::Enthalten in	Kubernetes Volume [cmdb_ci_kubernetes_Volume]
Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_Workload]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Kubernetes-Service [cmdb_ci_kubernetes_service]	Stellt Bereit::Bereitgestellt Von	Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_Workload]
Kubernetes-Bereitstellung [cmdb_ci_kubernetes_deployment]	Besitzt::Im Besitz Von	Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset]
Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset]	IInstantiates:: Instanziiert von	Kubernetes Pod [cmdb_ci_kubernetes_Pod]
Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_Workload]	Bereitgestellt von::Stellt bereit für	Kubernetes Service [cmdb_ci_kubernetes_Service]
Kubernetes Bereitstellung [cmdb_ci_kubernetes_Deployment]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]
Kubernetes Daemonset [cmdb_ci_kubernetes_Daemonset]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]
Kubernetes Statussatz [cmdb_ci_kubernetes_statefulset]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]
Kubernetes Namespace [cmdb_ci_kubernetes_Namespace]	Enthält::Enthalten in	OpenShift Bereitgestellte Konfiguration [cmdb_ci_openshift_dep_conf]
	Enthält::Enthalten in	OpenShift Build-Konfiguration [cmdb_ci_openshift_build_conf]
	Enthält::Enthalten in	OpenShift Route [cmdb_ci_openshift_Route]
	Enthält::Enthalten in	OpenShift Image-Stream [cmdb_ci_openshift_images_Stream]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]
Linux-Server [cmdb_ci_linux_server]	Enthält::Enthalten in	Kubernetes Pod [cmdb_ci_kubernetes_Pod]
	Wird ausgeführt:Wird ausgeführt auf	Docker-Container [cmdb_ci_docker_container]
	Hostet::Gehostet auf	Kubernetes Knoten [cmdb_ci_kubernetes_node]
OpenShift Bereitstellungskonfiguration [cmdb_ci_openshift_dep_conf]	Enthält::Enthalten in	[cmdb_ci_config_file_tracked]

Der Erweiterungsabschnitt *`Collect Container Repository`* des Kubernetes-Musters identifiziert diese Beziehungen.

CI	Beziehung	CI
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]

CI-Beziehungen, die von der Istio Service Mesh-Erweiterung erfasst werden

Voraussetzungen für die Istio Service Mesh-Erweiterung:

- Stellen Sie sicher, dass Istio Service Mesh- und Prometheus-Komponenten auf konfiguriert sind Kubernetes Cluster.
- Stellen Sie sicher, dass Prometheus die Serviceverbindungsinformationen mit erkennt `Queryistio_Requests_total` Befehl.
- Stellen Sie sicher, dass die Anwendungsservices verbunden sind, und überprüfen Sie den Service-to-Service-Datenverkehr-Flow im Kiali-Diagramm.

Weitere Informationen zur Anwendung Bookinfo finden Sie unter: https://istio.io/latest/docs/examples/bookinfo/

CI	Beziehung	CI
Kubernetes Service [cmdb_ci_kubernetes_Service]	Stellt eine Verbindung her mit::Connected by	Kubernetes Service [cmdb_ci_kubernetes_Service]

CI-Beziehungen, die von erfasst wurden Kubernetes Ereignismuster

Diese Beziehungen werden zur Unterstützung von erstellt Kubernetes Ereignis-Discovery:

CI	Beziehung	CI
Kubernetes Cluster [cmdb_ci_kubernetes_Cluster]	Enthält::Enthalten in	Kubernetes Service [cmdb_ci_kubernetes_Service]
	Enthält::Enthalten in	Kubernetes Pod [cmdb_ci_kubernetes_Pod]
	Cluster von::Cluster	Kubernetes Knoten [cmdb_ci_kubernetes_node]
	Verwaltet::Verwaltet von	[cmdb_ci_linux_server]
Kubernetes Pod [cmdb_ci_kubernetes_Pod]	Enthält::Enthalten in	Docker-Container [cmdb_ci_docker_container]
	Enthält::Enthalten in	Docker-Image [cmdb_ci_docker_image]
	Enthält::Enthalten in	Kubernetes Volume [cmdb_ci_kubernetes_Volume]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]
Linux-Server [cmdb_ci_linux_server]	Enthält::Enthalten in	Kubernetes Pod [cmdb_ci_kubernetes_Pod]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Wird ausgeführt:Wird ausgeführt auf	Docker-Container [cmdb_ci_docker_container]
	Hostet::Gehostet auf	Kubernetes Knoten [cmdb_ci_kubernetes_node]

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping Verwendet die Tag-basierte Discovery, um Anwendungsservicezuordnungen einschließlich zu erstellen Kubernetes Komponenten. Service-Mapping Enthält die folgenden vorkonfigurierten CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Kubernetes-Service [cmdb_ci_kubernetes_service]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
OpenShift-Projekt [cmdb_ci_openshift_project]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Cluster::Cluster von	Kubernetes-Service [cmdb_ci_kubernetes_service]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	Bereitgestellte OpenShift-Konfiguration [cmdb_ci_openshift_dep_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Buildkonfiguration [cmdb_ci_openshift_build_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Route [cmdb_ci_openshift_route]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Image-Stream [cmdb_ci_openshift_images_stream]

Kubernetes-Dashboard

Nach Discovery Schließt die Erkennung von Komponenten von ab Kubernetes Bereitstellung, Sie Kann zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Und verwenden Kubernetes Explorer Dashboard zum Anzeigen von Kubernetes Umgebungen und Ressourcen Ihrer Organisation. Zur Verwendung von erweitert Kubernetes Dashboard, verifizieren Sie, dass Sie haben Discovery-AdministratorarbeitsbereichBeginnt ab Version 1.3.1 (August 2024 Store) . Weitere Informationen zu Kubernetes Explorer finden Sie unter Kubernetes Explorer.

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

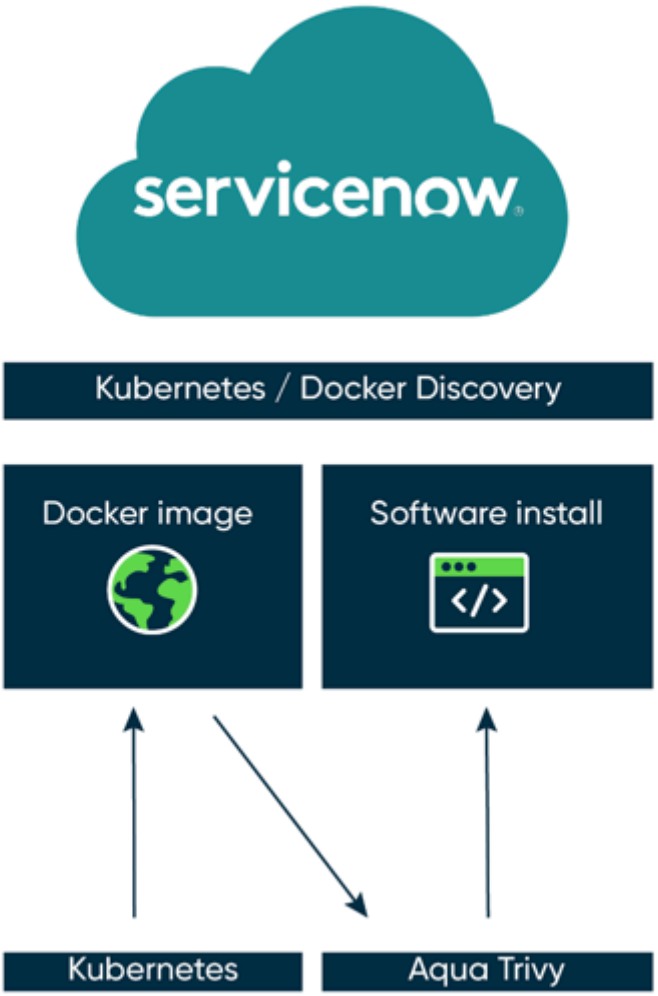
Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zum Ausführen von Kubernetes Muster im Debug-Modus, siehe KB0832567 Für Betriebsinformationen.

Container-Image-Scan für Softwareaufgliederung

Die ITOM-Transparenz Apps, Muster für Discovery und Service-Mapping Und Kubernetes Transparency Agent werden mit integriert Aqua Trivy Dient zum Sammeln von Daten zu Container-Images und BS-Paketen. Sie können Ihre Kontrolle über die Containerbereitstellung erhöhen, indem Sie Transparenz für die Containerkomponenten haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Vorteile des Bildscans

Durch das Scannen Ihrer Container erhalten Sie Einblick in das, was sich darin befindet Kubernetes Oder Docker Container oder BS-Pakete. Das Scannen von Bildern kann Ihnen auf verschiedene Arten helfen.

- Es hilft Ihnen, Software zu identifizieren, die in Containern für regulatorische und Compliance-Anwendungsfälle installiert ist.
- Es hilft Ihnen, Unternehmensrichtlinien wie die Verwendung von Golden Images, veralteter Software, obligatorischen Bezeichnungen oder Konfigurationsrichtlinieneinzuhalten.
- Außerdem können Sie lizenzierte Software verwalten, die in Containern ausgeführt wird.
- Sie können den Servicekontext auch abrufen, indem Sie Tags und Service-Mesh verwenden, um ihre Auswirkungen auf Ihre Organisation zu verstehen.

Anwendungsfälle für Bildscans mit ITOM-Transparenz

Sie können zwei verwenden ITOM-Transparenz Apps zum Scannen von Containerbildern, Muster für Discovery und Service-Mapping Und Kubernetes Sichtbarkeit-Agent. Muster ist ein Funktionssatz, der von verwendet wird Discovery, Cloud-Discovery, Und Service-Mapping. Kubernetes Sichtbarkeit-Agent ist eine Funktion von Agent Client Collector. Während Kubernetes Für eignet sich der Sichtbarkeit-Agent (früher CNO-V) besser Kubernetes Und dynamische

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

containerisierte Arbeitsauslastungen, ist musterbasierte Discovery besser für nicht-Kubernetes geeignet Docker Container.

Anwendungsfall Nr. 1

Sobald eine Anwendung in Container-Images verpackt wurde, kann ein Sicherheitsexperte das Basis-Image sowie das endgültige Image auf Schwachstellen scannen und BS-Pakete, Softwareabhängigkeiten und Anwendungsdatensätze identifizieren. Dies gilt speziell für den containerisierten MSSQL-Server.

Sichtbarkeitsmethoden für Anwendungsfall Nr. 1

Sichtbarkeitsmethoden	Methodenmerkmale	Was erkannt wurde
Muster für Discovery und Service-Mapping Und Aqua Trivy: • Am besten geeignet für selbst gehostet oder Cloud Kubernetes Bereitstellungen mit Zugriff auf Bearer-Token und Anmeldeinformationen. • Unterstützt das Scannen öffentlicher und selbst gehosteter Repository-Bilder.	• Musterbasierte Discovery ohne Cloud-Discovery: ○ Verwendet ein Bearer-Token. ○ Manuell erstellt Kubernetes Discovery-Zeitplan pro Cluster. • Musterbasierte Discovery mit Cloud-Discovery: ○ Kein Bearer-Token erforderlich. ○ Verwendet Cloud-Anmeldeinformationen. ○ Automatische Erstellung von Kubernetes Discovery-Zeitplan. • Weitere Informationen zum Scannen von Bildern mit Aqua Trivy, Siehe Container-Images scannen.	Erkannt mit Muster für Discovery und Service-Mapping: • Kubernetes Cluster • Kubernetes Services • Kubernetes Topologie • Docker Container und Images • Kubernetes Bereitstellung einschließlich OpenShift • Namespace • Bezeichnungen und Tags • Software in Containern • Details zur Account-Region können nur von erkannt werden Cloud-Discovery • Docker-Muster erfasst Daten zu bestimmten Objekten in einer Docker-Engine, die auf einem Linux-Host ausgeführt wird Weitere Informationen finden Sie unter: • Container-Image-Discovery • Kubernetes Discovery mithilfe von Mustern • Docker-Virtualisierung
Kubernetes Sichtbarkeit Agent und Aqua Trivy:	Kubernetes Die auf Sichtbarkeit Agent basierende Discovery	Erkannt mit Kubernetes Sichtbarkeit-Agent

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtbarkeitsmethoden für Anwendungsfall Nr. 1 (Fortsetzung)

Sichtbarkeitsmethoden	Methodenmerkmale	Was erkannt wurde
• Am besten geeignet für die Bereitstellung durch Cloud-native App-Teams. • Optionale Fähigkeit zur Überwachung Kubernetes Mit AIOps. • Für Cloud-Umgebungen wird nur AWS ECR (öffentlich und privat) unterstützt.	erfordert keine Einrichtung von Anmeldeinformationen und ist nicht erforderlich MID-Server. Zugriff erfolgt über ServiceAccount/ ClusterRole. Die Installation erfolgt über Helm Chart oder Kubernetes YAML-Datei. Die Discovery wird nahezu in Echtzeit ausgeführt. Verwenden Kubernetes Explorer zum Herunterladen SBOM.	• Kubernetes Namespaces • Knoten und Pods • Bereitstellungen • Statussätze • Daemonsets • Replikatsätze • Aufträge • Cronjobs • Services • Docker Container • Docker-Bild • Container-Repository • Details zur Account-Region können nur von erkannt werden Cloud-Discovery

Anwendungsfall 2

Ein Compliance-Beauftragter kann einen generieren SBOM#Um eine detaillierte Liste der Abhängigkeiten des Container-Images zu erhalten und sicherzustellen, dass die Software den Branchenvorschriften entspricht.

Sichtbarkeitsmethoden für Anwendungsfall Nr. 2

Sichtbarkeitsmethode	Methodenmerkmale
Kubernetes Muster oder Docker Muster	SBOM Die Erstellung ist Teil des Container-Scans.
Kubernetes Sichtbarkeit-Agent	SBOM Die Erstellung ist auch Teil des Container-Scans, Die Verwendung von ACC ist jedoch am besten für Organisationen geeignet, die Flexibilität benötigen, um sowohl eine vollständige als auch eine kontinuierliche Discovery durchzuführen.

Anwendungsfall Nr. 3

Ein Techniker hat einen Fehler in einem anwenderdefinierten Image gefunden und muss alle finden Kubernetes Pods, die mit diesem Image ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtbarkeitsmethoden für Anwendungsfall Nr. 3

Sichtbarkeitsmethode	Methodenmerkmale	Was erkannt wurde
Kubernetes pattern	Aqua Trivy Container-Scan ist nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	• Kubernetes Cluster • Kubernetes Container • Kubernetes Services • Bezeichnungen • Pods • Images • Tags
Kubernetes Muster mit Cloud-Discovery	Aqua Trivy Container-Scan ist nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	Alle oben genannten und Account- oder Regionsdetails

Anwendungsfall 4

Ein Techniker findet einen Fehler in einem anwenderdefinierten Image und muss alle finden Docker Container (nicht Kubernetes), die mit diesem Image ausgeführt werden.

Sichtbarkeitsmethode	Methodenmerkmale	Was erkannt wurde
Horizontale Discovery der ausgeführten VM Docker(Docker Muster)	Aqua Trivy Container-Scan ist nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	Siehe: Docker-Virtualisierung

Bildscannen mit Muster für Discovery und Service-Mapping

Kubernetes Und Docker Muster werden in integriert Aqua Trivy Führen Sie geplante Aufgaben durch, um Container-Images und BS-Pakete in festen Intervallen von 10 Images pro Minute zu erkennen. Während des Scans zeigt das Muster den Scanstatus an. Das Muster erkennt BS-Pakete, die sich auf ein Image beziehen. Anschließend werden die Image-Befehlsattribute wie die CI-Klasse gefunden. Basierend auf den Befehlsattributen erstellt das Muster Anwendungsdatensätze. Darüber hinaus verwendet das Muster angereicherte Skripts, um den Anwendungsdatensätzen Details hinzuzufügen. Danach ordnet das Muster die Beziehungen zwischen den BS-Paketen und den Containern zu.

Ein Teil der Daten wird in ausgefüllt CMDB Tabellen und ein Teil davon in Transformationstabellen (nicht-CMDB-temporäre Tabellen). Die Transformationstabellen werden mit dem Muster installiert. Zum Beispiel umfassen die Informationen, die Sie durch das Scannen erhalten, die Ursprungsregistrierung, den Softwarenamen und die Version.

Zugehörige Informationen

Cloud Native Operations für Transparenz

Verknüpfen Sie Softwarepaketinformationen nur mit Images

Verknüpfen Sie Softwarepaketinformationen mit Images anstatt mit Containern, um zu vermeiden, dass leere Datensätze mit kurzlebigen Containern verknüpft werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Softwarepaketinformationen werden mit Images und Containern verknüpft, wenn der verwendet wird *sn_itom_pattern.image_scan_process_container*Die Systemeigenschaft ist auf den Standardwert von festgelegt **Wahr** . Um diese Daten nur mit Bildern zu verknüpfen, legen Sie den Eigenschaftswert auf fest **Falsch** .

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. In **Name** Feld, suchen Sie nach sn_itom_pattern.image_Scan_Process_Container .
3. Wählen Sie die Eigenschaft *sn_itom_pattern.image_scan_process_container* aus.
4. In **Wert** Feld eingeben Falsch .
5. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Container-Images scannen

Container-Image-Discovery

Container-Images scannen

Aktivieren Sie das Scannen von Containerbildern mit Aqua Trivy Tool.

Vorbereitungen

Hinweis: Das Muster unterstützt nur das Linux-Betriebssystem und wird unter Linux ausgeführt MID-Server.

Überprüfen Sie das folgende Setup:

- Muster für Discovery und Service-Mapping, Ab 1.7.0 (Store-Release August 2023).
- CMDB CI-Klassenmodelle, Ab 1.43.0.
- Visibility Content, Ab 6,7.2.
- Damit der Scan der Container-Images erfolgreich ausgeführt wird, überprüfen Sie, ob alle vorhanden sind MID Servers Sind in Ihrer Umgebung für bestimmte Fähigkeiten konfiguriert und nicht auf festgelegt **Alle** . Weitere Informationen zum Konfigurieren von Fähigkeiten finden Sie unter MID-Server-Fähigkeiten .
- MID-Server Anforderungen:
  - 8 GB RAM MIT 4 GB JVM
  - MID-Server **Fähigkeit** Konfiguriert für **Container-Images Scannen**
  - Kann auf das Image-Repository zugreifen
- Aqua Trivy Ab 0.44.0 ist auf installiert MID-Server. Die letzte validierte Version ist 0.51.0. Weitere Informationen zur Installation von finden Sie Aqua Trivy, Siehe Übersicht über die Funktion „Container-Bild-Scan“ [KB1218504] artikel in Now Support Knowledge Base.
- Zum Sammeln Docker Oder Kubernetes Container-Image- und Umgebungsdatensätze, müssen Sie zuerst ausführen Docker Oder Kubernetes Discovery, bevor die Funktion „Container-Image-Scan“ aktiviert wird. Weitere Informationen finden Sie unter Kubernetes Discovery mithilfe von Mustern und Docker-Virtualisierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beginnend mit Muster für Discovery und Service-Mapping Version 1.18.0 unterstützt die Funktion „Container Image Scan“ auch Folgendes:
  - Mit einem Proxy MID-Server Zum Scannen der Container-Images in den folgenden Repositorys: Öffentlich, selbst gehostet privat und Amazon Elastische Container-Registrierung (Amazon ECR)-Repositorys. Dient zur Verwendung eines Proxy MID-Server, Stellen Sie sicher, dass MID-Server Proxy-Parameter sind korrekt konfiguriert. Weitere Informationen finden Sie unter MID-Server-Parameter .
  - Container-Images werden in selbst gehosteten privaten Repositorys gescannt. Um diese Repositorys zu scannen, müssen Sie Anmeldeinformationen für das Container-Image-Repository erstellen. Weitere Informationen finden Sie unter Anmeldeinformationen erstellen und testen und Anmeldeinformationen für Container-Image-Repository .
  - Bilderdatensätze werden aus erfasst Amazon ECR in öffentlichen und privaten Repositorys. Um diese zu erfassen Amazon ECR-Bilddatensätze, müssen Sie zuerst ausführen Amazon ECS-Ressourcen-Discovery, bevor der Container-Image-Scan aktiviert wird. Die AWS Cloud-Service-Account für erstellt Amazon Die ECS-Ressourcen-Discovery wird auch für den Container-Image-Scan verwendet. Weitere Informationen zu finden Amazon ECS-Ressourcen-Discovery, siehe Amazon ECS-Ressourcen-Discovery mit Mustern.
- Ab Version 1.27.0 Muster für Discovery und Service-Mapping Mit können Sie steuern, ob Softwarepakete mit Containern oder nur mit Images verknüpft werden sollen. Weitere Informationen finden Sie unter Verknüpfen Sie Softwarepaketinformationen nur mit Images.

Erforderliche Rolle: Administrator

Prozedur

1. Aktivieren Sie Muster für Discovery und Service-Mapping Container-Image-Scan durch Festlegen der Systemeigenschaft.
   a. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   b. In **Name** Suchfeld eingeben `sn_itom_pattern.Container_image_Scan` .
   c. Legen Sie den Wert auf fest **Wahr** .
2. Geben Sie in der URL-Leiste Folgendes ein: `<instance>.service-now.com/sn_itom_pattern_container_image_scan_status_list.do` Dient zum Überprüfen des Scanstatus der Bilder.
3. Wählen Sie den Image-Datensatz aus, um die Tabelle „Container-Image-BS-Pakete“ zu überprüfen.

Ergebnis

Das Scan-Container-Image-Muster sucht die Image-BS-Pakete und erstellt Anwendungsdatensätze basierend auf der Image-CI-Klasse. Die Tabelle „Container-Image-BS-Pakete“ befindet sich im Image-Datensatz. Das Muster erstellt auch Beziehungen zwischen den Konfigurationselementen. Weitere Informationen zu den erfassten Daten finden Sie unter Container-Image-Discovery.

Konfigurieren Sie SBOM Generierung

Aktivieren Sie die Software-Stückliste (SBOM) Erstellen und vermeiden Sie, dass doppelte SBOM-Dateien generiert werden, indem Sie die Systemeigenschaften festlegen.

Vorbereitungen

Überprüfen Sie das folgende Setup:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow AI Platform, Mindestens Utah Release
- Muster für Discovery und Service-Mapping Ist aktuell.
- CMDB CI-Klassenmodelle, Ist aktuell.
- Visibility Content Ist aktuell.
- MID-Server Anforderungen: 8 GB RAM mit 4 GB JVM und Scan-Container-Images. Weitere Informationen finden Sie unter Container-Images scannen

Erforderliche Rolle: discovery_admin

Prozedur

1. Wählen Sie aus SBOM Format.
   a. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   b. Auf der **Systemeigenschaften** Liste, suchen Sie nach `sn_itom_pattern.sbom_Format` Und wählen Sie den Datensatz aus.
   c. Legen Sie fest **Wert** Feld im gewünschten Format.
   Die verfügbaren Formate sind:
      - Zyklonedx
      - Spdx-JSON
      - Spdx

      Hinweis: Wert wird auf festgelegt **Keine** Deaktiviert die Erstellung der SBOM.
2. Legen Sie fest *`sys_attachment`* Systemeigenschaft zur Vermeidung von Duplikaten SBOM Dateien aus der Generierung.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**
   b. Auf der **Tabellen** Formular in **Bezeichnung** Feld eingeben `*Anhängen` .
   c. Wählen Sie aus **Anhang** Datensatz.
   d. Wählen Sie aus **Anwendungszugriff** Registerkarte.
   e. Wählen Sie aus **Kann löschen** Kontrollkästchen.
   f. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Laden Sie eine Software-Stückliste herunter (SBOM)

Laden Sie eine Software-Stückliste herunter (SBOM)

Software-Stückliste herunterladen (SBOM), um Transparenz für die Komponenten des Container-Images zu erhalten, z. B. die installierten Betriebssystempakete.

Vorbereitungen

Die SBOM Muss konfiguriert worden sein. Weitere Informationen finden Sie unter Konfigurieren Sie SBOM Generierung.

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter ein `sn_itom_pattern_Container_image_Scan_Status_list.do` .
2. Wählen Sie das Bild aus, für das Sie benötigen SBOM In der Liste Status des Container-Image-Scans. Wenn der Scan-Status lautet **Keine** Statt **Gescannt** , Warten Sie, bis sich der Status ändert, bevor Sie den Bilddatensatz auswählen.
3. Laden Sie herunter SBOM Durch Auswahl von **Herunterladen** In **Verwalten Sie Anhänge** Abschnitt.

Container-Image-Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Scan-Container-Image-Muster zur Erkennung Docker Images und BS-Paketdaten. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Informationen zum Durchführen eines Container-Image-Scans finden Sie unter Container-Images scannen.

Das Scan-Container-Image-Muster unterstützt Aqua Trivy Ab Version 0.44.0. Die letzte validierte Version ist 0.51.0.

Beginnend mit Muster für Discovery und Service-Mapping In Version 1.18.0 unterstützt das Scan-Container-Image-Muster das Scannen von Container-Images in den folgenden Repositorys:

- Öffentliche Repositorys
- Selbst gehostete private Repositorys
- Amazon Elastische Container-Registrierung (Amazon ECR), sowohl öffentliche als auch private Repositorys

Ab Version 1.27.0 Muster für Discovery und Service-Mapping Mit können Sie steuern, ob Softwarepakete mit Containern oder nur mit Images verknüpft werden sollen. Weitere Informationen finden Sie unter Verknüpfen Sie Softwarepaketinformationen nur mit Images.

Daten erfasst von Discovery Für Container-Image-Scans

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Container-Image scannen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendungstabelle [cmdb_ci_appl]	
Name [name]	Name der Containeranwendung. Erforderliches Namensformat des MSSQL-Anwendungsdatensatzes: ApplicationTableName@ContainerName Beispiel: MSFT SQL Instance@/sql1
Tabelle der Container-Umgebungsvariablen [cmdb_Container_Environment_variables]	
Container [Container]	Name des Containers.
Schlüssel [key]	Name der Container-Umgebungsvariablen.
Wert [value]	Wert der Container-Umgebungsvariablen.

Temporäre Tabellen für Container-Image-Scans

Hinweis: Wenn Sie die Version 1.0.98 zum Sammeln der Daten verwenden, werden die angereicherten Skripts nur mit MSSQL unterstützt.

Während der horizontalen Erkennung erfasste Daten

Feld	Beschreibung
Scan-Status des Containerbilds [sn_itom_pattern_Container_image_Scan_Status]	
Bild [image]	Name des Container-Images.
Nachricht [Nachricht]	Fehler oder Probleme beim Scanvorgang.
CI-Klasse [ci_class]	Die Image-CI-Klasse basierend auf den Image-Befehlsdetails.
Discovery-Status [Discovery_Status]	Der Discovery-Statusdatensatz des Image-Scans.
Scan-Status [Scan_Status]	Der Scan-Status. Verfügbare Werte: • Keine: Das Bild wurde noch nicht gescannt. • In Bearbeitung: Der Bildscan wird ausgeführt. **Hinweis:** Wenn ein oder mehrere Bilder ausgeführt werden, wird der nächste Scan nicht ausgelöst. • Gescannt: Das Bild wurde erfolgreich gescannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der horizontalen Erkennung erfasste Daten (Fortsetzung)

Feld	Beschreibung
	• Fehler: Während des Bildscans ist Ein Problem aufgetreten. Details finden Sie in der Nachrichtenspalte. • Übersprungen: Die Bild-URL ist nicht ordnungsgemäß formatiert oder nicht erreichbar.
Tabelle „Container-Image-BS-Pakete“ [sn_itom_pattern_Container_image_os_Packages]	
Bild [image]	Name des Container-Images.
Paketname [Package_Name]	Name des Softwarepakets.
Paketversion [Package_Version]	Version des Softwarepakets.
Paket-Maintainer [Package_Maintainer]	Name des Paketbetreuers.
Container-Anreicherungsskripts [sn_itom_pattern_Container_enrich_scripts]	
Aktiv [aktiv]	Gibt an, ob der Status des Anreicherungsskripts aktiv ist.
CI-Typ [ci_type]	Der CI-Typ, für den das Anreicherungsskript gilt.
Bestellung [order]	Ausführungsreihenfolge eines bestimmten Skripts.
Skript [Skript]	Der Anreicherungsskriptname.

Beziehungen

Diese Beziehungen werden erstellt, um die Container-Image-Discovery zu unterstützen.

CI	Beziehung	CI
cmdb_ci_appl	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_oslv_container
cmdb_ci_docker_container	Erstreckt sich von	cmdb_ci_oslv_container
cmdb_ci_oslv_container	Erstreckt sich von	cmdb_ci
cmdb_ci_oslv_container	Nur Referenz	cmdb_Container_Environment_variables
Container_Enrich_scripts	Erstreckt sich von	sys_metadata
cmdb_Container_Environment	Erstreckt sich von	cmdb_key_value

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_db_mssql_instance	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_docker_container

Zugehörige Informationen

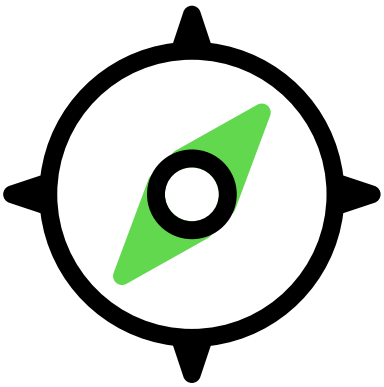
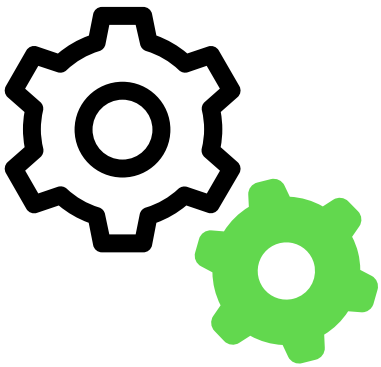
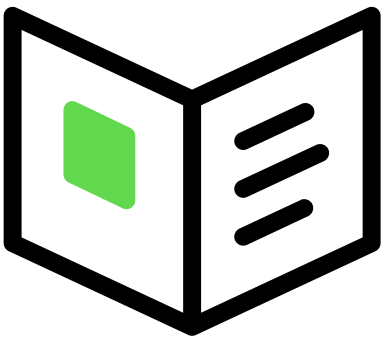
Docker-Virtualisierung

Kubernetes Discovery mithilfe von Mustern

Kubernetes Discovery mit Agent Client Collector für Kubernetes – Transparenz

Agent Client Collector für Kubernetes – Transparenz Erkennt Änderungen an Ressourcen in einem Kubernetes Cluster. Es führt eine kontinuierliche Discovery durch, meldet alle Änderungen an Ihre Instanz zurück und aktualisiert den Configuration Management Database (CMDB) Mit den neuesten Daten.

Erste Schritte

Untersuchen	Konfigurieren	Referenz
		
Allgemeine Übersicht über Agent Client Collector für Kubernetes – Transparenz.	Agent Client Collector für Kubernetes – Transparenz Installations- und Konfigurationsaufgaben.	Referenzinformationen, z. B. gesammelte Daten Agent Client Collector für Kubernetes – Transparenz Support-Matrix und erweiterte Konfigurationsoptionen.

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow-Universität

Jetzt erstellen

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

https://www.servicenow.com/

ServiceNow Store

ServiceNow Store

Support

- https://support.servicenow.com/now
- Known Error-Portal

Agent Client Collector für Kubernetes – Transparenz erkunden

Agent Client Collector für Kubernetes – Transparenz Ermöglicht Ihnen, Einblick in lokale Umgebungen zu erhalten Kubernetes Cluster sowie die folgenden Cloud-Bereitstellungen: Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), Azure Kubernetes Engine (AKS), Red Hat OpenShift, Und Rancher.

Agent Client Collector für Kubernetes – Transparenz Erkennt Änderungen an Ressourcen in einem Kubernetes Cluster. Es führt eine kontinuierliche Discovery durch, meldet alle Änderungen an Ihre Instanz zurück und aktualisiert den Configuration Management Database (CMDB) Mit den neuesten Daten.

Funktionsweise

Wenn Sie bereitstellen Agent Client Collector für Kubernetes – Transparenz, Kubernetes Erstellt eine Bereitstellungsressource im Cluster. Diese Ressource verwendet ein in gespeichertes Geheimnis Kubernetes Um eine Verbindung mit herzustellen ServiceNow Instanz.

Die Agent Client Collector für Kubernetes – Transparenz Die Bereitstellungsressource enthält einen Pod namens Informer, der eine Verbindung mit herstellt Kubernetes API-Server und empfängt Ereignisse für die Ressourcen im Cluster von der IT. Der Informer sendet die gesammelten Daten über die Tabelle „ECC-Warteschlange“ (External Communication Channel) mithilfe von an die Instanz ServiceNow Tabellen-API zum Lesen und Schreiben in die Warteschlange. Der Informer aktualisiert dann die entsprechenden Tabellen in CMDB.

Hinweis: Wenn der Informer die Änderungen nicht melden kann, z. B. aufgrund eines Netzwerkproblems, werden die Ressourcen, die dem Cluster während des Ereignisses hinzugefügt wurden, zu hinzugefügt CMDB Nach dem nächsten vollständigen Discovery-Zyklus. Die Ressourcen, die während des Ereignisses aus dem Cluster entfernt wurden, werden als Abwesend markiert und nach zwei vollständigen Discovery-Zyklen gelöscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu finden Kubernetes Ressourcen, für die der Informer Daten und erfasst CMDB Tabellen, die ausgefüllt werden, siehe Durch Agent Client Collector für Kubernetes – Transparenz erfasste Daten.

Anfängliche und regelmäßige Discovery

Bei der ersten Discovery findet der Informer alle Ressourcen in Kubernetes Cluster und meldet sie an Ihre Instanz. Alle 30 Sekunden sendet der Informer bis zu 1 MB Daten an die Instanz. Es dauert normalerweise bis zu zwei Minuten, um Daten in einem Cluster mit 1.000 Pods zu melden, und eine weitere Minute pro zusätzlichen 1.000 Pods. Ein einzelner Informer-Pod kann einen Cluster mit Zehntausenden von Pods verarbeiten. Wenn der Informer aus irgendeinem Grund verlässt, Kubernetes Startet automatisch neu.

Nach der ersten Discovery überwacht der Informer kontinuierlich das Hinzufügen, Aktualisieren und Löschen von Ressourcen im Cluster. Ressourcen, die aus dem Cluster gelöscht wurden, werden mit install_Status=absent markiert und aus gelöscht CMDB Innerhalb von Stunden in einer regelmäßigen Bereinigung.

Auswirkung des Informers auf den Kubernetes API-Server

Der Informer hat minimale Auswirkungen auf die Kubernetes API-Server. Ruft die vollständige Liste der relevanten Ressourcen nur einmal ab und speichert sie im Arbeitsspeicher. Ab dann wird sie mit synchronisiert Kubernetes API-Server und ruft nie wieder die vollständige Liste ab. Während der regelmäßigen und vollständigen Discovery-Zyklen bei Bedarf sendet der Informer die gespeicherte Liste der Ressourcen erneut an die Instanz.

Agent Client Collector für Kubernetes – Transparenz Benchmark für Leistung und Skalierbarkeit

Für Agent Client Collector für Kubernetes – Transparenz Benchmarks, siehe Leistungsergebnisse für CNO für Transparenz [KB1555851] artikel in Now Support Knowledge Base.

Agent Client Collector für Kubernetes – Transparenz konfigurieren

Einrichten Agent Client Collector für Kubernetes – Transparenz Durch Ausführen der beschriebenen Verfahren.

Informationen zu erweiterten Konfigurationsoptionen finden Sie unter Verwaltung und Fehlerbehebung von CNO für Transparenz (Cloud-Native-Operations) [KB1532614] artikel in Now Support Knowledge Base.

Bereiten Sie sich auf vor Agent Client Collector für Kubernetes – Transparenz Bereitstellung

Bereiten Sie Ihren vor ServiceNow Instanz und Kubernetes Cluster für Agent Client Collector für Kubernetes – Transparenz Bereitstellung.

Vorbereitungen

- Stellen Sie sicher, dass die folgenden Anwendungen installiert und aktiviert sind:
  - Muster für Discovery und Service-Mapping
- Stellen Sie sicher, dass Kubernetes Das Befehlszeilen-Tool kubectl ist installiert und konfiguriert, um mit Ihrem Cluster zu kommunizieren. Weitere Informationen finden Sie unter Kubectl Dokumentation.
- Wenn Sie ein Helm-Diagramm für die Installation verwenden möchten, stellen Sie sicher, dass das Helm-Tool verfügbar ist. Weitere Informationen finden Sie unter Ruder Dokumentation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: administrator für Schritte, die auf ausgeführt werden ServiceNow Instanz.

Prozedur

1. Auf der ServiceNow Instanz, navigieren Sie zu **Alle** > **Anwenderadministration** > **Anwender**an.
2. Wählen Sie einen Anwender mit mindestens der Rolle „MID_Server“ aus, oder erstellen Sie ihn. Informationen zum Hinzufügen eines neuen Anwenders zu Ihrer Instanz finden Sie unter Einen Benutzer erstellen . Informationen zum Gewähren einer Rolle für einen Anwender finden Sie unter Einem Benutzer eine Rolle zuweisen .
3. In Kubernetes Cluster, wählen oder erstellen Sie einen Namespace, in dem Sie bereitstellen möchten Agent Client Collector für Kubernetes – Transparenz.
   So erstellen Sie einen Namespace:
   a. Öffnen Sie das kubectl-Befehlszeilentool.
   b. Führen Sie den folgenden Befehl aus, nachdem Sie DEN NAMESPACE durch den entsprechenden Wert ersetzt haben:

      `Kubectl erstellt Namespace-NAMESPACE`
4. Erstellen Sie einen Kubernetes Geheimnis, das enthält ServiceNow Anmeldeinformationen für den Zugriff auf Ihren ServiceNow Instanz.

   Hinweis: Stellen Sie sicher, dass die Anmeldeinformationen dem Anwender entsprechen, den Sie im vorherigen Schritt erstellt oder identifiziert haben.

   a. Öffnen Sie das kubectl-Befehlszeilentool.
   b. Führen Sie den folgenden Befehl aus, nachdem Sie INSTANCE_NAME, USERNAME, PASSWORD und NAMESPACE durch die relevanten Werte ersetzt haben:

```
kubectl create secret generic k8s-informer-cred-INSTANCE_NAME
 --from-literal=.user=USERNAME --from-literal=.password=PASSWORD -n NAMESPACE
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Informer eine Verbindung mit herstellt ServiceNow Instanz über einen Proxy-Server können Sie den Proxy-Anwender und das Passwort angeben, indem Sie dem Geheimnis die Schlüssel .proxyUser und .proxyPassword hinzufügen. Zum Beispiel:

  ```
  kubectl create secret generic k8s-informer-cred-INSTANCE_NAME
   --from-literal=.user=USERNAME --from-literal=.password=PASSWORD
   --from-literal=.proxyUser=PROXY_USER
   --from-literal=.proxyPassword=PROXY_PASSWORD -n NAMESPACE.
  ```

  Wenn Sie .proxyUser nicht angeben, Agent Client Collector für Kubernetes – Transparenz Geht davon aus, dass keine Authentifizierung erforderlich ist. Wenn Sie .proxyUser, aber nicht .proxyPassword angeben, gibt das System einen Fehler in den Protokollen zurück und bricht den Informer ab.

- Wenn Ihre Organisation verwendet Amazon Elastic Kubernetes Service (EKS), Sie können das Geheimnis in speichern AWS Geheimnismanager. Der Informer ruft dann ab ServiceNow Anmeldeinformationen für den Zugriff auf Ihre -Instanz von AWS Geheimnismanager. Weitere Informationen finden Sie unter CNO für Transparenz: Instanz-Anmeldeinformationen werden im AWS Secrets Manager [KB1581074] gespeichert. artikel in Now Support Knowledge Base.
- Wenn Ihre Organisation Azure verwendet Kubernetes Service (AKS), können Sie das Geheimnis in speichern Microsoft Azure Schlüsselspeicher. Der Informer ruft dann ab ServiceNow Anmeldeinformationen für den Zugriff auf Ihre Instanz über den Azure Key Vault. Weitere Informationen finden Sie unter Instanz-Anmeldeinformationen werden in Microsoft Azure Key Vault gespeichert [KB1647736] artikel in Now Support Knowledge Base.
- Wenn Ihre Organisation verwendet Google Kubernetes Engine (GKE), Sie können das Geheimnis in speichern Google Cloud Geheimer Manager. Der Informer ruft dann ab ServiceNow Anmeldeinformationen für den Zugriff auf Ihre -Instanz von Google Cloud Geheimer Manager. Weitere Informationen finden Sie unter CNO für Transparenz: Anmeldeinformationen werden in Google Cloud Secret Manager gespeichert [KB1709597] artikel in Now Support Knowledge Base.
- Wenn Ihre Organisation eine anwenderdefinierte Stamm-CA (Certificate Authority) verwendet, können Sie eine anwenderdefinierte CA im Informer-Pod bereitstellen, damit der Informer mit kommunizieren kann ServiceNow Instanz. Weitere Informationen finden Sie unter Verwenden einer anwenderdefinierten Stammzertifikatstelle beim Verbinden des Informers mit der Instanz [KB1710906] artikel in Now Support Knowledge Base.
- Als Alternative zur Standardauthentifizierung kann der Informer die OAuth 2,0-Autorisierung verwenden, um eine Verbindung mit herzustellen ServiceNow Instanz für erhöhte Sicherheit. Wenn der Informer OAuth 2,0 verwendet, gibt die Instanz ein Zugriffstoken mit einer Ablaufzeit aus, anstatt bei jeder Ressourcenanforderung Anmeldeinformationen zu erfordern. Weitere Informationen finden Sie unter Verbindung von CNO zur Transparenz mit dem OAuth-Protokoll [KB1648198] artikel in Now Support Knowledge Base.

5. **Wahlweise:** Wenn die Richtlinie Ihrer Organisation dies erfordert, platzieren Sie das Informer-Docker-Image im Image-Repository Ihrer Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Beginnt in Agent Client Collector für Kubernetes – Transparenz Version 3.9.0 (Informer-Version 2,3.0), veröffentlicht im November 2024, unterstützt das Docker-Image sowohl arm64- als auch amd64-Architekturen. Das Upgrade vom vorherigen auf das neue Image führt nicht zu Unterbrechungen. Das neue Image erfordert jedoch mehr Speicherplatz in Ihrem Image-Repository als das vorherige.

a. Rufen Sie das Image aus Docker-Hub ab, und übertragen Sie es in das Repository Ihrer Organisation.

(Optional) Ersetzen VERSION Mit der Nummer des neuesten Release, angegeben in CNO für Helm Chart für Sichtbarkeit und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] artikel in Now Support Knowledge Base.

```
Docker pull docker.io/servicenowdocker/informer:VERSION
Docker tag docker.io/servicenowdocker/informer:VERSION COMPANY_REPO:VERSION
Docker push COMPANY_REPO:VERSION
```

b. Wenn das Image-Repository eine Authentifizierung erfordert, erstellen Sie im angegebenen Namespace ein Geheimnis mit dem Namen k8s-Informer-Repository-cred.

Zum Beispiel:

```
kubectl create secret docker-registry k8s-informer-repo-cred --docker-server
https://index.docker.io/v2/ --docker-username DOCKER_USERNAME --docker-password
DOCKER_TOKEN --docker-email=user@servicenow.com -n NAMESPACE
```

6. **Wahlweise:** Wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy fließt, identifizieren Sie den Namen und Port des Proxy-Hosts, der in Ihrem Cluster verwendet wird.

Hinweis: Fragen Sie Ihre Organisation Kubernetes Team für diese Informationen. Sie müssen sie im Installationsprozess bereitstellen.

7. **Wahlweise:** Aktivieren Agent Client Collector für Kubernetes – Transparenz Dient zur gleichzeitigen Verarbeitung weiterer Daten.
Standardmäßig kann die Back-End-Seite des Informers Daten aus etwa 300 Clustern gleichzeitig verarbeiten. Wenn Sie mehr Cluster haben oder Ihre Cluster häufigen Änderungen unterzogen werden, können Sie die Anzahl der gleichzeitigen Worker-Threads erhöhen, die für die Verarbeitung der Daten verwendet werden. Weitere Informationen finden Sie unter Anzahl der CNO für Sichtbarkeit gleichzeitiger Worker-Threads steuern [KB1580241] artikel in Now Support Knowledge Base.

Ergebnis
Ihr ServiceNow Instanz und Kubernetes Cluster sind bereit für Agent Client Collector für Kubernetes – Transparenz Bereitstellung.

Nächste Maßnahme
Kubernetes Visibility Agent (KVA) installieren.

Kubernetes Visibility Agent (KVA) installieren

Sie können installieren Agent Client Collector für Kubernetes – Transparenz Entweder mithilfe eines Helm-Diagramms oder des Kubernetes YAML-Datei.

Vorbereitungen
Erforderliche Rolle: keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt den Standard Agent Client Collector für Kubernetes – Transparenz Installationsprozess. Normalerweise verwenden Sie ein Helm-Diagramm, um die Installation durchzuführen, Sie können aber auch konfigurieren und ausführen Kubernetes YAML-Datei bereitgestellt von ServiceNow.

Hinweis: Alternativ können Sie bereitstellen Agent Client Collector für Kubernetes – Transparenz Mit dem Terraform Helm-Provider. Weitere Informationen finden Sie unter Installieren Sie CNO für Transparenz mit dem Terraform Helm Provider [KB1540556] artikel in Now Support Knowledge Base.

Prozedur

Installieren Agent Client Collector für Kubernetes – Transparenz Entweder mithilfe eines Helm-Diagramms oder des Kubernetes YAML-Datei bereitgestellt von ServiceNow.

- Installieren Agent Client Collector für Kubernetes – Transparenz Mithilfe eines Helm-Diagramms.

  a. Bearbeiten Sie den Helm-Installationsbefehl.

  i. Ersetzen Sie im folgenden Befehl NAMESPACE, INSTANCE_NAME und CLUSTER_NAME durch die relevanten Werte, und ersetzen Sie HELM_URL durch die URL der neuesten Version, die in angegeben ist CNO für Helm Chart für Sichtbarkeit und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] artikel in Now Support Knowledge Base.

```
helm install -n NAMESPACE --set acceptEula=Y --set instance.name=INSTANCE_NAME
 --set clusterName="CLUSTER_NAME" {--set image.repository=COMPANY_REPO --set
 image.tag=COMPANY_TAG} {--set proxyUrl=http://proxy_host:proxy_port} k8s-informer
 HELM_URL
```

Hinweis:

- Die geschweiften Klammern geben an, dass die von ihnen umgebenen Codesegmente optional sind. Verwenden Sie diese Codesegmente, wenn das Image aus dem Image-Repository Ihrer Organisation abgerufen werden muss oder wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy fließt.
- Durch Bestehen `--Setzen akzeptEula=Y` , Sie stimmen der Endanwender-Lizenzvereinbarung zu. Sie können die Endanwender-Lizenzvereinbarung lesen, indem Sie EULA.pdf aus Informer-helm-<VERSION_NUMBER>.tgz extrahieren.
- Wenn der Informer in OpenShift installiert ist, fügen Sie hinzu *`openShift`*Parameter für den Befehl, und legen Sie ihn auf fest `Wahr` :

```
helm install -n NAMESPACE --set acceptEula=Y --set
 instance.name=INSTANCE_NAME --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG}
 {--set proxyUrl=http://proxy_host:proxy_port} {--set openShift=true}
 k8s-informer HELM_URL
```

Hinweis: Wenn der Informer nicht in OpenShift installiert ist, muss dieser Parameter nicht festgelegt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ii. Konfigurieren Sie im Befehl nach Bedarf zusätzliche Einstellungen:

- Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods
- Ändern Sie die Häufigkeit der vollständigen Discovery in Agent Client Collector für Kubernetes – Transparenz
- Deaktivieren Sie die kontinuierliche Discovery in Agent Client Collector für Kubernetes – Transparenz
- Unterdrücken Sie häufige Änderungen in Kubernetes Cluster, um die Belastung Ihrer Instanz zu reduzieren. Wenn diese Funktion aktiv ist, meldet der Informer keine Änderungen oberhalb der konfigurierten Schwellenwertrate an die Instanz zurück. Weitere Informationen finden Sie unter Unterdrücken häufiger Changes in Kubernetes-Clustern, die von CNO aus Gründen der Sichtbarkeit gemeldet wurden [KB1580745] artikel in Now Support Knowledge Base.
- Steuern Sie die maximale Anzahl vollständiger Erkennungen, die Informer auf mehreren Clustern gleichzeitig ausführen können. Weitere Informationen finden Sie unter Planen von vollständigen Erkennungen in CNO für Sichtbarkeit [KB1580250] artikel in Now Support Knowledge Base.
- (Optional) Anwendungsservice-Zuordnungen werden aktiviert

b. Führen Sie den Befehl aus.

- Installieren Agent Client Collector für Kubernetes – Transparenz Mit Kubernetes YAML-Datei.

a. Laden Sie herunter Kubernetes YAML-ZIP-Datei bereitgestellt in CNO für Helm Chart für Sichtbarkeit und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] artikel in Now Support Knowledge Base.

b. Extrahieren Sie die Dateien k8s_Informer.yaml und EULA.pdf aus der ZIP-Datei.

c. Bearbeiten Sie die Datei k8s_Informer.yaml.

- Ändern Sie den Wert von ACCEPT_EULA in „Y“, Wie folgt:

```
- name: ACCEPT_EULA
  value: "Y"
```

Hinweis: Indem Sie den Wert in ändern „Y“, Sie stimmen der Endanwender-Lizenzvereinbarung zu, die in der Datei EULA.pdf enthalten ist.

- Ersetzen Sie alle Vorkommen von <NAMESPACE> durch den Namespace, in dem Sie den Informer installieren möchten.
- Ersetzen Sie alle Vorkommen von <INSTANCE_NAME> durch den Namen Ihrer Instanz ohne Domänennamen.
- Ersetzen Sie <CLUSTER_NAME> durch den Namen Ihres Clusters, wie er in angezeigt wird CMDB.
- Wenn der Informer in OpenShift installiert ist, ändern Sie den Wert der OPENSHIFT-Umgebungsvariablen in Wahr.
- (Optional) Anwendungsservice-Zuordnungen werden aktiviert

d. Führen Sie den folgenden Befehl aus:

```
kubectl apply -f k8s_informer.yaml
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Agent Client Collector für Kubernetes – Transparenz Wird auf bereitgestellt Kubernetes Cluster und beginnt mit dem Streamen von Daten in Ihre Instanz.

Nächste Maßnahme
Für Informationen zu Agent Client Collector für Kubernetes – Transparenz Administration und Fehlerbehebung finden Sie unter Verwaltung und Fehlerbehebung von CNO für Transparenz (Cloud-Native-Operations) [KB1532614] artikel in Now Support Knowledge Base.

Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods

Legen Sie die Arbeitsspeichergrenze für fest Agent Client Collector für Kubernetes – Transparenz Informer-Pod.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Der Speicherverbrauch des Informer-Pods hängt hauptsächlich von der Anzahl der im Cluster enthaltenen Ressourcen ab. Legen Sie die Speicherbeschränkung des Informer-Pods auf mindestens (Anzahl der Pods)/8 MB mit mindestens 200 MB fest. Zum Beispiel:

Geschätzte Pod-Anzahl	1000	5.000	30000
Minimales Arbeitsspeicherlimit	200Mi	625Mi	3.75Gi

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Fügen Sie bei Verwendung eines Helm-Diagramms im Helm-Installationsbefehl das folgende Befehlszeilenargument hinzu:

  `--Set memoryLimit=MEM_LIMIT`

  Beispiel: `--Set memoryLimit=625Mi`

- Bei Verwendung von „k8s_Informer.yaml“ fügen Sie unter der Zeile mit „Limits:“ die Zeile hinzu `Arbeitsspeicher: MEM_LIMIT` .

  Im folgenden Beispiel beträgt MEM_LIMIT 625Mi.

```
resources:
  limits:
    cpu: 100m
    memory: 625Mi
```

Ändern Sie die Häufigkeit der vollständigen Discovery in Agent Client Collector für Kubernetes – Transparenz

Passen Sie an, wie oft Sie möchten Agent Client Collector für Kubernetes – Transparenz Informer zum Ausführen einer vollständigen Discovery.

Vorbereitungen
Erforderliche Rolle: keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig führt der Informer alle 24 Stunden (1440 Minuten) eine vollständige Discovery aus. Sie können diese Häufigkeit ändern, indem Sie das folgende Verfahren ausführen. Ändern Sie beispielsweise den Wert in 2880, um festzulegen Agent Client Collector für Kubernetes – Transparenz Führen Sie alle 48 Stunden (2880 Minuten) eine vollständige Discovery aus.

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Bei Verwendung eines Helm-Diagramms: Fügen Sie im Helm-Installationsbefehl das folgende Befehlszeilenargument hinzu:

  `--fullDiscoveryMin=<Häufigkeit in Minuten> festlegen`

- Bei Verwendung von k8s_Informer.yaml: Ersetzen Sie den Standardwert durch den erforderlichen Wert in der Zeile unter FULL_DISCOVERY_MIN.

Deaktivieren Sie die kontinuierliche Discovery in Agent Client Collector für Kubernetes – Transparenz

Deaktivieren Sie die kontinuierliche Discovery von Agent Client Collector für Kubernetes – Transparenz Wenn Sie nur regelmäßige Snapshots Ihrer Clusterressourcen benötigen. Wenn Sie mehrere Cluster mit häufigen Änderungen haben, reduziert das Deaktivieren der kontinuierlichen Discovery die Belastung Ihrer Instanz.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Fügen Sie bei Verwendung eines Helm-Diagramms im Helm-Installationsbefehl das folgende Befehlszeilenargument hinzu: `--continuousDiscovery=falsch festlegen`

- Geben Sie bei Verwendung von k8s_Informer.yaml den Wert „falsch“ in die Zeile unter CONTINUOUS_DISCOVERY ein.

Zeigen Sie an Kubernetes Clusterversion in CMDB

Erstellen Sie Agent Client Collector für Kubernetes – Transparenz Informer füllen das entsprechende Feld im CI „cmdb_ci_kubernetes_Cluster“ aus, um anzuzeigen Kubernetes Clusterversion.

Vorbereitungen

Verwenden ServiceNow Muster für Discovery und Service-Mapping Anwendungsversion 1.11.0 oder höher.

Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie ein Helm-Diagramm verwenden, legen Sie im Befehl „Helm-Installation“ fest *getClusterVersion*Parameter auf „wahr“:

  ```
  --Set getClusterVersion=wahr
  ```

- Wenn Sie die Datei k8s_Informer.yaml verwenden, legen Sie die Umgebungsvariable GET_CLUSTER_VERSION auf „wahr“ fest.

Erstellen Sie für jedes ein CI cmdb_ci_linux_Server Kubernetes Knoten

Konfigurieren Sie, wenn Sie möchten Agent Client Collector für Kubernetes – Transparenz Informer zum Erstellen eines cmdb_ci_linux_Server-CI für jedes Kubernetes Knoten.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig erstellt der Informer ein cmdb_ci_linux_Server-ci für jeden Kubernetes Knoten. Wenn dieses CI redundant ist oder andere Flows in Ihrer Organisation stört, können Sie den zugehörigen Konfigurationsparameter auf „falsch“ festlegen.

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie ein Helm-Diagramm verwenden, legen Sie im Befehl „Helm-Installation“ fest *createServerCi*Parameter auf „falsch“:

  ```
  --Set createServerCi=false
  ```

- Wenn Sie die Datei k8s_Informer.yaml verwenden, legen Sie die Umgebungsvariable CREATE_SERVER_CI auf „falsch“ fest.

Entfernen Sie inaktive CIs

Beginnend mit Kubernetes Visibility Agent (KVA)Die Plugin-App Release 3.11.0 und Informer Release 2,5 optimieren die KVA-Leistung, indem inaktive Namespace-Konfigurationselemente als deaktiviert markiert werden, wenn die Ressourcen nicht vorhanden sind, ohne sie automatisch zu löschen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die stillgelegte Löschstrategie ist standardmäßig nicht aktiviert. Wenn diese Option aktiviert ist, wird *Install_Status* Wert inaktiver Namespace-Konfigurationselemente (CIs) in Kubernetes Die Namespace-Tabelle ist auf „deaktiviert“ festgelegt, sodass diese CIs nicht von gelöscht werden *table cleaner*Geplante Aufgabe .

Wenn diese Strategie nicht aktiviert ist, wird *Install_Status* Wert inaktiver Namespace-CIs Ist auf „Abwesend“ festgelegt. Die CIs werden automatisch von den vorhandenen gelöscht *table cleaner*Geplante Aufgabe.

Hinweis: Diese Löschstrategie gilt nur für Namespace-CI-Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie die Funktionskennzeichnung (Retired_DELETION_Strategy_enabled) In Ihren Systemeigenschaften .

```
// feature flag with default as false
sn_acc_visibility.retired_deletion_strategy_enabled
// retired install status with default as '7'
sn_acc_visibility.retired_item_install_status
//retired operational status with default as '6'
sn_acc_visibility.retired_item_operational_status
```

2. Erstellen Sie eine geplante Standardtabellenbereinigungsaufgabe, um die abwesenden Namespace-CIs zu entfernen, wie in gezeigt .

Zugehörige Informationen

Planen oder führen Sie einen Auftrag aus, um Datensätze zu löschen

Definieren Sie Listen von Bezeichnungen und Anmerkungen ein- und ausschließen

In Agent Client Collector für Kubernetes – Transparenz, Definieren Sie Listen von Bezeichnungen und Anmerkungen in ein- und ausschließen Kubernetes Ressourcen, die der Informer in abruft Configuration Management Database (CMDB).

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

Erstellen Sie eine ein- oder Ausschlussliste, indem Sie das entsprechende Verfahren ausführen.

Aufgabe	Prozedur
Erstellen Sie eine Einschlussliste	• Fügen Sie bei Verwendung eines Helm-Diagramms im Befehl Helm install eine kommagetrennte Include-Liste von Be–zeichnungen und Anmerkungen hinzu. Beispiel: `--Set IncludeLabelsAndAnnotations="label1,label2"` • Wenn Sie die Datei k8s_Informer.yaml verwenden, fügen Sie Werte unter der Umgebungsvariable INCLUDE_LABELS_–AND_ANNOTATIONS hinzu.
Erstellen Sie eine Ausschlussliste	• Fügen Sie bei Verwendung eines Helm-Diagramms im Befehl Helm install eine kommagetrennte Include-Liste von Be–zeichnungen und Anmerkungen hinzu. Beispiel: `--Set ExcludeLabelsAndAnnotations="label1,label2"`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Prozedur
	• Wenn Sie die Datei k8s_Informer.yaml verwenden, fügen Sie Werte unter der Umgebungsvariablen „EXCLUDE_LA–BELS_AND_ANNOTATIONS“ hinzu.

Fügen Sie anwenderdefinierte Bezeichnungen und Anmerkungen zu hinzu Kubernetes Ressourcen

Fügen Sie allen von bereitgestellten Ressourcen anwenderdefinierte Bezeichnungen und Anmerkungen hinzu Agent Client Collector für Kubernetes – Transparenz In Kubernetes Cluster.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Bei Verwendung eines Helm-Diagramms fügen Sie im Befehl Helm-Installation die anwenderdefinierten Attribute der Datei „values.yaml“ hinzu.

  Verwenden Sie das in diesem Beispiel gezeigte Format:

  `--Set commonLabels.mylabel1=value1 --Set common Labels.mylabel2=value2 --Set common Annotations.myannotation1=value3` .

- Wenn Sie die Datei k8s_Informer.yaml verwenden, fügen Sie den relevanten Ressourcen in der Datei anwenderdefinierte Bezeichnungen und Anmerkungen manuell hinzu.

Hinweis:

Bezeichnungs- und Anmerkungsnamen müssen alphanumerisch sein und dürfen keine Leerzeichen oder Sonderzeichen enthalten. Einschränkungen für Bezeichnungswerte finden Sie unter Kubernetes-Dokumentation .

Upgrade Agent Client Collector für Kubernetes – Transparenz Informer Remote

Upgrade Agent Client Collector für Kubernetes – Transparenz Informer-Pods in Kubernetes Cluster Remote von der aus ServiceNow Instanz, um eine Abhängigkeit von zu vermeiden Kubernetes administrator. Sie können einen einzelnen Informer oder mehrere Informer zusammen upgraden.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Eigenschaften**an.
2. In **Image Des Kubernetes-Sichtbarkeitsmitarbeiters** Feld das Image festlegen, auf das Sie Informer aktualisieren möchten, die derzeit ausgeführt werden, und wählen Sie dann aus **Speichern** .
   Verwenden Sie das folgende Format: Repository:Tag. Beispiel: `Serviceowdocker/Informer:2.1.1` .
3. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Startseite**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In Kubernetes Informer-Liste führen Sie die relevanten Schritte aus, um einen Informer oder mehrere Informer gleichzeitig zu aktualisieren.

   Hinweis: Nur Informer mit dem Wert „Upgrade ausstehend“ im **Upgrade-Status** Feld kann aktualisiert werden. Der Ausführungsstatus der Informer muss entweder „aktiv“ oder „Angehalten“ sein.

Upgrade	Schritte
Ein Informer	**a.** Wählen Sie den Informer in der Liste aus, um sein Formular anzuzeigen. **b.** Wählen Sie im Abschnitt zugehörige Links des Formulars die Option aus **Informer Upgraden** .
Mehrere Informer	**a.** Wählen Sie mehrere Informer in der Liste aus. **b.** Von **Aktionen für ausgewählte Zeilen...** Listenmenü auswählen **Informer Upgraden** Menüelement.

   Der Upgradeprozess beginnt und **Upgrade-Status** Das Feld für jeden ausgewählten Informer zeigt den Wert für das Upgrade an. Das System lädt das neue Image herunter und startet den neuen Pod für jeden ausgewählten Informer.

   Wenn ein aktualisierter Pod eine Verbindung zur Instanz herstellt, wird der **Informer-Version** Feld zeigt die neue Versionsnummer an. Die **Upgrade-Status** Feld zeigt das gewünschte Bild in Verwendung an.

Überschreiben Sie Informer-Parameter aus der Instanz

Steuerung Agent Client Collector für Kubernetes – Transparenz Informer-Ausführungsparameter aus dem ServiceNow Instanz, um eine Abhängigkeit von zu vermeiden Kubernetes administrator.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Informer-Ausführungsparameter werden während der Bereitstellung mit konfiguriert Kubernetes YAML-Datei oder der Helm-Befehl. Wenn Sie diese Einstellungen später ändern müssen, können Sie dies direkt in der Instanz tun, ohne Ihren fragen zu müssen Kubernetes Team, um die Bereitstellung zu aktualisieren oder neu zu installieren.

Wenn Sie einen Parameter hinzufügen oder ändern, wird er über die ECC-Warteschlange mit dem Informer synchronisiert. Je nach Parameter muss der Informer-Pod möglicherweise neu gestartet werden. Für Parameter, die einen Neustart erfordern, muss die Umgebungsvariable „SELF_PATCHING_ALLOWED“ auf „wahr“ festgelegt sein, damit Änderungen beim Neustart wirksam werden. Wenn diese Variable auf „falsch“ festgelegt ist, wird der Informer nicht neu gestartet und verwendet weiterhin die alten Werte.

Hinweis: Informer-spezifische Parameter wirken sich nur auf einen bestimmten Informer aus. Wenn Sie einen Parameter hinzufügen, ohne ihn einem Informer zuzuweisen, wird standardmäßig ein globaler Parameter verwendet und wirkt sich auf alle Informer im System aus. Wenn sowohl globale als auch Informer-spezifische Parameter vorhanden sind, haben Informer-spezifische Parameter Vorrang.

Sie können die folgenden Parameter über die Instanz aktualisieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Bei Change neu starten
VERBOSE_LOGGING	Nein
OPENSHIFT	Ja
CREATE_SERVER_CI	Nein
INCLUDE_LABELS_AND_ANNOTATIONS	Nein
EXCLUDE_LABELS_AND_ANNOTATIONS	Nein
FULL_DISCOVERY_MIN	Ja
SEND_INTERVAL_SEC	Ja
CONTINUOUS_DISCOVERY	Ja
CLUSTER_RESOURCE_ID	Nein
CLUSTER_NAME	Nein

Informationen zum Zweck der einzelnen Parameter finden Sie unter Erweiterte Konfigurationsoptionen für CNO für Transparenz [KB1648891] artikel in Now Support Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Konfigurationsparameter**an.
2. Wählen Sie einen Parameter in aus **Kubernetes-Informer-Parameter** Liste.
3. Ändern Sie den konfigurierten Wert nach Bedarf, und wählen Sie dann aus **Aktualisieren** .

Anwendungsservice-Zuordnungen werden aktiviert

S Servicezuordnungen Ordnen Sie Anwendungsservices basierend auf dem Datenverkehr zwischen den Arbeitsauslastungen in zu Kubernetes Verwenden Istio- oder Linkerd-Servicenetze oder ServiceNow DaemonSet und sendet diese Informationen an ServiceNow Instanz.

A Pplikation Service Zuordnungen Zuordnung Der Datenverkehr zwischen den Arbeitsauslastungen in KubernetesMit Istio- oder Linkerd-Servicenetze oder einem ServiceNow DaemonSet als Teil von KVA Installation . Weitere Informationen finden Sie unter . Siehe Kubernetes Visibility Agent (KVA) installieren.

- Wenn Sie einen verwenden ServiceNow DaemonSet: Auf jedem Kubernetes-Knoten wird ein Pod ausgeführt und meldet alle 60 Sekunden neue erkannte Verbindungen an den Haupt-Informer-Pod . Bis Erfahren Sie, wie Sie vorgehen können Aktivieren Sie die Anwendungsservice-Zuordnungen mit ServiceNow DaemonSet, siehe Aktivieren Sie Servicezuordnungen mit DaemonSet.
- Wenn Sie Service-Meshes verwenden, über einen Prometheus-Server verfügen und die Prometheus-URL angeben, fragt der Informer den Prometheus-Server regelmäßig ab, um Informationen zu Verbindungen zu erhalten, die vom Service-Mesh gemeldet werden. Informationen zum Aktivieren der Anwendungsservice-Zuordnungen mit Istio- oder Linkerd-Servicemeshes finden Sie unter Aktivieren Sie Service-Zuordnungen mithilfe von Service-Meshes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie Servicezuordnungen mit DaemonSet

Aktivieren Anwendungsservice-Zuordnungen basierend auf dem Datenverkehr zwischen den Arbeitsauslastungen in KubernetesDurch Verwendung von ServiceNow DaemonSet als Teil von Kubernetes Visibility Agent (KVA) Installation.

Vorbereitungen

Erforderliche Rolle: Discovery_admin.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen verwenden ServiceNow DaemonSet, ein Pod wird auf jedem Kubernetes-Knoten ausgeführt und meldet dem Haupt-Informer-Pod alle 60 Sekunden über erkannte neue Verbindungen. Weitere Informationen finden Sie unter Kubernetes Visibility Agent (KVA) installieren

Prozedur

Legen Sie auch Parameter fest Während des Helm-Diagramms Archivinstallation Oder durch Ändern von Kubernetes YAML-Datei bereitgestellt von ServiceNow.

Methode	Aktionen

Während Helm-Diagramm Archivinstallation	**1.** In Ruder `Installieren` Befehl, fügen Sie den folgenden Parameter hinzu:
	`--set connectionsDiscovery.method=servicenow`
	2. Wenn die Richtlinie Ihrer Organisation dies erfordert, rufen Sie das Daemon–Set-Image aus dem Docker-Hub ab, und platzieren Sie es im Image-Repository Ih–rer Organisation .
	Ersetzen Der Platzhalter X-Zeichen Mit der Nummer des neuesten Release Be–reitgestellt in CNO für Helm Chart für Sicht-barkeit und Kubernetes-YAML-Dateiveröffentli-chungen [KB1564347] artikel in Now Support Knowledge Base.
	`Docker pull servicenowdocker/informer_ds:X.X.X`
	`Docker tagservicenowdocker/informer_ds:X.X.X COMPANY_REPO:X.X.X`
	3. In `Helm-Installation` Befehl, fügen Sie die folgenden Parameter hinzu:
	`--Set image.dsRepository=COMPANY_REPO – Set image.dsTag=X.X.X`

Wird geändert k8s_Informer.yaml **Datei**	**1.** In k8s_Informer.yaml Datei, u Ncomment DaemonSet, ServiceAccount (verwen–det vom DaemonSet) und Service.Deploy–

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Aktionen
	ment-Ressourcen gemäß Die Anweisun–gen in Datei . 2. Heben Sie die Kommentare der Zeilen mit Umgebungsvariablen auf. 3. Wenn Ihre Prometheus-Server-URL nicht die Standardadresse ist, entfernen Sie die Kommentare der Zeilen mit der Umge–bungsvariablen *PROMETHEUS_URL* Und än–dern Sie den Wert. 4. Führen Sie den folgenden Befehl aus: `kubectl apply -f k8s_informer.yaml`

Nächste Maßnahme

Erstellen Sie Anwendungsservice-Zuordnungen

Aktivieren Sie Service-Zuordnungen mithilfe von Service-Meshes

E Nable-Anwendungsservice-Zuordnungen basierend auf dem Datenverkehr zwischen den Arbeitsauslastungen in KubernetesDurch Verwendung von Istio- oder Linkerd- oder Service-Meshes als Teil von Kubernetes Visibility Agent (KVA) Installation.

Vorbereitungen

Sie müssen über einen Prometheus-Server verfügen und die Prometheus-URL angeben.

Erforderliche Rolle: Discovery_admin.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein Service-Mesh verwenden, kommuniziert ein Pod, der auf jedem Knoten (Informer) ausgeführt wird, mit einem Prometheus-Server, um die Verkehrsinformationen zu erhalten. Weitere Informationen finden Sie unter Kubernetes Visibility Agent (KVA) installieren

Prozedur

Legen Sie auch Parameter fest Während Helm-Diagramm Archivinstallation Oder durch Ändern Die Kubernetes YAML-Datei bereitgestellt von ServiceNow.

Methode	Aktionen
Während Ruder Installation	In Die Helm-Installation Befehl Fügen Sie den folgenden Parameter hinzu: `--set connectionsDiscovery.method=<METHOD>` Wobei <METHOD> die URL für Istio (http://prometheus.istio-system:9090) oder Linkerd (http://prometheus.linkerd-viz:9090) ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Aktionen
	Hinweis: Wenn Ihre Prometheus-Server-URL nicht die Standardadresse ist, verwenden Sie den folgenden Parameter: `--set connectionsDiscovery.prometheusUrl`

Ändern Die k8s_Informer.yaml **Skript**	1. Greifen Sie auf zu k8s_Informer.yaml Skript.
	2. Festlegen Die Umgebungsvariable *`k8s_Informer.yaml`* Durch Eingabe Entweder Istio oder Linkerd In Anführungszeichen :
	`-- name: GET_CONNECTIONS_METHOD value: ""`
	3. Führen Sie den folgenden Befehl aus:
	`kubectl apply -f k8s_informer.yaml`

Nächste Maßnahme

Erstellen Sie Anwendungsservice-Zuordnungen

Erstellen Sie Anwendungsservice-Zuordnungen

C Erstellen Sie eine Servicezuordnung, die Anwendungsservices basierend auf dem Datenverkehr zwischen den Arbeitsauslastungen in zuordnet Kubernetes Verwenden Istio- oder Linkerd-Servicenetze oder ServiceNow DaemonSet .

Vorbereitungen

Erforderliche Rolle: discovery_admin

Sie sollten zuerst aktivieren Die Anwendungsservice-Zuordnungen , Mithilfe von Istio- oder Linkerd-Service-Meshes oder einem ServiceNow DaemonSet Als Teil von Kubernetes Visibility Agent (KVA) Installation. Weitere Informationen finden Sie unter . Siehe Erstellen Sie Anwendungsservice-Zuordnungen .

Prozedur

1. Navigieren zu **Alle** Und geben Sie ein `kubernetes-Servicezuordnungen` In Navigation Filter .
2. Wählen Sie den Kubernetes-Service aus Zu verwenden Als Einstiegspunkt für diese Karte.
3. Wählen Sie Aus **Erstellen Sie Servicezuordnungen** .
   - Wenn der Service nicht vorhanden ist, Die Servicezuordnung wird mit dem Standardnamen im folgenden Format erstellt: `Name@Namespace@Clustername` . Sie können diesen Namen ändern .
   - Wenn der Service Für diesen CI-Stamm Ist bereits vorhanden S , Nachricht Service <service-name> Bereits exi S ts und hat dasselbe Stamm-CI. Wird angezeigt.

   Das Serviceformular wird geöffnet.
4. **Wahlweise:** Zeigen Sie die Karte an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie Aus **Öffnen Sie im CMDB-Arbeitsbereich** .

b. Wählen Sie im CMDB-Arbeitsbereich aus **Öffnen Sie Karte** .

Ergebnis

Die Anwendungsservicezuordnung wird erstellt und ist im CMDB-Arbeitsbereich sichtbar.

Zusätzliche Ressourcen werden von abgerufen Kubernetes Cluster in der CMDB

Sie können konfigurieren Agent Client Collector für Kubernetes – Transparenz Informer, von dem zusätzliche Ressourcen abgerufen werden sollen Kubernetes Cluster in der Configuration Management Database (CMDB), Zusätzlich zu den Ressourcen, die standardmäßig an die Datenbank gesendet werden. Indem Sie zusätzliche Ressourcen über den Standardsatz hinaus abrufen, können Sie die Transparenz von verbessern Kubernetes Cluster.

Der Informer sammelt Daten zu Kubernetes Ressourcen, sendet die gesammelten Daten an die Instanz und aktualisiert die entsprechenden Tabellen in CMDB. Für eine Liste der Ressourcen, die der Informer in abruft CMDB Standardmäßig finden Sie unter Von CNO gesammelte Daten zur Transparenz .

Für jeden zusätzlichen Kubernetes Ressource, die der Informer in abrufen soll CMDB, Erstellt das System ein Konfigurationselement (Configuration Item, ci) in der Zieltabelle cmdb_ci_kubernetes_component. Alternativ können zusätzliche Ressourcen in anwenderdefinierte Tabellen abgerufen werden, die die Tabelle „cmdb_ci_kubernetes_component“ erweitern. Sie können beispielsweise eine Tabelle u_cmdb_ci_kubernetes_configmap für alle ConfigMap-Ressourcen im Cluster erstellen. Das System erstellt eine Beziehung und eine Referenz aus der Tabelle zum Cluster-CI für jede zusätzliche Ressource. Wenn die Ressource Namespaced ist, wird eine Beziehung zum Namespace-CI erstellt.

Standardmäßig ruft der Informer die folgenden Informationen aus dem ab Kubernetes Cluster für jede zusätzliche Ressource:

- Name
- Namespace (für Ressourcen mit Namespacen)
- Kubernetes-ID
- API-Version
- Art
- Bezeichnungen und Anmerkungen

Zusammen mit diesen Standarddaten können Sie dem Informer weitere Informationen zu den zusätzlichen Ressourcen in abrufen lassen CMDB. Standardmäßig speichert das System diese zusätzlichen Daten im Attributfeld der Tabelle „cmdb_ci_kubernetes_component“. Sie können auch ein anwenderdefiniertes Feld pro zusätzlicher Ressource zum Speichern der zusätzlichen Informationen erstellen.

Agent Client Collector für Kubernetes – Transparenz Ermöglicht Ihnen das Filtern zusätzlicher Ressourcen durch Definieren von Filterbedingungen. Wenn eine Bedingung eine Übereinstimmung zeigt, sendet der Informer die Ressource an den CMDB.

Für detailliertere Informationen und Verfahren zum Abrufen zusätzlicher Ressourcen von Kubernetes Cluster in der CMDB, Siehe Erkennung zusätzlicher Kubernetes-Ressourcen mit CNO für Transparenz (Informer) [KB1638668] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade Agent Client Collector für Kubernetes – Transparenz

Sie können ein Upgrade durchführen Agent Client Collector für Kubernetes – Transparenz Entweder mithilfe eines Helm-Diagramms oder des Kubernetes YAML-Datei.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Dieses Verfahren beschreibt den Standard Agent Client Collector für Kubernetes – Transparenz Upgradeprozess. Normalerweise verwenden Sie ein Helm-Diagramm, um das Upgrade durchzuführen. Alternativ können Sie ein Upgrade durchführen Agent Client Collector für Kubernetes – Transparenz Durch Konfigurieren und Ausführen von Kubernetes YAML-Datei bereitgestellt von ServiceNow. In beiden Fällen muss vor dem Upgrade nicht deinstalliert werden.

Sie können auch ein Upgrade durchführen Agent Client Collector für Kubernetes – Transparenz Informer-Pods in Kubernetes Cluster Remote von der aus ServiceNow Instanz. Weitere Informationen finden Sie unter Upgrade Agent Client Collector für Kubernetes – Transparenz Informer Remote.

Prozedur

Upgrade Agent Client Collector für Kubernetes – Transparenz Entweder mithilfe eines Helm-Diagramms oder des Kubernetes YAML-Datei bereitgestellt von ServiceNow.

- Upgrade Agent Client Collector für Kubernetes – Transparenz Mithilfe eines Helm-Diagramms.

  a. Bearbeiten Sie den Helm-Upgrade-Befehl.

  i. Ersetzen Sie im folgenden Befehl NAMESPACE, INSTANCE_NAME und CLUSTER_NAME durch die relevanten Werte, und ersetzen Sie HELM_URL durch die URL der neuesten Version, die in angegeben ist CNO für Helm Chart für Sichtbarkeit und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] artikel in Now Support Knowledge Base.

```
helm upgrade -n NAMESPACE --set acceptEula=Y --set
 instance.name=INSTANCE_NAME --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG} {--set
 proxyUrl=http://proxy_host:proxy_port} k8s-informer HELM_URL
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die geschweiften Klammern geben an, dass die von ihnen umgebenen Codesegmente optional sind. Verwenden Sie diese Codesegmente, wenn das Image aus dem Image-Repository Ihrer Organisation abgerufen werden muss oder wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy fließt.
- Durch Bestehen `--Setzen akzeptEula=Y` , Sie stimmen der Endanwender-Lizenzvereinbarung zu. Sie können die Endanwender-Lizenzvereinbarung lesen, indem Sie EULA.pdf aus Informer-helm-<VERSION_NUMBER>.tgz extrahieren.
- Wenn der Informer in OpenShift installiert ist, fügen Sie hinzu *`openShift`*Parameter für den Befehl, und legen Sie ihn auf fest `Wahr` :

```
helm upgrade -n NAMESPACE --set acceptEula=Y --set
 instance.name=INSTANCE_NAME --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG}
 {--set proxyUrl=http://proxy_host:proxy_port} {--set openShift=true}
 k8s-informer HELM_URL
```

Hinweis: Wenn der Informer nicht in OpenShift installiert ist, muss dieser Parameter nicht festgelegt werden.

ii. Konfigurieren Sie im Befehl nach Bedarf zusätzliche Einstellungen:

- Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods
- Ändern Sie die Häufigkeit der vollständigen Discovery in Agent Client Collector für Kubernetes – Transparenz
- Deaktivieren Sie die kontinuierliche Discovery in Agent Client Collector für Kubernetes – Transparenz
- Unterdrücken Sie häufige Änderungen in Kubernetes Cluster, um die Belastung Ihrer Instanz zu reduzieren. Wenn diese Funktion aktiv ist, meldet der Informer keine Änderungen oberhalb der konfigurierten Schwellenwertrate an die Instanz zurück. Weitere Informationen finden Sie unter Unterdrücken häufiger Changes in Kubernetes-Clustern, die von CNO aus Gründen der Sichtbarkeit gemeldet wurden [KB1580745] artikel in Now Support Knowledge Base.
- Steuern Sie die maximale Anzahl vollständiger Erkennungen, die Informer auf mehreren Clustern gleichzeitig ausführen können. Weitere Informationen finden Sie unter Planen von vollständigen Erkennungen in CNO für Sichtbarkeit [KB1580250] artikel in Now Support Knowledge Base.

b. Führen Sie den Befehl aus.

• Upgrade Agent Client Collector für Kubernetes – Transparenz Mit Kubernetes YAML-Datei.

a. Laden Sie herunter Kubernetes YAML-ZIP-Datei bereitgestellt in CNO für Helm Chart für Sichtbarkeit und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] artikel in Now Support Knowledge Base.

b. Extrahieren Sie die Dateien k8s_Informer.yaml und EULA.pdf aus der ZIP-Datei.

c. Bearbeiten Sie die Datei k8s_Informer.yaml.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie den Wert von ACCEPT_EULA in „Y“ , Wie folgt:

```
- name: ACCEPT_EULA
  value: "Y"
```

Hinweis: Indem Sie den Wert in ändern „Y“ , Sie stimmen der Endanwender-Lizenzvereinbarung zu, die in der Datei EULA.pdf enthalten ist.

- Ersetzen Sie alle Vorkommen von <NAMESPACE> durch den Namespace, in dem Sie den Informer installieren möchten.
- Ersetzen Sie alle Vorkommen von <INSTANCE_NAME> durch den Namen Ihrer Instanz ohne Domänennamen.
- Ersetzen Sie <CLUSTER_NAME> durch den Namen Ihres Clusters, wie er in angezeigt wird CMDB.
- Wenn der Informer in OpenShift installiert ist, ändern Sie den Wert der OPENSHIFT-Umgebungsvariablen in Wahr .

d. Führen Sie den folgenden Befehl aus:

```
kubectl apply -f k8s_informer.yaml
```

Nächste Maßnahme

Für Informationen zu Agent Client Collector für Kubernetes – Transparenz Administration und Fehlerbehebung finden Sie unter Verwaltung und Fehlerbehebung von CNO für Transparenz (Cloud-Native-Operations) [KB1532614] artikel in Now Support Knowledge Base.

Agent Client Collector für Kubernetes – Transparenz – Referenz

Referenzinformationen zu Agent Client Collector für Kubernetes – Transparenz.

Durch Agent Client Collector für Kubernetes – Transparenz erfasste Daten

Die Agent Client Collector für Kubernetes – Transparenz Informer erfasst Daten zu Kubernetes Ressourcen und füllt verschiedene aus CMDB Tabellen.

Die Agent Client Collector für Kubernetes – Transparenz Informer sammelt Daten zu folgenden Themen Kubernetes Ressourcen:

- Namespaces
- Knoten
- Bereitstellungen
- Statussätze
- Daemonsets
- Replikatsätze
- Aufträge
- Cronjobs
- Pods
- Services
- ReplikationController
- Ingresses

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Informer sammelt Daten zu folgenden Themen OpenShift Ressourcen:

- BereitstellungConfig
- BuildConfig
- Routen
- Gruppen
- Anwender
- Projekte
- Images
- ImageStreams

Der Informer füllt Folgendes aus CMDB Tabellen:

- cmdb_ci_kubernetes_cluster
- cmdb_ci_kubernetes_namespace
- cmdb_ci_kubernetes_node
- cmdb_ci_kubernetes_deployment
- cmdb_ci_kubernetes_statefulset
- cmdb_ci_kubernetes_daemonset
- cmdb_ci_kubernetes_replicaset
- cmdb_ci_kubernetes_Job
- cmdb_ci_kubernetes_cronjob
- cmdb_ci_kubernetes_pod
- cmdb_ci_kubernetes_service
- cmdb_ci_kubernetes_replicationController
- cmdb_ci_kubernetes_Eingang
- cmdb_ci_docker_container
- cmdb_ci_docker_image
- cmdb_ci_Container_Repository_entry
- cmdb_ci_Container_Repository
- cmdb_ci_linux_server
- cmdb_ci_openshift_dep_conf
- cmdb_ci_openshift_Build_conf
- cmdb_ci_openshift_Route
- cmdb_ci_openshift_Group
- cmdb_ci_openshift_user
- cmdb_ci_openshift_Project
- cmdb_ci_openshift_Images
- cmdb_ci_openshift_images_Stream

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector für Kubernetes – Transparenz Informer-Statusfelder

Die Felder in Agent Client Collector für Kubernetes – Transparenz Informer-Tabelle beschreibt den Status der Informer-Pods, die in bereitgestellt werden Kubernetes Cluster.

Agent Client Collector für Kubernetes – Transparenz Informer-Tabelle

Feld	Beschreibung
Informer-Name	Vom System generierter Name des Informers basierend auf der eindeutigen ID des Clusters. Wenn ein neues Cluster-CI erstellt wird, ist der Informer-Name mit dem Namen identisch, den Sie für den Cluster konfiguriert haben. Wählen Sie dieses Feld aus, um die verfügbaren Aktionen für den ausgewählten Informer anzuzeigen.
Kubernetes Cluster	Verweis auf das Cluster-CI. Wählen Sie dieses Feld aus, um Details zum Cluster anzuzeigen.
Vollständiger Discovery-Status	Status der aktuellen vollständigen Discovery. Mögliche Werte sind: Leer, in Bearbeitung, in Warteschlange, Abgeschlossen, Fehlgeschlagen. **Hinweis:** Die vollständige Discovery wird entweder regelmäßig oder bei Bedarf durchgeführt. Standardmäßig wird sie einmal täglich ausgeführt.
Letzte vollständige Discovery	Die Zeit, zu der die letzte vollständige Discovery abgeschlossen wurde.
Informer-Version	Die Version des Informer-Pods, der im Cluster ausgeführt wird.
Status	Der Status des Informers. Mögliche Werte sind: Nach oben, unten, Angehalten. **Hinweis:** Der Status eines Informers wird als ausgefallen betrachtet, wenn in den letzten 15 Minuten keine Nachricht empfangen wurde.
Status Der Kontinuierlichen Discovery	Der Status der kontinuierlichen Discovery. Mögliche Werte sind: Ein oder aus.
Upgrade-Status	Der Upgradestatus von Informern im Cluster. Mögliche Werte sind: Upgrade ausstehend, Upgrade,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector für Kubernetes – Transparenz Informer-Tabelle (Fortsetzung)

Feld	Beschreibung
	gewünschtes Image in Verwendung, Upgrade mit kubectl/Helm. **Hinweis:** Wenn der Upgradestatus eines Informers „Upgrade mit kubectl/Helm“ lautet, wenden Sie sich an Ihren Kubernetes administrator zum manuellen Upgrade des Informers.

Agent Client Collector für Kubernetes – Transparenz Support-Matrix

Die Agent Client Collector für Kubernetes – Transparenz Die Komponente wird in mehreren Versionen von unterstützt Kubernetes Und OpenShift Und in verschiedenen Kubernetes Umgebungen.

Aktuelle Informationen finden Sie unter CNO für Support-Matrix für Transparenz [KB1700730] artikel in Now Support Knowledge Base.

Agent Client Collector für Kubernetes – Transparenz Erweiterte Konfiguration

Dieser Abschnitt bezieht sich auf erweiterte Konfigurationsoptionen für Agent Client Collector für Kubernetes – Transparenz Komponente wird in ausgeführt Kubernetes Cluster.

Aktuelle Informationen finden Sie unter Erweiterte Konfigurationsoptionen für CNO für Transparenz [KB1648891] artikel in Now Support Knowledge Base.

Discovery konfigurieren

Konfigurieren Sie die Elemente, die Discovery für die Erkundung Ihres Netzwerks benötigt, zum Beispiel Anmeldeinformationen, Zeitpläne und IP-Adressen.

Konfiguration – Übersicht

Discovery kann nach einem regulären, konfigurierbaren Zeitplan ausgeführt oder manuell gestartet werden. Die von Ihnen angegebenen IP-Adressbereiche informieren Discovery darüber, welche spezifischen Geräte untersucht werden sollen. Zum Abrufen nützlicher Informationen benötigt Discovery Anmeldeinformationen für Geräte in einem bestimmten Bereich, damit Discovery eine Verbindung zu den erkannten Geräten herstellen und verschiedene Probes für sie ausführen kann. Discovery vergleicht die erkannten Geräte mit Konfigurationselementen (CI) in der CMDB und aktualisiert alle passenden Geräte. Wenn Discovery kein passendes CI in der CMDB findet, wird ein CI erstellt.

Verfahrensweisen zur Konfiguration von Discovery

Über die folgenden Links erhalten Sie Informationen zur Konfiguration von Discovery für Ihre Umgebung. Zur Ausführung von Discovery müssen Sie nicht alle diese Verfahren durchführen. Die Plattform stellt viele Standardwerte bereit, die für die meisten Erkennungsvorgänge geeignet sind und die Sie für die Erkundung Ihres Netzwerks verwenden können. Um Discovery schnell verwenden zu können, verwenden Sie das Guided Setup, mit dessen Hilfe Sie die Einrichtung einer einfachen Erkennung beschleunigen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfahrensweisen zur Konfiguration

Konfiguration der Discovery-IP-Adresse	Discovery-Klassifizierer	Discovery-Status
Domänentrennung und Erkennung	Parameter der Discovery-Klassifizierung	Discovery Konfigurationskonsole
SNMP-Unterstützung für Discovery	Discovery-Bezeichner	
Discovery und SCCM zusammen	Discovery-Eigenschaften	Discovery-Homepage

Discovery anfordern

Discovery Ist als separates Abonnement vom Rest des verfügbar ServiceNow AI Platform Und erfordert Discovery Plugin (com.snc.Discovery).

Vorbereitungen

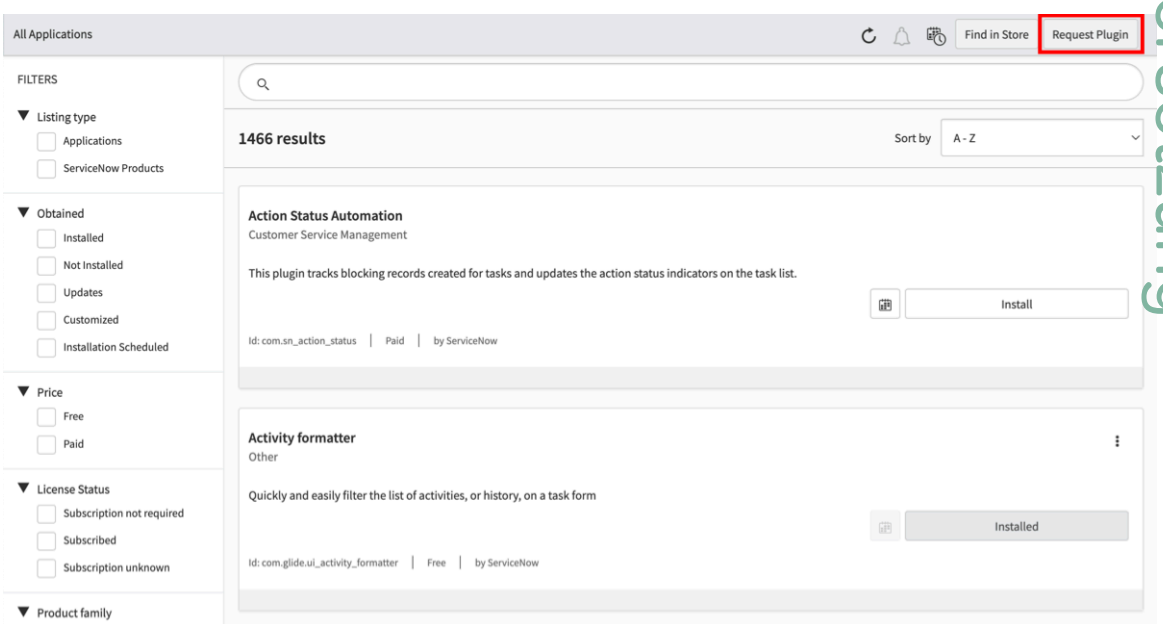
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Um einen zu kaufen Discovery Abonnement, wenden Sie sich an Ihren ServiceNow Account-Manager oder Vertriebsmitarbeiter. Wenn Discovery Plugin ist aktiviert, mehrere Plugins und Anwendungen sind ebenfalls installiert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Prozedur

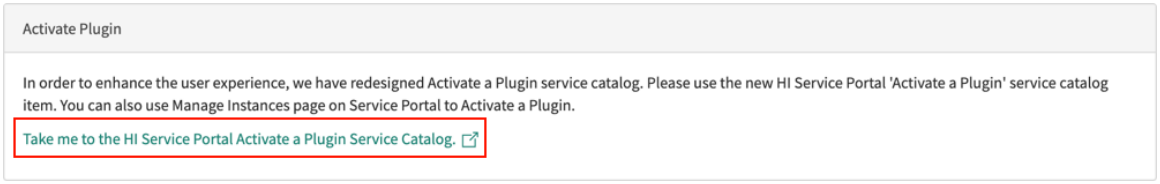
1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

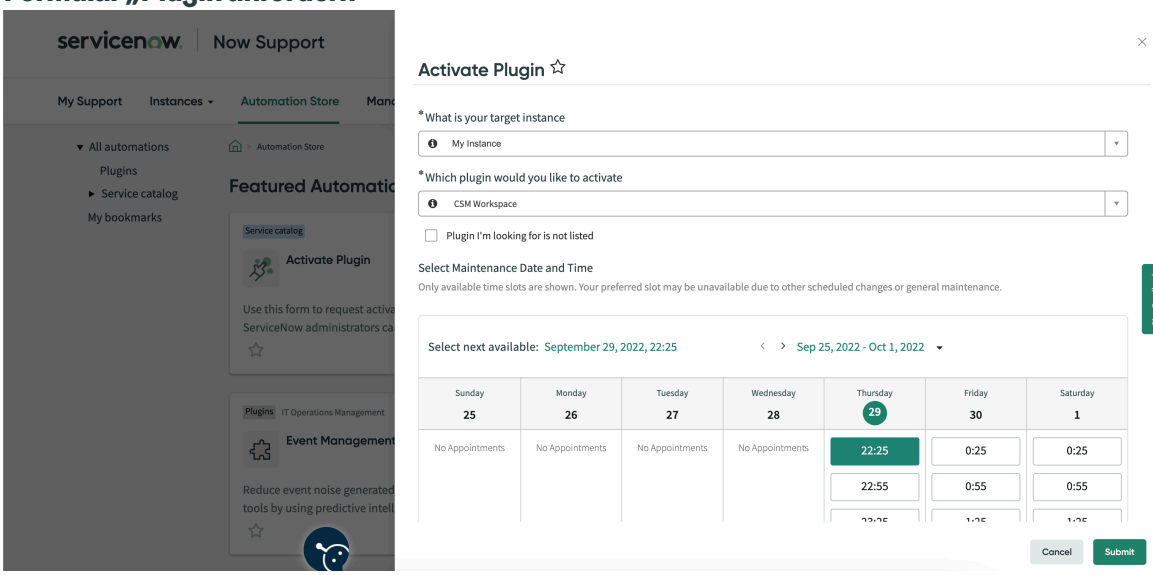
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Discovery einrichten

Um nach der Aktivierung von Discovery loszulegen, haben Sie verschiedene Möglichkeiten.

Hinweis: Wenn sowohl das Plugin „Discovery“ (com.snc.discovery) in der Instanz als auch ein Sprach-Plugin (z. B. Spanisch) aktiviert ist, stellen Sie sicher, dass die Sprache für den MID-Server im Benutzerdatensatz ebenfalls auf „English/None“ (Englisch/Keine) festgelegt ist.

Wählen Sie die Setupmethode aus:

Setupmethode	Beschreibung
Guided Setup	Verwenden Sie diese Methode, wenn Sie alles für die Verwendung von Discovery einrichten möchten, einschließlich eines MID Servers. Das Guided Setup für Discovery stellt eine Reihe von Aufgaben bereit, die Sie beim Konfigurieren von Discovery in Ihrer ServiceNow-Instanz unterstützen. Zum Öffnen Discovery Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .
Ohne Guided Setup	Verwenden Sie diese Methode, wenn Sie die Komponenten jeweils einzeln einrichten möchten. Sie können MID Server, Anmeldeinformationen und Rollen getrennt konfigurieren und dann einen der Erkennungstypen aus dem Erkennungszeitplan konfigurieren.
Discovery Schnellstart	Verwenden Sie diesen Assistenten, um alles zu konfigurieren, was Sie für die Subnetz- und CI-Erkennung in Ihrer Umgebung benötigen. Bevor Sie Schnellstart verwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupmethode	Beschreibung
	können, müssen Sie Ihre MID Server installieren und validieren und die erforderlichen Anmeldeinformationen erstellen.

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Discovery ohne Guided Setup einrichten

Wenn Sie das Guided Setup nicht verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen, um die Anwendung zu aktivieren und um den MID Server und Discovery einzurichten.

Vorbereitungen

- Gewähren Discovery Rolle: Stellen Sie sicher, dass Anwender, von denen erwartet wird, dass sie konfigurieren und ausführen Discovery Haben Sie in Ihrem Netzwerk die Rolle Discovery_admin. Diese Rolle gewährt Zugriff auf die Tabellen in Discovery.
- Bestimmen Sie einen Computer als Host für den MID Server.
- Sammeln Sie die Anmeldeinformationen, die der MID Server für den Zugriff auf die zu erkennenden Geräte benötigt.
- Bestimmen Sie, welche IP-Adressen von Discovery gescannt werden müssen. Gruppieren Sie in einem sehr komplexen Netzwerk IP-Bereiche in Range Sets, die für verschiedene Zeitpläne wiederverwendbar sind. Discovery scannt nicht außerhalb dieser Bereiche.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Installieren Sie einen oder mehrere MID-Server auf physischen oder virtuellen Servern, die die erfüllen Systemanforderungen des MID-Servers Und konfigurieren Sie sie, um mit dem entsprechenden zu kommunizieren ServiceNow Instanz.
   Installieren Sie zuerst mindestens zwei MID Server, und weisen Sie sie verschiedenen Zeitplänen und IP-Bereichen zu, um Erkennungen schneller abzuschließen. Seit dem Istanbul-Release müssen Sie sicherstellen, dass dem MID Server die Anwendung Discovery oder die Anwendung **ALLE** zugewiesen ist.
2. Stellen Sie die MID-Server-Konnektivität sicher, indem Sie zu navigieren **Discovery** > **MID-Server**an.
   Wenn die MID Server ordnungsgemäß konfiguriert sind, werden sie in der Liste der MID Server angezeigt.
3. Wenn ein MID Server in der Instanz nicht als Auswahl angezeigt wird, führen Sie die folgenden Prüfungen durch:
   - Stellen Sie sicher, dass die URL in der bereitgestellten zugehörigen Liste „Konfigurationsparameter“ korrekt ist.
   - Wenn der MID Server unter Windows installiert ist, stellen Sie sicher, dass der ServiceNow MID Server-Service ordnungsgemäß mit den richtigen Anmeldeinformationen konfiguriert ist und ausgeführt wird.
   - Überprüfen Sie das MID Server-Protokoll auf Fehler.
     - Navigieren Sie in der -Instanz zu **Discovery** > **MID-Server** > **[MID-Server]** > **Protokolle**an.
     - Navigieren Sie auf dem MID Server-Host zum Verzeichnis agent\logs\agent0.log0.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Standardauthentifizierung aktiviert ist, müssen ein Benutzername und ein Passwort angegeben werden.
- Der MID Server hat möglicherweise keinen ausgehenden Zugriff an Port 443 (SSL), oder ein Proxy-Server verhindert möglicherweise die TCP-Kommunikation mit der Instanz.
- Stellen Sie sicher, dass keine Firewalls die Kommunikation zwischen dem MID Server und der Instanz blockieren.

4. Legen Sie die Anmeldeinformationen fest In der -Instanz für alle Computer, Drucker und Netzwerkgeräte in Ihrer Umgebung.
   Anmeldeinformationen für Windows-Geräte (mithilfe des WMI-Protokolls) werden von der für den MID Server-Service auf dem Windows-Serverhost konfigurierten Anmeldung bereitgestellt. Anmeldeinformationen für UNIX, vCenter und SNMP müssen für die Instanz konfiguriert werden. Discovery ermittelt automatisch, welche Anmeldeinformationen für einen bestimmten Computer oder ein bestimmtes Gerät funktionieren.
5. Definieren Sie Erkennungszeitpläne, und führen Sie sie aus.

   Der Discovery-Zeitplan ist die Kontrollinstanz für die Ausführung von Erkennungen. Der Zeitplan steuert, wann Discovery ausgeführt wird, definiert den zu verwendenden MID Server, den Typ der Discovery, der ausgeführt werden soll, und die abzufragenden IP-Adressen. Erstellen Sie so viele Zeitpläne wie erforderlich, verwenden Sie verschiedene Arten von Erkennungen, und konfigurieren Sie sie so, dass sie jederzeit ausgeführt werden können. Lassen Sie Discovery gemäß dem konfigurierten Zeitplan ausführen, oder führen Sie Discovery zum gewünschten Zeitpunkt manuell aus. Sie können einen einzelnen Zeitplan für das gesamte Netzwerk oder separate Zeitpläne für jeden Standort oder jedes VLAN einrichten. Wenn Sie die zu scannende IP-Adresse in Ihrem Netzwerk nicht kennen, führen Sie zuerst eine Discovery im Netzwerk aus, um die IP-Netzwerke zu erkennen. Nach der Erkennung können Sie diese Netzwerke in Range Sets von IP-Adressen konvertieren, die Sie in einem Discovery-Zeitplan verwenden.

   Hinweis: Verwenden Sie für erweiterte Erkennungen Discovery Verhaltenweisen, etwa für Erkennungen, die einen Lastenausgleich oder das Scannen über mehrere Domänen hinweg erfordern.

6. Validieren Sie die Discovery-Ergebnisse.
   Öffnen Sie die ECC-Warteschlange, analysieren Sie die XML-Nutzlast, und überprüfen Sie dann das Discovery-Protokoll. Weitere Informationen finden Sie im Abschnitt zur Validierung von Ergebnissen in Horizontale Erkennung planen.

Discovery Schnellstart

Discovery Schnellstart ist ein Assistent, der Sie bei der schnellen Inbetriebnahme von Discovery unterstützt. Verwenden Sie Discovery Schnellstart-Aufgaben, um IP-Bereiche oder Subnetze in Ihrer Umgebung zu erkennen und anschließend die Konfigurationselemente (CI) in diesen Subnetzen zu identifizieren.

Installieren und validieren Sie MID Server noch vor der Verwendung von Discovery Schnellstart. Siehe MID-Server-Installation Für Details.

Subnetzerkennung konfigurieren und planen

Bei der Subnetzerkennung werden alle Subnetze in Ihrer Umgebung erkannt, um verfügbare IP-Bereiche zu bestimmen und sicherzustellen, dass MID Server für den Zugriff auf diese Bereiche verfügbar sind.

Vorbereitungen

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

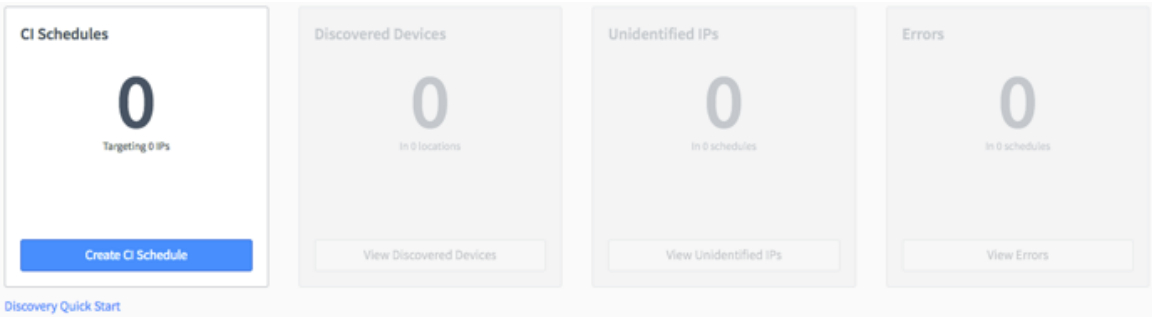
Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieser Phase besteht in der Erkennung aller Subnetze in Ihrem Netzwerk. Dazu muss Discovery über die richtigen SNMP-Anmeldeinformationen verfügen, um die ermittelten Router zu identifizieren. Mit den von Ihnen bereitgestellten Anmeldeinformationen liest Discovery zunächst die Routertabellen des Routers, der mit dem MID Server verbunden ist, um verbundene Router zu identifizieren. Discovery geht dann von innen nach außen durch das Netzwerk von Router zu Router, bis alle lokalen Subnetze erkannt wurden.

Nachdem Discovery die Subnetze identifiziert hat, werden in Vorbereitung auf die CI-Erkennungsphase die IP-Bereiche dieser Subnetze automatisch qualifizierten MID Servern zugewiesen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**an.
   Beim ersten Zugriff auf die Startseite von Discovery wird ein Willkommensbildschirm angezeigt. Nachdem Sie die Subnetzerkennung konfiguriert und den Zeitplan ausgeführt haben, zeigt Schnellstart die Subnetzergebnisse an.
2. Klicken Sie auf **Discovery-Schnellstart**, um mit der Konfiguration zu beginnen.



Hinweis: Fall Sie noch keinen MID Server eingerichtet haben, klicken Sie, wenn Sie aufgefordert werden, den MID Server-Benutzer zu erstellen, den MID Server herunterzuladen und zu installieren sowie ihn zu validieren, auf **MID Server-Einrichtung mit Anleitung**. Über Links im Guided Setup gelangen Sie zu Discovery Schnellstart, um mit der Konfiguration der Subnetzerkennung fortzufahren. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

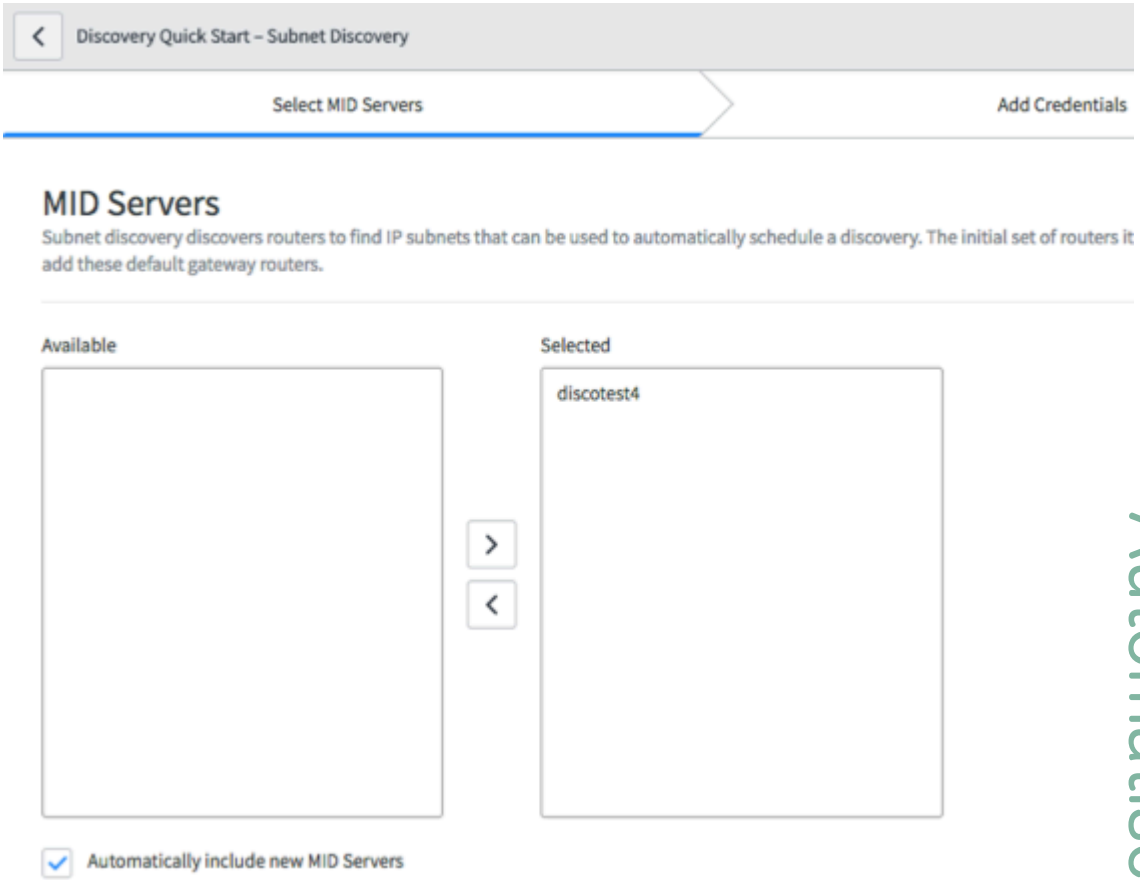
3. Wählen Sie auf der Registerkarte **MID Server auswählen** qualifizierte MID Server für die Subnetzerkennung aus.

   a. Verschieben Sie die MID Server, die Sie für die Subnetzerkennung verwenden möchten, aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
   Verfügbare MID Server müssen die folgenden Anforderungen erfüllen:

   - Sie müssen konfiguriert sein und den Status **In Betrieb** aufweisen.
   - Sie müssen validiert sein.
   - Ihnen müssen die Anwendung Discovery oder **ALLE** Anwendungen angefügt sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



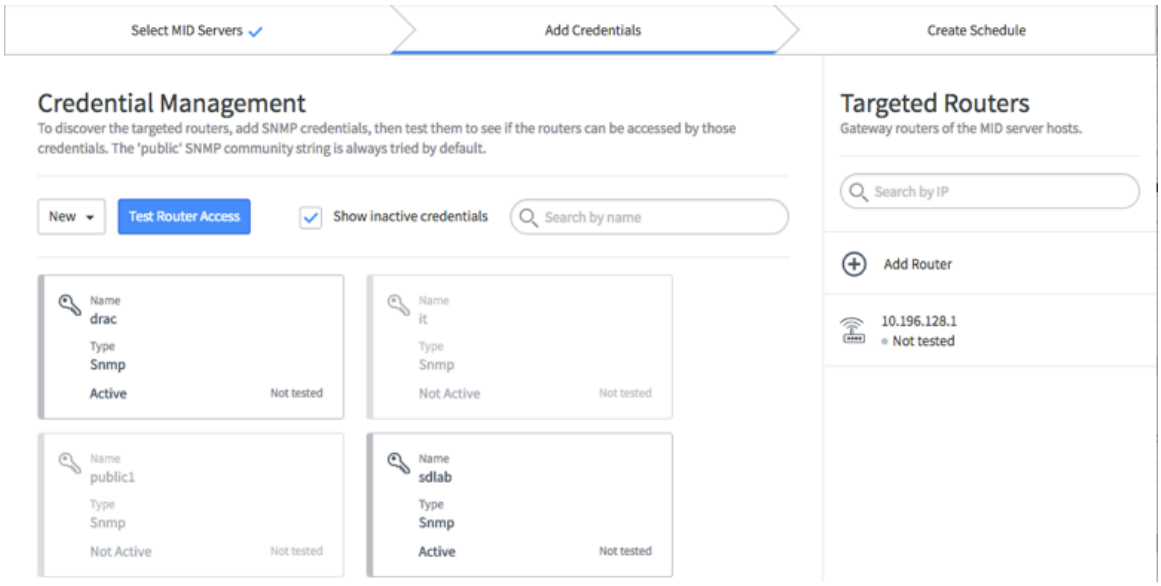
b. Wenn Sie möchten, dass Discovery alle neuen MID Server verwendet, die die Setupkriterien erfüllen, aktivieren Sie das Kontrollkästchen **Neue MID Server automatisch einschließen** aus.

c. Klicken Sie auf **Next (Weiter)**.

4. Fügen Sie auf der Registerkarte **Anmeldeinformationen hinzufügen** Anmeldeinformationen für die zu erkennenden Router hinzu.
Diese Registerkarte zeigt alle SNMP-Anmeldeinformationen, die bereits konfiguriert sind. Router, die in der Liste **Zielrouter** angezeigt werden, sind Standard-Gateway-Router, mit denen der MID Server-Host verbunden ist.

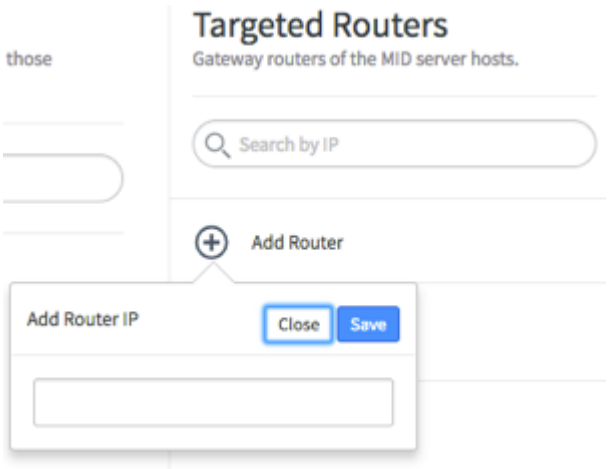
Hinweis: Sie können nach dem Erstellen eines Zeitplans zum Hinzufügen von Anmeldeinformationen zu dieser Phase zurückkehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Klicken Sie auf **Neu**, um gegebenenfalls SNMP-Community- oder SNMP V3-Anmeldeinformationen hinzuzufügen.

b. Wenn die Liste der Zielrouter nicht alle erwarteten Router enthält, klicken Sie auf das Pluszeichen, und fügen Sie den Router anhand der IP-Adresse hinzu.



c. Nachdem Sie alle erforderlichen Anmeldeinformationen konfiguriert haben, klicken Sie auf **Routerzugriff testen**, um zu prüfen, ob Discovery Ihre Anmeldeinformationen für den Zugriff auf Router verwenden kann.
Die Gateway-Router werden in der Spalte **Router** angezeigt, und zwar unabhängig davon, ob die Anmeldeinformationen auf den Router zugreifen können. Diese Router, auf die mit den Anmeldeinformationen erfolgreich zugegriffen werden kann, werden mit dem Indikator **Erfolg** angezeigt. Die Router, die nicht erreichbar sind, werden mit dem Indikator **Fehlgeschlagen** angezeigt.

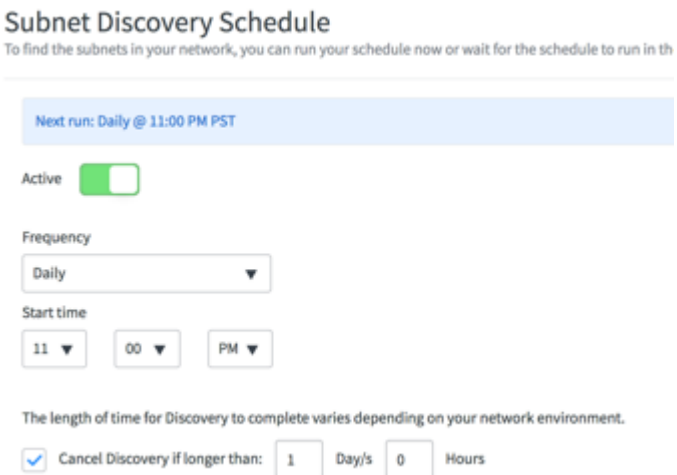
Sie können die Liste mithilfe des Felds **Nach IP durchsuchen** oder mithilfe der Optionen **Erreichte Router** oder **Nicht erreichte Router** in der Auswahlliste **Ansicht** filtern.

d. Klicken Sie auf **Next (Weiter)**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Erstellen Sie auf der Registerkarte **Zeitplan erstellen** einen Zeitplan zur regelmäßigen Ausführung der Subnetzerkennung.
   Bei der Ausführung dieses Zeitplans findet die Subnetzerkennung statt, und die automatische Zuweisung des IP-Subnetzes wird ausgelöst, durch die die erkannten Subnetze qualifizierten MID Servern zugewiesen werden.

   a. Schließen Sie den Zeitplan mithilfe der Felder in der Liste ab.



   - **Akti** : Aktiviert oder deaktiviert diesen Zeitplan.
   - **Frequenz**: Legen Sie fest, wie oft der Zeitplan ausgeführt werden soll:
     - **Täglich**: Discovery zu einem bestimmten Zeitpunkt jeden Tag ausführen.
     - **Wöchentlich**: Discovery an einem bestimmten Tag jeder Woche ausführen.
     - **Monatlich**: Discovery an einem bestimmten Tag des Monats ausführen. Wenn der festgelegte Tag nicht im Monat liegt, wird der Zeitplan in diesem Monat nicht ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan nicht im Februar ausgeführt.
     - **Einmal**: Discovery einmal am angegebenen Datum und zur gewünschten Uhrzeit ausführen.
     - **Regelmäßig** : Ausführen Discovery Jede festgelegte Zeit. Verwenden Sie **Wiederholungsintervall** Feld zum Definieren der Zeit in Tagen, Stunden, Minuten und Sekunden. Die erste Erkennung wird zu dem Zeitpunkt ausgeführt, der im Feld **Start** festgelegt ist. Die nachfolgenden Enrkennungen werden nach Ablauf jedes **Wiederholungsintervall**-Zeitraums ausgeführt.
   - **Discovery abbrechen, wenn länger als**: Beenden Sie den Discovery-Prozess, wenn er die angegebene Dauer überschreitet. Discovery kann aufgrund einer Vielzahl von Faktoren, einschließlich der Größe Ihres Netzwerks, übermäßig lange dauern.

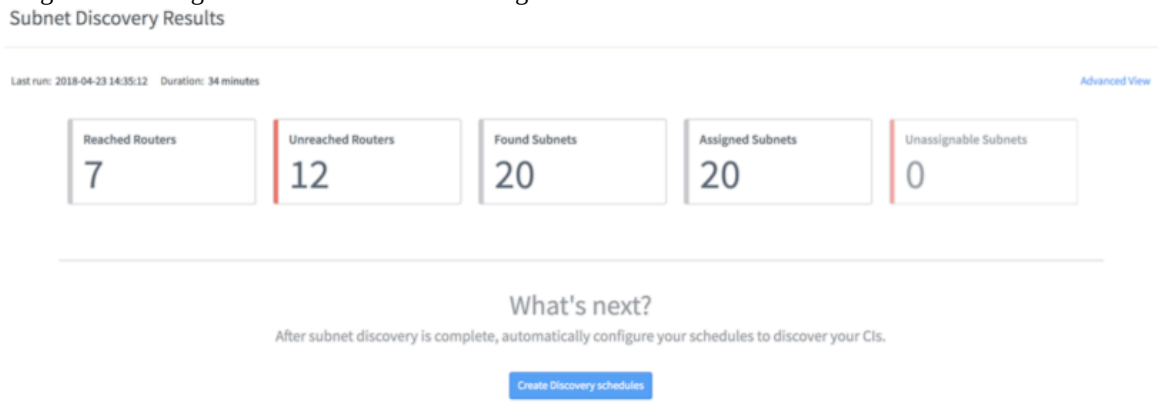
     Hinweis: Eine MID-Server-Verarbeitung findet statt, wenn Discovery abgebrochen wird/ abschließen darf. Alle Ausgabedatensätze, die MID-Server nicht erfasst haben, werden jedoch abgebrochen.

   b. Klicken Sie auf eine der folgenden Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beenden und ausführen** speichert den Zeitplan und führt die Erkennung sofort aus.
- **Fertigstellen** speichert den Zeitplan. Discovery wird dann in dem im Zeitplan angegebenen Intervall ausgeführt.

6. Zeigen Sie die Ergebnisse der Subnetzerkennung an.



a. Klicken Sie auf die einzelnen Kacheln, um Details anzuzeigen.
Wenn die Subnetzerkennung noch nicht ausgeführt wurde, wird für jede Kachel der Wert **0** angezeigt.
   - **Erreichte Router**: Die Anzahl der Router, auf die Discovery zugreifen konnte und die erkannt wurden
   - **Unerreichte Router**: Die Anzahl der Router, auf die Discovery nicht zugreifen konnte
   - **Subnetze gefunden**: Die Anzahl der durch Discovery gefundenen Subnetze
   - **Zugewiesene Subnetze**: Die IP-Subnetze, die mindestens einem MID Server zugewiesen wurden
   - **Unzuweisbare Subnetze**: IP-Subnetze, die keinem MID Server zugewiesen wurden

b. Klicken Sie auf **Zeitplan bearbeiten**, um zur Registerkarte **MID Server auswählen** zurückzukehren. Beheben Sie Probleme mit der Subnetzerkennung, indem Sie zur Seite für den Routerzugriff zurückkehren und sicherstellen, dass alle Anmeldeinformationen ordnungsgemäß konfiguriert sind. Testen Sie auch den Routerzugriff für alle Anmeldeinformationen.

c. Klicken Sie auf **Erweiterte Ansicht**, um das Formular „Automatisierungstatussatz“ anzuzeigen. Dieses Formular zeigt detaillierte Ergebnisse sowohl für die Subnetzerkennung als auch für die automatische Zuweisung von IP-Bereichen an.

CI-Erkennung konfigurieren und planen

Mit den von Ihnen angegebenen Anmeldeinformationen findet der Schnellstart-Assistent alle Konfigurationselemente (CI) für die während der Subnetzerkennung identifizierten IP-Bereiche.

Vorbereitungen

Sie sollten dieses Verfahren nach Abschluss von Subnetzerkennung konfigurieren und planen in Discovery Schnellstart ausführen.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieser Phase besteht in der Erstellung der Zeitpläne, die zum Erkennen der CIs in jedem Subnetz erforderlich sind. Discovery Schnellstart erledigt dies automatisch und führt diese Zeitpläne dann mit den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von Ihnen angegebenen Anmeldeinformationen aus. Sie können jederzeit zusätzliche Anmeldeinformationen hinzufügen. Optional können Sie Standorte für jeden der Subnetzrouter definieren. Discovery erstellt dann separate Zeitpläne für jeden Standort.

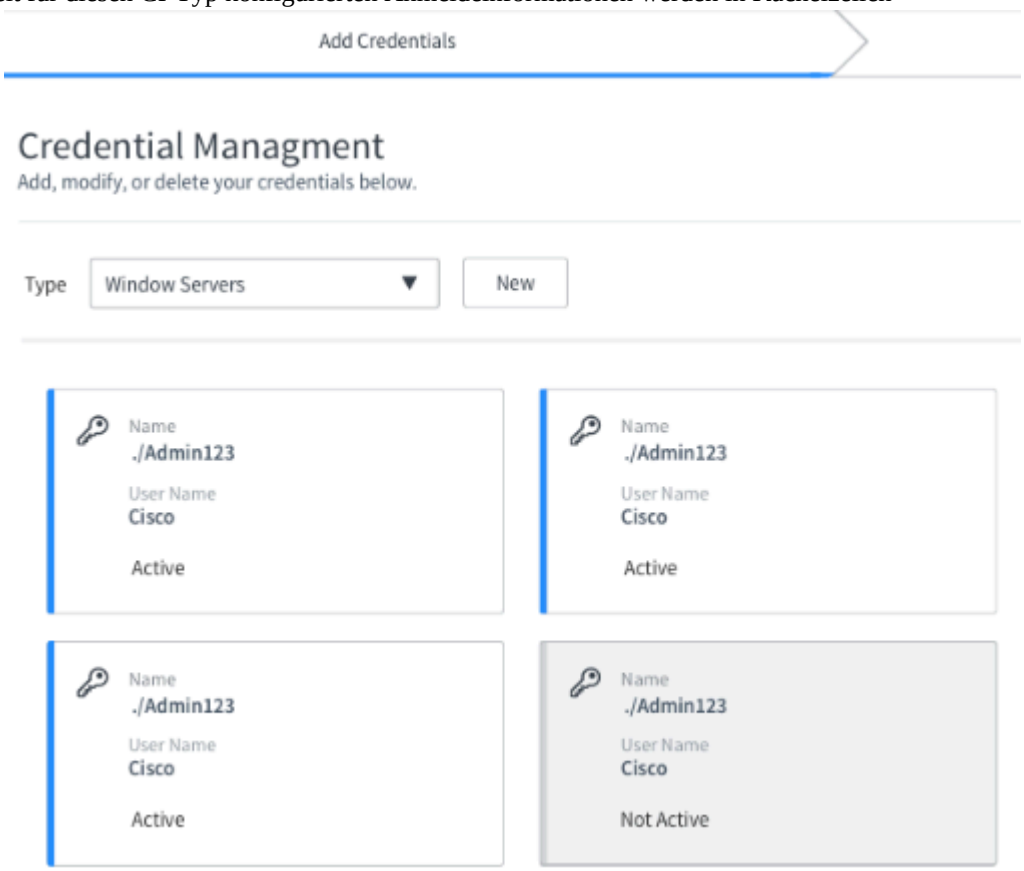
Sie müssen mit den Typen der Anmeldeinformationen vertraut sein, die Sie für die CIs in Ihrem Netzwerk benötigen. Jeder CI-Typ erfordert andere Anmeldeinformationen. Beispiel: Wenn Discovery Verwendet Muster anstelle von Proben, die für Muster möglicherweise erforderlich sind Anwendbare Anmeldeinformationen .

Überprüfen Sie die Anforderungen für die zu erkennenden CI-Typen. Konsultieren Sie Durch ITOM-Transparenz erfasste Daten, und suchen Sie dann den spezifischen Geräte-, Computer oder Anwendungstyp.

Prozedur

1. Erstellen Sie auf der Registerkarte **Anmeldeinformationen hinzufügen** in Discovery Schnellstart die für die Erkennung von CIs in Ihrem Netzwerk erforderlichen Anmeldeinformationen.

   a. Wählen Sie im Feld **Typ** den Anmeldeinformationstyp aus, den Sie verwalten möchten.
   Alle derzeit für diesen CI-Typ konfigurierten Anmeldeinformationen werden in Kachelzeilen



   angezeigt.

   b. Klicken Sie auf **Neu**, um Anmeldeinformationen hinzuzufügen.
   Das Formular „Anmeldeinformationen hinzufügen“, in dem Sie neue Anmeldeinformationen angeben können, wird angezeigt.

   c. Klicken Sie auf **Weiter**, um zur Phase **Routerstandort** zu wechseln.

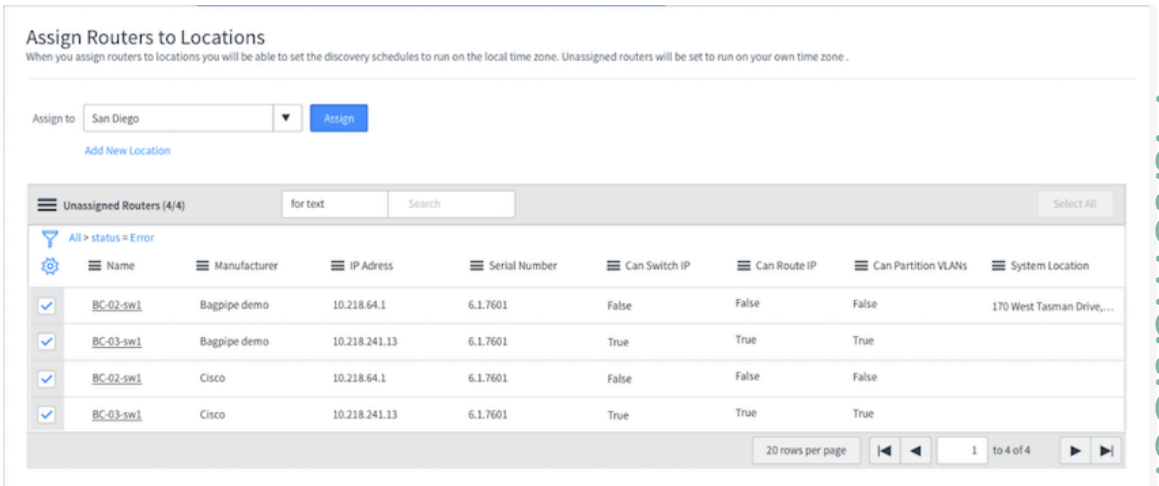
2. **Optional:** Weisen Sie auf der Registerkarte **Routerstandort zuweisen** allen Routern, die durch die Subnetzerkennung gefunden wurden, einen Standort zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei der Konfiguration von Routerstandorten haben Sie die Möglichkeit, für jeden Standort einen Zeitplan zu erstellen. Wenn Sie keine Standorte zuweisen, wird für alle Ihre Subnetze ein einziger Discovery-Zeitplan erstellt. Wenn Sie einem Standort eine Zeitzone zuweisen, erstellt Discovery einen Zeitplan, der in der Zeitzone dieses Standorts ausgeführt wird. Wenn Sie einem Standort keine Zeitzone zuweisen, wird der Zeitplan dieses Standorts in der lokalen Zeitzone des Benutzers ausgeführt.

Hinweis: Ein Subnetz kann mehreren Routern angehören. Wenn Zeitpläne nach Standort erstellt werden, erkennt Discovery Subnetze, die von mehreren Routern mit mehreren Zeitplänen verwaltet werden.

Die Liste der Gateway-Router zeigt die Geräte an, die derzeit keinem Standort zugewiesen sind.



a. Aktivieren Sie die Kontrollkästchen für die Router, denen Sie einen Standort zuweisen möchten. Nutzen Sie die Spalte **Systemstandort** in der Tabelle als Hilfsmittel zur einfacheren Zuordnung eines Standorts zu einem Router.

b. Wählen Sie den Standort in der Auswahlliste **Zuweisen zu** aus.

c. Wenn sich der Standort noch nicht in der Liste befindet, klicken Sie auf **Neuen Standort hinzufügen**, und fügen Sie den Standort hinzu.

d. Stellen Sie sicher, dass für den Standort eine Zeitzone definiert ist.
Mit Zeitzonen können Sie einen Zeitplan für jeden Standort basierend auf der Zeitzone erstellen.

e. Klicken Sie auf **Zuweisen**.

Hinweis: Nicht zugewiesene Router können standortbasierten Zeitplänen nicht hinzugefügt werden.

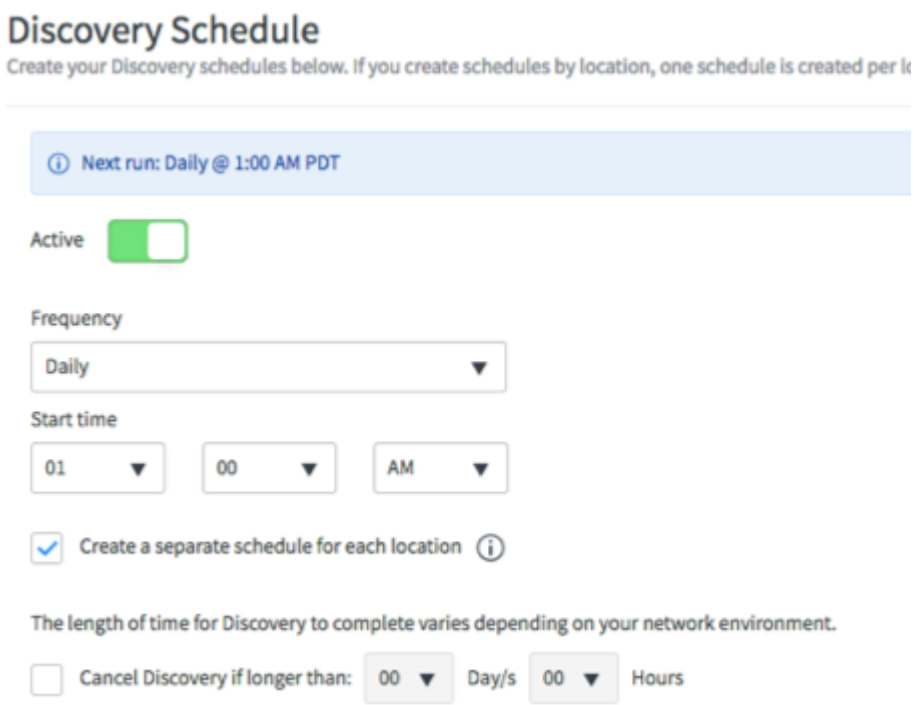
f. Klicken Sie auf **Next (Weiter)**.

3. Erstellen Sie einen Discovery-Zeitplan für CIs.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Schließen Sie den Zeitplan mithilfe der Felder in der Liste ab.



- **Akti** : Aktiviert oder deaktiviert diesen Zeitplan.
- **Frequenz**: Legen Sie fest, wie oft der Zeitplan ausgeführt werden soll:
  - **Täglich**: Discovery zu einem bestimmten Zeitpunkt jeden Tag ausführen.
  - **Wöchentlich**: Discovery an einem bestimmten Tag jeder Woche ausführen.
  - **Monatlich**: Discovery an einem bestimmten Tag des Monats ausführen. Wenn der festgelegte Tag nicht im Monat liegt, wird der Zeitplan in diesem Monat nicht ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan nicht im Februar ausgeführt.
  - **Einmal**: Discovery einmal am angegebenen Datum und zur gewünschten Uhrzeit ausführen.
  - **Regelmäßig** : Ausführen Discovery Jede festgelegte Zeit. Verwenden Sie **Wiederholungsintervall** Feld zum Definieren der Zeit in Tagen, Stunden, Minuten und Sekunden. Die erste Erkennung wird zu dem Zeitpunkt ausgeführt, der im Feld **Start** festgelegt ist. Die nachfolgenden Enrkennungen werden nach Ablauf jedes **Wiederholungsintervall**-Zeitraums ausgeführt.
- **Erstellen Sie einen separaten Zeitplan für jeden Standort** : Erstellen Sie automatisch Zeitpläne für alle von Ihnen konfigurierten Routerstandorte. Diese Zeitpläne werden an dem von Ihnen angegebenen Tag und der angegebenen Uhrzeit ausgeführt, jedoch in ihrer eigenen lokalen Zeitzone. Deaktivieren Sie dieses Kontrollkästchen, um einen einzigen Zeitplan für alle Ihre Standorte zu erstellen, der in der lokalen Zeitzone des Anwenders ausgeführt wird. Diese Option ist nur verfügbar, wenn Sie die Router-Standorte konfiguriert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Discovery abbrechen, wenn länger als**: Beenden Sie den Discovery-Prozess, wenn er die angegebene Dauer überschreitet. Discovery kann aufgrund einer Vielzahl von Faktoren, einschließlich der Größe Ihres Netzwerks, übermäßig lange dauern.

  Hinweis: Eine MID-Server-Verarbeitung findet statt, wenn Discovery abgebrochen wird/abschließen darf. Alle Ausgabedatensätze, die MID-Server nicht erfasst haben, werden jedoch abgebrochen.

b. Klicken Sie auf eine der folgenden Optionen, um den Schnellstart abzuschließen:

- **Beenden und ausführen** speichert den Zeitplan und führt die Erkennung sofort aus.
- **Fertigstellen** speichert den Zeitplan. Discovery wird dann in dem im Zeitplan angegebenen Intervall ausgeführt.

Migrieren Sie von CAPI zu Mustern

Migrieren Sie von Cloud API (CAPI)-basiert Cloud-Discovery Zu musterbasiert Cloud-Discovery. Die Aufgabe erfordert eine unterstützte Instanz und einige Plugins. Die Migration funktioniert für Amazon Web Services (AWS) und Microsoft Azure. Der Administrator kann diese Aufgabe ausführen, nachdem die erste Instanz eingerichtet wurde.

Vorbereitungen

Stellen Sie sicher, dass Ihr ServiceNow AI Platform Hat Folgendes:

- Die Release-Version ist Paris oder höher.
- Die Muster für Discovery und Service-Mapping Plugin (sn_itom_pattern).

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Migration ausgelöst wird, deaktiviert das Skript die entsprechenden CAPI-Discovery-Schritte für die Cloud-Umgebung, um zu verhindern, dass sie während der Cloud-Discovery ausgelöst werden. Außerdem aktiviert das Skript die entsprechenden Cloud-Muster für die Umgebung, die zur Ausführung der zukünftigen Cloud-Discovery verwendet wird. Nach der Migration verwendet die Discovery die neuesten Muster anstelle der Legacy-Discovery-Methode CAPI.

Hinweis:

Die CAPI-basierte Discovery-Methode wird in Zukunft veraltet sein.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **CPG zu Muster migrieren**an.
2. Lesen Sie auf der Seite „CAPI zu Mustermigration“ die Anweisungen, und wählen Sie aus **Voraussetzungsprüfung Ausführen** .
3. Nachdem der erforderliche Scan bestanden wurde, können Sie entweder wie folgt auswählen:
   - Alle migrieren: Migrieren Sie sowohl AWS als auch Azure zusammen.
   - AWS migrieren oder Azure migrieren: Migrieren Sie jede Instanz einzeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie Migrieren aus, und bestätigen Sie, um die Migration fortzusetzen.

Hinweis:

Informationen zu Problemen während der Migration finden Sie in den Schritten zur Fehlerbehebung, die im dokumentiert sind Migration von CAPI zu Muster: Verfahren für den Wechsel von CAPI-basierter Cloud-Discovery zu musterbasierter Cloud-Discovery [KB0827153] artikel in Now Support Knowledge Base.

Discovery-Eigenschaften

Mit Discovery-Eigenschaften können Sie zahlreiche Aspekte des horizontalen Erkennungsprozesses steuern.

Für Informationen zum Discovery Eigenschaften, die Agent Client Collector Verwendet, siehe Push-basierte Discovery und horizontale IP-basierte Discovery zusammen verwenden.

Bearbeiten Sie Folgendes Discovery Eigenschaften, indem Sie zu navigieren **Discovery-Definition** > **Eigenschaften**an.

IP-Eigenschaften

Feld	Beschreibung
glide.discovery.exclude_ip_sync_classes	Definiert CI-Klassen, deren IP-Adressen nicht ersetzt werden sollen, wenn die von Discovery zurückgegebene Adresse nicht mit einer der NICs des Geräts übereinstimmt. Verwenden Sie eine kommagetrennte Liste, um mehrere Klassen zu definieren. Vom System wird im CI-Datensatz standardmäßig die Verwaltungs-IP eines Lastenausgleichsmoduls verwendet, die von Discovery zurückgegeben wird, anstatt sie durch die IP-Adresse einer der NICs des Lastenausgleichsmoduls zu ersetzen. • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_lb
glide.discovery.enforce_unique_ips	Eindeutige IP-Adressen erzwingen: Die IP-Adresse wird ignoriert, nachdem nachfolgende Geräte von Discovery gefunden worden sind, die dieselbe IP-Adresse verwenden. Jedes Mal, wenn ein Computer, ein Drucker oder ein Netzwerkgerät mit einer gültigen IP-Adresse erkannt wird, wird das IP-Adressfeld aller anderen Geräte mit derselben IP-Adresse gelöscht. Wenn inaktiv, wird die IP-Adresse für jedes Gerät gespeichert. • **Typ**: true | false • **Standardwert**: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkeigenschaften

Feld	Beschreibung
glide.discovery.bgp_router_disable	BGP-Routererkundung deaktiviert: Deaktivierung der Ausführung des Probe **SNMP – Routing** oder des Musters, wenn ein Router erkannt wird, von dem das BGP-Protokoll ausgeführt wird. Normalerweise IST diese Exploration inaktiv, da BGP-Routingtabellen sehr groß sind und solche Router im Allgemeinen nur an der Peripherie großer Netzwerke arbeiten, in denen eine weitere Netzwerk-Discovery irrelevant wäre. Dieser Wert könnte auf „falsch“ gesetzt werden, wenn Ihr Unternehmen nur BGP-Router als Edge-Router zwischen relativ kleinen Netzwerken (z. B. zwischen Gebäuden auf einem einzelnen Campus) verwendet. Wenn Sie die Tabelle [Discovery_device_neighbors] während der Erkennung der horizontalen Ebene 2 der bgp-fähigen Geräte ausfüllen müssen, legen Sie fest **BGP-Routererkundung deaktiviert** Eigenschaft bis **Nein** . Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen mit zu wenig Arbeitsspeicher auf dem MID-Server. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.network_discovery	Debugging der Netzwerkerkennung: Ermöglicht die umfassende Protokollierung aller Netzwerk-Discovery-Aktivitäten auf der Instanz. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Monitoring von Erkennungen und Problemlösung
glide.discovery.discoverable.network.max.netmask.bits	Maximale Netzmaskengröße für auffindbare Netzwerke (Bits): Die maximale Anzahl von Bits in einer regulären Netzmaske für Netzwerke, die von einer Netzwerk-Discovery erkannt werden. Eine *reguläre* Netzmaske ist eine Netzmaske, die binär als eine Zeichenfolge von Einsen, gefolgt von einer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zeichenfolge von Nullen, ausgedrückt werden kann. Beispiel: 255.255.255.0 ist regulär, und 255.255.255.64 ist irregulär. Reguläre Netzwerke werden im Allgemeinen wie folgt ausgedrückt: 10.0.0.0/24, d. h. eine Netzwerkadresse von 10.0.0.0 mit einer Netzmaske von 255.255.255.0. Größere Bitzahlen bedeuten Netzwerke mit einer kleineren Anzahl von Adressen. Beispielsweise enthält das Netzwerk 10.128.0.128/30 vier Adressen: eine Netzwerkadresse (10.128.0.128), eine Broadcast-Adresse (10.128.0.131) und zwei verwendbare Adressen (10.128.0.129 und 10.128.0.130). Kleine Netzwerke werden normalerweise in Netzwerkgeräten konfiguriert, damit Loopback-Adressen oder Netzwerke bereitgestellt werden können, die ausschließlich von Punkt-zu-Punkt-Verbindungen verwendet werden. Da diese Arten von Netzwerken im Allgemeinen nicht von Netzwerk Discovery entdeckt werden müssen, wäre es nützlich, sie herauszufiltern. Wenn Sie diese Eigenschaft auf einen Wert von 1 bis 32 festlegen, können Sie die Größe der erkannten regulären Netzwerke begrenzen. Wenn Sie einen anderen Wert festlegen, werden alle Netzwerke erkannt. Unregelmäßige Netzwerke werden immer entdeckt. Der Standardwert ist 28, was bedeutet, dass reguläre Netzwerke mit 8 oder weniger Adressen nicht erkannt werden können. • **Typ**: Ganzzahl • **Standardwert**: 28
glide.discovery.network_owner_method	Auswahlmethode für Netzwerkrouter: Diese Eigenschaft steuert die Methode, die zur Entscheidung verwendet wird (während Netzwerk Discovery) welcher Router als Router ausgewählt werden soll, der einem bestimmten IP-Netzwerk zugeordnet werden soll. Die möglichen Werte sind: • **Erster Router** : Der erste Router, der das Netzwerk erkennt, ist zugeordnet • **Letzter Router** : Der letzte Router, der das Netzwerk erkennt, ist zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Die Meisten Netzwerke** : Der Router mit den am häufigsten angeschlossenen Netzwerken ist zugeordnet • **Geringste Netzwerke** : Der Router mit den am wenigsten angeschlossenen Netzwerken ist zugeordnet • **Typ**: Auswahlliste • **Standardwert**: Die meisten Netzwerke • **Zusatzoptionen**: Erster Router, Letzter Router, Die wenigsten Netzwerke
glide.discovery.physical_interface_types	Physikalische Schnittstellentypen: Eine durch Kommas getrennte Liste von Schnittstellentypen, die für die Netzwerkerkennung als *physisch* angesehen werden. Wenn ein Router (oder ein weiterleitungsfähiges Gerät) über eine Schnittstelle dieses Typs verfügt, werden die mit dieser Schnittstelle verbundenen Netzwerke als lokal mit diesem Gerät verbunden angesehen. Die Standardschnittstellentypen umfassen die Typen Ethernet, 802.11 und Token Ring. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Zeichenfolge • **Standardwert**: 6,117,9,71,209
glide.discovery.switch_interface_types	Switch-Schnittstellentypen: Kommagetrennte Liste von Schnittstellentypen, die berücksichtigt werden. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. Geräte mit beliebigen Schnittstellentypen, die NICHT in dieser Liste angezeigt werden, werden als Router klassifiziert, wenn sie über Weiterleitungsfunktionen verfügen. Eine vollständige Liste der Schnittstellentypnummern finden Sie auf der IANA-Website im Abschnitt „ifType-Definitionen.“ • **Typ**: Zeichenfolge • **Standardwert**: 7,8,9,26,53,62,69,71,78,115,117,209

Andere Discovery-Eigenschaften

Feld	Beschreibung
com.snc.use_external_credentials	Ermöglicht die Verwendung des externen Speichers von Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: true | false • **Standardwert**: true
com.glide.processing.framework.max_thread_utilization_percentage	Ermöglicht Ihnen das Ändern des Skalierungsfaktors für `discovery.sensor` Und `discovery.cloud.sensor` Warteschlangen. Durch Erhöhen des Werts können Sie den Skalierungsfaktor erhöhen, wodurch sich die Anzahl der Worker-Threads pro App-Knoten erhöht. • **Typ**: Ganzzahl • **Standardwert**: 30 • Höchstwert: 75 **Hinweis:** Dieses Verhalten gilt nur, wenn `discovery.use.event.processing` Ist auf festgelegt **Wahr** .
com.glide.queue.discovery.cloud.sensors.processing_jobs.priority	Verwaltet die Mitarbeiterpriorität des Hintergrundauftrags für Cloud-basiert Discovery Aufträge bei Verwendung des Ereignis-Frameworks. Durch Erhöhen des Werts wird die Priorität verringert. • **Typ**: Ganzzahl • **Standardwert**: 100 **Hinweis:** Dieses Verhalten gilt nur, wenn `discovery.use.event.processing` Ist auf festgelegt **Wahr** .
com.glide.queue.discovery.sensors.processing_jobs.priority	Verwaltet die Mitarbeiterpriorität des Hintergrundauftrags für IP-basiert Discovery Aufträge bei Verwendung des Ereignis-Frameworks. Durch Erhöhen des Werts wird die Priorität verringert. • **Typ**: Ganzzahl • **Standardwert**: 100 **Hinweis:** Dieses Verhalten gilt nur, wenn `discovery.use.event.processing` Ist auf festgelegt **Wahr** .
discovery.event.pin.jobs	Ermöglicht die Ausführung von Ereignisprozessoren auf bestimmten Knoten. Wenn auf festgelegt **Wahr** , Aufträge werden Knoten zugewiesen, um die Arbeit gleichmäßig zu verteilen. Wenn auf festgelegt **Falsch** , Aufträge werden zufällig

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zugewiesen, was den Discovery-Durchsatz erhöhen kann. • Typ: Wahr | Falsch • Standardwert: falsch **Hinweis:** Dieses Verhalten gilt nur, wenn `discovery.use.event.processing` Ist auf festgelegt **Wahr** .
discovery.event.separate.cloud.events	Reduziert die Verarbeitungszeit durch Trennung von `discovery.sensor` Und `discovery.cloud.sensor` Ereigniswarteschlangen für Cloud- und IP-basierte Erkennungen. Wenn diese Eigenschaft auf festgelegt ist **Falsch** , Die Ereignisverarbeitung verwendet nur `discovery.sensor` Warteschlange. • Typ: Wahr | Falsch • Standardwert: wahr **Hinweis:** Dieses Verhalten gilt nur, wenn `discovery.use.event.processing` Ist auf festgelegt **Wahr** .
discovery.use.event.processing	Aktiviert Discovery Dient zur Verwendung des Ereignis-Frameworks bei der Verarbeitung von Aufträgen. • Typ: Wahr | Falsch • Standardwert: falsch
glide.discovery.active_processes_filter	Active Processes Filter: Optimierung für die Zuordnung von Anwendungsabhängigkeiten. Filtert die aktiven Prozesse, die von zurückgegeben werden Discovery Nur für diejenigen, die eine Übereinstimmung in der Prozessklassifikationstabelle haben. • **Typ**: true | false • **Standardwert**: false
glide.discovery.adme.aggregation_interval	ADME – Aggregationsintervall (Sek): Wie oft (in Sekunden) sofortige Daten in Blöcke zusammengefasst werden. Es muss mindestens 60 Sekunden betragen und es muss ein Vielfaches des ADME-Abtastintervalls sein. • **Typ**: integer • **Standardwert**: 3600

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.adme.base_dir_unix	ADME – Unix-Basisverzeichnis: Ein vorhandenes Verzeichnis auf den UNIX-Zielcomputern, das als Arbeitsbereich verwendet werden soll. Muss ein absoluter Pfad zum Verzeichnis sein. • **Typ**: true | false • **Standardwert**: false
Mid.powershell.target_Base_dir	PowerShell: Ziel-Basisverzeichnis: Eine Netzwerkfreigabe auf den Zielcomputern von Windows, die als Arbeitsbereich verwendet werden soll. • **Typ**: Zeichenfolge • **Standardwert**: admin$\temp
glide.discovery.adme.max_total_samples	ADME – Maximale Anzahl Samples: Die Anzahl der vom Skript genommenen Samples. Die Ausführung des Skripts wird beendet, nachdem diese Anzahl von Mustern entnommen wurde. • **Typ**: Ganzzahl • **Standardwert**: 100
glide.discovery.adme.rolling_window_size	ADME - Rollfende Fenstergröße. Wie viele kürzlich aggregierte Blöcke sollen gespeichert werden? Ein aggregierter Block besteht aus dem ADME-Aggregationsintervall und den ADME-Abtastintervallabtastungen. Nur die neuesten Blöcke werden beibehalten. • **Typ**: Ganzzahl • **Standardwert**: 24
glide.discovery.adme.sampling_interval	ADME - Abtastintervall (Sek): Wie oft werden Prozess- und Verbindungsdaten in Sekunden erfasst? Muss mindestens 5 Sekunden betragen. • **Typ**: Ganzzahl • **Standardwert**: 120
glide.discovery.adm.update.applications	Steuert, ob Anwendungs-CIs basierend auf dem Status des laufenden Prozesses aktualisiert werden sollen. Wenn Discovery Erkennt den Server erneut und stellt fest, dass ein zuvor ausgeführter Prozess im Datensatz „cmdb_running_Process“ nicht mehr aktiv ist, „Abwesend“ auf festgelegt ist **Wahr** . Darüber hinaus wird install_status für das zugehörige Anwendungs-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	CI von „Installiert“ auf „Abwesend“ aktualisiert. Wenn der laufende Prozess für das zugehörige Anwendungs-CI bei nachfolgenden Scans wieder online ist, wird install_status auf „Installiert“ zurückgesetzt. **Hinweis:** Dieses Verhalten funktioniert nur für Anwendungs-CIs, die mithilfe von Mustern erkannt werden. • **Typ**: true | false • **Standardwert**: true (für zbooted-Instanzen oder neue Aktivierungen)
glide.discovery.allow_loopback_adapters	Loopback-Adapter-Filter: Ermöglicht, dass Netzwerk-Loopback-Adaptern auf SNMP-Geräten erkannt werden, anstatt bei der Erkennung herausgefiltert zu werden. Wenn diese Eigenschaft auf **wahr** festgelegt ist, werden Netzwerk-Loopback-Adressen erkannt und der CMDB hinzugefügt. • **Typ**: true | false • **Standardwert**: false
glide.discovery.application_mapping	Anwendungszuordnung: Aktiviert den Teil der Anwendungszuordnung von Discovery **Wichtig:** Durch Deaktivieren dieser Eigenschaft wird die Erstellung von Beziehungen zwischen Anwendungen deaktiviert, aber *Nicht* Deaktivieren Sie die ADM-Probes und -Sensoren, und verhindern Sie auch die Prozessklassifizierung. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Application Dependency Mapping (ADM) für Discovery
glide.discovery.certs.cert_admin_user_id	Zertifikatsbestand-Management: Enthält die Benutzer-ID des Benutzers, auf den in der Zertifikatsaufgabe und im Incident, die über einen geplanten Auftrag erstellt werden, verwiesen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Zertifikat-Administrator
glide.discovery.certs.days_before_expiration_to_create_renewal_task	Zertifikatsbestand-Management: Zeitpunkt (Anzahl der Tage) vor Ablauf des Zertifikats, zu dem eine Erneuerungsaufgabe erstellt werden soll • **Typ**: Ganzzahl • **Standardwert**: 60
glide.discovery.certs.en_incident_creation_for_expired_certipts	Zertifikatsbestand-Management: Ermöglicht der geplanten Aufgabe, die Incidents für abgelaufene Zertifikate zu erstellen, z. B. Zertifikate, deren Gültigkeit nach dem aktuellen Systemdatum oder der aktuellen Systemzeit liegt. Diese Eigenschaft ist standardmäßig aktiviert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.certs.enable_renewal_task_creation_for_discovered_certificates	Zertifikatsbestand-Management: Aktiviert die Erstellung von Erneuerungsaufgaben für alle erkannten Zertifikate Diese Eigenschaft ist standardmäßig aktiviert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.certs.slack_channel_id	Zertifikatsbestand-Management: Enthält die Slack-Kanal-ID, an die Zertifikatbenachrichtigungen gesendet werden. • **Typ**: Zeichenfolge • **Standardwert**: leer
glide.discovery.count.use_optimized_counter	Führt optimierten Code zum Aktualisieren von „Discovery_Status.Started“ und „discovery_status.completed“ aus. Wenn auf festgelegt **Wahr** , Geschäftsregeln für Discovery_Status werden nicht ausgeführt, wenn „gestartet“ oder „Abgeschlossen“ geändert wird. Es gibt zwei Ausnahmen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	1. Wenn eine Anforderung zum Inkrementieren der Startanzahlen ausgelöst wird und sich der Wert „Discovery_Status.State“ noch auf „Start“ befindet. 2. Wenn discovery_status.completed in den gleichen Wert wie „Discovery_Status.Started“ geändert wird. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.ci_identification	CI-Identifikationsdebugging: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird die Debug-Protokollierung (im CI-Identifikationsprotokoll) für die CI-Identifikation aktiviert. • **Typ**: true | false • **Standardwert**: false
glide.discovery.discover_aws_ec2_host_metadata	Bei der IP-basierten Discovery für einen bestimmten Host werden zusätzlich Probes ausgeführt, die AWS EC2-Metadaten abrufen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.discover_azure_host_metadata	Bei der IP-basierten Discovery für einen bestimmten Host werden zusätzlich Probes ausgeführt, die Azure-Metadaten abrufen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.discover_software	Softwarepakete erkennen: Erkennen von Softwarepaketen aktivieren. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Erkennung von allgemeinen Softwarepaketen
glide.discovery.domain.name.nbt	Legen Sie den BS-Domänennamen über NBT oder WMI fest. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird der Windows-Domänenname von NBT festgelegt. Andernfalls wird es von WMI festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: true | false • **Standardwert**: true
glide.discovery.enable_adme	ADME: Aktivieren Sie die erweiterte ADM-Sonde. Wenn auf festgelegt **Wahr** , Die erweiterte ADM-Probe wird ausgelöst und greift nur nach Bedarf auf die ADM-Probe zurück. • **Typ**: true | false • **Standardwert**: falsch
glide.discovery.enable_file_tracking	Aktivieren Sie das Tracking der Konfigurationsdatei als Teil des musterbasierten Horizontale Discovery. Wenn auf festgelegt **Wahr** , Mit dem System können Sie Pfade von Konfigurationsdateien für Anwendungen angeben, die durch Muster erkannt werden. Sie können nachverfolgte Konfigurationsdateien nachverfolgen und vergleichen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.enable_mac_address_verification	Aktiviert die Überprüfung der MAC-Adresse, um festzustellen, ob ein Gerät seine IP-Adresse während einer Ermittlung geändert hat. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird die MAC-Adresse eines erkannten Geräts von Discovery an den MID Server übergeben, damit von den Probes festgestellt werden kann, ob sich die IP-Adresse geändert hat, während Discovery ausgeführt wird. Wenn das Gerät IP-Adressen geändert hat, dann Discovery Stoppt die Verarbeitung dieser IP-Adresse und aktualisiert den Discovery Protokoll mit einer Warnmeldung. Discovery Die Verarbeitung anderer IP-Adressen wird nicht beendet. • **Typ**: true | false • **Standardwert**: falsch Öffnen Sie die Tabelle Systemeigenschaften [sys_properties], um diese Eigenschaft zu finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.enable.software_filter	Windows-Softwarefilter: Aktivieren Sie die Windows-Softwarefilter für Discovery . • **Typ**: wahr | falsch • **Standardwert**: true
glide.discovery.enable.software_simplify	Aktiviert die Bereinigung für den Namen und die Version der Software. Bei Festlegung auf **true** werden alle angehängten Versionen oder häufig gefundenen Ausdrücke aus dem Namen sowie führende Nullen in der Version entfernt. Wenn auf festgelegt **Falsch** , Rohdaten werden in der Tabelle beibehalten. Verwenden Sie mit **Glide.Discovery.enable.Software_Simplify_sccm** Eigenschaft zur Vermeidung von Diskrepanzen zwischen Softwaredaten zwischen Discovery und SCCM. • **Typ**: true | false • **Standardwert**: true **Hinweis:** Sobald die Eigenschaft auf festgelegt ist **Falsch** , Um die Bereinigung zu deaktivieren, werden für eine bestimmte Software doppelte Datensätze generiert. Name und Version sind die primären Bezeichner.
Glide.Discovery.enable.Software_Simplify_sccm	Aktiviert die Bereinigung für SCCM-Software. Wenn auf festgelegt **Wahr** , Discovery ändert den Namen der Software so, dass er mit SCCM identisch ist. Wenn auf festgelegt **Falsch** , Discovery bereinigt den Namen nicht. Verwenden Sie mit **Glide.Discovery.enable.Software_Simplify** Eigenschaft zur Vermeidung von Diskrepanzen zwischen Softwaredaten zwischen Discovery und SCCM. • **Typ**: true | false • **Standardwert**: false
Glide.Discovery.enable_ssm	Aktiviert AWS SSM-basierte Discovery. • Typ: Wahr | Falsch • Standardwert: falsch
Glide.Discovery.ssm.enable_Windows	Aktiviert AWS SSM-basierte Discovery auf Windows Computer als allgemeiner Systemanwender, der jeden Befehl ausführen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Typ: Wahr | Falsch • Standardwert: falsch
glide.discovery.file_tracking.max_file_size	Dateiverfolgung: Die maximale Dateigröße für den Inhalt der verfolgten Konfigurationsdatei. • **Typ**: integer • **Standardwert**: 500000
glide.discovery.file_tracking.max_files_per_ci	Dateiverfolgung: Die maximale Anzahl verfolgter Konfigurationsdateien pro CI. • **Typ**: integer • **Standardwert**: 50
glide.discovery.file_tracking.change_limit_count	Dateiverfolgung: Anzahl der zulässigen Änderungen an einer verfolgten Konfigurationsdatei im definierten Zeitfenster. • **Typ**: integer • **Standardwert**: 4
glide.discovery.file_tracking.change_limit_days	Dateiverfolgung: Zeitfenster (in Tagen), das die Anzahl der Änderungen an einer verfolgten Konfigurationsdatei begrenzt. • **Typ**: integer • **Standardwert**: 7
glide.discovery.fqdn.regex	Regulärer Ausdruck für den DNS-Hostnamen und Domänennamen: Bei der standardmäßigen Analyse des vollqualifizierten Domänennamens (Fully Qualified Domain Name, FQDN) wird der erste Name durch Punkte getrennt als Hostname und der Rest des Namens als Domänenname ausgewählt. Beispielsweise hat „machine1.testlab.service-now.com“ den Hostnamen „machine1“ und den Domänennamen „testlab.service-now.com.“ Die Eigenschaft erlaubt den regulären Ausdruck mit zwei Erfassungsgruppen, wobei die erste Gruppe den Hostnamen und die zweite Gruppe den Domänennamen darstellt. • **Typ**: Zeichenfolge • **Standardwert**: ^([^.]+)\.((?:[^.]+\.)+[^.]+)$
glide.discovery.hostname.always_update	Aktualisieren Sie immer den Hostnamen. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird der Hostname bei der Erkennung immer mit dem zuletzt entdeckten Wert aktualisiert, abhängig davon, ob die Quelle vertrauenswürdig ist. Beachten Sie, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	dies dazu führen kann, dass von Hand eingegebene Werte überschrieben werden. Diese Eigenschaft gilt nur für die Probe-basierte Discovery. • **Typ**: true | false • **Standardwert**: true
glide.discovery.hostname.case	Groß- und Kleinschreibung des Hostnamens Wenn **Kleinbuchstaben** Ist ausgewählt, übersetzen Sie den Hostnamen immer in Kleinbuchstaben. Wenn **Großbuchstaben** Ist ausgewählt, übersetzen Sie den Hostnamen immer in Großbuchstaben. Wenn **Keine Änderung** Ist ausgewählt, lassen Sie den Hostnamen intakt. Dies betrifft in erster Linie Hostnamen, die mit NETBIOS ermittelt wurden. Einige nicht standardmäßige DNS-Systeme geben jedoch möglicherweise einen Teil oder den gesamten Namen in Großbuchstaben zurück. • **Typ**: Auswahlliste • **Standardwert:** Kleinschreibung • **Zusatzoptionen**: Großbuchstaben, Keine Änderung
glide.discovery.hostname.dns_nbt_trusted	DNS oder NetBIOS ist vertrauenswürdige Hostnamenquelle: Bei Festlegung auf **wahr** wird dem über DNS oder NetBIOS erkannten Gerätenamen vertraut. Wenn aktiviert, wird der über DNS oder NBT gefundene Hostname von CI verwendet. **Hinweis:** Für Linux, AIX, Und Solaris Muster: Verwenden Sie nicht den DNS-Namen als Hostnamen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.hostname.include_domain	Schließt Domänennamen in Hostnamen ein: Bei Festlegung auf **wahr** wird der Domänenname als Teil des Hostnamens eingeschlossen. Zum Beispiel "bosco.service-now.com" anstelle von "bosco". **Hinweis:** Für AIX Und Solaris Muster: Verwenden Sie nicht den DNS-Namen als Hostnamen. • **Typ**: true | false • **Standardwert**: false
glide.discovery.hostname.snmp_trusted	SNMP ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über SNMP erkannten Gerätenamen vertraut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn diese Option aktiviert ist, wird jeder über SNMP gefundene Gerätename verwendet, anstatt des Namens, der durch eine Reverse-DNS-Suche gefunden wurde. • **Typ**: true | false • **Standardwert** : Falsch (für neu Discovery Kunden, die in beginnen Zurich, Standardwert ist „wahr“.)
glide.discovery.hostname.ssh_trusted	SSH ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über SSH erkannten Gerätenamen vertraut. Wenn diese Option aktiviert ist, wird jeder über SSH gefundene Gerätename verwendet, anstatt des Namens, der durch eine Reverse-DNS-Suche gefunden wurde. **Hinweis:** Für Linux, AIX, Und Solaris Muster: Verwenden Sie nicht den DNS-Namen als Hostnamen. • **Typ**: true | false • **Standardwert** : Falsch (für neu Discovery Kunden, die in beginnen Zurich, Standardwert ist „wahr“.)
glide.discovery.hostname.wmi_trusted	WMI ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über WMI erkannten Gerätenamen vertraut. Wenn aktiviert, wird jeder über WMI gefundene Gerätename verwendet anstatt Der Name wurde durch eine Reverse-DNS-Suche gefunden. • **Typ**: true | false • **Standardwert** : Falsch (für neu Discovery Kunden, die in beginnen Zurich, Standardwert ist „wahr“.)
glide.discovery.ip_based.active	Dadurch können Scans für alle IP-Adressen desselben Geräts im selben Discovery-Zeitplan den vollständigen Zyklus durchlaufen. Dies ist auf festgelegt **Wahr** Für Proben-zu-Muster-migrierte Instanzen: Discovery Versucht nicht, eine zusätzliche IP-Adresserkennung durchzuführen. • **Typ**: true | false • **Standardwert**: true (Für Instanzen, die von Probe zu Muster migriert wurden.)
glide.discovery.ip_service_affinity	IP-Service-Affinität: Wenn diese Eigenschaft auf **wahr** gesetzt ist, ist die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	IP-Service-Affinität aktiviert. IP-Service-Affinität erlaubt Discovery den letzten Port der erkannten IP-Adresse zu speichern. **Hinweis:** Sie müssen ip_Service_Affinity-Datensätze aktivieren, wenn Sie mehrere SSH-Ports verwenden. • **Typ**: true | false • **Standardwert** : Falsch (für neu Discovery Kunden, die in beginnen Zurich, Standardwert ist „wahr“.) • **Mehr erfahren**: IP-Service-Affinität für Discovery und Orchestration prüfen
glide.discovery.L3_mapping	Ordnen Sie Server und Netzwerkgeräte Routern und Layer-3-Switches zu, wenn die Eigenschaft „L3-Zuordnung“ aktiviert ist, ordnet sie Server und Netzwerkgeräte den zugehörigen Routern und Layer-3-Switches zu. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Netzwerk-Discovery
glide.discovery.log_message_length	Protokollnachrichtenlänge: Beschränkung der maximalen Nachrichtenlänge, die in der Tabelle „Discovery-Protokoll“ angezeigt wird. Ein Wert von 0 oder eine negative Zahl deaktiviert dieses Limit. • **Typ**: Ganzzahl • **Standardwert**: 200 • **Mehr erfahren**: Protokolle für horizontale Erkennung
glide.discovery.mark_esx_servers_as_absent	Wenn diese Eigenschaft auf „wahr“ festgelegt ist, werden die ESX-Server als „Abwesend“ markiert und nicht als deaktiviert markiert, wenn der ESX-Server nicht in der Nutzlast gefunden wird. • **Typ**: true | false • **Standardwert**: false
glide.discovery.max_concurrent_invocations_per_schedule	Maximale Anzahl gleichzeitiger Aufrufe pro Zeitplan: Verhindert, dass eine unbegrenzte Anzahl von Aufrufen das System überschwemmt, wenn ein Zeitplan länger als die Zeit zwischen Aufrufen dauert. Der Wert ist eine ganze Zahl, die die maximale Anzahl automatisierter Aufrufe desselben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zeitplans festgelegt, die gleichzeitig ablaufen können. Wenn das Limit erreicht wurde, werden nachfolgende geplante Aufrufe abgebrochen. Der Standardwert ist 3. Ein Wert von 0 oder eine negative Zahl deaktiviert diese Einschränkung. • **Typ**: Ganzzahl • **Standardwert**: 3 **Hinweis:** Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „auch wenn abgebrochen“ festgelegt ist.
glide.discovery.network_discovery.functionality	Netzwerke-Discovery-Funktionalität: Die Funktionalität, die zum Erkennen von Netzwerken verwendet wird. Normalerweise sollte dies **Nur SNMP** sein. • **Typ**: Zeichenfolge • **Standardwert**: Nur SNMP
glide.discovery.perf.metrics.enable_collection	Gibt an, ob Discovery-Leistungsmetriken erfasst werden sollen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_build	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Discovery-Build gruppiert wird. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_status	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Discovery-Status gruppiert wird. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_target	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Ziel-IP-Adresse gruppiert wird. • **Typ**: true | false • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.populate_software_instance_table	Bei Festlegung auf „true“ werden von Discovery folgende Tabellen für die Software-Erkennung gefüllt: cmdb_software_instance und cmdb_sam_sw_install. • **Typ**: true | false • **Standardwert**: falsch Verwenden Sie diese Eigenschaft nur, wenn Sie Software Asset Management mit Discovery in einer Version vor Jakarta verwenden und die Tabelle cmdb_software_instance ausfüllen möchten. Öffnen Sie die Tabelle Systemeigenschaften [sys_properties], um diese Eigenschaft zu finden.
glide.discovery.roundingInterval.cpu	CPU-Geschwindigkeitsrundung: Geben Sie die Zahl ein, auf der die CPU-Geschwindigkeit gerundet werden soll. Die Einheiten sind in MHz. • **Typ**: Ganzzahl • **Standardwert**: 1
glide.discovery.roundingInterval.ram	Speicher-Rundung: Geben Sie die Zahl ein, auf die der Computer-RAM gerundet werden soll. Die Einheiten sind in MB. • **Typ**: Ganzzahl • **Standardwert**: 1
Glide.Discovery.schedule_Monitoring.Dry_Run	Bestimmt, ob der Auftrag im Modus „Probelauf“ ausgeführt wird. Wenn auf festgelegt **Wahr** , Der Auftrag protokolliert die Entscheidung nur im Discovery-Protokoll, ändert jedoch nicht den Status des Status, andernfalls ändert der Auftrag den Status des Status bei Bedarf. • **Typ**: true | false • **Standardwert**: false
Glide.Discovery.schedule_Monitoring.schedule_types_to_Exclude	Bestimmt den Typ der zu verfolgenden Status. Der Wert befindet sich im Attribut „Erkennen“ im Zeitplan. • **Typ**: Zeichenfolge • **Standardwert** Cls
Glide.Discovery.schedule_Monitoring.stale_Check_seconds	Bestimmt die Anzahl in Sekunden, in der ein Status als veraltet betrachtet wird. Ein veralteter Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ist ein Status, der in den letzten X Sekunden nicht aktualisiert wurde. • **Typ**: Ganzzahl • **Standardwert** 1200 (20 Min.). Wenn nichts konfiguriert ist, beträgt der Standardwert 2x das Intervall des Auftrags.
glide.discovery.sensors.fire_ssh_probe	Wenn die VIPs (Load Balancer Virtual Services) nicht als Teil der SNMP-Probe-Nutzlast zurückgegeben wurden, lösen Sie die SSH-Probe aus. Wählen Sie diese Option aus, um den SSH-Port am Lastenausgleichsmodul zu verwenden, anstatt nur SNMP zu verwenden. • **Typ**: true | false • **Standardwert**: true
glide.discovery.sensors.netapp_native_7mode	Für 7-Modus NetApp Speicherserver, verwenden Sie native Discovery anstelle von SMI-S.
glide.discovery.sensors.netapp_native_cluster_mode	Für Clustermodus NetApp Speicherserver, verwenden Sie native Discovery anstelle von SMI-S.
glide.discovery.sensors.save_attachments	Speichern von ECC-Warteschlangenanhängen: Das normale Verhalten von Erkennungssensoren besteht darin, Anlagen an ECC-Warteschlangeneinträgen nach erfolgreicher Sensorbearbeitung zu löschen. Wenn diese Eigenschaft auf „wahr“ gesetzt wird, wird dieses Verhalten außer Kraft gesetzt und die Beibehaltung von Anhängen erzwungen. Dies ist normalerweise nur für Debugging-Zwecke nützlich. • **Typ**: true | false • **Standardwert**: true
glide.discovery.shazzam_ranges_json	JSON für IP-Bereiche in Shazzam verwenden, wenn auf festgelegt **Wahr** , Discovery codiert die IP-Bereiche von Shazzam als JSON, wodurch die Nutzlastgröße drastisch reduziert wird. • **Typ**: true | false • **Standardwert**: true
glide.discovery.shazzam_simplify_ranges	Wenn diese Eigenschaft auf **true** gesetzt ist, erkennt Shazzam, ob eine IP in mehreren Bereichen desselben Discovery-Zeitplans enthalten ist, und entfernt die doppelte IP aus allen Bereichen außer einem. Die Deduplizierung ist auf Zeitpläne mit einem einzigen Verhalten beschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zeitpläne mit mehreren Verhaltensweisen funktionieren, doppelte IPs werden jedoch nicht entfernt. • **Typ**: true | false • **Standardwert**: true
glide.discovery.software_filter_keys	Windows-Softwarefilter: Wenn die Windows-Softwarefilterung aktiviert ist und der Name einer erkannten Software einen der kommagetrennten Werte enthält, wird sie herausgefiltert. • **Typ**: Zeichenfolge • **Standardwert** : Sprachpaket, Hotfix-Sicherheitsupdate
glide.discovery.software_sccm_managed	Windows-Software wird von SCCM verwaltet: Wenn auf festgelegt **Wahr** , Discovery Füllt keine Software für Computer-CIs aus, die auch von SCCM verwaltet werden. • **Typ**: true | false • **Standardwert**: false • **Mehr erfahren**: Discovery und SCCM zusammen
glide.discovery.use_cmdb_identifiers	CMDB-Bezeichner: Wenn diese Eigenschaft auf **wahr** gesetzt ist, werden Identifizierung und Abgleich von der CMDB-API durchgeführt und nicht über die alte Discovery-Implementierung. • **Typ**: true | false • **Standardwert**: true
glide.discovery.use_probe_results_cache	Probe-Ergebniscache verwenden: Wenn auf festgelegt **Wahr** , Der Cache wird überprüft, um festzustellen, ob die Ergebnisse der Probe von einem Sensor verarbeitet werden müssen. Sie muss nur verarbeitet werden, wenn sich die Ergebnisse seit dem letzten Erkennungslauf geändert haben. • **Typ**: true | false • **Standardwert**: false • **Mehr erfahren**: Probes erstellen oder ändern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: In früheren Versionen war diese Eigenschaft standardmäßig **true**. Der Wert in dieser Eigenschaft wird während eines Upgrades auf Kingston nicht geändert.
glide.discovery.virtual_interface_types	Typen virtueller Schnittstellen: Liste der Schnittstellentypen (durch Kommas getrennt), die für die Netzwerkerkennung als „virtuell“ betrachtet werden können. Wenn also ein Router (oder ein Gerät, das Routing ausführen kann) über eine Schnittstelle dieses Typs verfügt, werden die an diese Schnittstelle angeschlossenen Netzwerke als virtuell mit diesem Gerät verbunden betrachtet. Die Standardschnittstellentypen enthalten den propVirtual-Typ. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Ganzzahl • **Standardwert**: 53
glide.discovery.warn_minor_version	Bei geringfügigen Versionskonflikten warnen: Wenn diese Eigenschaft auf **wahr** gesetzt ist, werden Warnungen protokolliert, wenn bei der Verarbeitung der Discovery-Sensoren minor_version-Diskrepanzen erkannt werden. • **Typ**: true | false • **Standardwert**: false
glide.ecc_agent.validated.override	Eine Überschreibung des validierten Felds „ecc_agent“: Wenn diese Eigenschaft auf „wahr“ gesetzt ist, werden „ecc_agent“-Datensätze immer als gültig behandelt. • **Typ**: true | false • **Standardwert**: false Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** Um diese Eigenschaft zu finden.
glide.eccprobe.awsrestprobe.max_retries	Legen Sie fest, wie oft die AWS-Anforderung maximal erneut versucht werden soll, wenn ein Fehler vom Typ „Quotenbegrenzung überschritten“ auftritt. Der Höchstwert ist 10. Beachten Sie, dass Neuversuche ein exponentielles Backoff (2^x) aufweisen. Die Festlegung negativer Werte ist gleichbedeutend mit der Festlegung des Höchstwerts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 4
glide.eccprobe.awsrestprobe.max_wait	Legen Sie die maximale Gesamtzeit (Sekunden) fest, innerhalb derer ein neuer Versuch der AWS-Anforderung erfolgt. Höchstwert: 2.046 Sekunden. Die Festlegung negativer Werte ist gleichbedeutend mit der Festlegung des Höchstwerts. • **Typ**: Ganzzahl • **Standardwert**: 30
glide.eccprobe.max_queued_probes_per_run	Legen Sie die maximale Anzahl von Probes fest, die von einem Knoten während einer Ausführung aufgenommen werden können. • **Typ**: Ganzzahl • **Standardwert**: 20
glide.eccprobe.node_agent_id	ECC-Warteschlangeneinträge mit „mid.server. ${VALUE}“ werden von den Knoten aufgenommen und verarbeitet. Dieser muss eindeutig sein und darf nicht mit einem MID Server-Namen identisch sein. • **Typ**: Zeichenfolge • **Standardwert**: NODE_AGENT
sn_disco_firewall.default.rule.task.policy.owner.group	Firewall-Audits und Reporting: Gibt den Namen der Zuweisungsgruppe an, die Firewall-Regelaufgaben besitzt oder diesen zugewiesen ist • **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Aufgabenbesitzer-Gruppenname
sn_disco_firewall.default.rule.task.approval.group	Firewall-Audits und Reporting: Gibt den Namen der Genehmigungsgruppe an, die zum Genehmigen der Firewall-Regelaufgaben verwendet wird. • **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Genehmigungsgruppenname
sn_Disco_certmgmt.enable_csr_Generation	Aktiviert die automatische CSR-Generierung für Zertifikatbestand und -Verwaltung **Neues Zertifikat Anfordern** Und **Neues Zertifikat Anfordern (Automatisiert)** Formulare. Diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Funktion ist aus Sicherheitsgründen standardmäßig deaktiviert. • Typ: Wahr | Falsch • Standardwert: falsch
sn_Disco_certmgmt.private_key_size	Ändert die Größe des privaten Schlüssels, wenn die automatische CSR-Generierung in Zertifikatbestand und -Verwaltung verwendet wird **Neues Zertifikat Anfordern** Und **Neues Zertifikat Anfordern (Automatisiert)** Formulare. Diese Eigenschaft akzeptiert Werte: 512 | 1024 | 2048 | 4096. • Typ: Ganzzahl • Standardwert: 2048
sn_Disco_Workspace.Visibility_Diagnostic_Utility.enabled	Legen Sie diese Option auf „wahr“ fest, um Virtual Agent auf dem zu aktivieren Discovery-Administratorarbeitsbereich **Diagnose** Seite. • Typ: Wahr | Falsch • Standardwert: falsch

Konfiguration der Discovery-IP-Adresse

Verwenden Sie eine oder mehrere Methoden in beliebiger Kombination, um das Netzwerk oder Netzwerksegment für die Abfrage von Discovery zu definieren. Sie können bestimmte IP-Bereiche in Ihre Abfrage einbeziehen oder daraus ausschließen.

Hinweis: Wenn Sie die IP-Adressen in Ihrem Netzwerk nicht kennen, führen Sie zuerst eine Netzwerk-Discovery aus, um zunächst die IP-Netzwerke zu ermitteln. Konvertieren Sie anschließend die IP-Netzwerke in Range Sets von IP-Adressen.

Wenn Ihre Integrationen die Tabellen sys_metadata und sys_update_xml füllen, müssen Sie die Aktualisierungs- und Metadatendatensätze nach dem Import von discovery_range_item oder discovery_range_item_ip löschen.

IPv6-Adressen werden für IP-Adressbereiche oder IP-Netzwerke nicht unterstützt.

Es gibt drei Typen von IP-Sammlungen:

Typ der IP-Sammlung	Beschreibung
IP-Adressenliste	Verwenden Sie IP-Adresslisten, um einzelne Adressen zur Abfrage hinzuzufügen. Diese Adressen sind in keinem vorhandenen IP-Bereich oder IP-Netzwerk enthalten. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ der IP-Sammlung	Beschreibung
	die IP-Adresse des Geräts oder einen Hostnamen (DNS-Namen) eingeben. Wenn Sie einen Hostnamen eingeben, muss er sein Einer IP-Adresse zugeordnet .
IP-Adressbereich	Sie können willkürliche IP-Adressbereiche für die Abfrage definieren. Dieser Prozess stellt eine gute Möglichkeit dar, ausgewählte Segmente eines Netzwerks oder Subnetzes einzubeziehen. Discovery liegen jedoch keine Informationen darüber vor, ob der IP-Bereich Adressen für private Netzwerke oder Broadcast-Adressen enthält, und scannt alle Adressen im Bereich. Wenn Netzwerk- und Broadcast-Adressen enthalten sind, sind die Ergebnisse ungenau. Zum Erkennen von IP-Netzwerken konfigurierte Erkennungen sind genauer als Erkennungen, die für IP-Adressbereiche konfiguriert sind. Es sollten nur diejenigen IP-Adressen in Ihrem Bereich einbezogen werden, die für verwaltbare Geräte im öffentlichen Netzwerk reserviert sind. **Hinweis:** Um mögliche Leistungsprobleme zu vermeiden, beschränken Sie Erkennungszeitpläne auf einen maximalen Bereich von /16 oder nicht mehr als 65.000 IPs. Sie können die Erkennungszeitpläne auch in noch kleinere IP-Adressbereiche aufteilen.
IP-Netzwerk	Sie können auch ein gesamtes IP-Netzwerk scannen. Ein IP-Netzwerk umfasst den Bereich der verfügbaren IP-Adressen in diesem Netzwerk. Der Scan umfasst auch die Netzwerkadresse (die niedrigste Adresse im Bereich) und die Broadcast-Adresse (die höchste Adresse im Bereich). Nachdem Sie die Netzwerkerkennung durchgeführt haben, konvertieren Sie die gefundenen IP-Netzwerke in Range Sets, die Sie zur Erkennung anderer Geräte verwenden. IP-Netzwerke werden in CIDR-Schreibweise dargestellt. Beispiele für die CIDR-Schreibweise: • 192.168.0.0/24 • 10.11.128.192/26 Netzwerk- oder Broadcast-Adressen für ein Netzwerk werden von Discovery nicht gescannt. Die entsprechenden Bereiche für die beiden Netzwerke: • 192.168.0.1–192.168.254 • 10.11.128.193–10.11.128.254 Die Broadcast-Adresse verhindert und bewirkt erhebliche Fehler in den Discovery-Daten. Alle Geräte im Netzwerk werden zurückgegeben. Dies gilt auch für die Netzwerkadresse, durch die eine willkürliche Anzahl von redundanten Geräten hinzugefügt werden kann. Diese integrierte Steuerung macht IP-Netzwerke zur besten Methode, um festzulegen, welche IP-Adressbereiche abgefragt werden sollen.

Eigenschaften der IP-Adressauswahl

Sie können Systemeigenschaften verwenden, um die Auswahl der IP-Adressen für die angegebenen CI-Klassen zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgenden Eigenschaften, um zu bestimmen, ob das System die von Discovery zurückgegebene IP-Adresse im CI-Datensatz eines Geräts ersetzen soll, wenn die Adresse nicht mit der einer Netzwerkschnittstelle (NIC) auf dem Gerät übereinstimmt. Das ist wichtig für die Erkennung von Geräten mit Verwaltungs-IP-Adressen, die sich von IP-Adressen unterscheiden, die einer oder mehreren NICs auf dem Gerät zugeordnet sind. Da die Verwaltungs-IP-Adresse eines Geräts im Erkennungszeitplan für dieses Gerät verwendet wird, handelt es sich hierbei um die Adresse, die von Discovery zurückgegeben wird. Verwenden Sie die folgenden Eigenschaften, um zu bestimmen, welche IP-Adresse für CIs einer beliebigen Klasse verwendet werden soll.

Feld	Beschreibung
glide.discovery.exclude_ip_sync_classes	Definiert CI-Klassen, deren IP-Adressen nicht ersetzt werden sollen, wenn die von Discovery zurückgegebene Adresse nicht mit einer der NICs des Geräts übereinstimmt. Verwenden Sie eine kommagetrennte Liste, um mehrere Klassen zu definieren. Vom System wird im CI-Datensatz standardmäßig die Verwaltungs-IP eines Lastenausgleichsmoduls verwendet, die von Discovery zurückgegeben wird, anstatt sie durch die IP-Adresse einer der NICs des Lastenausgleichsmoduls zu ersetzen. • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_lb
glide.discovery.enforce_unique_ips	Eindeutige IP-Adressen erzwingen: Die IP-Adresse wird ignoriert, nachdem nachfolgende Geräte von Discovery gefunden worden sind, die dieselbe IP-Adresse verwenden. Jedes Mal, wenn ein Computer, ein Drucker oder ein Netzwerkgerät mit einer gültigen IP-Adresse erkannt wird, wird das IP-Adressfeld aller anderen Geräte mit derselben IP-Adresse gelöscht. Wenn inaktiv, wird die IP-Adresse für jedes Gerät gespeichert. • **Typ**: true | false • **Standardwert**: false

Erstellen Sie einen schnellen IP-Bereich für einen Discovery Zeitplan

In Schnellbereichen können Administratoren IP-Adressen definieren, die in einer durch Kommas getrennten Zeichenfolge durchsucht werden, ohne dass separate Datensätze erstellt werden müssen.

Vorbereitungen

Für Kurzbereiche werden nur MID Server verwendet, die aktiv und validiert sind. Für die MID Server muss die Anwendung Discovery angegeben sein (oder ALLE Anwendungen), und die IP-Bereiche müssen konfiguriert sein, wenn Sie die automatische Auswahlfunktion im Erkennungszeitplan verwenden.

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können IP-Adressen in einem der folgenden Formate eingeben:

- Ein IP-Bereich, der durch einen Schrägstrich und die Anzahl der Bits im Subnetz festgelegt ist. Beispielsweise durchsucht der String 10.10.10.0/24 24-Bit-IP-Adressen von 10.10.10.0 bis 10.10.10.254.
- Ein IP-Bereich, der durch einen Bindestrich definiert wird. Der String 10.10.11.0-10.10.11.165 durchsucht beispielsweise die IP-Adressen von 10.10.11.0 bis 10.10.11.165.
- Eine durch Kommas getrennte Liste bestimmter IP-Adressen. Beispiel: Mit der Zeichenfolge 10.0.2.1,10.0.2.15 werden die IP-Adressen 10.0.2.1 und 110.0.2.15 gescannt.

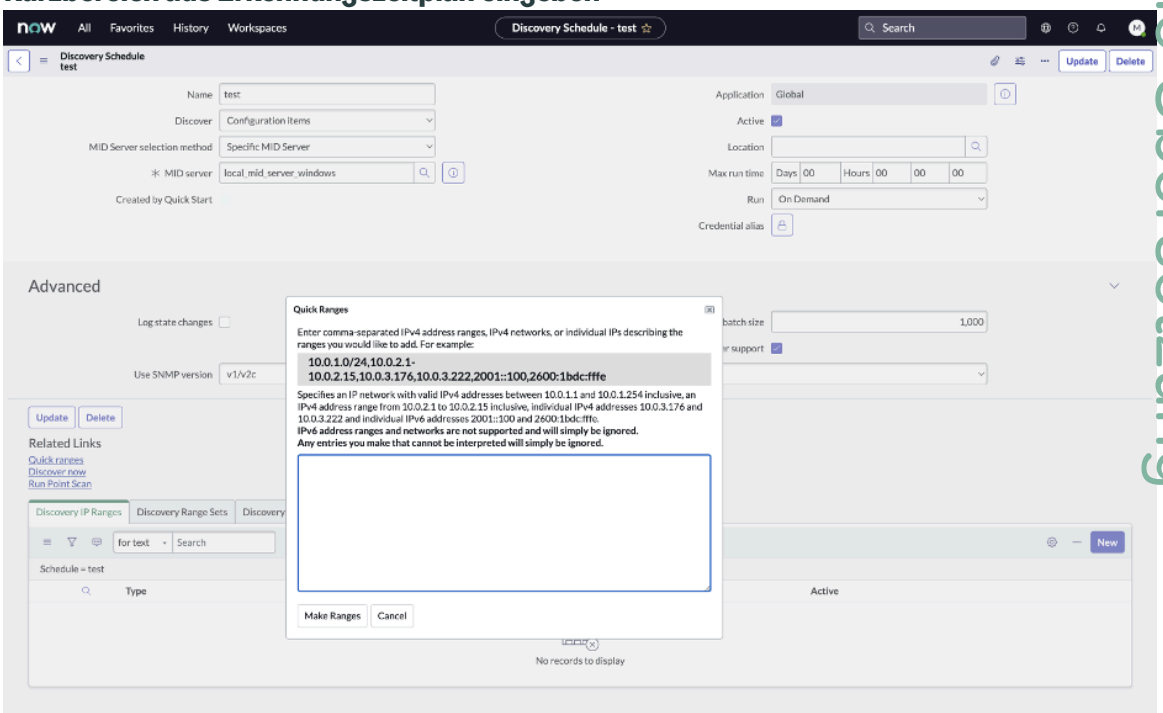
Hinweis: IPv6-Adressbereiche und -Netzwerke werden nicht unterstützt und entsprechend ignoriert. Alle anderen Eingaben, die nicht interpretiert werden können, werden ebenfalls ignoriert.

Prozedur

1. Klicken Sie im Formular „Discovery-Zeitplan“ auf den zugehörigen Link **Kurzbereiche**.
2. Geben Sie die IP-Bereiche und spezifischen IP-Adressen ein, die gescannt werden sollen.
3. Klicken Sie auf **Bereiche erstellen**.

Hinweis: Die Schnittstelle für den Kurzbereich dient nur zur Eingabe von IP-Adressen und kann nicht zum Bearbeiten von bereits übermittelten IP-Adressen verwendet werden.

Kurzbereich aus Erkennungszeitplan eingeben



Die Instanz zeigt die Einträge automatisch im richtigen Format an.

4. Wählen Sie zum Ändern von IP-Adressbereichen die IP-Adressdatensätze in der zugehörigen Liste **Discovery-Range Sets** aus.

Hinweis: Das Überschreibverhalten gilt nicht für Discovery Bereichssätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Bereiche mit Import Sets in Erkennungszeitpläne importieren

Eine Methode zur Eingabe einer großen Anzahl von IP-Netzwerken in Discovery-Zeitpläne ist die Verwendung von Importsätzen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Allgemeine Gruppen von IP-Adressen, die als Bereiche bezeichnet werden, können in erweiterten Erkennungszeitplänen verwendet werden.

Hinweis: Sie können auch die IPAM-Integration verwenden, um eine große Anzahl von IP-Netzwerken in Discovery-Zeitpläne einzugeben. Siehe IPAM-Integration Weitere Informationen finden Sie unter .

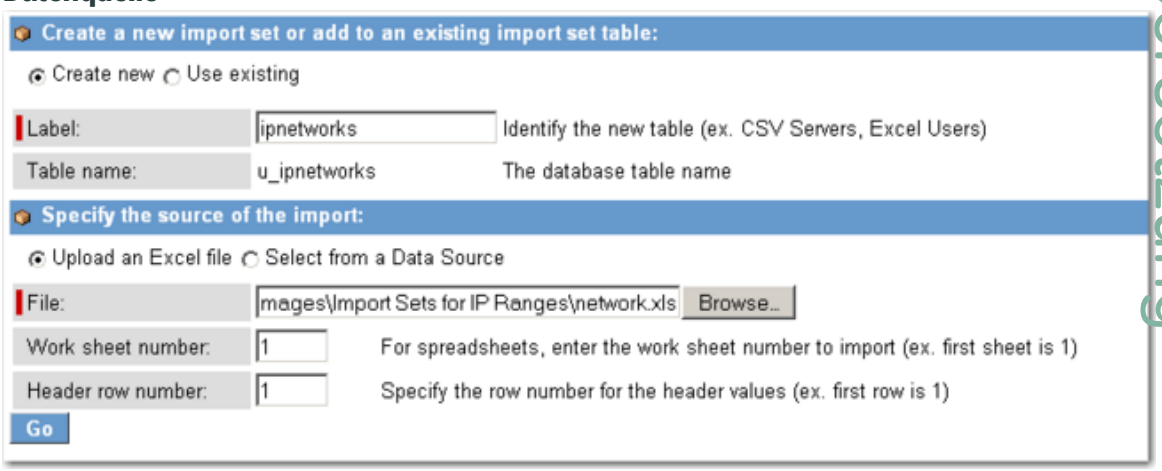
Verwenden Sie eine Datenquelle, die zugeordnet werden kann. Schließen Sie die folgenden Felder ein:

- Start-IP: Die erste IP-Adresse im Bereich (einschließlich)
- Ende-IP: Die letzte IP-Adresse im Bereich (einschließlich)

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Daten laden**an.
2. Identifizieren Sie die Datei oder Datenquelle, die die gewünschten Informationen enthält.
3. Erstellen Sie einen Tabellennamen, zum Beispiel `ipnetworks`.
4. Klicken Sie auf **Excel-Datei hochladen**, und navigieren Sie zur Quelldatei.
5. Klicken Sie auf **Start**, um die Datei zu importieren.

Datenquelle



6. Navigieren zu **System-Importsätze** > **Transformationszuordnung erstellen** Und ordnen Sie die Elemente in der Excel-Tabelle den Feldern der CMDB im IP-Bereich der Zieltabelle zu `[ip_address_Range]` Tabelle.
7. Weisen Sie der Transformationszuordnung einen eindeutigen und aussagekräftigen Namen zu.
8. Übermitteln Sie das Formular, und klicken Sie dann in der zugehörigen Liste **Feldkarten** auf **Neu**.
9. Ordnen Sie die Felder in der Excel-Tabelle den Feldern in der Tabelle „IP-Bereich“ `[ip_address_range]` zu. Für die folgenden Adressfelder benötigen Sie Werte: **Start-IP** und **Ende-IP**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf den zugehörigen Link **Zuordnungsassistent**, und verwenden Sie die angezeigten Listen, um die Felder zwischen Tabelle und Datenquelle (der Excel-Tabelle in diesem Beispiel) aufzulösen.
11. Klicken Sie auf **Speichern**.

    Daraufhin wird wieder das Formular „Tabellen-Transform Map“ angezeigt.
12. Klicken Sie unter „Zugehörige Links“ auf **Umwandeln**, um die Daten in die entsprechenden Felder in der Tabelle „IP-Bereich“ [ip_address_range] zu verschieben.

    Die importierten IP-Bereiche können jetzt in jedem erweiterten Erkennungszeitplan verwendet werden.

Schließen Sie IP-Bereiche aus einem aus Discovery Bereich festgelegt

Sie können einen Bereich von IP-Adressen angeben, die Sie aus Ihrem ausschließen möchten Discovery Abfrage.

Vorbereitungen

Bevor ein Discovery-Zeitplan ausgeführt wird, wird die Anzahl der ausgeschlossenen IP-Adressen summiert. Wenn mehr als 500.000 ausgeschlossene IP-Adressen vorhanden sind, wird die Erkennung abgebrochen, und über DiscoveryLogger wird ein Fehler in Bezug auf den Status protokolliert.

Hinweis: Das Ausschließen von IP-Adressen wird für IPv6-Bereiche oder -Subnetze nicht unterstützt.

Erforderliche Rolle: Discovery_admin oder Agent_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery Bereiche**an.
2. Wählen Sie eines der Range Sets aus.
3. Wählen Sie einen der Typen in der zugehörigen Liste **Discovery-IP-Bereiche** aus.
4. Klicken Sie in der zugehörigen Liste **Discovery-Bereichselement ausschließen** auf **Neu**.
5. Wählen Sie eine der folgenden Optionen aus **Typ** Dropdown-Liste.

Option	Beschreibung
IP-Adressenliste	Ermöglicht Ihnen das Ausschließen nicht aufeinanderfolgender IP-Adressen, indem Sie einzelne IP-Adressen im auflisten **Discovery-Bereichselement-IPs** Zugehörige Liste. **Hinweis:** Nachdem Sie ausgewählt haben **IP-Adressliste** Als **Typ** , Sie müssen mit der rechten Maustaste auf den Header klicken und auswählen **Speichern** Bevor Sie mit dem Hinzufügen von IPs zur zugehörigen Liste beginnen können.
IP-Adressenbereich	Ermöglicht es Ihnen, einen Bereich von IPs auszuschließen, indem Sie die Anfangs- und Endadressen angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
IP-Netzwerk	Ermöglicht Ihnen das Ausschließen eines IP-Netzwerks durch Angabe der Netzwerk-IP und der Netzwerkmaske.

6. Klicken Sie auf **Absenden**.

Globale Ausschlussliste für IP-Adressen und -Bereiche verwenden

Mithilfe der globalen Ausschlussliste können Administratoren globale IP-Ausschlusslisten definieren, die für alle Discovery-Zeitpläne gelten, anhand denen Konfigurationselemente, IP-Adressen oder Netzwerke erkannt werden. Die Liste hilft, den Zugriff auf sensible IPs zu verhindern, da sie die Erkennung blockiert, wenn sich die IP-Adresse in der Ausschlussliste befindet. Diese Funktion gilt nur für Horizontal Discovery Ab Rome-Release.

Vorbereitungen

Globale IP-Ausschlussbereiche sind standardmäßig aktiv. Deaktivieren Sie zum Deaktivieren die Option **Aktiv** Kontrollkästchen. Dadurch werden die Datensätze inaktiv, und die Einträge werden nicht aus Discovery ausgeschlossen. Sie können der globalen Ausschlussliste eine einzelne IP-Adresse oder einen IP-Bereich hinzufügen. Die Tabelle „IP-Ausschlussliste“ [ip_exclusion] verweist auf vorhandene IP-Erfassungstabellen und unterstützt drei Arten von Sammlungen: IP-Adressliste, IP-Adress-Subnetz und IP-Adressbereich.

Hinweis: Die Verwendung der globalen Ausschlussliste für IP-Adressen und -Bereiche wird für IPv6-Adressen nicht unterstützt. Während die Anwenderoberfläche weiterhin das Hinzufügen von IPv6-Adressen zur Liste ermöglicht, werden diese Adressen ignoriert und während des Ausschlussvorgangs übersprungen Discovery.

Erforderliche Rolle: Rolle „Discovery_admin“ oder „Agent_admin“

Prozedur

1. Navigieren zu **Alle** > **Globaler IP-Ausschluss** > **IP-Ausschluss**an.
2. Klicken Sie auf **Neu**, um einen neuen IP-Ausschlussdatensatz zu erstellen.
3. Klicken Sie im Feld „IP ausgeschlossen“ auf das Suchsymbol, um das Fenster „IP-Sammlungen“ aufzurufen.
4. Wählen Sie eine der aufgeführten IP-Sammlungen aus, oder klicken Sie auf **Neu**, um den Assistenten für IP-Sammlungen aufzurufen.
5. Wählen Sie im Assistenten für IP-Sammlungen eine der drei Arten von Sammlungen aus, die Sie erstellen möchten, und füllen Sie die erforderlichen Details aus.
   Für jeden Typ können Sie eine Beschreibung hinzufügen, warum Sie bestimmte IP-Adressen ausschließen möchten bzw. welche IP-Adressen ausgeschlossen werden.
   - IP-Adressbereich

     Füllen Sie die Details aus, und klicken Sie auf **Absenden**. Dieser neue Bereich wird der IP-Ausschlussliste hinzugefügt.
   - IP Address Subnet (IP-Adressen-Subnetz)

     Füllen Sie die Details aus, und klicken Sie auf **Absenden**. Dieses neue Subnetz wird der IP-Ausschlussliste hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP-Adressenliste

  Geben Sie den Namen ein, und **Speichern** Sie. Die zugehörige Liste wird am unteren Rand des Seite angezeigt. Wählen Sie in der Sammlungsliste ein vorhandenes Element aus, oder klicken Sie auf **Neu**, um eine neue Liste zu erstellen. Klicken Sie auf **Aktualisieren**. Merken Sie sich den von Ihnen erstellten Namen. Dieser neue Name wird der Sammlungsliste hinzugefügt. Wählen Sie diesen Namen aus der Liste aus, und klicken Sie erneut auf **Absenden**. Diese neue Adressliste wird der IP-Ausschlussliste hinzugefügt.

6. Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und wählen Sie einen Zeitplan aus.
7. Wenn der Zeitplan für die Erkennung von Konfigurationselementen, IP-Adressen oder Netzwerken vorgesehen ist, können Sie unten auf der Seite die Registerkarte „Globaler IP-Ausschluss“ sehen.

Ergebnis

Wenn die geplante Discovery ausgeführt wird, wird die Erkennung aller IP-Adressen übersprungen, die Teil des aktiven Datensatzes für den globalen IP-Ausschluss sind. Alle anderen IP-Adressen sollten erkannt werden.

Hinweis: Das Überschreibungsverhalten gilt nicht, wenn Discovery Zeitplan hat aktive globale IP-Ausschlüsse.

Wenn Sie versuchen, eine Schnell-Discovery auszuführen, die eine ausgeschlossene IP enthält, wird eine Fehlermeldung angezeigt, und Discovery wird nicht ausgelöst.

Domänentrennung und Erkennung

Die Domänentrennung wird in Discovery unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Übersicht über Domänentrennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können Daten nur in ihrer eigenen oder einer untergeordneten Domäne anzeigen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen können. Da die Unterstützung der Domänentrennung in Discovery als **Standard** gilt, erfolgt keine delegierte Verwaltung an die untergeordneten Domänen. Die SPs müssen die administrative Kontrolle behalten.

Funktionsweise der Domänentrennung in Discovery

Mehrere Domänen können durch einen einzelnen MID Server unterstützt werden. In Releases vor Kingston konnte jeder MID Server nur eine einzelne Domäne unterstützen. In neueren Releases ist das Trennen von Domänen nach MID Server nützlich, wenn die Domäne groß ist oder wenn sich die Ressourcen der Domäne im Rechenzentrum eines Kunden und nicht in dem eines SP befinden. Für Discovery auf MID Servern, die eine einzelne Domäne unterstützen, werden die erkannten CIs der Domäne des MID-Benutzers zugewiesen, der für die Authentifizierung gegenüber der ServiceNow-Instanz verwendet wird. Bei MID Servern mit mehreren Domänen werden die erkannten CIs der Domäne des Benutzers zugewiesen, der den Erkennungszeitplan erstellt hat.

Discovery implementiert die Trennung von Datendomänen durch den MID Server, indem während der Sensorverarbeitung die Identität des MID Server-Benutzers gewechselt wird. Discovery verwendet die Domäne, in der sich der MID Server-Benutzer befindet, um zu bestimmen, in welche Domäne die erkannten Daten eingefügt werden sollen. Discovery-Konfigurationsinformationen, einschließlich Klassifizierer, Bezeichner, Probes und Sensoren, werden nicht nach Domänen getrennt.

Service Provider verwenden in der Regel die IP-basierte Erkennung. In Fällen, in denen der SP die Netzwerkadressierung steuert, teilen sie den Adressraum auf ihre Kunden auf, um sicherzustellen, dass jede Domäne über einen eigenen IP-Adressraum verfügt. Der SP weist einem Kunden oder einer Domäne ein oder mehrere Subnetze zu und erstellt Erkennungszeitpläne für diese Subnetze.

Wenn der SP die Rechenzentren von Kunden remote verwaltet, kommt es häufig zu Überschneidungen zwischen Adressräumen, die von verschiedenen Kunden verwendet werden. In diesen Fällen kann der SP die Netzwerkadressübersetzung (NAT) für den IP-Bereich verwenden und einen Erkennungszeitplan ausführen.

Sobald die CIs der richtigen Domäne zugewiesen sind, werden Transparenz und Kontrolle über den Lese-/Schreibzugriff von der Plattform über die Domänenhierarchie bereitgestellt. Zeitpläne sind für Benutzer in ihren jeweiligen Domänen sichtbar. Domänenübergreifende Zeitplantransparenz ist nicht möglich, außer für den SP, der die übergeordnete Domäne steuert und für den alle Domänen sichtbar sind.

Domänentrennung für MID Server-Dateien

Sie können Versionen dieser spezifischen MID Server-Richtlinieneinträge erstellen, die nur ein MID Server aus derselben Domäne verwenden kann. Diese Prozesstrennung wird für Datensätze in Tabellen unterstützt, die die MID Server-synchronisierten Dateien [ecc_agent_sync_file] erweitern:

- MID Server-MIB-Datei [ecc_agent_mib]
- MID Server-JAR-Datei [ecc_agent_jar]
- MID Server-Skriptdatei [ecc_agent_script_files]

Standardmäßig sind alle Datensätze in diesen Tabellen Mitglieder der globalen Domäne. Ein Benutzer kann die globale Standarddomäne überschreiben und eine Version dieser Richtlinien zur Verwendung in der eigenen Domäne des Benutzers erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Anlagen in MIB- oder JAR-Dateisätzen werden möglicherweise nicht wie in einer Umgebung angezeigt, in der die Domäne nicht getrennt ist. Die Anhänge werden nicht angezeigt, weil die Tabelle **Anhänge** [sys_attachment] durch Daten getrennt ist. Wenn Daten zwischen Domänen aufgeteilt werden, kann ein Datensatz in einer untergeordneten Domäne nicht auf Datensätze in einer übergeordneten Domäne zugreifen.

Siehe MID-Server-Domänentrennung Anweisungen zum Einrichten der Domänentrennung über den MID-Server.

Domänengetrennte Tabellen

Datensätze in allen Tabellen, die die Tabelle „Grundlegendes Configuration Item“ [cmdb] erweitern, können nach Domänen getrennt werden. Darüber hinaus können Datensätze auch in den folgenden Tabellen nach Domänen getrennt werden:

- Seriennummer [cmdb_serial_number]
- TCP-Verbindung [cmdb_tcp]
- Fibre-Channel-Initiator [cmdb_fc_initiator]
- Fibre Channel-Ziele [cmdb_fc_target]
- IP-Adresse zu DNS-Name [cmdb_ip_address_dns_name]
- Service [cmdb_ip_service_ci]
- Virtuelles KVM-Gerät [cmdb_kvm_device]
- Load Balancer-Service-VLAN [cmdb_lb_service_vlan]
- Load Balancer VLAN-Schnittstelle [cmdb_lb_vlan_interface]
- Switch-Anschluss [cmdb_switch_port]

Zugehörige Informationen

Domänentrennung für Service Provider

Empfohlene Domain Separation-Verfahren für Service Provider

Discovery-Verhalten

Konfigurieren Sie domänengetrennt Discovery Zeitpläne

Konfigurieren des Anwenders „Ausführen als“ in einem Discovery Der Zeitplan leitet erkannte Konfigurationselemente (Configuration Items, CIs) an die richtige Domäne weiter und verwaltet die Datenisolierung.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

In domänengetrennten Umgebungen die Domäne des Anwenders, der einen erstellt Discovery Der Zeitplan bestimmt normalerweise, wo die erkannten Daten gespeichert werden. Durch das Zuweisen eines Anwenders „Ausführen als“ kann der Discovery-Prozess unter der Domäne und den Berechtigungen eines anderen Anwenders ausgeführt werden, sodass Administratoren steuern können, welche Domäne die Daten speichert und auf welche Ressourcen der Discovery-Prozess zugreifen kann, unabhängig davon, wer den Zeitplan erstellt hat.

Hinweis: Dieses Verfahren gilt nur für vorhandene Discovery Zeitpläne. Informationen zum Erstellen von Discovery Zeitplan, siehe Horizontale Erkennung planen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

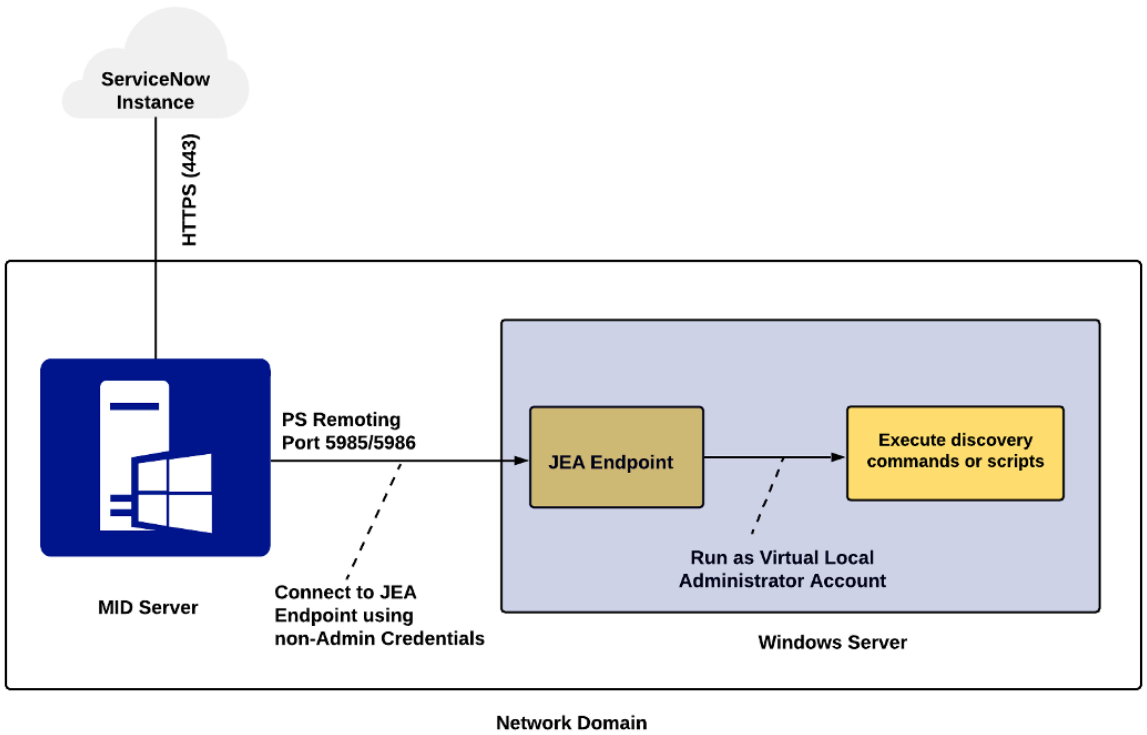
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. In **Name** Geben Sie den Namen des Zeitplans ein, den Sie konfigurieren möchten.
3. Doppelklicken Sie auf **Ausführen als** Feld für die Inline-Bearbeitung.
   Standardmäßig ist **Ausführen als** Spalte wird in der Tabelle „Discovery-Zeitpläne“ [Discovery_schedule] nicht angezeigt. Informationen zum Anpassen von Spalten in Tabellen finden Sie unter Personalisieren Sie eine Liste .
4. Geben Sie den Namen des Anwenders ein, als der Zeitplan ausgeführt werden soll.
5. Aktivieren Sie das Häkchen ( )-Symbol.

Microsoft Just Enough Administration (JEA) für Discovery

Microsoft JEA verbessert die Sicherheit, indem Benutzern ohne Administratorrechte der beschränkte Zugriff auf die für Discovery erforderlichen Befehle, Skripts und ausführbaren Dateien ermöglicht wird. Dadurch kann der MID-Server Informationen über einen Windows-Computer erfassen, ohne dass für das Ziel vollständige Administratorrechte erforderlich sind.

Microsoft JEA ermöglicht eine rollenbasierte Administration über PowerShell-Remoting, das Windows Remote Management (WinRM) zur Verwaltung der Kommunikation und Authentifizierung verwendet. Dieses Framework bietet eine sichere und zuverlässige Methode für die Verwaltung von Computern, die das HTTP-Protokoll verwenden. PowerShell-Remoting verwendet insgesamt zwei Ports (5985, 5986) für HTTP und HTTPS, was einfacher zu sichern ist als die Vielzahl von Ports, die bei der dynamischen WMI-Portzuordnung verwendet werden. Weitere Informationen zu Microsoft JEA finden Sie unter Just Enough Administration .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen für die Erkennung mit JEA

- ServiceNow-Instanz, auf der Release Rome oder höher ausgeführt wird.
- MID Server und Zielserver müssen Teil einer Windows-Domäne sein.
- Die JEA-Anmeldeinformationen, die nicht über Administratorrechte verfügen, müssen Anmeldeinformationen auf Domänenebene sein.
- Auf den Windows-Zielcomputern muss PowerShell 5.0 oder Windows Management Framework 5.1 installiert sein.
- Auf den Ziel-Windows-Computern muss PowerShell-Remoting aktiviert sein.

Hinweis: Zur Verbesserung der Sicherheit gibt es ab Rome ein neues Profil namens JEA v2. Microsoft rät davon ab, im JEA-Profil einen anderen Sprachmodus als **NoLanguage** anzugeben. JEA v2 legt den Sitzungstyp explizit auf **RestrictedRemoteServer** und den Sprachmodus auf **NoLanguage** fest, um zu verhindern, dass Benutzer am Endpunkt Skripts ausführen und Sicherheitsbeschränkungen umgehen können. ServiceNow unterstützt das vorhandene Beispielprofil in KB0782125 nicht mehr. Befolgen Sie die Anweisungen in KB0965705 , um JEA v2-Profile einzurichten und bereitzustellen.

JEA-Profile

Discovery mit JEA erfordert Profile, die aus einer PowerShell-Sitzungskonfiguration und mindestens einer PowerShell-Rollenfunktionsdatei bestehen. Sie können mehrere PowerShell-Rollenfunktionsdateien und mehrere Benutzergruppen erstellen, um die Rollen bei Bedarf verschiedenen Gruppen zuzuweisen. Ein Beispielprofil wird in KB0965705 als Referenzimplementierung bereitgestellt und dient als Ausgangspunkt. Die Konfigurationsdatei in der KB unterstützt alle sofort einsatzbereiten horizontalen Windows-Muster zum Zeitpunkt der Erstellung. ServiceNow ist nicht verantwortlich für die Bereitstellung und Einrichtung von JEA-Profilen auf Remotecomputern.

Microsoft bietet über die folgenden Links eine detaillierte Dokumentation:

- JEA-Rollenfunktionen
- JEA-Sitzungskonfiguration

Basiserkennung mit JEA-Beispielprofil

Das in KB0965705 bereitgestellte JEA-Beispielprofil wurde so konfiguriert, dass es viele grundlegende CIs und Attribute erkennt. Das Profil kann geändert werden und sollte nur als Baseline für die Erkennung mit JEA dienen.

Bei der Basiserkennung werden die folgenden Schlüsselattribute von Windows-Servern (cmdb_ci_win_server) und Windows-Desktops (cmdb_ci_computer) erkannt:

- Hostname
- DNS-Name
- Seriennummer
- Betriebssystem
- BS-Version
- BS-Service Pack
- Festplattenspeicher
- RAM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anzahl CPU-Kerne
- CPU-Anzahl
- CPU-Hersteller
- CPU-Typ

Darin eingeschlossen sind die folgenden CIs:

- Netzwerkadapter (cmdb_ci_network_adapter)
- Dateisystem (cmdb_ci_file_system)
- Speichergeräte (cmdb_ci_disk)
- Installierte Software (cmdb_software_instance)
- Laufende Prozesse (cmdb_running_process)
- Arbeitsspeichermodule (cmdb_ci_Memory_Module)
- Seriennummern (cmdb_serial_number)
- TCP/IP-Verbindung (cmdb_tcp)
- CI-IPs (cmdb_ci_ip_address)
- DNS-Namen für CIs (cmdb_ci_dns_name)
- Windows-Cluster (cmdb_ci_win_cluster, cmdb_ci_win_cluster_node, cmdb_ci_win_cluster_resource)
- Nachverfolgte Konfigurationsdateien (cmdb_ci_config_file_tracked)

Außerdem können die folgenden Anwendungs-CIs erkannt werden:

- MSSQL-DB unter Windows (cmdb_ci_db_mssql_instance)
- MySQL-DB unter Windows (cmdb_ci_db_mysql_instance)
- Oracle-DB unter Windows (cmdb_ci_db_mssql_instance)
- WebSphere unter Windows (cmdb_ci_app_server_websphere)

Zur Erkennung mit dem Beispielprofil werden die folgenden Probes und Muster verwendet:

- Windows - Classify (Probe)
- Windows OS - Servers (Muster)
- Windows OS - Desktops (Muster)
- Windows - Installed Software (Probe)
- Windows - ADM (Multi-Probe)
- My SQL Server On Windows (Muster)
- MSSql DB On Windows (Muster)
- Oracle DB on Windows (Muster)
- Windows - WebSphere - Cell (Probe)
- Windows - WebSphere - Web Applications (Probe)
- Windows - WebSphere - Web Services (Probe)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz für die Erkennung mit JEA vorbereiten

Um die ServiceNow®-Instanz für Discovery mit Microsoft Just Enough Administration (JEA) zu konfigurieren, definieren Sie die Windows-Anmeldeinformationen mit dem Domänennamen, und legen Sie die MID-Server-Konfigurationsparameter entsprechend fest.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** Und klicken Sie auf **Neu** .
2. Klicken Sie in der Liste mit den verfügbaren Anmeldeinformationsarten auf **Windows-Anmeldeinformationen**.
3. Erstellen Sie die Anmeldeinformationen für Nicht-Administratoren in folgendem Format für den **Benutzernamen**: *`domain\user name`*.
4. Senden Sie den Datensatz ab.
5. Navigieren zu **Alle** > **MID-Server** > **Server**an.
6. Wählen Sie ein aus **MID-Server** Zur Konfiguration aus der Liste der MID-Server.
7. Wählen Sie die zugehörige Liste **Konfigurationsparameter** aus.
8. Legen Sie Folgendes fest MID-Server-Konfigurationsparameter Wie angegeben:

   a. **mid.windows.management_protocol:** Dieser Parameter ist für die Erkennung mit JEA erforderlich. Der Standardwert lautet WMI, er muss jedoch auf MID Servern, die die Erkennung mit JEA verwenden, auf WinRM gesetzt werden.

   b. **Mid.powershell.jea.Endpunkt** : Dieser Parameter ist für Discovery mit JEA erforderlich.
   Dieser Parameter gibt den Namen des JEA-Endpunkts an, mit dem der MID Server auf Remotehosts eine Verbindung herstellt. Der Endpunktname wird beim Registrieren einer Konfigurationsdatei erstellt und darf nicht mit dem Namen der Konfigurationsdatei selbst verwechselt werden. Die Einstellung wirkt sich auf den gesamten MID Server aus, einschließlich WinRM-Remotesitzungen, die von Discovery auf dem MID Server erstellt wurden und auf diesen Endpunkt verweisen.

   Beispiel: Der PowerShell-Befehl **Register-PSConfiguration -name JEA_DISCO_V2 -path <session_configuration_file>** legt den Endpunktnamen auf JEA_DISCO_V2 fest. In diesem Fall muss **mid.powershell.jea.endpoint** auf JEA_DISCO_V2 aktualisiert werden.

9. **Wahlweise:** Verwenden Sie Folgendes MID-Server-Eigenschaft Und Systemeigenschaft So beheben Sie Probleme:

   a. **mid.probe.collect_debug_info** : Dies ist eine optionale MID-Server-Eigenschaft zum Sammeln von Debug-Informationen.
   Wenn diese Eigenschaft auf „true“ festgelegt ist, erfasst der MID Server Debug-Informationen zu Anmeldeinformationen und speichert sie in der Nutzlast der ECC-Eingabenachricht. Dies hat keine Auswirkungen auf die Funktionsweise von JEA.

   b. **Glide.Discovery.log_Debug_info** : Dies ist eine optionale Systemeigenschaft zum Sammeln von Debug-Informationen.
   Wenn diese Eigenschaft auf „true“ festgelegt ist, extrahiert der Erkennungssensor die Debug-Informationen aus der ECC-Eingabenachricht und schreibt diese in die Erkennungsprotokolltabelle, sodass sie beim Überprüfen des Erkennungsstatus sichtbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMP-Unterstützung für Discovery

Discovery bietet Unterstützung für die SNMP-Versionen 1, 2c und 3. Wenn Sie über aktive SNMP-v3-Anmeldeinformationen verfügen, sind die gültigen Optionen für die SNMP-Version „v3“ oder „Alle“. Wenn Sie über aktive SNMP-v1- oder SNMP-v2-Anmeldeinformationen (Community-Zeichenfolge) verfügen, sind gültige Optionen für die SNMP-Version „v1“, „v2c“ oder „Alle“. Der Standardwert ist „Alle“.

MID Server unterstützen standardmäßig alle SNMP-Protokollversionen. Sie können einen MID Server so einstellen, dass er nur bestimmte Versionen von SNMP unterstützt.

Informationen zu SNMP-Anmeldeinformationen finden Sie unter SNMP-Anmeldeinformationen .

SNMP-Probe-Parameter können bei der Erkennung eines SNMP-Geräts verwendet werden. Siehe SNMP-Probe-Parameter Weitere Informationen finden Sie unter .

SNMPv3-Benutzeranmeldeinformationen in Discovery hinzufügen

Richten Sie Ihre Anmeldeinformationen so ein, dass Discovery auf SNMPv3-Ziele zugreifen kann.

Vorbereitungen

Erforderliche Rolle: Administrator

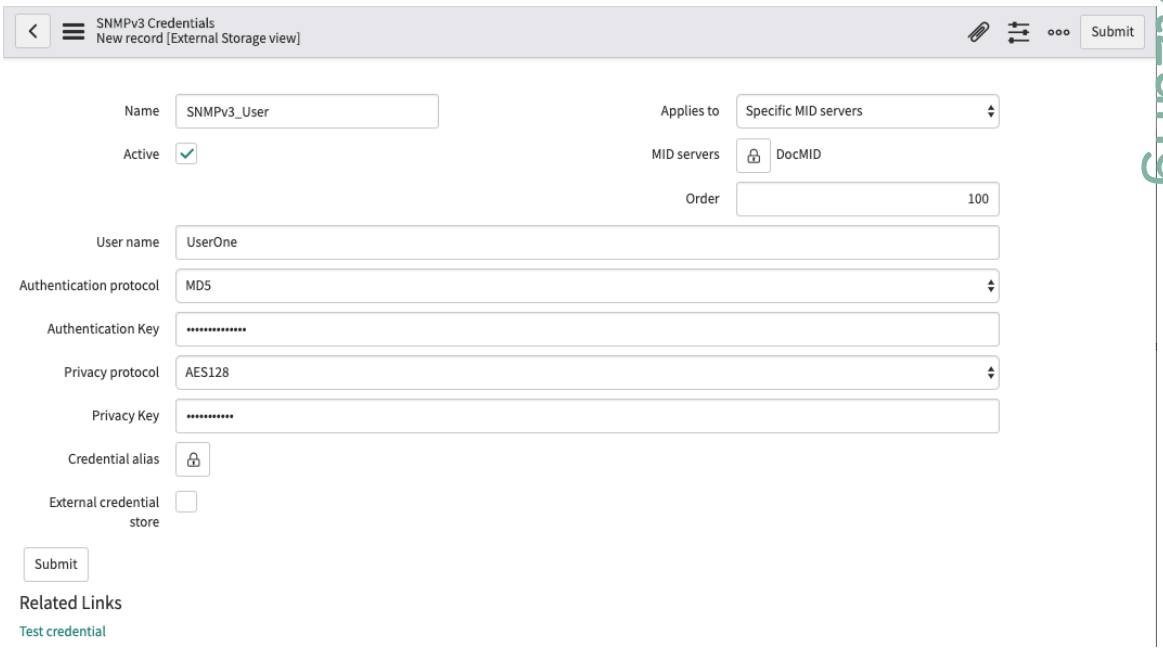
Warum und wann dieser Vorgang ausgeführt wird

Es ist auch ein MID Server-Parameter zum Steuern der SNMP-Versionen verfügbar. Siehe MID-Server-Parameter .

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **SNMPv3-Anmeldeinformationen**.
4. Füllen Sie das Formular mithilfe der Felder in der Tabelle.

Formular für SNMPv3-Anmeldeinformationen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SNMP-Community Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Sequenz) in der DiscoveryVersucht diese Anmeldeinformationen, während versucht wird, sich bei Geräten anzumelden. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername	Geben Sie den SNMP-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Benutzernamen erkennt.
Authentifizierungsprotokoll	Wählen Sie den Authentifizierungstyp aus, der für diese Anmeldeinformationen verwendet werden soll. Die Auswahlmöglichkeiten sind: ○ MD5 ○ SHA-1 ○ SHA-224 ○ SHA-256 ○ SHA-384 ○ SHA-512
Authentifizierungsschlüssel	Geben Sie den mit diesen Anmeldeinformationen zu verwendenden Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Wählen Sie das Verschlüsselungsprotokoll für diese Anmeldeinformationen aus. Die Auswahlmöglichkeiten sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	○ 3DES ○ AES128 ○ AES192 ○ AES256 ○ DES
Datenschutzschlüssel	Geben Sie den Schlüssel ein, der dem ausgewählten Datenschutzprotokoll zugeordnet ist.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für einen externen Anmeldeinformationsanbieter auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Speicher für Berechtigungsnachweise** aktiviert ist.
Datenschutz-Anmeldeinformations-ID	Geben Sie den für SNMPv3-Anmeldeinformationen konfigurierten Datenschutzkonto-Schlüssel in CyberArk ein. Wenn Sie ein Datenschutzprotokoll in CyberArk verwenden, muss dieses Feld denselben Wert aufweisen wie das Feld **Name** für das CyberArk-SNMPv3-Datenschutzkonto. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Eine externe Speicherung von Anmeldeinformationen ist nur verfügbar, wenn das External Credential Storage-Plugin aktiviert und die Ansicht **Externer Speicher** ausgewählt ist.
Anmeldeinformationsspeicher-Typ	Wählen Sie den Provider für den externen Speicher aus. Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.
Kontext verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen Kontextwert für diese Anmeldeinformationen hinzuzufügen. Dieses Feld wird in der **Discovery**-Ansicht angezeigt. Kontexte werden derzeit für externe Anmeldeinformationsspeicher nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	Hinweis: Ein Kontext ist eine Sammlung von Verwaltungsinformationen, auf die SNMPv3-Anmeldeinformationen zugreifen, in denen auf eine bestimmte OID verwiesen wird. Auf Kontexte wird manchmal verwiesen, damit Informationen über das Gerät gesammelt werden können, auf die mit den normalen Anmeldeinformationen nicht zugegriffen werden kann. Ein Kontext kann vom Hersteller bereitgestellt oder separat konfiguriert werden. Wenn Sie über mehrere SNMPv3-Anmeldeinformationen mit demselben Benutzernamen und denselben Schlüsseln verfügen, einige Ihrer Geräte jedoch einen Kontext benötigen und andere nicht, müssen Sie für jedes Gerät separate Datensätze erstellen.
Kontextname	Geben Sie den Kontextnamenswert für diese Anmeldeinformationen ein. Diese Option sollte nur verwendet werden, wenn Sie über Geräte verfügen, die diesen Wert für einen vollständigen Zugriff benötigen. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Kontext verwenden** aktiviert ist.

SNMPv3-Sicherheitsoptionen

Option	Zu konfigurierende Felder
noAuthNoPriv-Sicherheit	○ **Authentifizierungsprotokoll:** Keins ○ **Datenschutzprotokoll:** Keins ○ **Authentifizierungsschlüssel:** Leer lassen ○ **Datenschutzschlüssel:** Leer lassen
authNoPriv-Sicherheit	○ **Authentifizierungsprotokoll:** Festgelegt ○ **Datenschutzprotokoll:** Leer lassen ○ **Authentifizierungsschlüssel:** Festgelegt ○ **Datenschutzschlüssel:** Leer lassen
authPriv	○ **Authentifizierungsprotokoll:** Festgelegt ○ **Datenschutzprotokoll:** Festgelegt ○ **Authentifizierungsschlüssel:** Festgelegt ○ **Datenschutzschlüssel:** Festgelegt

SNMP-Version für Erkennungszeitplan festlegen

Sie müssen auch die SNMP-Version festlegen, nachdem Sie die entsprechenden Anmeldeinformationen ausgewählt haben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Es ist auch ein MID Server-Parameter zum Steuern der SNMP-Versionen verfügbar. Siehe MID-Server-Parameter .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**> *Ihr Discovery-Zeitplan.*
2. Wählen Sie im Feld **SNMP-Version verwenden** die entsprechende Version aus.

   Der Standardwert lautet **ALLE**. Sie können den Wert in **v1**, **v2c** oder **v3** ändern.

Discovery und SCCM zusammen

Verwenden Sie die folgenden Richtlinien, um häufige Probleme zu vermeiden, wenn Sie Discovery und System Center Configuration Manager (SCCM) gemeinsam verwenden.

Sie müssen entscheiden, ob Sie AI- oder Nicht-AI-Softwaredatenquellen (AI = Asset-Intelligenz) verwenden. Da die Softwarekorrelationsdaten für jede dieser Datenquellen unterschiedlich nachverfolgt werden, sollten Sie vermeiden, zwischen beiden hin- und herzuwechseln. Wenn Sie zwischen Datenquellen wechseln müssen, entfernen Sie vor dem Wechsel alle von SCCM importierten Softwareinstallationsdatensätze.

Wenn Software Asset Management nicht aktiviert ist, werden Softwareinstallationsdatensätze in der Tabelle „Softwareinstanz“ [cmdb_software_instance] gespeichert. Wenn Software Asset Management aktiviert ist, werden Softwareinstallationsdatensätze in der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] gespeichert.

Hinweis: Wenn Datensätze vor dem Wechsel nicht entfernt werden, sind möglicherweise doppelte Datensätze vorhanden. Falls AI- und Nicht-AI-Daten gemischt wurden, löschen Sie die Tabelle „Softwareinstallation“.

Übersicht über Service Graph Connector für Microsoft SCCM

Verwenden Sie Service Graph Connector für Microsoft SCCM, um Daten aus SCCM in die ServiceNow-Instanz abzurufen. Siehe Service Graph Connector für Microsoft SCCM Für weitere Details.

Hinweis: Wenn Sie Ihre Instanz auf eine Version von upgraden ServiceNow AI Platform Wenn Ihre SCCM-Version nicht unterstützt wird, können Sie diese Version weiterhin verwenden. Alle neuen Instanzen erfordern jedoch die Verwendung einer unterstützten SCCM-Version.

Upgrade auf neue Version

Die ServiceNow-SCCM-Integrationen sind in sich abgeschlossen und können unabhängig vorhanden sein. Für sie werden jeweils eigene Importsatztabellen, Datenquellen und Transformationszuordnungen verwendet. Von allen SCCM-Integrationen werden jedoch Daten in dieselben Tabellen innerhalb der ServiceNow-CMDB umgewandelt. So vermeiden Sie, dass die Daten von einer anderen Quelle überschrieben werden:

- Verwenden Sie eine einzige SCCM-Integration, und deaktivieren Sie alle anderen geplanten SCCM-Importe.
- Führen Sie einen vollständigen Import durch, um die Tabellen „cmdb_software_instance“, „cmdb_sam_sw_install“ und andere Tabellen alter SCCM-Daten zu löschen.

Softwaredaten mit SCCM oder Discovery erfassen

Wenn Discovery und SCCM auf einem System aktiviert sind, können sich die von beiden Tools erkannten Softwaredatensätze gegenseitig überschreiben.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Um festzulegen, wie Softwaredaten erfasst werden, konfigurieren Sie die Eigenschaft *glide.discovery.software_sccm_managed*.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Eigenschaften**an.
2. Legen Sie die Eigenschaft **Windows-Software wird von SCCM verwaltet** (*glide.discovery.software_sccm_managed*) entsprechend fest.
   Wenn diese Eigenschaft auf **Ja** festgelegt wird, wird die Software für Computer-CIs in der CMDB durch SCCM gefüllt. Ein interner Prozess bestimmt, dass der Computer von SCCM verwaltet wird, und Discovery füllt die Softwaredatensätze für Windows-Softwaredaten nicht. Die folgende Nachricht auf Informationsebene wird in die Discovery-Protokolldatei geschrieben.

   ```
   Software wird nicht gefüllt, da das CI von SCCM verwaltet wird
   ```

   Wenn das Kontrollkästchen deaktiviert ist, wird die Eigenschaft auf **Nein** festgelegt, und das System verwaltet Softwaredaten mit Windows.
3. Klicken Sie auf **Speichern**.

Wichtig: Wenn die SCCM-Integration aktiv ist, bevor Discovery aktiviert wird, und die Eigenschaft aktiviert ist, ignoriert Discovery das Füllen der Software für alle CIs, die auch über SCCM importiert werden. Wenn Discovery vor der SCCM-Integration aktiviert wird, können sich Softwareinstallationsdaten aus beiden Quellen vermischen.

Nächste Maßnahme

Verwenden Sie diese Discovery-Eigenschaften, um Diskrepanzen zwischen Softwaredaten zwischen Discovery und SCCM zu vermeiden: *glide.discovery.enable.software_simplify*Und *glide.discovery.enable.software_simplify_sccm*. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Discovery-Klassifizierer

Ein Klassifizierer teilt Discovery mit, welche Probes für die Identifizierungs- und Erkundungsphase der Erkennung ausgelöst werden sollen. Klassifizierer können auch die Probe „Horizontal Pattern“ auslösen, der anstelle von zusätzlichen Probes ein Muster für die Identifizierung und Erkundung startet.

Im Wesentlichen startet der Klassifizierer die Identifizierungsphase. Diese wird von Discovery verwendet, nachdem die Klassifizierungs-Probe wichtige Parameter an die Instanz zurückgegeben hat, die Discovery mitteilen, was als Nächstes zu tun ist.

In den meisten Fällen ist es nicht erforderlich, einen Klassifizierer zu erstellen oder einen Klassifizierer zu ändern. Wenn Sie jedoch Probleme mit der horizontalen Erkennung haben, sollten Sie gegebenenfalls die Bedingungen überprüfen, die bestimmen, wann ein Klassifizierer basierend auf den Parametern, die die Klassifizierungs-Probe an die Instanz zurückgibt, ausgeführt wird. Oder wenn Sie eine neue Art von CI erkennen möchten, die Discovery noch nicht erkennt, können Sie einen eigenen Klassifizierer erstellen.

Klassifizierung von Geräten, Prozessen und IP-Adressen

Die Discovery-Klassifizierung lässt sich in drei Typen unterteilen: Geräteklassifizierung, Prozessklassifizierung und IP-Adressklassifizierung (bzw. IP-Scan-Klassifizierung):

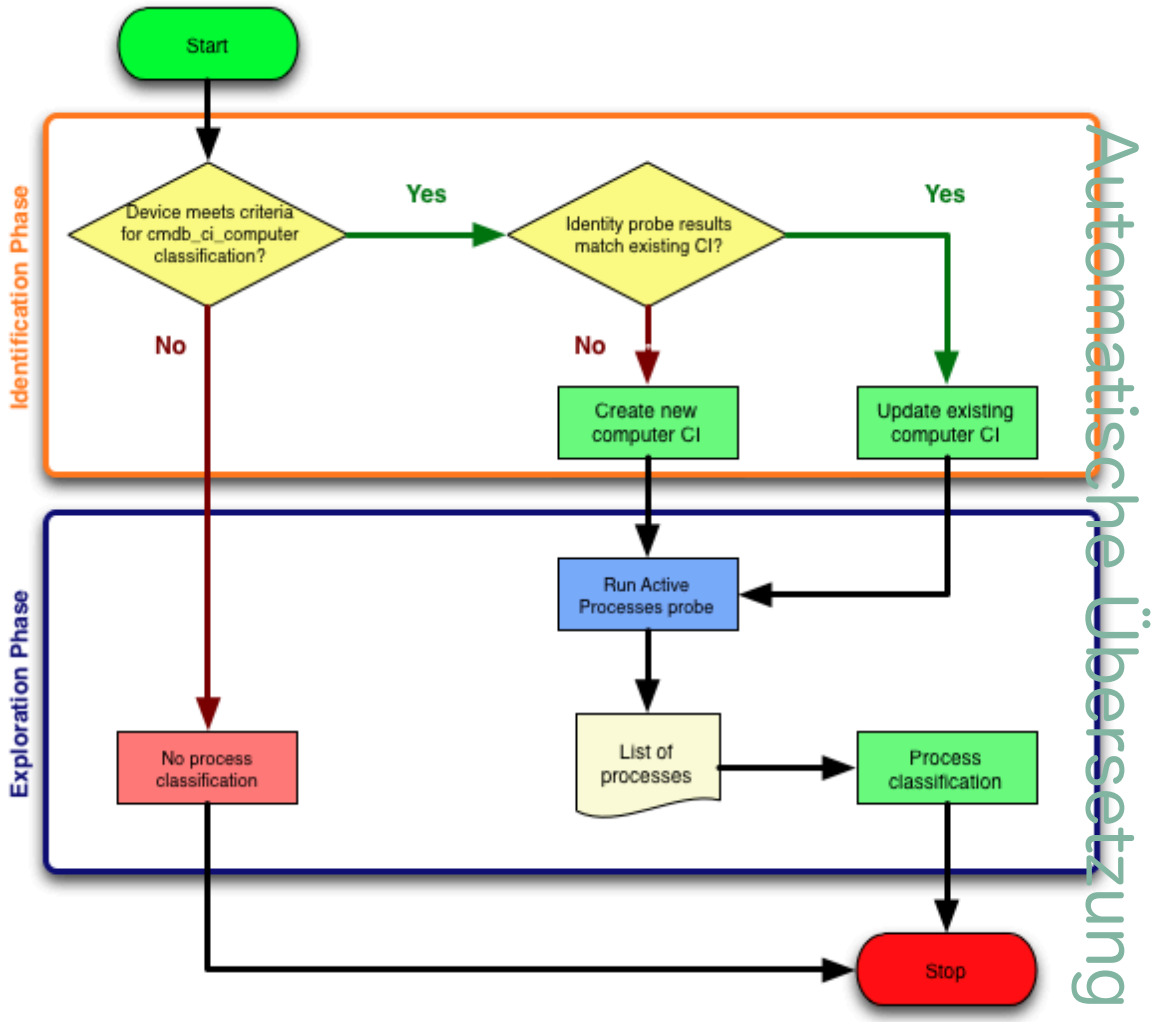
Geräteklassifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Klassifizierung der tatsächlichen Gerätetypen, zum Beispiel ein Computer mit Windows, ein Computer mit einer Flavour-Version oder UNIX oder LINUX, ein Router, ein Switch oder ein Lastenausgleichsmodul usw.

Wenn Discovery ein Computer-CI erkennt, wird eine aktive Prozess-Probe ausgelöst, um die Erkundung des Computer-CI voranzutreiben. Discovery vergleicht die Ergebnisse der aktiven Prozess-Probe mit den Prozessklassifizierungsbedingungen, um festzustellen, ob eine Übereinstimmung vorliegt.

Workflow der Klassifizierung von Computer-CIs



Ab dem Madrid-Release kann der horizontale Erkennungsprozess Geräte mit HTTP klassifizieren.

Von allen Protokollen, die Discovery verwenden (einschließlich WMI, SSH und SNMP), hat HTTP standardmäßig die niedrigste Priorität. Discovery verwendet die HTTP-Klassifizierung nur unter folgenden Umständen:

- Shazzam stellt fest, dass die Ports für den HTTP- (80) - und HTTPS-Verkehr (443) offen sind.
- Der horizontale Erkennungsprozess schlägt für die Port-Sonden mit höherer Priorität (WMI, SSH und SNMP) fehl, wenn die Ports für diese Protokolle nicht geöffnet sind oder wenn die Erkennung dieser Protokolle fehlschlägt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der horizontale Erkennungsprozess kann beispielsweise fehlschlagen, wenn SSH- und SNMP-Anmeldeinformationen nicht konfiguriert oder falsch sind.

Hinweis: Siehe Port-Sonden für weitere Informationen zur Funktionsweise von Port-Scanning und die Prioritäten der verschiedenen Protokolle.

Die HTTP-Klassifizierung startet die Sonde **HTTP Klassifizierung**, um das Gerät zu klassifizieren. Die Sonde **HTTP - Klassifizierung** führt eine GET-Anforderung für jedes Gerät für jede HTTP-Klassifizierung aus. Die URL der Anfrage setzt sich wie folgt zusammen: `PROTOCOL://IP:PORT/PATH`, wobei Folgendes gilt:

Weitere Informationen zu Port-Probes finden Sie unter Port-Sonden. Anweisungen zum Erstellen eines HTTP-Klassifizierern finden Sie unter HTTP-Klassifizierung erstellen.

Prozessklassifizierung

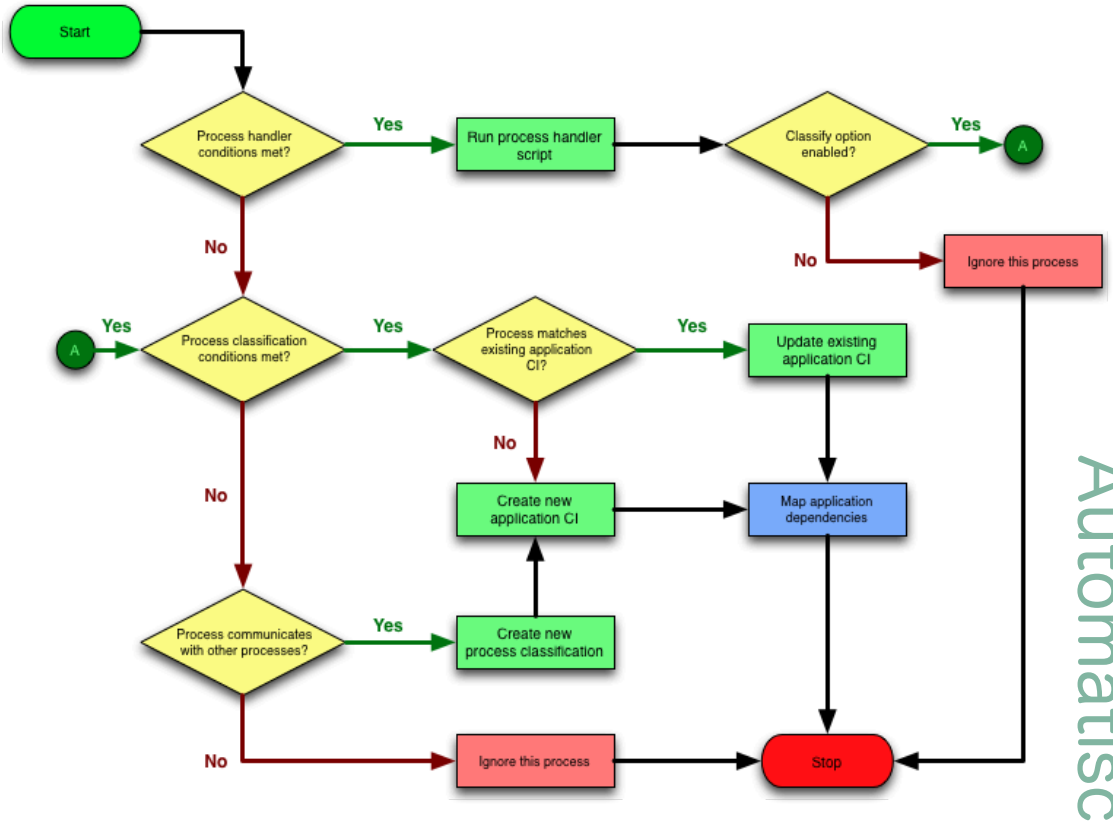
Das ist die Klassifizierung von Anwendungen basierend auf laufenden Prozessen.

Nachdem Geräte in der Tabelle „Computer“ [cmdb_ci_computer] und deren Erweiterungen identifiziert wurden, klassifiziert Discovery Prozesse während der letzten Phase der Erkennung: der Erkundungsphase. Genau wie in der Geräteklassifizierung gibt es auch in der *Prozessklassifizierung* eigene Klassifizierungskriterien und die Möglichkeit, Probes zu starten. Im Gegensatz zur Geräteklassifizierung werden jedoch bei der Prozessklassifizierung untergeordnete Konfigurationselemente (CIs) mit Beziehungen der Art *Wird ausgeführt auf::Wird ausgeführt* erstellt. Standardmäßig enthält Discovery Klassifizierungen für die gängigsten Prozesse.

Wenn ein Prozess den Klassifizierungskriterien entspricht, legt Discovery fest, ob das Prozess-Handler-Skript ausgeführt werden soll. Dieses Skript ändert die Parameterdaten, um Discovery dabei zu unterstützen zu erkennen, ob der Prozess ein vorhandenes oder neues Anwendungs-CI darstellt. Noch vor der Prozessklassifizierung verhindern Discovery-Prozess-Handler die Erstellung doppelter CIs, indem Parameter herausgefiltert werden, von denen bekannt ist, dass sie inkonsistente Werte enthalten. Jedes Mal, wenn Discovery ein Anwendungs-CI hinzufügt oder aktualisiert, wird auch die Zuordnung von Anwendungsabhängigkeiten des Anwendungs-CI von anderen CIs in der CMDB bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow der Klassifizierung von Prozessen



IP-Adressklassifizierung (IP-Scan)

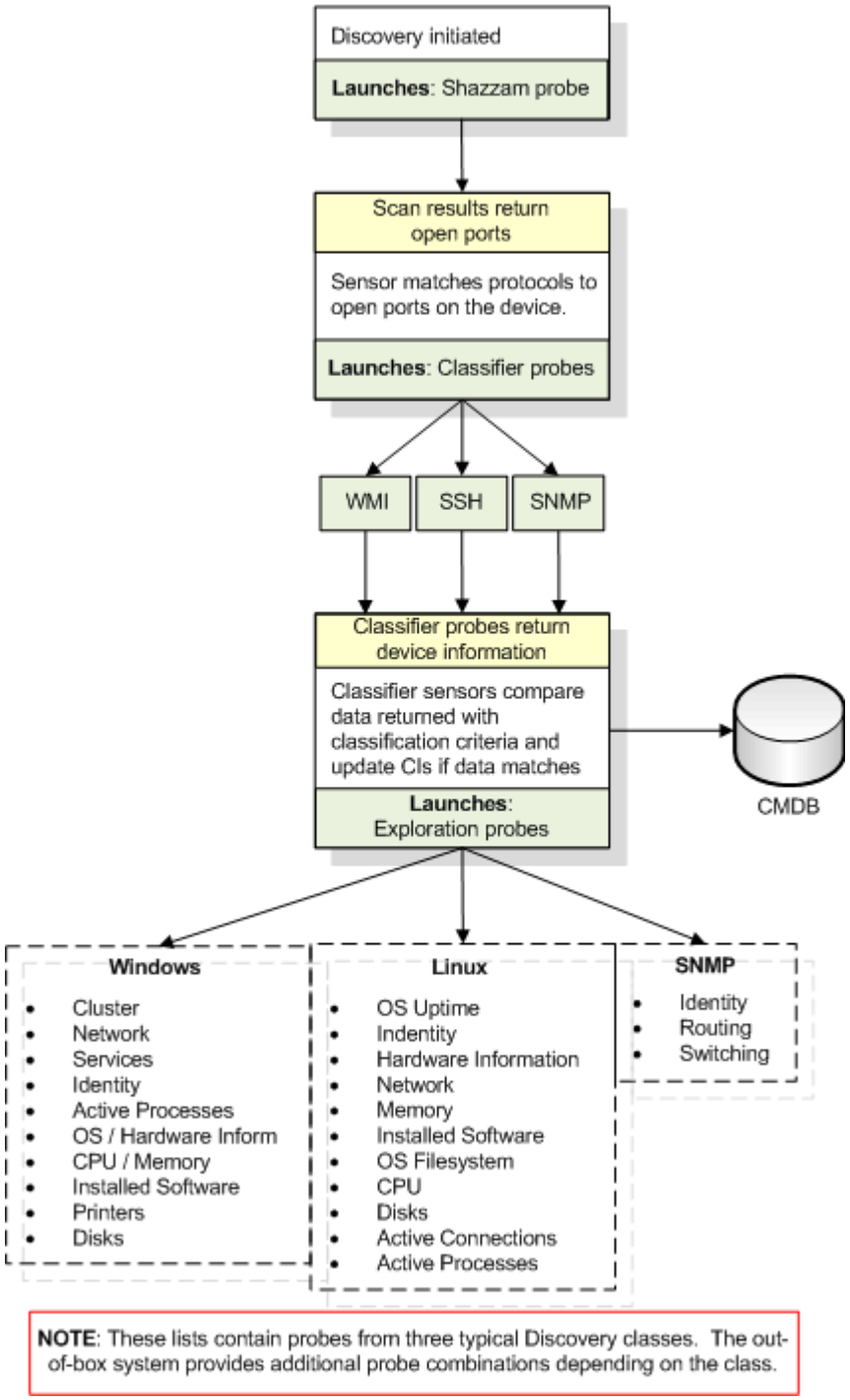
Die Erkennung von IP-Adressen erfolgt ohne Anmeldeinformationen, was bedeutet, dass Geräte und Software nur anhand der gefundenen offenen Ports und Banner identifiziert werden, ohne dass Sie Anmeldeinformationen erstellen müssen. Wenn die Klassifizierungskriterien für ein Gerät im IP-Scan-Modus erfüllt sind, aktualisiert Discovery automatisch das CI in der CMDB. Nachdem ein Gerät ordnungsgemäß klassifiziert wurde, startet Discovery die für diese Geräteklasse konfigurierten Erkundungs-Probes und beginnt mit der Erfassung detaillierter Informationen über das CI.

Im Discovery-Standardsystem löst die Linux-Klassifizierung elf Erkundungs-Probes aus, die Informationen wie Datenträgergröße, Arbeitsspeicher und die Anzahl der aktuellen Verbindungen zurückgeben. Die Daten dieser Probes werden zu unterschiedlichen Zeiten zurückgegeben und in der ECC-Warteschlange gespeichert, bis die Verarbeitung abgeschlossen ist.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit einem IP-Scan (keine Bezeichner):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Scan-Klassifizierung



Unter Klassifizierung für Erkennung von IP-Adressen finden Sie weitere Details zu den Parametern, die Klassifizierern für diesen Typ von Erkennung zur Verfügung stehen.

Klassifiziererkriterien

Klassifizierer stellen auch Kriterien bereit, mit denen Sie angeben können, wann Discovery den Klassifizierer unter den von Ihnen definierten Bedingungen verwenden soll. Die Kriterien basieren auf den Parametern, die eine Klassifizierer-Probe an Discovery zurückgibt. Kriterien werden mit dem Parameter, einem Operator und einem Wert erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet.

Klassifizierer und Muster

Zur Identifizierung und Erkundung von CIs kann Discovery anstelle von Probes auch Muster verwenden. Discovery löst Muster über die Probe „Horizontal Discovery“ aus, die für einen Klassifizierer angegeben werden kann. Sie können eigene Muster erstellen und über die Probe „Horizontal Discovery“ einem Klassifizierer hinzufügen. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen. Möglicherweise verwenden Sie bereits eines der vordefinierten Muster, die mit Discovery bereitgestellt werden. Sie können dies überprüfen, indem Sie im Klassifizierer überprüfen, ob die Probe „Horizontal Pattern“ angegeben ist.

Debugging-Informationen zur Klassifizierung protokollieren

Fügen Sie die folgende Systemeigenschaft hinzu, um Debugging-Informationen zu Klassifizierungen zu protokollieren. Die resultierenden Protokolleinträge listen den Namen jedes ausgeführten Klassifizierers auf sowie alle Namen und Werte, die den Kriterien im Klassifizierer zur Verfügung stehen.

Systemeigenschaft	Beschreibung
glide.discovery.debug.classification	Aktiviert Debugging-Informationen für die Prozessklassifizierung. • **Typ**: true | false • **Standardwert**: false • **Speicherort**: Zu Tabelle „Systemeigenschaften“ [sys_properties] hinzufügen. Weitere Informationen finden Sie unter Systemeigenschaft hinzufügen .

Möglichkeiten der Discovery-Klassifizierung

- Erstellen oder ändern Sie einen Erkennungsklassifizierer, wenn Sie CIs klassifizieren möchten, die von Discovery noch nicht klassifiziert werden, oder wenn Sie andere Probes auslösen möchten, die sich noch nicht in einem Klassifizierer befinden. Sie können Klassifizierer ändern, die Discovery für die Standard-CI-Erkennung, für Prozessklassifizierer für Anwendungen und für Klassifizierer basierend auf IP-Adress-Scans verwendet.

  Bevor Sie Klassifizierer ändern, prüfen Sie die Parameter, die für jeden Klassifiziererтyp verfügbar sind.

- Wenn sich Windows-Computer in Ihrem Netzwerk befinden, können Sie anstelle von WMI das WinRM-Protokoll verwenden, um für eine effizientere Datenübertragung und Ausführung von Remotebefehlen zu sorgen. Standardmäßig verwendet Discovery WMI. Anweisungen zu den Klassifiziereränderungen, die Sie mit WinRM vornehmen können, finden Sie unter Windows-Remoteverwaltung für Klassifizierung verwenden.
- Wenn Sie Windows-Computer haben, die als Server fungieren, und Sie möchten, dass sie nach ihrer Funktion und nicht nach dem Betriebssystem klassifiziert werden, können Sie die Kriterien des Klassifizierers „Windows“ ändern. Anweisungen dazu finden Sie unter Neuklassifizierung von Windows Workstation-Computers als Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-CI-Klassifizierung erstellen

Eine CI-Klassifizierung ermöglicht Discovery die Erkennung der gängigsten Betriebssysteme, Netzwerkgeräte und Prozesse.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Das Hinzufügen von SNMP-OID-Klassifizierungen mit einer Net-SNMP-Modul-OID ab 1.3.6.1.4.1.8072.3.2 oder einer Windows-Betriebssystem-OID ab 1.3.6.1.4.1.311.1.1.3 kann zu einer falschen Klassifizierung von Geräten und falschen Modellnamen führen und ist nicht mehr zulässig. Dies sind Vorlagensystem-OIDs, die auf einem Gerät verbleiben können, wenn der Hersteller sie nicht durch spezifische OIDs für ihr eigenes Modell ersetzt. Beispielsweise kann eine Check Point Smart-1 3050 Firewall, die Linux als Betriebssystem verwendet, die OID für einen Linux-Server (1.3.6.1.4.1.8072.3.2.10) aufweisen. Das führt dazu, dass die Firewall falsch klassifiziert wird. Wenn mindestens zwei Geräte dieselbe OID aufweisen, konfigurieren Sie Klassifizierungskriterien, die die Geräte voneinander unterscheiden. Weitere Details hierzu finden Sie in KB0751287 .

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung**an.
2. Wählen Sie den Typ der Klassifizierung aus, die Sie erstellen möchten.
3. Klicken Sie in der Liste der Klassifizierungen für den ausgewählten Typ auf **Neu**.
4. Füllen Sie das Formular anhand der Felder in der Tabelle aus.

Felder im Klassifizierungsformular

Feld	Eingabewert
Name	Name des Konfigurationselements (CI)
OID	SNMP-System-OID zum Abgleich dieses Geräts. Wenn der OID-Wert mit dem eines SNMP-Geräts übereinstimmt, verwendet Discovery die Informationen, um die CMDB mit dem angegebenen Hersteller, Modell und Klassifizierer zu füllen.
Operator	Operator zur Bestimmung der Übereinstimmung und der SNMP-OID. Die Auswahlmöglichkeiten lauten **Ist** und **Beginnt mit**. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP-System-OIDs“ verfügbar.
Aktiv	Aktiviert oder deaktiviert diesen Klassifizierer. Wenn ein Klassifizierer deaktiviert ist, stoppt das System die Klassifizierung auf dieser Ebene und startet keine Klassifizierer niedrigeren Ranges. Beispiel: Wenn der Klassifizierer für Windows 2008 Server deaktiviert ist, beendet das System die Erkennung an dieser Stelle und startet den Klassifizierer für Windows 2012 Server nicht.
Reihenfolge	Reihenfolge (Sequenz), in der die Plattform diesen Klassifizierer ausführt
Tabelle	Tabelle für diese Klassifizierung. Beispiel: Wenn dieser Datensatz einen Linux-Server klassifiziert, wählen Sie die Tabelle „Linux-Server“ [cmdb_ci_linux_server] aus.
Klassifizierung	Klassifizierung eines SNMP-Geräts, zum Beispiel **A10 Load Balancer**. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP-System-OIDs“ verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

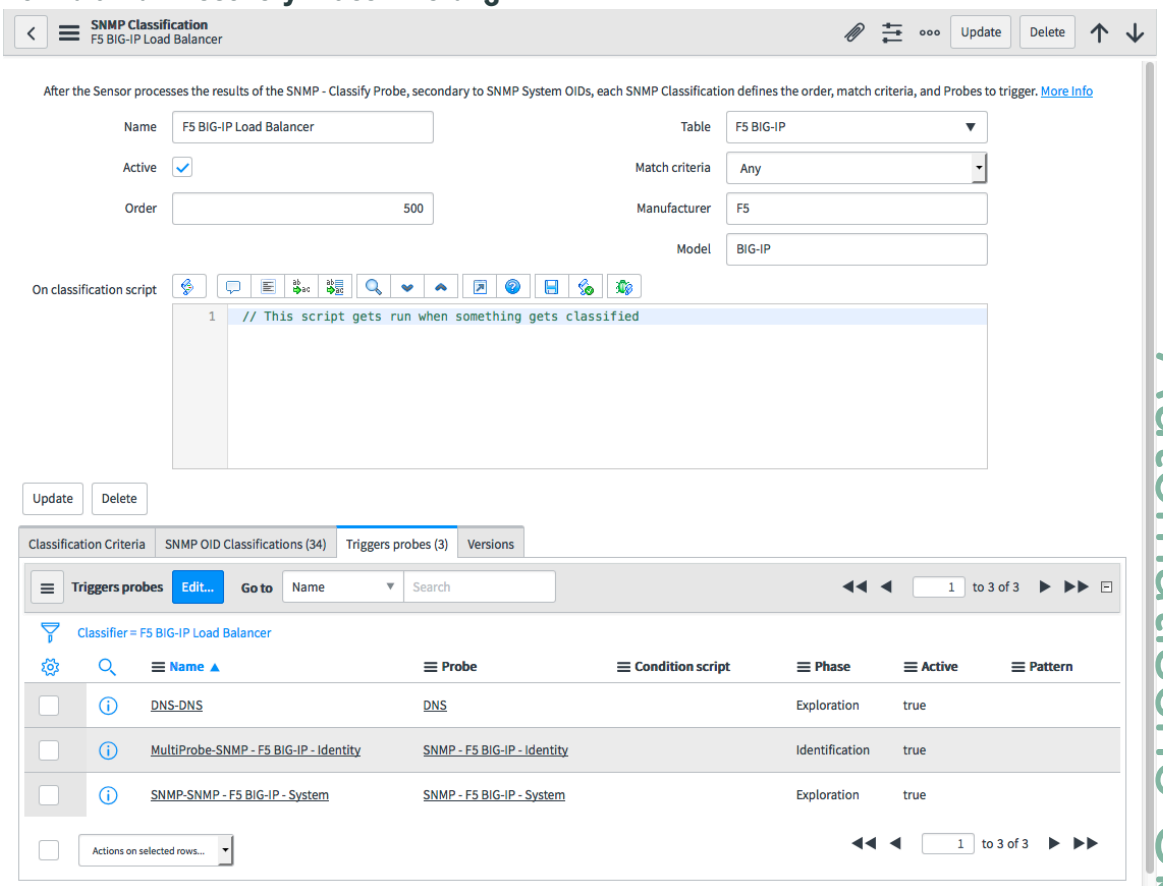
Feld	Eingabewert
Beziehungstyp	Typ der Beziehung für diesen Klassifizierer, zum Beispiel **Wird ausgeführt auf::Wird ausgeführt**. Dieses Feld ist nur für Anwendungs- und Prozessklassifizierer verfügbar.
Kriterien anpassen	Kriterien, die erfüllt sein müssen, um dieses Gerät zu klassifizieren. Die Auswahlmöglichkeiten lauten, bezogen auf Parameter, **Beliebig** und **Alle**.
Hersteller	Name des Herstellers eines Netzwerkgeräts. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP“ und „SNMP-System-OIDs“ verfügbar.
Modell	Modellnummer eines Netzwerkgeräts. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP“ und „SNMP-System-OIDs“ verfügbar.
Beim Klassifikations-Skript	Skript, das ausgeführt wird, wenn die Klassifizierungskriterien erfüllt sind. Verwenden Sie dieses Skript, um spezielle Aufgaben auszuführen, nachdem ein Gerät klassifiziert wurde. Es besteht die Möglichkeit, die Hashmap `g_probe_parameters` aus einem Klassifizierungsskript zu verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispielsweise wird mit diesem Code der Parameter *`node_port`* für alle ausgelösten Probes auf 16001 festgelegt: `(JS), g_probe_parameters['node_port'] = 16001; //`
Zugehörige Listen	
Klassifizierungskriterien	Kriterien, die aus bestimmten Parametern und den Werten gebildet werden, die sie enthalten müssen, um Geräte, die Discovery im Netzwerk erkennt, mit CIs in der CMDB abzugleichen. Eine detaillierte Beschreibung dieser Parameter finden Sie unter Parameter der Discovery-Klassifizierung.
SNMP-OID-Klassifizierungen	Eindeutige „Fingerabdrücke“ aller SNMP-Geräte, die im Lieferumfang des Basisprodukts von Discovery enthalten sind. Benutzer können OIDs für SNMP-Geräte hinzufügen, die sich nicht in dieser Liste befinden. Diese zugehörige Liste ist nur für SNMP-Geräte verfügbar.
Auslösertests	Erkundungs-Probes, die Discovery startet, um detaillierte Informationen über ein CI zu sammeln, das im Netzwerk klassifiziert wurde. Wenn Sie Muster für die horizontale Erkennung verwenden möchten, fügen Sie die Probe Horizontal Pattern in die Spalte **Probe** ein, und geben dann das Muster in der Spalte **Muster** an. ⚠ **Warnung:** Geben Sie Ihr Muster nicht in der Spalte **Probe** an. Wählen Sie die Probe „Horizontal Pattern“ aus, die das angegebene Muster startet.
Versionen	Listet Versionen dieses Klassifizierers auf. Bei jeder Änderung des Klassifiziererdatensatzes wird eine neue Version erstellt. Um eine vorherige Version wiederherzustellen, öffnen Sie den gewünschten Datensatz, und wählen Sie **Diese Version wiederherstellen** unter **Zugehörige Links** aus.

Dieses Beispiel zeigt ein ausgefülltes CI-Klassifizierungsformular mit definierten Erkundungs-Probes. Anweisungen zum Erstellen von Probes finden Sie unter Discovery-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probes und -Sensoren. Die hier definierten Probes werden gestartet, wenn das Gerät ordnungsgemäß klassifiziert ist, es sei denn Discovery ist so konfiguriert, dass es nach der Klassifizierung anhält.

Formular für Discovery-Klassifizierung



Discovery-Prozessklassifizierung erstellen

Eine Prozessklassifizierung ermöglicht Discovery die Erstellung eines bestimmten CI-Typs aus Informationen, die während der Identifizierungs- und Erkundungsphase gesammelt wurden.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Prozess die Klassifizierungskriterien erfüllt, verwendet Discovery den Prozessklassifizierungsdatensatz zum Erstellen eines CI. Sie können Discovery auch dazu veranlassen, vorhandene CIs zu aktualisieren oder bestimmte Prozesse zu ignorieren, indem Sie einen Prozess-Handler erstellen.

Hinweis: Dot-Walking wird auf dem übergeordneten Element, das den Prozessbefehl ausführt, nicht unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie Werte in die Klassifizierungsfelder ein (siehe Tabelle).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierungsfelder

Feld	Eingabewert
Tabelle	Wählen Sie die Tabelle aus, in der diese Klassifizierung CI-Datensätze generiert. Diese Tabelle muss eine Erweiterung der Anwendungstabelle [cmdb_ci_appl] sein.
Beziehungstyp	Wählen Sie den CI-Beziehungstyp für diese Klassifizierung aus. Das Beziehungsfeld ist nur für Prozess- und Scan-Anwendungsklassifizierungen verfügbar. Für Discovery-Prozessklassifizierungen wird normalerweise einer der folgenden Beziehungstypen verwendet: ○ *Wird ausgeführt auf::Wird ausgeführt*: Definiert die Beziehung einer Anwendung mit dem Host, auf dem sie ausgeführt wird. Diese Beziehung wird aus der Perspektive des Hosts und der Anwendung ausgedrückt. Beispiel: Meine Datenbankanwendung wird auf server001 ausgeführt::server001 führt meine Datenbankanwendung aus. ○ *Abhängig von::Verwendet von*: Definiert die Beziehung einer Anwendung, die mit einer anderen Anwendung kommuniziert. Diese Beziehung wird aus der Perspektive der jeweiligen Anwendung ausgedrückt. Beispiel: Die Anwendung Tomcat ist von der Datenbank MySQL abhängig::Die Datenbank MySQL wird von Tomcat verwendet. ○ *Virtualisiert von::Virtualisiert*: Definiert die Beziehung eines virtuellen Computers mit ihrem Host. Diese Beziehung wird aus der Perspektive des virtuellen Computers und des Hosts ausgedrückt. Beispiel: server001 wird virtualisiert von Server ESX::Server ESX virtualisiert server001.
Aktiv	Wählen Sie diese Option aus, um den Prozessklassifizierungsdatensatz zu aktivieren. Nur aktive Prozessklassifizierungen können Anwendungs-CI-Datensätze erstellen.
Reihenfolge	Geben Sie die Reihenfolge ein, in der Discovery diese Prozessklassifizierung ausführen soll, wenn für eine Tabelle mehrere Klassifizierungen verfügbar sind. Discovery führt Prozessklassifizierungen von der niedrigsten zur höchsten Ordnungszahl aus.
Testen mit	Listet das Host-CI auf, bei dem die Bedingungen einer automatisch generierten Prozessklassifizierung erfüllt wurden. Verwenden Sie dieses Feld, um Änderungen an der Prozessklassifizierung zu testen. Auf diese Weise können Sie sicherstellen, dass sich die aktualisierte Klassifizierung wie erwartet verhält.
Bedingung	Verwenden Sie den Condition Builder, um die Übereinstimmungs- und Klassifizierungskriterien für die Prozessklassifizierung zu erstellen. Dieses Feld ersetzt sowohl das Feld **Kriterien anpassen** als auch die zugehörige Liste **Klassifizierungskriterien**. Der Upgrade-Prozess konvertiert alle vorhandenen Klassifizierungskriterien in Bedingungen. **Hinweis:** Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

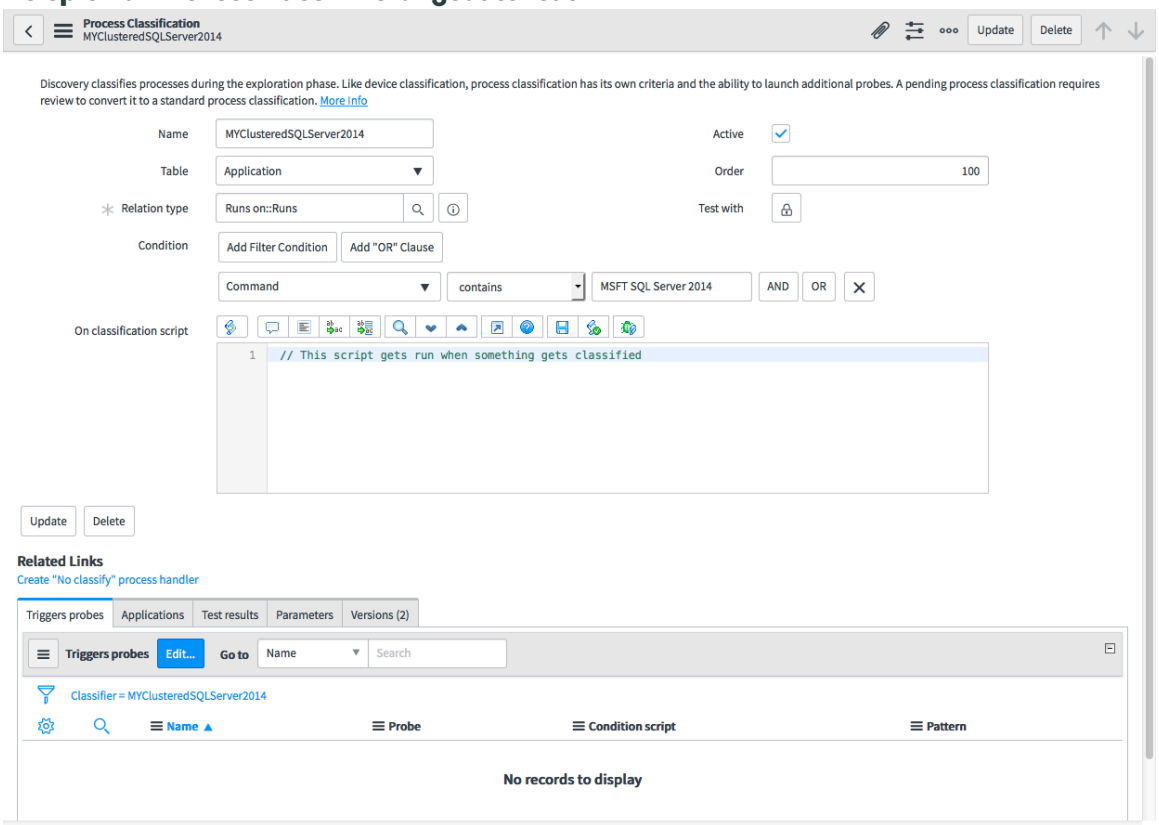
Feld	Eingabewert
	Hinweis: Nur die folgenden Bedingungen funktionieren: ◦ Name ◦ PID ◦ PPID ◦ command ◦ parameters ◦ listening_on_ports ◦ connecting_to_ports ◦ connecting_to ◦ key_parameters ◦ classify
Beim Klassifikations-Skript	Geben Sie ein Skript ein, das ausgeführt werden soll, wenn Bedingung und Klassifizierungskriterien erfüllt sind. Verwenden Sie dieses Skript, um spezielle Aufgaben auszuführen, nachdem ein Gerät klassifiziert wurde. Es besteht die Möglichkeit, die Hashmap `g_probe_parameters` aus einem Klassifizierungsskript zu verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispiel: Der folgende Code legt den Parameter `'node_port'` für alle ausgelösten Probes auf 16001 fest: `g_probe_parameters['node_port'] = 16001;` Unter Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery finden Sie weitere Beispiele und eine Liste der Objekte, die Sie für diese Art von Skript verwenden können.
Auslösertests	Wählen Sie die Erkundungs-Probes aus, die von Discovery gestartet werden sollen. Diese Probes erfassen detaillierte Informationen über ein klassifiziertes CI. Discovery startet diese Probes nicht, wenn es so konfiguriert ist, dass es nach der Klassifizierung anhält. Wenn Sie Muster für die horizontale Erkennung verwenden möchten, fügen Sie die Probe Horizontal Pattern in die Spalte **Probe** ein, und geben dann das Muster in der Spalte **Muster** an. **Warnung:** Geben Sie Ihr Muster nicht in der Spalte **Probe** an. Sie müssen die Probe „Horizontal Pattern“ auswählen, die das angegebene Muster startet.
Anwendungen	Verwenden Sie diese zugehörige Liste, um die Anwendungs-CIs anzuzeigen, die dieser Prozessklassifizierung entsprechen.
Testergebnisse	Verwenden Sie diese zugehörige Liste, um anzuzeigen, wie Discovery Prozesse auf dem im Feld **Testen mit** angegebenen Host klassifiziert und bessere Klassifizierungsbedingungen erzielt werden.
Parameter	Verwenden Sie diese zugehörige Liste, um die Parameter anzuzeigen, die diesem Prozess zugeordnet sind, und um bessere Klassifizierungsbedingungen zu erzielen. Unter Parameter der Discovery-Klassifizierung finden Sie eine Liste der Parameter, die Sie verwenden können.
Versionen	Verwenden Sie diese zugehörige Liste, um vorherige Versionen des Prozessklassifizierungsdatensatzes anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
5. Geben Sie Elemente aus zugehörigen Listen ein.
6. Klicken Sie auf **Aktualisieren**.

Example:

Beispiel für Prozessklassifizierungsdatensatz



Nächste Maßnahme

Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach Anwendungen zu suchen. Sie können auch Prozess-Handler erstellen oder ändern, die die Erstellung doppelter CIs basierend auf Prozessklassifizierungen verhindern, wenn dies ein Problem für Ihre Umgebung darstellt.

Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery

Verwenden Sie ein *Bei Klassifikations*-Skript in einem Prozessklassifizierer, um einen Anwendungsdatensatz anzupassen. Diese Art von Skript wird in Prozessklassifizierern verwendet.

Standardname der Anwendung ändern

Standardmäßig weisen Anwendungsnamen das folgende Format auf: `<Name des Prozessklassifizierers>@<Name des Computer-CI, auf dem sich der Prozess befindet>`;

Beispiel: Für einen MySQL-Server, der auf Computer „computerA“ ausgeführt wird, lautet der Anwendungsname `mysql@machineA`.

Sie können das Feld **Beim Klassifikations-Skript** im Prozessklassifizierungsdatensatz verwenden, um den standardmäßigen Anwendungsnamen an Ihre geschäftlichen Anforderungen anzupassen. Das folgende Skript ändert beispielsweise den standardmäßigen Anwendungsnamen, um ein Suffix hinter dem Prozessklassifizierer einzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var computerName = g_sensor.deviceGR.name;
var processClassiferName = g_classification.name;
current.name = processClassiferName + "999" + "@" + computerName;
```

In diesem Beispiel wird der Name des Anwendungsdatensatzes in mysql999@machineA geändert.

Eine weitere gängige Technik ist die Festlegung des Anwendungsnamens basierend auf den Variablen name, command und parameter. Ein Eclipse-Prozess kann beispielsweise die folgenden Werte für diese Variablen aufweisen:

Name	"eclipse"
command	"/glide/eclipse/Eclipse.app/Contents/MacOS/eclipse"
parameter	"-psn_0_1884620"

Wenn eine Eclipse-Anwendung auf Computer „computerA“ ausgeführt wird, benennt ServiceNow die Anwendung in „eclipse@computerA“ um. Das folgende Skript hängt den Parameterwert als Teil des Anwendungsnamens an.

```
var computerName = g_sensor.deviceGR.name;
var processClassiferName = g_classification.name;
current.name = processClassiferName + parameters + "@" + computerName;
```

In diesem Beispiel wird der Name des Anwendungsdatensatzes in „eclipse-psn_0_1884620@computerA“ geändert.

Manchmal ist es hilfreich, Werte an die ausgelösten Probes in der Prozessklassifizierung zu übergeben. Erstellen Sie dazu ein benutzerdefiniertes Skript, das ein Name/Wert-Paar für das Objekt g_probe_parameters definiert. Beispiel:

```
g_probe_parameters['processCommand'] = command;
```

In diesem Beispiel übergibt das Skript den Parameter processCommand mit dem Wert der Variablen command, wenn ein Klassifizierungsdatensatz eine Probe auslöst.

Skriptobjekte

Verwenden Sie im Skript die folgenden Objekte:

Skriptobjekt	Beschreibung
aktuell	Verweist auf ein JavaScript-Objekt mit [property:value]-Paar, um den Anwendungsdatensatz zu aktualisieren. (Es handelt sich dabei nicht um ein tatsächliches GlideRecord-Objekt der Anwendung.)
g_sensor	Verweist auf die Sensorklasse des ausgeführten Prozesses. Dieses Objekt enthält ein deviceGR-Objekt, das auf den CI-Datensatz des Computers verweist, auf dem sich der Prozess befindet.
g_classification	Verweist auf den Prozessklassifiziererdatensatz selbst
Name	Verweist auf den Prozessnamen
command	Verweist auf den Prozessbefehl
parameters	Verweist auf die Prozessparameter
g_probe_parameters	Ein JavaScript-Objekt, das die Übergabe von Parametern an die ausgelösten Probes ermöglicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Discovery-Prozess-Handler erstellen

Discovery-Prozess-Handler erstellen

Prozess-Handler verhindern, dass doppelte CIs entstehen, indem vor der Prozessklassifizierung Parameter mit bekanntermaßen inkonsistenten Werten herausgefiltert werden. Sie können neue Klassifizierer erstellen oder vorhandene bearbeiten.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesshandler**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „Prozesshandler“ aus.

Formular „Prozesshandler“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Prozess-Handler-Datensatz ein.
Aktiv	Aktivieren Sie das Kontrollkästchen zum Ausführen des Prozess-Handler.
Klassifizieren	○ Aktivieren Sie das Kontrollkästchen, um die Klassifizierung aller Datensätze zu laufenden Prozessen [cmdb_running_process] zu aktivieren, die den Bedingungen dieses Prozess-Handler entsprechen. ○ Deaktivieren Sie das Kontrollkästchen, um die Klassifizierung aller Datensätze zu laufenden Prozessen [cmdb_running_process] zu deaktivieren, die den Bedingungen dieses Prozess-Handler entsprechen.
Bedingung	Wählen Sie die Bedingungen aus, die den Prozess-Handler zum Ausführen des Skripts auslösen. In den meisten Fällen enthält diese Bedingung entweder spezifische Namen von ausführbaren Dateien oder bestimmte Parameter.
Skript	Geben Sie in die Tabelle „Laufender Prozess“ [cmdb_running_process] das JavaScript ein, das Sie für den aktuellen Datensatz ausführen möchten, wenn die **Bedingung** erfüllt ist. Die `current`-Variable verweist auf einen GlideRecord eines laufenden Prozesses. Das Skript sollte `current.parameters` auf bestimmte Werte untersuchen, Zeichenfolgen ersetzen, um diese Werte zu bearbeiten, und das Ergebnis in `current.key_parameters` speichern. ServiceNow verwendet das Feld **key_parameters** zusammen mit dem Prozessnamen, um zu bestimmen, ob der Prozess auf einem bestimmten Computer eindeutig ist. Weitere Optionen finden Sie unter Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach Anwendungen zu suchen, und überprüfen Sie dann die Ergebnisse in der CMDB für die gefundenen Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Klassifizierung erstellen

Ein HTTP-Klassifizierer ermöglicht dem horizontalen Erkennungsprozess, Geräte über das HTTP-Protokoll zu finden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Geräte über HTTP/REST klassifizieren möchten, können Sie zusätzliche HTTP-Klassifizierungen erstellen, anstatt durch ein anderes Protokoll. Verwenden Sie die HTTP-Klassifizierung nur für die Geräteerkennung, nicht für die Anwendungserkennung.

Wichtig: Die HTTP-Klassifizierungsprobe versucht standardmäßig nicht mehr Anmeldeinformationen über das HTTP-Protokoll. Um dieses Verhalten zu überschreiben, können Sie aktivieren `mid.http_classy.allow_credentials_over_http`. Das Aktivieren dieser Einstellung kann jedoch Anmeldeinformationen für MitM-Angriffe (man-in-the-Middle) verfügbar machen. Daher wird dringend empfohlen, diese Eigenschaft auf festzulegen **Falsch** Und verwenden Sie HTTPS, wann immer möglich.

Standardmäßig wird der Klassifizierer „F5 HTTP“ bereitgestellt, um F5-Lastenausgleichsmodule mit REST zu klassifizieren. Das Muster **F5 LB REST** wird ebenfalls für die Erkundung des Geräts bereitgestellt. Sie müssen keine HTTP-Klassifizierung für F5-Lastenausgleichsmodule erstellen.

Von allen Protokollen, die Discovery verwenden (einschließlich WMI, SSH und SNMP), hat HTTP standardmäßig die niedrigste Priorität. Discovery verwendet die HTTP-Klassifizierung nur unter folgenden Umständen:

- Shazzam stellt fest, dass die Ports für den HTTP- (80) - und HTTPS-Verkehr (443) offen sind.
- Der horizontale Erkennungsprozess schlägt für die Port-Sonden mit höherer Priorität (WMI, SSH und SNMP) fehl, wenn die Ports für diese Protokolle nicht geöffnet sind oder wenn die Erkennung dieser Protokolle fehlschlägt. Der horizontale Erkennungsprozess kann beispielsweise fehlschlagen, wenn SSH- und SNMP-Anmeldeinformationen nicht konfiguriert oder falsch sind.

  Hinweis: Siehe Port-Sonden für weitere Informationen zur Funktionsweise von Port-Scanning und die Prioritäten der verschiedenen Protokolle.

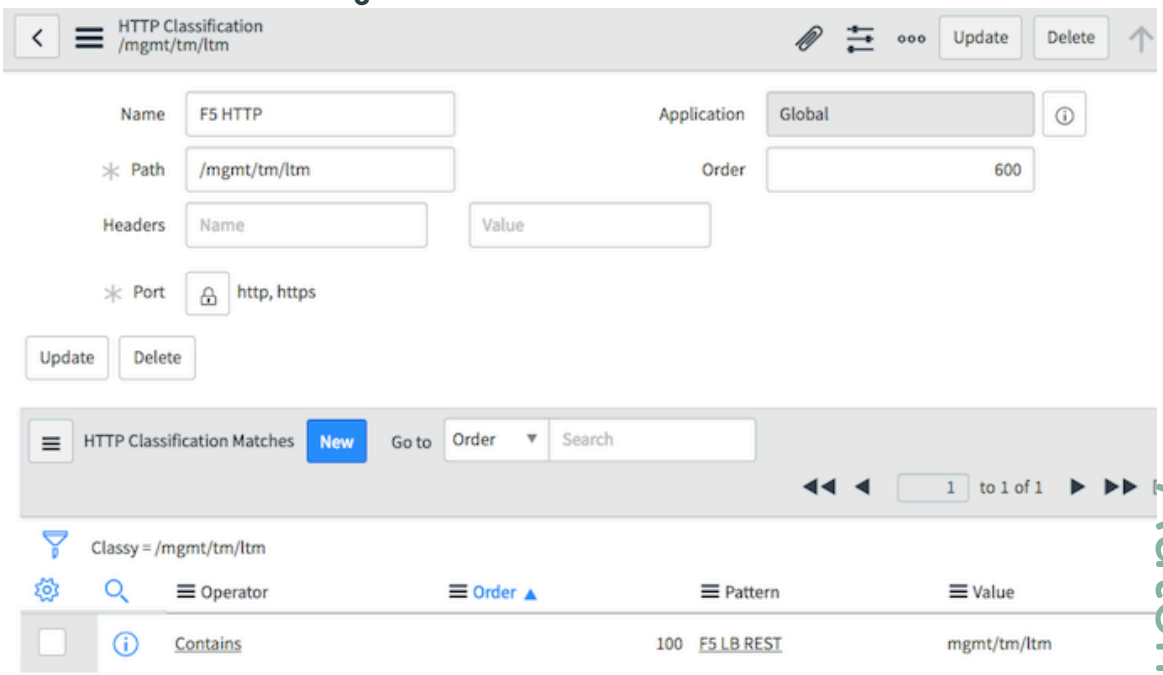
Die HTTP-Klassifizierung startet die Sonde **HTTP Klassifizierung**, um das Gerät zu klassifizieren. Die Sonde **HTTP - Klassifizierung** führt eine GET-Anforderung für jedes Gerät für jede HTTP-Klassifizierung aus. Die URL der Anfrage setzt sich wie folgt zusammen: PROTOCOL://IP:PORT/PATH, wobei Folgendes gilt:

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **HTTP**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die F5-HTTP-Klassifizierung



Feld	Beschreibung
Name	Geben Sie einen Namen für den Klassifizierer ein.
Pfad	Geben Sie den Pfad für die HTTP-GET-Anforderung ein.
Header	Fügen Sie einen Optionsheader mit einem Wert hinzu. Sie können eine Variable im Format ${variable} anstatt eines statischen Wertes verwenden. Unterstützte Header hängen vom REST-Webservice-Provider ab, mit dem Sie eine Verbindung herstellen möchten. In der Dokumentation Ihres Web Service Providers erfahren Sie, welche Header gültig oder erforderlich sind.
Port (IP-Dienst)	Wenn Sie möchten, dass dieser Klassifizierer einen benutzerdefinierten Port verwendet, der nicht bereits ein Standardwert in der Tabelle IP-Dienst [cmdb_ip_service] ist, führen Sie folgende Schritte aus: **a.** Wählen Sie das Suchsymbol, um die Liste der IP-Services anzuzeigen. **b.** Wählen Sie Aus **Neu** Und erstellen Sie eine Port-zu-Protokoll-Zuordnung. **c.** Wählen Sie diese Port-zu-Protokoll-Zuordnung dafür im Feld **Port**. Viele häufig verwendete Protokolle sind standardmäßig bereits Ports zugeordnet, z. B. http zu Port 80 und https zu Port 443.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie eine dieser standardmäßigen Port-zu-Protokoll-Zuordnungen verwenden möchten, geben Sie keine Werte in ein **Port** Feld. Die HTTP-Port-Sonde verwendet standardmäßig den richtigen Port.
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieses Klassifizierers darstellt. Wenn Discovery mehr als einen zutreffenden Klassifizierer verwendet, wird der Klassifizierer mit niedriger **Rang**-Nummer verwendet.
Protokoll [optional] Dieses Feld ist standardmäßig nicht sichtbar. Sie müssen das Formular konfigurieren, um es hinzuzufügen.	Wenn Sie eine eindeutige Port-zu-Protokoll-Zuordnung für das Fel **Port** konfigurieren, geben Sie in das Feld eine optionale Protokollüberschreibung ein, die Discovery mit diesem Klassifizierer verwendet. Wenn Sie beispielsweise Port 5000 und das HTTP-Protokoll verwenden möchten, fügen Sie die 5000/HTTP-Port-zu-Protokoll-Zuordnung zum Feld **Port** hinzu, und wählen Sie dann **http** im Feld **Protokoll**.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

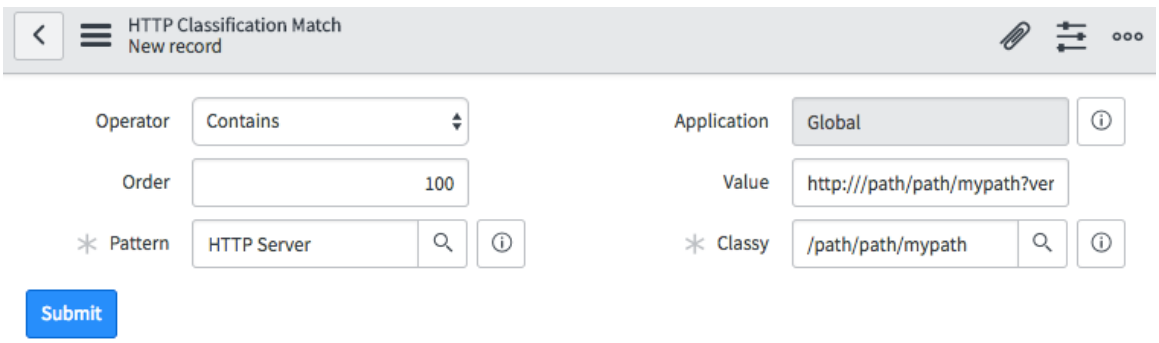
   Ein Datensatz wird in der Tabelle „HTTP-Klassifizierungen“ [discovery_classy_http] erstellt.

   Die zugehörige Liste „Übereinstimmung der HTTP-Klassifizierung“ wird angezeigt. Diese zugehörige Liste enthält Kriterien, die Sie für den Abgleich mit dem Hauptteil der Antwort auf die von Discovery gesendete GET-Anforderung konfigurieren können.

5. Definieren Sie in der zugehörigen Liste „Übereinstimmung der HTTP-Klassifizierung“ die Kriterien, und geben Sie das für diesen Klassifizierer zu startende Muster an:
   Die Kriterien müssen erfüllt sein, damit Discovery diesen HTTP-Klassifizierer verwenden kann.

   a. Wählen Sie **Neu**.

   b. Füllen Sie die Felder des Formulars „Übereinstimmung der HTTP-Klassifizierung“ aus (siehe Tabelle).



Feld	Beschreibung
Operator	Wählen Sie den Operator aus, mit dem das System die Bedingung bewertet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ **Enthält** ▪ **Ist gleich** ▪ **Regulärer Ausdruck**
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieser Bedingung darstellt. Wenn Discovery mehr als eine zutreffende Bedingung findet, wird die Bedingung mit niedriger Rang-Nummer verwendet.
Muster	Geben Sie das Muster an, das nach einer korrekten Übereinstimmung gestartet werden soll. Dieses Muster muss HTTP verwenden, um das Gerät zu ermitteln.
Wert	Geben Sie den Wert ein, den der Rumpf der zurückgegebenen REST-Methode haben muss.

c. Wählen Sie **Absenden**.

d. Wenn verschiedene Muster für verschiedene Versionen des Geräts vorhanden sind, das Sie erkennen möchten, definieren Sie beliebig viele HTTP-Klassifizierungsübereinstimmungen.

Klassifizierung für Erkennung von IP-Adressen

Discovery bietet eine Möglichkeit, Geräte zu klassifizieren, die über die IP-Adresserkennung erkannt werden, auch wenn keine Anmeldeinformationen verfügbar sind.

Wenn Sie keine CI-Erkennung, sondern eine Erkennung für IP-Adressen ausführen, geht Discovery von bestimmten Annahmen in Bezug auf die Geräte und Anwendungen aus, die auf den Geräten an den als offen vorgefundenen Ports ausgeführt werden. Die Klassifizierungsparameter für diesen Erkennungstyp werden anders generiert als bei Scans, bei denen Anmeldeinformationen verfügbar sind.

Die Syntax zum Erstellen von Parametern wird von den Feldern abgeleitet, die von der Shazzam-Probe zurückgegeben werden, wenn eine Discovery für IP-Adressen ausgeführt wird. Parameter für CIs und Anwendungen werden auf dieselbe Weise gebildet. Die Shazzam-Probe erstellt eine XML-Datei mit den folgenden Feldern:

- **Name**
- **port**
- **portprobe**
- **protocol**
- **Ergebnis**
- **service**

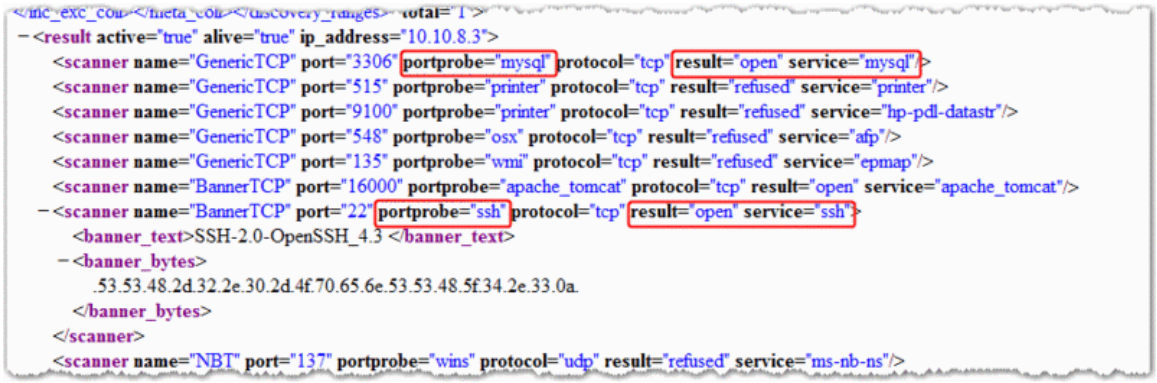
Hinweis: Optionale Felder, die zum Bilden von Parametern verwendet werden können, werden als untergeordnete Tags unter den Standardfeldern angezeigt. Beispiel hierfür sind die Felder **sysDescr** und **banner_text**.

Parameter werden im Format <portprobe.service.field> ausgedrückt. Der Wert für *field* kann aus jedem der Felder oder untergeordneten Tags in der XML-Datei stammen. Beispielsweise klassifizieren die folgenden Parameter ein Gerät als UNIX-Server und erkennen eine MySQL-Installation:

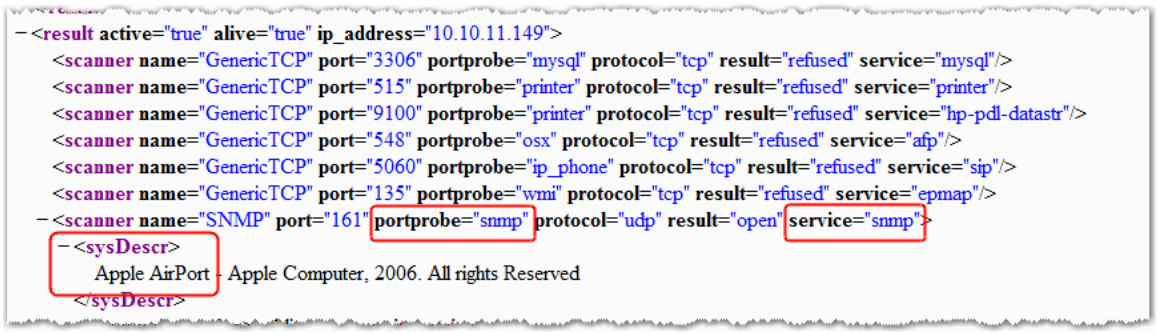
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *ssh.ssh.result*
- *mysql.mysql.result*

Diese Parameter wurden von den Werten in der folgenden XML-Datei abgeleitet, die von einer Shazzam-Probe generiert wurde, die einen IP-Scan durchführt. Das Feld *result* hat den Wert *open* für die Ports 22 und 3306 auf dem Zielgerät zurückgegeben. Das Feld *service* zeigt die Services an, die normalerweise über diese Ports kommunizieren.



Das Feld *sysDescr* kann je nach Hersteller zusätzliche Informationen zu Geräten bereitstellen. Diese XML-Datei der Shazzam-Probe zeigt Folgendes über Port 161 auf dem Gerät bei IP 10.10.11.149:



In den Klassifizierungskriterien kann der folgende Parameter mit **sysDescr** erstellt werden, der einen Apple AirPort-WLAN-Router zurückgibt:

```
snmp.snmp.sysDescr  contains  Apple AirPort
```

Klassifizierer für Erkennung von IP-Adressen ändern

Wenn Sie eine Erkennung vom Typ „IP-Adresse“ ausführen, scannen Port-Probes Geräte ohne Anmeldeinformationen. Anschließend kann Discovery die zu verwendenden Klassifizierer bestimmen. Sie können Port-Probes und zusätzliche Klassifizierer für die Erkennung von IP-Adressen hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Obwohl keine Anmeldeinformationen erforderlich sind, um nach zu scannen Windows Oder UNIX Geräte mit dieser Art von Scan, Anmeldeinformationen sind für SNMP-Geräte weiterhin erforderlich. Indem bestimmt wird, welche Ports auf den zu scannenden Geräten offen sind, kann die IP-Adressklassifizierung zum Beispiel den Gerätetyp (Computer, UPS usw.), das Betriebssystem, ausgeführte Anwendungen und Versionsnummern erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die IP-Adressklassifizierung versucht, Geräte zu klassifizieren, wenn keine Anmeldeinformationen verfügbar sind. Discovery verwendet jedoch Anmeldeinformationen, wenn sie verfügbar sind, auch wenn die IP-Adressklassifizierung konfiguriert ist.

Führen Sie die folgenden Schritte aus, um die IP-Adressklassifizierung zu verwenden:

Prozedur

1. Bestimmen Sie, welche Ports für die Klassifizierung verwendet werden sollen, und führen Sie ein Scanprogramm wie aus *Nmap* Für bestimmte IP-Adressen, um zu entscheiden, welche Ports die gewünschten Informationen zu einem Gerät oder einer Anwendung anzeigen.

   Der Scan kann verschiedene Arten von Daten offenlegen, die für die Konfiguration von Klassifizierungsparametern hilfreich sind. Ein Nmap-Scan zeigt Portnummern, ihren Status (offen oder geschlossen), ihre Servicenamen und alle verfügbaren Versionsinformationen an. Anhand der im folgenden Beispiel zurückgegebenen Portinformationen können Kriterien für die Klassifizierung von UNIX-Servern (Port 22), MySQL (Port 3306) und Apache Tomcat (Port 16000) erstellt werden.

```
Host is up (0.035s latency).
Not shown: 65521 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 d9:77:8b:68:1a:3a:b3:80:c3:a4:60:ba:61:7c:6f:65 (DSA)
|_2048 12:ed:36:6c:aa:dc:51:a0:ce:59:45:c9:c8:42:9b:85 (RSA)
80/tcp    open     http        Apache httpd 2.2.3 ((Red Hat))
|_html-title: Test Page for the Apache HTTP Server on Red Hat Enterprise Linux
111/tcp   open     rpcbind     2 (rpc #100000)
| rpcinfo:
| 100000  2    111/udp  rpcbind
| 100024  1    655/udp  status
| 100000  2    111/tcp  rpcbind
|_100024  1    658/tcp  status
443/tcp   open     ssl/http    Apache httpd 2.2.3 ((Red Hat))
|_html-title: Test Page for the Apache HTTP Server on Red Hat Enterprise Linux
658/tcp   open     status      1 (rpc #100024)
1720/tcp  filtered H.323/Q.931
2000/tcp  filtered cisco-sccp
3306/tcp  open     mysql       MySQL (unauthorized)
5060/tcp  filtered sip
10000/tcp open     http        Webmin httpd
|_html-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: 5B9D90CA66BB985FA0D070E0E02D93F4
16000/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
16001/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
16003/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
| robots.txt: has 1 disallowed entry
|_/
|_html-title: DBSymphony
```

2. Fügen Sie einen IP-Service und eine Port-Probe hinzu.

   Das sofort einsatzbereite System stellt Probes für einige der am häufigsten verwendeten Ports bereit, für eine effektive IP-Adressüberprüfung werden jedoch zusätzliche Port-Probes benötigt.

   a. Navigieren zu **Discovery-Definition** > **IP-Services** Und klicken Sie auf *Neu* .

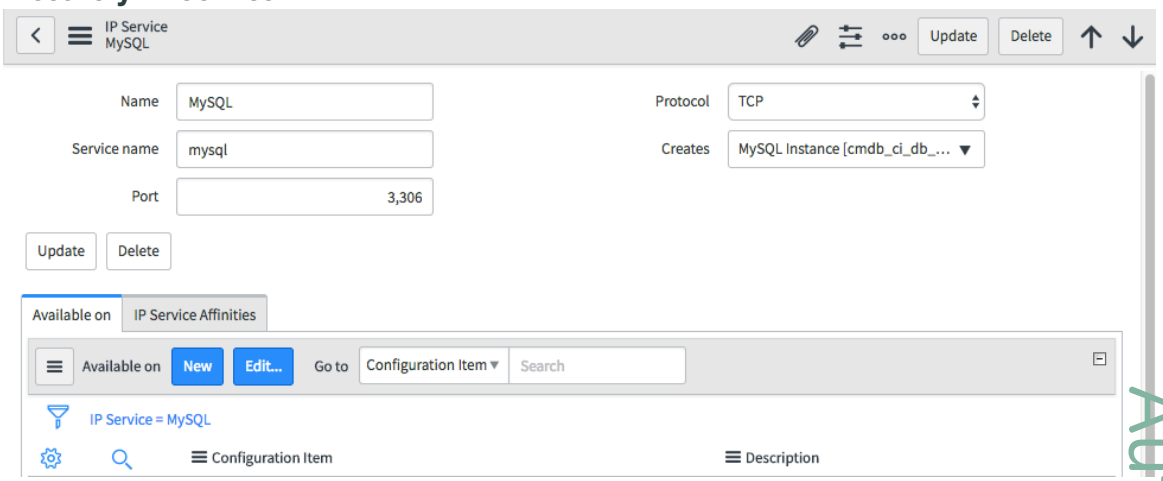
   b. Erstellen Sie einen neuen IP-Servicedatensatz mit der Portnummer und dem Service aus dem Nmap-Scan. In diesem Beispiel ordnen Sie den Service *mysql* zu Port 3306 zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und fügen das CI (*sanops02*), auf dem der Service ausgeführt wird, der zugehörigen Liste *Verfügbar am* hinzu.

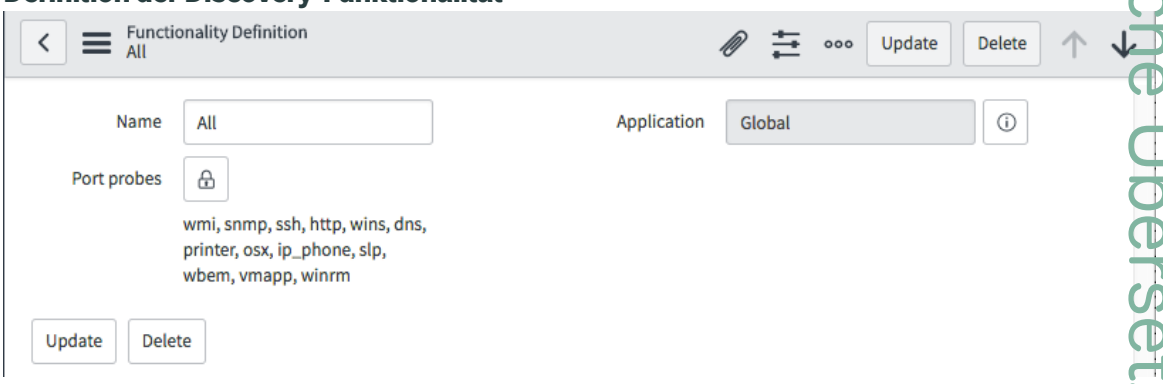
Discovery-IP-Service



c. Zur Verwendung von Standard Discovery, Navigieren Sie zu **Discovery-Definition** > **Funktionalitätsdefinition** Und wählen Sie den Datensatz für aus **Alle** .

d. Fügen Sie die neuen Port-Probes der Liste hinzu. Dadurch wird Discovery mitgeteilt, welche Port-Probes für IP-Adress-Scans ausgeführt werden sollen.

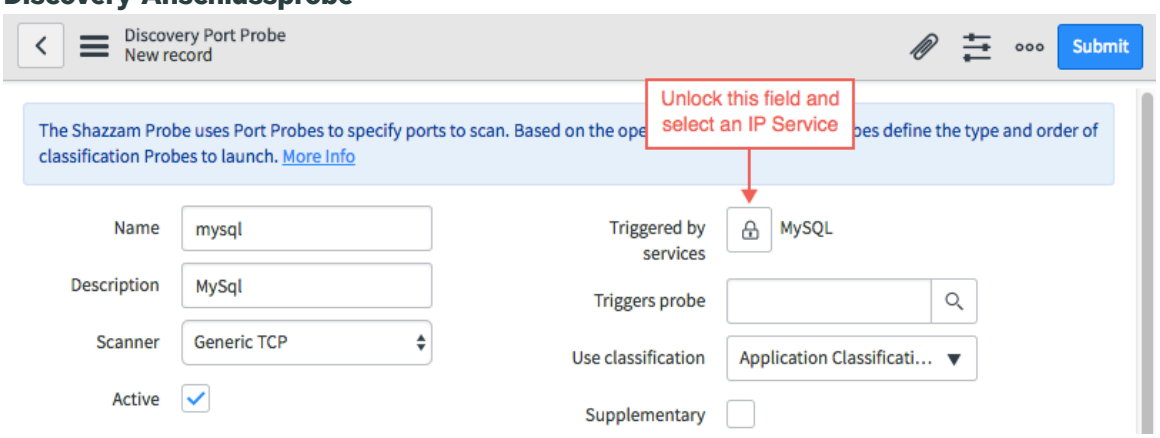
Definition der Discovery-Funktionalität



e. Speichern Sie den Datensatz, und navigieren Sie zu **Discovery-Definition** > **Anschlussprobes** Und klicken Sie auf **Neu** .

f. Erstellen Sie eine Port-Probe mit dem soeben definierten neuen IP-Service.

Discovery-Anschlussprobe



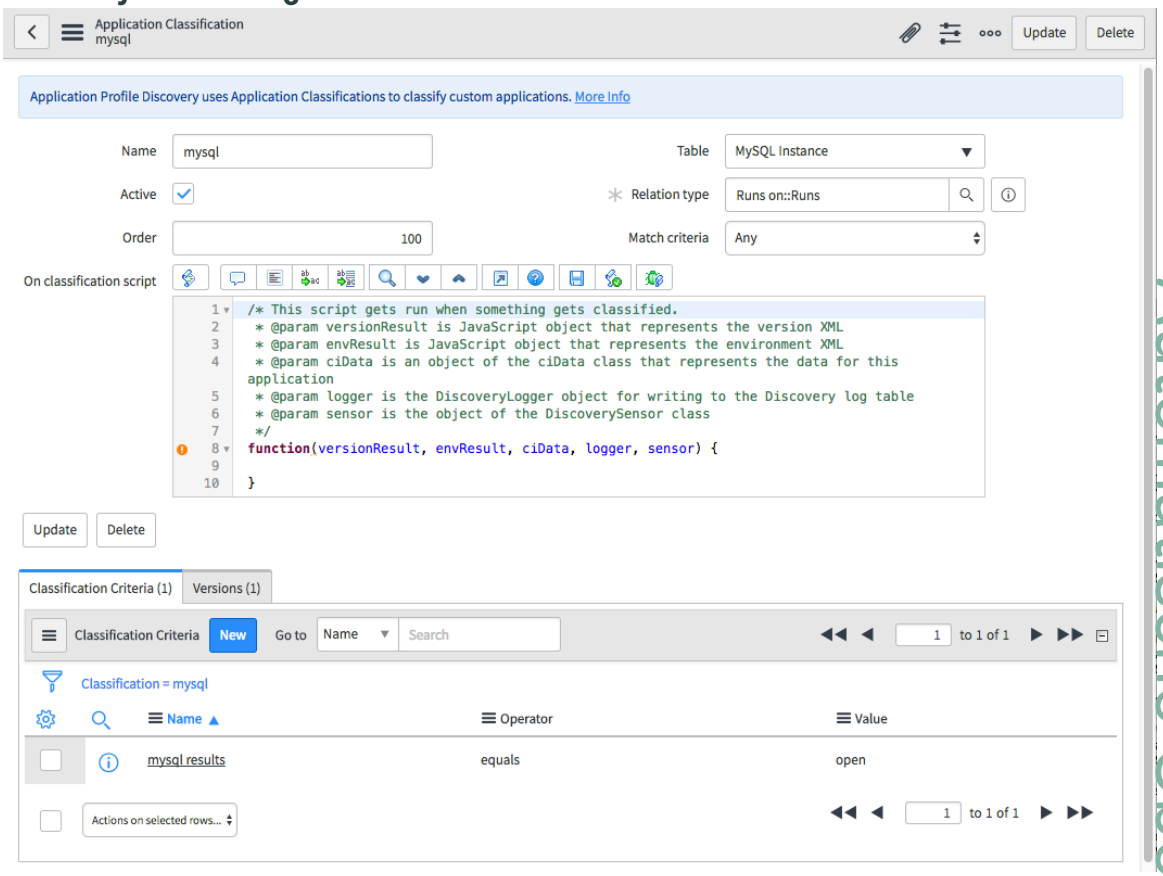
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine neue Klassifizierung, und fügen Sie den Parameter zum Scannen von IP-Adressen hinzu.

   In diesem Beispiel haben Sie einen Anwendungsklassifizierer erstellt, der Apache Tomcat anhand der Portinformationen erkennt, die durch den Nmap-Scan ermittelt wurden. Im folgenden Abschnitt finden Sie Details zum Bilden von Parametern für IP-Adress-Scans.

Discovery-Anwendungsklassifizierer



4. **Wahlweise:** Erstellen Sie in der zugehörigen Liste „Klassifizierungskriterien“ einen Kriterienfilter, der bestimmt, wann dieser Klassifizierer auf die erkannten Geräte angewendet wird.
   Unter den Parametern zur IP-Adressklassifizierung finden Sie eine Liste der Parameter, die Sie verwenden können.

Nächste Maßnahme

Führen Sie eine Erkennung von IP-Adressen über den Erkennungszeitplan aus, um nach Geräten zu suchen.

Windows-Remoteverwaltung für Klassifizierung verwenden

Sie können die Erkennung von Windows-Hosts mit dem WinRM-Protokoll (Windows-Remoteverwaltung) konfigurieren.

Vorbereitungen

- Installieren und konfigurieren Sie im lokalen Netzwerk einen Windows-MID Server.
- Der Service WinRM muss auf allen zur Erkennung fähigen Windows-Hosts aktiviert sein.

Erforderliche Rollen: discovery_admin, agent_admin, admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig verwendet das System für die Geräteklassifizierung von Windows-Hosts das WMI-Protokoll. Um für eine effizientere, ressourcenschonendere Datenübertragung und Ausführung von Remotebefehlen zu sorgen, können Administratoren stattdessen das WinRM-Protokoll verwenden.

Prozedur

1. Aktivieren Sie den Service WinRM auf allen Windows-Hosts, die zur Erkennung vorgesehen sind.
2. Navigieren zu **Discovery** > **MID-Server**an.
3. Wählen Sie den MID Server aus, den Sie für die Erkennung von Windows-Hosts verwenden möchten.
   Das System zeigt den MID Server-Datensatz an.
4. Klicken Sie in der zugehörigen Liste „Konfigurationsparameter“ auf **Neu**.
   Daraufhin wird der Datensatz eines MID Server-Konfigurationsparameters angezeigt.
5. Wählen Sie in der Auswahlliste des Felds **Parametername** den Parameter **mid.windows.management_protocol** aus.
6. Geben Sie den Wert **WinRM** ein.

MID Server-Konfigurationsparameter

7. Klicken Sie auf **Absenden**.
   Das System zeigt den MID Server-Datensatz an.
8. **Wahlweise:** Fügen Sie nach Bedarf weitere Protokollparameter der Windows-Remoteverwaltung hinzu.

Zusätzliche WinRM-Parameter

Parameter	Beschreibung	Standard	Erfordert einen Neustart des MID Servers
mid.powershell_api.winrm.remote_port	Gibt den Kommunikationsport an, den der MID Server für die Kommunikation mit dem WinRM-Protokoll verwendet	5985	Nein
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Pool pro Zielhost zulässig sind.	2	Ja
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Sitzungspool zulässig sind.	25	Ja

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standard	Erfordert einen Neustart des MID Servers
mid.powershell_api.idle_session_timeout	Gibt den Wert für den Timeout von Powershell-Sitzungen im Leerlauf in Sekunden an.	60.0	Ja

Nächste Maßnahme
Führen Sie eine Erkennung über den Erkennungszeitplan aus, um Windows-Computer in Ihrem Netzwerk zu finden.

Neuklassifizierung von Windows Workstation-Computers als Server

Standardmäßig klassifiziert Discovery Computer, die bestimmte Windows-Betriebssysteme verwenden, automatisch als Workstations. Möglicherweise möchten Sie jedoch bestimmte Computer in Ihrem Netzwerk, die als Server fungieren, nach ihrer Funktion und nicht nach dem Betriebssystem klassifizieren.

Vorbereitungen
Erforderliche Rolle: keine

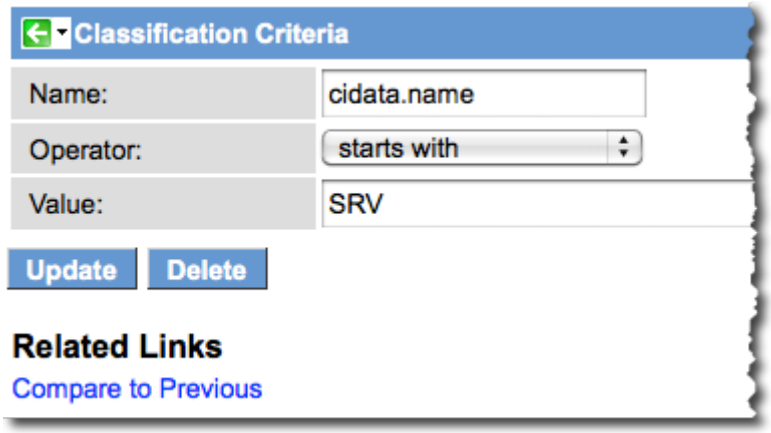
Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die folgenden Variablen (mit **cidata** als Präfix), um eine Bedingung für die Neuklassifizierung zu erstellen. Um die Neuklassifizierung beispielsweise basierend auf der IP-Adresse eines Computers durchzuführen, verwenden Sie `cidata.ip_address`.

- Name
- dsn_domain
- os_domain
- ip_address
- serial_number

Das folgende Verfahren reklassifiziert alle Betriebssysteme von Windows-Workstations (Windows Vista, XP oder Windows 7), die als Server fungieren.

Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Windows**an.
2. Erstellen Sie einen neuen Klassifizierungsdatensatz, zum Beispiel: Windows XP Server.
3. Wählen Sie als Tabelle „Windows Server“ [cmdb_ci_win_server] aus.
4. yxcvbnm,ooiuztreq12345tKlicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern** aus dem Kontextmenü.
   Die zugehörigen Listen **Klassifizierungskriterien** und **Auslösertests** werden angezeigt.
5. Konfigurieren Sie die folgenden **Klassifizierungskriterien**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Name	Wählen Sie in der Liste oben eine Variable zur Verwendung als Klassifizierungskriterium aus. Geben Sie etwa für eine Neuklassifizierung eines Computers nach dem Namen `cidata.name` ein. Dies funktioniert unabhängig vom Betriebssystem für Server mit einer einheitlichen Benennungskonvention wie SRV001, SRV002 usw.
Operator	Wählen Sie einen Operator für die Klassifizierungsbedingung aus. In Netzwerken mit Servern, die gemäß einer bestimmten Konvention benannt sind, können Sie **Beginnt mit** oder **Enthält**auswählen.
Wert	Geben Sie den Wert für die Bedingung ein. In unserem Beispiel eines Netzwerks mit Servernamenskonvention würde dieser Wert dem Stamm dieser Konvention entsprechen, zum Beispiel **SRV**. Diese Bedingung klassifiziert alle Computer als Server, deren Computername SRVXXX lautet.

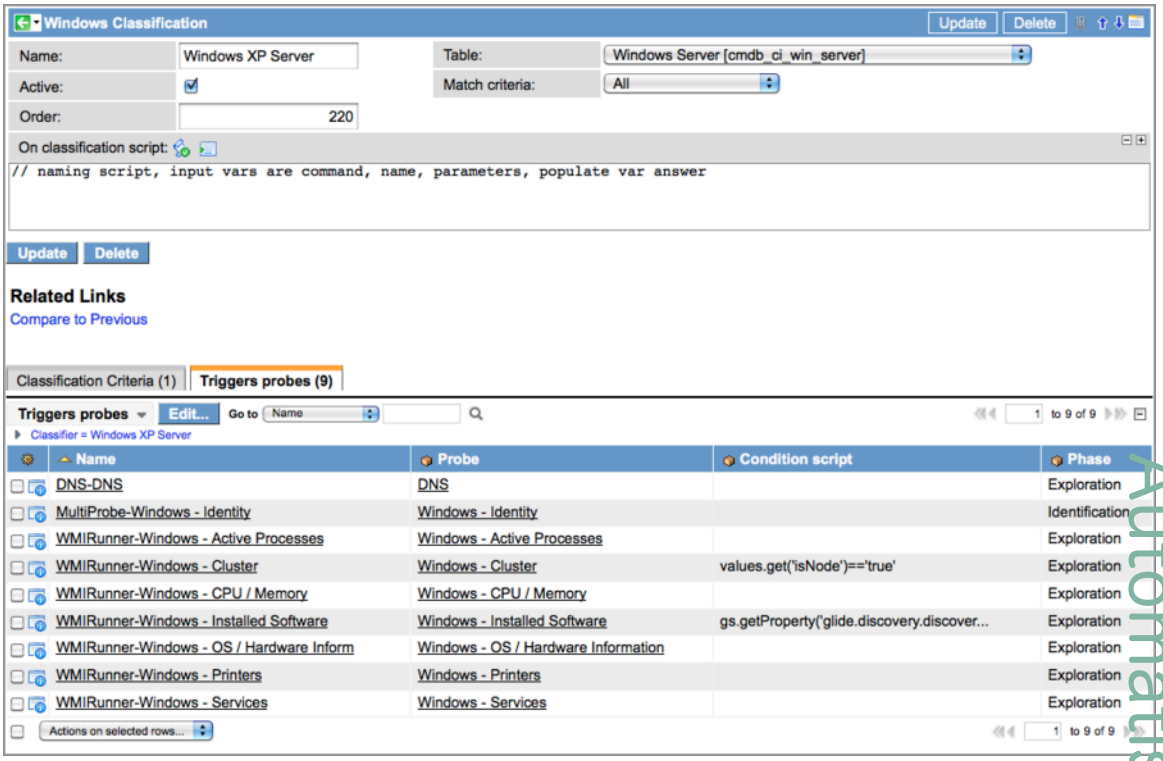
6. Wählen Sie die zugehörige Liste **Löst Probe aus** aus, und fügen Sie die entsprechenden Probes hinzu.

   a. Kopieren Sie die Liste der Probes aus einer anderen Windows-Serverklassifizierung, einschließlich der *`Bedingungsskripts`*.

   b. Stellen Sie sicher, dass die Probe **Windows - Identity** eine Phase vom Typ **Identifizierung** aufweist (Standardwert ist **Erkundung**).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das ausgefüllte Formular sieht wie folgt aus:



Nächste Maßnahme

Führen Sie eine Erkennung über den Erkennungszeitplan aus, um Windows-Computer in Ihrem Netzwerk zu erkennen, und prüfen Sie dann die Tabelle cmdb_ci_win_server und zugehörige Tabellen, um zu sehen, wie Daten in der CMDB gefüllt werden.

Parameter der Discovery-Klassifizierung

Die folgenden Parameter sind für Discovery-Klassifizierer verfügbar.

Hinweis: Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet.

Unix-Parameter

Die UNIX Parameter definieren die Merkmale verschiedener Computertypen, z. B. Linux, Solaris und HP-UX, Kommunikation mit SSH-Protokoll, Version 2.

Parameter	Beschreibung
Ausgabe	Die Rohausgabe der Klassifizierer-Probe (uname -a)
Typ	Gibt die Klassifizierung UNIX zurück
IP-Adresse	Gibt die IP-Adresse des erkannten Geräts zurück
Name	Der Name des Betriebssystems für dieses UNIX-CI. Beispiel: Linux Oder HP-UX.

Windows-Parameter

Windows-Parameter identifizieren Windows-Computer, die mit dem WMI-Protokoll kommunizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
isNode	Gibt an, ob die Instanz ein Knoten ist
Typ	Gibt die Klassifizierung *windows* zurück
isVIP	Gibt an, ob dieses CI eine virtuelle Maschine mit einer virtuellen IP-Adresse ist
ip_address	Gibt die IP-Adresse des erkannten Geräts zurück
Name	Name der Windows-Version
cidata.name	Hostname des Windows-Betriebssystems

SNMP-Parameter

SNMP-Parameter können die Eigenschaften verschiedener Gerätetypen wie Router, Switches und Drucker definieren.

Parameter	Beschreibung
powering	Der Wert *true* gibt an, dass das Gerät eine unterbrechungsfreie Stromversorgung (UPS) ist.
hosting	Der Wert *true* gibt an, dass das Gerät Programme hosten kann. Hosts sind Allzweckcomputer wie Server.
netware	Der Wert *true* gibt an, dass auf dem Gerät das Betriebssystem Netware ausgeführt wird.
Weiterleitung	Der Wert *true* gibt an, dass das Gerät über Weiterleitungsfunktionalität im Netzwerk verfügt.
ip_address	Gibt die IP-Adresse zurück, über die das jeweilige Gerät erkannt wurde. Ein Gerät kann über mehrere IP-Adressen verfügen.
sysdescr	Erforderliches beschreibendes Feld auf jedem beliebigen SNMP-Gerät, das nützliche Klassifizierungsdaten wie Betriebssystem und Version enthalten kann.
vlans	Der Wert *true* gibt an, dass das Gerät ein VLAN (Virtual Local Area Network) hosten kann.
hint_router	Der Wert *true* gibt an, dass Discovery ermittelt hat, dass das Gerät ein Router ist. Dieses Feld gilt nur für Geräte, die sowohl als Router als auch als Switch verwendet werden können.
block_router_exploration	Wenn dieser Parameter auf *true* gesetzt ist, startet Discovery keine Erkundungs-Probes für erkannte Router. Dieser Parameter wird nur für die Discovery im Netzwerk verwendet.
switching	Der Wert *true* gibt an, dass das Gerät über Netzwerk-Switching-Funktionalität verfügt.
mfr_apc	Der Wert *true* gibt an, dass das Gerät eine von American Power Conversion (APC) hergestellte unterbrechungsfreie Stromversorgung (UPS) ist.
printing	Der Wert *true* gibt an, dass das Gerät über Druckfunktionen verfügt.
block_switch_exploration	Wenn dieser Parameter auf *true* gesetzt ist, startet Discovery keine Erkundungs-Probes für erkannte Switches. Dieser Parameter wird nur für die Discovery im Netzwerk verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessparameter

Prozessparameter identifizieren Prozesse wie jene, die von LDAP, Apache-Servern und JBoss-Servern verwendet werden.

Parameter	Beschreibung
parameter	Die zur Ausführung des Prozesses verwendeten Parameter
command	Der zum Ausführen des Prozesses verwendete Befehl
Ausgabe	Die vollständige Ausgabe der aktuellen Zeile der Prozess-Probe
Typ	Gibt den Prozesstyp an (zum Beispiel *unix* oder *windows*).
PID	Die vom Betriebssystem eines Geräts generierte *Prozess-ID* zur Identifizierung eines laufenden Prozesses. Im Allgemeinen ist dieser Parameter kein praktisches Klassifizierungskriterium, da der Wert nicht statisch bleibt. Dies gilt jedoch nicht für Prozesse, die in einer Appliance ausgeführt werden, die nie neu gestartet wird.
Name	Name des erkannten Prozesses. In einigen Fällen ist dieser Parameter nicht zuverlässig, da mehrere Prozesse denselben Namen erhalten können. Unter Windows geben beispielsweise mehrere Prozesse für diesen Parameter *scvhost.exe* zurück.

IP-Service-Affinität für Discovery und Orchestration prüfen

Sie können in der Tabelle „IP-Services“ nach einer Liste von IP-Adressen suchen, die einem Protokoll zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „IP-Services“ ordnet einen Port einem Protokoll zu. Für häufig verwendete Port-Protokoll-Kombinationen werden standardmäßig Zuordnungen bereitgestellt, z. B. Port 80 für HTTP, Port 22 für SSH und Port 161 für SNMP.

Mithilfe der Systemeigenschaft `glide.discovery.ip_service_affinity` kann sich Discovery den letzten Port der erkannten IP-Adresse merken.

Wichtig: Sie sollten IP-Services nur dann ändern, wenn Ihre Organisation benutzerdefinierte Ports verwendet.

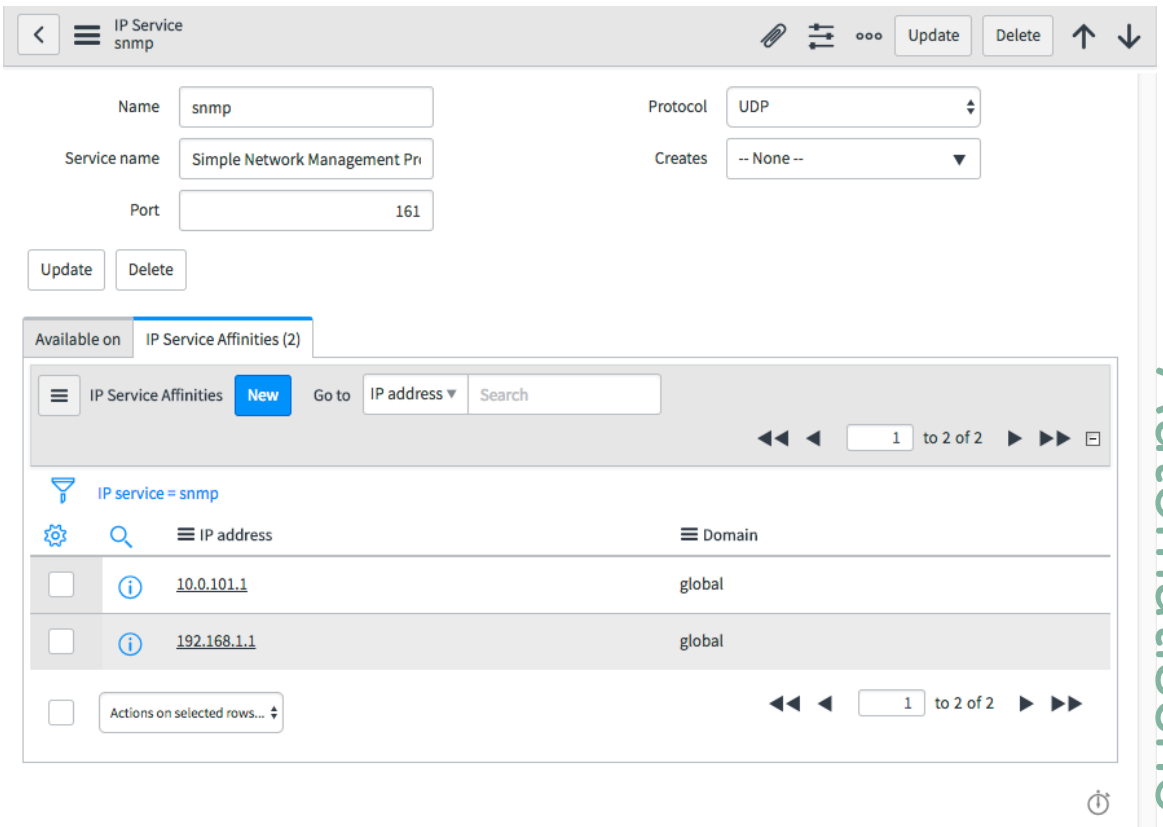
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **IP-Services**an.
2. Filtern Sie die Liste, um den entsprechenden IP-Service zu finden.
3. Klicken Sie auf den Namen des Service, um zu dieser IP-Serviceseite zu gelangen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **IP-Serviceaffinitäten**, um die Liste der IP-Adressen anzuzeigen, die diesem Service zugeordnet sind.

IP-Serviceaffinitäten



Discovery-Bezeichner

Nachdem Discovery ein CI klassifiziert hat, wird anhand von Bezeichnern bestimmt, ob das Gerät bereits in der CMDB vorhanden ist.

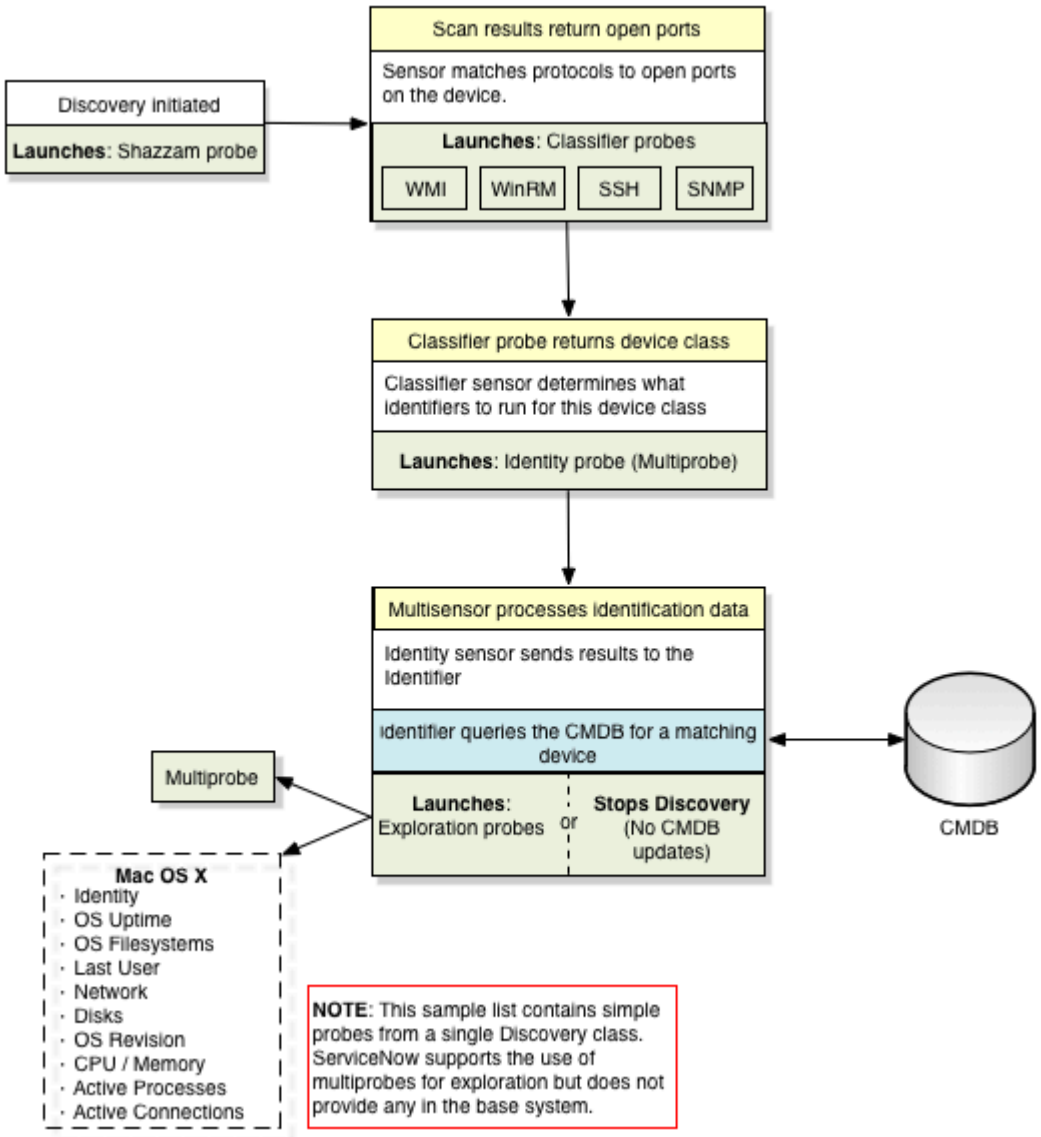
Discovery startet spezielle Identitäts-Probes, die Identifizierungsdaten für jedes Gerät sammeln und diese Daten in die Bezeichner einspeisen, die die Aktion bestimmen, die Discovery für das jeweilige Gerät ausführen muss. Bezeichner bestimmen genau die Identität des Geräts, um die Erstellung doppelter CIs zu verhindern. Dieser Identifizierungsschritt erfolgt nur für Erkennungen vom Typ „Konfigurationselement“, nicht für andere Erkennungstypen.

Die Identitäts-Probe im Discovery-Basissystem kann so konfiguriert werden, dass sie das Gerät auf Informationen wie Seriennummer, Name und Netzwerk-ID abfragt. Die Ergebnisse dieses Scans werden von einem Identitätssensor verarbeitet, der die Ergebnisse dann an den Bezeichner übergibt. Der Bezeichner versucht dann, ein passendes Gerät in der CMDB zu finden. Wenn der Bezeichner ein passendes CI findet, aktualisiert der Bezeichner das CI, oder es geschieht nichts. Wenn der Bezeichner kein passendes CI finden kann, wird entweder ein neues CI erstellt, oder es geschieht nichts. Wenn Discovery so konfiguriert ist, dass die Ausführung fortgesetzt wird, startet der Bezeichner die Erkundungs-Probes, die im Klassifizierungsdatensatz konfiguriert sind, um zusätzliche Informationen zum Gerät zusammenzutragen. Bei Erkundungs-Probes kann es sich um Multi-Probes oder einfache Probes handeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Seriennummern werden für eine genaue Asset-Nachverfolgung benötigt. Wenn Sie Baseline Probes, Sensoren oder Muster geändert haben, müssen Sie verifizieren, dass Seriennummern weiterhin erkannt werden. Darüber hinaus dürfen Sensoren oder Muster nicht so konfiguriert werden, dass die Syntax der Seriennummer geändert wird, z. B. durch Hinzufügen eines benutzerdefinierten Präfixes. Nicht dem Standard entsprechende Seriennummern können dazu führen, dass die Nachverfolgung von Assets ungenau ist.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit konfigurierten Bezeichnern.



Tabellen für CMDB-Bezeichner

Tabelle	Beschreibung
Bezeichner [cmdb_identifier]	Speichert alle Regeln für Bezeichner
Bezeichner-Eintrag [cmdb_identifier]	Speichert alle Attribute für Bezeichner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Bezeichner

Das Discovery-Standardsystem enthält die folgenden Regeln für Bezeichner, die jeweils einem bestimmten CI-Typ (Feld **sys_class_name** im CI-Datensatz) oder der Tabelle im Feld **Betrifft** zugeordnet sind und die entsprechenden Attribute für die Erkennung von CIs aus der angegebenen Tabelle enthalten. Wo erforderlich, um alle möglichen Vorkommen eines Attributs zu erkennen, werden Tabellen aus zugehörigen Listen (**Tabelle durchsuchen**) in die Regel einbezogen. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Sie eine CI-Identifizierungsregel .

Regeln für CMDB-Bezeichner

Regel	Gilt für Tabelle/Attribute	Tabelle/Attribute durchsuchen
ESX-Serverregel	ESX-Server [cmdb_ci_esx_server]: correlation_id	keine
Hardwareregel	Hardware [cmdb_ci_hardware] • serial_number • serial_number_type • Name • ip_address • mac_address	• Seriennummer [cmdb_serial_number] ◦ serial_number ◦ serial_number_type • Netzwerkadapter [cmdb_ci_network_adapter] ◦ ip_address ◦ mac_address
Speicherserverregel	Speicherserver [cmdb_ci_storage_server] • cim_object_path • Name • serial_number • serial_number_type • mac_address • ip_address	• Seriennummer [cmdb_serial_number] ◦ serial_number ◦ serial_number_type • Netzwerkadapter [cmdb_ci_network_adapter] ◦ ip_address ◦ mac_address
WBEM-Serviceregel	WBEM-Service [cmdb_ci_wbem_service]: cim_object_path	keine

Abgleichstrategie für Hardwareregel

sys_class_name kann kein Attribut für unabhängige Regeln wie cmdb_ci_hardware sein. Wenn Ihre Discovery-Identifizierungsstrategie davon abhängig ist, dass ein CI mit einer bestimmten Klasse abgeglichen wird, müssen Sie für jede Klasse, die Sie für den Abgleich verwenden möchten, eine neue Regel erstellen und diese Klasse im Feld **Betrifft** des Bezeichnerformulars angeben.

Beispielsweise können Sie einen Bezeichner für einen Linux-Server mit anderen Attributen als der Hardwareregel erstellen. Möglicherweise möchten Sie den Computernamen, die IP-Adresse und die MAC-Adresse zur Identifizierung verwenden. Dies ist eine Lösung

Automatische Übersetzung

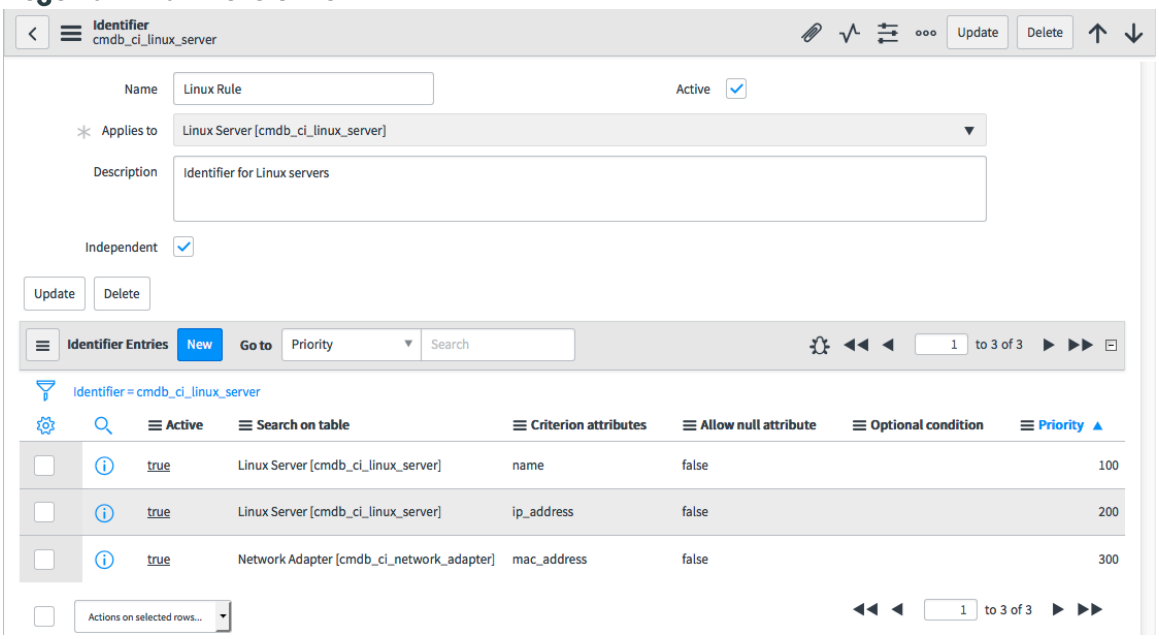
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für Netzwerke, die NIC-*Bonding* oder -*Teaming* verwenden, um die verfügbare Bandbreite zu erhöhen. Verbundene Schnittstellen scheinen dasselbe physische Gerät zu sein und dieselben IP- und MAC-Adresse zu verwenden. Durch die Verwendung des Attributs **name** kann Discovery zwischen den einzelnen Schnittstellen im verbundenen Kanal unterscheiden.

Wichtig: Wenn Sie einen Bezeichner mit dem Attribut **name** erstellen, vermeiden Sie es, die Namen der Adapter zu ändern. Discovery kann vorhandene CIs für umbenannte Adapter nicht auflösen. Discovery kennzeichnet den Installationsstatus dieses CIs als „Abwesend“ und erstellt ein anderes CI.

Ihre neue Regel würde wie folgt aussehen:

Regel für Linux-Bezeichner

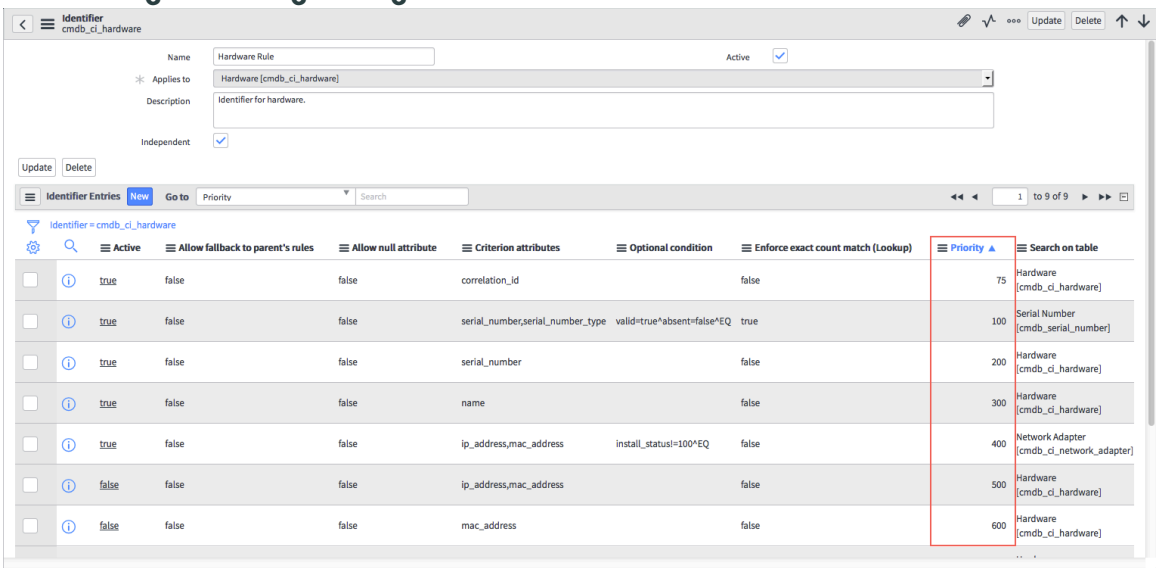


Auswertungsreihenfolge für Discovery-Bezeichner

Benutzerdefinierte Bezeichner müssen andere Werte für die *Reihenfolge* aufweisen als die der Standardbezeichner. Discovery analysiert Bezeichner und Attribute der Reihe nach von niedrigen Zahlen zu hohen. Sie können Bezeichner erstellen, die vor oder nach den Standardbezeichnern ausgeführt oder mit den Bezeichnern des Basissystems gemischt werden. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um zu verhindern, dass der jeweilige Bezeichner bzw. die jeweilige Regel ausgeführt wird. Die Auswertungsreihenfolge für CMDB-Bezeichner ist in jeder Regel festgelegt und steuert nur die Analysereihenfolge der Attribute in der jeweiligen Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswertungsreihenfolge in Regeln für CMDB-Bezeichner



Eigenschaften zur Verarbeitung doppelter CIs

Mit den Eigenschaften, die mit „Identifizierung und Abgleich“ installiert werden, können Sie steuern, wie Discovery doppelte CIs verarbeitet. Verwenden Sie die Eigenschaften glide.identification_engine.skip_duplicates und glide.identification_engine.skip_duplicates.threshold. Weitere Informationen finden Sie unter Eigenschaften für Identifizierung und Abgleich .

Eigenschaften, die Bezeichnerversionen steuern

Alle Instanzen verwenden Kennungen aus dem CMDB Identification and Reconciliation Framework. Bei Upgrades von früheren Versionen als Geneva werden die veralteten Kennungen beibehalten. Sie können jedoch mithilfe einer Eigenschaft zu den neuen Kennungen wechseln: glide.discovery.use_cmdb_identifiers. Wenn Sie ein Upgrade von einer Version vor Geneva durchgeführt haben, müssen Sie diese Eigenschaft manuell hinzufügen und auf true setzen, um die neuen Kennungen zu verwenden. Wenn Sie ein Upgrade von Geneva oder späteren Versionen durchgeführt haben, ist diese Eigenschaft in der Tabelle Systemeigenschaften [sys_properties] verfügbar. Um die Funktionalität in benutzerdefinierten veralteten Kennungen zu erhalten, müssen Sie diese in das neue Format der CMDB-Bezeichnerregeln konvertieren, bevor Sie diese Eigenschaft aktivieren. Das System konfiguriert Ihre benutzerdefinierten Kennungen nicht automatisch erneut für das neue Framework.

Hinweis: Wenn die Service-Zuordnung aktiv ist, werden die neuen Kennungen aus dem „CMDB Identification and Reconciliation Framework“ unabhängig vom Eigenschaftswert verwendet.

Funktionsweise von Discovery-Bezeichnern

Wenn Discovery die Klasse eines Geräts bestimmt hat, wird eine Identitäts-Probe gestartet, die so konfiguriert ist, dass sie mindestens einen Befehl mit einer einzigen Authentifizierung ausführt.

Die Identitäts-Probe im Discovery-Basissystem kann so konfiguriert werden, dass sie das Gerät auf Informationen wie Seriennummer, Name und Netzwerk-ID abfragt. Die Ergebnisse dieses Scans werden von einem Identitätssensor verarbeitet, der die Ergebnisse dann an den Bezeichner übergibt. Der Bezeichner versucht dann, ein passendes Gerät in der CMDB zu finden. Wenn der Bezeichner ein passendes CI findet, aktualisiert der Bezeichner das CI, oder es geschieht nichts. Wenn der Bezeichner kein passendes CI finden kann, wird

Automatische Übersetzung

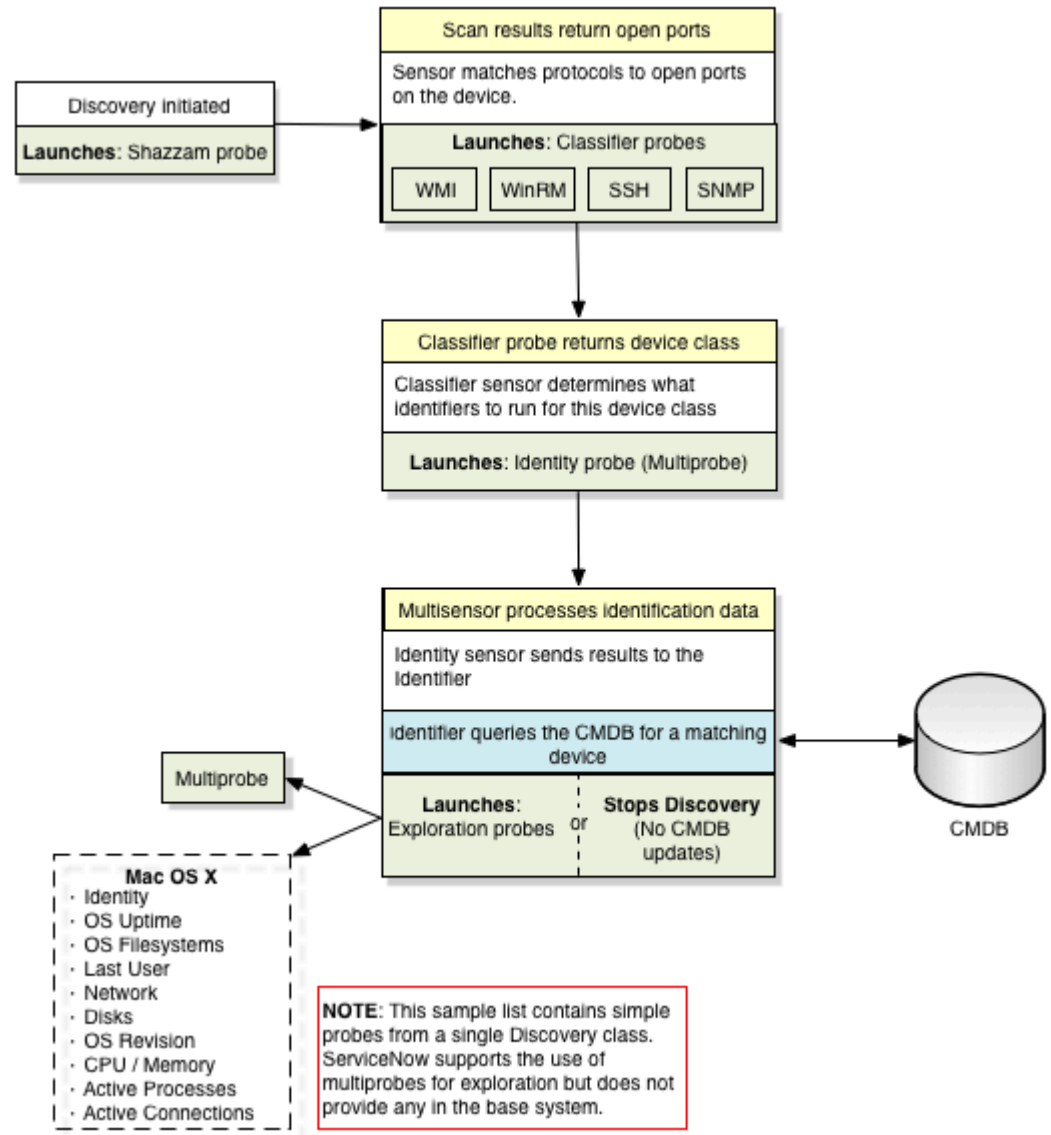
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

entweder ein neues CI erstellt, oder es geschieht nichts. Wenn Discovery so konfiguriert ist, dass die Ausführung fortgesetzt wird, startet der Bezeichner die Erkundungs-Probes, die im Klassifizierungsdatensatz konfiguriert sind, um zusätzliche Informationen zum Gerät zusammenzutragen. Bei Erkundungs-Probes kann es sich um Multi-Probes oder einfache Probes handeln.

Hinweis: Wenn Sie Muster für verwenden Discovery, Die Identitätsprobe wird nicht verwendet. Discovery Verwendet die entsprechenden Bezeichnerregeln basierend auf dem CI-Typ, den Sie erkennen möchten, wie in den Mustervorgängen angegeben. Von den Vorgängen im Muster und diesen Bezeichner-Regeln werden die Identifizierungs- und Untersuchungsphasen der Erkennung durchgeführt.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit konfigurierten Bezeichnern.

Discovery-Bezeichner



Identitäts-Probes in Discovery konfigurieren

Identitäts-Probes sind Multi-Probes, die mindestens eine einfache Probe enthalten und zum Extrahieren bestimmter Informationen von verwaltbaren Geräten konfiguriert sind. Sie können Ihre eigene Identitäts-Multi-Probe erstellen, um CIs zu identifizieren, die von Discovery noch nicht identifiziert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

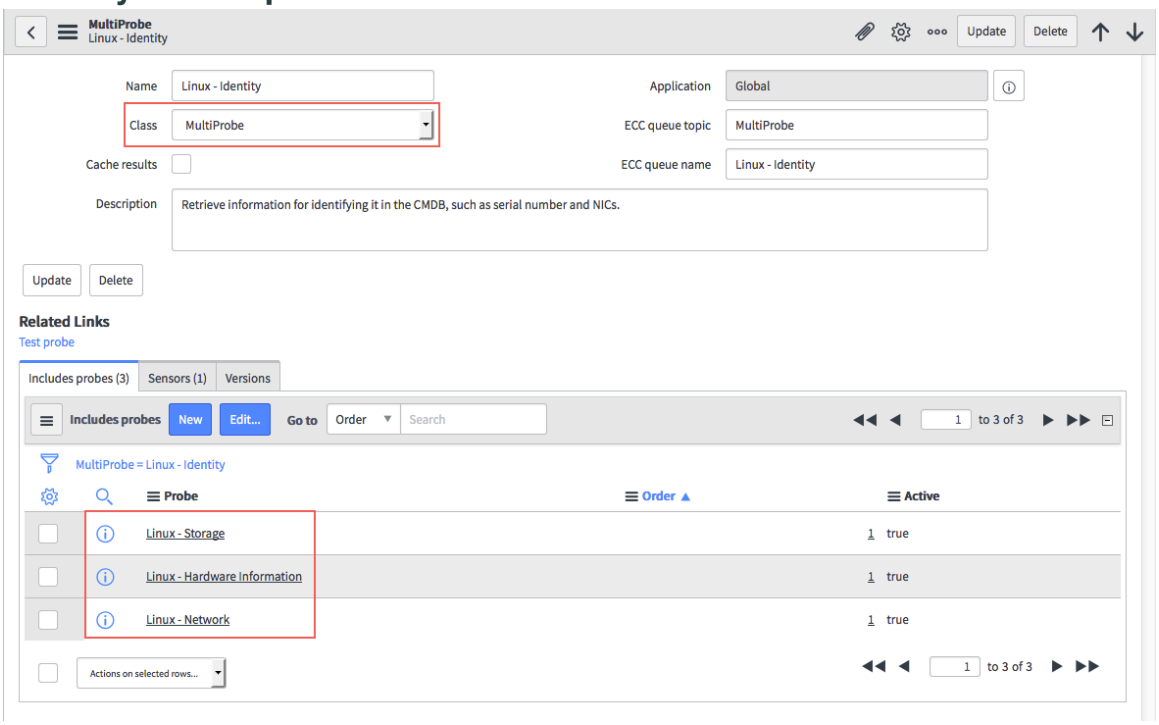
Warum und wann dieser Vorgang ausgeführt wird
Identitäts-Probes geben Informationen wie die Seriennummern von Geräten (es können mehrere pro Gerät vorhanden sein), den Computernamen und die Netzwerkidentifizierung (MAC-Adresse) zurück. Beispielsweise enthält die im System bereitgestellte Multi-Probe *Linux - Identity* zwei einfache SSH-Probes, die so konfiguriert sind, dass sie Hardware- und Netzwerkinformationen zum jeweiligen Gerät zurückgeben. Nachdem die Probe diese Informationen erkannt hat, übergibt sie die Daten an einen Multisensor, der für die Verarbeitung von Identitätsinformationen konfiguriert ist.

Hinweis: Eine Multi-Probe kann keinen weiteren Multi-Probe enthalten.

Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**an.
2. Wählen Sie eine Probe in der Liste aus, dessen **Klasse** *Multi-Probe* lautet.
3. Stellen Sie sicher, dass der Umfang auf **Global** festgelegt ist.
4. Klicken Sie in der zugehörigen Liste **Enthält Probes** auf **Bearbeiten**, um einfache Probes auszuwählen, die in diese Multi-Probe aufgenommen werden sollen.
5. Klicken Sie auf **Neu**, um eine neue einfache Probe zu erstellen.

Example:

Discovery-Identitätsprobes



Nächste Maßnahme
Identitätssensoren in Discovery konfigurieren, die Teil der Identitäts-Probes sind.

Identitätssensoren in Discovery konfigurieren

Wenn Sie eine Identitäts-Multi-Probe anpassen, können Sie auch einen Multisensor dafür konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Multisensoren übergeben die von den Identitäts-Probes zurückgegebenen Daten an die Discovery-Bezeichner. Die Bezeichner durchsuchen dann die CMDB nach übereinstimmenden CIs. Wenn die Identität eines Geräts aufgelöst wird, übergeben die Bezeichner den Ergebnisstatus für das Gerät an die Multisensoren, die entsprechend reagieren, indem sie entweder Erkundungs-Probes starten oder Discovery für dieses Gerät stoppen.

Prozedur

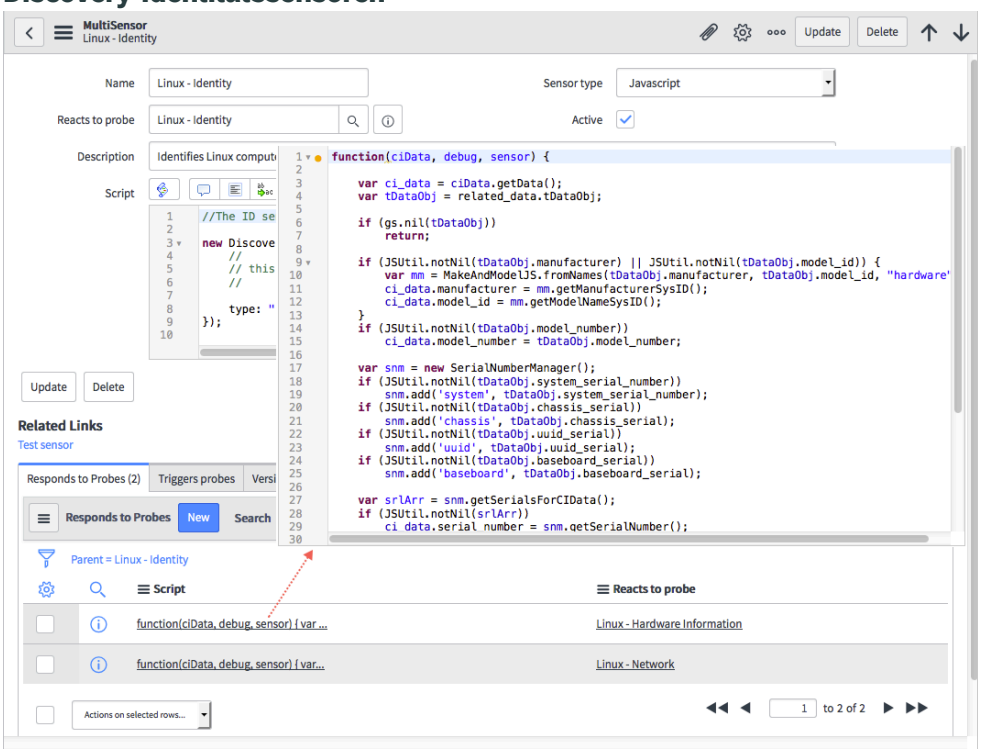
1. Navigieren zu **Alle** > **Discovery-Definition** > **Sensoren**an.
2. Wählen Sie vorhandene Identitäts-Multisensoren in der Liste aus.

   Hinweis: Zur Vermeidung von Verwechslungen müssen die in der Instanz bereitgestellten Multisensoren dieselben Namen wie die entsprechenden Multi-Probes aufweisen.

   Die zugehörige Liste **Reagiert auf Probes** enthält die einfachen Probes, die Daten an diese Multisensoren übergeben. Das sind dieselben einfachen Probes, die in der Liste „Enthält Probes“ im entsprechenden Multi-Probe-Datensatz angezeigt werden.
3. Klicken Sie für jede Probe in der Liste auf den Link **Skript**, um das Skript anzuzeigen, das von den Multisensoren zur Verarbeitung der Daten von der Probe ausgeführt wird.

Example:

Discovery-Identitätssensoren



Nächste Maßnahme

Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach CIs zu suchen und sicherzustellen, dass sie in der CMDB korrekt identifiziert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seriennummertypen zur Identifizierung

Wenn Discovery CIs findet, werden deren Seriennummern in der Tabelle „Seriennummer“ [cmdb_serial_number] aufgelistet, damit sie leicht zu identifizieren sind. Seriennummertypen variieren je nach CI, wie in den folgenden Beispielen beschrieben.

Wichtig: Seriennummern werden für eine genaue Asset-Nachverfolgung benötigt. Wenn Sie Baseline Probes, Sensoren oder Muster geändert haben, müssen Sie verifizieren, dass Seriennummern weiterhin erkannt werden. Darüber hinaus dürfen Sensoren oder Muster nicht so konfiguriert werden, dass die Syntax der Seriennummer geändert wird, z. B. durch Hinzufügen eines benutzerdefinierten Präfixes. Nicht dem Standard entsprechende Seriennummern können dazu führen, dass die Nachverfolgung von Assets ungenau ist.

Linux

Im Ergebnis von dmidecode | cat entspricht der Wert auf der linken Seite dem, wonach Discovery sucht. Der Wert auf der rechten Seite gibt an, wie die Nummer in der Tabelle „Seriennummer“ [cmdb_serial_number] gespeichert wird.

```
Serial Number : system_serial_number

UUID : uuid_serial

Serial Number : baseboard_serial

Serial Number : chassis_serial
```

Windows

Für Win32-WMI-Klassen entspricht der Wert auf der linken Seite dem Namen, unter dem die Nummer in der Tabelle „Seriennummer“ [cmdb_serial_number] gespeichert wird. Der Wert auf der rechten Seite entspricht dem WMI-Wert.

```
('system' : Win32_ComputerSystemProduct.IdentifyingNumber);

('uuid' : Win32_ComputerSystemProduct.UUID);

('chassis' : Win32_SystemEnclosure.SerialNumber);

('bios' : Win32_BIOS.SerialNumber);

('baseboard' : Win32_BaseBoard.SerialNumber);
```

SNMP

Für SNMP basiert die folgende Zuordnung auf dem Code. Die physischen Typen der Seriennummern stammen aus allen Instanzen von iso.org.dod.internet.mgmt.mib-2.entityMIB.

```
'cisco_stack' :
 'iso.org.dod.internet.private.enterprises.cisco.workgroup.ciscoStackMIB.chassisGrp.chassisSerialNumberString'

'cisco_chassis' : 'iso.org.dod.internet.private.enterprises.cisco.temporary.chassis.chassisId'

'foundry' :
 'iso.org.dod.internet.private.enterprises.foundry.products.switch.snChassis.snChasGen.snChasSerNum'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
'apc_pdu' :
 'iso.org.dod.internet.private.enterprises.apc.products.hardware.masterswitch.sPDUIdent.sPDUI
dentSerialNumber'

'printer' : 'iso.org.dod.internet.mgmt.mib-2.printmib.prtGeneral.prtGeneralEntry'

'standard' :
 'iso.org.dod.internet.private.enterprises.apc.products.hardware.ups.upsIdent.upsAdvIdent.upsA
dvIdentSerialNumber'
```

Discovery-Status

Der Discovery-Status bietet eine Zusammenfassung einer Erkennung, die über einen Zeitplan gestartet wurde. Sie können eine Erkennung, die gerade ausgeführt wird, auch über das Statusformular abbrechen.

Hinweis: Discovery-Zeitpläne, die über eine definierte Anzahl von Minuten keine Statusaktualisierungen haben, werden automatisch vom Discovery-Statusüberwachungsauftrag analysiert. Standardmäßig gilt dieser Auftrag für Discovery-Zeitpläne, die Konfigurationselemente erkennen. Weitere Informationen finden Sie unter Discovery-Statusüberwachungsauftrag artikel in der Now Support Knowledge Base.

Um auf das Formular „Discovery-Status“ zuzugreifen, navigieren Sie zu **Discovery** > **Status** Und öffnen Sie den Statusdatensatz für eine Discovery.

Jeder Datensatz in der Statusliste stellt die Ausführung einer Erkennung nach einem Zeitplan dar und zeigt allgemeine Informationen wie das Datum der Erkennung, den Modus, die Anzahl der an Geräte gesendeten Probe-Nachrichten und die Anzahl der verarbeiteten Sensordatensätze an. Ein Statusdatensatz enthält Daten, die Ihnen bei der Fehlerbehebung bei einer fehlgeschlagenen Erkennung helfen können. Verwenden Sie diese Daten, um Fehler im Verhalten einzelner Probes und Sensoren zu beheben oder diese Elemente sogar separat auszuführen. Verwenden Sie die Statussteuerungen, um in Probe-/Sensor-Threads für eine bestimmte Erkennung an beliebiger Stelle einzutreten, und folgen Sie dann dem Prozess in beide Richtungen. Sie können auch leicht erkennen, welche Klassifizierungs-Probe ausgeführt wurde und ein bestimmtes Gerät erkannt hat, indem Sie die Spalte der Klassifizierungs-Probe in der Geräteliste anzeigen.

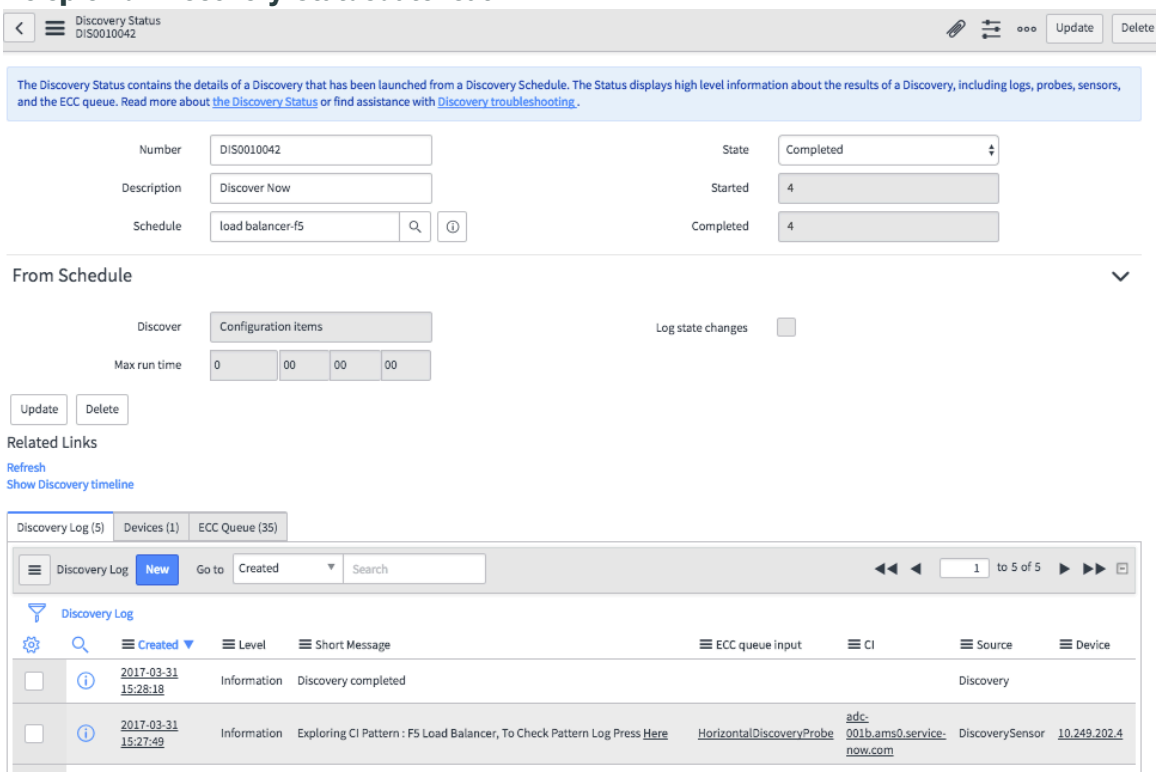
- **Aktualisieren**: Aktualisiert die zugehörigen Registerkarten, einschließlich **Discovery-Protokoll** und **ECC-Warteschlange** für noch laufende Erkennungsvorgänge.
- **Discovery-Zeitleiste**: Die Discovery-Zeitleiste ist eine grafische Anzeige einer Erkennung, die Informationen zu allen verwendeten Probes und Sensoren enthält.
- **Discovery log entries (Discovery-Protokolleinträge)**: Das Discovery-Protokoll zeigt Informationen wie Klassifizierungsfehler, CMDB-Updates und Authentifizierungsfehler an. Ein Discovery-Protokolldatensatz wird für jede Aktion erstellt, die einem Erkennungsstatus zugeordnet ist.
- **ECC queue entries (ECC-Warteschlangeneinträge)**: Einträge in der ECC-Warteschlange stellen einen zusammenhängenden Flow der Aktivitäten von Probes und Sensoren sowie die tatsächliche XML-Nutzlast bereit, die an eine oder von einer Instanz gesendet wird.
- **Device history (Geräteverlauf)**: Der Geräteverlauf bietet eine Zusammenfassung aller während der Erkennung gescannten Geräte und der Aktionen, die Sensoren in der CMDB ausgeführt haben.

Hinweis: Standardmäßig werden Discovery-Datensätze in der Statusliste nur jeweils über einen Zeitraum von 30 Tagen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der folgende Discovery-Statusdatensatz zeigt die Erkennung eines Lastenausgleichsmoduls mithilfe eines Musters.

Beispiel für Discovery-Statusdatensatz



Feld	Beschreibung
Nummer	Eine automatisch generierte Nummer für den Datensatz
Beschreibung	Art dieser Discovery-Ausführung. Normalerweise lautet die Beschreibung *Geplant*. Wenn Sie Discovery jedoch manuell über einen Zeitplan ausgeführt haben, wird im Feld *Beschreibung* für den Datensatz *Discovery starten* angezeigt.
Zeitplan	Name des Erkennungszeitplans
Status	Status der Erkennung: • **Wird gestartet** • **Aktiv** • **Abgeschlossen** • **Abgebrochen**
„Gestartet“ und „Abgeschlossen“	Die Anzahl der während der Erkennung gestarteten und abgeschlossenen Probes
Quelle	Optionales schreibgeschütztes Feld, das die Quelle der Erkennung anzeigt, zum Beispiel **Discovery planen** oder **Schnell-Discovery**. Wenn die Quelle der Discovery ein API-Aufruf war, lautet die Quelle **DiscoveryAPI**.
Über Zeitplan (schreibgeschützte Zeitplandaten)	
Erkennen	Zeigt den Discovery-Typ an. Die möglichen Typen sind: **Konfigurationselemente** , **IP-Adressen** , **Netzwerke** , Oder **Prozesse/Verbindungen** (ADM).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Maximale Laufzeit	Zeigt die maximale Dauer der Ausführung von Discovery nach diesem Zeitplan an
Statusänderungen protokollieren	Gibt an, dass Statusänderungen während dieser Discovery protokolliert wurden. Diese Status werden in den Feldern *Letzter* und *Aktuell* in der Liste **Discovery Devices** (Erkennungsgeräte) in diesem Formular angezeigt.

Zugehörige Informationen

Horizontale Erkennung planen

Erkennung über Discovery-Status abbrechen

Sie können eine Erkennung manuell über den Discovery-Statusdatensatz abbrechen, während sie ausgeführt wird.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Status**an.
2. Klicken Sie auf eine **Nummer**, um den Statusdatensatz zu öffnen.
3. Klicken Sie auf **Discovery abbrechen** unter **Zugehörige Links**.
   Discovery abbrechen ist nur für aktive Erkennungen verfügbar.

Ergebnis
Wenn ein Discovery-Status abgebrochen wird, werden alle zugehörigen Sensortransaktionen sofort beendet und alle geplanten Sensoraufträge aus dem System gelöscht. Nach dem Abbruch wird für den Bereinigungsstatus die **Abgeschlossene Anzahl** angezeigt, und der Abbruch wird im Discovery-Protokoll protokolliert. In der Tabelle „Warteschlange“ [ecc_queue] werden alle Datensätze auf den Status **Fehler** gesetzt, die zu Sensoren gehören, die die Transaktionsmengenregel überschreiten.

Discovery-Zeitleisten

Eine Discovery-Zeitleiste generiert die grafische Anzeige eines Discovery-Statusdatensatzes, einschließlich Informationen zu allen für die Erkennung verwendeten Probes und Sensoren.

Verwenden Sie Discovery-Zeitachsen, um Folgendes anzuzeigen:

- Den Flow von Probes und Sensoren, einschließlich derer, die mit Mustern im Rahmen einer Erkennung verwendet werden
- Die Dauer der einzelnen Probes und Sensoren, die während einer Erkennung ausgeführt wurden, und der Zeitanteil, der in der Warteschlange verbracht wurde und für die Verarbeitung erforderlich war
- Tooltips mit zusätzlichen Daten zu einer Probe und einem Sensor
- Datensätze aus der ECC-Warteschlange

Größe der Erkennungen in der Zeitleiste

Zeigen Sie Zeitleisten für eine gesamte Erkennung oder für einzelne Geräte in einer Erkennung an. Standardmäßig beträgt die maximale Größe der Discovery, die Sie in einer Zeitleiste anzeigen können, 300 Einträge in der ECC-Warteschlange (150 Probes und 150

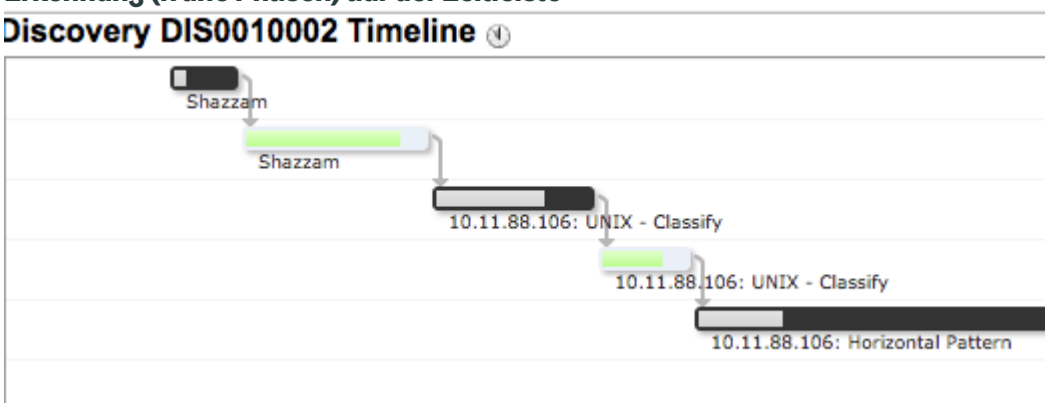
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sensoren). Um größere Erkennungen anzuzeigen, ändern Sie die Standardeinstellung in `Glide.Discovery.Timeline.max_entry` Eigenschaft.

Beispiel: Discovery-Zeitachsen

Dieses Beispiel zeigt die Discovery-Zeitleiste für die ersten beiden Phasen der Erkennung (Port-Scan und Klassifizierung):

Erkennung (frühe Phasen) auf der Zeitleiste



In diesem Beispiel werden die Shazzam-Probe und der Sensor ausgeführt, gefolgt von der Klassifizierer-Probe „Unix“ und dem Sensor. Der Klassifizierer ruft die Probe „Horizontal Pattern“ auf, die ein bestimmtes Muster ausführt.

Discovery-Zeitleiste anzeigen

Eine Discovery-Zeitleiste generiert die grafische Anzeige eines Discovery-Statusdatensatzes, einschließlich Informationen zu jeder ausgeführten Probe, jedem Sensor und jedem Muster.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

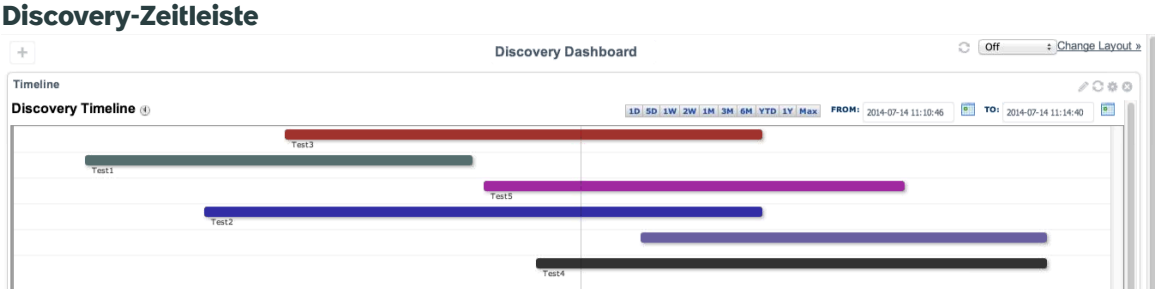
Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Status**an.
2. Wählen Sie in der Datensatzliste eine Discovery aus.
3. Klicken Sie auf den zugehörigen Link **Discovery-Zeitleiste anzeigen**.
4. Löschen Sie die Warnung, und wählen Sie dann die zugehörige Liste **Geräte** aus.
5. Klicken Sie auf die IP-Adresse eines Geräts.
6. Klicken Sie im Gerätedatensatz auf den zugehörigen Link **Discovery-Zeitleiste anzeigen**.

Die Discovery-Zeitleiste für dieses Gerät wird angezeigt.

Discovery-Zeitleiste



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Verwenden Sie den rosa Schieberegler am unteren Rand der Zeitleiste, um die Perspektive zu ändern.

   a. Bewegen Sie den Schieberegler von rechts nach links, um alle Aufgaben auf einer langen Zeitleiste anzuzeigen.

   b. Passen Sie die Endpunkte des Schiebereglers an, um die Vergrößerung zu ändern.
   Ein schmaler Schieberegler zoomt näher an die Zeitspannen heran und bietet eine detailliertere Ansicht komplexer Zeitleisten. Ein breiter Schieberegler vergrößert die Ansicht und macht einen größeren Teil der Zeitleiste auf dem Bildschirm sichtbar.

8. Verwenden Sie den Auswahlbereich oben im Bildschirm, um den sichtbaren Zeitrahmen anzupassen.
9. Klicken Sie auf **Max.**, um die Zeitleiste auf die Länge der Discovery zu beschränken.

Die Zeitskala wird automatisch auf die Länge der Discovery angepasst. Der verfügbare Zeitskalenbereich reicht von einem Tag bis zu einem Jahr.

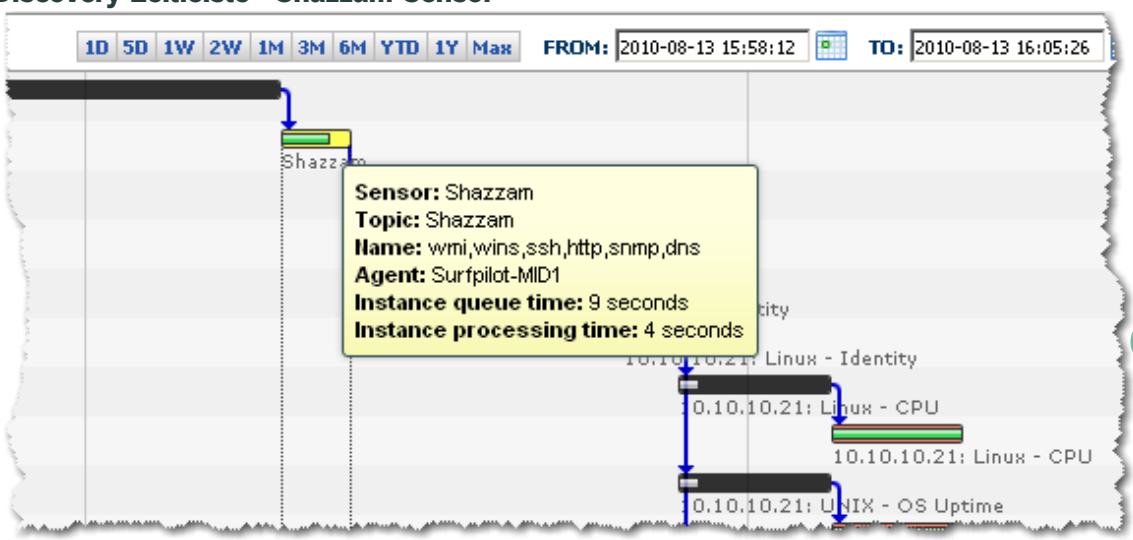
Tooltips

Discovery -Zeitleisten zeigen Leistungsdaten zu Probes und Sensoren sowie CI-Informationen in Tooltips an. Bewegen Sie den Cursor über eine Spanne, um diese Daten anzuzeigen.

Probes werden als schwarze Zeitrahmen angezeigt. Die Warteschlangenzeit einer Probe wird als silberner Balken innerhalb der Spanne angezeigt, und die Verarbeitungszeit wird durch den verbleibenden Platz dargestellt.

Sensorzeitspannen werden rot und die Warteschlangenzeit als grüner Balken angezeigt. Ausgewählte Zeitspannen beliebiger Art werden gelb angezeigt.

Discovery-Zeitleiste – Shazzam-Sensor



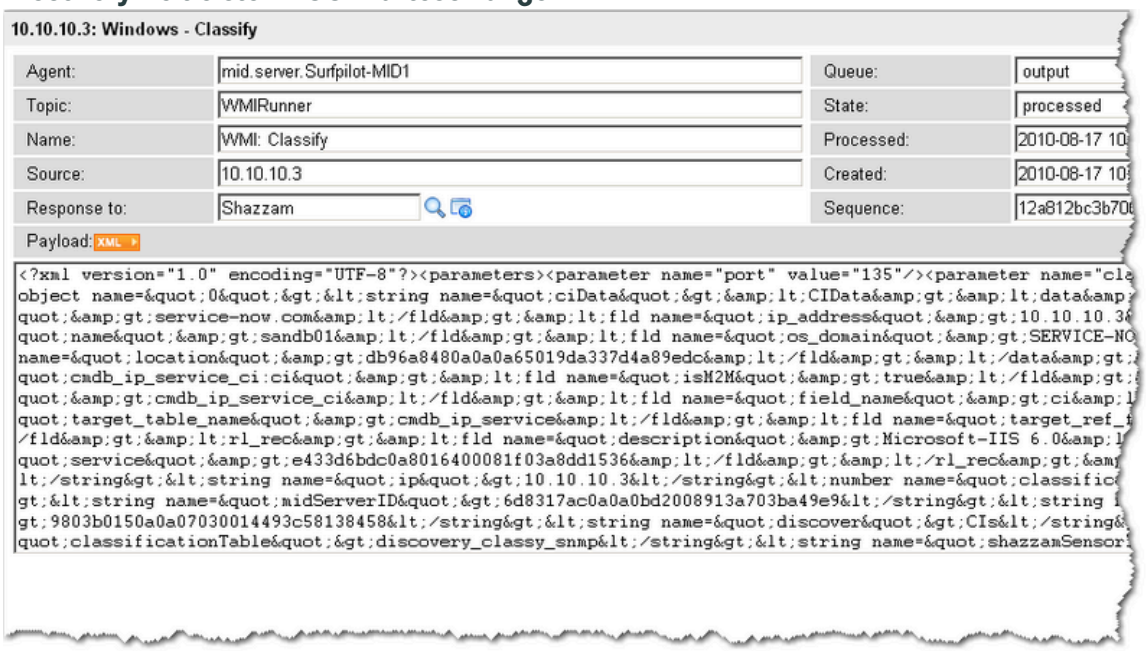
ECC-Warteschlange

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Doppelklicken Sie auf eine Zeitspanne, um den Datensatz der ECC-Warteschlange für diese Probe oder diesen Sensor zu öffnen.

Discovery-Zeitleiste – ECC-Warteschlange



ECC-Warteschlange für Discovery

Die ECC-Warteschlange (External Communication Channel) ist ein Verbindungspunkt zwischen ServiceNow Instanz und andere Systeme, die in die IT integriert werden, meist ein MID-Server.

Inhalte der ECC-Warteschlange

Die ECC-Warteschlange enthält Datensätze, die während aller Phasen der Erkennung erstellt werden. Jeder Datensatz ist eine Nachricht von der Instanz an das System, das Sie für die Discovery anvisieren, klassifiziert als **Ausgabe** , Oder eine Nachricht von diesem System an die Instanz, klassifiziert als **Eingabe** .

ECC-Warteschlangendatensätze bieten Ihnen einen verbundenen Flow von Probe- und Sensoraktivitäten zusammen mit der XML-Nutzlast, die an oder von einer Instanz gesendet wird, und den Assets, die Sie anvisieren.

Datensätze der ECC-Warteschlange automatisch löschen

Als Ihr IT-Asset Discovery Wird ausgeführt, kann die Größe der ECC-Warteschlange auf mehrere Gigabyte anwachsen. Die meisten Datensätze „abgeschlossene Aufgaben“ sind unnötig, einige können jedoch für die Behebung von Problemen wichtig sein.

Beispiel: Wenn Discovery Erfasst die Laufwerke auf einem bestimmten Windows-Server nicht ordnungsgemäß. Sie können in der ECC-Warteschlange die Daten anzeigen, die von der Probe „Windows – Systeminformationen“ zurückgegeben werden. Aus diesem Grund sollten Sie ECC-Warteschlangendaten aus beibehalten Discovery Mindestens einen Monat lang.

Standardmäßig werden Datensätze in der ECC-Warteschlange automatisch gelöscht, die älter als 7 Tage sind. Sie können den Löschzeitplan festlegen, indem Sie die ECC-Warteschlange (wie im nächsten Abschnitt erläutert) und den Tabellenrotationszeitplan aktualisieren. Die Namen für die Tabellenrotation lauten wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *ecc_queue_event*
- *ecc_queue*

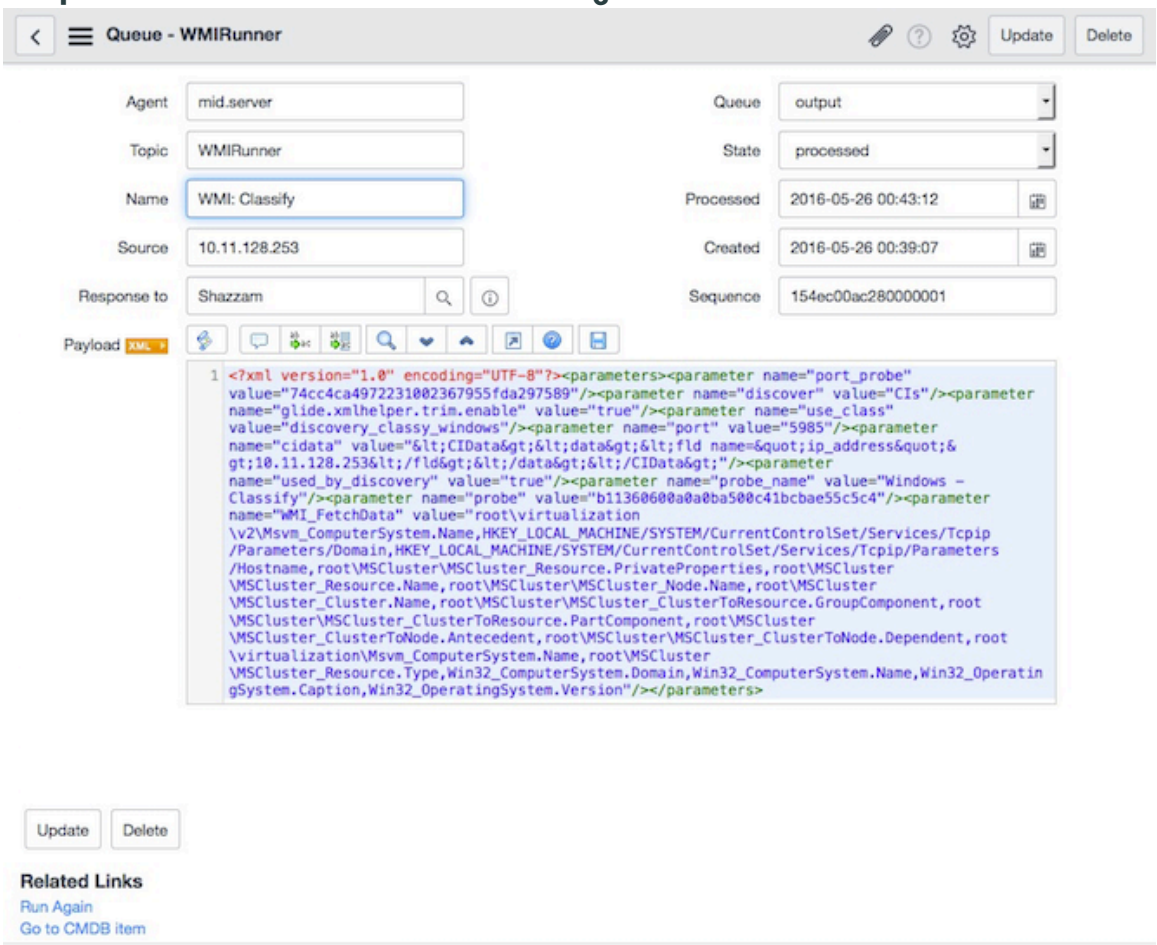
Auf ECC-Warteschlange zugreifen

Sie können über einen der folgenden Pfade auf die ECC-Warteschlange zugreifen:

- **Discovery** > **Ausgabe und Artefakte** > **ECC-Warteschlange**
- **ECC** > **Warteschlange**

Die folgende Abbildung enthält ein Beispiel für einen Datensatz in der ECC-Warteschlange. Dieser Datensatz zeigt, dass eine WMI-Klassifizierer-Probe zur Ausführung angewiesen und verarbeitet wurde. Beachten Sie die XML-Nutzlast, die als erfasste Daten der Discovery-Aufgabe zurückgegeben wurde. Siehe Die ECC-Warteschlange des MID-Servers Für eine Beschreibung der einzelnen Felder.

Beispiel für Datensatz einer ECC-Warteschlange



Statusangaben der ECC-Warteschlange

Eingabe- und Ausgabenachrichten werden verarbeitet, bis die Discovery abgeschlossen oder beendet ist. Sie können die ECC-Warteschlange überwachen, um zu sehen, wie Datensätze während der Discovery ausgefüllt werden, und um die status der einzelnen Datensatzänderungen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabedatensätze der ECC-Warteschlange werden von Business-Regeln (BR) verarbeitet, aber nicht alle Business-Regeln leiten diese ECC-Warteschlangeneingaben zur Verarbeitung weiter. Daher verbleiben einige ECC-Warteschlangeneingaben in einem **Bereit** status.

Der Prozess läuft wie folgt ab:

1. Wenn neue Probe-Anweisungen für einen MID Server verfügbar sind, erstellt das System einen Datensatz vom Typ **Ausgabe** mit dem Status **Bereit**.
2. Der MID Server startet dann die Verarbeitung der Probe-Anweisungen, und der Status wird in **In Verarbeitung** geändert, bevor er schließlich auf **Verarbeitet** gesetzt wird.
3. Wenn ein Ergebnis an den MID Server zurückgegeben wird und zum Senden an die Instanz bereit ist, erstellt das System einen Datensatz vom Typ **Eingabe** mit dem Status **Bereit**.
4. Während das System die Nutzlast verarbeitet, wird der Status in **In Verarbeitung** geändert, bevor er schließlich auf **Verarbeitet** gesetzt wird.

   Wenn Fehler auftreten, wird der Status in **Fehler** geändert. Sie können Fehler als Ausgangspunkt für die Behebung einer fehlgeschlagenen Discovery überprüfen.

Debuggen der Verarbeitung von ECC-Warteschlangendatensätzen

Um einen Skript-Debugger zu verwenden, verarbeiten Sie die Nutzlast in derselben Sitzung wie der Debugger. Überprüfen Sie die Business-Regel, die den bestimmten ECC-Warteschlangendatensatz verarbeitet, und den tatsächlichen Code, der die Nutzlast verarbeitet.

Eigenschaften und Parameter, die sich auf die ECC-Warteschlange auswirken

Mit den folgenden Eigenschaften lassen sich Aspekte der ECC-Warteschlange steuern:

Eigenschaft	Beschreibung
Anhänge der ECC-Warteschlange speichern	Das normale Verhalten von Erkennungssensoren besteht darin, Anhänge an ECC-Warteschlangeneinträgen nach erfolgreicher Sensorbearbeitung zu löschen. Durch Aktivierung dieser Eigenschaft wird dieses Verhalten außer Kraft gesetzt, Anhänge werden beibehalten. Dies erfolgt normalerweise zu Debugging-Zwecken. Um diese Eigenschaft zu aktivieren, navigieren Sie zu **Discovery-Definition** > **Eigenschaften**an.

Zugehörige Informationen

Den Inhalt der ECC-Warteschlange für einen MID Server verwalten

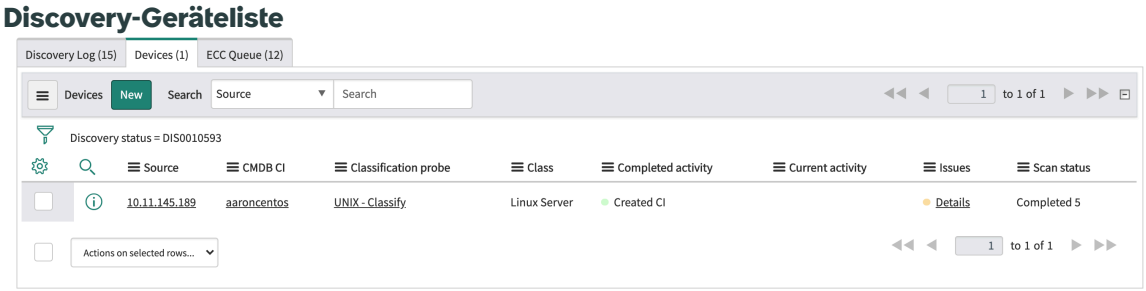
Discovery-Geräteverlauf

Die zugehörige Liste **Geräte** im Formular „Discovery-Status“ enthält eine zusammenfassende Liste aller gescannten Geräte.

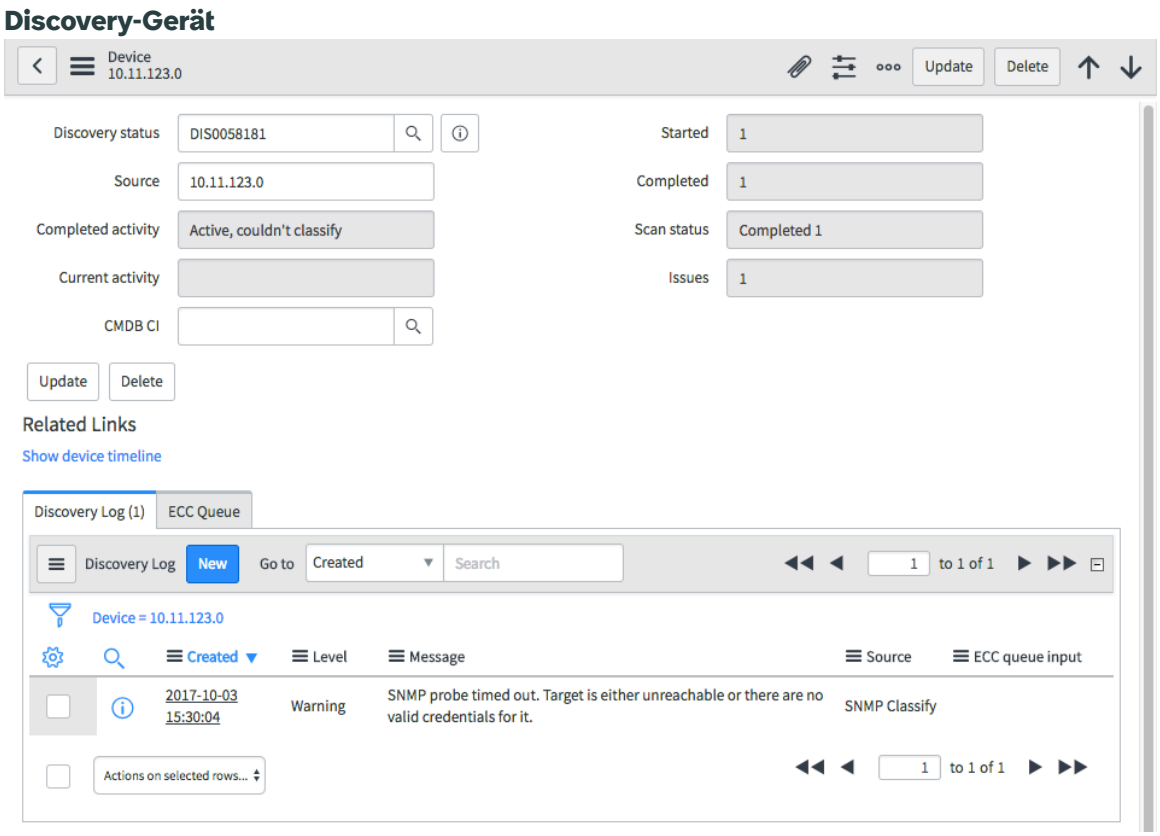
Während einer Discovery werden über die Liste aktuelle und abgeschlossene Aktivitäten nachverfolgt, und der inkrementelle Zähler für Scans wird angezeigt. Wenn Discovery für ein Gerät abgeschlossen ist, wird die endgültige Disposition in der Spalte *Abgeschlossene Aktivität* angezeigt. Erfolgreiche Erkennungen, die zu aktualisierten oder erstellten CIs führen, werden grün hervorgehoben. Wenn ein Geräteverlauf oder ein doppelter IP-Datensatz erstellt wird, wird auch die Klassifizierungs-Probe eingetragen. Um die Protokolleinträge für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler (zum Beispiel Verbindungsfehler) für ein bestimmtes Gerät anzuzeigen, klicken Sie auf den Link **Details** in der Spalte *Probleme*.



Klicken Sie auf die IP-Adresse eines Geräts in dieser Liste, um Details zu diesem Gerät anzuzeigen. Die Protokollergebnisse für dieses Gerät werden in der Liste unten im Formular angezeigt.



In diesem Formular sind die folgenden Felder verfügbar:

Feld	Eingabewert
Quelle	IP-Adresse des erkannten Geräts
Abgeschlossene Aktivität	Gibt das Ergebnis der Discovery für dieses Gerät oder die letzte abgeschlossene Aktivität für eine in Bearbeitung befindliche Discovery an, zum Beispiel *Identifiziertes CI*. Erfolgreiche Ergebnisse werden in Grün angezeigt.
Aktuelle Aktivität	Aktuelle Scan-Aktivität für dieses Gerät für eine in Bearbeitung befindliche Discovery, zum Beispiel *CI wird aktualisiert*
CMDB CI	Name des Geräts, wie in der CMDB angezeigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Gestartet	Anzahl der ausgeführten gerätespezifischen Probes. Diese Zahl enthält nicht die universellen Probes Shazzam und Ping, die anfänglich ausgeführt werden.
Abgeschlossen	Anzahl der Sensordatensätze, die aus den ausgeführten gerätespezifischen Probes erstellt wurden
Scan-Status	Zeigt die endgültige Anzahl von Scans einer abgeschlossenen Discovery oder einen inkrementellen Zähler der Scans für eine in Bearbeitung befindliche Discovery an. Beispiel: Scan 17 von 19
Probleme	Zeigt die Anzahl der Probleme an, die während der Discovery dieses Geräts aufgetreten sind. Wählen Sie die zugehörige Liste **Discovery-Protokoll** aus, um diese Probleme anzuzeigen.
Felder, die durch die Konfiguration des Formulars hinzugefügt werden können:	
DNS-Namen	Zeigt DNS-Namen für jedes erkannte Gerät an

Während verschiedener Phasen von Discovery, Möglicherweise werden verschiedene Werte in angezeigt **Aktivität Abgeschlossen** Feld in einem Discovery_device_history-Datensatz.

Potenzielle Werte für abgeschlossene Aktivität in „Discovery_device_history“

Wert	Wann dieser Wert angezeigt wird	Bedeutung
Häufige Beispiele		
Aktiv, nicht aktiv, nicht klassifiziert	Nach Shazzam	Gerät reagiert, hat jedoch keine offenen (aktiven) Ports, für die eine Klassifizierung ausgeführt werden kann.
Aktiv	Nach Shazzam	Das Gerät verfügt über offene (aktive) Ports, für die möglicherweise eine Klassifizierung ausgeführt werden kann.
Classified (Klassifiziert)	Probe Nach Der Klassifizierung	Wir konnten den Gerätetyp klassifizieren und fahren mit der Identifizierungsphase fort.
Aktiv, Klassifizierung nicht möglich	Probe Nach Der Klassifizierung	Der Gerätetyp konnte nicht klassifiziert werden. Manchmal enthält dieser Wert auch einen Grund dafür, warum wir nicht klassifizieren konnten. Beispiel: Aktiv, konnte nicht klassifiziert werden: Keine WMI-Verbindung.
Erstelltes CI	Probe/Muster nach Identifizierung oder nach Discovery – Ausführung der Business-Regel für Gerät abgeschlossen (für neues CI)	Neues CI wurde basierend auf Identifizierungsergebnissen erstellt.
Identifiziertes CI	Probe/Muster Nach Identifizierung	Vorhandenes CI wurde basierend auf Identifizierungsergebnissen gefunden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Potenzielle Werte für abgeschlossene Aktivität in „Discovery_device_history“ (Fortsetzung)

Wert	Wann dieser Wert angezeigt wird	Bedeutung
Identifiziert, zusätzliche IP ignoriert	Probe/Muster Nach Identifizierung	Gerät wurde bereits über eine andere IP in erkannt Discovery Status.
Aktualisiertes CI	Nach bestimmten Exploration-Probes/Mustern oder nach der Ausführung der Business-Regel „Gerät abgeschlossen“ (für vorhandenes CI)	CI wurde mit zusätzlichen Informationen aktualisiert.
Weniger häufige Beispiele		
Nicht klassifiziert	Nach Shazzam (nur für Anmeldeinformationslose Discovery Und der Wert „Erkennen“ auf der Discovery Zeitplan ist auf IP-Adressen festgelegt)	Für Anmeldeinformationslose Discovery Von der Ziel-IP konnten wir nicht mit einem vorhandenen CI in der Instanz abgleichen.
Classified (Klassifiziert)	Nach Shazzam (nur für Anmeldeinformationslose Discovery Und der Wert „Erkennen“ auf der Discovery Zeitplan ist auf IP-Adressen festgelegt)	Für Anmeldeinformationslose Discovery Von der Ziel-IP konnten wir mit einem vorhandenen CI in der Instanz abgleichen.
Aktiv, Windows-Cluster-VIP	Nach Windows: Klassifizieren	Das Gerät ist ein Windows-Cluster-VIP und wird als solches aktualisiert.
Klassifiziert, aber nicht deaktiviert	Probe Nach Der Klassifizierung	Wir haben eine Übereinstimmung mit einem Klassifiziertyp vorgenommen, aber der Klassifizierer selbst ist deaktiviert.
Klassifiziert, konnte nicht identifiziert werden	Probe/Muster Nach Identifizierung	Vorhandener CI-Datensatz konnte nicht erstellt oder abgeglichen werden.
Identifiziert, CI wird nicht aktualisiert	Probe/Muster Nach Identifizierung	Wir konnten einen CI-Datensatz ordnungsgemäß identifizieren, aber wir entscheiden uns dafür, das CI nicht zu aktualisieren.

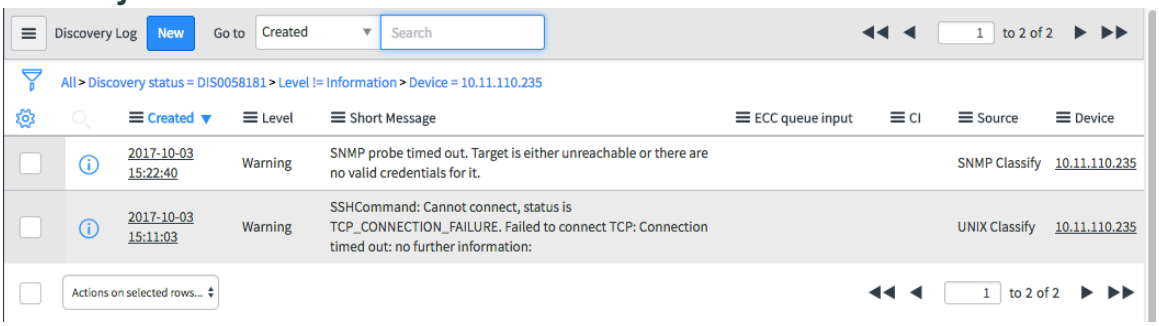
Jedes Gerät, das die folgenden Klassen oder eine der untergeordneten Klassen enthält, wird in der Discovery-Geräteverlaufstabelle angezeigt.

- Computer [cmdb_ci_computer]
- Netzwerkausrüstung [cmdb_ci_netgear]
- PDU [cmdb_ci_pdu]
- Drucker [cmdb_ci_printer]
- UPS [cmdb_ci_ups]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Probleme aufgetreten sind oder eine Discovery nicht abgeschlossen werden konnte, klicken Sie auf den Link **Details**, um die Protokolldatensätze für das Problem anzuzeigen. Der Ausfall einer Probe gilt als Problem, auch wenn das Gerät schließlich ordnungsgemäß klassifiziert und in der CMDB aktualisiert wurde.

Discovery-Details zu einem Gerät



Adress-Scan-Daten

Wenn Discovery nur nach IP-Adressen (ohne Anmeldeinformationen oder Bezeichner) scannt, werden keine Aktualisierungen an der CMDB vorgenommen. Alle erkannten IP-Adressen werden in dieser Liste angezeigt, einschließlich mehrerer IP-Adressen für dasselbe Gerät. Die Ergebnisse von IP-Adress-Scans enthalten geringfügig andere Informationen als die Ergebnisse eines CI-Scans. Da dem IP-Adress-Scan keine CMDB-Aktivität zugeordnet ist, zeigt die Spalte *Abgeschlossene Aktivität* nur den Klassifizierungsstatus an.

Mögliche Status sind:

- *Classified (Klassifiziert)*
- *Nicht klassifiziert*
- *Alive, not classified (Aktiv, nicht klassifiziert)*

Bei klassifizierten Geräten kann Discovery den Gerätetyp in der Spalte *Aktuelle Aktivität* angeben. Beispielsweise können Netzwerkgeräte als Cisco-Netzwerkgeräte klassifiziert werden und ein Computer als Windows-Computer.

Protokolle für horizontale Erkennung

Das System sammelt Protokolle, um die Aktivität widerzuspiegeln, die während einer horizontalen Erkennung basierend auf Mustern und Probes stattfindet. Verwenden Sie die Protokolle, um den Erkennungsprozess zu optimieren oder Probleme zu beheben.

Für die horizontale Erkennung werden vom System Protokolle der folgenden Typen generiert:

Probe-basiert

Die Protokolle für die Probe-basierte horizontale Erkennung decken Klassifizierungsfehler, CMDB-Aktualisierungen und Authentifizierungsfehler ab. Ein Discovery-Protokolldatensatz wird für jede Aktion erstellt, die einem Erkennungsstatus zugeordnet ist.

Hinweis: Das Discovery-Protokoll zeigt auch Fehler an, die während der Identifizierung auftreten, indem Protokolleinträge aus dem Protokoll der Identifizierungs-Engine übernommen werden. Siehe Überprüfen Sie die Ausführungsprotokolle Um weitere Informationen zur Identifizierungs-Engine und zu möglichen Fehlern zu erhalten.

Musterbasiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Protokolle für musterbasierte horizontale Erkennung enthalten die Informationen über Erkennungen, die mit Mustern durchgeführt wurden. Der Protokolldatensatz einer horizontalen Erkennung wird für eine komplette horizontale Erkennung erstellt, die die Ergebnisse aller im Muster angegebenen Vorgänge enthält.

Protokolle für horizontale Erkennung prüfen

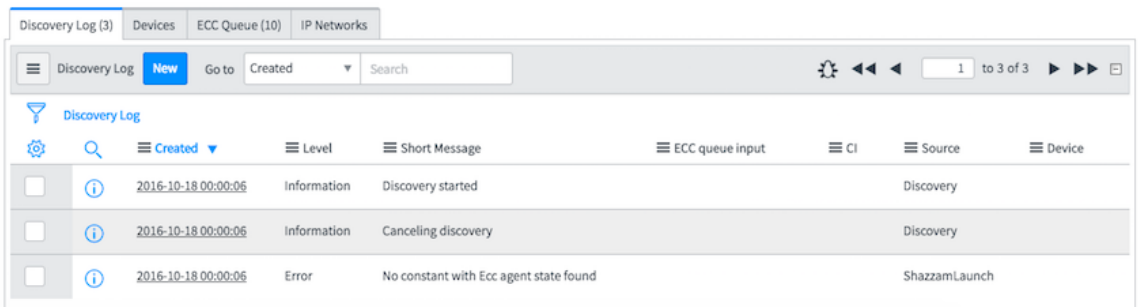
Greifen Sie auf die Protokolle zu, um den Erkennungsprozess zu verstehen und zu optimieren.

Vorbereitungen

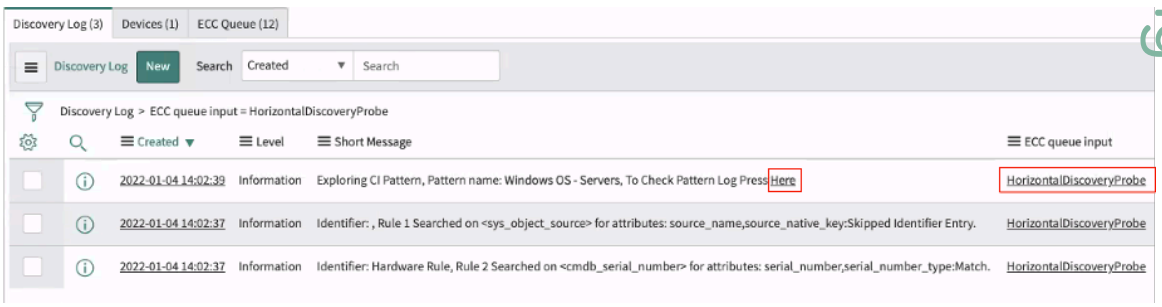
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Status**an.
2. Öffnen Sie einen Datensatz vom Typ Discovery-Status.
   In der zugehörigen Liste **Discovery-Protokoll** werden die Protokolle für die Probe-basierte Erkennung angezeigt. Weitere Informationen finden Sie unter Details zu Discovery-Protokollen.



3. **Wahlweise:** Suchen Sie die gewünschten Informationen zum relevanten Protokolleintrag:
   - Wählen Sie den Link in der Spalte **CI** aus, um den Datensatz für dieses CI zu öffnen.
   - Wählen Sie den Link in der Spalte **Erstellt** aus, um den Protokolldatensatz anzuzeigen.
   - Wählen Sie den Link der IP-Adresse in der Spalte **Gerät** aus, um die Protokolldatensätze für ein bestimmtes Gerät anzuzeigen.
4. Um Protokolle für die musterbasierte Erkennung anzuzeigen, klicken Sie bei einem Protokolleintrag mit dem Wert **HorizontalDiscoveryProbe** für **ECC-Warteschlangeneingabe** auf den Link **Hier**.

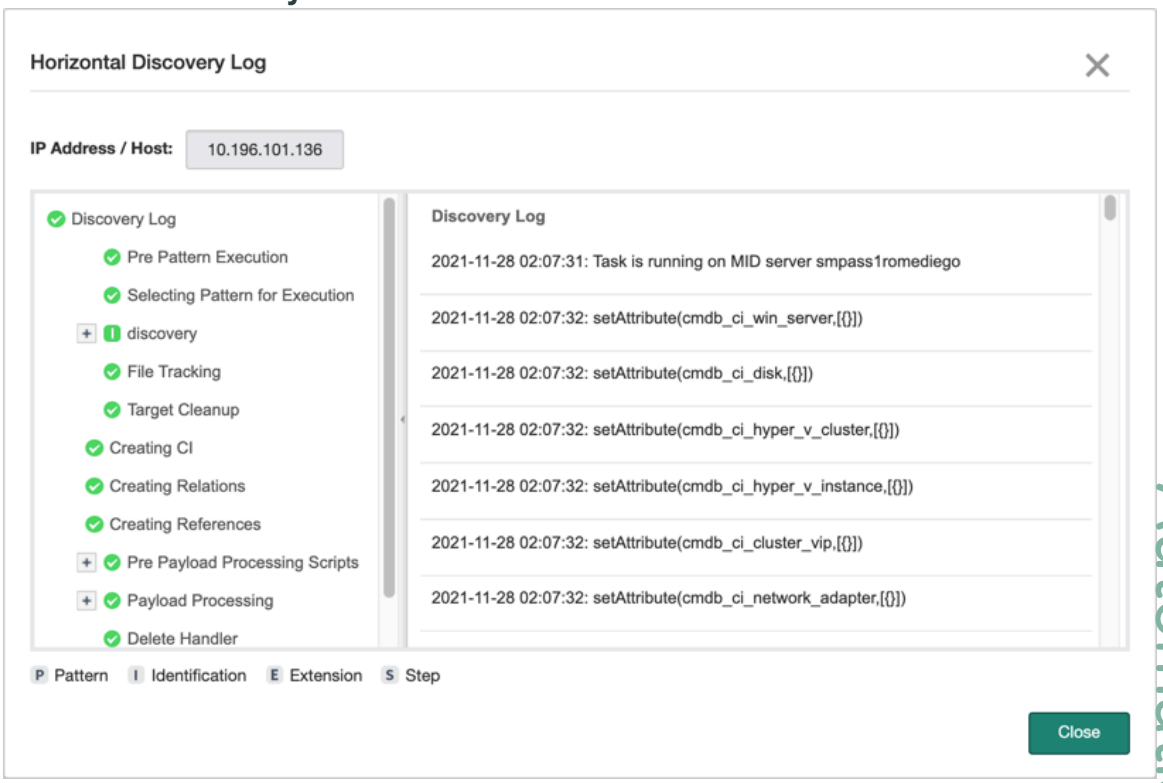


Das Fenster „Horizontales Discovery-Protokoll“ wird geöffnet und zeigt die Liste der musterbasierten Protokolleinträge an. Informationen zu protokollierten Erkennungsphasen finden Sie unter Details zu Discovery-Protokollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Horizontales Discovery-Protokoll



5. Wählen Sie ein Element in der linken Spalte aus, um weitere Informationen dazu in der rechten Spalte anzuzeigen.
6. **Wahlweise:** Um das Muster zu debuggen, wählen Sie den Namen des Identifizierungsabschnitts und dann die Schaltfläche **Debuggen** aus.
7. Um zum Protokolldatensatz zurückzukehren, wählen Sie **Schließen** aus.

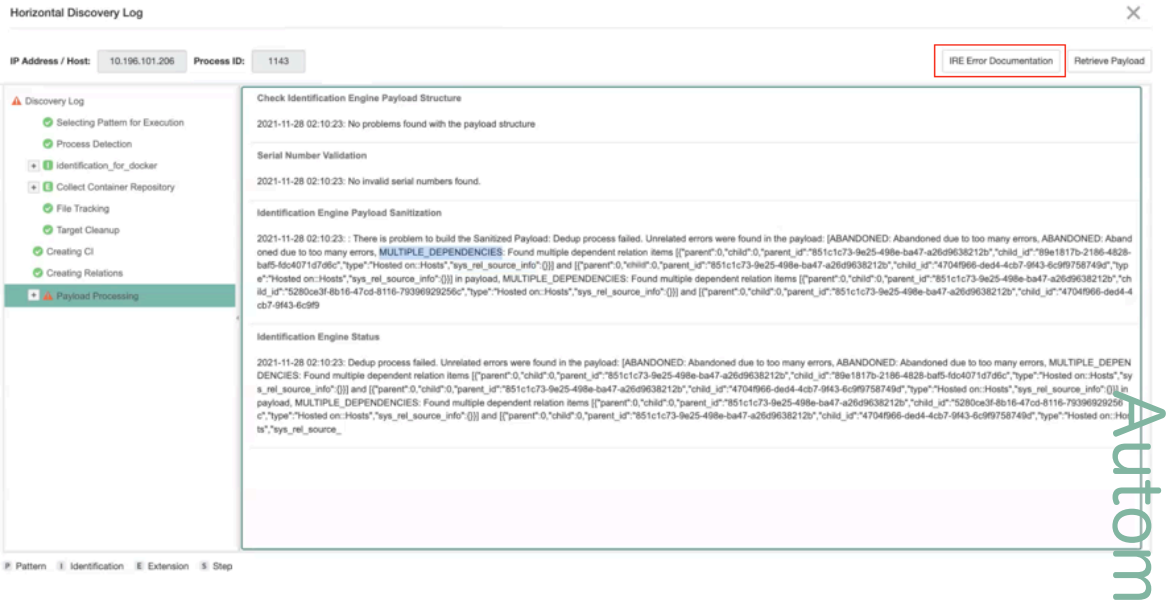
Nächste Maßnahme

- Um die musterbasierte Erkennung zu optimieren oder Probleme zu beheben, rufen Sie die Nutzlast wie unter KB0998923: Retrieve Payload Feature (Nutzlastfunktion abrufen) erläutert ab.
- Validiert Befehle, die in der musterbasierten Discovery verwendet werden, wenn einer der folgenden Fehler vorliegt:
  - Authentifizierungsproblem
  - Autorisierungs-/Berechtigungsproblem
  - Keine gültigen Anmeldeinformationen vorhanden
  - IP-Adresse nicht erreichbar von MID Server
  - Befehl mit falscher Syntax

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn bei der Verarbeitung der Nutzlast ein Fehler auftritt, wählen Sie die Schaltfläche **IRE-Fehlerdokumentation** aus, um mehr über den aufgetretenen Fehler der Identification and Reconciliation Engine (IRE) und dessen Behebung zu erfahren.



Zugehörige Informationen

Identification and Reconciliation Engine (IRE)

KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung

Change-Aufbewahrungszeit für Probe-basierte Discovery-Protokolle

Sie können konfigurieren, wie lange Protokolleinträge für die Probe-basierte horizontale Erkennung in Discovery aufbewahrt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden im Protokoll der Probe-basierten Erkennung Informationen 30 Tage bzw. 2.592.000 Sekunden lang aufbewahrt.

Prozedur

1. Öffnen Sie die Tabelle „Automatisch entleeren“, indem Sie `sys_auto_flush.list` in den Navigationsfilter eingeben.
2. Öffnen Sie den Datensatz **discovery_status**.
3. Ändern Sie den Wert im Feld **Alter in Sekunden**.
4. Damit die Änderung sofort wirksam wird, führen Sie den Tabellenbereinigungsauftrag in der Tabelle „Zeitplan“ [sys_trigger] aus.
5. Klicken Sie auf **Aktualisieren**.

Discovery Befehle für Probes und Muster

Discovery Befehle werden sowohl für die Probe- als auch für die musterbasierte Discovery verwendet, um auf Konfigurationselemente (Configuration Items, CIs) in Ihrer Umgebung zuzugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Informationen zu Service-Mapping Befehle, siehe Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Probe-basierte Discovery

Discovery Führt während der probenbasierten horizontalen Discovery verschiedene Arten von Befehlen aus. Einige dieser Befehle erfordern erhöhte Berechtigungen zur Ausführung.

Ressourcen für Informationen zu Befehlen und Berechtigungen für die probenbasierte Discovery

Befehl/Berechtigung	Ressource
SSH-Befehle, die einen privilegierten Anwender erfordern	SSH-Befehle, die während der probenbasierten Discovery einen privilegierten Anwender erfordern
SSH-Befehle, die keinen privilegierten Anwender erfordern	SSH-Befehle, die während der probenbasierten Discovery keinen privilegierten Anwender erfordern
Windows Befehle und Berechtigungen	Windows Probes und Berechtigungen
Zusätzliche Berechtigungen	Berechtigungen für Discovery-Probes

Musterbasierte Erkennung

Discovery Führt während der musterbasierten horizontalen Discovery verschiedene Arten von Befehlen aus. Einige dieser Befehle erfordern erhöhte Berechtigungen zur Ausführung. Für die musterbasierte Discovery können Sie alle Befehle anzeigen, die von einer bestimmten Infrastruktur oder einem bestimmten Anwendungsmuster auf der verwendet werden ServiceNow AI Platform Und validieren Sie sie, bevor Sie die Discovery ausführen. Für Cloud-Ressourcenmuster können Sie alle erforderlichen Berechtigungen in anzeigen Cloud-Discovery Mustertabelle.

Ressourcen für Informationen zum Anzeigen und Validieren musterbasierter Discovery-Befehle und -Berechtigungen

Aktion	Ressource
Zeigen Sie Befehle an, die von Infrastruktur- und Anwendungsmustern verwendet werden	• Zeigen Sie Befehle an, die in der musterbasierten Discovery verwendet werden • Befehlslistenformular für musterbasierte Discovery
Validiert Befehle, die von Infrastruktur- und Anwendungsmustern verwendet werden	• Validiert Befehle, die in der musterbasierten Discovery verwendet werden • Formular „Befehlsvalidierungsaufgaben“ für musterbasierte Discovery
Zeigen Sie Berechtigungen an, die für Cloud-Ressourcenmuster erforderlich sind	Cloud-Discovery Mustertabelle

Zugehörige Informationen

KB1123625: Tool zur Befehlsvalidierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Befehle an, die in der musterbasierten Discovery verwendet werden

Zeigen Sie alle Befehle an, die für ein Infrastruktur- oder Anwendungsmuster erforderlich sind, um sicherzustellen, dass Sie über ausreichende Berechtigungen zum Ausführen der Discovery verfügen.

Vorbereitungen

- Stellen Sie sicher, dass die folgenden Anwendungen installiert wurden:
  - Musterdesigner-Erweiterungen (sn_itom_pde)
  - Muster für Discovery und Service-Mapping (sn_itom_pattern)
- Wenn Sie Befehle zum ersten Mal anzeigen, haben Sie aktualisiert Muster für Discovery und Service-Mapping, Oder haben Sie ein Muster angepasst, aktualisieren Sie die Befehlsliste, indem Sie zu navigieren **Alle** > **Musterdesigner** > **Tool zur Befehlsvalidierung** > **Befehlsliste** Und auswählen **Aktualisieren Sie Die Befehlsliste** .

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. In **Name** Feld, suchen Sie nach dem relevanten Muster.
3. Wählen Sie den Namen des Musters aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie ihn aus **Listenmusterbefehle** .

Ergebnis

Sie werden zum Formular „Befehlsliste“ weitergeleitet, das nach dem ausgewählten Muster gefiltert ist.

Weitere Informationen zu den Formularfeldern der Befehlsliste finden Sie unter Befehlslistenformular für musterbasierte Discovery.

Zugehörige Informationen

Discovery Befehle für Probes und Muster

Validiert Befehle, die in der musterbasierten Discovery verwendet werden

Validiert Befehle, die in der musterbasierten Discovery verwendet werden

Validieren Sie Musterbefehle, um sich zu vergewissern, dass sie vom MID-Server erfolgreich ausgeführt werden können. Normalerweise können Befehle fehlschlagen, wenn Sie die Anmeldeinformationen nicht konfiguriert haben, die zum Ausführen dieser Befehle auf Ihrem erforderlich sind ServiceNow Instanz. Ein weiterer häufiger Grund für Befehlsfehler besteht darin, dass die für die Discovery verwendeten IP-Adressen nicht erreichbar sind.

Vorbereitungen

- Stellen Sie sicher, dass Sie über die folgenden Anwendungen verfügen:
  - Musterdesigner-Erweiterungen (sn_itom_pde)
  - Muster für Discovery und Service-Mapping (sn_itom_pattern)
- Überprüfen Sie das Protokoll für horizontale Erkennung basierend auf Mustern, wie in Protokolle für horizontale Erkennung prüfen beschrieben.
- Wenn Sie Befehle zum ersten Mal anzeigen, haben Sie aktualisiert Muster für Discovery und Service-Mapping, Oder haben Sie ein Muster angepasst, aktualisieren Sie die Befehlsliste,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

indem Sie zu navigieren **Alle** > **Musterdesigner** > **Tool zur Befehlsvalidierung** > **Befehlsliste** Und auswählen **Aktualisieren Sie Die Befehlsliste** .

- Um Anmeldeinformationen in einem IP-Bereich oder IP-Netzwerk testen zu können, installieren Sie die Skripteinbindung ParseIPRanges, die dem KB-Artikel KB1123625: Command Validation Tool (Befehlsvalidierungs-Tool) angefügt ist.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Unabhängig davon, ob Sie die Erkennung mithilfe von Mustern oder Probes durchführen, werden vom MID-Server Befehle für den Zugriff auf Konfigurationselemente (Configuration Items, CIs) ausgeführt. Die meisten Befehle erfordern Anmeldeinformationen, damit sie ausgeführt werden können. Darüber hinaus müssen Sie die Rolle eines Benutzers mit erweiterten Rechten annehmen, um einige dieser Befehle auszuführen. Wenn die erforderlichen Anmeldeinformationen fehlen, schlägt die Discovery fehl.

Für die musterbasierte Discovery können Sie alle Befehle, die von einem bestimmten Muster verwendet werden, gleichzeitig validieren.

Sie können Discovery-Befehle auch validieren, um zu überprüfen, ob die IP-Adressen, die Sie für die Discovery verwenden, erreichbar sind. Manchmal sind IP-Adressen falsch, oder die Server, von denen diese IP-Adressen verwendet werden, sind ausgefallen.

Wenn Sie Befehle validieren, die anwendbare Anmeldeinformationen enthalten, überprüft das Tool zur Befehlsvalidierung Verbindungen und Anmeldeinformationen Modul und verwendet relevante anwendbare Anmeldeinformationen, die dort konfiguriert sind.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Tool zur Befehlsvalidierung** > **Neu erstellen**an.
2. **Wahlweise:** Wählen Sie aus, um alle von einem Muster verwendeten Befehle zu validieren **Validiert Alle Musterbefehle** .
3. Füllen Sie die Felder wie in Formular „Befehlsvalidierungsaufgaben“ für musterbasierte Discovery beschrieben aus.
4. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
5. **Wahlweise:** Wenn die von Ihnen ausgewählten Befehle temporäre Variablen enthalten, fügen Sie die Werte für diese Variablen hinzu, bevor Sie diese Befehle validieren.

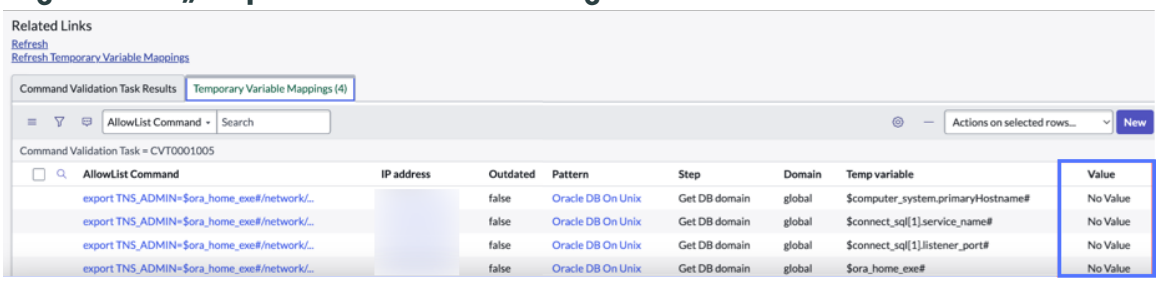
   a. Wählen Sie Aus **Aktualisieren Sie Temporäre Variablenzuordnungen** Unter **Zugehörige Links** .

   Das Tool erstellt eine Liste aller temporären Variablen für die ausgewählten Befehle und IPs.

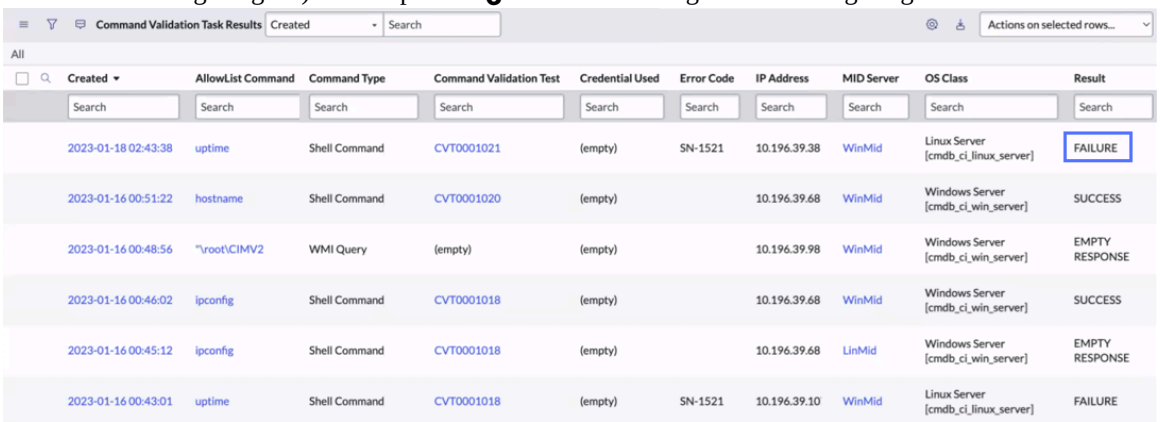
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie aus **Zuordnungen Temporärer Variablen** Registerkarte und geben Sie die Werte für die temporären Variablen ein.

Registerkarte „temporäre Variablenzuordnungen“



6. Wählen Sie **Run Command Validation** (Befehlsvalidierung ausführen) aus.
7. Überprüfen Sie, ob im Abschnitt **Command Validation Task Results** (Ergebnisse der Befehlsvalidierungsaufgabe) in der Spalte **Ergebnis** der Eintrag **FEHLER** angezeigt wird.

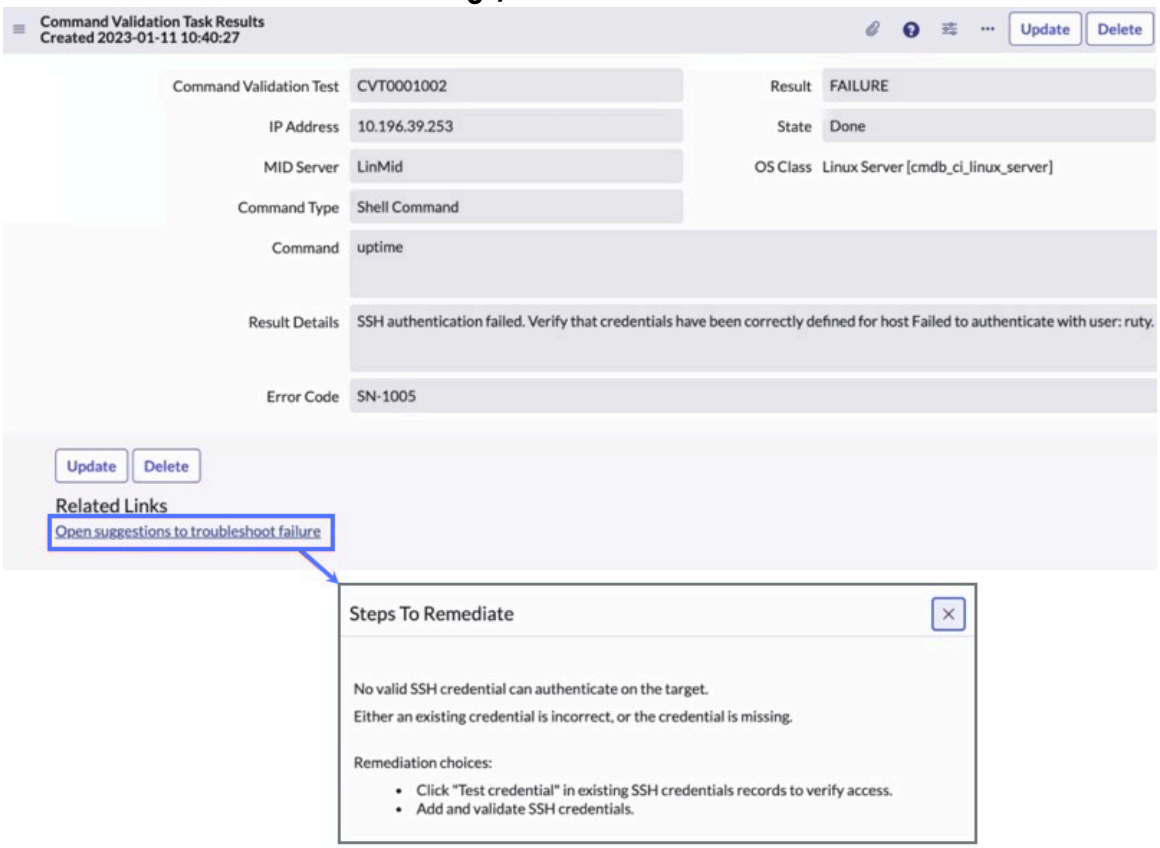


8. Wählen Sie den Link im aus **Test Der Befehlsvalidierung** Spalte.
9. Überprüfen Sie die Beschreibung im Feld **Ergebnisdetails**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

1. Wählen Sie aus **Öffnen Sie Vorschläge, um einen Fehler zu beheben** Link.



2. Befolgen Sie die Anweisungen im **Schritte zur Korrektur** Fenster.

Zugehörige Informationen

Discovery Befehle für Probes und Muster

Erste Schritte mit Anmeldeinformationen

Befehlslistenformular für musterbasierte Discovery

Erweiterte Discovery-Konfiguration

Sie können mehrere zusätzliche Discovery-Komponenten konfigurieren, zum Beispiel Application Dependency Mapping, die ECC-Warteschlange und Erweiterungen für den MID Server.

gMSA-Konfiguration für Discovery

Gruppenverwaltete Servicekonten (gMSAs) sind verwaltete Domänenkonten, die Sie zum Absichern von Services verwenden. gMSAs können für Discovery ohne Anmeldeinformationen verwendet werden.

Vorteile

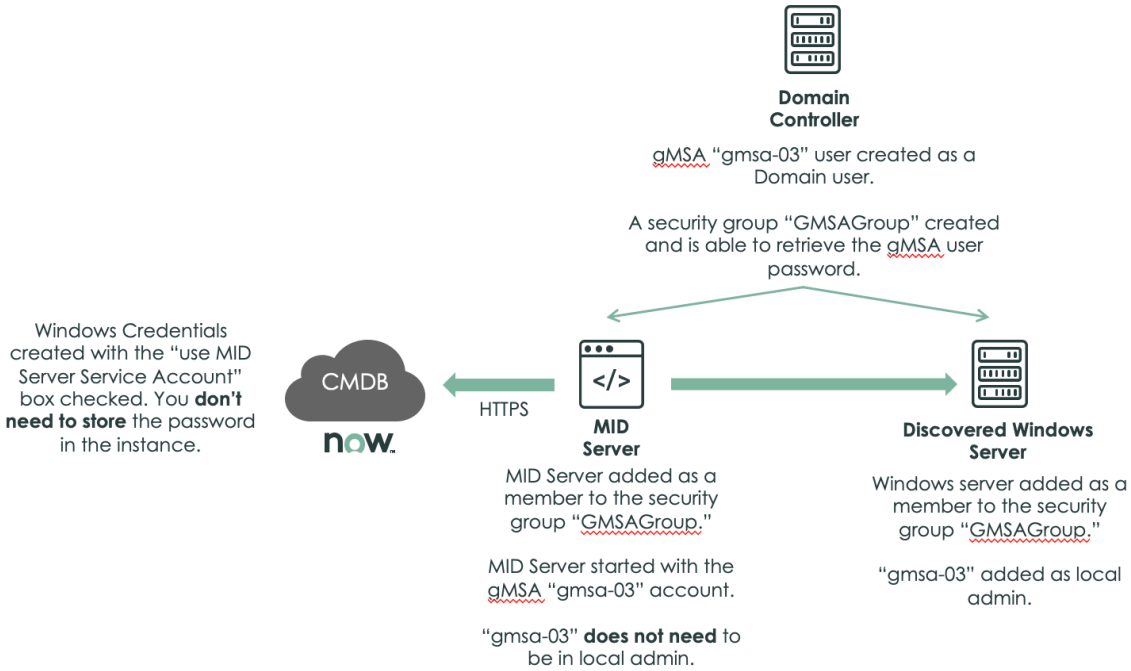
Nachdem Sie Discovery für die Verwendung von gMSA konfiguriert haben, wird die Passwortverwaltung für dieses Konto vom Windows-Betriebssystem verarbeitet. Daher können Sie Windows Discovery ausführen, ohne die Anmeldeinformationen für die ServiceNow-Instanz freizugeben. Es ergeben sich unter anderem die folgenden Vorteile:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie müssen gMSA-Passwörter nicht selbst verwalten.
- Sie können den Zyklus der gMSA-Passwortrotation für eine bessere Sicherheit auswählen.
- Sie müssen das Passwort nicht in der ServiceNow-Instanz speichern.
- Der gMSA-Benutzer muss nicht Mitglied einer Domänenadministratorgruppe sein.
- Der als MID-Server-Servicekonto verwendete gMSA-Benutzer muss sich nicht in der lokalen Administratorgruppe des MID-Server s befinden.

Allgemeine Ansicht von Discovery mit gMSA



gMSA für Discovery konfigurieren

Dient zur Verwendung von gMSAs ohne Anmeldeinformationen Discovery

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie in der PowerShell-Befehlszeile mit den folgenden Befehlen einen KDS-Stammschlüssel auf einem Domänencontroller:

   ```
   Add-KdsRootKey -EffectiveImmediately
   ```

   oder

   ```
   Add-KdsRootKey –EffectiveTime ((Get-Date).AddHours(-10))
   ```

2. Richten Sie Ihr gMSA und Ihre Sicherheitsgruppen mit den Informationen zu gruppenverwalteten Servicekonten unter https://docs.microsoft.com ein.
3. Starten Sie MID-Server Mit dem GMSA-Account gemäß den Anweisungen zur Verwendung von GMSA: Installieren Sie einen MID-Server unter Windows

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie Windows-Anmeldeinformationen für die Instanz und aktivieren Sie das Kontrollkästchen **MID Server-Service-Account verwenden**.
5. Starten Sie Discovery auf dem Server, auf dem der MID-Server gehostet wird, und auf einem anderen Computer.

Erkennung ohne Anmeldeinformationen mit Nmap

Wenn die Instanz aufgrund eines Authentifizierungsfehlers ein Konfigurationselement (CI) nicht identifiziert, kann Discovery oder Service Mapping ausgewählte Nmap-Befehle (Network Mapper) mit einem MID Server ausführen, um ohne Anmeldeinformationen einige Basisinformationen über das CI zu sammeln.

Ein MID-Server-Administrator kann dies Installieren Sie Nmap Auf einzelnen MID-Servern, die auf einem Windows-Host ausgeführt werden. Diese MID Server können dann einige Basisinformationen über CIs in Ihrem Netzwerk erkennen, wenn die normale Authentifizierung fehlschlägt.

Wichtig: Selbst gehostete Kunden, deren Netzwerksicherheit keine Downloads von install.service-now.com zulässt, muss Nmap manuell auf ihrem System installieren und konfigurieren. Beziehen Sie sich auf Installieren von Nmap auf einem selbst gehosteten System für Anweisungen.

Durch eine anmeldedatenlose Erkennung können Host- und Anwendungs-CIs erstellt und geändert werden, wenn Anmeldeinformationen fehlen oder falsch konfiguriert sind. Wenn eine auf Anmeldeinformationen basierende Erkennung erfolgreich durchgeführt wird, nachdem Nmap ein CI erstellt hat, gleicht das System die Informationen ab, die für die einzelnen Erkennungstypen gesammelt wurden.

Von Nmap erkennbare Elemente

Die während einer anmeldedatenlosen Erkennung ausgeführten Nmap-Befehle bieten folgende Möglichkeiten:

- Führen Sie eine umgekehrte DNS-Namensauflösung durch, um den Host anhand der IPv4-Adresse zu identifizieren.
- Geben Sie die MAC-Adresse des Hosts zurück, wenn sich dieser im selben Subnetz befindet wie der Host, der den Nmap-Befehl ausführt.
- Erkennen Sie auf einem Zielhost installierte Anwendungen.
- Erkennen Sie das Betriebssystem eines Zielhosts und die BS-Version.

Hinweis:

Die anmeldedatenlose Erkennung klassifiziert Router und Switches als Hardware. Dadurch werden keine CIs speziell für sie erstellt oder aktualisiert.

Die Erkennung ohne Anmeldeinformationen sollte nur in bekannten Subnetzen verwendet werden, in denen Anmeldeinformationen nicht praktikabel sind, und sollte nicht langfristig verwendet werden.

Nmap-Discovery-Scans ohne Anmeldeinformationen auf Cloud-Computing-Plattformen

Es stellt in vielen Fällen einen Verstoß gegen die Nutzungsbedingungen dar, Nmap-Scans zu oder von einer beliebigen Ressource innerhalb eines Cloud-Computing-Services wie Amazon Web Service, Microsoft Azure, IBM Cloud oder Google Cloud Platform auszuführen. Die Amazon Web Service(AWS)-Umgebung beispielsweise ist streng reguliert und erfordert die Erlaubnis von AWS über das Formular AWS-Schwachstellen-/Penetrationstestanforderung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht autorisierte Tests mit AWS-Services oder AWS-eigenen Ressourcen sind nicht zulässig. Aus diesem Grund ist eine Erkennung ohne Anmeldeinformationen in einer Cloud-Computing-Serviceumgebung nicht angezeigt. Wenn ein Verstoß gegen die entsprechenden Richtlinien vorliegt, kann dies zur Beendigung des Services führen. Bitte wenden Sie sich an Ihren Platform Service Provider, um Informationen über Einschränkungen oder Berechtigungsanforderungen für die Ausführung von Nmap zu erhalten.

Mit Nmap installierte Komponenten

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based], das die Nmap-Funktionalität bereitstellt, wird automatisch aktiviert, wenn entweder Discovery oder Service-Mapping aktiv ist. Das Plugin „Discovery - IP Based“ stellt die folgenden Nmap-Komponenten bereit:

Komponente	Beschreibung
Systemeigenschaft	Die Eigenschaft **mid.discovery.credentialless.enable** aktiviert oder deaktiviert Nmap für alle MID Server, auf denen Nmap installiert ist und die mit der Instanz verbunden sind. Diese Eigenschaft wird mit dem Plugin „Discovery“ installiert und ist standardmäßig aktiviert. Sie kann von einem Systemadministrator konfiguriert werden.
MID Server-Eigenschaften	Die folgenden Eigenschaften aus der Tabelle „MID Server-Eigenschaft“ [ecc_agent_property] sollten nicht konfiguriert werden: • **mid.nmap.version**: Version von Nmap, die auf MID Servern in Ihrer Umgebung installiert ist. Dieses Feld wird im Formular „MID Server“ [ecc_agent] angezeigt, nachdem Nmap installiert wurde. • **nmap.safe.scripts**: Definiert die Liste der Nmap-Skripts, die als sicher für die Verwendung während der Ausführung der Nmap-Phase zur Anwendungsversionserkennung (Befehlsoption -sV) klassifiziert sind • **nmap.npcap.version**: Die Version von Npcap, die mit Nmap installiert wird. Das Nmap-Installationsprogramm kann nur Upgrades von vorhandenen Npcap-Installationen durchführen, auf die es stößt.
Felder	• **Discovery-Port ohne Anmeldeinformationen [cl_port]**: Optionales Feld in der Anwendungstabelle [cmdb_ci_appl], in dem die Nummer eines Ports angezeigt wird, der durch die anmeldedatenlose Erkennung gescannt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	wurde. Anhand dieser Portnummer wird bestimmt, ob die CMDB das CI für eine von Nmap zurückgegebene Anwendung enthält oder ob ein neues CI erstellt werden muss. • **Discovery-Quelle [discovery_source]**: Optionales Feld in der Tabelle „Konfigurationselement“ [cmdb_ci], dem die Option **CredentiallessDiscovery** hinzugefügt wird. Diese Option zeigt an, dass die anmeldedatenlose Erkennung zum Erstellen eines CI verwendet wurde.
Nmap-Fähigkeit für MID Server	Die **Nmap** MID-Server-Fähigkeiten Wird dem MID-Server hinzugefügt, wenn Nmap installiert wird, und wird automatisch entfernt, wenn Nmap deinstalliert wird. Nur MID Server mit dieser Fähigkeit können anmeldedatenlose Erkennungen ausführen. Ein Systemadministrator kann diese Fähigkeit nicht manuell hinzufügen oder entfernen. Selbst gehostete Kunden mit der Wartungsrolle können die Nmap-Fähigkeit ändern oder löschen, *sollten dies jedoch unterlassen*. Service-Mapping überprüft nicht, ob vorhanden ist **Nmap** Fähigkeit und wählt den MID-Server nur basierend auf der IP-Adresse aus. Um sicherzustellen, dass Service-Mapping keinen MID-Server ohne auswählt **Nmap** Fähigkeit, installieren Sie Nmap auf allen MID-Servern, die den IP-Adressbereichen zugewiesen sind, für die Discovery ohne Anmeldeinformationen verfügbar sein soll. Wenn Service-Mapping einen MID-Server für Discovery ohne Anmeldeinformationen auswählt, der keine Nmap-Fähigkeiten hat, wird diese Fehlermeldung in der Zuordnung am Standort des erkannten CI angezeigt: `Nmap ist nicht auf dem MID-Server installiert. Stellen Sie sicher, dass alle MIDs, die für die Verarbeitung der ausgewählten IP-Adresse konfiguriert sind, über eine Nmap-Fähigkeit verfügen. Nmap-Stammverzeichnispfad ist nicht vorhanden: <path>` **Hinweis:** Die MID Server-Fähigkeit **ALLE** schließt die **Nmap**-Fähigkeit nicht ein.
Npcap	Npcap ist die Paketerfassungsbibliothek von Nmap für Windows. Mit Npcap kann Nmap schnell Port-Scans durchführen und die Familie des Betriebssystems identifizieren, das auf dem Ziel ausgeführt wird. Pro MID Server-Host wird nur eine Kopie von Npcap installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	Da Npcap von anderen Anwendungen verwendet werden kann, wird Npcap bei der Deinstallation von Nmap nicht automatisch deinstalliert. Sie müssen Npcap manuell deinstallieren, nachdem Sie sich davon überzeugt haben, dass keine weiteren Abhängigkeiten vorhanden sind.
Muster	• **Credentialless Discovery Network Device**: Scannt eine Host-IP-Adresse mit einem Nmap-Befehl, um den Host zu identifizieren. Dieses Muster startet das Skript **Credentialless Discovery Network Device – PreLaunch**, um die Liste der zu untersuchenden Ports aus der IP-Service-Tabelle [cmdb_ip_service] abzurufen. Ändern Sie dieses Skript nicht. • **Credentialless Discovery Application**: Scannt einen Port an einer IP-Adresse mithilfe eines Nmap-Befehls, um den Anwendungsservice zu identifizieren, der diesen Port aktiv abhört. Service Mapping startet dieses Muster, wenn alle auf Anmeldeinformationen basierten Portklassifizierungsschritte fehlschlagen. Discovery erstellt ein CI in der Anwendungstabelle [cmdb_ci_appl], wenn der Port geöffnet ist und den Service anhand des Namens und des Produkts identifizieren kann. Wenn der Service auf keinen der Scan-Versuche reagiert, konsultiert Nmap die Registrierung von Nmap-Services und ermittelt, welcher Service wahrscheinlich auf diesem Port ausgeführt wird. Wenn Nmap erraten muss, welche Anwendung auf einem gescannten Port ausgeführt wird, erstellt das Muster „Credentialless Discovery Application“ kein Anwendungs-CI und aktualisiert auch kein vorhandenes CI.
MID Server-Skripteinbindungen	• **SetCredentialLessDeviceClassName**: Bestimmt, welches Host-CI nach erfolgreicher Ausführung des Nmap-Befehls erstellt oder aktualisiert wird. *Ändern Sie dieses Skript nicht.* • **CredentialLessApplicationClassNameMapper**: Ordnet das Serviceprodukt, den Servicenamen und zusätzliche Serviceinformationen, die von Nmap für den gescannten Port bereitgestellt werden, einer unterstützten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	Anwendungstabelle in der Instanz zu. Systemadministratoren können dieses Skript ändern. • **SetCredentialLessApplicationClassName**: Stellt sicher, dass das Skript `CredentialLessApplicationClassNameMapper` nur einmal aufgerufen wird. *Ändern Sie dieses Skript nicht.*
System-Skripteinbindung	Die Skripteinbindung `CredentiallessDiscoveryAjax` wird für die Instanz ausgeführt und erledigt die Installation und Deinstallation von Nmap auf Windows MID Servern, die über UI-Aktionen im Formular ausgeführt werden. Ändern Sie dieses Skript nicht.

Hosterkennung ohne Anmeldeinformationen

Eine Hosterkennung ohne Anmeldeinformationen findet statt, wenn ein gescannter Host zwar in Betrieb, aber inaktiv ist oder wenn alle konfigurierten, auf Anmeldeinformationen basierten Klassifizierungs-Probes fehlgeschlagen sind.

Vorgehensweise zum Starten des Hosterkennungsmusters

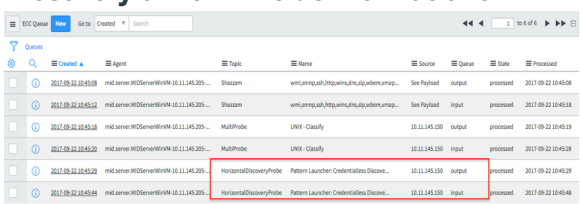
Wenn die Shazzam-Probe einen Host scannt, der zwar in Betrieb, aber inaktiv ist, und wenn auf Anmeldeinformationen basierte Klassifizierungs-Probes fehlschlagen, startet die horizontale Erkennung das Muster „Credentialless Discovery Network Device“, um Hostinformationen zu erfassen. Wenn für den gescannten Host kein CI definiert ist, startet Service Mapping die Probe HorizontalDiscoveryProbe, die wiederum das Muster Credentialless Discovery Network Device startet. Dieses Muster versucht, ein neues CI zu erstellen, wenn für den gescannten Host noch kein CI existiert, oder ein vorhandenes CI in der Hardwaretabelle [cmdb_ci_hardware] zu aktualisieren.

Wichtig: Damit das Muster Credentialless Discovery Network Device gestartet werden kann, muss die Systemeigenschaft `mid.discovery.credentialless.enable` auf **true** festgelegt sein. Zum Deaktivieren legen Sie diese Eigenschaft auf **false** fest.

ECC-Warteschlangeneinträge

Das System erstellt die folgenden Einträge in der ECC-Warteschlange, während die HorizontalDiscoveryProbe ausgeführt wird.

Discovery ohne Anmeldeinformationen

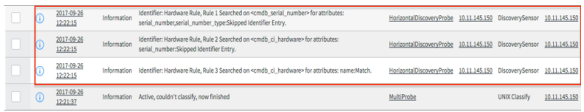


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollnachrichten

Diese Protokollnachrichten werden während der Ausführung der HorizontalDiscoveryProbe veröffentlicht.

Hostbezeichner ohne Anmeldeinformationen

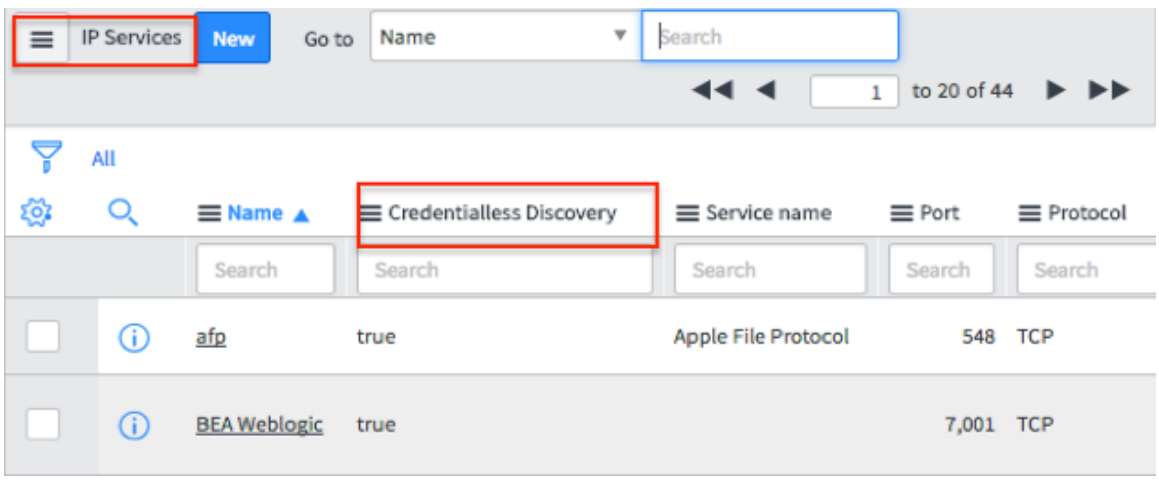


Nmap-Befehl

Der auf dem MID Server ausgeführte Nmap-Befehl bestimmt, ob der Host in Betrieb ist. Unter Verwendung der IP-Adresse und einer Liste von Ports, die durch das Muster an Nmap übergeben werden, führt Nmap eine umgekehrte DNS-Namensauflösung durch, um den der IP-Adresse zugeordneten Hostnamen zu identifizieren. Wenn mehrere Hostnamen konfiguriert sind, wird der erste von Nmap zurückgegebene Name verwendet. Wenn kein Hostname konfiguriert ist, wird zum Erstellen des Host-CI die IP-Adresse des Remotehosts verwendet. Die in der Nmap-Installation enthaltene Npcap-Paketerfassungsbibliothek identifiziert die Familie des Hostbetriebssystems. Wenn sich der gescannte Host im selben Subnetz wie befindet Windows MID-Server Host, der Nmap ausführt, wird die MAC-Adresse des Remote-Hosts zurückgegeben.

Hinweis: Die Liste der Ports, für deren Scan Nmap während der Hosterkennung ohne Anmeldeinformationen konfiguriert ist, wird in der Tabelle „IP-Service“ [cmdb_ip_service] gespeichert, die bearbeitet werden kann. Standardmäßig sind alle Ports zum Scannen verfügbar. Um die Verwendung eines beliebigen Ports für einen Nmap-Scan zu blockieren, legen Sie den Wert in der Spalte **Discovery ohne Berechtigung [cI_discovery]** auf **false** fest.

Portliste ohne Anmeldeinformationen



Host-CIs erstellen oder aktualisieren

Nach der erfolgreichen Ausführung des Musters „Credentialless Discovery Network Device“ wird das MID Server-Skript `SetCredentialLessDeviceClassName` ausgeführt, um die Betriebssystemfamilie des erkannten Hosts zu identifizieren. Die Systemklasse des Host-CI basiert auf der Betriebssystemfamilie, die von Nmap zurückgegeben wird. Wenn die Betriebssystemfamilie mit einem der sechs unterstützten Serverbetriebssysteme übereinstimmt, verwendet das System eine Serverklasse, die von der Basisklasse „Hardware“ [cmdb_ci_Hardware] abgeleitet ist, z. B. Linux Server [cmdb_ci_linux_Server]. Wenn keine Übereinstimmung gefunden wird, verwendet das System die Basisklasse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn das Problem mit den Anmeldeinformationen gelöst ist und Discovery erneut ausgeführt wird, aktualisiert die Instanz das von der anmeldedatenlosen Erkennung erstellte Host-CI mit der Seriennummer, dem Hostnamen und der Systemklasse, die von der auf Anmeldeinformationen basierenden Erkennung bereitgestellt werden.

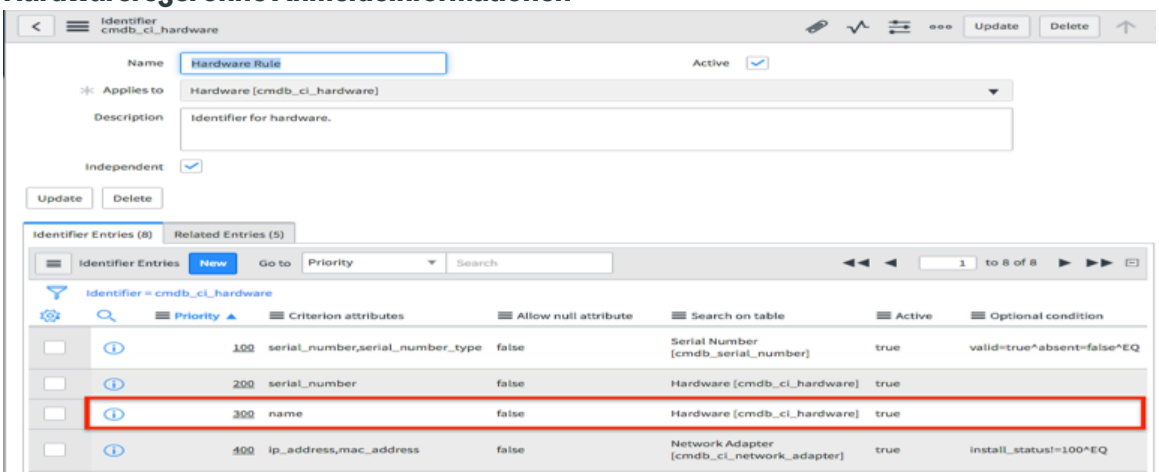
Unterstützte BS-Familien

BS-Familie	CI-Tabelle
AIX	cmdb_ci_aix_server
HP-UX	cmdb_ci_hpux_server
Linux	cmdb_ci_linux_server
Solaris	cmdb_ci_solaris_server
OS X oder iOS	cmdb_ci_osx_server
Windows	cmdb_ci_win_server
Nicht definiert	cmdb_ci_hardware

Hardwareidentifizierung

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based] fügt der Hardwareregel für die Basistabelle „Hardware“ [cmdb_ci_hardware] einen Bezeichner hinzu, der dem **Namen** des Host-CI für Nmap-Scans entspricht. Die Hardwareregel wird sowohl von der auf Anmeldeinformationen basierenden als auch der anmeldedatenlosen Erkennung verwendet.

Hardwareregel ohne Anmeldeinformationen



Anwendungserkennung ohne Anmeldeinformationen

Die Anwendungserkennung ohne Anmeldeinformationen versucht, einen Anwendungsservice zu identifizieren, der einen bestimmten Port an einer bestimmten IP-Adresse aktiv abhört.

Muster zur Anwendungserkennung

Service Mapping startet das Muster „Credentialless Discovery Application“, wenn alle auf Anmeldeinformationen basierten Portklassifizierungsschritte fehlschlagen. Das Muster führt auf einem Windows-MID Server mit installiertem Nmap einen Nmap-Befehl aus, der so konfiguriert ist, dass er eine Anwendungs-/Versionserkennung für eine bestimmte IP-Adresse und einen bestimmten Port des Remotehosts durchführt. Wenn der von Nmap gescannte Port offen ist, führt das Muster die MID Server-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skripteinbindung `CredentialLessApplicationClassNameMapper` aus, die das Serviceprodukt, den Servicenamen und zusätzliche Informationen zuordnet, die von Nmap für eine unterstützte ServiceNow-Anwendungstabelle bereitgestellt werden. Wenn das Skript das zurückgegebene Produkt einer entsprechenden Tabelle zuordnen kann, die von der Basisanwendungstabelle [cmdb_ci_appl] abgeleitet ist, übergibt das Skript diese Informationen an das Muster. Das Muster übergibt die Übereinstimmung an den Discovery-Bezeichner, um gegebenenfalls ein CI erstellen oder abgleichen zu können. Wenn die von Nmap zurückgegebenen Informationen mit keiner abgeleiteten Tabelle übereinstimmen, verwendet die Instanz die Basisanwendungstabelle [cmdb_ci_appl], um das CI zu erstellen.

Wichtig: Damit das Muster „Credentialless Discovery Application“ gestartet werden kann, muss die Systemeigenschaft `mid.discovery.credentialless.enable` auf **true** festgelegt sein. Zum Deaktivieren legen Sie diese Eigenschaft auf **false** fest.

Beispiel-Scan

Die folgenden Informationen wurden vom Port-Scan einer Nmap-Anwendungs-/Versionserkennung auf einem Linux-Testsystem zurückgegeben. Sie veranschaulichen den Typ der Anwendungsdaten, die von Nmap-Scans zurückgegeben werden können.

Informationen	Port
Portstatus	open
Servicename	ssh
Serviceprodukt	OpenSSH
Zusätzliche Serviceinformationen	Protocol 2.0

Standardmäßige Anwendungszuordnungen

Die MID Server-Skripteinbindung `CredentialLessApplicationClassNameMapper` ist mit einer Teilmenge der gängigsten Anwendungstabellen konfiguriert, die für Discovery und Service Mapping verfügbar sind. Ein Benutzer mit der Rolle agent_admin kann diese Skripteinbindung bearbeiten, um zusätzliche CI-Tabellen hinzuzufügen, die von der Anwendungserkennung ohne Anmeldeinformationen zur Zuordnung zu einer abgeleiteten CI-Anwendungsklasse verwendet werden kann.

In dieser Tabelle werden Beispiele für geschlossene Übereinstimmungen angezeigt, die von Nmap auf einem Testsystem zurückgegeben werden, das CMDB-Identifizierung und -Abgleich Konnte in definierte Produkte aufgelöst werden. In vielen Fällen war der von Nmap zurückgegebene Servicename nicht erforderlich, um eine Übereinstimmung zu bestimmen. Stattdessen waren in der Tabelle aufgeführte Servicenamen erforderlich, um eine Übereinstimmung zu bestimmen.

Von Nmap zurückgegebene Produkte, die nicht in definierte Discovery-Produkte aufgelöst werden können, haben das folgende Namensformat: ***<serviceProduct>:<serviceExtrainfo>:<serviceName>***. Wenn ein beliebiger Wert in dieser Zeichenfolge NULL ist, wird er aus dem Namen gelöscht.

- **serviceProduct**: Von Nmap zurückgegebene Serviceproduktinformationen
- **serviceExtrainfo**: Alle zusätzlichen Informationen, die Nmap über die Anwendung zurückgibt und die zur Identifizierung der Anwendung beitragen könnten, zum Beispiel Protokollinformationen
- **serviceName**: Name des installierten Service oder Daemon des Produkts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für gute Entsprechungen, die gelöst wurden

Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
Serviceprodukt	**Servicename**	**Zusätzliche Serviceinformatione**	**Erkanntes Produkt**	**CI-Anwendungstabelle**
Apache Tomcat/ Coyote JSP Engine 1.1	N/V	NULL	Tomcat	cmdb_ci_app_server_tomcat
Apache httpd 2.2.10 ((Linux/SUSE))	N/V	NULL	Apache-Webserver	cmdb_ci_apache_web_server
IBM HTTP Server	N/V	Abgeleitet von Apache	Apache-Webserver	cmdb_ci_apache_web_server
IBM DB2-Datenbankserver (QDB2/LINUX)	N/V	NULL	DB2-Instanz	cmdb_ci_db_db2_instance
Microsoft Exchange smtpd	smtp	NULL	Exchange-Clientzugriffsserver	cmdb_ci_exchange_cas
Microsoft Exchange 2010-Protokollkopierer	msexchange-logcopier	NULL	Exchange-Postfach	cmdb_ci_exchange_mailbox_server
JBoss-Service httpd	N/V	NULL	JBoss	cmdb_ci_app_server_jboss
Microsoft IIS httpd 6.0	N/V	NULL	Microsoft iis-Webserver	cmdb_ci_microsoft_iis_web_server
Microsoft SQL Server 2005 9.00.4035; SP3	N/V	NULL	Microsoft SQL Server	cmdb_ci_db_mssql_instance
MongoDB 2.5.1	N/V	NULL	MongoDB-Instanz	cmdb_ci_db_mongodb_instance
MySQL 5.5.51	N/V	NULL	MySQL-Instanz	cmdb_ci_db_mysql_instance
nginx 1.4.6 (Ubuntu)	N/V	NULL	Nginx-Webserver	cmdb_ci_nginx_web_server
PostgreSQL-DB	N/V	NULL	PostgreSQL-Instanz	cmdb_ci_db_postgresql_instance
Oracle WebLogic Server	N/V	NULL	Weblogic	cmdb_ci_app_server_weblogic
IBM WebSphere MQ 6.0	N/V	NULL	IBM WebSphere MQ	cmdb_ci_appl_ibm_wmq
IBM WebSphere Application Server 6.1	N/V	NULL	IBM Websphere	cmdb_ci_app_server_websphere
OpenSSH : ssh	N/V	NULL	OpenSSH	cmdb_ci_appl
Oracle-Instanz	N/V	NULL	Oracle-Datenbank	cmdb_ci_db_ora_instance
Oracle-Instanz	N/V	NULL	Oracle TNS Listener	cmdb_ci_db_ora_instance
product-A	service-B	NULL	product-A:service-B	cmdb_ci_appl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für gute Entsprechungen, die gelöst wurden (Fortsetzung)

Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
Serviceprodukt	Servicename	Zusätzliche Serviceinformatione	Erkanntes Produkt	CI-Anwendungstabelle
product-A	service-B	extrainfo-C	product-A:extrainfo-C:service-B	cmdb_ci_appl

Beispiele für nicht eindeutig übereinstimmende Anwendungen

In diesem Beispiel stimmen die von Nmap zurückgegebenen Informationen mit keiner abgeleiteten Tabelle überein. Die Instanz muss die Basisanwendungstabelle [cmdb_ci_appl] verwenden, um das CI zu erstellen.

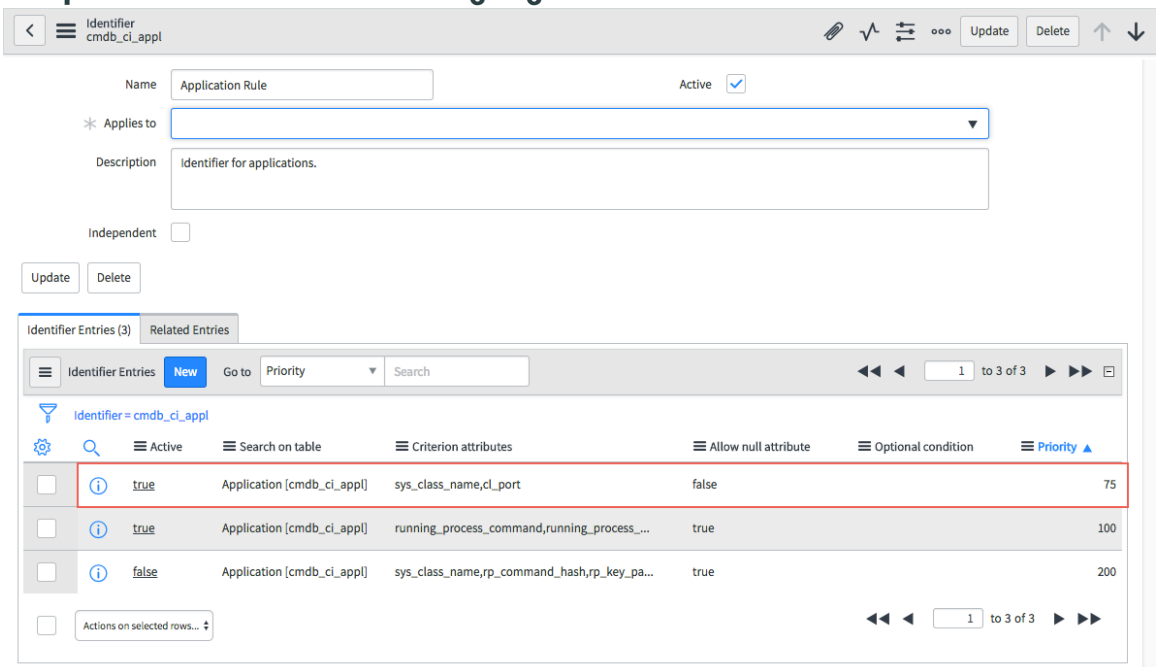
Gescannte Anwendung	Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
	Serviceprodukt	Servicename	Zusätzliche Serviceinformati	Erkanntes Produkt	CI-Anwendungstab
ExchangeHub	Microsoft Windows RPC	msrpc	„null“	Microsoft Windows RPC:msrpc	cmdb_ci_appl
HAProxy Lastenausgleichsmodul	IBM HTTP Server (Abgeleitet von Apache)	http	„null“	IBM HTTP Server (Abgeleitet von Apache):http	cmdb_ci_appl
SharePoint	Oracle-Datenbank	http	„null“	Oracle Database:http	cmdb_ci_appl
SharePoint	Oracle-Instanz	N/V	„null“	Oracle-Datenbank	cmdb_ci_appl

Anwendungsidentifizierung

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based] fügt der Anwendungsregel für die Anwendungstabelle [cmdb_ci_appl] einen Bezeichner hinzu, der dem sys_class_name und cl_port für Nmap-Scans entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nmap-Bezeichner für die Anwendungsregel



Nmap-Befehle und mit der anmeldedatenlosen Erkennung erfasste Daten

Nmap wird beim Erfassen von Daten in Phasen ausgeführt und führt einen kontrollierten Satz sicherer Befehle mit zwei Mustern zum Untersuchen von Anwendungen und Geräten aus.

Von Nmap bei der Hosterkennung zurückgegebene Daten

Für einen Host, von dem Nmap feststellt, dass er in Betrieb ist, gibt Nmap die folgenden Daten zurück:

- **Betriebssystemfamilie**: Wenn die Betriebssystemfamilie eine der sechs unterstützten Serverbetriebssystemfamilien ist, wird ein Host-CI verwendet, das der entsprechenden Serverklasse zugeordnet ist, um das Host-CI zu erstellen oder zu aktualisieren. Wenn die von Nmap zurückgegebene Betriebssystemfamilie nicht zu den unterstützten Serverbetriebssystemen gehört, wird ein Host-CI erstellt oder mithilfe der Hardwarebasisklasse [cmdb_ci_hardware] aktualisiert.
- **MAC-Adresse**: Wenn sich der gescannte Host im selben Subnetz wie der MID Server-Host unter Windows befindet, der die Nmap-Befehle ausführt, gibt Nmap die MAC-Adresse des Remotehosts zurück.

Von Nmap während der Hosterkennung ausgeführte Befehle

Der MID Server übergibt die IP-Adresse eines Remotehosts an den Nmap-Befehl und eine Reihe von Ports, die der IP-Servicetabelle entnommen sind. Der Host muss von Nmap gemeldet werden, damit er in Betrieb ist. Der Host ist in Betrieb, wenn der von Nmap zurückgegebene Portstatus **Offen** oder **open/filtered (Offen/Gefiltert)** lautet. Wenn gemeldet wird, dass der Host in Betrieb ist, wird die zurückgegebene Betriebssystemfamilie untersucht, um die Klasse zu bestimmen, die zum Erstellen oder Aktualisieren des Host-CI verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
-PS	Mit der Option TCP-SYN wird bestimmt, ob der Host online ist. Diese Option sendet ein leeres TCP-Rohpaket mit dem SYN-Flag an alle in der Scan-Liste angegebenen Ports. Nmap meldet, dass der Host online ist, wenn ein SYN/ACK-TCP-Paket zurückgegeben wird und wenn ein RST zurückgegeben wird, wodurch angegeben wird, dass der Port geschlossen ist. Der Nmap-Hostcomputer unterbricht die neu entstehende Verbindung mit einem RST anstelle eines ACK, da die SYN/ACK-Antwort aus dessen Sicht unerwartet ist. Wenn mehrere Port-Probes angegeben sind, werden sie parallel gesendet. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows
-PA	Erkennt Paketfilterungsgeräte. Diese Option ist eine TCP-ACK-Hosterkennung mit einer angegebenen Liste von Ports. Wenn keine Liste definiert ist, wird der Standardport 80 verwendet. Nmap sendet ein leeres TCP-Rohpaket mit gesetztem ACK-Flag. Diese Aktion bestätigt Daten über eine hergestellte TCP-Verbindung und veranlasst den Remotehost, mit einem RST-Paket zu antworten. Wenn der Remotehost mit einem RST-Paket antwortet, weiß Nmap, dass der Host online ist. Die ACK-Ping-Probe kann die Paketfilterung von TCP-SYN-Paketen durch zustandslose Paketfilterung, Netzwerkentitäten wie Firewalls, Router und Host-Routingtabellen/Firewall-Software überwinden. Stateful-Firewalls verwerfen unerwartete Pakete, wodurch das ACK-Paket verworfen wird, was die Wahrscheinlichkeit erhöht, dass die SYN-TCP-Probe durchkommt. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows **Hinweis:** Beide Pakettypen, Ping-SYN (-PS) und Ping ACK (-PA), können zusammen im selben Scan-Versuch konfiguriert werden.
-O	Aktiviert die BS-Erkennung für einen Remotehost und gibt den Namen des Anbieters, das zugrunde liegende BS, die BS-Generation und den Gerätetyp wie Router oder Switch an Nmap verwendet Fingerprinting anhand des TCP/IP-Stapels, um die auf dem Host ausgeführte Betriebssystemfamilie zu bestimmen. Nmap sendet eine Reihe von TCP- und UPD-Paketen an den Host und untersucht die Antworten. Nachdem die Antworten gründlich getestet wurden, vergleicht Nmap die Ergebnisse mit seiner Datenbank **nmap-os-db** und gibt die BS-Details aus, wenn eine Übereinstimmung vorliegt. Wenn Nmap das Betriebssystem nicht erraten kann und mindestens ein offener und ein geschlossener Port gefunden wurden, werden ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
	Fingerabdruck und eine URL generiert, die an nmap.org übermittelt werden können. Bei der BS-Erkennung werden keine Skripts der Nmap Scripting Engine (NSE) verwendet. Die BS-Erkennung wird nach der Erkennung der Anwendungs-/Serviceversion ausgeführt, wodurch die Genauigkeit der BS-Erkennung verbessert wird. Die Ergebnisse der beiden Scan-Typen können sich jedoch widersprechen. Die BS-Erkennung wird auf der TCP-Transportschicht ausgeführt, während die Versionserkennung für die Anwendung bzw. den Service auf einer höheren Ebene im TCP-Stapel ausgeführt wird. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows
-p	Liste der zu scannenden Ports
-T4	*Aggressive* Timing-Vorlage von Nmap
-v	Zum Aktivieren ausführlicher Details. Dieser Befehl wird normalerweise verwendet, um Betrachtern der Standardausgabe den Fortschritt anzuzeigen. Dies kann jedoch dazu führen, dass die Skripts der Nmap Scripting Engine (NSE) zusätzliche Details enthalten.
-Pn	Zum Deaktivieren des Standard-Ping. Mit diesem Befehl wird die anfänglichen Scan-Phase der Nmap-Hosterkennung übersprungen, und alle Hosts werden so behandelt, als wären sie online. Verwenden Sie diesen Befehl, wenn Sie einen Port-Scan durchführen möchten, auch wenn die von den Discovery-Standard-Probes ausgeführten Ports keinen offenen Port finden.
-r	Scannt Ports nacheinander ohne Randomisierung
--reason	Gibt den Grund an, aus dem Nmap einen Port mit einem bestimmten Status klassifiziert hat
--system-dns	Anstelle der DNS-Namensserver wird für die umgekehrte DNS-Suche der DNS-Resolver des Betriebssystems verwendet. Diese Option ist langsamer als die Verwendung von DNS-Servern, da sie jeweils nur eine IP-Adresse auflösen kann, während mehrere rDNS-Anforderungen parallel ausgeführt werden. Der zurückgegebene Wert stimmt jedoch mit dem vom MID Server zurückgegebenen Wert überein, der zum Erstellen von Host-CIs verwendet wird.
-X -	Leitet `stdout` an eine XML-Datei um
2> <*Datenpfad*>	Leitet Fehlermeldungen, die Nmap an `stderr` geschrieben hat, zur angegebenen Datei um

Von Nmap während der Anwendungserkennung zurückgegebene Daten

Für einen Host, von dem Nmap feststellt, dass er in Betrieb ist, gibt Nmap die folgenden Daten zurück:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Portstatus**:
  - **Offen**: Eine Anwendung akzeptiert an dem Port aktiv TCP- (oder UDP-)Pakete.
  - **open|filtered (Offen|Gefiltert)**: Nmap kann nicht bestimmen, ob ein Port offen oder gefiltert ist. Ein offener Port gibt möglicherweise keine Antwort zurück, wenn UDP-, IP-Protokoll-, FIN-, NULL- und Xmas-Scans von Nmap verwendet werden.
- **Servicename**: Name des Service, der an dem Service-Port aktiv TCP- (oder UDP-)Pakete akzeptiert
- **Serviceprodukt**: Name der Anwendung, die an dem von Nmap identifizierten offenen Port ausgeführt wird
- **Zusätzliche Serviceinformationen**: Alle zusätzlichen, von Nmap zurückgegebenen Informationen, die Discovery zum Identifizieren der Anwendung verwenden kann

Von Nmap während der Anwendungserkennung ausgeführte Befehle

Der MID Server übergibt dem Nmap-Befehl eine IP-Adresse für einen Remotehost und einen zu scannenden Port. Nmap versucht, die Anwendung zu identifizieren, die den Port aktiv abhört, und bestimmt dann, ob ein neues CI erstellt oder ein vorhandenes aktualisiert werden soll. Der Host muss von Nmap gemeldet werden, damit er in Betrieb ist.

Zur Kursbestimmung verwendet Nmap die folgenden Informationen:

- Serviceprodukt
- Servicename
- Zusätzliche Serviceinformationen
- Status des gescannten Ports

Hinweis: Die Werte für das Serviceprodukt und den Servicenamen dürfen nicht NULL sein, und der Servicename darf nicht mit einem Fragezeichen enden. Nmap fügt Servicenamen ein Fragezeichen hinzu, wenn die Anwendung, die den gescannten Port abhört, erraten werden muss. Die Instanz erstellt oder aktualisiert kein Anwendungs-CI, wenn Nmap den Anwendungsnamen nicht aus der statischen Registrierungsdatei nmap-services abrufen kann.

Befehl	Beschreibung
-sS	TCP-SYN-Port-Scan (Stealth). Dies ist die standardmäßige Scan-Option, die niemals TCP-Verbindungen herstellt. Scans können zwischen **offenen**, **geschlossenen** und **gefilterten** Ports unterscheiden. Der TCP-SYN-Scan implementiert einen halboffenen Reset, der die Anforderung abbricht, bevor die Verbindung hergestellt werden kann. Der Port ist **offen** (die Anwendung horcht), wenn ein SYN/ACK zurückgegeben wird. Der Port ist **geschlossen**, wenn ein RST zurückgegeben wird. Wenn nach mehreren erneuten Übertragungen keine Antwort eingeht, wird der Port als **gefiltert** markiert. Der Port wird auch als gefiltert markiert, wenn ein ICMP-Fehler „nicht erreichbar“ (Typ 3, Code 1,2,3,9,10,13) empfangen wird. Anforderungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
	• Rohpaketberechtigungen • Ausführung als Root • Windows-Administratorrechte
-sV	Probes öffnen Ports, um Serviceprotokoll, Anwendungsname, Versionsnummer, Hostname, Gerätetyp, BS-Familie und verschiedene Details wie die SSH-Protokollversion zu bestimmen. Wenn Nmap eine Antwort erhält, die nicht mit der Datenbank übereinstimmt, werden ein Fingerabdruck und eine URL zur Übermittlung an **nmap.org** ausgegeben. Nmap sucht in seiner statischer Registrierungsdatei `nmap-services` nach der Portnummer, um den Namen eines Anwendungsservice zu bestimmen, der den Port möglicherweise aktiv abhört. Der von Nmap zurückgegebene Servicename wird mit einem Fragezeichen versehen, das anzeigt, dass Nmap seine Identität erraten musste. Die Instanz erstellt oder aktualisiert kein Anwendungs-CI, wenn Nmap die Anwendung an einem offenen Port errät. **Hinweis:** Dieser Befehl erfordert keine Rohpaketberechtigungen.
--datadir	Pfad zu dem Verzeichnis, das den sicheren Satz von Nmap-Skripts enthält, die während der Anwendungs-/Versionserkennung ausgeführt werden sollen
-p	Einzelner zu scannender Port
-T4	*Aggressive* Timing-Vorlage von Nmap
-v	Zum Aktivieren ausführlicher Details. Dieser Befehl wird normalerweise verwendet, um Betrachtern der Standardausgabe den Fortschritt anzuzeigen. Dies kann jedoch dazu führen, dass die Skripts der Nmap Scripting Engine (NSE) zusätzliche Details enthalten.
-Pn	Zum Deaktivieren des Standard-Ping. Mit diesem Befehl wird die anfänglichen Scan-Phase der Nmap-Hosterkennung übersprungen, und alle Hosts werden so behandelt, als wären sie online. Verwenden Sie diesen Befehl, wenn Sie einen Port-Scan durchführen möchten, auch wenn die von den Discovery-Standard-Probes ausgeführten Ports keinen offenen Port finden.
-r	Scannt Ports nacheinander ohne Randomisierung
--reason	Gibt den Grund an, aus dem Nmap einen Port mit einem bestimmten Status klassifiziert hat
--system-dns	Anstelle der DNS-Namensserver wird für die umgekehrte DNS-Suche der DNS-Resolver des Betriebssystems verwendet. Diese Option ist langsamer als die Verwendung von DNS-Servern, da sie jeweils nur eine IP-Adresse auflösen kann, während mehrere rDNS-Anforderungen parallel ausgeführt werden. Der zurückgegebene Wert stimmt jedoch mit dem vom MID Server zurückgegebenen Wert überein, der zum Erstellen von Host-CIs verwendet wird.
-X -	Leitet `stdout` an eine XML-Datei um
2> *<Datenpfad>*	Leitet Fehlermeldungen, die Nmap an `stderr` geschrieben hat, zur angegebenen Datei um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PowerShell für Discovery und Service-Mapping

MID Server verwenden PowerShell und PowerShell Remoting für den Zugriff auf Konfigurationselemente (CIs) während der horizontalen Erkennung und der Erkennung von oben nach unten. Überprüfen Sie die MID Server-Parameter und Skripteinbindungen, Probe-Parameter und Anmeldeinformationen für die Verwendung von PowerShell.

PowerShell dient zur Steuerung und Automatisierung der Verwaltung von Windows-Servern und -Anwendungen.

MID Servers können PowerShell für die direkte Kommunikation mit Windows-Servern verwenden, wobei sowohl WMI- als auch WinRM-Protokolle verwendet werden. Für Windows-Services, die das WinRM-Protokoll verwenden, richtet der PowerShell-Prozess eine sichere PSSession ein (PowerShell-Remoting-Sitzung) ein, bis MID-Server die Abfrage eines Windows-Servers beendet. Bei Windows-Servern, die das WMI-Protokoll verwenden, sendet der PowerShell-Prozess jeden PowerShell-Befehl mit Anmeldeinformationen.

PowerShell ist auch die bevorzugte Methode für die Erkennung in mehreren Windows-Domänen. PowerShell ermöglicht es einem einzelnen MID-Server, sich auf Servern in verschiedenen Domänen mit in der Instanz gespeicherten Anmeldeinformationen zu authentifizieren.

Wenn Sie die MID Servers nicht für die Verwendung von PowerShell und PowerShell Remoting konfigurieren, verwenden die MID Servers WMI.

Wie PowerShell Discovery funktioniert

Die folgenden Beschreibungen erläutern, wie MID Server PowerShell zum Bereitstellen von Probes verwenden.

Probe und Sensor

Wenn eine Windows-Maschine mit PowerShell klassifiziert und eine MSSQL-Instanz erkannt wird, wird eine Probe namens *`Windows - MSSQL`* gestartet. Die Probe gibt die SQL-Datenbankkataloge und -version an einen passenden Sensor zurück.

Probe Parameter

Der Probe-Parameter *`WMI_ActiveConnections.ps1`* enthält ein Skript, das netstat.exe auf einem Zielserver ausführt, wenn PowerShell aktiviert ist. Dieses Skript extrahiert die Informationen zu Windows-Serververbindungen, z. B. Prozess-IDs, Ports und IP-Adressen.

Berechtigungen

Discovery verwendet PowerShell-Anmeldeinformationen von Windows aus der Tabelle „Anmeldeinformationen“ [discovery_credentials] oder die Anmeldeinformationen des Domänenadministrators des MID-Server-Services. Wenn Discovery PowerShell-Anmeldeinformationen in der Anmeldeinformationstabelle des Typs (Windows) Verwendet die Anmeldeinformationen des MID-Server Service.

MID-Server-Skripteinbindungen

Die folgenden Skripteinbindungen wurden für PowerShell-Erkennungen hinzugefügt. Diese Skripts werden auf dem MID Server ausgeführt, um die Skripte zu generieren, die Discovery für WMIRunner und PowerShell verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- GenerateWMIScriptJS: Generiert ein Javascript-Skript für die Probe „WMIRunner“.
- GenerateWMIScriptPS1: Generiert ein PowerShell-Skript für die PowerShell-Erkennung.

MID Server-Parameter für PowerShell

Optionale Parameter für den MID Server finden Sie unter MID Server-Parameter für PowerShell. Nachdem Sie die Einstellung für einen Parameter geändert haben, müssen Sie den MID-Server-Service neu starten.

PowerShell-Versionsanforderungen

MID Server, die PowerShell verwenden, müssen auf einem unterstützten Windows-Betriebssystem installiert sein. ServiceNow unterstützt die folgenden PowerShell-Versionen.

Version 3.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery
- PowerShell 3.0 unterstützt Windows Server 2003 nicht.

Version 4.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery

Version 5.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery

Hinweis: PowerShell-Version 6.0 wird **nicht** unterstützt. Viele der cmdlets, von denen die Erkennung abhängig ist, wurden aus dieser Version entfernt. Beispielsweise sind nur cmdlets mit WinRM für Remotevorgänge verfügbar.

Windows PowerShell-Ausführungsrichtlinien

Windows PowerShell hat vier verschiedene Ausführungsrichtlinien. Kunden können die Richtlinien für die Skriptausführung mit ihren Gruppenrichtlinieneinstellungen festlegen. Weitere Informationen finden Sie auf der Microsoft-Website für die PowerShell -Dokumentation.

- Restricted: Es können keine Skripte ausgeführt werden. Windows PowerShell kann nur im interaktiven Modus verwendet werden.
- AllSigned: Nur Skripte, die von einem vertrauenswürdigen Herausgeber signiert wurden, können ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- RemoteSigned: Heruntergeladene Skripte müssen von einem vertrauenswürdigen Herausgeber signiert werden, bevor sie ausgeführt werden können.
- Unrestricted: Keine Einschränkungen, alle Skripte können ausgeführt werden.

Hinweis: Wenn Sie eine andere Richtlinie als „Unrestricted“ haben, muss das Skript signiert werden.

MID Server zur Verwendung von PowerShell einrichten

Konfigurieren Sie MID-Server in Ihrer Organisation, um PowerShell für die horizontale und Top Down-Discovery von zu verwenden Windows Server.

Vorbereitungen
Erforderliche Rolle: Administrator

Hinweis: Dies ist standardmäßig aktiviert.

PowerShell Version 2.0 wird nicht unterstützt. Daher wird ein Upgrade auf eine höhere Version empfohlen. Wenn der MID-Server erkennt, dass er über Version 2.0 verfügt, funktioniert er möglicherweise nur teilweise. Der MID-Server erstellt einen Datensatz in der Problemtabelle mid_server mit einer Meldung, die besagt, dass PowerShell Version 2 veraltet ist. Ein Upgrade von PowerShell auf Version 5 wird empfohlen.

Prozedur

1. Laden Sie PowerShell herunter, und installieren Sie sie auf jedem MID-Server Für Erkennung konfiguriert Windows Computer.
   Wenn auf dem Host eine kompatible PowerShell verfügbar ist, müssen Sie nichts anderes tun.
2. Bestimmen Sie, welche Anmeldeinformationen MID-Server für PowerShell verwenden.
   - Um Windows-Computer mit Anmeldeinformationen aus der Anmeldeinformationstabelle zu erkennen, legen Sie den Parameter `mid.powershell.use_credentials` auf **true** fest. Die Verwendung von Anmeldeinformationen aus der Anmeldeinformationstabelle ist das Standardverhalten, wenn PowerShell aktiviert ist.
   - Um zu erzwingen, dass Discovery und Service-Mapping die Anmeldeinformationen des MID-Server-Servicebenutzers verwenden, legen Sie den Parameter `mid.powershell.use_credentials` für den MID Server auf **false** fest. Der MID-Server-Service benötigt Anmeldeinformationen des Domänenadministrators, um Zugriff auf die Windows-Computer in der Domäne zu erhalten.
3. **Wahlweise:** Konfigurieren Sie bei Bedarf erweiterte Parameter für PowerShell und PowerShell-Remoting für jeden MID-Server separat.
   Sie können PowerShell jedoch deaktivieren, indem Sie ändern `mid.use_powershell`Und `mid.sa.prefer_powershell`, Diese Methode ist veraltet und sollte nicht verwendet werden.

PowerShell-Remoting für Discovery

Probe-Entwickler können das PowerShell-Framework zur Remoteausführung verwenden, um die Remoteausführung von Skripts auf Zielgeräten automatisch zu verarbeiten. Das einheitliche Framework beseitigt Inkonsistenzen bei der Remoteausführung, erhöht die Effizienz und verbessert die Stabilität.

Anforderungen

Zur Verwendung des PowerShell-Framework für die Remoteausführung müssen die folgenden Anforderungen erfüllt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der MID Server muss in der Lage sein, auf die Netzwerkfreigabe des Ziels zu schreiben und von dieser zu lesen.
- Das Remoteziel muss über PowerShell 3 oder höher (bis 5.1) verfügen.
- Für MID Server, die WinRM oder WMI verwenden und das Skript auf das Remoteziel kopieren sollen, müssen die Bereiche MachinePolicy und UserPolicy auf „Nicht definiert“ festgelegt sein. Wenn das Skript nicht kopiert wird, kann die Ausführungsrichtlinie eine beliebige andere, einschließlich „Beschränkt“, sein.

Weitere Informationen finden Sie unter MID Server zur Verwendung von PowerShell einrichten.

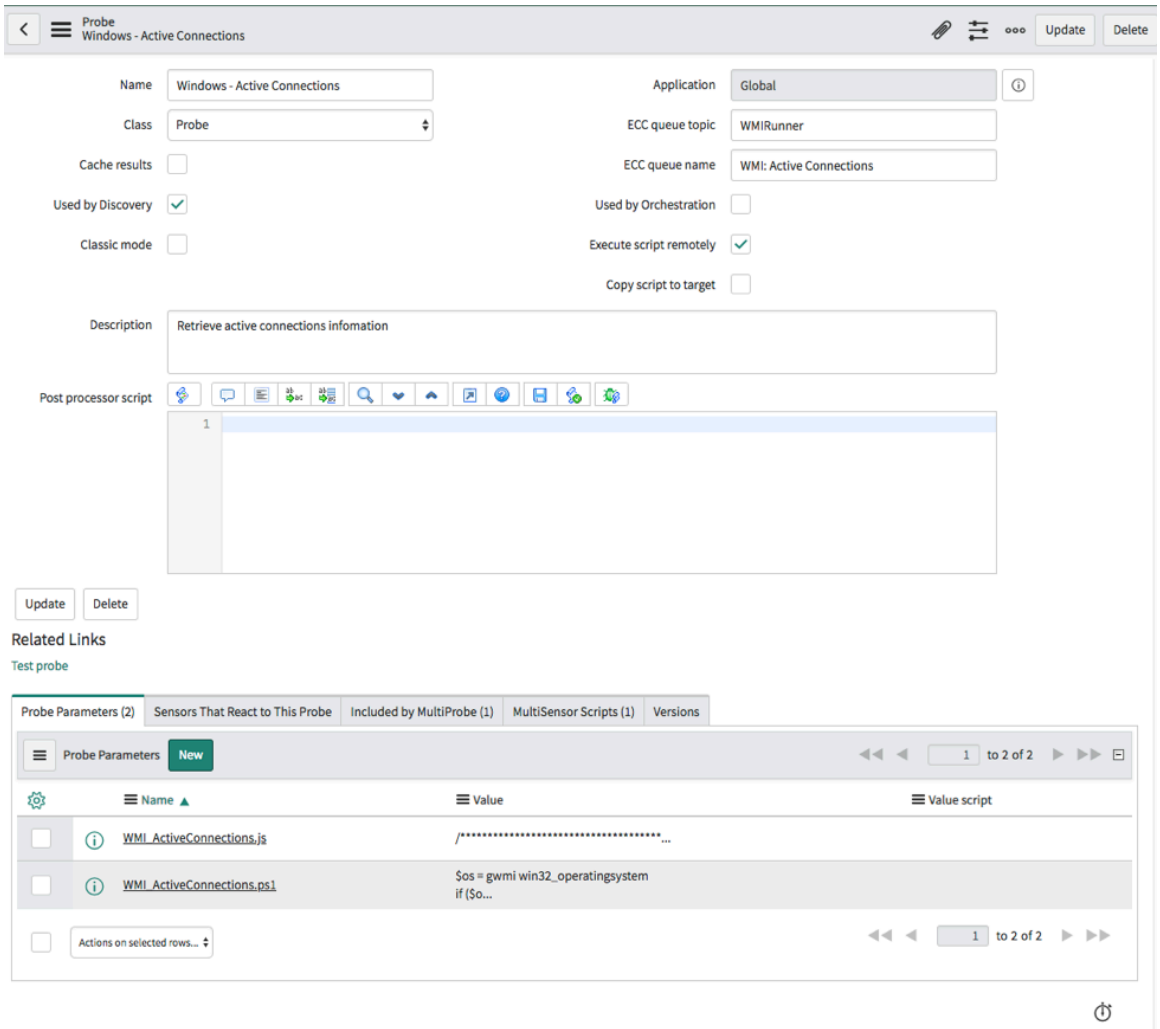
Anwendungserkennung

Das PowerShell-Framework zur Remoteausführung bietet Optionen zum Kopieren von Dateien auf das Remoteziel, wenn ein Scan ausgeführt wird. Das Kopieren von Dateien auf das Ziel ist für Probes wie „Windows - File discovery“ wichtig, da das Skript sich selbst auf dem Remoteziel aufruft, um einen neuen Prozess zu starten. Auf MID Servern, die WMI zur Remoteausführung von Skripts verwenden, kann ein launchProcess-Fehler auftreten, wenn das Skript zu lang ist. Durch das Kopieren des Skripts auf das Remoteziel wird dieser Fehler behoben. Das Kopieren eines Skripts auf ein Remoteziel kann dazu führen, dass das Skript auf dem Ziel von Virenschutzsoftware markiert wird. Um Probleme mit Virenschutzsoftware zu vermeiden, fügen Sie die Skripts der Liste der zulässigen Elemente der Virenschutzanwendung hinzu.

Probe-Konfiguration

Im Folgenden finden Sie die Konfigurationsseite der Probe „Windows - Active Connections“, der in der Multi-Probe „Windows - ADM“ enthalten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Kontrollkästchen **Skript remote ausführen** wird angezeigt, wenn das ECC-Warteschlangenthema WMIRunner oder PowerShell lautet. Wenn das Kontrollkästchen aktiviert ist, werden Skripts auf dem Remoteziel ausgeführt. Andernfalls werden Skripts auf dem MID Server ausgeführt.

Das Kontrollkästchen **Skript in Ziel kopieren** wird angezeigt, wenn **Skript remote ausführen** aktiviert ist. Wenn **Skript in Ziel kopieren** aktiviert ist, wird das Skript auf das Ziel kopiert und dort ausgeführt. Wenn **Skript in Ziel kopieren** deaktiviert ist, wird das Skript auf dem Ziel ausgeführt, ohne es zu kopieren.

Entwicklung von PowerShell-Probes

Das PowerShell-Framework zur Remoteausführung stellt eine einheitliche Methode zum Ausführen von in einem Probe-Parameter enthaltenen PowerShell-Skripts auf einem Remotezielserver dar. Das Framework beseitigt die Notwendigkeit, dass Probe-Entwickler für die Remoteausführung eigenen Code verfassen müssen, wodurch Inkonsistenzen zwischen Entwicklern auftreten könnten. Das Framework verarbeitet die Remoteausführung von Skripts automatisch, weswegen Probe-Entwickler Skripts so schreiben, als ob die Probe Informationen lokal erfassen würde.

Das Framework verarbeitet die Remoteausführung unabhängig davon, ob der MID Server für WMI oder WinRM konfiguriert ist. Wenn der MID Server für WMI konfiguriert ist, führt die Probe mithilfe von launchProcess Befehle auf dem Remoteziel aus. Die Verwendung von launchProcess erschwert die Remoteausführung und kann zu Fehlern führen. Ein für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

WinRM konfigurierter MID Server verwendet jedoch nicht launchProcess und ist daher effizienter und stabiler.

Von Discovery ausgeführte PowerShell-Befehle

Diese Seite enthält die PowerShell-Cmdlets und ihre Parameter, die Discovery zur Steuerung und Automatisierung der Verwaltung von Windows-Servern und -Anwendungen ausführt. Enthalten sind die Probe-Parameter und MID Server-Skripts, die die Befehle enthalten.

Cmdlet/Parameter	Beschreibung
Add-Content • Pfad • Codierung • Wert	Hängt Inhalte an ein angegebenes Element oder eine angegebene Datei an. Sie können den Inhalt angeben, indem Sie ihn in den Befehl eingeben oder indem Sie ein Objekt angeben, das den Inhalt enthält. **Probe** Windows - File discovery (filebaseddiscovery.ps1) **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1
Add-Member • NotePropertyName • NotePropertyValue • MemberType • Name • Wert	Ermöglicht das Hinzufügen von Eigenschaften und Methoden zu einer Instanz eines Windows PowerShell-Objekts. Beispielsweise können Sie ein NoteProperty-Mitglied hinzufügen, das eine Beschreibung des Objekts enthält, oder ein ScriptMethod-Mitglied, das ein Skript zum Ändern des Objekts ausführt. **Probe** Windows - File discovery (filebaseddiscovery.ps1) **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1
Add-Type • TypeDefinition • AssemblyName • MemberDefinition • Name • Namespace • PassThru	Fügt in Ihrer Windows PowerShell-Sitzung eine Microsoft .NET Framework-Klasse hinzu. Sie können dann das Cmdlet „New-Object“ verwenden, um Objekte zu instanziieren und diese Objekte wie jedes andere .NET Framework-Objekt zu verwenden. Wenn Sie Ihrem Windows PowerShell-Profil den Befehl Add-Type hinzufügen, ist die Klasse in allen Windows PowerShell-Sitzungen verfügbar. **Probes** • Windows - MSSQL (sqlinfo.ps1) • Windows - Azure (is.azure.ps1) **MID Server-Skript** • Credentials.psm1 • RegistryAPI.psm1 • LaunchProc.psm1
Compare-Object • Eigenschaft • PassThru	Vergleicht zwei Objektsätze. Ein Objektsatz ist der Referenzsatz, der andere Satz ist der Differenzsatz. Das Ergebnis des Vergleichs gibt an, ob ein Eigenschaftswert nur im Objekt aus dem Referenzsatz oder, wenn der Parameter IncludeEqual angegeben ist, in beiden Objekten vorkommt. **MID Server-Skript**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	DiagnosticsUtil.psm1
ConvertTo-SecureString • Zeichenfolge • AsPlainText • Erzwingen	Konvertiert verschlüsselte Standardzeichenfolgen in sichere Zeichenfolgen. Es kann auch Nur-Text in sichere Zeichenfolgen konvertieren. Es wird mit ConvertFrom-SecureString und Read-Host verwendet. Die von dem Cmdlet erstellte sichere Zeichenfolge kann mit Cmdlets oder Funktionen verwendet werden, die einen Parameter vom Typ SecureString erfordern. **Probes** Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** Credentials.psm1
ConvertTo-Json	Konvertiert ein beliebiges Objekt in eine Zeichenfolge im JSON-Format (JavaScript Object Notation). Eigenschaften werden in Feldnamen sowie Feldwerte in Eigenschaftswerte konvertiert, und Methoden werden entfernt. **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1
Copy-Item • Pfad • Ziel • Erzwingen • Recurse • PassThru	Kopiert ein Element von einem Speicherort an einen anderen Speicherort im selben Namespace. Beispielsweise kann eine Datei in einen Ordner kopiert werden, jedoch nicht auf ein Zertifikatlaufwerk. **MID Server-Skript** • ADMELauncherWMI.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1
Foreach-Object: Prozess	Führt einen Vorgang für jedes Element in einer Sammlung von Eingabeobjekten durch. Die Eingabeobjekte können an das Cmdlet weitergeleitet oder mithilfe des InputObject-Parameters angegeben werden. **Probes** • Windows - JBoss Find web.xml List (indwebxml.ps1) • Windows - MSSQL (sqlinfo.ps1) **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • PSScript.ps1
Format-List	Formatiert die Ausgabe eines Befehls als Liste von Eigenschaften, in denen jede Eigenschaft in einer separaten Zeile angezeigt wird. Mit Format-List können Sie alle oder ausgewählte Eigenschaften eines Objekts als Liste formatieren und anzeigen. **MID Server-Skript** RegistryAPI.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Get-ChildItem • Pfad • Datei • Recurse • Filter • Verzeichnis • Einbeziehen	Ruft die Elemente an einem oder mehreren angegebenen Speicherorten ab. Wenn das Element ein Container ist, werden die Elemente innerhalb des Containers, sogenannte untergeordnete Elemente, abgerufen. Mit dem Parameter Recurse können Sie Elemente in allen untergeordneten Containern abrufen. **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • PSScript.ps1 • RegistryAPI.psm1
Get-Content • Roh • Pfad	Ruft den Inhalt von Elementen am durch den Pfad angegebenen Speicherort ab, zum Beispiel den Text in einer Datei. Dabei wird der Inhalt Zeile für Zeile gelesen, und es wird eine Sammlung von Objekten zurückgegeben, von denen jedes eine Inhaltszeile repräsentiert. **Probes** Windows - ADM Enhanced **MID Server-Skript** • ADMELauncherWMI.psm1 • ADMELauncherWinRM.psm1 • ScriptAPI.psm1
Get-Date: Uformat	Ruft ein DateTime-Objekt ab, das das aktuelle Datum oder ein von Ihnen angegebenes Datum darstellt. Datum und Uhrzeit können in verschiedenen Windows- und UNIX-Formaten formatiert werden. Mit Get-Date können Sie eine Datums- oder Uhrzeitzeichenfolge generieren und diese Zeichenfolge dann an andere Cmdlets oder Programme senden. **Probes** Windows - File Discovery (filebaseddiscovery.ps1) **MID Server-Skript** • DiagnosticsUtil.psm1 • LaunchProc.psm1
Get-Item	Ruft das Element am angegebenen Speicherort ab. Der Inhalt des Elements wird nicht am Speicherort abgerufen, es sei denn, Sie verwenden ein Platzhalterzeichen (*), um den gesamten Inhalt des Elements anzufordern. **Probes** Windows - ADM Enhanced **MID Server-Skript**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	• ExecuteRemote.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
Get-ItemProperty • Pfad • Name • ErrorAction	Ruft die Eigenschaften der angegebenen Elemente ab. Beispielsweise können Sie mit diesem Cmdlet den Wert der Eigenschaft LastAccessTime eines Dateiobjekts abrufen. Sie können dieses Cmdlet auch zum Anzeigen von Registrierungseinträgen und deren Werten verwenden. **MID Server-Skript** • RegistryAPI.psm1 • ScriptAPI.psm1 • NmapInstallation.psm1
Get-Member: Mitgliedstyp	Ruft die Mitglieder, Eigenschaften und Methoden von Objekten ab. Verwenden Sie zum Festlegen des Objekts den Parameter InputObject, oder leiten Sie ein Objekt an Get-Member weiter. Verwenden Sie zum Abrufen von Informationen über statische Mitglieder (die Mitglieder der Klasse, nicht der Instanz) den Parameter Static. Wenn Sie nur bestimmte Typen von Mitgliedern abrufen möchten, zum Beispiel NoteProperties, verwenden Sie den Parameter MemberType. **Probes** Windows - ADM Enhanced **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1
Get-Process • ID • ErrorVariable (alias EV) • PSProvider	Ruft die Prozesse auf einem lokalen Computer oder Remotecomputer ab. Ohne Parameter ruft dieses Cmdlet alle Prozesse auf dem lokalen Computer ab. Sie können einen bestimmten Prozess auch anhand des Prozessnamens oder der Prozess-ID (PID) angeben oder ein Prozessobjekt über die Pipeline an dieses Cmdlet übergeben. **Probes** Windows - File Discovery (filebaseddiscovery.ps1) **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • Get-PEB.psm1
Get-PSDrive • Name • ErrorAction • PSProvider	Ruft die Laufwerke in der aktuellen Sitzung ab. Sie können ein bestimmtes Laufwerk oder alle Laufwerke in der Sitzung abrufen. **Probes** Windows - ADM Enhanced **MID Server-Skript** • ADMELauncherWMI.psm1 • Credentials.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Get-PSSession	Ruft die von Benutzern verwalteten Windows PowerShell-Sitzungen (PSSessions) auf lokalen und Remotecomputern ab **MID Server-Skript** Credentials.psm1
Get-Variable: Name	Ruft die Windows PowerShell-Variablen in der aktuellen Konsole ab. Sie können nur die Werte der Variablen abrufen, indem Sie den Parameter ValueOnly angeben, und Sie können die zurückgegebenen Variablen nach Namen filtern. **MID Server-Skript** • ExecuteRemote.psm1 • PSScript.ps1 • DiagnosticsUtil.psm1
Get-WmiObject • ComputerName • Filter • Anmeldeinformationen • Identitätswechsel • Authentifizierung • ErrorAction (alias EA) • Liste • Namespace • Klasse	Ruft Instanzen von WMI-Klassen (Windows Management Instrumentation) oder Informationen über die verfügbaren WMI-Klassen ab. Um einen Remotecomputer anzugeben, verwenden Sie den Parameter ComputerName. Wenn der Parameter List angegeben ist, ruft das Cmdlet Informationen über die in einem angegebenen Namespace verfügbaren WMI-Klassen ab. Wenn der Parameter Query angegeben ist, führt das Cmdlet eine WQL-Anweisung (WMI Query Language) aus. **Probes** • Windows - MSSQL (sqlinfo.ps1) • Windows - Storage 2008 - PS (storage.ps1) **MID Server-Skript** • ExecuteRemote.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
Get-WSManInstance: ResourceURI	Ruft eine Instanz einer Verwaltungsressource ab, die durch einen Ressourcen-URI (Uniform Resource Identifier) angegeben ist. Die abgerufenen Informationen können ein komplexer XML-Informationssatz (ein Objekt) oder ein einfacher Wert sein. **MID Server-Skript** ScriptAPI.psm1
Gruppenobjekt: NoElement	Zeigt Objekte in Gruppen basierend auf dem Wert einer angegebenen Eigenschaft an. Group-Object gibt eine Tabelle mit einer Zeile für jeden Eigenschaftswert und einer Spalte zurück, in der die Anzahl der Elemente mit diesem Wert angezeigt wird. **MID Server-Skript** RegistryAPI.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Import-Module • Name • DisableNameChecking • Global	Fügt der aktuellen Sitzung mindestens ein Modul hinzu. Die von Ihnen importierten Module müssen auf dem lokalen Computer oder einem Remotecomputer installiert sein. **Probes** Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** • Credentials.psm1 • PSScript.ps1
Invoke-Command • Sitzung • ScriptBlock • ErrorAction • ErrorVariable • ArgumentList (Alias ist „args“) • FilePath	Führt Befehle auf einem lokalen Computer oder Remotecomputer aus und gibt die gesamte Ausgabe der Befehle zurück, einschließlich Fehler. Mit einem einzigen Befehl Invoke-Command können Sie Befehle auf mehreren Computern ausführen. **Probes** Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** • ADMELauncherWinRM.psm1 • Credentials.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • Get-PEB.psm1 • WMIFetch.psm1
Invoke-Expression	Wertet oder führt eine angegebene Zeichenfolge als Befehl aus und gibt die Ergebnisse des Ausdrucks oder Befehls zurück. Ohne Invoke-Expression würde eine an die Befehlszeile übermittelte Zeichenfolge unverändert zurückgegeben (als Echo-Zeichenfolge wiederholt). **MID Server-Skript** • NmapInstallation.ps1 • ScriptAPI.psm1
Invoke-WmiMethod • Name • ComputerName • Argumentlist • Anmeldeinformationen • ErrorAction	Ruft die Methoden von WMI-Objekten (Windows Management Instrumentation) auf **MID Server-Skript** • LaunchProc.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
Messobjekt: Summe	Berechnet die Eigenschaftswerte bestimmter Objekttypen. Measure-Object führt abhängig von den Parametern im Befehl drei Arten von Messungen durch. **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
New-Item • ItemType • Pfad • Erzwingen • ErrorAction	Erstellt ein neues Element und legt dessen Wert fest. Welche Elementtypen erstellt werden können, hängt vom Speicherort des Elements ab. Beispielsweise erstellt New-Item im Dateisystem Dateien und Ordner. In der Registrierung erstellt New-Item hingegen Registrierungsschlüssel und -einträge. **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
New-Object • TypeName • Eigenschaft • ArgumentList	Erstellt eine Instanz eines Microsoft .NET Framework- oder COM-Objekts **Probes** • Windows - AWS Relationship (AWS_InstanceID.ps1) • Windows - Azure (is.azure.ps1) • Windows - MSSQL (sqlinfo.ps1) • Windows - File Discovery (filebaseddiscovery.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** • ADMELauncherWMI.psm1 • CollectConnectionsAndProcessesInfo.ps1 • Credentials.psm1 • Get-PEB.psm1 • LaunchProc.psm1 • WMIFetch.psm1 XMLUtil.psm1 • ExecuteRemote.psm1
New-PSDrive • PSProvider • Stamm • ErrorAction • Anmeldeinformationen • Name • Bereich	Erstellt temporäre und persistente Laufwerke, die einem Speicherort in einem Datenspeicher wie einem Netzlaufwerk, einem Verzeichnis auf einem lokalen Computer oder einem Registrierungsschlüssel zugeordnet sind, sowie persistente, in Windows zugeordnete Netzlaufwerke, die einem Speicherort im Dateisystem auf einem Remotecomputer zugeordnet sind. **MID Server-Skript** • ADMELauncherWMI.psm1 • ScriptAPI.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
New-Variable • Namer • Wert • Erzwingen	Erstellt eine neue Variable in Windows PowerShell. Sie können der Variablen während der Erstellung einen Wert zuweisen oder den Wert nach der Erstellung zuweisen oder ändern. **MID Server-Skript** PSScript.ps1
New-PSSession • Anmeldeinformationen • SessionOption	Erstellt eine Windows PowerShell-Sitzung (PSSession) auf einem lokalen Computer oder Remotecomputer. Beim Erstellen einer PSSession stellt Windows PowerShell eine dauerhafte Verbindung zu einem Remotecomputer her. **MID Server-Skript** PSRemoteSession.psm1
New-PSSessionOption	Erstellt ein Objekt, das erweiterte Optionen für eine von Benutzern verwaltete Sitzung enthält. Sie können das Objekt als Wert des Parameters SessionOption von Cmdlets verwenden, die eine PSSession erstellen, zum Beispiel New-PSSession, Enter-PSSession und Invoke-Command. **MID Server-Skript** PSRemoteSession.psm1
New-Timespan • Start • Ende	Erstellt ein Zeitspannenobjekt, das ein Intervall darstellt. Sie können diesen Befehl für die Addition oder Subtraktion von Zeit bei einem DateTime-Objekt verwenden. **Probes** Windows - File Discovery (filebaseddiscovery.ps1)
Ausgabedatei: Dateipfad	Sendet die Ausgabe an eine Datei. Sie können diesen Operator anstelle von > verwenden, wenn Sie die zugehörigen Parameter verwenden müssen. **Probes** Windows - File Discovery (filebaseddiscovery.ps1)
Out-Null	Sendet die Ausgabe an NULL, wodurch sie effektiv gelöscht wird **MID Server-Skript** Get-PEB.psm1
Out-String	Konvertiert die von Windows PowerShell verwalteten Objekte in ein Array von Zeichenfolgen. Standardmäßig akkumuliert Out-String die Zeichenfolgen und gibt sie als einzelne Zeichenfolge zurück. Sie können den Parameter stream jedoch auch dazu verwenden, Out-String anzuweisen, jeweils eine Zeichenfolge zurückzugeben. Mit diesem Cmdlet können Sie die Zeichenfolgenausgabe durchsuchen und sie wie in herkömmlichen Shells bearbeiten, wenn die Objektbearbeitung weniger praktisch ist. **MID Server-Skript** Get-PEB.psm1
Receive-Job	Ruft die Ergebnisse von Windows PowerShell-Hintergrundaufträgen ab, zum Beispiel solchen, die mit dem Cmdlet Start-Job oder dem Parameter AsJob eines beliebigen Cmdlet gestartet wurden. Sie können die Ergebnisse aller Aufträge abrufen oder Aufträge anhand von Name, ID, Instanz-ID, Computername, Speicherort bzw. Sitzung oder durch Übermittlung eines Auftragsobjekts identifizieren. **MID Server-Skript**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	LaunchProc.psm1
Remove-Item • Recurse • Pfad • Erzwingen	Löscht mindestens ein Element. Da es von vielen Anbietern unterstützt wird, kann es viele verschiedene Elementtypen löschen, einschließlich Dateien, Ordner, Registrierungsschlüssel, Variablen, Aliase und Funktionen. **MID Server-Skript** • ExecuteRemote.psm1 • NmapInstallation.ps1 • LaunchProc.psm1 • CollectConnectionsAndProcessesInfo.ps1
Remove-Job	Löscht Windows PowerShell-Hintergrundaufträge. Sie können Aufträge starten, indem Sie Start-Job oder den Parameter AsJob eines beliebigen Cmdlet verwenden. Sie können dieses Cmdlet zum Löschen aller Aufträge oder zum Löschen von Aufträgen basierend auf Name, ID, Instanz-ID, Befehl oder Status bzw. durch Übergabe eines Auftragsobjekts an Remove-Job verwenden. Ohne Parameter oder Parameterwerte hat Remove-Job keine Auswirkungen. **MID Server-Skript** LaunchProc.psm1
Remove-PSDrive: Name	Löscht temporäre Windows PowerShell-Laufwerke, die mit dem Cmdlet New-PSDrive erstellt wurden **MID Server-Skript** • ADMELauncherWMI.psm1 • ScriptAPI.psm1
Remove-PSSession: Sitzung	Schließt Windows PowerShell-Sitzungen (PSSessions) in der aktuellen Sitzung. Das Cmdlet beendet alle Befehle, die in PSSessions ausgeführt werden, beendet die PSSession und gibt die Ressourcen frei, die von der PSSession verwendet wurden. Wenn die PSSession mit einem Remotecomputer verbunden ist, schließt dieses Cmdlet auch die Verbindung zwischen dem lokalen Computer und dem Remotecomputer. **Probes** Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** Credentials.psm1
Remove-Variable • Name • Wert	Löscht eine Variable und ihren Wert aus dem Bereich, in dem sie definiert ist, zum Beispiel in der aktuellen Sitzung. Sie können dieses Cmdlet nicht verwenden, um Variablen zu löschen, die als Konstanten festgelegt oder systemspezifisch sind. **MID Server-Skript** PSScript.ps1
Rename-Item • Pfad • NewName	Ändert den Namen eines angegebenen Elements. Dieses Cmdlet wirkt sich nicht auf den Inhalt des Elements aus, das umbenannt wird. Sie können Rename-Item nicht zum Verschieben eines Elements verwenden, beispielsweise durch Angabe eines Pfads zusammen mit dem neuen Namen. Um ein Element zu verschieben und umzubenennen, verwenden Sie das Cmdlet Move-Item.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	Probes Windows - File Discovery (filebaseddiscovery.ps1)
Select-Object • ExpandProperty (Alias Expand) • Eigenschaft • ExcludeProperty	Dient zur Auswahl bestimmter Eigenschaften eines Objekts oder Objektsatzes. Mit dem Cmdlet lassen sich außerdem spezifische Objekte, eine bestimmte Anzahl von Objekten oder Objekte an einer bestimmten Position in einem Array auswählen. Alias ist „Select“. **Probes** Windows - MSSQL (sqlinfo.ps1) **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • RegistryAPI.psm1
Select-String • Muster • NotMatch	Sucht nach Text und Textmustern in Eingabezeichenfolgen und Dateien. Sie können es wie Grep in UNIX und Findstr in Windows verwenden. Sie können Select-String oder den entsprechenden Alias sls eingeben. **MID Server-Skript** CollectConnectionsAndProcessesInfo.ps1
Select-XML • Xpath • Inhalt • Namespace	Ermöglicht die Verwendung von XPath-Abfragen zur Suche nach Text in XML-Zeichenfolgen und -Dokumenten. Geben Sie eine XPath-Abfrage ein, und verwenden Sie den Parameter Content, Path oder Xml, um die zu durchsuchende XML-Datei anzugeben. **MID Server-Skript** ScriptAPI.psm1
Set-Content • Pfad • Wert • Erzwingen • Codierung	Schreibt oder ersetzt den Inhalt im angegebenen Element, zum Beispiel einer Datei. Sie können den Inhalt in den Befehl eingeben oder Inhalt über die Pipeline an Set-Content senden. **MID Server-Skript** • ADMELauncherWinRM.psm1 • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1
Set-Location: Pfad	Legt den Arbeitsort auf einen angegebenen Speicherort fest: ein Verzeichnis, Unterverzeichnis, Registrierungsspeicherort oder beliebiger Anbieterpfad. **MID Server-Skript** Credentials.psm1
Set-StrictMode: Version	Konfiguriert den strikten Modus für den aktuellen Umfang und alle untergeordneten Bereiche und aktiviert bzw. deaktiviert ihn. Im strikten Modus generiert Windows PowerShell einen Abschlussfehler, wenn der Inhalt eines Ausdrucks, Skripts oder Skriptblocks gegen grundlegende bewährte Codierungsregeln verstößt. **MID Server-Skript** Get-PEB.psm1
Set-Variable	Weist einer angegebenen Variablen einen Wert zu oder ändert den aktuellen Wert. Wenn die Variable nicht vorhanden ist, wird sie durch das Cmdlet erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
• Name • Wert • Option • Bereich	**MID Server-Skript** • PSScript.ps1 • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1
Sortierobjekt: Eigenschaft	Sortiert Objekte in aufsteigender oder absteigender Reihenfolge basierend auf den Werten der Eigenschaften des Objekts. Sie können eine einzelne Eigenschaft oder mehrere Eigenschaften (für eine Sortierung mit mehreren Schlüsseln) angeben und eine Sortierung auswählen, bei der die Groß-/Kleinschreibung berücksichtigt bzw. nicht berücksichtigt wird. Sie können Sort-Object auch anweisen, nur die Objekte mit einem eindeutigen Wert für eine bestimmte Eigenschaft anzuzeigen. **Probes** Windows - MSSQL (sqlinfo.ps1) **MID Server-Skript** DiagnosticsUtil.psm1
Split-Path • Blatt • Pfad • Übergeordnet	Gibt nur den angegebenen Teil eines Pfads zurück, zum Beispiel den übergeordneten Ordner, einen Unterordner oder einen Dateinamen. Das Cmdlet kann auch Elemente abrufen, auf die der geteilte Pfad verweist, und feststellen, ob der Pfad relativ oder absolut ist. **Probes** • Windows - Weblogic - Find (findconfig.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) **MID Server-Skript** • Credentials.psm1 • LaunchProc.psm1 • PSScript.ps1 • ExecuteRemote.psm1
Start-Sleep • S (Alias für Sekunden) • M (Alias für Millisekunden)	Hält die Aktivität für den angegebenen Zeitraum in einem Skript oder einer Sitzung an. Sie können es verwenden, während Sie auf den Abschluss eines Vorgangs warten oder eine Pause einlegen, bevor Sie den Vorgang wiederholen. **Probes** Windows - Active Connections Multiple (WMI_ActiveConnections.ps1) **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • LaunchProc.psm1 • NmapInstallation.ps1
Stop-Job	Beendet gerade laufende Hintergrundaufträge der Windows PowerShell. Sie können dieses Cmdlet zum Anhalten aller Aufträge oder zum Anhalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	bestimmter Aufträge basierend auf Name, ID, Instanz-ID oder Status bzw. durch Übergabe eines Auftragsobjekts an Stop-Job verwenden. **MID Server-Skript** LaunchProc.psm1
Test-Path • Pfad • PathType	Bestimmt, ob alle Elemente des Pfads vorhanden sind. Gibt $True zurück, wenn alle Elemente vorhanden sind, und $False, wenn nicht alle da sind. Kann auch bestimmen, ob die Pfadsyntax gültig ist und ob der Pfad zu einem Container, einem Terminal oder einem Blattelement führt **MID Server-Skript** • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • PSScript.ps1 • RegistryAPI.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • CollectConnectionsAndProcessesInfo.ps1
Test-WSMan • Computer • Port	Sendet eine Identifizierungsanforderung, die bestimmt, ob der WinRM-Service auf einem lokalen Computer oder Remotecomputer ausgeführt wird. Wenn der Service auf dem getesteten Computer ausgeführt wird, zeigt das Cmdlet das Identitätsschema von WS-Management, die Protokollversion, den Produktanbieter und die Produktversion des getesteten Service an. **MID Server-Skript** ScriptAPI.psm1
Where-Object	Wählt Objekte mit bestimmten Eigenschaftswerten aus der Sammlung von Objekten aus, die an sie übergeben werden. Beispielsweise sind mit dem Cmdlet Where-Object folgende Auswahlvorgänge möglich: Dateien, die nach einem bestimmten Datum erstellt wurden, Ereignisse mit einer bestimmten ID oder Computer mit einer bestimmten Version von Windows. **MID Server-Skript** • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • WMIFetch.psm1
Write-Error • Nachricht • Kategorie	Deklariert einen nicht endenden Fehler. Standardmäßig werden Fehler im Fehlerstream zusammen mit der Ausgabe an das anzuzeigende Hostprogramm gesendet. **Probes** • Windows - MySQL Configuration (mysqlconfig.ps1ps1) • Windows - MySQL Version (mysqlinfo.ps1) • Oracle - Instance Pfile (oraclepfile.ps1)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	• Oracle - Instance Version (oracleversion.ps1) • Windows - MSSQL (sqlinfo.ps1) **MID Server-Skript** • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1
Write-Host: NoNewLine	Schreibt benutzerdefinierte Ausgaben an einen Host. Sie können die Farbe des Texts mithilfe des Parameters ForegroundColor und die Hintergrundfarbe mithilfe des Parameters BackgroundColor angeben. Mit dem Parameter Separator können Sie eine Zeichenfolge angeben, die zum Trennen von angezeigten Objekten verwendet wird. Das jeweilige Ergebnis hängt von dem Programm ab, das Windows PowerShell hostet. **Probes** • Windows - Network ARP Table (arpTable.ps1) • Windows - Weblogic - Find (findconfig.ps1) • Windows - JBoss Get (findjbossservicexml.ps1) • Windows - WebSphere - Web Services () • Windows - JBoss Find (findwebxml.ps1) • Windows - Weblogic - Get () • Windows - WebSphere - Cell (getcellxml.ps1) • Windows - WebSphere - Web Applications (getserverindexxml.ps1) • Oracle - Instance PFile (oraclepfile.ps1) • Oracle - Instance Version (oracleversion.ps1) • Windows - MSSQL (sqlinfo.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) • Windows - Storage 2008 - PS (storage.ps1) • Windows - Active Connections Multiple (WMI_ActiveConnections.ps1) **MID Server-Skript** • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • PSScript.ps1 • RegistryAPI.psm1 • ScriptAPI.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	• WMIFetch.psm1 • DiagnosticsUtil.psm1 • NmapInstallation.ps1
Write-Output	Sendet die angegebenen Objekte an den nächsten Befehl in der Pipeline. Wenn dies der letzte Befehl in der Pipeline ist, werden die Objekte in der Konsole angezeigt. **Probes** • Windows - Azure (is.azure.ps1) • ExecuteRemote (testExecuteRemote.ps1) • Windows - File Discovery (filebaseddiscovery.ps1) **MID Server-Skript** Get-PEB.psm1
Ausführlich Schreiben: Nachricht	Schreibt Text in den ausführlichen Nachrichtenstrom in Windows PowerShell. Normalerweise wird der ausführliche Nachrichtenstrom verwendet, um Informationen über die Befehlsverarbeitung bereitzustellen, die für das Debugging eines Befehls verwendet wird. **MID Server-Skript** • Get-PEB.psm1 • LaunchProc.psm1 • ExecuteRemote.psm1

MID Server-Parameter für PowerShell

Parameter steuern das Verhalten eines bestimmten MID-Servers und haben eine niedrigere Priorität als die MID-Server-Eigenschaften.

Die folgenden Parameter sind optional.

Hinweis: Nachdem Sie die Einstellung für einen Parameter geändert haben, müssen Sie den MID-Server-Service neu starten.

Name	Beschreibung
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Sitzungspool zulässig sind. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID Servers. • Typ: Ganzzahl • Standardwert: 25

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
mid.powershell_api.session_pool.target.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Pool pro Zielhost zulässig sind. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID Servers. • Typ: Ganzzahl • Standardwert: 3
mid.powershell_api.winrm.use_ssl	Erfordert die Verwendung von SSL-Zertifikaten für HTTPS-Verbindungen mit WinRM. • Typ: wahr | falsch • Standardwert: false
mid.powershell_api.winrm.additional_pssesion_options	Steuert die erweiterten Optionen für eine PSSession. Weitere Informationen zu erweiterten Optionen für eine PSSession finden Sie unter https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/new-pssessionoption?view=powershell-6 .
mid.powershell_api.winrm.remote_https_port	Konfiguriert den Port für das Verbinden zu Windows-Servern mit PowerShell über HTTPS. • Typ: Ganzzahl • Standardwert: 5986
mid.powershell_api.winrm.remote_port	Konfiguriert den Port für das Verbinden zu Windows-Servern mit PowerShell über HTTP. • Typ: Ganzzahl • Standardwert: 5985
mid.powershell_api.winrm.skip_ssl_cert_check	Überspringt die Prüfung für das SSL-Zertifikat, wenn WinRM für HTTPS-Verbindungen verwendet wird. • Typ: wahr | falsch • Standardwert: false
mid.powershell_api.winrm.skip_ssl_cert_check_options	Überspringt spezifische Prüfungen für SSL-Zertifikate, wenn WinRM für HTTPS-Verbindungen verwendet wird. Konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Sie MID-Server, um Prüfungen für Zertfifikate aus einer Certification Authority (CA) zu überspringen, aus dem Common Name (CN), der den mit dem Zertifikat verknüpften Host festlegt, und für widerrufene Zertifikate. • Typ: Zeichenfolge • Standardwert: -SkipCACheck -SkipCNCheck -SkipRevocationCheck
mid.powershell_api.wmi.use_reverse_dns_lookup	Aktivieren Sie diese Eigenschaft, um die Kerberos-Authentifizierung zu verwenden, wenn das WMI-Protokoll für die Kommunikation mit Windows-Zielgeräten verwendet wird. Wenn diese Option aktiviert ist, führt das System eine umgekehrte DNS-Suche von IP-Adressen durch, wodurch die Verwendung von vollqualifizierten Domänennamen (FQDN) anstelle von IP-Adressen ermöglicht wird. Dies kann die Kerberos-Authentifizierung erleichtern. **Hinweis:** Hinweis: Wenn die umgekehrte DNS-Suche fehlschlägt, verwendet das System möglicherweise die IP-Adresse. Darüber hinaus kann sich die Durchführung umgekehrter DNS-Suchen für IP-Adressen auf die Leistung auswirken. • Typ: wahr | falsch • Standardwert: False
mid.powershell.use_credentials	Legt die Anmeldeinformationen fest, die Discovery mit PowerShell verwendet werden sollen. Die Einstellung *wahr* lässt MID-Server Proben ausführen mit den Windows Anmeldeinformationen aus der entsprechenden Tabelle. Um Proben mit den Anmeldeinformationen des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Benutzers für den Service MID-Server auszuführen, stellen Sie diesen Parameter auf *falsch* ein. • Typ: true | false • Standardwert: true
mid.use_powershell	Aktiviert oder deaktiviert PowerShell für Discovery. Starten Sie MID-Server neu, nachdem Sie den Wert geändert haben. Wenn PowerShell nicht installiert ist oder die installierte Version niedriger als Version 2.0 ist, wird Discovery zur Verwendung von WMIRunner zurückgesetzt. • Typ: true | false • Standardwert: true
mid.powershell.path	Ermöglicht es einem Administrator, auf eine bestimmte PowerShell auf einem MID-Server zu verweisen, wenn mehr als eine PowerShell installiert ist. Geben Sie den Pfad zum Ordner an, das die ausführbare PowerShell-Datei enthält, zum Beispiel C:\mypowershell oder C:\mypowershell \. ServiceNow hängt automatisch die Zeichenfolge „powershell.exe“ an den Pfad an. Konfigurieren Sie diesen Parameter, wenn sowohl 32-Bit- als auch 64-Bit-PowerShells auf demselben MID-Server aktiv sind und die richtige PowerShell für den Kontext gestartet werden muss. 64-Bit Windows verwendet die Dateisystemumleitung und der MID-Server wird als 32-Bit-Anwendung ausgeführt. Wenn ein Pfad in %WinDir%\System32 festgelegt werden soll, leitet Windows automatisch auf %WinDir%\SysWOW64 um. Geben Sie den Pfad als %WinDir%\Sysnative an, um eine Umleitung zu vermeiden. Legen Sie statt C:\WINDOWS\system32\WindowsPowerShell\v1.0\ zum Beispiel C:\WINDOWS\sysnative\WindowsPowerShell\v1.0\ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: Bei einer 64-Bit-Version von Windows XP kann ein Microsoft-Hotfix erforderlich sein, um diese Funktion zu aktivieren. Um Anwendungen zu finden, die auf einem 64-Bit-Windows-Computer ausgeführt werden, muss MID-Server auf einem 64-Bit-Windows-Host-Computer ausgeführt werden. • Typ: Zeichenfolge (Pfad) • Standardwert: keiner
mid.powershell.enforce_utf8	Aktivieren Sie diesen Parameter, um Befehle auf einem Windows-Zielsystem zu zwingen, die UTF-8-codierte Ausgabe zurückzugeben. Bei Deaktivierung kann das Zielsystem seine Standardcodierung verwenden. Dieser Parameter ist nur gültig, wenn PowerShell aktiviert ist. Das Festlegen dieses Werts auf „false“ kann zu falschen Werten in der CMDB führen, wenn von einem Probe Nicht-ASCII-Zeichen zurückgegeben werden. • Typ: true | false • Standardwert: true
mid.powershell.local_mid_service_credential_fallback	Gibt die Anmeldeinformationen an, die der MID Server verwendet, wenn alle anderen Anmeldeinformationen fehlschlagen. • Typ: wahr | falsch • Standardwert: true
mid.powershell_api.idle_session_timeout	Gibt den Wert für den Timeout von PowerShell-Sitzungen im Leerlauf in Sekunden an. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID-Server. • Typ: Ganzzahl • Standardwert: 60

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
mid.powershell.command.parameter_passing	Aktivieren Sie diesen Parameter, um die Übergabe von PowerShell-Parametern von der Befehlszeile aus zuzulassen. • Typ: wahr | falsch • Standardwert: false
mid.powershell.command.script.parameter_passing	Aktivieren Sie diesen Parameter, um die Übergabe von PowerShell-Skripts von der Befehlszeile aus zuzulassen. • Typ: wahr | falsch • Standardwert: falsch
mid.windows.management_protocol	Ermöglicht Administratoren die Auswahl des für die Geräte- und Prozessklassifizierung verwendeten Windows-Verwaltungsprotokolls. Verfügbare Optionen: • WMI • WinRM • Typ: Zeichenfolge • Standardwert: WMI
mid.windows.probe_timeout	Legt das Timeout-Intervall für alle Windows-Probes auf einem bestimmten MID Server fest. Dieser Wert wird von den Werten überschrieben, die für einzelne Probes mit dem Probe-Parameter „wmi_timeout“ konfiguriert wurden. • Typ: Ganzzahl • Standardwert: 600

Application Dependency Mapping (ADM) für Discovery

Application Dependency Mapping (ADM) erkennt CIs durch die Erkennung von TCP-Verbindungen zwischen Geräten.

Wenn die ADM-Erkennung aktiviert ist, führt Discovery während der Erkundungsphase stets die ADM-Probes aus, um den TCP-Datenverkehr in Ihrem Netzwerk zu erkennen. Mithilfe dieser TCP-Verbindungen kann Discovery zusätzliche CIs finden und Beziehungen zwischen ihnen herstellen.

IPv6 wird für ADM unterstützt.

Hinweis: ADM bietet derzeit keine Unterstützung für mehrere Sprachen. Wenn die zurückgegebenen Werte nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Erkennung schlägt fehl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßige und erweiterte ADM-Erkennung

Standardmäßige ADM-Erkennung

Löst eine ADM-Probe aus, die mithilfe der Befehle `netstat` und `lsof` einen einzelnen Snapshot von TCP-Verbindungen auf Zielcomputern erstellt. Es werden jedoch keine neuen TCP-Verbindungen erkannt, die zwischen diesen 24-Stunden-Intervallen auftreten.

Die standardmäßige ADM-Erkennung ist standardmäßig aktiviert.

Erweiterte ADM-Erkennung (ADME)

Löst eine erweiterte ADM-Probe aus, die ein Skript auf Hostcomputern installiert, auf denen Discovery reguläre Muster basierend auf aktiven TCP-Verbindungen erstellt. Sie können eine Reihe von Eigenschaften und Probe-Parametern verwenden, die mehrere Aspekte der erweiterten ADM-Erkennung steuern.

Die ADME-Erkennung ist standardmäßig nicht aktiviert.

Service-Mapping verwendet die ADM-Probes für die datenverkehrsbasierende Erkennung. Weitere Informationen finden Sie unter Erkennung auf Basis von Predictive Intelligence.

Anforderungen

Sowohl die standardmäßige als auch die erweiterte ADM-Erkennung unterstützen die folgenden Betriebssysteme:

- Windows
- Unix
- Solaris (Auf Solaris-Computern ist erweitertes ADM in globalen Zonen verfügbar. Für lokale Zonen ist nur Standard-ADM verfügbar.)
- AIX
- HP-UX

Zur Verwendung des WMI-Protokolls ist Version 3.0 von PowerShell erforderlich.

Hinweis:

Wenn Sie die Ausführungsrichtlinie des Windows-Servers auf RemoteSigned oder AllSigned festlegen, kann ADME PowerShell-Skripts ausführen. Sie müssen das ServiceNow-Zertifikat zu den vertrauenswürdigen Herausgebern importieren, damit die Skripts ordnungsgemäß ausgeführt werden.

TCP-Nachverfolgungsdatei für erweitertes ADM

Beim ersten Start der erweiterten Probe durch Discovery werden keine TCP-Informationen erfasst. Stattdessen stellt die erweiterte Probe nur die TCP-Nachverfolgungsdatei bereit, in der Informationen über die erkannten TCP-Verbindungen gespeichert werden. Nach der erneuten Ausführung von Discovery übermittelt die erweiterte Probe den Inhalt der TCP-Nachverfolgungsdatei über den MID Server zurück an die Instanz. Die Informationen werden in der CMDB gespeichert.

Die TCP-Nachverfolgungsdatei wird standardmäßig an folgenden Speicherorten gespeichert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Windows: admin$\temp\{Ihr_Instanzname}. Während der Überwachung von TCP-Verbindungen werden die Informationen im Arbeitsspeicher abgelegt und später in der Datei gespeichert.
- Linux: /tmp/{Ihr_Instanzname}.

Sie können den Speicherort und andere Aspekte der Nachverfolgungsdatei mit ADM-Eigenschaften ändern.

Wenn Sie erweitertes ADM deaktivieren, bereinigt Discovery die Ordner im Hostdateisystem, wenn Discovery das nächste Mal ausgeführt wird. Nur die TCP-Nachverfolgungsdatei verbleibt.

Anforderungen für erweitertes ADM auf Linux-Computern

Ändern Sie die Datei sudoers, sodass die folgenden Befehle einbezogen werden:

Windows

- Unterstützte Dienstprogramme: netstat
- Erforderliche sudoer-Befehle: Keine
- Zusätzliche Anforderungen: Keine

AIX

- Unterstützte Dienstprogramme:
  - netstat
  - lsof (wenn netstat nicht funktioniert)
- Erforderliche sudoer-Befehle:
  - Cmnd_Alias ADME_CMDS=/usr/bin/netstat -Aan, /usr/sbin/lsof -iTCP -n -P
  - discoUser ALL=(root)NOPASSWD:ADME_CMDS
  - Defaults:discoUser ! requiretty
- Zusätzliche Anforderungen: Keine

Solaris

- Unterstützte Dienstprogramme:
  - netstat (für Solaris Version 11.2)
  - lsof (für Solaris-Versionen vor 11.2)
- Erforderliche sudoer-Befehle:
  - Cmnd_Alias ADME_CMDS = /usr/bin/netstat,/opt/csw/bin/lsof -iTCP -n -P -zglobal
  - discoUser ALL=(root) NOPASSWD:ADME_CMDS
  - Defaults!ADME_CMDS !requiretty
  - Cmnd_Alias ADME_PS = /usr/ucb/ps
  - discoUser ALL=(root) NOPASSWD:ADME_PS
  - Disco ALL=(root) /usr/bin/pfiles
  - Disco ALL=(root) /usr/bin/pgrep

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Defaults!ADME_PS !requiretty

Hinweis: Sie müssen **-zglobal** hinzufügen, damit lsof ausgeführt wird.

- Zusätzliche Anforderungen: Fügen Sie den lsof-Pfad dem sicheren Pfad hinzu. Beispiel: Wenn der Pfad zu lsof /opt/csw/bin lautet, muss der sichere Pfad secure_path = /usr/bin:/usr/sbin:/bin:/sbin:/opt/csw/bin lauten.

Hinweis: Die Befehle mit PS gelten sowohl für Standard-ADM als auch für erweitertes ADM.

HP-UX

- Unterstützte Dienstprogramme: lsof
- Erforderliche sudoer-Befehle:
  - Cmnd_Alias ADME_CMDS = /usr/local/bin/lsof -iTCP -n -P
  - discoUser ALL=(root) NOPASSWD:ADME_CMDS
  - Defaults!ADME_CMDS !requiretty

Hinweis: Netstat wird nicht unterstützt.

- Zusätzliche Anforderungen: Keine

Centos und Ubuntu

- Unterstützte Dienstprogramme: Keine
- Erforderliche sudoer-Befehle:
  - Cmnd_Alias ADME_CMDS = /usr/sbin/lsof -iTCP -n -P, /usr/bin/netstat -antp, /sbin/ss -tlnp, /sbin/ss -tenp
  - discoUser ALL=(root) NOPASSWD:ADME_CMDS
  - Defaults!ADME_CMDS !requiretty
- Zusätzliche Anforderungen: Keine

Beachten Sie in Bezug auf die sudo-Befehle Folgendes:

- ADME_CMDS ist eine Variable, die auf eine Liste von Befehlen verweist.
- /usr/bin/ ist das Verzeichnis, in dem sich lsof und netstat befinden.
- discoUser ist ein Benutzer, der über Root-Zugriff verfügen muss.

Einrichten und verwenden Erweitertes ADM

Führen Sie die folgenden Schritte aus, um erweitertes ADM einzurichten und zu verwenden:

1. Aktivieren Sie erweitertes ADM mit der Discovery-Eigenschaft glide.discovery.enable_adme.
2. Bestimmen Sie das Basisverzeichnis, in dem die TCP-Nachverfolgungsdatei auf den Hostcomputern abgelegt wird. Wenn Sie den Speicherort ändern möchten, geben Sie ihn in den folgenden Discovery-Eigenschaften an:
   - glide.discovery.adme.base_dir_unix
   - Mid.powershell.target_Base_dir

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie basierend auf den Betriebssystemen der Hostcomputer eine der folgenden Aktionen aus:
   - Linux: Ändern Sie die Datei sudoers, damit die erforderlichen Befehle einbezogen werden:
   - Windows: Legen Sie den Parameter `mid.windows.management_protocol` auf dem MID Server fest, um WinRM oder WMI zu verwenden. Dieser Parameter legt das Protokoll fest, das Ihr MID Server für die Kommunikation mit Windows-Remotehosts verwendet.
4. Erstellen Sie einen Zeitplan, und führen Sie Discovery aus.
5. Zeigen Sie die Ergebnisse in den TCP-Tabellen an.
6. Steuern Sie optional die Größe der TCP-Nachverfolgungsdatei und die Nutzlast mithilfe von Parametern für die erweiterten ADM-Probes. Unter Erkennung von TCP-Verbindungen finden Sie die Namen der Probes und Parameter.

Parameter und Eigenschaften für ADM-Erkennung konfigurieren

Mithilfe von Eigenschaften können Sie die ADM-Erkennung aktivieren oder deaktivieren und den Speicherort der TCP-Nachverfolgungsdatei für erweitertes ADM festlegen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch die Größe der TCP-Nachverfolgungsdatei und die Nutzlast mithilfe von Parametern für die erweiterten ADM-Probes steuern. Unter Erkennung von TCP-Verbindungen finden Sie die Namen der Probes und Parameter.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Discovery** Zum Festlegen der Systemeigenschaften.
2. Navigieren zu **Discovery-Definition** > **Probes** Zum Festlegen der Probe-Parameter.
3. Konfigurieren Sie die folgenden Eigenschaften und Probe-Parameter.
   Weitere Informationen finden Sie im Wissensartikel KB0822767 .

ADM-Eigenschaften und Probe-Parameter

Probe Parameter	Systemeigenschaft	Beschreibung
	glide.discovery.enable_adme	ADME: Aktivieren Sie die erwe ADM-Sonde. Bei „Ja“ wird die erweiterte ADM-Probe ausgelös greift nur nach Bedarf auf die AI Probe zurück. ◦ **Typ**: true | false ◦ **Standardwert**: falsch
	glide.discovery.application_mapping	Aktivieren Sie die Anwendungszuordnungsfu Wenn diese Eigenschaft au „true“ festgelegt ist, lösen Erkennungen die relevante ADM-Sonde während der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe Parameter	Systemeigenschaft	Beschreibung
		Erkundungsphase aus, wer Discovery einen Server finde **Wichtig:** Durch Deaktiv dieser Eigenschaft wird die Erstellung von Beziehungen zwischen Anwendungen deaktiviert, aber *Nicht* Deaktivieren Sie die ADM-Probes und -Sensoren, und verhindern Sie auch die Prozessklassifizierung. ○ **Typ**: true | false ○ **Standardwert**: true
sampling_interval	glide.discovery.adme.sampling_interval	ADME - Abtastintervall (Sek): W werden Prozess- und Verbindung in Sekunden erfasst? Muss mind Sekunden betragen. ○ **Typ**: integer ○ **Standardwert**: 120
base_dir	glide.discovery.adme.base_dir_unix	ADME – Unix-Basisverzeichnis Ein vorhandenes Verzeichnis au den UNIX-Zielcomputern, das a Arbeitsbereich verwendet werde soll. Muss ein absoluter Pfad zur Verzeichnis sein. Die UNIX- und Linux-Anmeldeinformationen Sie für die Verbindung zum Ger verwenden, müssen auch auf die Ordner zugreifen können. ○ **Typ**: Zeichenfolge ○ **Standardwert**: /tmp
powershell_param_base_dir	Mid.powershell.target_Base_dir	PowerShell: Ziel-Basisverzeichn Eine Netzwerkfreigabe auf den Zielcomputern von Windows, di Arbeitsbereich verwendet werde Wenn Sie das Verzeichnis ände es sich auch um einen freigegebe Netzwerkordner handeln. ○ **Typ**: Zeichenfolge ○ **Standardwert**: admin$\te
aggregation_interval (Unix) powershell_param_aggregation_interval (Windows)	glide.discovery.adme.aggregation_interval	ADME – Aggregationsintervall (Wie oft (in Sekunden) sofortige in Blöcke zusammengefasst wer muss mindestens 60 Sekunden b

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe Parameter	Systemeigenschaft	Beschreibung
		und es muss ein Vielfaches des A Abtastintervalls sein. ○ **Typ**: integer ○ **Standardwert**: 3600
rolling_window_size (Unix) powershell_param_rolling_window_size (Windows)	glide.discovery.adme.rolling_window_size	ADME - Rollfende Fenstergröße viele kürzlich aggregierte Blöcke gespeichert werden? Ein aggregi Block besteht aus dem ADME-Aggregationsintervall und den A Abtastintervallabtastungen. Nur neuesten Blöcke werden beibeha ○ **Typ**: Ganzzahl ○ **Standardwert**: 24
max_total_samples (Unix) powershell_param_max_total_samples (Windows)	glide.discovery.adme.max_total_samples	ADME – Maximale Anzahl Samples: Die Anzahl der vom Sk genommenen Samples. Die Ausf des Skripts wird beendet, nachde Anzahl von Mustern entnommen ○ **Typ**: Ganzzahl ○ **Standardwert**: 100

4. Klicken Sie auf **Speichern**.

Discovery-Verhalten

Discovery-Verhalten bestimmen die von Shazzam gestarteten Probes und die MID Server, von denen diese Probes gestartet werden.

Im Gegensatz zu einem Scan, der von einem einzelnen MID Server in einem bestimmten IP-Adressbereich durchgeführt wird, kann ein Verhalten mehreren MID Servern in demselben IP-Adresssegment oder in verschiedenen Netzwerksegmenten unterschiedliche Aufgaben zuweisen. Verhalten sind in Erkennungszeitplänen für Erkennungen verfügbar, in denen Konfigurationselemente (CI) in der CMDB aktualisiert werden.

Verhalten können in den folgenden Szenarien verwendet werden:

- Lastenausgleich: Ein Verhalten ermöglicht den Lastenausgleich in Systemen, die mehrere MID Server verwenden, die in einer oder mehreren Domänen bereitgestellt werden.
- Verschiedene Protokolle in mehreren Domänen: Konfigurieren Sie einen MID Server für die Suche nach allen Protokollen in einer Domäne und einem anderen MID Server, um einen WMI-Scan in einer zweiten Domäne durchzuführen.
- Zugriffssteuerungslisten (ACLs): Discovery kann SNMP-Geräte scannen, die durch eine ACL geschützt sind, wenn der MID Server-Hostcomputer Zugriff über diese ACL erhält. Verwenden Sie ein Verhalten, um einen MID Server zum Scannen von durch eine ACL geschützten Geräten zu konfigurieren.
- Geräte, die zwei Protokolle ausführen: Auf einigen Geräten werden möglicherweise zwei Protokolle gleichzeitig ausgeführt. Das häufigste Beispiel für zwei auf einem Gerät

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ausgeführte Protokolle sind die Protokolle SSH und SNMP. Ein Verhalten kann steuern, welches der beiden Protokolle für bestimmte Geräte untersucht wird. Das Verhalten verhindert dann die Erkundung des jeweils anderen Protokolls.

Verhalten ermöglichen zudem die effiziente Discovery von SSH- und SNMP-Geräten sowie WMI-Geräten, die mit mehreren MID Servern in mehreren Windows-Domänen ausgeführt werden.

Beispiel: Eine Organisation verfügt über zwei Windows-Domänen und verschiedene UNIX-Computer und SNMP-Geräte in ihrem Netzwerk. Die Herausforderung besteht darin, alle Geräte effizient und ohne doppelten Aufwand zu erkennen. Jede Domäne enthält einen Windows MID-Server, der zum Scannen der IP-Adressen aus den beiden in angegebenen Domänen verwendet wird Discovery Zeitplan sowie die SSH- und SNMP-Geräte. Es wird ein Verhalten benötigt, das die Arbeit angemessen aufteilt, um zu vermeiden, dass etwas zweimal gescannt wird. In diesem Beispiel wird davon ausgegangen, dass sich beide Domänen an demselben geografischen Standort befinden und dass ein einzelner Zeitplan ausreicht.

Hinweis: Die bevorzugte Methode für die Ausführung von Discovery über mehrere Windows-Domänen hinweg besteht in der Verwendung von PowerShell. Damit kann sich ein einzelner MID Server auf Computern in verschiedenen Domänen mit für die Instanz gespeicherten Anmeldeinformationen authentifizieren.

Discovery-Verhalten erstellen

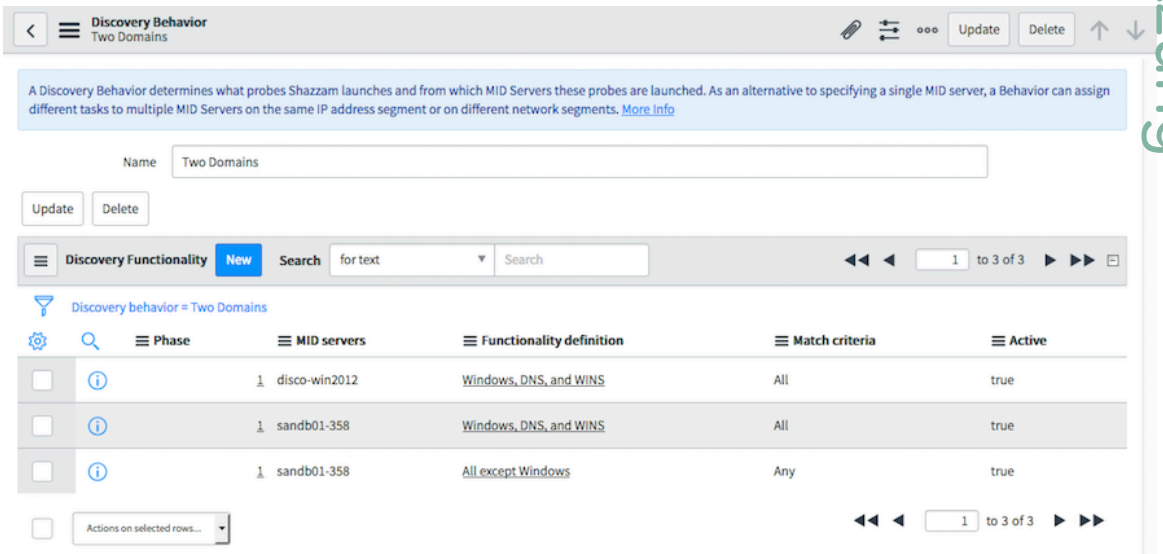
Erstellen Sie ein Discovery-Verhalten, um festzulegen, welche Probes von Shazzam gestartet werden und welcher MID Server verwendet wird.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Verhalten** Und klicken Sie auf **Neu** .
2. Geben Sie einen Namen ein.
3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.



4. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Die Funktionalität definiert, was jeder MID-Server in diesem Verhalten tun muss, insbesondere welche Protokolle erkannt werden sollen.

5. Füllen Sie die Formularfelder folgendermaßen:

Feld	Beschreibung
Phase	Geben Sie eine ganze Zahl ein, die eine beliebige Phase darstellt. Die Phase wird verwendet, um eine oder mehrere Funktionalitäten zu gruppieren. Alle Funktionalitäten innerhalb einer bestimmten Phase werden gemeinsam ausgeführt, und alle Phasen werden in numerischer Reihenfolge ausgeführt. Alle Funktionalitäten in einem Verhalten können dieselbe Phase aufweisen. Die Shazzam-Probe wird einmal für jede Phase in einem Verhalten ausgeführt, weswegen eine geringere Anzahl von Phasen wünschenswert ist. Führen Sie mehrere Verhaltensphasen nur aus, wenn Geräte im Netzwerk mehrere Protokolle wie SSH und SNMP ausführen. In diesem Beispiel legen Sie eine Phase für den SSH-Scan und eine weitere Phase für den SNMP-Scan fest.
Aktiv	Lassen Sie diese Option ausgewählt, um die Discovery-Funktionalität anzuwenden.
Funktionalitätsdefinitionen	Klicken Sie auf das Suchsymbol, und wählen Sie dann eine vorkonfigurierte Funktionalität aus, die das Protokoll oder die Liste der von jedem MID Server gescannten Protokolle definiert.
Kriterien anpassen	Definieren Sie hier Kriterien für MID Server unter Windows.
MID Server	Wählen Sie mindestens einen MID Server aus, um diese Funktionalität für die folgenden Discovery-Typen auszuführen: ○ IP-Scan ○ CI-Scan Discovery gleicht die Last automatisch aus, wenn mehrere MID Server ausgewählt werden.

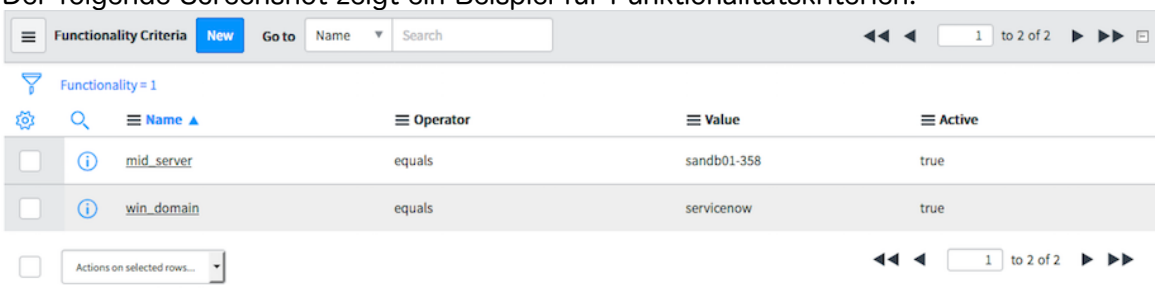
6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Um Kriterien hinzuzufügen, die erfüllt sein müssen, damit die Funktionalität ausgelöst wird, klicken Sie in der zugehörigen Liste „Funktionalitätskriterien“ auf **Neu**, füllen die Formularfelder aus und klicken dann auf **Senden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Name	Der Name im Kriterium entspricht der Variablen, die die folgenden Informationen übergibt: ○ mid_server: Der MID Server, der die Ergebnisse der Shazzam-Probe verarbeitet ○ win_domain: Die Windows-Domäne des Zielgeräts
Operator	Wählen Sie einen logischen Operator aus.
Wert	Geben Sie den tatsächlichen Namen des MID Servers (mid_server) oder der Domäne (win_domain) ein, der/die für dieses Kriterium an Discovery übergeben werden soll. Dieses Feld kann auch den Wert mid_domain enthalten, der die Windows-Domäne des MID Servers definiert, der die Shazzam-Ergebnisse verarbeitet.

Hinweis: Funktionalitätskriterien sind nur für MID Server unter Windows erforderlich, und das auch nur, wenn das Verhalten Discovery domänenübergreifend steuert. Wenn die Instanz die Shazzam-Probe für eine Discovery startet, in der ein Verhalten mehrere MID Server zum Scannen mehrerer Domänen definiert, bestimmen die Funktionalitätskriterien, welcher MID Server die Ergebnisse der Probe verarbeitet.

Der folgende Screenshot zeigt ein Beispiel für Funktionalitätskriterien.



Nächste Maßnahme

Horizontale Erkennung planen Vom Typ **Konfigurationselement** , Und wählen Sie aus **Verhalten Verwenden** Für die MID-Server-Auswahlmethode.

Lastenausgleichsverhalten einrichten

Wenn mehrere MID-Server so konfiguriert sind, dass dasselbe Protokoll gescannt wird, können Anwender das Lastenausgleichverhalten einrichten, um die Arbeit zwischen MID-Servern automatisch auszugleichen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verhalten ermöglichen einen Lastenausgleich, wenn mehrere MID Server so konfiguriert sind, dass sie dasselbe Protokoll scannen. Beispiel: Eine Organisation hat 50 Remotestandorte, deren Größe zwischen 10 und mehreren Hundert Geräten variiert. Alle Außenstellen sind Teil derselben Windows-Domäne, die von einem zentralen Standort aus verwaltet wird. An diesem zentralen Standort sind drei MID Server installiert: zwei zum Scannen aller Windows-Geräte und einer zum Scannen der verbleibenden Geräte. Da sich einige der Zweigstellen in anderen Zeitzonen befinden, müssen für jede Zeitzone unterschiedliche Zeitpläne zur Ausführung von Discovery außerhalb der Spitzenzeiten erstellt werden. Dasselbe Verhalten kann für jeden Zeitplan verwendet werden, und das Verhalten gleicht die beiden aus Windows MID-Server automatisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie einen Verhaltensdatensatz.

   a. Erstellen Sie eine neue Discovery Verhaltensdatensatz und benennen Sie ihn etwas beschreibendes, z. B. *LoadBalanced* .

   b. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

   Diese Aktion speichert den Datensatz und erstellt im Formular die zugehörige Liste „Discovery-Funktionalität“.

2. Definieren Sie die Windows-Funktionalität.

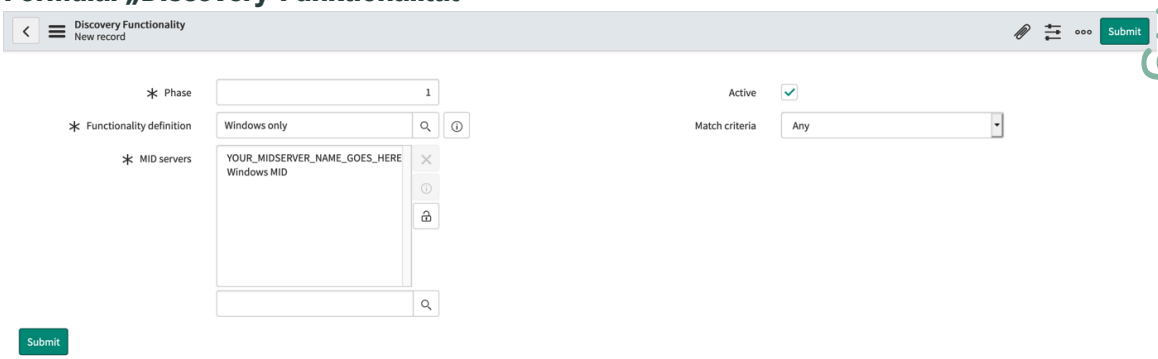
   a. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**.

   b. Erstellen Sie mithilfe der im Folgenden beschriebenen Felder einen neuen Datensatz.

   c. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein.
Funktionalität	Wählen Sie in der Liste *Windows only (WMI) (Nur Windows (WMI))* aus. Diese Funktionalität definiert das Protokoll, das gescannt wird. Da Sie WMI zum Scannen ausgewählt haben, müssen Sie Windows MID Server für diese Funktionalität auswählen.
MID-Server	Wählen Sie die beiden MID-Server aus, die Sie die Last für die WMI-Probes teilen möchten. Wenn Sie mehrere MID-Server in dieses Feld eingeben, sagen Sie dies Discovery Um die Last zwischen diesen Servern automatisch auszugleichen. Wenn Sie für jeden Server separate Funktionen erstellen, erfolgt kein Lastenausgleich.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*.

Formular „Discovery-Funktionalität“



3. Erstellen Sie Funktionalitätskriterien.

Hinweis: Die gesamte Windows-Funktionalität erfordert Kriterien zum Identifizieren der Windows-Domäne und zum Definieren von speziellem Verhalten für die genannten MID Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

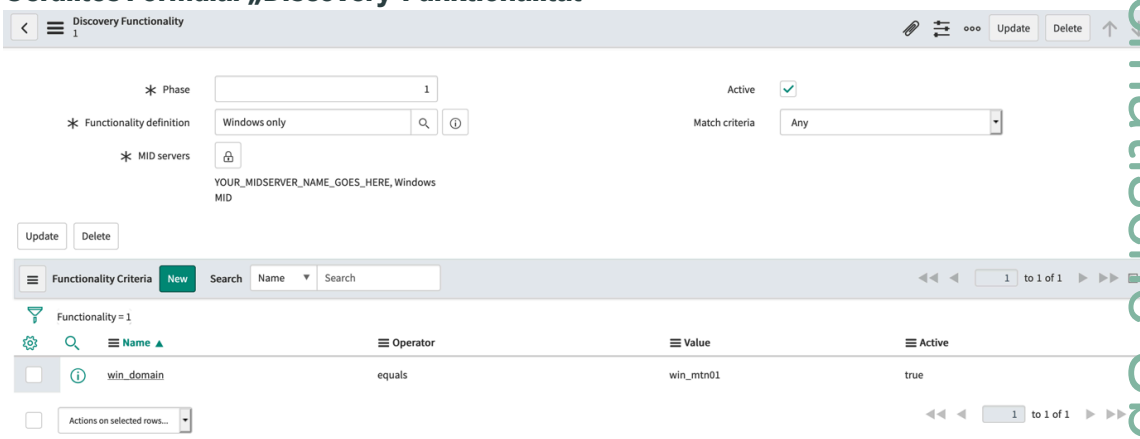
a. Klicken Sie in der zugehörigen Liste auf **Neu**.

b. Geben Sie die folgenden Werte ein:

Feld	Eingabewert
Name	Geben Sie Ein Win_Domain Um zu benennen Windows Domäne, die Discovery Scannt mit den von uns definierten MID-Servern.
Operator	Wählen Sie Aus *Ist gleich* Als Operator.
Wert	Dies ist der Name der Windows-Domäne, die diese MID Server nach Geräten scannen.
Aktiv	Aktivieren Sie die Kriterien, indem Sie dieses Kontrollkästchen aktivieren (`true`).

Die abgeschlossenen Kriterien werden in angezeigt Discovery Formular „Funktionalität“ für Windows MID-Server.

Gefülltes Formular „Discovery-Funktionalität“



4. Definieren Sie die Funktionalität für die restlichen Scans.

Erstellen Sie einen zweiten Datensatz zum Scannen nach allen verbleibenden Protokollen (SSH, SNMP usw.) mit den folgenden Einstellungen:

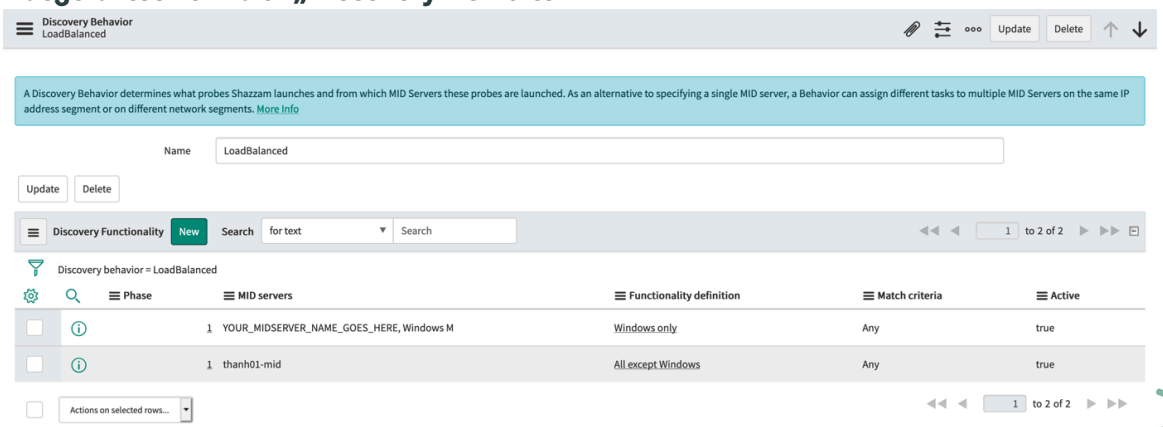
Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein. Diese Phase wird gleichzeitig mit den WMI-Scans und mit derselben Shazzam-Probe ausgeführt. Aus Effizienzgründen verwenden Sie dieselbe Phasennummer, da Sie wissen, dass keines der Geräte in den Ziel-IP-Bereichen mehrere Protokolle (zum Beispiel SSH und SNMP) ausführt. Wenn auf Geräten mehrere Protokolle ausgeführt wurden, geben Sie eine zweite oder sogar eine dritte Phase an, um zuerst das richtige Protokoll für jedes Gerät zu erkennen.
Funktionalität	Wählen Sie in der Liste *All except Windows (no WMI) (Alle außer Windows (kein WMI))* aus. Diese Funktionalität veranlasst den MID Server, alle verbleibenden Protokolle zu scannen, nachdem Discovery die WMI-Scans ausgeführt hat.
MID Server	Geben Sie den Namen des MID Servers ein, der nach allen anderen Geräten scannt. Wenn Sie den automatischen Lastenausgleich verwenden möchten, können Sie diesem Feld einen zusätzlichen MID Server hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das ausgefüllte Formular „Discovery-Verhalten“ sieht wie folgt aus. Für diesen MID Server müssen keine Funktionalitätskriterien erstellt werden.

Ausgefülltes Formular „Discovery-Verhalten“



5. Erstellen Sie einen Discovery-Zeitplan Für jede Zeitzone und benennen Sie das gerade erstellte Verhalten.

a. Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und klicken Sie auf **Neu** In der Datensatzliste.

b. Wählen Sie im Feld **Erkennen** den Typ *Konfigurationselemente* aus.

c. In **MID-Server-Auswahlmethode** Feld auswählen *Verhalten Verwenden*
Mit dieser Aktion wird angezeigt **Verhalten** Feld.

d. Klicken Sie auf das Lupensymbol, und wählen Sie das zu verwendende Verhalten aus.
Wählen Sie in diesem Beispiel aus *LoadBalanced* .

e. Wählen Sie den entsprechenden Zeitpunkt zum Ausführen von Discovery für diesen Standort aus.

f. Klicken Sie auf **Kurzbereiche**, und definieren Sie die IP-Adressbereiche, Netzwerke und Listen, die für diesen Standort durchsucht werden sollen.

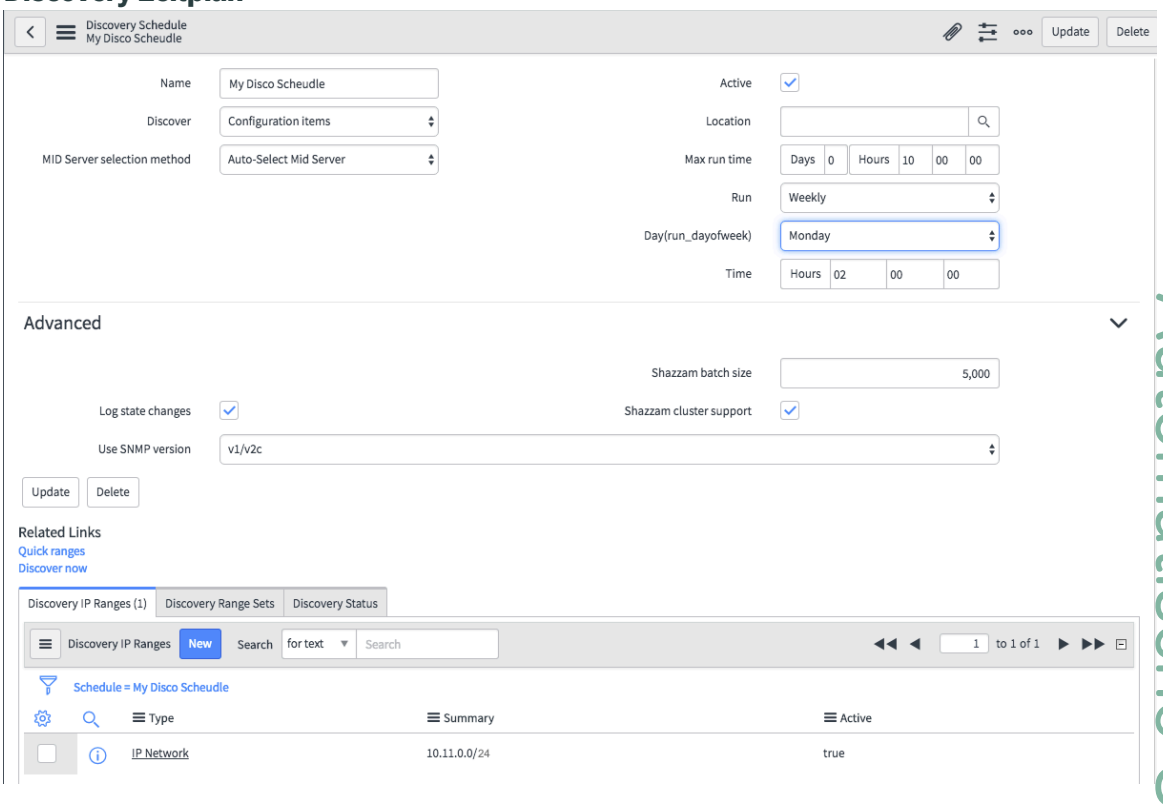
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Speichern Sie den Datensatz.

h. Erstellen Sie zusätzliche Zeitpläne für jede Zeitzone oder Region im Netzwerk, und wählen Sie dasselbe Verhalten aus.

Discovery Zeitplan



Beispiele für Funktionalitäten eines Discovery-Verhaltens

Dieses Beispiel für ein Discovery-Verhalten erfordert drei Funktionalitäten für das Verhalten.

Für dieses Verhalten erstellen Sie die folgenden drei Funktionalitäten: einen MID Server zum Scannen von Domäne A nur für Windows-Geräte, eine zweite Funktionalität für denselben MID Server zum Scannen nach allen SSH- und SNMP-Geräten und eine dritte Funktionalität, die einen zweiten MID Server benennt, der Domäne B nach Windows-Geräten scannt. Die Begründung hierfür lautet wie folgt:

- Ein MID Server unter Windows kann nur Windows-Computer in der Windows-Domäne erkennen, der er angehört. Dies liegt einzig und allein an der Funktionsweise der Windows-Authentifizierung. Aus diesem Grund wird eine WMI-Funktionalität für jede Domäne benötigt.
- Ein MID Server kann unter Windows mit den richtigen Anmeldeinformationen SSH- und SNMP-Geräte überall erkennen. WMI-, SSH- und SNMP-Funktionalitäten können jedoch nicht über Windows-Domänen kombiniert werden. Das liegt daran, dass die Funktionalitätskriterien für WMI-Scans die Discovery auf eine bestimmte Domäne beschränken. Aus diesem Grund erfordern die SSH- und die SNMP-Erkennung jeweils eine eigene Funktionalität.
- Jeder Computer soll nur einmal gescannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionalität 1: WMI-Scan auf Domäne A

Sie konfigurieren einen MID Server zum Scannen nach dem WMI-Protokoll auf Domäne A. WMI-Scans authentifizieren sich auf Windows-Computern mit den Domänenanmeldeinformationen des MID Server-Computers unter Windows. MID Server können unter Windows nicht außerhalb ihrer eigenen Domänen nach dem WMI-Protokoll suchen.

Erstellen Sie die erste Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer **1** in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **Windows, DNS und WINS** aus. Diese Funktionalität definiert das WMI-Protokoll, das gescannt wird, und löst die Domäne auf. Da Sie sich dafür entschieden haben, nach WMI zu scannen, müssen Sie für diese Funktionalität einen Windows-MID Server auswählen.
MID Server	Wählen Sie einen Windows-MID Server aus Domäne A aus, in diesem Fall **sandb01-358**.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in **Alle**.

Funktionalitätskriterien erstellen

Alle Windows-Funktionalitäten erfordern Kriterien zum Identifizieren der Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt. Klicken Sie zum Erstellen von Funktionalitätskriterien in der zugehörigen Liste auf **Neu**, und geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in Domäne A durchführt:

Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: • Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans in Domäne A ausführt. • Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium **ist gleich** als Operator aus.
Wert	• Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne A auf Windows-Geräte scannt. • Geben Sie für den Wert *win_domain* den Namen der Domäne A ein, die dieser MID Server nach Windows-Geräten scannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (true) aktivieren.

Die festgelegten Kriterien werden im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Funktionalität 2: SSH und SNMP

Sie möchten in Ihrem Netzwerk nach UNIX-Computern und -Netzwerkgeräten scannen, diese aber Geräte nicht zweimal klassifizieren. Einer Ihrer MID Server ist so konfiguriert, dass er SSH und SNMP mit einer anderen Funktionalität klassifiziert, als für WMI-Scans verwendet wird. Sie müssen keine Kriterien für Nicht-WMI-Funktionalität erstellen.

Erstellen Sie die zweite Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **All except Windows (no WMI) (Alle außer Windows (kein WMI))** aus. Diese Funktionalität scannt nur nach den Protokollen SSH und SNMP.
MID Server	Wählen Sie den MID Server aus Domäne A aus, in diesem Fall **sandb01-358**.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*. Für Nicht-WMI-Funktionalitäten werden keine Kriterien verwendet.

Funktionalität 3: WMI-Scan auf Domäne B

Damit müssen Sie nur noch eine Funktionalität für die WMI-Scans in Domäne B erstellen. Aufgrund des Windows-Authentifizierungsmechanismus müssen Sie einen Windows-MID Server zum Scannen von Domäne B konfigurieren, der ein Mitglied dieser Domäne ist.

Erstellen Sie die dritte Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **Windows, DNS und WINS** aus. Diese Funktionalität definiert das WMI-Protokoll, das gescannt wird, und löst die Domäne auf. Da Sie sich dafür entschieden haben, nach WMI zu scannen, müssen Sie für diese Funktionalität einen Windows-MID Server auswählen.
MID Server	Wählen Sie einen Windows-MID Server aus Domäne B aus, in diesem Fall **disco-win2003**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in *Alle*.

Funktionalitätskriterien erstellen

Alle Windows-Funktionalitäten erfordern Kriterien zum Identifizieren der Windows-Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt. Klicken Sie zum Erstellen von Funktionalitätskriterien in der zugehörigen Liste auf **Neu**, und geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in Domäne B durchführt:

Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: • Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans in Domäne B ausführt. • Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium **ist gleich** als Operator aus.
Wert	• Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne B auf Windows-Geräte scannt. • Geben Sie für den Wert *win_domain* den Namen der Domäne B ein, die dieser MID Server nach Windows-Geräten scannt.
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (true) aktivieren.

Die festgelegten Kriterien werden im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Beispiel für Discovery-Verhalten: Auf ACL-geschütztes SNMP-Gerät zugreifen

Greifen Sie mit auf ein SNMP-Gerät zu, das durch eine ACL geschützt ist Discovery Verhalten.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Eine bestimmte Art von Zugriffssteuerungsliste (ACL) auf einem SNMP-Gerät kann verhindern, dass Discovery dieses Gerät identifiziert. Diese Liste definiert Hostcomputer anhand von IP-Adressen, die zum Ausführen von Agents auf SNMP-Geräten zugelassen sind. In diesem Beispiel sollen alle Geräte in einem IP-Bereich klassifiziert, identifiziert und aktualisiert werden, einschließlich der durch eine ACL geschützten SNMP-Geräte. Dazu müssen ein MID Server mit Zugriff auf die geschützten SNMP-Geräte installiert und ein Verhalten erstellt werden, mit dem nach allen Protokollen gescannt werden kann, sodass alle Geräte gefunden werden und keine zusätzliche Arbeit anfällt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Installieren Sie einen MID Server auf einem von der ACL zugelassenen Host.

   Zum Scannen der SNMP-Geräte in einem durch eine ACL geschützten Netzwerk muss ein MID Server auf einem Hostcomputer installiert werden, für den anhand der IP-Adresse in der ACL angegeben ist, dass er über Zugriff auf die SNMP-Geräte verfügt. Da dieser MID Server nur SNMP-Geräte scannt, kann er auf jedem unterstützten Betriebssystem installiert werden. Der andere MID Server, der zur Erkennung von WMI und SSH konfiguriert ist, kann auf jedem Windows-Host installiert werden, für den die angegebenen IP-Bereiche sichtbar sind.

2. Installieren Sie zusätzliche MID Server, wenn Sie eine dieser Funktionen für den Lastenausgleich konfigurieren möchten.

3. Erstellen Sie einen Verhaltensdatensatz.

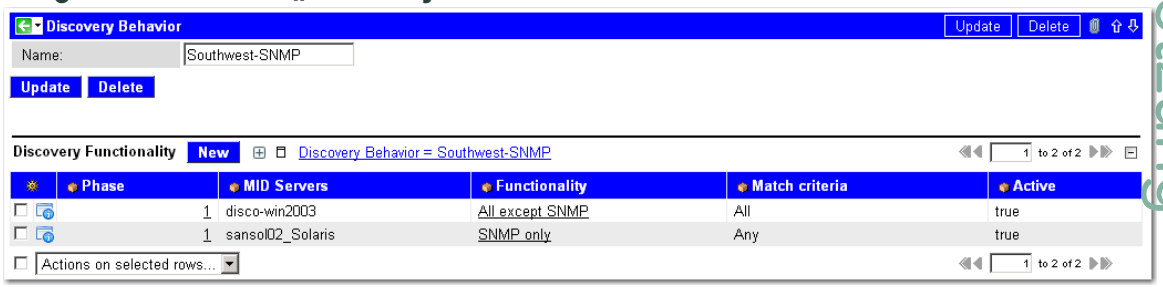
   a. Erstellen Sie einen neuen Discovery-Verhaltensdatensatz, und geben Sie ihm einen beschreibenden Namen wie *Southwest-SNMP*.

   b. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.
   Diese Aktion speichert den Datensatz und erstellt im Formular die zugehörige Liste „Discovery-Funktionalität“.

   c. Um dieses Verhalten abzuschließen (wie in Abbildung 1 gezeigt), müssen Sie Funktionalitäten mit den MID Servern erstellen, die Sie zu diesem Zweck installiert haben.

   Für die Funktionalität, die nach dem WMI-Protokoll scannt, müssen Sie Kriterien definieren, die die Windows-Domäne und den verwendeten MID Server angeben. Da diese Discovery auf einer Windows-Domäne ausgeführt wird, können Sie eine Funktionalität für WMI und SSH (**All except SNMP (Alle außer SNMP)**) mit demselben MID Server konfigurieren.

Ausgefülltes Formular „Discovery-Verhalten“



4. Definieren Sie die Funktionalitäten.
   Erstellen Sie für dieses Verhalten zwei Funktionalitäten: eine für SNMP auf dem MID Server, der auf dem in der ACL angegebenen Host installiert ist, und eine weitere für WMI und SSH auf einem zweiten MID Server.

   a. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**, um Funktionalitäten hinzuzufügen.

   b. **Hinweis:** Konfigurieren Sie den auf dem berechtigten Hostcomputer installierten MID Server so, dass er nur nach dem SNMP-Protokoll scannt.

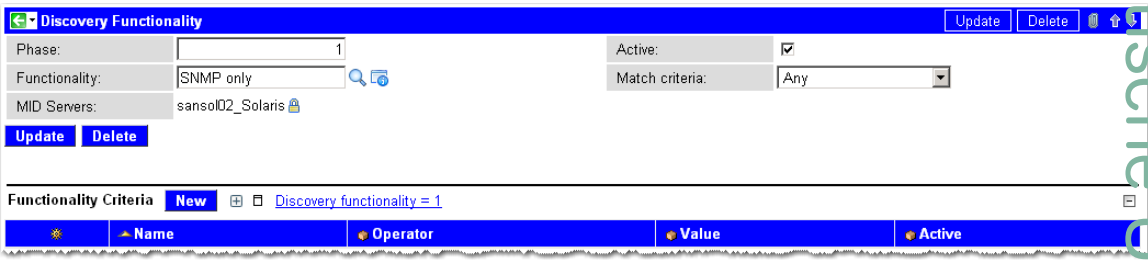
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie die erste Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein. Beide Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste *Nur SNMP* aus. Diese Funktionalität definiert das Protokoll, das gescannt wird.
MID Server	Wählen Sie einen MID Server (*sansol02_Solaris*) aus, der auf einem Solaris-Host installiert ist und dem durch die ACL Zugriff auf die SNMP-Geräte gewährt wird. Wenn Discovery einen automatischen Lastenausgleich für diese Funktionalität ausführen soll, können Sie mehrere MID Server auswählen.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*. Für SNMP-Funktionalitäten werden keine Kriterien verwendet.

Nur nach SNMP scannen



c. **Hinweis:** In der zweiten Funktionalität scannt Discovery Ihre Domäne nach den Protokollen WMI und SSH. Da WMI eines der Protokolle ist, muss der MID Server für diese Funktionalität auf einem Windows-Computer installiert sein und über Kriterien verfügen.

Erstellen Sie die zweite Funktionalität mit den folgenden Werten:

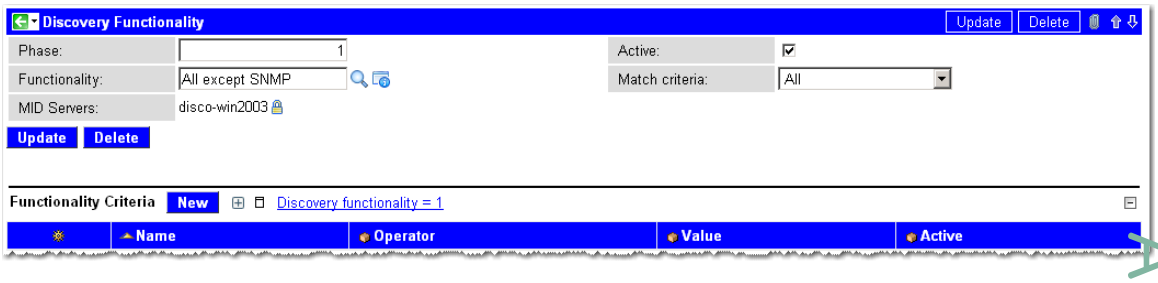
Feld	Eingabewert
Phase	Geben Sie Phasennummer 1 in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Protokoll-Scans gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste *All except SNMP (Alle außer SNMP)* aus. Diese Funktionalität definiert die Protokolle, nach denen gescannt wird. Da WMI eines der ausgewählten Protokolle ist, müssen Sie einen Windows-MID Server für diese Funktionalität verwenden.
MID Server	Wählen Sie einen Windows-MID Server in Ihrer Domäne aus. In diesem Fall wählen Sie *disco-win2003* aus. Wenn Discovery einen automatischen Lastenausgleich für diese Funktionalität ausführen soll, können Sie mehrere MID Server auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in *Alle*.

Nach allen außer SNMP scannen



d. **Hinweis:** Funktionalitäten, die nach WMI scannen, erfordern Kriterien zum Identifizieren der Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt.

Um Funktionalitätskriterien für einen WMI-Scan zu erstellen, klicken Sie in der zugehörigen Liste auf **Neu**.

e. Geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in unserer Domäne durchführt:

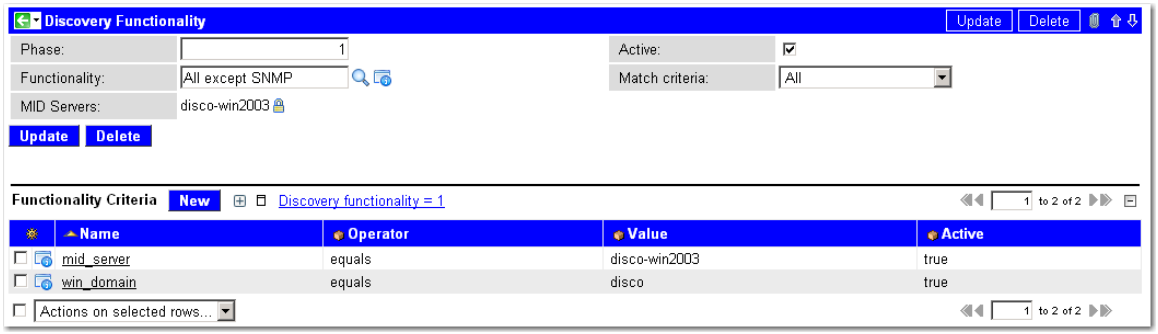
Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: ▪ Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans ausführt. ▪ Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium *ist gleich* als Operator aus.
Wert	▪ Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne B auf Windows-Geräte scannt. ▪ Geben Sie für den Wert *win_domain* den Namen Ihrer Windows-Domäne ein.
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (`true`) aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die festgelegten Kriterien werden wie folgt im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Funktionalitätskriterien für WMI-Scans



5. Erstellen Sie den Zeitplan.

   a. Erstellen Sie einen Discovery-Zeitplan, und benennen Sie das soeben erstellte Verhalten.

   b. Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und klicken Sie auf **Neu** In der Datensatzliste.

   c. Wählen Sie im Feld **Erkennen** den Modus *Konfigurationselemente* aus.
   Mit dieser Aktion wird angezeigt **Verhalten** Feld.

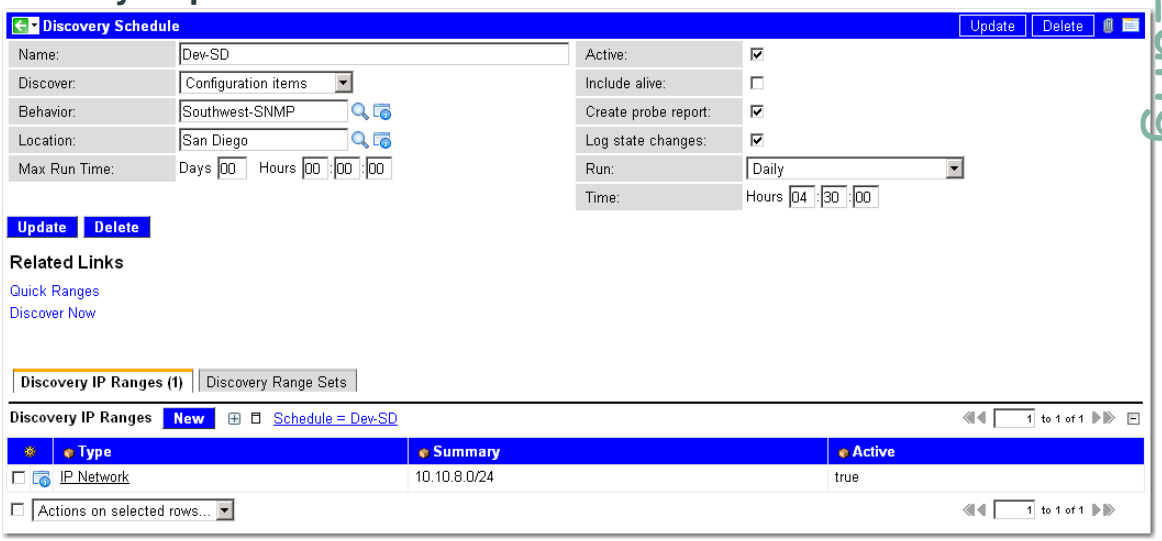
   d. Klicken Sie auf das Lupensymbol, und wählen Sie das zu verwendende Verhalten aus.
   Wählen Sie in diesem Beispiel *Southwest-SNMP* aus.

   e. Wählen Sie den entsprechenden Zeitpunkt zum Ausführen von Discovery für diesen Standort aus.

   f. Klicken Sie auf **Kurzbereiche**, und definieren Sie die IP-Adressbereiche, Netzwerke und Listen, die für diese Domäne gescannt werden sollen.

   g. Speichern Sie den Datensatz.

Discovery-Zeitplandatensatz



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Löschstrategien für Mustererkennung

Wenn Sie eine Discovery mit einem Muster durchführen, können Sie auswählen, was mit Konfigurationselementen (Configuration Items, CIs) geschehen soll, die sich in der CMDB befinden, aber Discovery Kann nicht mehr gefunden werden.

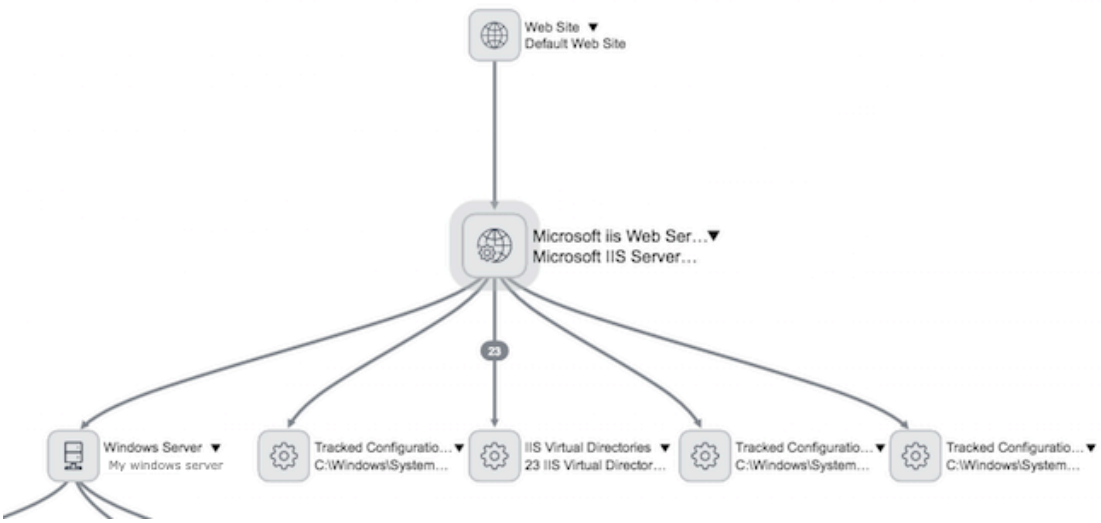
Hinweis: Löschstrategien sind nur mit Mustern verfügbar, nicht mit Probes/Sensoren.

Wenn Sie ein Muster zum Ausführen der Discovery verwenden, identifizieren Sie einen CI-Typ, der der ist *Haupt-CI* Sie versuchen zu finden, z. B. einen IIS-Webserver oder Tomcat-Server. Discovery Kann auch finden *Zugehörige CIs* Und füllen Sie die CMDB entsprechend aus. Zum Beispiel nach Discovery Findet einen IIS-Server mit dem IIS-Muster. Er kann auch diese zugehörigen CIs finden:

- Den Windows-Computer, der den Webserver hostet
- Die Konfigurationsdateien für den IIS-Server
- Die Website, die der IIS-Server hostet

Die Abhängigkeitszuordnung zum Haupt-CI zeigt auch die zugehörigen CIs an, wie in der folgenden Grafik dargestellt:

Beispiel für ein Haupt-CI des IIS-Servers und die zugehörigen CIs

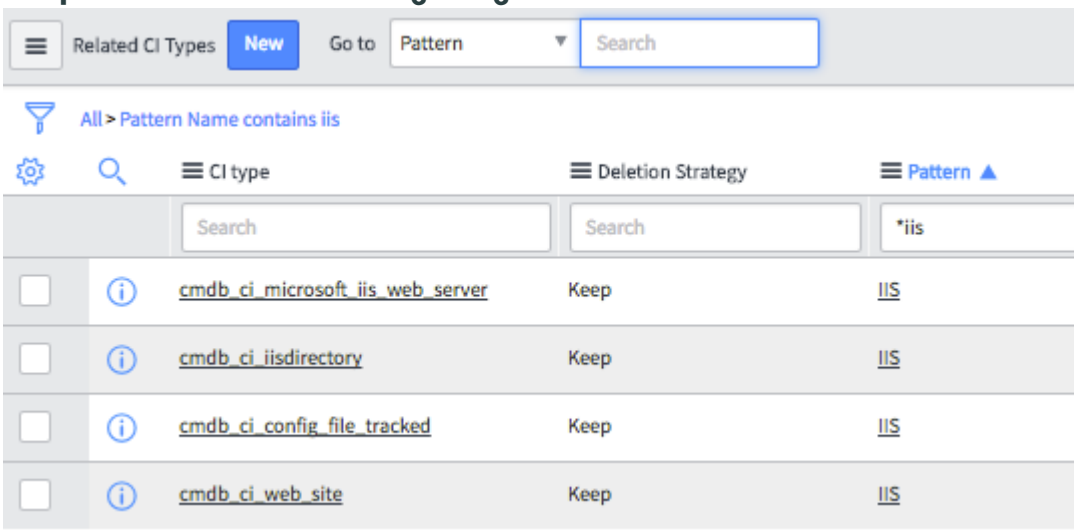


Nachdem Sie das Haupt-CI und die zugehörigen CIs zum ersten Mal mithilfe eines Musters erkannt haben, müssen Sie manuell einen Eintrag in der Tabelle „zugehörige CI-Typen“ [sa_ci_to_pattern] für jede Beziehung zwischen dem Haupt-CI und einem zugehörigen CI-Typ konfigurieren. In diesen Datensätzen bestimmen Sie die Löschstrategie für jedes zugehörige CI basierend auf seinem Typ. Beachten Sie, dass Sie keine Löschstrategie für das Haupt-CI für den Mustertyp „Infrastruktur“ festlegen können.

Sie können eine Liste der Beziehungen anzeigen, wie in der folgenden Abbildung dargestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für zu einem IIS-Server gehörige CIs



Die Löschungsstrategie für zugehörige CIs wird wirksam, wenn die beiden folgenden Bedingungen zutreffen:

- Nachdem Sie ausgeführt haben Discovery Mit dem Muster erneut.
- Discovery erkennt das Haupt-CI erfolgreich, aber nicht das zugehörige CI.

Für die Löschungsstrategie sind die folgenden Optionen verfügbar:

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** , Bedeutet das Discovery Die nachverfolgte Konfigurationsdatei wurde nicht gefunden. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen. **Hinweis:** Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Stillgelegt** , Bedeutet das Discovery Verwendet diese Konfigurationsdatei nicht mehr. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Hinweis: Löschstrategien sind für zugehörige Einträge nicht verfügbar, bei denen es sich um Regeln handelt, die auf zugehörigen CIs basieren. Weitere Informationen finden Sie unter Zugehörige Einträge .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Löschungsstrategie festlegen

Legen Sie eine Löschstrategie fest, wenn Sie Aktionen für ein zugehöriges Konfigurationselement (CI) ausführen möchten, das Discovery Kann nicht mehr über Muster-Discovery gefunden werden. Sie können das Haupt-CI nur löschen, wenn es sich um einen Mustertyp „Anwendung“ oder „Cloud-Ressource“ handelt.

Vorbereitungen

- CIs: Ein Haupt-CI und zugehörige CIs, die im Erkennungsprozess bei der Mustererkennung erkannt wurden
- Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Löschungsstrategien für alle erkannten CIs festlegen, einschließlich Konfigurationsdatei-CIs. Die Art und Weise, wie Sie auf die Löschstrategie für nachverfolgte Konfigurationsdateien zugreifen, unterscheidet sich jedoch vom Verfahren in diesem Thema. Siehe Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen für Anweisungen.

Prozedur

1. Öffnen Sie die Liste der zugehörigen CI-Typen, indem Sie `sa_ci_to_pattern.list` im Anwendungsfilter eingeben.
2. Filtern Sie die Liste, um den CI-Typ zu finden, der durch die Mustererkennung einem Haupt-CI zugehörig ist. Wenn Sie eine Löschungsstrategie für eine Cloud-Datenbank festlegen möchten, durchsuchen Sie die Liste nach dem CI-Typ *`cmdb_ci_cloud_database`*.

   Beachten Sie, dass für die CI-Typen *`cmdb_ci_cloud_database`* der Wert **Ist-Haupt-CI** auf **true** festgelegt ist. Das gibt an, dass Sie eine Löschungsstrategie für AWS- und Azure-Datenbanken festlegen können, selbst wenn es sich dabei um das Haupt-CI handelt, das durch die Cloud-Erkennung erkannt wird.

CI type	Deletion Strategy	Is Main CI ▼	Pattern
cmdb_ci_cloud_database	Mark as Absent	true	Amazon AWS Relational Database Service
cmdb_ci_cloud_database	Mark as Absent	true	Azure DataBase

3. Doppelklicken Sie in der Listenansicht auf den Wert im entsprechenden Feld in der Spalte **Löschungsstrategie**.
4. Wählen Sie einen neuen Wert aus:

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** , Bedeutet das Discovery Die nachverfolgte Konfigurationsdatei wurde nicht gefunden. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
	Hinweis: Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Stillgelegt** , Bedeutet das Discovery Verwendet diese Konfigurationsdatei nicht mehr. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Konfigurationsdateien nachverfolgen

Bei der horizontalen Erkennung können Konfigurationsdateien, die zu bestimmten Anwendungen gehören, erkannt und der CMDB hinzugefügt werden. Sie können die Änderungen an diesen Dateien nachverfolgen, indem Sie sie mit vorherigen Versionen vergleichen.

Warnung: Konfigurationsdateien enthalten sensible Systeminformationen. Um nicht autorisierten Zugriff zu verhindern, stellen Sie sicher, dass in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] Zugriffssteuerungslisten (ACL) platziert sind. Erlauben Sie nur autorisierten Benutzern, diese Tabelle anzuzeigen, oder deaktivieren Sie die Einstellung **Inhalt speichern**.

Komponenten zum Nachverfolgen der Konfigurationsdatei

CI-Typ

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden.In einem Basissystem sind für viele CI-Typen Konfigurationsdateipfade vorgegeben. Sie können neue Definitionen für die Nachverfolgung von Konfigurationsdateien hinzufügen oder ändern. Siehe Nachverfolgung von Changes in Konfigurationsdateien ändern für Anweisungen.

Muster

Die Nachverfolgung der Konfigurationsdatei ist für Muster verfügbar, die Anwendungen erkennen. Für das Muster können Sie Definitionen zur Dateinachverfolgung erstellen, die den CI-Typ angeben, zu dem das Anwendungs-CI gehört, sowie den Pfad der Konfigurationsdatei. Geben Sie so viele Definitionen für die Nachverfolgung von Dateien an wie nötig. Sie können auch angeben, ob Sie den Inhalt von Konfigurationsdateien speichern möchten, damit Sie den Inhalt verschiedener Versionen anzeigen und vergleichen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Die Nachverfolgung der Konfigurationsdatei ist nicht für Erkennungen verfügbar, die mit traditionellen Probes und Sensoren durchgeführt werden.

Die Klassifizierung, die das Muster auslöst, muss die Probe „Horizontal Pattern“ angeben, der wiederum das Muster angeben muss. Wenn Sie ein Upgrade Ihrer Instanz auf die aktuelle Version durchführen, sind nicht alle Klassifizierer so konfiguriert, dass sie für die Erkennung standardmäßig Muster verwenden.

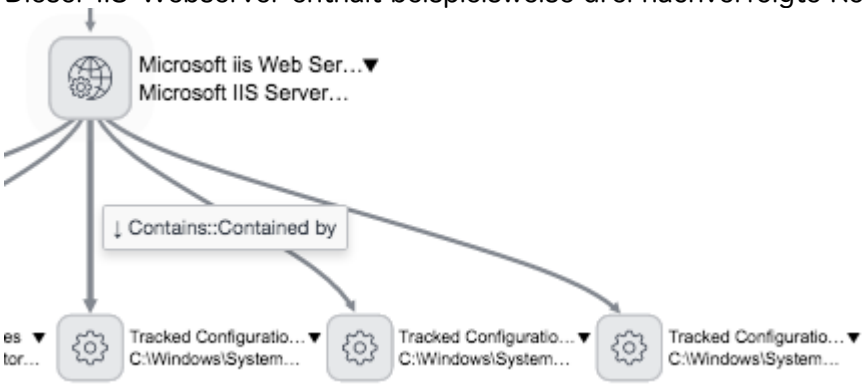
CMDB

Alle Konfigurationsdateien werden als CI in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] gespeichert. Wenn Sie das Speichern des Inhalts aktivieren, enthalten diese CI-Datensätze den Inhalt der Konfigurationsdateien, einschließlich vorheriger Versionen. Im CI-Datensatz der Konfigurationsdatei können Sie verschiedene Versionen vergleichen.

Abhängigkeitszuordnungen und Anwendungsservice-Zuordnungen

Sowohl Abhängigkeitsübersichten als auch Serviceinstanz zuordnungen zeigen nachverfolgte Konfigurationsdateien an. Die Beziehung zwischen einer Konfigurationsdatei und ihrem Host ist eine *Beziehung vom Typ „Enthält“*. Die Anwendung enthält die Konfigurationsdatei.

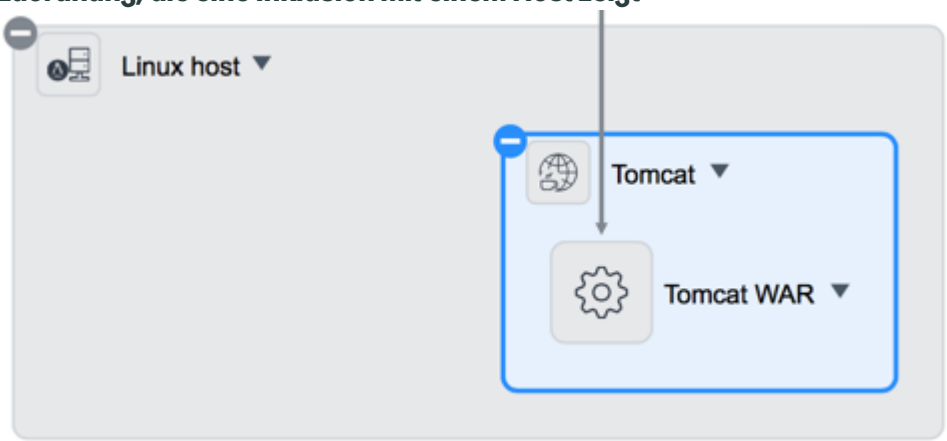
Dieser IIS-Webserver enthält beispielsweise drei nachverfolgte Konfigurationsdateien:



Manchmal organisieren Sie CI-Typen als Haupt-CI-Typ und seine zugehörigen CI-Typen. In einer Serviceinstanzzuordnung Service-Mapping Zeigt Änderungen an Konfigurationsdateien zugehöriger CIs für die Haupt-CIs in Einschlüssen an. Bei Inklusionen behandelt das System auf einem Server gehostete Anwendungen als unabhängige Objekte. Die Tomcat-WAR-CI wird beispielsweise getrennt von ihrem Host, den Tomcat-CIs, angezeigt. In diesem Fall zeigt Service-Mapping Änderungen an Konfigurationsdateien von Tomcat WAR an, wenn Sie Tomcat auswählen. Zusätzlich zeigt Service-Mapping Änderungen an Konfigurationsdateien des Hardware-Servers an, der Inklusionen hostet. In diesem Beispiel handelt es sich um einen Linux-Server:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnung, die eine Inklusion mit einem Host zeigt



Löschungsstrategie

Sie können angeben, was Sie mit den CI-Datensätzen nachverfolgter Konfigurationsdateien tun möchten, wenn sie bei der Erkennung nicht mehr erkannt werden. Sie können den CI-Datensatz der Konfigurationsdatei beibehalten, automatisch löschen, nur die CI-Beziehungen löschen oder als abwesend markieren.

Erkennungsmuster, die die Nachverfolgung von Konfigurationsdateien standardmäßig unterstützen

Die folgenden Muster bieten standardmäßig Definitionen von nachverfolgten Dateien:

Klassifizierun	Muster	CI-Typ	Dateipfad der nachverfolgten Datei
Apache-Server	Apache On Unix Apache On Windows	Apache-Webserver [cmdb_ci_apache_web_server]	$config_file
MySQL-Server	MySQL server On Windows and Linux	MySQL-Instanz [cmdb_ci_db_mysql_instance]	$config_file
Microsoft IIS Server	IIS	Microsoft IIS-Webserver [cmdb_ci_microsoft_iis_web_ser	EVAL(javascript: var rtrn = '';var winDir = CTX.getCommandManager().shellCommand("echo %WinDir%", false, null, null, CTX);rtrn = winDir.trim() + '\\System32\\Inetsrv\\Config*.config';)
		Virtuelles IIS-Verzeichnis [cmdb_ci_iisdirectory]	$install_directory + "*.config"
TIBCO BusinessWorks und EMS	ActiveMatrix BusinessWorks	ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]	$config_file
	Enterprise Message Service	Tibco Enterprise Message Service [cmdb_ci_appl_tibco_message]	$config_file

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierun	Muster	CI-Typ	Dateipfad der nachverfolgten Datei
Oracle	Oracle DB on Windows	Oracle-Instanz [cmdb_ci_db_ora_instance]	$install_directory + "\network\admin *.ora"
		Oracle-Instanz [cmdb_ci_db_ora_instance]	$install_directory + "\dbs*.ora"
	Oracle DB on Unix	Oracle-Instanz [cmdb_ci_db_ora_instance]	$install_directory + "/dbs/*.ora"
		Oracle-Instanz [cmdb_ci_db_ora_instance]	$install_directory + "/network/admin/ *.ora"
Tomcat	Tomcat	Tomcat [cmdb_ci_app_server_tomcat]	$install_directory + "/conf/server.xml"
		Tomcat WAR [cmdb_ci_app_server_tomcat_w	$install_directory + "/WEB-INF/ web.xml"
WMB	WMB On Unix	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	$install_directory + "/*/etc/config/ */*.prop"
	WMB On Windows	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	$install_directory + "*\etc\config* *.prop"
WMQ	WMQ On Windows	IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]	$install_directory + "*\config*"
	WMQ On Windows	IBM MQ-Manager [cmdb_ci_appl_ibm_wmq]	$install_directory + "/bin/*.sh"

Beschreibung

1. Aktivieren Sie die Nachverfolgung von Konfigurationsdateien, indem Sie die Discovery-Eigenschaft glide.discovery.enable_file_tracking auf „true“ setzen.

   Sie können auch andere Eigenschaften konfigurieren, um die Größe und Anzahl der nachverfolgten Konfigurationsdateien, das Zeitfenster, in dem Änderungen an Konfigurationsdateien für eine bestimmte Version nachverfolgt werden, und die Anzahl der zulässigen Änderungen an einer Konfigurationsdatei während dieses Zeitfensters zu steuern. Details siehe Discovery-Eigenschaften.

2. Führen Sie die folgenden Schritte aus, um den unbefugten Zugriff auf sensible Informationen aus Konfigurationsdateien zu verhindern:

   a. Stellen Sie sicher, dass in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] Zugriffssteuerungsregeln (ACL) platziert sind. Erlauben Sie nur autorisierten Benutzern, diese Tabelle anzuzeigen, oder deaktivieren Sie die Einstellung **Inhalt speichern**.

   b. Stellen Sie sicher, dass die Rolle tracked_file_reader, die den Zugriff auf Konfigurationsdateidaten steuert, den richtigen Benutzern und Benutzergruppen zugewiesen ist. Standardmäßig enthält die Rolle itil die Rolle tracked_file_reader, die allen Benutzern mit der Rolle itil Zugriff auf Informationen in Konfigurationsdateien gewährt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Stellen Sie sicher, dass die Probe „Horizontal Discovery“ für den Klassifizierer der zu erkennenden Software aktiviert ist. Falls nicht, können Sie sie aktivieren, das Muster angeben und dann die anderen Probes deaktivieren. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen.
4. Fügen Sie Definitionen von nachverfolgten Dateien hinzu, oder ändern Sie sie, um den CI-Typ oder Dateipfad zu ändern.
5. Definieren Sie die Löschungsstrategie für nachverfolgte Dateien, um festzulegen, was mit den CI-Datensätzen der nachverfolgten Konfigurationsdateien geschehen soll, wenn sie bei der Mustererkennung nicht mehr zu finden sind.
6. Führen Sie eine horizontale Erkennung auf den Hosts aus, auf denen die Anwendungen ausgeführt werden, die Sie mit Mustern erkennen möchten. Öffnen Sie den CI-Datensatz der Anwendung, und überprüfen Sie die zugehörige Liste „Nachverfolgte Konfigurationsdateien“.
7. Vergleichen Sie zwei Versionen von nachverfolgten CI-Konfigurationsdateien, um die tatsächlich vorgenommenen Änderungen anzuzeigen.

Nachverfolgung von Changes in Konfigurationsdateien ändern

Konfigurieren Sie das System, um Informationen zu Änderungen in Konfigurationsdateien zu einem Konfigurationselement (CI) zu sammeln. Service-Mapping Verwendet diese Informationen, um Anwender darüber zu benachrichtigen, dass sich CI-Konfigurationsdateien geändert haben, und um tatsächliche Änderungen an Konfigurationsdateien direkt in den Serviceinstanzzuordnungen anzuzeigen.

Vorbereitungen

Um die Nachverfolgung von Konfigurationsdateien für ein CI zu aktivieren, für das das System Dateien nachverfolgt, konfigurieren Sie die Klassifizierung für den CI-Typ, zu dem dieses CI gehört:

- Für CI-Typen, die Anwendungen darstellen, können Sie für das relevante Muster eine Discovery-Prozessklassifizierung erstellen. Fügen Sie in der Spalte **Probe** die Probe Horizontal Pattern hinzu, und geben Sie Ihr Muster anschließend in der Spalte **Muster** an.
- Führen Sie für CI-Typen, die SNMP-Geräte darstellen, die Konfiguration gemäß der Beschreibung in Discovery-CI-Klassifizierung erstellen durch.

Hinweis: CI-Klassifizierungen für Hosts müssen nicht erstellt werden, da diese Klassifizierungen im Basissystem enthalten sind.

Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Das System verfolgt Konfigurationsdateien als Teil des horizontalen Erkennungsprozesses eines CI, zu dem diese Dateien gehören. Konfigurationsdateien enthalten CI-Einstellungen und -Parameter. Service-Mapping Verwendet diese Informationen, um Anwender darüber zu benachrichtigen, dass sich CI-Konfigurationsdateien geändert haben, und um tatsächliche Änderungen an Konfigurationsdateien direkt in anzuzeigen Serviceinstanz Zuordnungen. Informationen darüber, wie das System Konfigurationsdateien nachverfolgt und wie es Informationen zu diesen Dateien speichert und aktualisiert, finden Sie unter Konfigurationsdateien nachverfolgen.

Für CI-Typen mit Prozessklassifizierern, die Muster auslösen, verfolgt das System Konfigurationsdateien nach. Die Muster enthalten Definitionen für nachverfolgte Dateien. Dies beinhaltet den CI-Typ, zu dem die Anwendung gehört, und den Pfad der Konfigurationsdatei. Mehrere Muster, zum Beispiel das Muster „IIS“, stellen Definitionen für nachverfolgte Dateien standardmäßig bereit. Sie können diese Standarddefinitionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwenden oder für jedes Muster, das von einem Prozessklassifizierer ausgelöst wird, eigene erstellen.

Prozedur

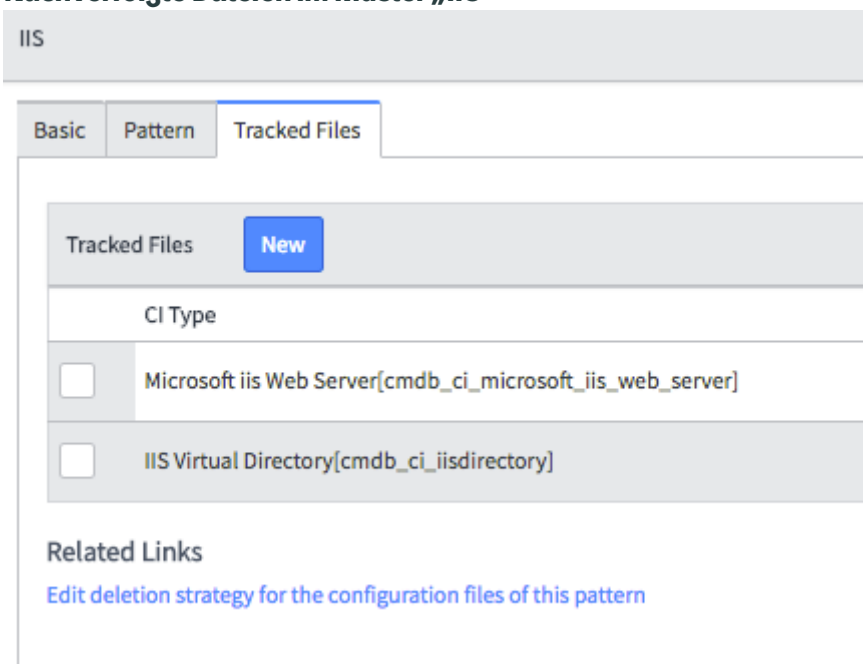
1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf das Muster für das relevante CI.

   Wichtig: Durch die Aktivierung der Nachverfolgung von Konfigurationsdateien wird der Inhalt eines Musters nicht geändert.

3. Klicken Sie auf die Registerkarte **Nachverfolgte Dateien**.
   Für Erkennungsmuster, die die Nachverfolgung von Konfigurationsdateien unterstützen, wird standardmäßig mindestens eine Definition für nachverfolgte Dateien angezeigt.

   Wenn die Registerkarte „Nachverfolgte Dateien“ nicht angezeigt wird, stellen Sie sicher, dass das Muster als Prozessklassifizierer angegeben ist. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen.

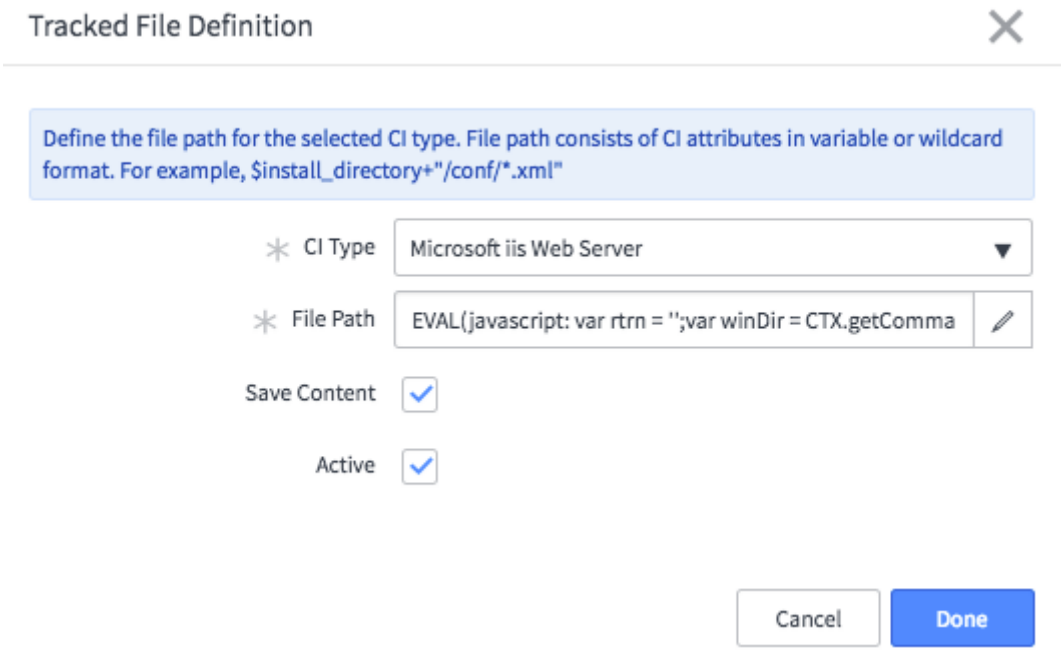
   Nachverfolgte Dateien im Muster „IIS“

4. Klicken Sie auf **Bearbeiten**, um eine vorhandene Definition hinzuzufügen, oder klicken Sie auf **Neu**, um eine neue zu erstellen.
5. Füllen Sie die Formularfelder aus, oder ändern Sie sie (siehe Tabelle):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Definition für nachverfolgte Dateien für die Erkennung von IIS-Servern



Feld	Beschreibung
CI-Typ	Wählen Sie entweder den primären oder den zugehörigen CI-Typ aus, zu dem die Konfigurationsdatei gehört.
Dateipfad	Definieren Sie den Pfad der zu überwachenden Konfigurationsdatei. Sie können Mustervariablen und Platzhalterzeichen verwenden. Zum Beispiel für den folgenden Pfad: <den Ordner mit dem Parameter "Installationsverzeichnis"> / conf / <beliebige XML-Datei>, geben Sie $ Installationsverzeichnis + "/ conf / *. Xml" ein.
Inhalt speichern	Aktivieren Sie dieses Kontrollkästchen, um diese Datei für die Anzeige und den direkten Vergleich mit der ServiceNow-Instanz verfügbar zu machen.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Nachverfolgung dieser Konfigurationsdatei zu aktivieren.

6. Klicken Sie auf **Erledigt**.
7. Legen Sie gegebenenfalls die Löschungsstrategie für nachverfolgte Dateien fest (siehe Beschreibung in Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen).

Nächste Maßnahme

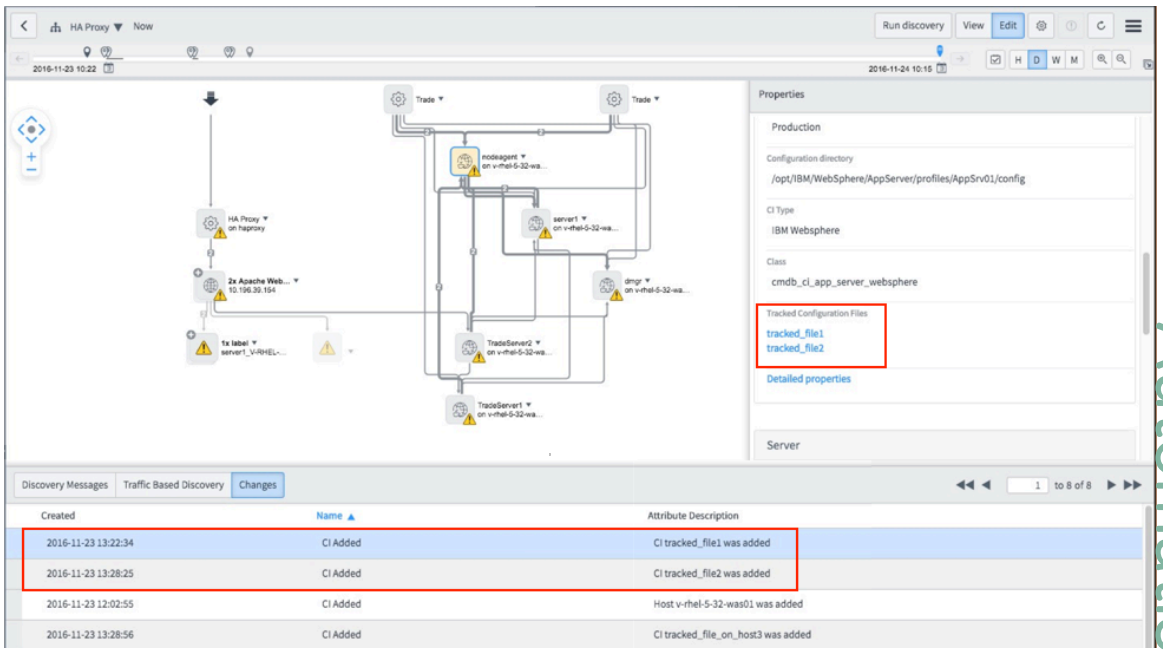
Führen Sie eine Erkennung auf den Hosts aus, auf denen die Anwendungen ausgeführt werden, die Sie mit Mustern erkennen möchten, öffnen Sie den CI-Datensatz der Anwendung, und überprüfen Sie die zugehörige Liste „Nachverfolgte Konfigurationsdateien“.

Wenn Sie Service-Mapping verwenden, vergewissern Sie sich, dass die Komponente begonnen hat, Informationen über Änderungen an Konfigurationsdateien zu erfassen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren Sie zur Zuordnung des Serviceinstanz , die die CIs enthält.
2. Vergewissern Sie sich, dass auf der Registerkarte „Changes“ die Liste einen Datensatz der von Ihnen vorgenommenen Änderungen enthält. Zum Beispiel, dass die Konfigurationsdatei hinzugefügt, geändert oder gelöscht wurde.



Versionen von CI-Konfigurationsdateien vergleichen

Sie können zwei Versionen von nachverfolgten CI-Konfigurationsdateien vergleichen, um die tatsächlich an ihnen durchgeführten Änderungen zu sehen.

Vorbereitungen

Erforderliche Rolle: Administrator

Wenn Discovery und Service-Mapping eine zu verfolgende Konfigurationsdatei nicht wie gewünscht nachverfolgen, führen Sie die erweiterte Konfiguration wie in Nachverfolgung von Changes in Konfigurationsdateien ändern beschrieben durch.

Warum und wann dieser Vorgang ausgeführt wird

Discovery und Service-Mapping überprüfen die Konfigurationsdateien während der horizontalen Erkennung mithilfe von Mustern auf Changes. Wenn eine Konfigurationsdatei geändert wird, speichert das System die Version der Datei. Sie können den Zeitstempel verwenden, um zwischen Versionen zu unterscheiden.

Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Prozedur

1. So vergleichen Sie die neueste und die vorherige Version der CI-Konfigurationsdatei aus Service-Mapping:

   a. Navigieren zu **Alle** > **Service-Mapping** > **Services** > **Business-Services**an.

   b. Klicken Sie neben dem erforderlichen Business Service auf **Karte anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Suchen Sie auf der Registerkarte **Changes** nach dem Change-Datensatz für die geänderte CI-Konfigurationsdatei.

Wichtig: Der Name des Change muss **Datei geändert** lauten.

d. Klicken Sie mit der rechten Maustaste auf den Change-Datensatz für die geänderte CI-Konfigurationsdatei, und wählen Sie **Change in nachverfolgten Dateiinhalten anzeigen** aus.
Die Registerkarte „Vergleich nachverfolgter Konfigurationsdateien“ wird geöffnet und zeigt die neuesten und die vorherigen Versionen der Konfigurationsdatei an.

e. Fahren Sie mit 3 fort.

2. So vergleichen Sie zwei beliebige Versionen der CI-Konfigurationsdatei aus der Liste der Versionen von Discovery aus:

- Navigieren zu **Alle** > **Discovery** > **Nachverfolgte Konfigurationsdateien** Und sortieren oder filtern Sie die Liste nach Kriterien wie **Zugehöriges CI** Oder **Host** .
- Öffnen Sie im Konfigurationsmodul einen CI-Datensatz für den CI-Typ, zu dem die Konfigurationsdatei gehört. Um beispielsweise einen Tomcat-Server zu finden, navigieren Sie zu **Alle** > **Konfiguration** > **Anwendungsserver** > **Tomcat**, Und wählen Sie dann den spezifischen Tomcat-Server aus. Die Liste der Konfigurationsdateien wird in der zugehörigen Liste der nachverfolgten Konfigurationsdateien angezeigt.

a. Wählen Sie eine Konfigurationsdatei aus der Liste aus.
Der Datensatz der nachverfolgten Konfigurationsdatei enthält folgende Angaben:

Feld	Beschreibung
Dateiname	Name und Dateipfad der Datei
Dateigröße	Dateigröße
Zuletzt geändert	Datum, an dem die Datei zuletzt geändert wurde
Dateiinhalt	Inhalt der Datei, wenn Sie die Option zum Speichern des Inhalts in der Dateiverfolgungsdefinition ausgewählt haben.

b. Klicken Sie in der zugehörigen Liste **Inhaltsversionen** auf eine der Versionen in der zugehörigen Liste **Aktualisierungszeit**.
Dieselben Informationen über die Konfigurationsdatei werden zusammen mit der Aktualisierungszeit angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf **Vergleichen**.
Die Registerkarte „Vergleich nachverfolgter Konfigurationsdateien“ wird geöffnet und zeigt die Versionen der Konfigurationsdatei an, die Sie ausgewählt haben.

3. Überprüfen Sie die tatsächlichen Änderungen.

Hervorhebungsfarben geben die Art der Änderung an:

- Lila - Aktualisierte Linie
- Pink - Neue Linie
- Grau - Zeile gelöscht

4. Navigieren Sie mit den Pfeilen in der oberen rechten Ecke zwischen den Änderungen.

Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen

Sie können angeben, was Sie mit den CI-Datensätzen nachverfolgter Konfigurationsdateien tun möchten, wenn sie bei der Mustererkennung nicht mehr erkannt werden.

Vorbereitungen

Ein Muster, das nachverfolgte Konfigurationsdateien angibt

Erforderliche Rolle: Discovery_admin, Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Löschungsstrategien für alle erkannten CIs festlegen, nicht nur Konfigurationsdatei-CIs. Für Standard-CIs greifen Sie jedoch auf eine andere Weise auf die Löschungsstrategie zu als für Konfigurationsdatei-CIs. Siehe Löschungsstrategie festlegen für Anweisungen.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster** Und öffnen Sie das gewünschte Muster.

2. Klicken Sie auf die Registerkarte **Nachverfolgte Dateien**.

3. Klicken Sie unter **Zugehörige Links** auf **Löschstrategie für die Konfigurationsdateien dieses Musters bearbeiten**.
Die Liste „Zugehörige CI-Typen“ wird mit gefilterten Datensätzen in der Tabelle „Zugehöriger CI-Typ“ [sa_ci_to_pattern] angezeigt. Der Filter zeigt nur Datensätze mit dem CI-Typ „Nachverfolgte Konfigurationsdateien“ [cmdb_ci_config_file_tracked] an. Das ist die Tabelle, in der das System Konfigurationsdatei-CIs speichert.

4. Doppelklicken Sie in der Listenansicht auf den Wert im entsprechenden Feld in der Spalte **Löschungsstrategie** für die nachverfolgte Konfigurationsdatei.

5. Wählen Sie einen neuen Wert aus:

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** , Bedeutet das Discovery Die nachverfolgte Konfigurationsdatei wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
	nicht gefunden. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen. **Hinweis:** Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert **Status** Feld [install_Status] des Konfigurationsdatei-CI-Datensatzes als **Stillgelegt** , Bedeutet das Discovery Verwendet diese Konfigurationsdatei nicht mehr. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Zugehörige Informationen

CI-Löschstrategien für Mustererkennung

Löschungsstrategie festlegen

Quellennamen der Discovery-Ergebnisse ändern

Sie haben die Möglichkeit, den Quellennamen der Ergebnisse einer Erkennung zu ändern. Das kann hilfreich sein, wenn Discovery in Ihrem Netzwerk zusammen mit einem anderen Erkennungsprodukt ausgeführt wird und Sie benutzerdefinierte Bezeichner verwenden möchten.

Vorbereitungen

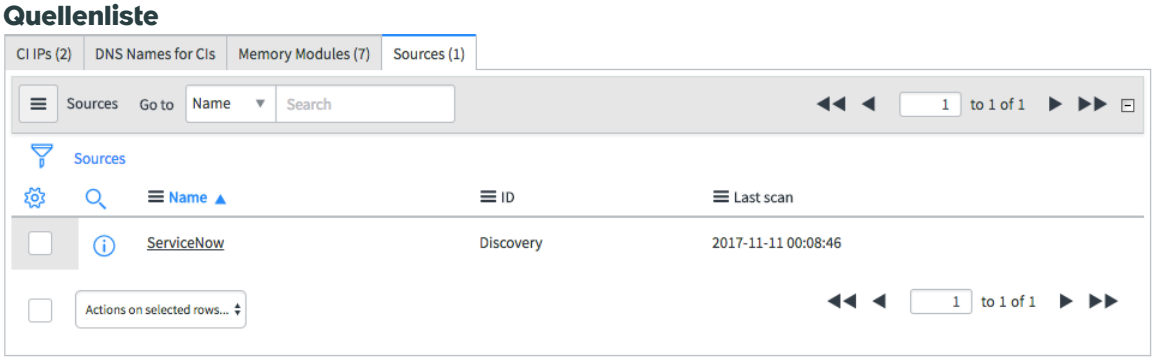
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

In der Tabelle „Quelle“ [sys_object_source] werden Informationen gespeichert, die die Quelle einer Erkennung, die ID dieser Quelle sowie Datum und Uhrzeit des letzten Scans identifizieren.

Um diese Informationen anzuzeigen, konfigurieren Sie ein CI-Formular, und fügen Sie die zugehörige Liste **Quellen** hinzu. Diese Tabelle wird automatisch gefüllt, wenn das Plugin Discovery aktiviert ist.

Quellenliste



So migrieren Sie Ihre Discovery-Quelle zu ServiceNow:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktualisieren Sie die Systemeigenschaft `glide.discovery.source_name` auf den Wert ServiceNow.
2. Bearbeiten Sie den Wörterbucheintrag für die Tabelle „Konfigurationselement“ [cmdb_ci].
3. Aktualisieren Sie die Auswahlliste für die Spalte *discovery_source*, sodass nur der Wert ServiceNow für ein Erkennungsprodukt vorhanden ist.
4. Öffnen Sie eine Liste für die Tabelle „Konfigurationselement“ [cmdb_ci], und filtern Sie sie nach einem Feldwert *Discovery-Quelle*, den Sie ändern möchten.
5. Verwenden Sie die Option *Alle aktualisieren*, um den Wert in ServiceNow zu ändern.
6. Öffnen Sie eine Liste für die Tabelle „Quelle“ [sys_object_source], und filtern Sie sie nach dem Feldwert des Namens, den Sie ändern möchten.
7. Verwenden Sie die Option *Alle aktualisieren*, um den Wert in ServiceNow zu ändern.

Plugin „Discovery API“

Das Plugin „Discovery API“ bietet APIs für bereichsbezogene Anwendungen und wird geladen, wenn das Plugin „Discovery“ aktiviert wird.

Details zu diesen Discovery API-Methoden finden Sie unter ServiceNow® Developer Site. Sie werden hier nach Klasse aufgelistet.

Hinweis: Java API-Methoden können nicht angepasst werden.

DiscoveryAPI - Scoped

Die Methoden in dieser Klasse starten eine Schnellerkennung einer einzelnen IPv4-Adresse und geben Zusammenfassungen zuvor gestarteter Discovery-Status für ein einzelnes CI oder für alle gescannten CIs zurück. Ein MID Server wird basierend auf der angegebenen IP-Adresse oder der angegebenen Anwendung automatisch ausgewählt.

- `discoverIpAddress()`: Erkennt eine einzelne IPv4-Adresse
- `reportCiIpAddressStatus()`: Gibt eine Zusammenfassung des Discovery-Status eines Konfigurationselements anhand des spezifischen Status sys_id und der IPv4-Adresse zurück
- `reportCiStatus()`: Gibt eine Zusammenfassung eines CI-Discovery-Status anhand eines spezifischen Discovery-Status sys_id zurück

ReportCiStatusOutputJS

Die Methoden sind Getter, die bestimmte Objekteigenschaften für die DiscoveryAPI-Methode `reportCiIpAddressStatus` zurückgeben und die Informationen dann in eine JSON-Zeichenfolge konvertieren.

- `getCiOperationStatus()`: Wird verwendet, um den Status des gescannten CI zurückzugeben
- `getCmdbCI()`: Wird verwendet, um den Wert im Feld cmdb_ci aus der Tabelle discovery_device_history für das gescannte CI zurückzugeben
- `getDiscoveryState()`: Wird verwendet, um den Wert aus dem Feld **Status** in der Tabelle „Discovery-Status“ [discovery_status] zurückzugeben
- `getIpAddress()`: Wird verwendet, um den Wert aus dem Feld „Quelle“ in der Tabelle discovery_device_history für das gescannte CI zurückzugeben
- `getIssues()`: Wird verwendet, um den Wert aus dem Feld „Probleme“ in der Tabelle discovery_device_history für das gescannte CI zurückzugeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `getIssuesLink()`: Wird verwendet, um den Wert aus dem Feld issues_link in der Tabelle discovery_device_history für das gescannte CI zurückzugeben.
- `toJson()`: Wird verwendet, um das Objekt `ReportCiStatusOutputJS` zu serialisieren.

Filter für laufende Prozesse

Filtern Sie alle Prozesse mithilfe von Kombinationen aus Namen und Schlüsselparametern, um sie an die Instanz zurückzugeben. Standardmäßig können Sie BS-Prozesse filtern. Durch Filterprozesse wird die Anzahl der in der Datenbank erstellten, aktualisierten oder gelöschten Datensätze reduziert, was die Gesamtleistung der Datenbank verbessern kann.

Vorbereitungen

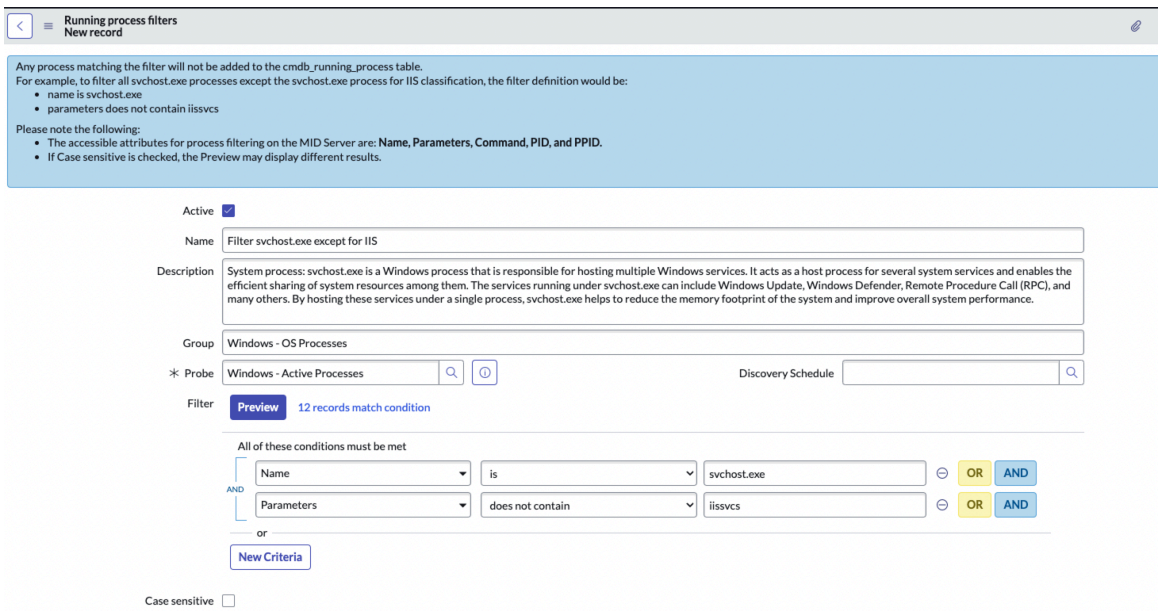
Erforderliche Rolle: discovery_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Um dem Filter Prozesse hinzuzufügen, müssen Sie Konfigurationen mit dem Filterdatensatz „laufender Prozess“ [running_Process_Filter] einrichten. Diese Datensätze stellen sicher, dass die gefilterten Prozesse nicht die Tabelle „laufender Prozess“ [cmdb_running_Process] ausfüllen.

Prozedur

1. Navigieren Sie zu running_Process_Filter.list.
2. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
   Das Formular und die Beschreibungen werden unten erläutert.



Feld	Beschreibung
Aktiv	Aktivieren Sie das Kontrollkästchen, um ein- oder auszuschließen.
Name	Name für den Datensatz.
Beschreibung	Kurzbeschreibung des Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gruppe	Ein Name für den Konfigurationstyp. Filter für laufende Prozesse können beliebig gruppiert werden, damit sie leichter in der Tabelle identifiziert und ausgewählt werden können.
Probe	Pflichtfeld. Welche Probe diesen Filter verwendet. Oft Linux Oder Windows Aktive Prozesse oder ADM erweitert. Wenn die Probe ausgeführt wird, sendet die Instanz die Datensätze „running_Process_Filter“ als Probe-Parameter. Die Probe verwendet dies dann, um die Ergebnisse zu filtern, bevor die Informationen an die Instanz zurückgesendet werden.
Discovery-Zeitplan	Sie können den Filter auf einen bestimmten anwenden Discovery Zeitplan. Wenn Sie dieses Feld verlassen, gilt es für alle Zeitpläne, auch für schnell Discovery.
Filter	Prozesse, die dem Filter entsprechen, werden nicht der Tabelle „cmdb_running_process“ hinzugefügt. Wenn Sie beispielsweise alle svchost.exe Prozesse mit Ausnahme des svchost.exe-Prozesses für die IIS-Klassifizierung filtern möchten, lautet die Filterdefinition: ○ Name ist svchost.exe ○ Parameter enthält nicht iissvcs Informationen zum Festlegen von Filterbedingungen finden Sie unter: Bedingungsgenerator
Groß-/Kleinschreibung beachten	Gilt für das Feld Filter. Wenn Groß-/Kleinschreibung beachtet ist, kann der Filter mehr oder weniger Informationen abrufen, als Sie möchten. Der Standardwert ist aus.
OOB-Filter	Es gibt Linux Und Windows Filter zur Auswahl. Unter Sofort einsatzbereite Prozessfilter finden Sie weitere Details.

3. Geben Sie die Details ein, und klicken Sie auf **Senden**.

Sofort einsatzbereite Prozessfilter

Es gibt eine Vielzahl von Linux Und Windows Sofort einsatzbereite Prozessfilter, die aktiviert sind und zum Filtern von Prozessen verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter

Name	Beschreibung
DhClient	Dhclient ist ein Systemprozess in Linux Das für die dynamische Konfiguration von Netzwerkschnittstellen mit dem Dynamic Host Configuration Protocol (DHCP) verantwortlich ist. Er kommuniziert mit einem DHCP-Server, um Netzwerkkonfigurationsinformationen wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server abzurufen. Dhclient wird häufig in Umgebungen verwendet, in denen Netzwerkadressen dynamisch zugewiesen werden, z. B. in Privat- und Netzwerken kleiner Unternehmen.
Crond	Crond ist ein Systemservice in Linux Das unterstützt das Cron-Zeitplanungsdienstprogramm. Es ist für die Ausführung geplanter Aufgaben zu angegebenen Zeiten und Intervallen verantwortlich. Crond wird häufig zur Automatisierung von Systemwartungsaufgaben wie Sicherungen und Protokollrotation sowie zum Ausführen anwenderdefinierter Skripts und Anwendungen zu bestimmten Zeiten verwendet.
Ruhezustand	Der Ruhezustand-Prozess ist ein Befehl, der verwendet wird, um die Ausführung eines Shell-Skripts oder Befehls für einen bestimmten Zeitraum anzuhalten. Dies ist eine einfache Möglichkeit, die Ausführung eines Skripts oder Befehls für eine bestimmte Dauer zu verzögern.
Agetty	Agetty ist ein Systemservice in Linux Die Anmeldesitzungen der virtuellen Konsole verwaltet. Es bietet eine Terminal-Schnittstelle, über die Anwender sich beim System anmelden und auf die Befehlszeilenschnittstelle zugreifen können. Agetty ist für die Initialisierung des Terminals, die Anzeige der Anmeldeaufforderung und die Authentifizierung der Anmeldeinformationen des Anwenders verantwortlich.
dbus-Daemon	dbus-Daemon ist ein Systemservice in Linux Das das D-Bus-Nachrichtenbussystem implementiert. Sie ist dafür verantwortlich, die Kommunikation zwischen Anwendungen und Systemservices auf demselben Host oder in einem Netzwerk zu aktivieren. dbus-Daemon verwaltet den Nachrichtenbus und sendet Nachrichten zwischen Anwendungen und Services, sodass sie Daten austauschen und Services anfordern können.
Rsyslogd	Rsyslogd ist ein Systemservice in Linux Das Systemprotokolle verwaltet und zentrale Protokollierungsfunktionen bereitstellt. Es handelt sich um ein leistungsstarkes und flexibles Protokollierungssystem, mit dem Administratoren Protokollnachrichten konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	und verwalten können, die von verschiedenen Anwendungen und Services auf einem System oder im Netzwerk generiert werden. Rsyslogd bietet erweiterte Funktionen wie Protokollfilterung, Protokollweiterleitung und Protokollrotation und unterstützt eine Vielzahl von Ausgabeformaten und -Zielen, einschließlich Dateien, Datenbanken und Remote-Syslog-Server. Rsyslogd wird häufig in Serverumgebungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Anwenderoberfläche konfiguriert werden.
Auditd	Auditd ist ein Systemservice in Linux Das ein Audit-Framework für die Nachverfolgung sicherheitsrelevanter Ereignisse im System bereitstellt. Es erfasst und protokolliert Sicherheitsereignisse, die von den Kernel- und Anwenderbereichsanwendungen generiert werden und für forensische Analysen, Compliance-Überwachung und Angriffserkennung verwendet werden können. Auditd kann so konfiguriert werden, dass Warnungen generiert oder andere Aktionen basierend auf vordefinierten Regeln oder Richtlinien ausgeführt werden.
Irqbalance	Irqbalance ist ein Systemservice in Linux Das Unterbrechungsanforderungen (IRQs) zwischen Prozessoren in einem Multicore-System ausgleicht, um die Leistung zu verbessern und die Latenz zu reduzieren. Es erkennt und überwacht IRQ-Aktivitäten und verteilt IRQs an den am wenigsten ausgelasteten Prozessor, was dazu beitragen kann, Verarbeitungsengpässe zu reduzieren und die Systemreaktionsfähigkeit zu verbessern. Irqbalance wird häufig in Hochleistungs-Computing-Umgebungen und anderen Systemen mit hoher Unterbrechungsaktivität verwendet.
Systemd-Journald	Systemd-Journald ist ein Systemservice in Linux Das ein zentralisiertes Protokollierungssystem für System- und Anwendungsprotokolle bereitstellt. Es wurde entwickelt, um Protokolldaten auf strukturierte und effiziente Weise zu erfassen und zu speichern, und ermöglicht eine erweiterte Abfrage und Filterung von Protokolldaten. Systemd-Journald bietet eine einheitliche Schnittstelle für den Zugriff auf und die Verwaltung von Protokollen über verschiedene hinweg Linux Verteilungen und können mithilfe einer Konfigurationsdatei oder einer Befehlszeilenschnittstelle konfiguriert werden. Es wird häufig in Server- und Desktop-Umgebungen verwendet, um System- und Anwendungsprobleme zu überwachen und zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
Abrtd	Abrtd ist ein Systemprozess, der unter ausgeführt wird Linux Systeme und ist verantwortlich für die Erkennung von Anwendungsabstürzen und die Meldung an den Systemadministrator. Der Prozess erfasst Informationen über die abgestürzte Anwendung, z. B. Core-Dumps, und speichert sie in einem Bericht.
atd	atd ist ein Systemservice in Linux Mit dieser Option können einmalige Aufträge zu einem bestimmten Zeitpunkt und Datum ausgeführt werden. Es ist nützlich, um Aufträge auszuführen, die zu einem bestimmten Zeitpunkt ausgeführt werden müssen, oder um Aufgaben zu automatisieren, die einmal in der Zukunft ausgeführt werden müssen.
Lvmetad	Lvmetad ist ein Systemservice in Linux Das Metadaten-Caching für Logical Volume Management (LVM) bereitstellt. Es speichert Metadateninformationen zu LVM-Volumes und -Geräten im Cache, was die Leistung von LVM-Vorgängen verbessern und den Zeitaufwand für das Scannen und Initialisieren von LVM-Geräten reduzieren kann. Lvmetad wird häufig in Systemen verwendet, die stark auf LVM angewiesen sind, z. B. Virtualisierungsumgebungen und Speicherserver.
Polkitd	Polkitd ist ein Systemservice in Linux Das ein Autorisierungs-Framework für die Steuerung des Zugriffs auf privilegierte Aktionen und Ressourcen bereitstellt. Es ermöglicht Anwendern ohne Berechtigungen, bestimmte Aufgaben auszuführen oder auf bestimmte Ressourcen zuzugreifen, die erhöhte Berechtigungen erfordern, z. B. die Installation von Software oder die Konfiguration von Netzwerkeinstellungen, indem sie aufgefordert werden, sich mit ihrem Passwort oder auf andere Weise zu authentifizieren. Polkitd bietet eine Richtlinien-Engine, die von Administratoren konfiguriert werden kann, um feingranulierte Zugriffssteuerungen für bestimmte Anwender, Gruppen oder Anwendungen zu definieren.
Acpid	Acpid ist ein Systemservice in Linux Die auf ACPI-Ereignisse (Advanced Configuration and Power Interface) abhört, die von der Hardware generiert wurden, und das Betriebssystem benachrichtigt. Sie ist für die Verwaltung von Stromversorgungsereignissen wie das Drücken eines ein-/Ausschaltschalters und die Ausführung anwenderdefinierter Aktionen als Reaktion darauf verantwortlich.
Anacron	Anacron ist ein Systemservice in Linux Dies ermöglicht die Planung regelmäßiger Aufgaben,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	ähnlich wie Cron, aber mit der zusätzlichen Möglichkeit, sicherzustellen, dass verpasste Aufgaben ausgeführt werden, wenn das System das nächste Mal verfügbar wird. Es ist nützlich, um regelmäßige Aufgaben auszuführen, die aufgrund von Systemausfallzeiten oder Anwenderinaktivität verzögert werden können.
(sd-pam)	sd-pam ist ein Systemservice in Linux Das unterstützt das PAM-Framework (Pluggable Authentication Modules). Sie ist für die Verarbeitung von Anwenderauthentifizierungs- und Autorisierungsanforderungen von verschiedenen Systemservices und -Anwendungen verantwortlich.
Netzwerkmanager	NetworkManager ist ein Systemservice in Linux Verwaltet die Netzwerkkonnektivität für Desktops, Laptops und andere Geräte. Es bietet eine einheitliche Schnittstelle für die Konfiguration und Verwaltung von kabelgebundenen, drahtlosen, mobilen Breitbandverbindungen und anderen Netzwerkverbindungen, die Verarbeitung von IP-Adressierung, DNS-Konfiguration und anderen Netzwerkeinstellungen. NetworkManager wird häufig in Desktop-Umgebungen und grafischen Anwenderoberflächen verwendet und kann mithilfe einer grafischen Anwenderoberfläche oder Befehlszeilenschnittstelle konfiguriert werden.
Hcid	Hcid ist ein Systemservice in Linux Das unterstützt Bluetooth-Konnektivität. Sie ist für die Verwaltung von Bluetooth-Geräten, -Verbindungen und -Services im System verantwortlich. Hcid bietet eine Schnittstelle für Anwendungen und Systemservices zur Interaktion mit Bluetooth-Geräten und wird zum Konfigurieren und Verwalten von Bluetooth-bezogenen Einstellungen wie Gerätepaarung, Authentifizierung und Autorisierung verwendet.
hidd	hidd ist ein Systemprozess in Linux Das unterstützt Bluetooth Human Interface Devices (HID), z. B. Tastaturen und Mäuse. Es ist für die Verwaltung von Bluetooth-Verbindungen und die Bereitstellung einer gemeinsamen Schnittstelle für HID-Geräte zur Kommunikation mit dem System verantwortlich. hidd wird häufig in Desktop-Umgebungen verwendet, um die Verwendung drahtloser Eingabegeräte mit dem System zu ermöglichen.
Iscsid	Iscsid ist ein Systemprozess in Linux Das unterstützt das iSCSI-Protokoll, das für den Zugriff auf Speichergeräte über ein Netzwerk verwendet wird. Es ist verantwortlich für die Erkennung von iSCSI-Zielen, die Einrichtung und Verwaltung von iSCSI-Sitzungen und die Bereitstellung des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Zugriffs auf iSCSI-Geräte, als ob es sich um lokal angeschlossenen Speicher handelte. Iscsid wird häufig in Virtualisierungsumgebungen und anderen Systemen verwendet, die Remotezugriff auf Speicherressourcen erfordern.
Klogd	Klogd ist ein Systemprozess in Linux Die für die Protokollierung von Kernel-Nachrichten im Systemprotokoll verantwortlich ist. Er überwacht den Kernel-Protokollpuffer auf neue Nachrichten und schreibt sie in die Systemprotokolldatei oder sendet sie an einen Remote-Protokollierungsserver. Klogd wird häufig zur Behebung von Kernelproblemen und zur Überwachung der Systemaktivität sowie zum Sammeln von Diagnoseinformationen für Systemadministratoren und Entwickler verwendet.
Mischung tty1	Mingetty ist ein Systemprozess in Linux Die eine Terminal-Anmeldeaufforderung auf einer virtuellen Konsole bereitstellt. Es ist verantwortlich für die Initialisierung des Terminalgeräts, die Anzeige der Anmeldeaufforderung und die Akzeptanz der Anmeldeinformationen für die Anwenderanmeldung. Mingetty tty wird für jede virtuelle Konsole in einem verwendet Linux System und kann für Systemverwaltungs- und Debugging-Aufgaben sowie für die Ausführung konsolenbasierter Anwendungen verwendet werden.
ModemManager	ModemManager ist ein Systemservice in Linux Das mobile Breitband (GSM/CDMA/UMTS/ LTE) und andere Modemverbindungen verwaltet. Es bietet eine einheitliche Schnittstelle für die Konfiguration und Verwaltung von Modemgeräten, die Verarbeitung von Verbindungen zum Internet oder anderen Netzwerken und die Überwachung der Modemaktivität. ModemManager wird häufig auf Laptops, Tablets und anderen Mobilgeräten verwendet, die drahtlose Netzwerkkonnektivität erfordern.
Pcscd	Pcscd ist ein Systemservice in Linux Das unterstützt Smartcard-Lesegeräte und Smartcards. Sie ermöglicht Anwendungen den Zugriff auf Smartcards und deren Inhalte über den PC/SC-Schnittstellenstandard (Personal Computer/Smart Card). Pcscd bietet eine einheitliche Schnittstelle für den Zugriff auf verschiedene Arten von Smartcard-Lesegeräten und kann von Anwendungen wie Webbrowsern, E-Mail-Clients und Authentifizierungssystemen verwendet werden, die die Unterstützung von Smartcards erfordern.
Power-Profile-Daemon	Power-Profile-Daemon ist ein Systemservice in Linux Verwaltet Energieprofile und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Energieverwaltungseinstellungen für Laptops und andere Mobilgeräte. Es bietet eine einheitliche Schnittstelle zum Konfigurieren und Verwalten von Energiesparfunktionen wie Bildschirmhelligkeit, CPU-Frequenzskalierung und Ruhemodi, basierend auf Anwendereinstellungen und Systemnutzungsmustern. Power-Profile-Daemon wird häufig in Desktop-Umgebungen und grafischen Anwenderoberflächen verwendet und kann mithilfe einer grafischen Anwenderoberfläche oder einer Befehlszeilenschnittstelle konfiguriert werden.
pulseaudio	pulseaudio ist ein Systemservice in Linux Die Audiogeräte, Streams und Anwendungen verwaltet. Es bietet eine einheitliche Audioschnittstelle für Eingabe- und Ausgabe-Audio-Streams und unterstützt erweiterte Funktionen wie Lautstärkeregelung, Mischen und Audio-Effekte. pulseaudio wird häufig in Desktop-Umgebungen und grafischen Anwenderoberflächen verwendet und kann über eine grafische Anwenderoberfläche oder Befehlszeilenschnittstelle konfiguriert werden. Es unterstützt eine Vielzahl von Konfigurationen von Audio-Hardware und -Software, einschließlich mehrerer Audiogeräte und Netzwerk-Audio-Streaming.
Chronyd	Chronyd ist ein Systemservice in Linux Die für die Synchronisierung der Systemuhr mit einer Referenzzeitquelle verantwortlich ist. Es implementiert das Network Time Protocol (NTP) und kann verwendet werden, um die Systemuhr mit einer Vielzahl von Zeitquellen zu synchronisieren, einschließlich GPS-Uhren und Atomuhren. Chronyd wird häufig in Umgebungen verwendet, in denen eine genaue Zeitsynchronisierung wichtig ist, z. B. im Finanzhandel oder in der wissenschaftlichen Forschung.
Rtkit-Daemon	Rtkit-Daemon ist ein Systemservice in Linux Die Echtzeitplanung und Prioritätsverwaltung für Audio- und andere zeitsensible Anwendungen bietet. Sie soll sicherstellen, dass diese Anwendungen Zugriff auf die CPU und andere Systemressourcen erhalten, die sie benötigen, um ordnungsgemäß zu funktionieren, und Audio-Störungen, Latenzen oder andere Leistungsprobleme vermeiden. Rtkit-Daemon verwendet Linux Echtzeitfähigkeiten und bietet eine einfache Schnittstelle für Anwendungen, um Echtzeitplanung und -Priorität anzufordern. Es wird häufig in Desktop-Umgebungen und Audioanwendungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Anwenderoberfläche konfiguriert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
SSD	SSSSD ist ein Systemservice in Linux Das zentralisierte Authentifizierungs-, Identitäts- und Zugriffsmanagement für eine Vielzahl von Services und Anwendungen bietet. Es wurde entwickelt, um die Verwaltung von Anwenderaccounts und Anmeldeinformationen in großen Umgebungen mit mehreren Domänen zu vereinfachen und bietet eine einheitliche Schnittstelle für Authentifizierung, Autorisierung und Identitätslösung. SSSSD unterstützt eine Vielzahl von Identitätsquellen, einschließlich lokaler Dateien, LDAP-Verzeichnisse und Active Directory-Domänen, und bietet erweiterte Funktionen wie Offline-Authentifizierung, Caching und Failover. Sie wird häufig in Enterprise-Umgebungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Anwenderoberfläche konfiguriert werden.
Sssd_kcm	„Sssd_kcm“ ist ein Systemservice in Linux Der einen Kerberos-Anmeldeinformations-Cache-Manager für den System Security Services Daemon (SSSD) bereitstellt. Es wurde entwickelt, um die Sicherheit und Leistung der Kerberos-basierten Authentifizierung und Autorisierung zu verbessern, indem Kerberos-Anmeldeinformationen und -Tickets lokal zwischengespeichert und eine einheitliche Schnittstelle für den Zugriff darauf bereitgestellt wird. „Sssd_kcm“ wird häufig in Unternehmensumgebungen verwendet, die Kerberos für die zentrale Authentifizierung und Zugriffssteuerung verwenden, und kann mithilfe einer Konfigurationsdatei oder einer grafischen Anwenderoberfläche konfiguriert werden.
Systemd – hostnamed	Systemd-hostnamed ist ein Systemservice in Linux Die Hostname- und DNS-Auflösungskonfiguration bereitstellt. Sie soll die Konfiguration von netzwerkbezogenen Einstellungen wie Hostname, Domänenname und DNS-Server vereinfachen. Systemd-hostnamed bietet eine einheitliche Schnittstelle zum Konfigurieren dieser Einstellungen für verschiedene Bereiche Linux Verteilungen und können mithilfe einer Konfigurationsdatei oder einer Befehlszeilenschnittstelle konfiguriert werden. Es wird häufig in Server- und Desktop-Umgebungen verwendet, um Netzwerkeinstellungen während des Systemstarts oder der Laufzeit zu konfigurieren.
Systemd-timesyncd	Systemd-timesyncd ist ein Systemservice in Linux Bietet die Zeitsynchronisierung für die Systemuhr. Er synchronisiert die Systemuhr mit einem Remote-Zeitserver über das Netzwerk und kann so konfiguriert werden, dass mehrere Zeitquellen zur Redundanz verwendet werden. Systemd-timesyncd

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	wird häufig in Server- und Desktop-Umgebungen verwendet, um eine genaue Zeiterfassung für verschiedene System- und Anwendungsfunktionen sicherzustellen.
Hald	Hald ist ein Systemservice in Linux Die für die Erkennung und Verarbeitung von Hardware-Ereignissen verantwortlich ist, z. B. das Einfügen und Entfernen von Speichergeräten und anderen Hardwarekomponenten. Es bietet eine gemeinsame Schnittstelle für Anwendungen und Systemservices zur Interaktion mit der Hardware und wird zum Konfigurieren und Verwalten von Systemressourcen wie Eingabegeräten und Speichervolumes verwendet. Hald wird häufig in Desktop-Umgebungen verwendet, um Plug-and-Play-Funktionalität für Hardwaregeräte bereitzustellen.
xfs	xfs ist ein leistungsstarkes Journaling-Dateisystem für Linux Das für Skalierbarkeit und große Dateien optimiert ist. Es wurde ursprünglich von Silicon Graphics, Inc. Für die Verwendung in ihrem IRIX-Betriebssystem entwickelt und später auf portiert Linux. xfs unterstützt Funktionen wie Snapshots, Online-Größenänderung und erweiterte Dateiberechtigungen. Es wird häufig in High-Performance-Computing, Medien und Unterhaltung und anderen Branchen verwendet, in denen die Verarbeitung großer Dateien und Datensätze entscheidend ist.
Audispd	Audispd ist ein Systemservice in Linux Die für die Verarbeitung von Audit-Ereignissen verantwortlich ist, die vom Auditing-Subsystem des Kernel generiert wurden. Es ist Teil des Audit-Frameworks und wird verwendet, um eine sichere Protokollierung von Systemereignissen für Audits und forensische Zwecke bereitzustellen. Audispd kann so konfiguriert werden, dass Audit-Ereignisse an verschiedene Ziele gesendet werden, z. B. syslog oder einen zentralen Protokollserver.
Automatisieren	Automount ist ein Systemservice in Linux Die automatische Bereitstellung von Dateisystemen ermöglicht, wenn Anwender oder Anwendungen darauf zugreifen. Ermöglicht das On-Demand-Bereitstellen von Dateisystemen, wodurch der Zeitaufwand und die Systemressourcen für unnötige Dateisystembereitstellungen reduziert werden. Automatisches Laden ist besonders in Umgebungen mit einer großen Anzahl von vernetzten Dateisystemen oder Wechseldatenträgern nützlich.
avahi-Daemon: Chroot-Helfer	avahi-Daemon ist ein Systemservice in Linux Das das Zeroconf-Protokoll für die Service-Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	in lokalen Netzwerken implementiert. Der chroot-Helfer ist eine Komponente von Avahi-Daemon, die für die Einrichtung einer chroot-Umgebung für den Service verantwortlich ist. Dies trägt zur Erhöhung der Sicherheit bei, indem der Zugriff von Avahi-Daemon auf das System eingeschränkt wird.

Windows Sofort einsatzbereite Filter

Name	Beschreibung
System-Leerlaufprozess	In Windows Das Betriebssystem „System-Leerlaufprozess“ ist kein Prozess, sondern eine Systeminaktivitätsaufgabe, die ausgeführt wird, wenn die CPU nichts anderes zu tun hat. Sie stellt den Prozentsatz der Zeit dar, in der die CPU inaktiv und für die Verarbeitung anderer Prozesse verfügbar ist. Daher ist es eine wichtige Systemkomponente, die die aktuelle CPU-Auslastung anzeigt, wenn keine anderen Prozesse ausgeführt werden.
svchost.exe	svchost.exe ist ein Windows Prozess, der für das Hosting mehrerer verantwortlich ist Windows Services. Er fungiert als Hostprozess für mehrere Systemservices und ermöglicht die effiziente gemeinsame Nutzung von Systemressourcen. Die Services, die unter svchost.exe ausgeführt werden, können Folgendes umfassen Windows Aktualisieren, Windows Defender, Remote Procedure Call (RPC) und viele andere. Durch das Hosting dieser Services in einem einzigen Prozess trägt svchost.exe dazu bei, den Speicherbedarf des Systems zu reduzieren und die Gesamtleistung des Systems zu verbessern.
wmiprvse.exe	wmiPrvSE.exe ist ein Windows Systemprozess, der Verwaltungsinformationen und -Steuerung über bereitstellt Windows Management Instrumentation (WMI)-Framework. Er wird als Service im Hintergrund ausgeführt und ermöglicht Anwendungen und Skripts den Zugriff auf Systemverwaltungsinformationen, die Ausführung administrativer Aufgaben und die Überwachung der Systemleistung. WmiPrvSE.exe kann sowohl im lokalen als auch im Remote-Modus ausgeführt werden und zur Verwaltung einer Vielzahl von Systemressourcen verwendet werden, einschließlich Hardware, Software und Netzwerkkomponenten. Dies ist eine wichtige Komponente von Windows Betriebssystem und wird normalerweise von Systemadministratoren und IT-Fachleuten verwendet.
conhost.exe	conhost.exe ist ein Windows Prozess, der als Host für Konsolenanwendungen dient. Es wurde in eingeführt Windows7 und ist für die Verwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	der Befehlsaufforderungsfenster und anderer konsolenbasierter Anwendungen verantwortlich. conhost.exe bietet verbesserte Kompatibilitäts- und Sicherheitsfunktionen im Vergleich zum Vorgänger, dem csrss.exe-Prozess, der für denselben Zweck in älteren Versionen von verwendet wurde Windows.
WUDFHost.exe	WUDFHost.exe ist ein Windows User-Mode Driver Framework (UMDF) – Hostprozess, der Anwendermodustreiber verwaltet, die im Kontext von ausgeführt werden Windows Driver Foundation (WDF). Es bietet ein Framework für die Entwicklung und Ausführung von Treibern im Anwendermodus anstatt im Kernel-Modus, wodurch die Stabilität und Zuverlässigkeit des Systems verbessert wird. WUDFHost.exe wird für Plug-and-Play-Geräte und andere treiberbasierte Hardwarekomponenten verwendet. Sie wird im Hintergrund ausgeführt und verbraucht normalerweise niedrige Systemressourcen.
LogonUI.exe	LogonUI.exe ist ein Windows Systemprozess, der den verwaltet Windows Anmeldebildschirm und Anwenderauthentifizierung. Wenn ein Anwender versucht, sich bei anzumelden Windows Computer, LogonUI.exe zeigt den Anmeldebildschirm an und fordert den Anwender auf, seine Anmeldeinformationen einzugeben. Sobald die Anmeldeinformationen des Anwenders eingegeben wurden, überprüft LogonUI.exe sie und gewährt dem Anwender Zugriff auf das System. LogonUI.exe ist eine wichtige Komponente von Windows Betriebssystem und darf nicht beendet oder deaktiviert werden.
csrss.exe	Der Prozess csrss.exe ist eine kritische Komponente von Windows Betriebssystem. Sie ist für die Verarbeitung bestimmter Funktionen im Zusammenhang mit der grafischen Anwenderoberfläche (GUI) verantwortlich, z. B. die Verwaltung von Fenstern und Konsolen. Der Prozess wird in einer separaten Sitzung von der Sitzung des Anwenders ausgeführt, um die Stabilität und Sicherheit des Betriebssystems sicherzustellen. Es handelt sich um einen wichtigen Systemprozess, der nicht beendet werden darf, es sei denn, es liegt ein bestimmter und gültiger Grund dafür vor.
dllhost.exe	dllhost.exe ist ein Windows Systemprozess, der für die Ausführung und Verwaltung von COM-Komponenten (Component Object Model) verantwortlich ist. COM-Komponenten sind wiederverwendbare Softwaremodule, auf die von anderen Programmen zugegriffen werden kann. Sie werden häufig verwendet, um die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	prozessübergreifende Kommunikation zwischen verschiedenen Anwendungen zu erleichtern. Der Prozess dllhost.exe hostet diese COM-Komponenten und stellt ihre ordnungsgemäße Ausführung und Verwaltung sicher. Es wird häufig von einer Vielzahl von verwendet Windows Anwendungen und Services.
Fontdrvhost.exe	Fontdrvhost.exe ist ein Windows Systemprozess, der die Installation, Entfernung und Aufzählung von Schriftartdateien verwaltet. Es ist für das Laden und Rendern von Schriftarten in Anwendungen verantwortlich, die verwenden Windows Schriftart-Cache-Service. Fontdrvhost.exe wird im Hintergrund ausgeführt und hat keine sichtbare Schnittstelle. Es ist wichtig, um die Schriftartenbibliothek des Systems zu verwalten und sicherzustellen, dass Schriftarten bei Bedarf für Anwendungen verfügbar sind.
wlanext.exe	wlanext.exe ist ein Windows Systemprozess, der WLAN-Konfigurationen und -Vorgänge unterstützt. Sie ist für die Verwaltung der Drahtlosnetzwerkadapter und die Implementierung der Funktionalität des WLAN AutoConfig-Service verantwortlich, der die automatische Konfiguration von Drahtlosnetzwerken ermöglicht und das WPS-Protokoll (Wi-Fi Protected Setup) unterstützt. Der Prozess wird im Hintergrund ausgeführt und kann über die Servicekonsole oder die Eingabeaufforderung verwaltet werden.
winlogon.exe	winlogon.exe ist ein Systemprozess in Windows Verwaltet die Anmeldung und Abmeldung von Anwendersitzungen. Es ist verantwortlich für die Authentifizierung von Anwendern und das Laden ihres Anwenderprofils bei der Anmeldung sowie das Schließen offener Anwendungen und das Speichern von Anwenderdaten, wenn sich ein Anwender abmeldet oder das System herunterfährt. Winlogon.exe wird als Service im Hintergrund ausgeführt und ist für das ordnungsgemäße Funktionieren von von unerlässlich Windows Betriebssystem.
unsecapp.exe	unsecapp.exe ist ein Windows Systemprozess, der sich auf das verteilte Komponentenobjektmodell (Distributed Component Object Model, DCOM) bezieht. Sie wird im Hintergrund ausgeführt und fungiert als Vermittler zwischen einem Client und einer Serveranwendung, die über DCOM kommunizieren. Wenn ein Client eine Anforderung über DCOM an einen Server sendet, ist unsecapp.exe dafür verantwortlich, die Sicherheitsaspekte der Kommunikation zu verarbeiten und sicherzustellen, dass die Anforderung autorisiert ist. Es handelt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	sich um einen legitimen Systemprozess, der sich normalerweise im Ordner C:\Windows\System32 befindet.
w3wp.exe	w3wp.exe ist ein Windows Prozess, der für steht Windows Prozess Der Prozessaktivierung – Service Worker-Prozess. Sie wird vom Webserver „Internetinformationsservices“ (IIS) zum Hosten und Verwalten von ASP.NET-Webanwendungen verwendet. w3wp.exe ermöglicht die gleichzeitige Ausführung mehrerer Webanwendungen auf demselben Server und bietet für jede Anwendung eine sichere, isolierte Umgebung. Sie ist eine kritische Komponente des IIS-Servers und wird häufig genau überwacht, um die Stabilität und Leistung von Webanwendungen sicherzustellen.
dwm.exe	dwm.exe ist ein Windows Systemprozess, der für Desktop steht Windows Manager. Es ist für die Verwaltung grafischer Effekte wie transparente Fenster und Fensteranimationen in verantwortlich Windows Betriebssystem. Der Prozess ist auch für das Rendern des Desktops, die Verwaltung von Fenstern und die Bereitstellung visueller Effekte wie Aero Glass verantwortlich. Es wurde mit eingeführt Windows Vista und wurde seitdem in allen nachfolgenden Versionen von enthalten Windows.
lsass.exe	lsass.exe ist ein kritischer Systemprozess in Windows Das Authentifizierungs- und sicherheitsbezogene Funktionen wie lokale und Remote-Anmeldung, Passwortänderungen und Durchsetzung von Sicherheitsrichtlinien verarbeitet. Dies ist eine Kernkomponente von Windows Betriebssystem und ist für das ordnungsgemäße Funktionieren des Systems erforderlich.
System	System ist kein Windows Verarbeiten Sie im traditionellen Sinne. Stattdessen bezieht es sich auf eine Sammlung von Prozessen und Services, die für das Funktionieren des Betriebssystems entscheidend sind. Diese Prozesse und Services sind für die Verwaltung von Hardwaressourcen, die Verarbeitung von Systemereignissen und die Bereitstellung wichtiger Funktionen wie Speicherverwaltung, Prozessplanung und Sicherheit verantwortlich. Mit anderen Worten: System ist der Kern von Windows Betriebssystem.
smss.exe	„smss.exe“ oder „Sitzungsmanager-Subsystem“ ist ein kritischer Systemprozess in Windows Die für das Starten von Anwendermodusanwendungen während des Systemstarts verantwortlich ist. Außerdem werden System-Threads erstellt, systemweite Datenstrukturen initialisiert und Anforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	zum Herunterfahren und Neustarten des Systems verarbeitet. Dies ist einer der ersten Prozesse, der während des gestartet wird Windows Startprozess.
services.exe	services.exe ist ein Systemprozess in Windows Verantwortlich für die Verwaltung von Systemservices, einschließlich Starten und Stoppen und Steuerung ihrer Konfigurationseinstellungen. Sie wird im Hintergrund ausgeführt und bietet wichtige Funktionen für das Betriebssystem.
wininit.exe	wininit.exe ist ein Systemprozess in Windows Die während des Startvorgangs des Betriebssystems ausgeführt wird. Seine Hauptfunktion besteht in der Initialisierung kritischer Systemservices und Prozesse, die für die ordnungsgemäße Funktion des Systems erforderlich sind. Er ist für die Ausführung von verantwortlich Windows Startsequenz, einschließlich Starten des Session Manager-Prozesses (smss.exe).
spoolsv.exe	spoolsv.exe ist ein Systemserviceprozess in Windows Die den Druckprozess verwaltet. Es ist verantwortlich für das Warteschlangen- und Spooling von Druckaufträgen, die Kommunikation mit dem Drucker und die Sicherstellung, dass jeder Auftrag korrekt gedruckt wird. Der Prozess wird im Hintergrund ausgeführt und ist für das ordnungsgemäße Funktionieren des Drucksubsystems in entscheidend Windows. Wenn beim Prozess spoolsv.exe Fehler auftreten, kann dies zu Druckproblemen und -Fehlern führen.
taskhostw.exe	taskhostw.exe ist ein Windows Systemprozess, der als Host für verschiedene Hintergrundaufgaben dient, die auf dem System ausgeführt werden. Es verwaltet und führt Aufgaben wie aus Windows Updates, Wartungsaufgaben und anwenderdefinierte Aufgaben. Es handelt sich um einen kritischen Systemprozess, und das Beenden kann zu Systeminstabilität führen.
SearchProtocolHost.exe	SearchProtocolHost.exe ist ein Windows Prozess, der für die Indizierung und Ausführung von Suchvorgängen im System verantwortlich ist. Es ist Teil von Windows Suchservice, mit dem Anwender schnell nach Dateien und Ordnern auf ihrem Computer suchen können. Der Prozess SearchProtocolHost.exe wird im Hintergrund ausgeführt und indiziert Dateien und Ordner basierend auf anwenderdefinierten Suchkriterien. Wenn eine Suchabfrage ausgeführt wird, wird der Prozess aktiviert und ruft die relevanten Suchergebnisse ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
SearchIndexer.exe	SearchIndexer.exe ist ein Windows Systemprozess, der Dateien und Ordner auf lokalen und vernetzten Laufwerken indiziert, um eine schnellere Suche zu ermöglichen. Er wird im Hintergrund ausgeführt und indiziert kontinuierlich neue oder geänderte Dateien, um eine aktuelle Indexdatenbank zu erhalten. Der Prozess ist für wichtig Windows Suchfunktion und finden Sie in den meisten Windows Betriebssysteme.
Explorer.exe	explorer.exe ist ein Kernprozess in Windows Betriebssysteme, die für die Bereitstellung der Anwenderoberfläche, des Desktops und der Dateiverwaltungsfunktionen verantwortlich sind. Sie wird häufig als bezeichnet Windows Explorer oder Datei-Explorer und ermöglicht Anwendern das Navigieren und Verwalten von Dateien, Ordnern und Anwendungen auf ihrem Computer.
SearchFilterHost.exe	SearchFilterHost.exe ist ein Windows Systemprozess, der für die Indizierung und Suche von Dateien auf dem Computer verantwortlich ist. Dies ist eine Komponente von Microsoft Windows Suchservice, mit dem Anwender schnell nach Dateien und Dokumenten auf ihrem Computer suchen können. Der Prozess wird im Hintergrund ausgeführt und kann beim Indizieren von Dateien eine beträchtliche Menge an Systemressourcen verwenden.
SCNotification.exe	SCNotification.exe ist ein Windows Systemprozess, der für die Anzeige von Systembenachrichtigungen wie Warnungen und Nachrichten für den Anwender verantwortlich ist. Es ist Teil von Windows Shell-Experience-Host-Prozess (ShellExperienceHost.exe), der die Anwenderoberfläche für das Startmenü, die Taskleiste und das Aktionscenter in verwaltet Windows10.
sihost.exe	sihost.exe ist ein Systemprozess in Windows Das für das Starten des Startmenüs und die Verarbeitung seiner Interaktionen verantwortlich ist. Sie ist ein wichtiger Teil der Anwenderoberfläche und bietet eine grafische Oberfläche für die Interaktion mit dem System.
MonitoringHost.exe	MonitoringHost.exe ist ein legitimer Systemprozess, der Teil von ist Windows Betriebssystem. Wird von verwendet Windows Infrastruktur für Fehlerberichterstattung (WER), an die Telemetrie- und Diagnosedaten erfasst und gesendet werden sollen Microsoft, Die dann verwendet wird, um die Stabilität und Leistung von zu verbessern Windows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Discovery Dient zur Verwendung des Ereignis-Frameworks

Konfigurieren Discovery Dient zur Verarbeitung von Aufträgen mit der Ereignis-Framework-Methode, mit der Sie die Discovery-Drosselung effektiv verwalten und Aufgaben basierend auf ihrer Wichtigkeit in der Warteschlange priorisieren können.

Vorbereitungen

Bestätigen Sie Folgendes:

- Discovery-Administratorarbeitsbereich Verwendet Version 1.9.0 oder höher.
- ServiceNow AI Platform Verwendet Version XP9, YP4 oder höher als YP4.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Ereignis-Framework-Methode nicht verwendet wird, Discovery Erstellt einen Datensatz für das einmalige Zeitplanelement [sys_Trigger] für jeden ECC-Warteschlangensensor oder Mustereingabedatensatz (External Communication Channel). Nachdem die Aufgabe verarbeitet wurde, löscht der Systemplaner sys_Trigger. Dieser Ansatz führt zu zusätzlichem Overhead und kann zu einer erheblichen Datenbankanwendung führen und bietet gleichzeitig eingeschränkte Kontrolle darüber, wie Sensoren verarbeitet werden.

Das Ereignis-Framework reduziert die Abwanderung von Datenbanken, indem im Laufe der Zeit mehrere Ereignistabellen durchlaufen werden. Anstatt alte Datensätze nacheinander zu löschen, werden ganze Tabellen gelöscht, wenn sie nicht mehr benötigt werden, und sie werden wiederverwendet. Dieser Ansatz ist viel effizienter und trägt dazu bei, dass das System reibungslos läuft.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Wählen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] die aus `discovery.use.event.processing`Eigenschaft.
3. Legen Sie fest **Wert** Feld bis **Wahr** .
4. Wählen Sie **Aktualisieren**.

Ergebnis

Wenn der ECC-Warteschlange ein Eingabedatensatz hinzugefügt wird, wird eine Geschäftsregel ausgelöst, die ein Ereignis auslöst. Das System verarbeitet diese Ereignisse in regelmäßigen Abständen mit einer Standardpriorität von 100.

Hinweis: Um eine Auftragspriorität zu aktualisieren, konfigurieren Sie `com.glide.queue.discovery.sensors.processing_jobs.priority`Und `com.glide.queue.discovery.cloud.sensors.processing_jobs.priority`Systemeigenschaften. Weitere Informationen finden Sie unter Konfigurieren Sie die Auftragspriorität von Background Worker für Ereignis-Framework.

Wird Optimiert Discovery Laden Sie für Ereignis-Framework

Sie können optimieren Discovery Eigenschaften zum Anpassen des Durchsatzes und zur Verbesserung der Sicherheit beim Anheften von Aufträgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignis-Framework Discovery Optimierung

Problem	Aktion	Zugehörige Aufgabe
Ihre Instanz ist langsam	Verringern Sie den Skalierungsfaktor	Passen Sie den Skalierungsfaktor für Ereignis-Framework-Aufträge an
Discovery Ist langsam	Erhöhen Sie den Skalierungsfaktor	Passen Sie den Skalierungsfaktor für Ereignis-Framework-Aufträge an
Discovery Ist langsam, wenn sowohl Cloud als auch IP Discovery Werden ausgeführt	Verwenden Sie eine einzelne Warteschlange für Cloud- und IP-basierte Ereignisse	Konfigurieren Sie eine einzelne Warteschlange für Cloud- und IP-basierte Ereignisse
Discovery Greift anderen Arbeiten vor	Reduzieren Sie die Mitarbeiterpriorität des Hintergrundauftrags	Konfigurieren Sie die Auftragspriorität von Background Worker für Ereignis-Framework
Knoten werden zu viele ausgeführt Discovery Aufträge gleichzeitig	Konfigurieren Sie Ereignisprozessoren für die Ausführung auf bestimmten Knoten	Konfigurieren Sie Ereignisprozessoren für die Ausführung auf bestimmten Knoten

Passen Sie den Skalierungsfaktor für Ereignis-Framework-Aufträge an

Passen Sie den Skalierungsfaktor an, um die Anzahl der Worker-Threads pro App-Knoten zu ändern, wodurch der Durchsatz erhöht oder verringert wird.

Vorbereitungen

Bestätigen Sie Folgendes:

- Discovery-Administratorarbeitsbereich Verwendet Version 1.9.0 oder höher.
- ServiceNow AI Platform® Verwendet Version XP9, YP4 oder höher als YP4.
- Die *`discovery.use.event.processing`*Systemeigenschaft ist aktiviert. Weitere Informationen finden Sie unter Konfigurieren Discovery Dient zur Verwendung des Ereignis-Frameworks.
- Die **Auftragskonfigurationstyp** Feld des Formulars „Warteschlangenregistrierung“ ist auf festgelegt **Mit Knoten skalieren** . Weitere Informationen finden Sie unter Referenz des Formulars für Warteschlangenregistrierung.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Instanz während langsam wird Discovery Wird ausgeführt, können Sie den Skalierungsfaktor anpassen, um die Anzahl der Worker-Threads pro App-Knoten zu ändern. Der Standardskalierungsfaktor ist auf 2 festgelegt, was zwei Worker-Threads pro App-Knoten entspricht.

Wenn Sie beispielsweise den Skalierungsfaktor auf 3 erhöhen, Discovery Verwendet drei Worker-Threads pro App-Knoten, wodurch der Durchsatz erhöht wird. Umgekehrt wird der Skalierungsfaktor auf 1 Grenzwerte reduziert Discovery Zu einem einzelnen Worker-Thread pro App-Knoten, was den Durchsatz verringert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemrichtlinie** > **Warteschlangenregistrierung**an.
2. Wählen Sie einen oder mehrere Auftragstypen aus, für die Sie den Skalierungsfaktor anpassen möchten.

Auftragstyp	Aktion
IP-basiert	Wählen Sie Aus `discovery.sensors`Aus der Tabelle „Warteschlangenregistrierung“ [Queue_Registry].
Cloud-basiert	Wählen Sie Aus `discovery.cloud.sensors`Aus der Tabelle „Warteschlangenregistrierung“ [Queue_Registry].

3. In **Skalierungsfaktor** Feld, legen Sie einen Wert fest.

   Hinweis: Der Standardwert für den Höchstwert ist 3. Um den Skalierungsfaktor über 3 hinaus zu erhöhen, konfigurieren Sie `com.glide.processing.framework.max_thread_utilization_percentage`Eigenschaft. Weitere Informationen zu dieser Eigenschaft finden Sie unter Discovery-Eigenschaften. Anweisungen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie eine einzelne Warteschlange für Cloud- und IP-basierte Ereignisse

Konfigurieren Sie Cloud- und IP-basierte Ereignisse, um eine einzelne Warteschlange freizugeben, was die Auswirkungen von reduziert Discovery Auf App-Knoten.

Vorbereitungen

Bestätigen Sie Folgendes:

- Discovery-Administratorarbeitsbereich Verwendet Version 1.9.0 oder höher.
- ServiceNow AI Platform® Verwendet XP9, YP4 oder höher als YP4.
- Die `discovery.use.event.processing`Systemeigenschaft ist aktiviert. Weitere Informationen finden Sie unter Konfigurieren Discovery Dient zur Verwendung des Ereignis-Frameworks.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Bei Verwendung einer einzelnen Warteschlange Cloud-Discovery Aufträge haben häufig eine höhere Priorität als IP-basiert Discovery Aufträge. Durch die Trennung von cloudbasierten und IP-basierten Auftragswarteschlangen können Interferenzen zwischen vermieden werden Discovery Typen. Ausgleich ist jedoch möglich Discovery Durchsatz und Instanzauswirkung umfassen Kompromisse.

Instanzauswirkung basierend auf der Warteschlangenkonfiguration

Separate Warteschlangen	Einzelne Warteschlange
Mehr Worker-Threads, was mehr Datenbankaktivität bedeutet	Weniger Worker-Threads, was weniger Datenbankaktivität bedeutet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanzauswirkung basierend auf der Warteschlangenkonfiguration (Fortsetzung)

Separate Warteschlangen	Einzelne Warteschlange
Weitere Auswirkungen auf Aufträge, die nicht mit zusammenhängen Discovery	Weniger Auswirkungen auf Aufträge, die nicht mit zusammenhängen Discovery
Cloud-Discovery Wirkt sich nicht auf IP aus Discovery	Cloud-Discovery Kann IP vorgreifen Discovery

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Wählen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] die aus *discovery.event.separate.cloud.events*Eigenschaft.
3. Legen Sie fest **Wert** Feld bis **Falsch** .
4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie die Auftragspriorität von Background Worker für Ereignis-Framework

Konfigurieren Sie die Auftragspriorität von Hintergrundarbeitern, um zu verhindern, dass nicht kritische Aufgaben wichtige Arbeiten vorgreifen, was die Systemeffizienz und -Stabilität fördert.

Vorbereitungen

Bestätigen Sie Folgendes:

- Discovery-Administratorarbeitsbereich Verwendet Version 1.9.0 oder höher.
- ServiceNow AI Platform® Verwendet Version XP9, YP4 oder höher als YP4.
- Die *discovery.use.event.processing*Systemeigenschaft ist aktiviert. Weitere Informationen finden Sie unter Konfigurieren Discovery Dient zur Verwendung des Ereignis-Frameworks.
- Die *com.glide.queue.discovery.sensors.processing_jobs.priority*Und *com.glide.queue.discovery.cloud.sensors.processing_jobs.priority*Systemeigenschaften sind konfiguriert. Weitere Informationen finden Sie unter Systemeigenschaft hinzufügen .

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig haben Ereignis-Framework-Aufträge eine Priorität von 100. Wenn Discovery Ist wichtiger Arbeit vorweggenommen, können Sie verwenden *com.glide.queue.<queue_name>.processing_jobs.priority*Eigenschaft zum Anpassen der Priorität.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Wählen Sie einen oder mehrere Auftragstypen aus, für die Sie die Priorität anpassen möchten.

Auftragstyp	Aktion
IP-basiert	Wählen Sie Aus *com.glide.queue.discovery.sensors.processing_jobs* der Tabelle „Systemeigenschaften“ [sys_properties].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auftragstyp	Aktion
Cloud-basiert	Wählen Sie Aus `com.glide.queue.discovery.cloud.sensors.processi` der Tabelle „Systemeigenschaften“ [sys_properties].

3. In **Wert** Feld eingeben `110` .

   Hinweis: Erhöhen der Zahl in **Wert** Das Feld senkt die Priorität des Auftrags, während es durch eine Verringerung der Anzahl erhöht wird.

4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie Ereignisprozessoren für die Ausführung auf bestimmten Knoten

Konfigurieren Sie *discovery.event.pin.jobs*Systemeigenschaft, mit der Ereignisprozessoren auf bestimmten Knoten ausgeführt und die Arbeit gleichmäßig verteilt werden können. Der Skalierungsfaktor berechnet die Anzahl der Knoten, pinnt Aufträge jedoch nicht an bestimmte Knoten an.

Vorbereitungen

Bestätigen Sie Folgendes:

- Discovery-Administratorarbeitsbereich Verwendet Version 1.9.0 oder höher.
- ServiceNow AI Platform® Verwendet Version XP9, YP4 oder höher als YP4.
- Die *discovery.use.event.processing*Systemeigenschaft ist aktiviert. Weitere Informationen finden Sie unter Konfigurieren Discovery Dient zur Verwendung des Ereignis-Frameworks.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die *discovery.event.pin.jobs*Die Systemeigenschaft bestimmt, wie Aufträge Knoten zugewiesen werden. Wenn diese Eigenschaft auf festgelegt ist **Wahr** , Aufträge werden gleichmäßig auf bestimmte Knoten verteilt, die Flexibilität bei der Planung ist jedoch eingeschränkt. Wenn die Eigenschaft auf festgelegt ist **Falsch** , Aufträge werden zufällig zugewiesen, was zunehmen kann Discovery Durchsatz.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Wählen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] die aus *discovery.event.pin.jobs*Eigenschaft.
3. Legen Sie fest **Wert** Feld bis **Wahr** .
4. Wählen Sie **Aktualisieren**.

Nach dem Klonen Discovery Konfiguration

Wenn ein Klon auftritt, Discovery Zeitpläne werden aus der Quellinstanz in die Zielinstanz kopiert. Eine zusätzliche Konfiguration ist erforderlich, damit diese Zeitpläne in der Zielinstanz ordnungsgemäß funktionieren, sodass Sie Cloud- und IP-basiert ordnungsgemäß konfigurieren können Discovery Plant und sorgt für optimale Leistung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Allgemeine Informationen zum Klonen von Instanzen finden Sie unter HÄUFIG GESTELLTE Fragen klonen – häufig gestellte Fragen [KB0715621] artikel in Now Support Knowledge Base.

Anweisungen zum Deaktivieren oder Abbrechen von Discovery Zeitplan nach dem Erstellen eines Klons finden Sie unter Ein Post-Clone-Skript zum Deaktivieren und Abbrechen von Discovery-Zeitplänen [KB0789119] artikel in Now Support Knowledge Base.

Zielkonfiguration nach dem Klonen für IP-basiert Discovery Zeitpläne

Nach Abschluss von Klon anfordern Die Konfiguration des Prozesses nach dem Klonen wird durch bestimmt MID-Server Auswahlmethode, die Sie in ausgewählt haben Discovery Zeitplan für die Quellinstanz.

Zielinstanzkonfiguration für IP-basiert Discovery Zeitpläne

Methode für MID-Server-Auswahl	Nächste Schritte
Spezifischer MID	Aktualisieren Sie MID-Server Datensatz für jeden Discovery Zeitplan.
Cluster	Erstellen Sie den Cluster, und hängen Sie an MID-Server Auf den Cluster und aktualisieren Sie dann den Clusternamen in Discovery Zeitplan. Alternativ können Sie den MID-Cluster-Datensatz [ecc_Agent_Cluster] aus den Klon-Ausschlusstabellen [Clone_Data_exclude] entfernen. Weitere Informationen finden Sie unter Schließen Sie eine Tabelle vom Klonen aus .
Verhalten verwenden	Erstellen Sie das Verhalten, erstellen Sie eine Funktionalität, oder hängen Sie eine vorhandene Funktionalität an, und kehren Sie dann zurück zu Discovery Planen Sie das Verhalten, und hängen Sie es an Discovery Zeitplan. **Hinweis:** Discovery Funktionalitäten werden nicht mit einer Instanz geklont.
Automatische Auswahl	Verifiziert, dass alle MID-Server in der Zielinstanz mit Ziel-IP-Bereichen, unterstützten Anwendungen und Fähigkeiten eingerichtet sind.

Zielkonfiguration nach dem Klonen für Cloud-Discovery Zeitpläne

Nach Abschluss von Klon anfordern Prozess, müssen Sie auf die Tabelle „Cloud-Service-Account“ [cmdb_ci_Cloud_Service_Account] zugreifen und die Service-Accounts mit dem richtigen Verweis auf aktualisieren Discovery Anmeldeinformationen. Sie müssen auch die MID-Server für aktualisieren Discovery Zeitplan. Zusätzliche Konfiguration nach dem Klonen wird durch bestimmt MID-Server Auswahlmethode, die Sie im Original ausgewählt haben Discovery Zeitplan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zielinstanzkonfiguration für Cloud-Discovery Zeitpläne

Methode für MID-Server-Auswahl	Nächste Schritte
Spezifischer MID	Aktualisieren Sie MID-Server Datensatz für jeden Discovery Zeitplan.
Cluster	Erstellen Sie den Cluster, und hängen Sie an MID-Server Auf den Cluster und aktualisieren Sie dann den Clusternamen in Discovery Zeitplan. Alternativ können Sie den MID-Cluster-Datensatz [ecc_Agent_Cluster] aus den Klon-Ausschlusstabellen [Clone_Data_exclude] entfernen. Weitere Informationen finden Sie unter Schließen Sie eine Tabelle vom Klonen aus .
Verhalten verwenden	Erstellen Sie das Verhalten, erstellen Sie eine Funktionalität, oder hängen Sie eine vorhandene Funktionalität an, und kehren Sie dann zurück zu Discovery Planen Sie das Verhalten, und hängen Sie es an der Zielinstanz an. **Hinweis:** Discovery Funktionalitäten werden nicht mit einer Instanz geklont.
Automatische Auswahl	Überprüfen Sie, ob alle MID-Server mit Ziel-IP-Bereichen, unterstützten Anwendungen und Fähigkeiten eingerichtet sind.

Weitere Informationen finden Sie unter Cloud-Discovery-Zeitpläne nach dem Instanzklon fehlgeschlagen [KB1759363] artikel in Now Support Knowledge Base.

Klonausschlüsse

Anmeldeinformationsaliasse werden geklont, ihre Anmeldeinformationen werden jedoch nicht geklont. Wenn Discovery Zeitpläne haben Anmeldeinformationsaliasse. Sie müssen zur Tabelle „Aliasse für Verbindungen und Anmeldeinformationen“ [sys_alias] wechseln und bestätigen, dass der Alias auf die richtigen Anmeldeinformationen verweist. Aktualisieren Sie nach dem Klonen Discovery Plant und fügt Anmeldeinformationen in der Zielinstanz hinzu.

Außerdem nein MID-Server Zugehörige Tabellen werden geklont. Weitere Informationen finden Sie unter MID-Server und -Klone [KB0786475] artikel in Now Support Knowledge Base.

Zugehörige Informationen

Mit Instanz Klon

Discovery verwenden

Ausführen Discovery Plant und führt aus Discovery Probes, Sensoren und Muster, um Ihre IT-Ressourcen zu finden und hinzuzufügen CMDB.

- Erkennungen im Netzwerk ausführen
- Discovery-Probes und -Sensoren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster und horizontale Erkennung
- Discovery Ressourcennutzung
- Monitoring von Erkennungen und Problemlösung

Erkennungen im Netzwerk ausführen

Sie können Erkennungen über Zeitpläne oder Skripts ausführen, um Konfigurationselemente zu erstellen, Subnetze zu definieren oder Ressourcen in AWS- und Azure-Clouds zu erkennen.

Voraussetzungen für die MID Server-Konfiguration

Stellen Sie vor dem Erstellen eines Discovery-Zeitplans sicher, dass Ihre MID Server ordnungsgemäß konfiguriert sind.

- **Unterstützte Applikationen**: Wählen Sie die Anwendungen aus, die den MID Server verwenden dürfen. Sie können die Anwendungsoption **ALLE** verwenden, damit alle Anwendungen den MID Server verwenden können.
- **IP-Bereiche**: Definieren Sie die IP-Adressbereiche, die der MID Server scannen kann. Um MID Server-Treffer zu finden, muss der im Erkennungszeitplan konfigurierte IP-Bereich in die Bereiche fallen, die von einem oder mehreren MID Servern unterstützt werden.

  Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Bereich auf die IP-Adresse, über die Sie die Kontrolle haben, und schließen Sie unnötige Bereiche aus.

- **Fähigkeiten**: Erstellen Sie die Fähigkeiten, die der MID Server unterstützt. Sie können die Fähigkeitenoption **ALLE** verwenden, damit alle Anwendungen den MID Server verwenden können.

Voraussetzungen für die Discovery-Konfiguration

Stellen Sie sicher, dass Ihre MID Server sich auf den erkannten Geräten authentifizieren können und dass sie ordnungsgemäß Konfigurationselemente klassifizieren können.

- **Anmeldeinformationen**: Konfigurieren Sie die MID Server mit den Anmeldeinformationen, die sie für die Abfrage der Geräte im Netzwerk benötigen. Der MID Server testet alle verfügbaren Anmeldeinformationen auf jedem erkannten Gerät und erzeugt dann eine Affinität für alle erfolgreichen Anmeldeinformationen. Weitere Informationen finden Sie unter Anmeldeinformationsaffinität für Discovery und Orchestration .
- **Klassifizierungen**: Die in der Basisplattform bereitgestellten Geräte- und Prozessklassifizierungen reichen normalerweise aus. Erstellen Sie nach Bedarf Klassifizierungen für die Geräte, Prozesse und Anwendungen im Netzwerk, die nicht von den Standardklassifizierern abgedeckt werden.

Erste Schritte zur Ausführung einer Erkennung

1. Verwenden Sie die Discovery-Konfigurationskonsole, um mit der Erkennung zu beginnen. Die Konsole bietet Konfigurationsoptionen, mit denen Sie die Gerätetypen, Anwendungen, Softwaredateien und Software-CIs auswählen können, die Discovery erkennen soll. Wenn Sie ein CI auswählen, das vom Scannen ausgeschlossen werden soll, deaktiviert die Instanz die/den zugehörige(n) Probe oder Klassifizierer, die/den Discovery zum Identifizieren des CI verwendet. Informationen zu den ersten Schritten finden Sie unter Discovery Konfigurationskonsole.
2. Ermitteln Sie die Art der Erkennung, die ausgeführt werden soll:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie eine *CI-Erkennung* aus, um die Geräte, Computer und Anwendungen in Ihrem Netzwerk zu ermitteln. Das ist die häufigste Art der Erkennung. Führen Sie die CI-Erkennung über den Erkennungszeitplan aus. Sie können einen wiederkehrenden Zeitplan einrichten oder eine Erkennung bei Bedarf ausführen. Der Erkennungszeitplan bietet auch Konfigurationsoptionen für MID Server und die Shazzam-Port-Probe.
- Führen Sie eine *Netzwerkerkennung* aus, um die internen IP-Netzwerke in Ihrer Organisation zu ermitteln. Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung nicht erforderlich. Diese Erkennung ist für Organisationen konzipiert, die in ihren Netzwerken keine vollständigen Kenntnisse der für Discovery verfügbaren IP-Adressen haben.
- Führen Sie eine *serverlose Erkennung* aus, um Anwendungen auf Hostcomputern zu ermitteln, ohne zunächst den Host erkennen zu müssen. Die serverlose Erkennung basiert auf Infrastrukturmustern zum Untersuchen von CIs auf einem Host. Bei dieser Art von Erkennung werden die Scanphase und Klassifizierungsphase der Erkennung übersprungen. Zur Verwendung dieser Art von Erkennung benötigen Sie profunde Kenntnisse über Muster. Informationen zu ersten Schritten mit Mustern finden Sie unter Muster und horizontale Erkennung.

3. Nachdem Sie eine Erkennung ausgeführt haben, überwachen Sie die Ergebnisse der Erkennung, und beheben Sie gegebenenfalls auftretende Fehler:
   - Verwenden Sie den Erkennungsstatus, um eine Zusammenfassung einer Erkennung anzuzeigen und auf die ECC-Warteschlange zuzugreifen, die die Aktivität von Probes und Sensoren sowie die tatsächliche XML-Nutzlast anzeigt, die an eine oder von einer Instanz gesendet wird.
   - Verwenden Sie Discovery-AdministratorarbeitsbereichDient zur Überwachung laufender Discovery-Vorgänge.
   - Verwenden Sie die Discovery-Homepage, um auf Details über alle Zeitpläne, Cloud-Ressourcen (virtuelle Computer), erkannten Geräte und zugehörigen Fehler zuzugreifen, die möglicherweise aufgetreten sind. Die Fehlerdetails schließen mögliche Nachbesserungsschritte ein.

Zugehörige Informationen

Discovery Ressourcennutzung

Discovery Konfigurationskonsole

Verwenden Sie die Discovery-Konfigurationskonsole, um zu bestimmen, welche Art von CIs und CI-Informationen Sie erkennen möchten.

Standardmäßig findet Discovery alle Informationen in Ihrem Netzwerk, die in Probes und Mustern angegeben sind. Verwenden Sie die Steuerelemente in dieser Konsole, um die Daten auszuwählen, die Discovery der CMDB hinzufügt, die Ihre Organisation benötigt. Sie können die folgenden Aspekte von Discovery steuern:

- Die Discovery ganzer CI-Typen, z. B. Windows Server.
- Die Erkennung bestimmter CI-Details, z. B. BS-Informationen zu Windows Server.
- Die Discovery von ARP-Daten für Netzwerke, UNIX, Und Windows Geräte.
- Erkennung von Softwarepaketen, die von Ihnen hinzugefügte Stichwortbegriffe enthalten, zum Beispiel Hotfix und Sicherheitsupdate
- Dateibasiert Discovery Von Software auf UNIX Und Windows Durch bestimmte Erweiterung oder einen bestimmten Ordner, z. B. .cert oder .ext

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Discovery gibt alle Daten vom Ziel an die Instanz zurück, bevor die Konsoleneinstellungen angewendet werden. Wenn die Instanz die CMDB aktualisiert, ignoriert sie alle ausgeschlossenen Daten.

Anforderungen und Zugänglichkeit

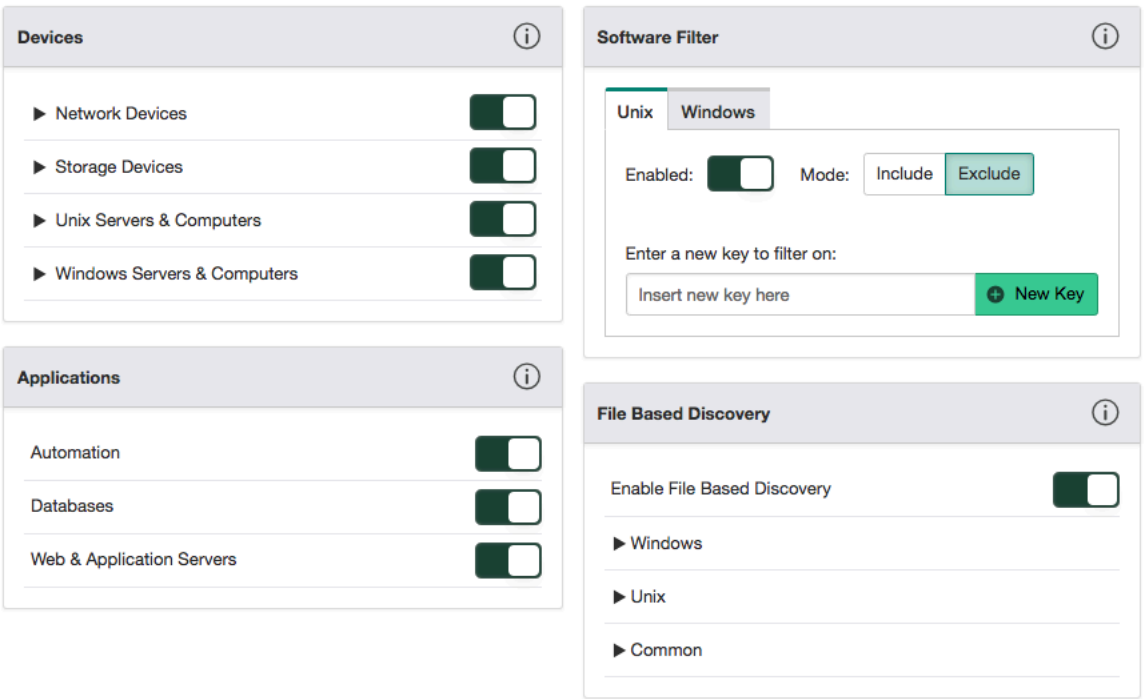
Wenn Sie Internet Explorer verwenden, müssen Sie Version 8 oder höher verwenden. Die Konfigurationskonsole unterstützt die Tastaturnavigation und Sprachausgabe.

Konsolenübersicht

Navigieren Sie zum Öffnen der Konfigurationskonsole zu **Discovery-Definition** > **Konfigurationskonsole**an.

Die Konsole ist in die folgenden Abschnitte unterteilt. Verwenden Sie die Umschalttasten, um verschiedene Optionen zu aktivieren (rechts zum Aktivieren, links zum Deaktivieren).

- **Geräte**: Netzwerkgeräte wie Drucker, Speichergeräte wie Speicher-Switches sowie Unix- und Windows-Computer
- **Anwendungen**: Automatisierungsanwendungen wie Puppet, Datenbanken wie MSSQL sowie Webserver wie Tomcat
- **Softwarefilter** : UNIX Und Windows Anwendungen, die von Ihnen eingegebene Stichwörter enthalten oder ausschließen
- **Dateibasierte Discovery** : Softwaredateien nach Pfad, Ordner und Erweiterungen, die gescannt oder ignoriert werden sollen



Geräteerkennung

Durch Deaktivieren der Erkennung von Gerätedaten auf oberster Ebene werden die zugehörigen Port-Probes und Musterbibliotheken deaktiviert. Beispielsweise wird durch das Blockieren von Netzwerkgeräten die Port-Probe „SNMP“ deaktiviert. Das Blockieren von Geräten auf der zweiten Ebene der Hierarchie hat folgende Auswirkungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geräteklassenkategorien deaktivieren Klassifizierer.
- Geräteinformationskategorien deaktivieren Probes und Musterbibliotheken.

Sie können die Erkennung von ARP-Daten aktivieren oder deaktivieren. Diese Option ist standardmäßig deaktiviert. Nach dem Upgrade werden ARP-Daten erst erkannt, wenn Sie sie in der Discovery-Konfigurationskonsole aktivieren. ARP-Daten können in drei Geräteklassen gesteuert werden: Netzwerk, UNIX, Und Windows.

Zu den potenziellen Auswirkungen gehören:

- Ohne ARP-Daten wird der Netzwerkpfad möglicherweise nicht untersucht, wenn Sie verwenden Service-Mapping Mit L2 oder L3 Discovery.
- Nach dem Upgrade und der erneuten Ausführung Discovery, ARP-Daten werden für vorhandene Kunden nicht ausgefüllt. Alte Daten werden gemäß der Löschstrategie des sofort einsatzbereiten Verhaltens (OOB) automatisch geleert. Dies ist eine einmalige Aktivität, es sei denn, Sie ändern die OOB-Konfiguration. Daher müssen Sie ausführen Discovery Zeitplan basierend auf dem Gerätevolumen.
- Wenn Sie die Netzwerkgerätesuche für Netzwerkgeräte deaktiviert haben, sollten Sie ARP auch deaktiviert lassen, um das alte Verhalten vor dem Upgrade beizubehalten.

Anwendungserkennung

Die Deaktivierung der Erkennung von Anwendungsdaten wirkt sich auf alle Hostgeräte aus, auf denen die Anwendung ausgeführt wird. Beispiel: Wenn Sie konfigurieren Discovery Um Datenbanken zu ignorieren, werden keine Informationen für Linux oder gesammelt Windows Datenbanken. Umgekehrt, wenn Sie das System so konfigurieren, dass ein Gerätetyp wie z. B. ignoriert wird Windows Server, es werden keine Datenbanken untersucht, die auf diesem Server ausgeführt werden, auch wenn sie für die Erkennung konfiguriert sind. Die Instanz kann die auf einem Server ausgeführten Anwendungen erst identifizieren, nachdem sie diesen Server erkannt hat.

Wenn Sie ein Element aus dem Abschnitt **Applikationen** ausschließen, deaktiviert das System den entsprechenden Prozessklassifizierer. Die zu dieser Klassifizierung gehörenden Probes, einschließlich der Probe „Horizontal Pattern“, der Muster startet, werden nie gestartet.

Erkennung von Software

Sie können die Discovery von Softwarepaketen basierend auf den Stichwörtern filtern, für die sie enthalten Windows Und UNIX Computer. Ein Stichwort kann ein beliebiger Begriff sein, der in einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Softwarepaketnamen enthalten ist. Stichwörter zum Filtern von Software werden in der Tabelle „Softwarefilterschlüssel“ [discovery_spkg_keys] gespeichert. Das System stellt keine Standardfilterschlüsselwörter für bereit UNIX Software.

Wichtig: Die Softwarefilterung nach Stichwörtern erfolgt, nachdem die Probe ihre Nutzlast an die Instanz und nicht auf dem Zielhost zurückgegeben hat.

Die folgenden Standardstichwörter werden für bereitgestellt Windows Und werden standardmäßig herausgefiltert:

- Hotfix
- Sprachpaket
- Sicherheitsupdate

File-based Discovery

Sie können konfigurieren Discovery Dient zum Scannen oder Ignorieren von Pfaden, Ordnern und Erweiterungen für die dateibasierte Discovery. Discovery Scannt dann einen Windows Oder UNIX Dateisystem mit diesen Einstellungen zum Identifizieren von Dateifingerabdrücken. Installierte Softwareprodukte, die mit diesen Attributen erkannt werden, werden mit Produkten in einer umfangreichen Bibliothek zur Softwarenormalisierung abgeglichen.

Auswirkungen auf Discovery-Tabellen

Diese Tabelle zeigt, was in Discovery-Tabellen deaktiviert ist, wenn Sie die Discovery-Konfigurationskonsole verwenden.

Bei Deaktivierung von	Deaktiviertes Feld
Gerätekategorien der obersten Ebene, zum Beispiel: • Netzwerkgeräte • Windows-Server und -Computer • Unix-Server und -Computer	In der Tabelle „Anschlussprobes“ [discovery_port_probe] ist das Feld **CIs** deaktiviert. Die Tabelle „Anschlussprobes“ [discovery_port_probe] wird aus der Tabelle „Protokollkategorie“ [discovery_category_protocol] referenziert.
Geräteklassen, zum Beispiel: • Windows 2008 Server • Linux-Server	In der Tabelle „Klassifizierer“ [discovery_classy] für den zugehörigen Klassifizierer ist das Feld **Aktiv** deaktiviert. Die Tabelle „Klassifizierer“ [discovery_classy] wird in der Tabelle „Geräteklassifizierungskategorie“ [discovery_category_device_class] referenziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Deaktivierung von	Deaktiviertes Feld
Geräteinformationen, zum Beispiel: • Erkundung von Netzwerkgeräten • Windows-Speicher • ARP-Daten	Die **Aktiv** Das Feld ist sowohl für die Klassifizierungsprobes [Discovery_Classifier_Probe] als auch für deaktiviert Discovery Muster-Tabellen [sa_pattern] für die zugehörige Probe oder das zugehörige Muster, die die Identifizierung und Untersuchung des CI durchführt. Diese Tabellen werden von der Tabelle „Geräteinfokategorie“ [discovery_category_device_info] referenziert.
Applikationen	Das Feld **Aktiv** ist in der Tabelle „Prozessklassifizierer“ [discovery_classy] für den zugehörigen Prozessklassifizierer deaktiviert. Die Tabelle „Prozessklassifizierer“ [discovery_classy_proc] wird in der Tabelle „Anwendungskategorie“ [discovery_category_appl] referenziert.

Hinweis: Wenn Sie Muster für die Discovery verwenden und die Erkennung von Geräteklassen oder Geräteinformationen deaktivieren, deaktiviert das System die Musterbibliotheken, die die Geräteinformationen erfassen. Beispiel: Wenn Sie einen haben Windows Muster, in dem Sie eine gemeinsame Bibliothek erstellen, die Betriebssysteminformationen sammelt, und dann die Sammlung von Betriebssystemdaten deaktivieren. Die gemeinsame Bibliothek, die Betriebssystemdaten sammelt, ist deaktiviert. Weitere Informationen zum Vorgang der gemeinsamen Bibliothek finden Sie unter KB1698521: Muster erstellen oder anpassen .

CIs aus der Erkennung ausschließen

Verwenden Sie die Discovery-Konfigurationskonsole, um zu bestimmen, welche Geräte und Anwendungen von der Erkennung ausgeschlossen werden sollen.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**an.
2. Wenn Sie bestimmte Geräte und Geräteinformationen ausschließen möchten, erweitern Sie die Kategorie für Gerätetypen.
3. Um zu sehen, welche Anwendungen sich deaktivieren lassen, bewegen Sie den Mauszeiger über den Anwendungstyp.
4. Klicken Sie auf den Umschalter, um die CIs zu deaktivieren, die Sie von der Erkennung ausschließen möchten.
   Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Zu erkennende Anwendungen und Geräte anpassen

Mithilfe der Discovery-Konfigurationskonsole können Sie Anwendungen und Geräte aktivieren und deaktivieren. Einige sind als sofort einsatzbereit aufgeführt, aber Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können auch anpassen, welche spezifischen Anwendungen und Geräte Sie gemäß Ihren spezifischen Anforderungen in die Erkennung einschließen möchten.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Passen Sie die Anwendungen an.
   a. Navigieren zu **Discovery-Definition** > **Anwendungskategorien**an.
   b. Klicken Sie Auf **Automatisierung** , **Datenbanken** , Oder **Web- Und Anwendungsserver** .
   c. Entsperren Sie die Liste der Prozessklassifizierer.
   d. Um eine Anwendung aus der Liste zu entfernen, markieren Sie sie, und klicken Sie dann zum Entfernen auf **X**.
   e. Um sie der Liste hinzuzufügen, geben Sie den Namen in das Feld ein, und drücken Sie die **Eingabetaste**.
   f. Klicken Sie auf **Sperren** Symbol.
   g. Klicken Sie auf **Aktualisieren**.
   Bei der nächsten Ausführung von Discovery werden die von Ihnen konfigurierten Typen spezifischer Anwendungen verarbeitet.
2. Passen Sie Geräte an.
   a. Navigieren zu **Discovery-Definition** > **Geräteinformationskategorien**an.
   b. Um einen neuen Datensatz zu erstellen, klicken Sie auf **Neu**.
   c. Geben Sie die Details ein, und klicken Sie auf **Senden**.
   d. Um ein vorhandenes Gerät zu aktualisieren, klicken Sie auf eines der aufgelisteten Geräte.
   e. Nehmen Sie Änderungen vor, und klicken Sie auf **Aktualisieren** oder **Löschen**.

Zu erkennende Software filtern

Verwenden Sie die Discovery-Konfigurationskonsole, um die Software zu filtern, die Sie der CMDB hinzufügen.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**an.
2. Wählen Sie im Bereich „Softwarefilter“ die Registerkarte für das gewünschte Betriebssystem (**Unix** oder **Windows**) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügen Sie Stichwörter zum Filtern von Softwarepaketen hinzu, bzw. löschen Sie sie.

   a. Um ein Stichwort hinzuzufügen, geben Sie es in das dafür vorgesehene Feld ein, und klicken Sie auf **Neuer Schlüssel**.

   b. Um ein Stichwort zu löschen, klicken Sie auf das rote **x**-Symbol rechts neben dem Stichwort.
   Discovery sucht nach Softwarepaketen, die diese Begriffe im ausgewählten Betriebssystem enthalten, und schließt sie entweder in die CMDB ein bzw. aus ihr aus. Zum Filtern von UNIX-Softwarepaketen stellt das System keine Standardstichwörter bereit, wohl aber für Windows:

   - Hotfix
   - Sprachpaket
   - Sicherheitsupdate

   Diese Standardstichwörter schließen Patch-bezogene Software standardmäßig aus. Entfernen Sie, um die Discovery von Sicherheits-BS-Patch zu aktivieren `Hotfix`Und `Security Update`Aus der Ausschlussliste. Dadurch kann Discovery Patch- und Hotfix-Daten in die CMDB einbeziehen.

4. Wählen Sie aus, ob Softwarepakete mit den Stichwörtern im Namen **einbezogen** oder **ausgeschlossen** werden sollen.

   - **Einbeziehen**: Es werden nur Softwarepakete hinzugefügt, die mit den Stichwörtern übereinstimmen.
   - **Ausschließen**: Es werden alle Softwarepakete hinzugefügt mit Ausnahme derjenigen, die mit den Stichwörtern übereinstimmen.

5. Deaktivieren Sie die Softwarefilterung für **UNIX** oder **Windows**.

   Wenn der Filter für ein Betriebssystem deaktiviert ist, werden alle erkannten Softwarepakete für dieses Betriebssystem der CMDB hinzugefügt, ohne dass eine Filterung stattfindet.

   Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Dateibasierte Discovery konfigurieren

Verwenden Sie die Discovery-Konfigurationskonsole zum Konfigurieren mehrerer Einstellungen, um Ihre gesamte installierte Software zu erkennen und zu verwalten.

Vorbereitungen

Erforderliche Rolle: administrator oder admin

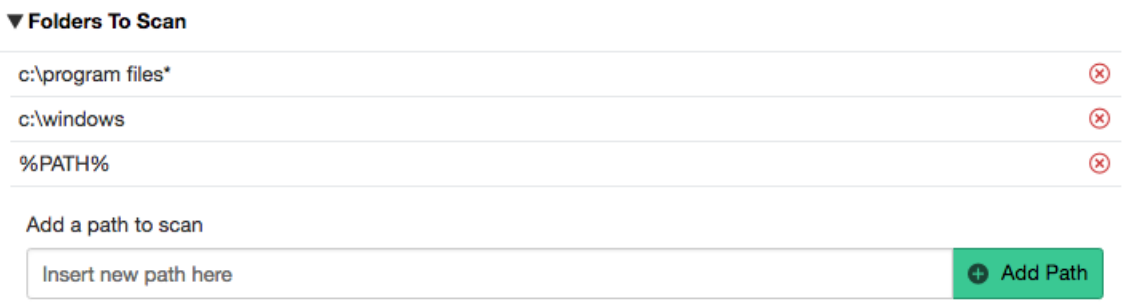
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**an.
2. Aktivieren Sie die File-based Discovery.
   Standardmäßig ist sie deaktiviert.
3. Wählen Sie anpassbare Optionen speziell für Windows- und UNIX-Computer sowie Optionen, die für beide Betriebssysteme gelten.
   Einige Optionen haben Standardwerte, andere (wie zu ignorierende Ordner und Erweiterungen) sind leer, bis Sie Werte hinzufügen.
4. Klicken Sie unter Windows und/oder UNIX auf den Pfeil, um die Zielpfadoptionen zu erweitern.
5. Konfigurieren Sie Standardoptionen.

   Zu scannende Ordner

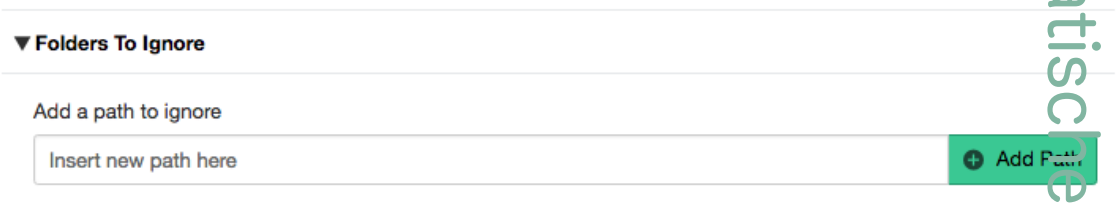
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gibt an, nach welchen Ordnern unter Windows und/oder UNIX gescannt werden soll. Standardwerte werden aufgelistet. Sie können auch zusätzliche Pfade zum Scannen hinzufügen.



Zu ignorierende Ordner

Gibt an, welche Ordner und untergeordneten Ordner/Dateien in der Liste der zu scannenden Windows- oder UNIX-Ordner ignoriert werden sollen. Wenn Sie beispielsweise „C:\Programme“ als zu scannenden Ordner angegeben haben, können Sie zusätzlich „C:\Programme\Temp“ als zu ignorierenden Ordner angeben. Wenn die dateibasierte Discovery einen Windows-Server scannt, werden alle Dateien und Unterordner unter C:\Programme mit Ausnahme von C:\Programme\Temp gescannt.

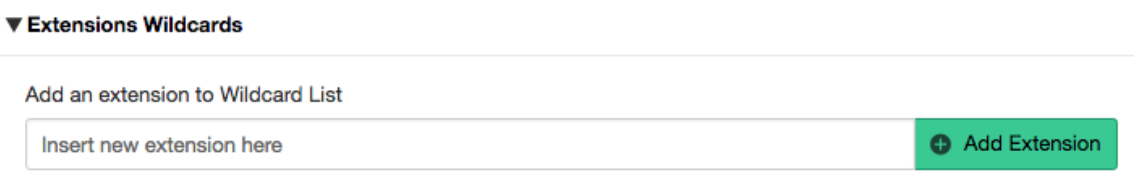


Ausschlussliste für Erweiterungen

Geben Sie Erweiterungen (.txt, .war, .exe usw.) an, die Sie für Windows ignorieren möchten.

Platzhalter für Erweiterungen

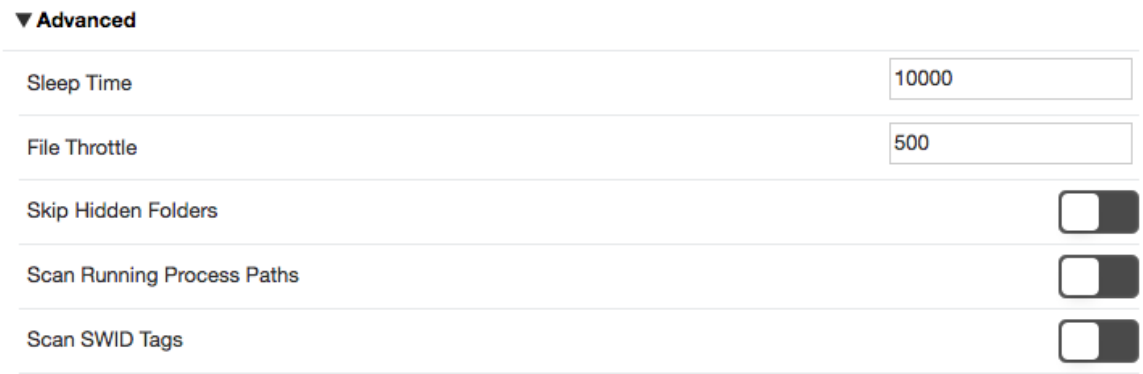
Geben Sie Erweiterungen (.cert, .crt usw.) an, nach denen Sie unter Windows immer scannen möchten. Dadurch können Sie nach Erweiterungen wie *.cert scannen, bei denen der Dateiname selbst möglicherweise nicht bekannt ist. Auf diese Weise können Sie Zertifikate (.cert oder .crt) und Java-Schlüsselspeicherdateien (.jks) erkennen.



6. Konfigurieren Sie **erweiterte Windows**-Einstellungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeit Energiesparmodus

Legt die Dauer des Ruhezustands in Millisekunden während jedes Drosselintervalls beim Scannen nach Windows-Dateien fest. Der Standardwert ist 10000. Ändern Sie diesen Wert nur, wenn Sie ein fortgeschrittener Benutzer sind. Wenn Sie ein fortgeschrittener Benutzer sind und eine Änderung vornehmen müssen, stellen Sie sicher, dass Sie die Einstellung auf einen Wert ungleich 0 festlegen.

Dateidrosselung

Legt die Anzahl der Dateien fest, die vor dem Ruhezustand unter Windows gescannt werden soll. Der Standardwert ist 500. Ändern Sie diesen Wert nur, wenn Sie ein fortgeschrittener Benutzer sind. Wenn Sie ein fortgeschrittener Benutzer sind und eine Änderung vornehmen müssen, stellen Sie sicher, dass Sie die Einstellung auf einen Wert ungleich 0 festlegen.

Versteckte Ordner überspringen

Überspringt ausgeblendete Ordner auf Zielcomputern, wenn nach Dateisignaturen gesucht wird. Bei Windows-Geräten hängt die Sichtbarkeit eines Ordners von einem Ausgeblendet-Attribut ab, das für jeden Ordner festgelegt werden kann.

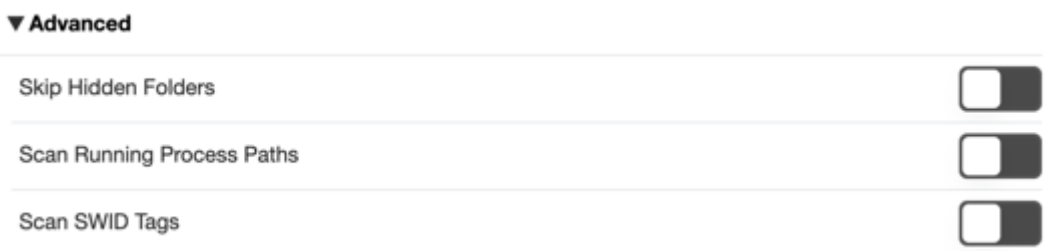
Laufende Prozesspfade scannen

Aktiviert die Verwendung laufender Prozesspfade in der Liste der Zielpfade zum Scannen. Dadurch werden automatisch Pfade hinzugefügt, die bekanntermaßen laufende Prozesse enthalten und daher höchstwahrscheinlich Dateien von Interesse für die Bestimmung von Softwareinstallationen enthalten.

SWID-Tags Scannen

Scannt nach und analysiert SWID-Tags (Softwareidentifizierungs-Tags). Diese Option ist nur sichtbar, wenn SAMP aktiviert ist. Wenn „SWID-Tags Scannen“ aktiviert ist, werden das Softwareprodukt, der Herausgeber und die Version in der Nutzlast zurückgegeben, die direkt in die Softwareinstallationstabelle eingefügt wird, wobei die Software-Abgleich-API umgangen wird. Standardmäßig ist sie deaktiviert.

7. Konfigurieren Sie **erweiterte UNIX**-Einstellungen.



Versteckte Ordner überspringen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überspringt ausgeblendete Ordner, wenn nach Dateisignaturen gesucht wird. Bei Unix-basierten Geräten sind dies Ordner, denen ein „.“ im Namen vorangestellt ist.

Laufende Prozesspfade scannen

Aktiviert die Verwendung laufender Prozesspfade in der Liste der Zielpfade zum Scannen. Dadurch werden automatisch Pfade hinzugefügt, die bekanntermaßen laufende Prozesse enthalten und daher höchstwahrscheinlich Dateien von Interesse für die Bestimmung von Softwareinstallationen enthalten.

SWID-Tags Scannen

Scannt nach und analysiert SWID-Tags (Softwareidentifizierungs-Tags). Diese Option ist nur sichtbar, wenn SAMP aktiviert ist. Wenn „SWID-Tags Scannen“ aktiviert ist, werden das Softwareprodukt, der Herausgeber und die Version in der Nutzlast zurückgegeben, die direkt in die Softwareinstallationstabelle eingefügt wird, wobei die Software-Abgleich-API umgangen wird. Standardmäßig ist sie deaktiviert.

8. Konfigurieren Sie **gemeinsame** Einstellungen für Windows oder UNIX.

Maximale Dateien

Legt die maximale Anzahl von Dateien fest, die erkannt werden sollen. Das ist die Anzahl der pro CI/IP gescannten Dateien.

Häufigkeit

Legt die Häufigkeit fest, mit der die dateibasierte Discovery für das CI ausgeführt wird.

Ergebnis

Die dateibasierte Discovery ist jetzt aktiviert, konfiguriert und zur Ausführung bereit. Weitere Informationen finden Sie unter Dateibasierte Discovery ausführen.

Anmeldeinformationen für Standardauthentifizierung erstellen

Erstellen Sie Anmeldeinformationen, um auf zuzugreifen ServiceNow® Instanz.

Vorbereitungen

Erforderliche Rolle: System_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung**.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: 100

5. Wählen Sie **Absenden**.

Ergebnis
Die Anmeldeinformationen für die Standardauthentifizierung zur Verwendung mit der Serverinstanz werden erstellt.

Horizontale Erkennung planen

Ein Discovery-Zeitplan bestimmt, nach welcher horizontalen Discovery sucht, wann sie ausgeführt wird und welche MID Servers Werden verwendet. Erstellen Sie einen Discovery-Zeitplan für Ihre lokale Umgebung oder einen Zeitplan für die Erkennung der Ressourcen in Ihrem Cloud-Service-Account.

Vorbereitungen
Stellen Sie sicher, dass Ihr Erkennungszeitplan den bewährten Best Practices für Sicherheit entspricht, z. B. indem Sie den Bereich der Erkennungsziele beschränken und die sichersten Anmeldeinformationen verwenden.

Stellen Sie sicher, dass Sie Ihre Anmeldeinformationen testen , bevor Sie einen Zeitplan ausführen. Ungültige Anmeldeinformationen sind eine der Hauptursachen für fehlgeschlagene Erkennungen.

Erforderliche Rollen: Discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können einen Discovery-Zeitplan verwenden, um die horizontale Discovery zu starten, die Probes, Sensoren und Mustervorgänge verwendet, um Ihr Netzwerk nach CIs zu durchsuchen. Verwenden Sie dieses Verfahren, um einen Zeitplan manuell aus dem zu erstellen **Discovery-Zeitpläne** Formular.

Service-Mapping Stellt auch einen Discovery-Zeitplan für die Top Down-Discovery bereit. Weitere Informationen finden Sie unter Erkennung von oben nach unten mithilfe von Service-Mapping planen.

Verwenden Sie **Discovery-Zeitpläne** Modul in DiscoveryAnwendung zu:

- Konfigurieren Sie einen Zeitplan zum Erkennen von Ressourcen in Ihrem Cloud-Servicekonto.
- Konfigurieren Sie einen Zeitplan zum Erkennen von Zertifikaten aus URL-Scans.
- Konfigurieren Sie die Geräteidentifikation nach IP-Adresse oder anderen Kennungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie fest, ob Anmeldeinformationen in Geräte-Probes verwendet werden.
- Benennen Sie MID-Server Zur Verwendung für einen bestimmten Discovery-Typ.
- Erstellen oder deaktivieren Sie einen Zeitplan, der steuert, wann die Erkennung in Ihrem Netzwerk ausgeführt wird.
- Konfigurieren der Verwendung mehrere Shazzam-Probes für den Lastenausgleich.
- Konfigurieren Sie die Verwendung mehrerer MID Servers für den Lastausgleich.
- Führen Sie einen Discovery-Zeitplan manuell aus.
- Führen Sie eine Discovery für eine einzelne IP-Adresse aus.

Hinweis: Um die Ausführungsergebnisse Ihrer Zeitpläne sowohl für die IP-basierte als auch für Cloud-Discovery anzuzeigen, verwenden Sie die Zusammenfassungen auf der Discovery-Homepage. Die Homepage veröffentlicht die Details aller möglicherweise aufgetretenen Fehler und zeigt mögliche Aktionen zur Behebung von Problemen an.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne** Zum Erstellen eines neuen Datensatzes.
2. Wählen Sie den Typ des Zeitplans zum Öffnen von:
   - **Neu**: Es wird ein neuer horizontaler Zeitplan für die Erkennung von Komponenten in Ihrem Netzwerk erstellt.
   - **Schnelle Discovery** : Führt eine horizontale Discovery für eine einzelne IP-Adresse aus, ohne dass ein Zeitplan erforderlich ist.
   - **Einen Cloud-Discovery-Zeitplan erstellen**: Mit dem Discovery Manager-Assistenten wird ein Zeitplan für die Erkennung von Ressourcen in einem Cloud-Servicekonto erstellt.
3. Füllen Sie das Formular „Discovery-Zeitplan“ aus , Mithilfe der Felder in der Tabelle. Weitere Informationen finden Sie unter Formularreferenz für Discovery-Zeitplan.
4. Klicken Sie mit der rechten Maustaste auf den Header des Datensatzes , und wählen Sie im Kontextmenü **Speichern** aus.
5. Um einen Bereich von zu erkennenden IP-Adressen zu erstellen, klicken Sie unter **Zugehörige Links** auf **Kurzbereiche**.

   Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Bereich der Erkennungsziele, indem Sie unnötige Netzwerke und Geräte ausschließen.

6. Definieren Sie die Häufigkeit der Ausführung des Zeitplans wie in beschrieben Optionen für Discovery-Zeitpläne ausführen.

Schnell-Discovery ausführen

Mit einer Schnell-Discovery bzw. mit DiscoverNow können Administratoren die Erkennung einer CI-Konfiguration für eine einzelne IP-Adresse ausführen, ohne dass ein Zeitplan benötigt wird.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Plattform wählt automatisch den richtigen MID Server für die Erkennung aus, wenn dieser mit der ausgewählten IP-Adresse verknüpft ist. Wenn für das Netzwerk, in dem diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Adresse angezeigt wird, kein MID Server konfiguriert ist, können Sie einen MID Server auswählen. Verwenden Sie diese Funktion, um neue Geräte im Netzwerk zu erkennen, sobald sie mit dem Netzwerk verbunden sind, anstatt auf eine regelmäßig durchgeführte, geplante Erkennung zu warten.

Um das System so zu konfigurieren, dass automatisch der zu verwendende MID Server ermittelt wird, richten Sie die IP-Bereichsfunktionen für jeden MID Server in Ihrem System ein.

Sie können DiscoverNow aus einem Discovery-Zeitplanformular oder Skript ausführen.

Hinweis: Schnell-Discovery mit einer IPv6-Zieladresse wird unterstützt.

Prozedur

1. Öffnen Sie Schnell-Discovery über einen der folgenden Navigationspfade:
   - Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und klicken Sie auf **Schnelle Discovery** In der Header-Leiste.
   - Navigieren zu **Discovery** > **Startseite** Und klicken Sie auf **Discovery-Schnellstart** Unter der Kachel Zeitpläne.

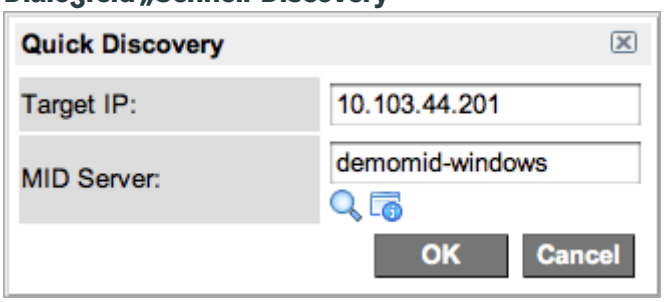
   Ein Dialogfeld wird angezeigt, in dem Sie zur Eingabe einer IP-Adresse und des Namens des zu verwendenden MID Servers aufgefordert werden. Nur MID-Server, die **In Betrieb** und **Überprüft** sind, stehen zur Verfügung.
2. Geben Sie die Ziel-IP-Adresse für eine Erkennung in das Feld **Ziel-IP** ein.

   Hinweis: DiscoverNow unterstützt derzeit keine IP-Netzwerkerkennung. Stellen Sie sicher, dass Sie nur eine einzelne IP-Adresse und nicht das gesamte Netzwerk eingeben, zum Beispiel 10.105.37.0/24.

   Wenn ein MID Server dem Subnetz zugewiesen ist, das die Ziel-IP-Adresse enthält, und derzeit den Betriebsstatus **In Betrieb** aufweist, wird der Name automatisch im Feld **MID Server** angezeigt. Wenn mehrere MID Server gefunden werden, wählt das System einen für Sie aus. Der Wert im Feld **MID Server** kann überschrieben werden, wenn Sie einen anderen MID Server auswählen möchten.

   Wichtig: Wenn der ausgewählte MID Server Teil eines Clusters mit Lastenausgleich und aus irgendeinem Grund nicht verfügbar ist, weist die Instanz Schnell-Discovery *keinen* anderen MID Server aus diesem Cluster zu. Sie müssen einen anderen MID Server aus der Liste der entsprechenden MID Server auswählen.
3. Wenn für dieses Netzwerk kein MID Server definiert ist, wählen Sie einen in der Liste der verfügbaren MID Server aus.

Dialogfeld „Schnell-Discovery“

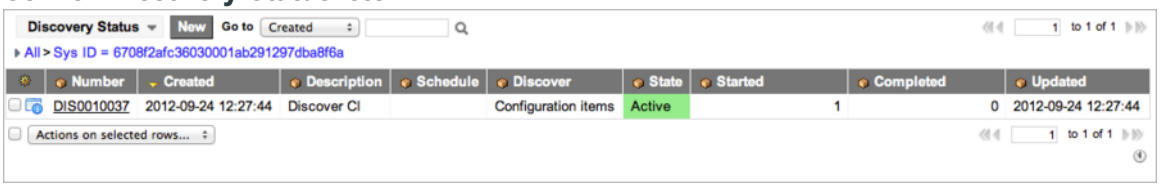


4. Klicken Sie auf **OK**, um die Erkennung auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Statusdatensatz für die Erkennung wird angezeigt. Die Spalte **Zeitplan** ist leer, da dieser Erkennung kein Zeitplan zugeordnet ist.

Schnell-Discovery-Statusliste



DiscoverNow aus einem Skript ausführen

Sie können DiscoverNow aus einem Skript ausführen, etwa aus einem Hintergrundauftrag, aus einer Geschäftsregel oder aus Webservices.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie das folgende Skript:

```
var d = new Discovery();
var statusID = d.discoveryFromIP(TARGET_IP, TARGET_MIDSERVER);
```

   Die Methode *`discoveryFromIP`* nimmt zwei Argumente an: *`IP`* und *`MID Server`*. Das Argument *`IP`* ist obligatorisch, das Argument *`MID Server`* optional.

2. Geben Sie zur Auswahl des MID Servers entweder die *`sys_id`* oder den Namen des MID Servers als Argument an.
   Wenn Sie keinen MID Server benennen, versucht das System automatisch, einen gültigen Server zu finden. Gültige MID Server weisen den Status **In Betrieb** auf und können die angegebene IP-Adresse erkennen. Wenn das System einen gültigen MID Server erkennt und eine Discovery ausführt, gibt die Methode *`discoveryFromIP`* die *`sys_id`* des Discovery-Statusdatensatzes zurück. Wenn diese IP-Adresse von keinem MID Server erkannt wird, gibt die Methode den Wert **undefined** zurück.

   Wenn Sie TARGET_MIDSERVER manuell angeben, validiert das System den angegebenen Wert und stellt sicher, dass die Tabelle „MID Server“ den angegebenen MID Server-Datensatz enthält. Wenn die Validierung erfolgreich ist, gibt die Methode discoveryFromIP die sys_id des Statusdatensatzes der Erkennung zurück. Wenn die Validierung fehlschlägt, gibt die Methode den Wert **undefined** zurück.

Erkennungsergebnisse validieren

Validieren Sie die Ergebnisse Ihrer Erkennung, indem Sie auf die ECC-Warteschlange zugreifen, die XML-Nutzlast analysieren und das Discovery-Protokoll überprüfen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

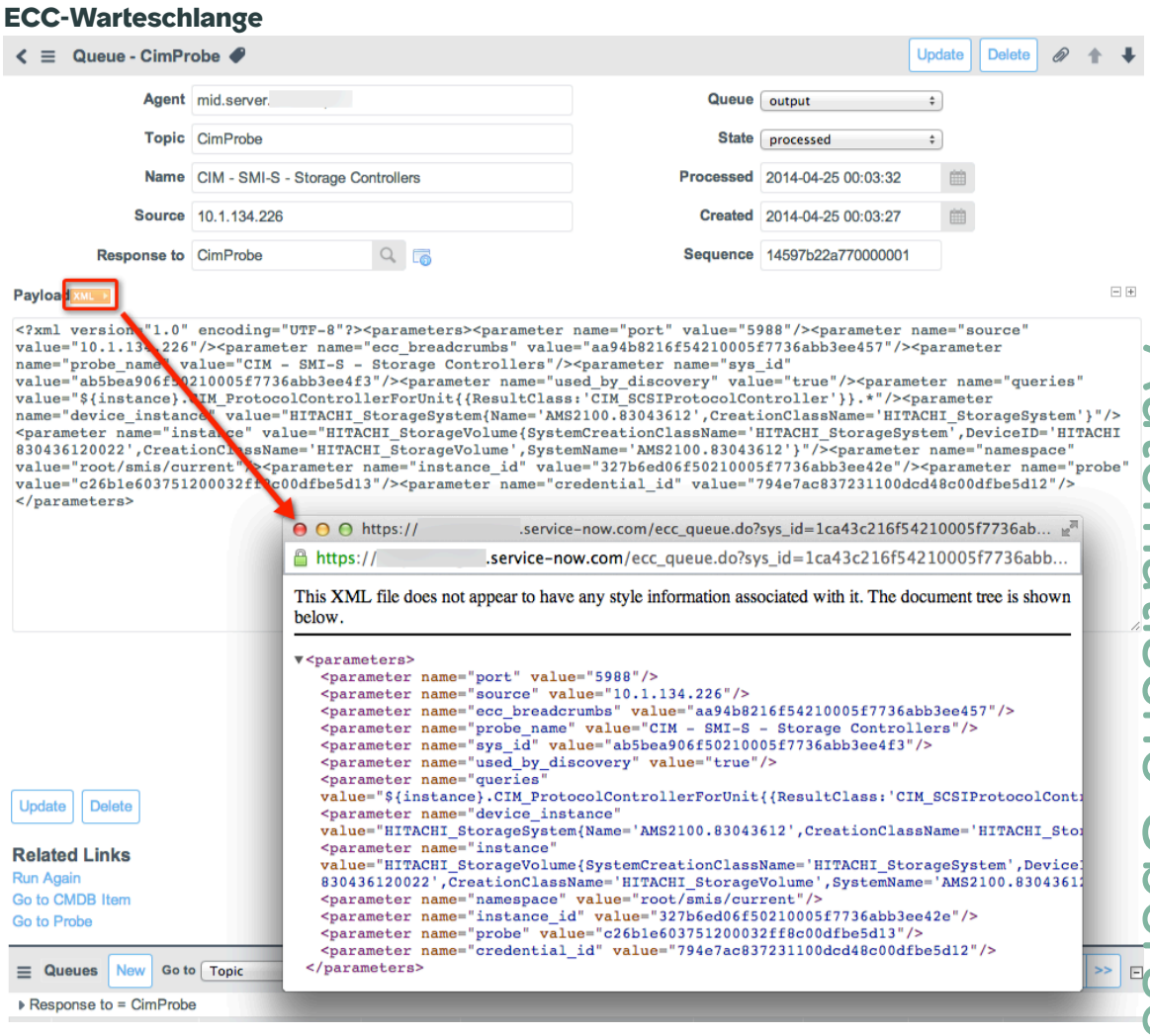
Warum und wann dieser Vorgang ausgeführt wird

Anfängliche Erkennungen ergeben häufig unerwartete Ergebnisse, zum Beispiel zuvor unbekannte Geräte und Prozesse oder fehlgeschlagene Authentifizierungen. Die Ergebnisse müssen auch bekannte Geräte genau identifizieren und die CMDB entsprechend aktualisieren. Machen Sie sich mit dem Netzwerk, das einer Erkennung unterzogen wird, und den zurückgegebenen Datentypen für die verschiedenen Erkennungstypen vertraut. Verwenden Sie das Discovery-Protokoll und die ECC-Warteschlange, um den Discovery-Prozess zu überwachen, wenn Daten von Probes oder Mustervorgängen zurückgegeben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

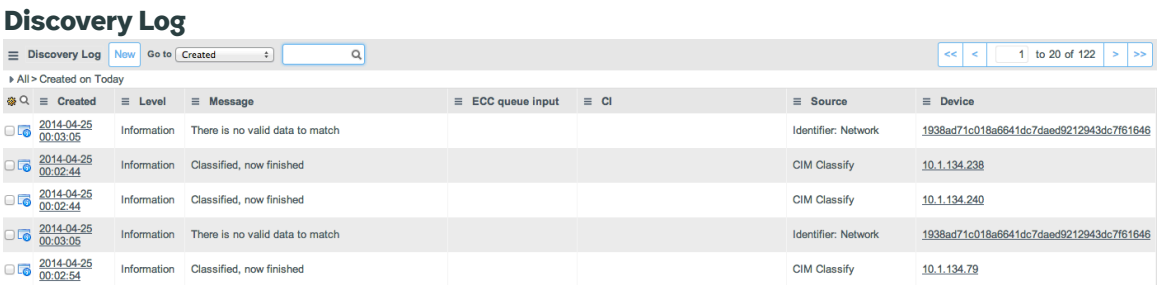
Prozedur

1. Klicken Sie auf das Symbol **XML** in einem Datensatz in der ECC-Warteschlange, um die tatsächliche Nutzlast einer Probe anzuzeigen.



2. Klicken Sie auf das Symbol **XML** in einem Datensatz in der ECC-Warteschlange, um die tatsächliche Nutzlast einer Probe anzuzeigen.
3. Verschaffen Sie sich im Formular „Discovery-Protokoll“ einen kurzen Überblick über die Performance der Probes.

   Um anzuzeigen Discovery Protokoll, navigieren Sie zu **Discovery** > **Discovery-Protokoll**an.



Das Discovery-Protokoll enthält die folgenden Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Informationen
Erstellt	Zeigt den Zeitstempel der gestarteten Probe an. Klicken Sie auf diesen Link, um den Datensatz für die in dieser Liste gestartete Probe anzuzeigen.
Ebene	Zeigt den Typ der von dieser Probe zurückgegebenen Daten an. Mögliche Ebenen: ○ Debuggen ○ Fehler ○ Informationen ○ Warnung
Nachricht	Nachricht, die die Aktion beschreibt, die aufgrund der von der Probe zurückgegebenen Informationen durchgeführt wurde
Eingabe für ECC-Warteschlange	Zeigt den Namen der ECC-Warteschlange an, der der Protokollnachricht zugeordnet ist
CI	Das erkannte CI. Klicken Sie auf diesen Link, um den CMDB-Datensatz für dieses CI anzuzeigen.
Quelle	Zeigt den Namen der Probe an, die die Protokollnachricht generiert hat
Gerät	Zeigt die durch die Probe erkundete IP-Adresse an. Klicken Sie auf diesen Link, um alle Protokolleinträge für die Aktion zu untersuchen, die Discovery für diese IP-Adresse durchgeführt hat.

Hinweis: Wenn Sie eine aktive Erkennung abbrechen, beachten Sie die folgenden Informationen:

- Vorhandene Sensoraufträge, deren Ausführung gestartet wurde, werden sofort beendet.
- Vorhandene Sensoraufträge, die sich im Status **Bereit** befinden, deren Ausführung aber noch nicht gestartet wurde, werden aus dem System gelöscht.

4. Zeigen Sie die Discovery-Homepage an, um auf Details über alle Zeitpläne, Cloud-Ressourcen (virtuelle Computer), erkannten Geräte und zugehörigen Fehler zuzugreifen, die möglicherweise aufgetreten sind. Die Fehlerdetails schließen mögliche Nachbesserungsschritte ein.

MID Server-Auswahlreihenfolge für Erkennungszeitpläne

Bei der Suche nach einem MID-Server folgt die Anwendung Discovery der folgenden Reihenfolge.

Automatische Auswahl des MID Servers

Wenn Sie im Formular „Discovery-Zeitplan“ **MID Server automatisch auswählen** als **Methode für MID Server-Auswahl** auswählen, wird bei der Discovery die folgende Reihenfolge eingehalten.

Hinweis: Die automatische MID-Server-Auswahl wird bei IPv6 nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Discovery sucht nach einem MID-Server, für den auch ein entsprechender IP-Bereich konfiguriert ist.
2. Wenn kein MID Server diese Kriterien erfüllt, wird nach einem MID-Server mit der Anwendung **ALLE** gesucht, für die auch ein entsprechender IP-Bereich konfiguriert ist.
3. Wenn mehrere MID-Server die Kriterien erfüllen, wählt Discovery den ersten MID-Server mit dem Status **In Betrieb** aus. Wenn mehrere MID-Server aktiv sind, wird einer zufällig ausgewählt.
4. Wenn keiner aktiv ist, wird der für die Anwendung Discovery angegebene standardmäßige MID-Server verwendet, sofern dieser aktiv ist.
5. Wenn kein standardmäßiger MID Server aktiv ist, wird der für die Anwendung **ALLE** angegebene standardmäßige MID-Server verwendet, sofern dieser aktiv ist.
6. Wenn kein standardmäßiger MID-Server angegeben ist, durchläuft Discovery die vorherigen Schritte und sucht nach MID Servern mit dem Status **Angehalten** oder **Wird aktualisiert...**.

Hinweis: Wenn ein MID-Server angehalten ist oder aktualisiert wird, verarbeitet er Befehle erst, nachdem er in den Status **In Betrieb** zurückgekehrt ist.

MID Server-Cluster

Die folgenden Schritte werden ausgeführt, wenn Sie im Formular **Discovery** als **Methode für MID Server-Auswahl** die Option **Spezieller MID Server-Cluster** auswählen und das Cluster ein Lastenausgleichscluster ist:

1. **Discovery** verwendet den ersten MID-Server im Cluster, der mit dem Status **In Betrieb** gefunden wird.
2. Wenn mehrere MID-Server aktiv sind, wird einer zufällig ausgewählt. Wenn keine MID Servers gefunden werden, wird im Cluster nach MID Servers n mit dem Status **Angehalten** oder **Wird aktualisiert...** gesucht.

Die folgenden Schritte werden ausgeführt, wenn das Cluster ein Failover-Cluster ist:

1. **Discovery** verwendet den MID-Server mit dem niedrigsten Wert für **Reihenfolge**, der außerdem den Status **In Betrieb** aufweist.
2. Wenn kein MID Servers gefunden wird, wird im Cluster nach MID Servers n mit dem Status **Angehalten** oder **Wird aktualisiert...** gesucht, wobei der Server mit dem niedrigsten Wert für **Reihenfolge** ausgewählt wird.

Hinweis: **Discovery** ignoriert bei der Auswahl eines MID-Server s aus dem Cluster den standardmäßigen MID-Server und **ALLE** Anwendungen.

Port-Scanphase (Shazzam-Phase)

Während der Port-Scanphase erfasst Discovery alle Ziel-IP-Adressen. Sie werden gleichmäßig auf MID Servers aufgeteilt, die den Kriterien entsprechen (MID Servers sind für den Port-Scan qualifiziert). Die Shazzam-Batch-Größe, die Sie im Discovery-Zeitplan konfiguriert haben, bestimmt die Anzahl der IP-Adressen, die jede Shazzam-Probe scannen kann. In dieser Phase wird ermittelt, wie viel Arbeit jeder MID-Server während der Port-Scanphase verrichtet.

Beispiel: Drei qualifizierte MID Servers müssen 16.000 IP-Adressen scannen, und Sie verwenden die standardmäßige Shazzam-Batch-Größe von 5.000. Zwei der MID Servers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verarbeiten 5.000 IP-Adress-Scans (jeweils eine Shazzam-Probe). Der andere MID-Server verarbeitet 6.000 IP-Adress-Scans, wozu er zwei Shazzam-Probes startet.

Hinweis:

Shazzam kann IP-Listen mit bis zu 5000 Adressen verarbeiten, die sowohl IPv4- als auch IPv6-Typen enthalten. Wenn Ihr Zeitplan eine IP-Liste mit mehr als 5000 IPv6-IP-Adressen enthält, wird der Discovery Wird abgebrochen. Wenn Sie nur IPv6-Adressen verwenden, müssen Sie eine Liste und keinen IP-Adressbereich verwenden. IPv6-Adressbereiche und -Netzwerke werden nicht unterstützt und entsprechend ignoriert.

Zugehörige Informationen

MID Server-Pause

Clusterkonfiguration des MID Servers

File-based Discovery

Mithilfe von File-based Discovery können Sie identifizieren, welche Software auf Ihren Windows- und UNIX-Servern und -Geräten ausgeführt wird, selbst wenn keine Registrierungsinformationen verfügbar sind. Anschließend können Sie Datensätze Ihrer Softwarelizenzen verwalten, nach nicht lizenzierten Dateien suchen, unzulässige oder beschädigte Dateien erkennen und Bedrohungen durch unerwünschte Dateien bewerten.

Benötigte Plugins

Das Plugin „File-based Discovery“ [com.snc.discovery.file_based_discovery] ist für die Dateisignaturfilterung erforderlich. Ihr Discovery Das Abonnement enthält dieses Plugin, Sie müssen es jedoch tun Aktivierung anfordern . Einmal dateibasiert Discovery Plugin ist aktiv, die Software Asset Management– Dateisignatur-Normalisierung Das Plugin [com.snc.file_Signature_normalization] ist ebenfalls aktiviert. Weitere Informationen zu finden Dateisignatur-Normalisierung Plugin, siehe Normalisierung Der Dateisignatur .

Funktionsweise der dateibasierten Discovery

Die dateibasierte Discovery verbessert die Erkennung vorhandener installierter Software. Sie durchsucht Zielserver anhand einer bekannten Liste von Dateisignaturen und verarbeitet diese Dateien mit festgelegten Regeln. Die resultierenden Daten verbessern die Erkennung installierter Software und identifizieren nicht registrierte Softwareprodukte. Informationen zur Verwendung von Agent Client Collector Visibility – Inhalt Informationen zum Ausführen einer dateibasierten Discovery finden Sie unter Erkennen Sie Java-Installationsdaten mit Agent Client Collector Visibility – Inhalt Dateibasierte Discovery.

Die dateibasierte Discovery wird in der Erkundungsphase der normalen Discovery ausgelöst. Dateibasierte Discovery-Probes suchen in von Ihnen konfigurierten Pfaden nach bestimmten Dateierweiterungen oder Dateinamen. Die resultierenden Dateiinformationen werden in der Probe-Nutzlast zurückgegeben. Der Sensor versucht, die erkannten Dateien anhand der von der Probe zurückgegebenen Informationen (Name, Größe und Version der Datei) mit installierter Software abzugleichen. Die dateibasierte Discovery verwendet Dateisignaturen, um Software zu erkennen, die möglicherweise nicht registriert wurde. Diese Informationen werden dann in der Tabelle „Dateiinformationen“ [cmdb_file_information] mit einem Verweis auf das CI des Servers gespeichert. Sie können die von jedem CI gefundenen Dateien in einer zugehörigen Liste in dieser Tabelle anzeigen. Weitere Informationen finden Sie unter Zugehörige Liste der CI-Komponenten Wenn Software Asset Management (SAM) aktiv ist, wenn eine Datei mit einem Softwareprodukt übereinstimmt, Discovery Füllt die Produkt- und Herausgeberinformationen für diese Datei aus. Verwenden Sie diese Informationen, um zu verstehen, welche Software auf Ihrem Server ausgeführt wird, und um Bedrohungen durch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

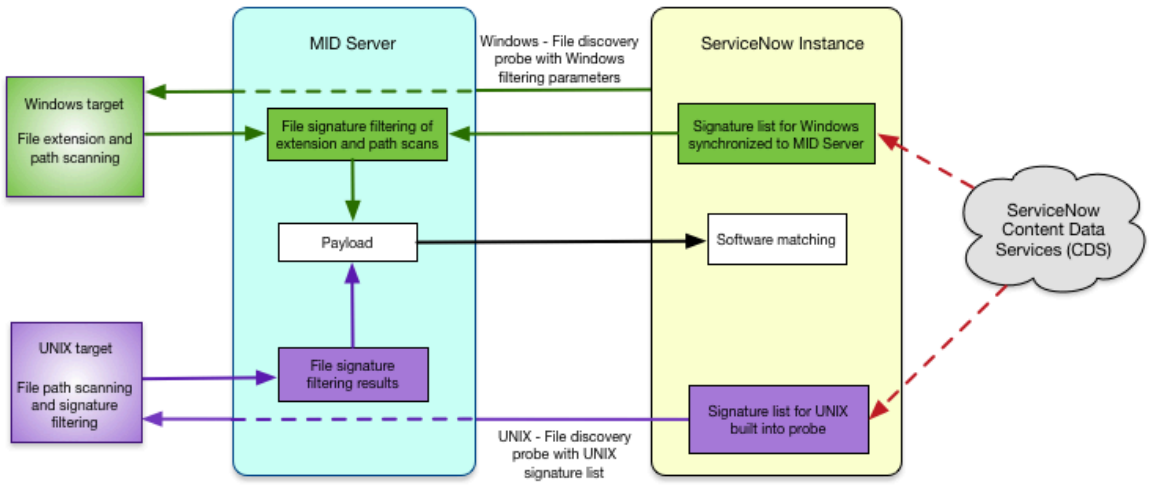
unerwünschte Dateien zu bewerten. Discovery verwendet Listen bekannter Dateisignaturen für Windows und UNIX, um den Umfang der Suche zu beschränken. Der Filterprozess für Windows- und UNIX-Hosts wird unterschiedlich ausgeführt, da sich ihre Signaturlisten erheblich unterscheiden. Die viel kleinere UNIX-Signaturliste ist in der Probe „Unix - File Discovery“ enthalten und wird direkt am Ziel verarbeitet. Die Windows-Signaturliste ist viel größer und kann nicht auf dem Ziel verarbeitet werden. Die Probe „Windows - File Discovery“ durchsucht das Ziel nach bestimmten Dateierweiterungen und Pfaden und gibt diese Ergebnisse an den MID-Server zurück. Der MID-Server führt die Dateisignaturfilterung anhand der gesamten Windows-Liste durch. Anschließend sendet der MID-Server alle Dateiinformationen zur Normalisierung und zum Abgleich an die Instanz zurück.

Wenn SAMP für die Instanz aktiv ist, erstellt oder aktualisiert die dateibasierte Discovery identifizierte Softwareprodukte in der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] und aktualisiert die Lizenzen übereinstimmender Softwarepakete. Ohne SAMP werden keine Softwaredatensätze erstellt, und in die Tabelle „Dateiinformationen“ [cmdb_file_information] werden nur Dateiinformationen aufgenommen.

in der Discovery-Konfigurationskonsole können Sie SWID-Tags aktivieren. Wenn das SWID-Tag aktiviert ist und die dateibasierte Discovery ausgeführt wird, wird die Tabelle [cmdb_swid_tag] mit den SWID-Tag-Informationen gefüllt. Informationen zur auf einem bestimmten Computer installierten Software umfassen Name, Dateiinformationen, Herausgeber, Version, Installationsverzeichnis bzw. -gerät sowie Inhalt. Die Spalte „software_installation“ in [cmdb_swid_tag] ist ein Verweis auf die Tabelle [cmdb_sam_sw_install].

Hinweis: Base64-Paket ist eine Voraussetzung für jeden UNIX Oder Linux Server zum Scannen von SWID-Tag-Dateien mit dateibasiert Discovery.

Filterungs-Flow für dateibasierte Discovery

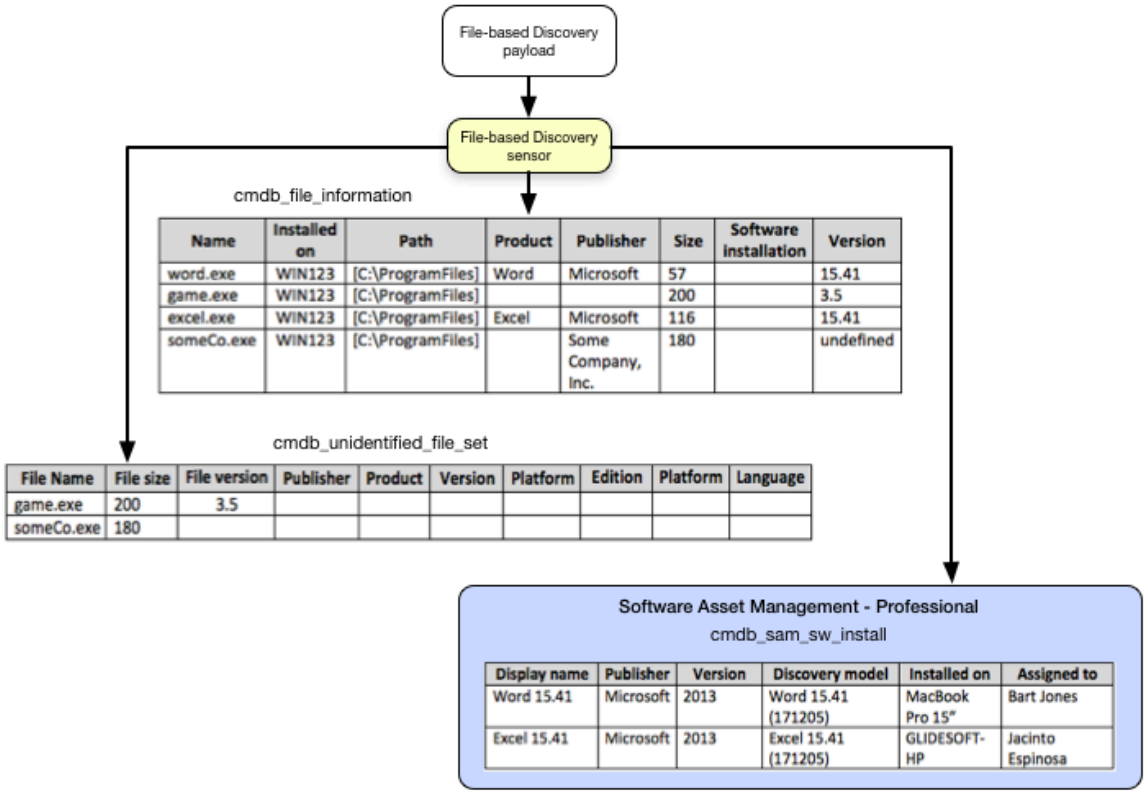


Dateibasiert Discovery Fügt eine beliebige Datei ein, die vom Normalisierungsprozess nicht übereinstimmt, in die Tabelle „nicht identifizierter Dateisatz“ [cmdb_unidentified_file_Set] ein. Sie können die Datensätze in dieser Tabelle aktualisieren und zusätzliche Details für zuvor nicht identifizierte Dateien angeben. Wenn Sie Werte für die Felder **Produkt** und **Herausgeber** für eine Datei angeben, können die Einstellungen in SAMP die dateibasierte Discovery aktivieren, um diese Datei für den Abgleich installierter Software in zukünftigen Erkennungen zu verwenden.

Hinweis: Sie können die dateibasierte Discovery jederzeit deaktivieren, indem Sie die entsprechende Einstellung in der Discovery-Konfigurationskonsole ändern. Wenn Sie die dateibasierte Discovery deaktivieren, bevor Scanergebnisse zurückgegeben werden, werden die Dateidaten ignoriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenschema für dateibasierte Discovery



Hinweis:

Dateibasiert Discovery Unterstützt Windows, UNIX, Und macOS Geräte. Die UNIX Probe ist POSIX-konform und sollte auf jedem Linux-/Solaris-Server ausgeführt werden. ServiceNow bietet Unterstützung für die Windows-Versionen 2008, 2008R2, 2012R2, 2016, 2019 und höher mit PowerShell 3.0 bis 5.1. Wir unterstützen auch die AIX-Versionen 5.3, 6.1 und 7.1 sowie HP/UX 8.11.

Wenn Sie „File-based Discovery“ unter Ubuntu Version 20 ausführen, modifizieren Sie die standardmäßige Bourne-Shell (sh) so, dass sie auf die Bourne-Again-Shell (bash) verweist.

Versionsinformationen werden für die Dateien nur mit Versionsinformationen gefüllt, die von Probes zurückgegeben werden. Nicht alle Dateien weisen Versionen auf. Dateien mit Erweiterungen wie exe, jar usw. weisen Versionen auf.

Reference

1. Referenzinformationen für dateibasierte Discovery

Dateibasierte Discovery ausführen

Führen Sie die dateibasierte Discovery aus, um die gesamte von Ihnen installierte Software zu erkennen, egal ob sie registriert ist oder nicht. Über die Discovery-Konfigurationskonsole können Sie die dateibasierte Discovery jederzeit aktivieren und konfigurieren.

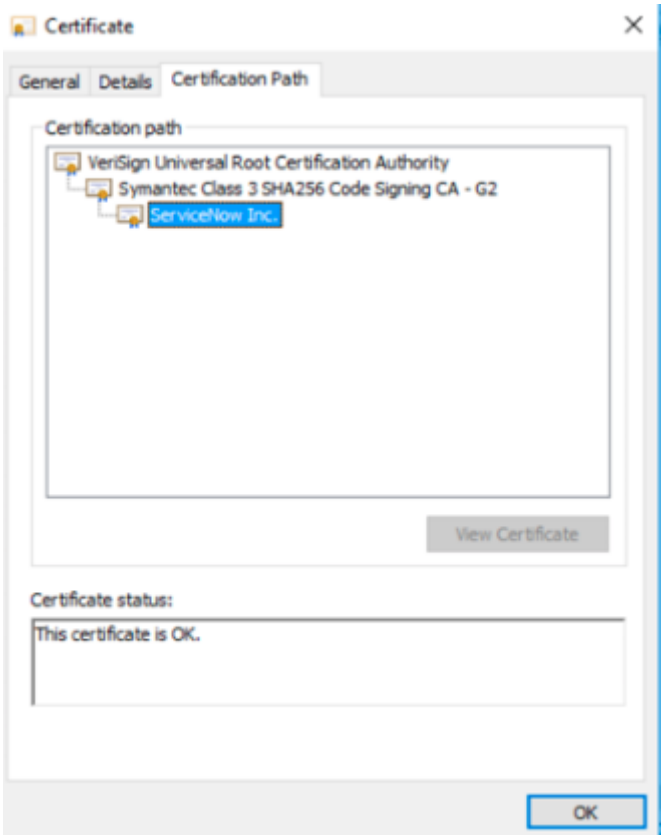
Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Richten Sie das PowerShell-Skript ein.
   Standardmäßig besitzt das Skript **filebaseddiscovery.ps1** eine ServiceNow-Signatur. Ihre Zertifikatkette wird bis zur Zertifizierungsstelle VeriSign Universal Root aufgelöst, der Windows standardmäßig vertraut. Da Powershell-Skripts von ServiceNow-Herausgeber signiert werden, fügen Sie den ServiceNow-Herausgeber Ihrem vertrauenswürdigen Herausgeber-Repository hinzu.



   Wenn die Ausführungsrichtlinie die Verwendung Ihres eigenen Zertifikats verlangt oder Sie Änderungen am Skript vornehmen müssen, signieren Sie das Skript erneut.

   a. Navigieren Sie zur Probe „Windows - File discovery“.
   b. Öffnen Sie den Probe-Parameter **filebaseddiscovey.ps1**.
   c. Kopieren Sie den Inhalt des Felds **Wert** in eine Datei.
   d. Nehmen Sie die erforderlichen Änderungen an der Datei vor, und entfernen Sie dann den (alten) Signaturblock am Ende der Datei.
   e. Signieren Sie das Skript erneut: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-authenticodesignature?view=powershell-6 .

      Nach dem erneuten Signieren sollte die Datei einen neuen Signaturblock am Ende aufweisen.

   f. Kopieren Sie den gesamten Dateiinhalt, und ersetzen Sie den alten Wert im Probe-Parameter **filebaseddiscovery.ps1** aus Schritt b.

      Die dateibasierte Windows-Discovery sollte jetzt mit dem aktualisierten signierten Skript ausgeführt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Antivirensoftware verwenden, stellen Sie sicher, dass Sie alle einschließen ServiceNow Windows PowerShell-Skripts, damit die Antivirensoftware sie nicht als Bedrohung sieht.

2. Aktivieren Dateibasiert Discovery Plugin.
3. Aktivieren und konfigurieren Sie die dateibasierte Discovery.
   Mit der Discovery-Konfigurationskonsole können Sie die dateibasierte Discovery aktivieren und mehrere Komponenten konfigurieren, um Ihre gesamte installierte Software zu erkennen und zu verwalten.

   Um die Performance für bestehende Kunden nicht zu beeinträchtigen, ist die dateibasierte Discovery standardmäßig deaktiviert.

4. Dateibasierte Discovery-Scans konfigurieren
   Nach der Ausführung der Discovery und der Rückgabe von Dateiinformationen für ein CI wird die dateibasierte Discovery für dieses Ziel erst dann wieder ausgeführt, wenn das Intervall abgelaufen ist. Da die Ausführung von Scans für die dateibasierte Discovery die Performance beeinträchtigt, ist es wichtig zu bestimmen, wie häufig gescannt wird. Aus Leistungsaspekten wird jedoch davon abgeraten, ein häufigeres Intervall als „Monatlich“ auszuwählen.

   a. Erweitern Sie in der Discovery-Konfigurationskonsole den Eintrag **Verbreitet**, und geben Sie dann die maximale Anzahl der Dateien ein, die erkannt werden sollen.

   Hinweis: Das Erhöhen dieses Werts kann sich auf die Leistung auswirken.

   b. Legen Sie die **Häufigkeit** für die Ausführung der dateibasierten Discovery für das CI fest.
   Der Standardwert ist „Monatlich“.

   Hinweis: Die dateibasierte Discovery wird erst ausgelöst, wenn die erste Content Data Service-Synchronisierung (CDS) erfolgt. Bei der CDS-Synchronisierung kann es etwa 24 Stunden dauern, bis der erste Datensatz von CDS synchronisiert ist. Weitere Informationen finden Sie unter . Normalisierung Der Dateisignatur .

Ergebnis

Die dateibasierte Discovery sollte basierend auf der festgelegten Konfiguration ausgeführt werden. .

Reference

1. Referenzinformationen für dateibasierte Discovery

Lösung von Problemen bei der dateibasierten Discovery

Wenn Probleme beim Einrichten oder Ausführen der dateibasierten Discovery auftreten, führen Sie die hier aufgeführten Aktionen durch, um sie zu beheben.

Problem	Ursache/Aktion
Fehlermeldung: Daten der Datei-Discovery noch nicht synchronisiert...	• Planen Sie genug Zeit ein, damit CDS die samp_file_*-Tabellen synchronisieren kann. • Überprüfen Sie die Tabelle cds_client_schedule, und überprüfen Sie, ob der Zeitstempel für die samp_file_*-Tabellen aktualisiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Ursache/Aktion
Während der Erkennung wird die dateibasierte Discovery nicht ausgelöst.	• Die Funktion wurde nicht aktiviert. Überprüfen Sie die Konfigurationskonsole der Discovery-Definition, und stellen Sie sicher, dass die dateibasierte Discovery aktiviert ist. • Das Intervall zwischen den Scans ist zu lang. Überprüfen Sie die Intervalleinstellung für die Konfigurationskonsole der Discovery-Definition.
Während der Erkennung wird die dateibasierte Discovery nicht ausgelöst.	Überprüfen Sie die von der Discovery-Tabelle [discovery_private_properties] verwalteten internen Eigenschaften auf folgende Elemente. Geben Sie zum Anzeigen dieser Tabelle in den Navigationsfilter **discovery_private_properties.list** ein, und drücken Sie die **Eingabetaste**. • File_discovery.file_extensions_windows muss eine Liste der zu scannenden Windows-Dateierweiterungen enthalten. • File_discovery.unix_filename_timestamp muss einen anderen Zeitstempel als 1970 aufweisen. • File_discovery.windows_filename_timestamp muss einen anderen Zeitstempel als 1970 aufweisen.
Fehler im MID Server-Protokoll durch FileDiscoveryFilter oder MID Server-Problem generiert	• Überprüfen Sie, ob die Aufnahmeliste der dateibasierten Erkennung vorhanden ist. Die Aufnahmeliste befindet sich im MID Server-Installationsordner in /agent/work. Wenn sie nicht vorhanden ist, war die Synchronisierung nicht erfolgreich. • Überprüfen Sie den MID Server-Datensatz für die Instanz, um zu ermitteln, ob ein MID Server-Problem generiert wurde. • Der MID Server verwendet den geskripteten SOAP-Service GetMIDInfo, um die Aufnahmeliste zu synchronisieren. Überprüfen Sie, ob dieses Skript Fehler generiert hat. • Klicken Sie im MID Server-Datensatz auf den zugehörigen Link **Aktualisierung des Dateierkennungsfilter**, um die Dateinamen mit diesem MID Server zu synchronisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Ursache/Aktion
PowerShell-Fehler	• Nehmen Sie das Skript in Ihre Virenschutzsoftware auf. • Fügen Sie den Herausgeber von ServiceNow dem Repository vertrauenswürdiger Herausgeber hinzu.

Reference

1. Referenzinformationen für dateibasierte Discovery

Referenzen für die dateibasierte Discovery

Das folgende Referenzmaterial enthält weitere Details zur dateibasierten Discovery.

Möglichkeiten zur Minimierung der Beeinträchtigung der Performance durch die dateibasierte Discovery

Große Netzwerke werden gescannt, insbesondere für Windows Computer, kann die Scan-Zeit erheblich verlängern. Darüber hinaus kann das Scannen von Dateien hohe CPU-Anforderungen auf den Zielcomputern und hohe Nutzlasten verursachen, die die Verarbeitungszeit erheblich verlängern. Um Leistungsprobleme zu vermeiden, können Sie mit der dateibasierten Discovery die Verarbeitung mit vielen der in der Discovery-Konfigurationskonsole konfigurierten Einstellungen optimieren.

- **Scannen in mehreren Phasen**: Probes werden in mehreren Phasen ausgelöst, um lange Scanzeiten zu reduzieren. Die erste Probe erstellt den Scanprozess auf dem Ziel. Dieser wird im Hintergrund ausgeführt. Nachfolgende Probes überprüfen bei jeder Ausführung von Discovery den Fortschritt dieses Scans und geben die Ergebnisse zurück, wenn der Scan abgeschlossen ist. Beispiel: Wenn ein Dateiscan über Schnell-Discovery oder einen Discovery-Zeitplan initiiert wird, werden keine Informationen zurückgegeben, wenn noch ein Hintergrundscan ausgeführt wird. Wenn der Scan bei der nächsten Erkennung des Servers abgeschlossen ist, gibt die Probe die Daten zurück.

  Wichtig: Beim Scannen in mehreren Phasen durch die dateibasierte Discovery werden Ergebnisse nicht sofort zurückgegeben. Erwarten Sie keine Ergebnisse von einem dateibasierten Scan, bis Discovery auf diesen Zielen erneut ausgeführt wird und die Liste der vom vorherigen Scan erkannten Dateien abruft.

- **Zu scannende Ordner**: Sie können sowohl den Umfang des Scans auf bestimmte Ordner beschränken als auch ausgeblendete Ordner scannen.
- **Zu scannende Erweiterungen**: Sie können sowohl alle Dateien für eine bestimmte Liste von Erweiterungen abrufen als auch bestimmte Dateierweiterungen beim Scannen ignorieren.
- **UNIX-Dateinamen scannen** : Da die Anzahl der eindeutigen Dateinamen zur Identifizierung der installierten Software auf verwendet wird UNIX Ist relativ klein, die vollständige Liste der Dateinamen ist in enthalten UNIX Probe. Dadurch kann die Probe die ermittelten Dateien anhand der Signaturliste für das Ziel filtern. Es ist keine zusätzliche Filterung erforderlich, bis die Ergebnisse an die Instanz zurückgegeben werden.
- **Scannen Sie Windows-Dateinamen** : Für Windows Dateibasiert Discovery, Die Probe initiiert keinen Scan im Ziel für die vollständige Signaturliste. Stattdessen generiert Discovery eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste von Dateierweiterungen, die die Probe mit dem Ziel abgleicht. Diese reduzierte Liste wird dann auf gefiltert MID-Server Für das gesamte Windows Signaturliste.

- **Reduzierte Nutzlasten**: Durch Filtern der Scanergebnisse mit der Dateisignaturliste, bevor die Ergebnisse an die Instanz gelangen, reduziert Discovery die Größe der Nutzlast von Zielservern. Nur die Dateien aus den Zielen, die den in dieser Liste angegebenen Dateien entsprechen, werden an die Instanz zurückgegeben.
- **Drosselung scannen** : , Um die Auswirkungen auf zu reduzieren Windows CPU- und E/A-Leistung auf Remote-Zielen, Windows Dateibasiert Discovery Ist so konfiguriert, dass während Scans gelegentlich in den Ruhezustand versetzt wird. Sie können dieses Verhalten mit den Discovery-Eigenschaften feinabstimmen. Drosselung Windows Scans können dazu führen, dass diese Scans länger dauern.

Tabellen der dateibasierten Discovery

Die folgenden Tabellen werden vom Plugin für die dateibasierte Discovery [com.snc.discovery.file_based_discovery] zum Speichern von Daten bereitgestellt:

Dateiinformationen [cmdb_file_information]

In dieser Tabelle werden alle Dateien (übereinstimmende und nicht übereinstimmende) gespeichert, die für ein bestimmtes CI erkannt wurden. Die Dateien sind in einer zugehörigen Liste mit CI-Computerdatensätzen verfügbar. In der Standardansicht werden die folgenden Spalten bereitgestellt:

- **Pfad**: Pfad, unter dem die Datei auf dem Ziel gefunden wurde
- **Produkt**: Software-Produktname. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Herausgeber**: Name des Herausgebers der Datei, zum Beispiel Oracle oder Microsoft. Dies ist eine Referenz auf die Unternehmenstabelle [core_company]. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Größe**: Größe der Datei
- **Softwareinstallation**: Name der installierten Software, die dieser Datei zugeordnet ist, aus der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install]. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Version**: Version der Datei Derzeit für Windows Nur.

Nicht identifizierter Dateisatz [cmdb_unidentified_file_set]

Diese Tabelle speichert alle von Discovery zurückgegebenen Dateien, die mit oder ohne SAMP nicht mit einem Softwareprodukt abgeglichen werden können. Discovery füllt Name, Größe und Version jeder nicht übereinstimmenden Datei im Datensatz. Diese optionalen Felder können verwendet werden, um die Datei weiter zu identifizieren und für zukünftige Dateizuordnungen verfügbar zu machen:

- Herausgeber
- Produkt
- Version
- Edition
- Plattform
- Sprache

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Eine Funktion in Software Asset Management Professional (SAMP) ermöglicht die Freigabe von Signaturdaten in dieser Tabelle für Content Data Services (CDS). Bei aktivierter Datenfreigabe lädt das System automatisch Datensätze aus der Tabelle „Nicht identifizierter Dateisatz“ [cmdb_unidentified_file_set] in CDS hoch, wenn Sie die fehlenden Informationen ergänzen. Durch den Upload der identifizierten Dateien werden diese zur Verbesserung des zukünftigen Dateivergleichs verfügbar gemacht. Weitere Informationen finden Sie unter Fügen Sie ein anwenderdefiniertes Softwareprodukt hinzu .

Dateibasierte Discovery – Fehlerbehebung

Wenn beim Einrichten oder Ausführen von Discovery Probleme auftreten, konsultieren Sie Lösung von Problemen bei der dateibasierten Discovery.

Zugehörige Informationen

File-based Discovery

Anwendungen basierend auf Fingerabdrücken erkennen

Erkennen Sie Anwendungen basierend auf Vorschlägen von ServiceNow Predictive Intelligence. Predictive Intelligence klassifiziert und kategorisiert die erkannten laufenden Prozesse automatisch als Fingerabdrücke der Anwendung und macht Vorschläge. ITOM-Transparenz nutzt Predictive Intelligence zur ersten Analyse erkannter Prozesse und empfiehlt Anwendungen, für die eine Erkennung durchgeführt werden sollte. Mit dieser Methode erstellt ITOM-Transparenz automatisch eine CI-Klasse für die Configuration Management Database (CMDB), einen Klassifizierer oder ein Muster für die neue Anwendungs-CI-Klasse.

Vorbereitungen

Führen Sie eine horizontale Erkennung für alle relevanten IP-Bereiche durch (siehe Beschreibung in IP-Netzwerke in Discovery-Range Sets konvertieren). Geben Sie alle relevanten Anmeldeinformationen für den Zugriff von ITOM-Transparenz auf die Anwendungen und Geräte an, die Sie erkennen möchten.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Erkennung von Anwendungen anhand von Fingerabdrücken ist besonders nützlich, wenn Sie keine Muster verwenden können, die standardmäßig oder über den ServiceNow Store verfügbar sind. Beispielsweise wenn Sie nicht standardmäßige, selbst entwickelte Anwendungen oder brandneue Anwendungen erkennen möchten.

Die Funktion Discovery von ITOM-Transparenz verwendet Application Dependency-Mapping (ADM), um an TCP-Ports ausgeführte Prozesse und Anwendungen zu erkennen, die diese Prozesse ausführen. Wenn Sie Anwendungen anhand von Fingerabdrücken erkennen, gehen Sie noch einen Schritt weiter. Die auf Fingerabdrücken basierte Erkennungsmethode analysiert Prozesse, die ADM nicht für die Erkennung verwendet hat.

Die auf Fingerabdrücken basierte Erkennung nutzt Algorithmen, um laufende Prozesse zu identifizieren und in Gruppen zu organisieren. Diese Prozessgruppen werden zu vorgeschlagenen Anwendungen oder Kandidaten. Sie überprüfen vorgeschlagene Anwendungen und wählen aus, welche erkannt werden sollen. Die Liste der vorgeschlagenen Anwendungen wird stündlich aktualisiert.

Während der Fingerabdruckerkennung erstellte Muster werden sowohl für die horizontale Erkennung als auch für die Erkennung von oben nach unten verwendet. Damit Service-Mapping ein solches Muster korrekt ausführen kann, müssen Sie definieren, wann dieses Muster ausgeführt werden soll. Dazu legen Sie fest, vor oder nach welchem anderen Muster Service-Mapping dieses neue Muster ausführen soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine Anwendung basierend auf einem Anwendungsvorschlag erkennen, führt die auf Fingerabdrücken basierte Erkennung die folgenden Schritte aus:

1. Die auf Fingerabdrücken basierte Erkennung erstellt für die neue Anwendung eine CI-Klasse in der CMDB. Die neue CI-Klasse erweitert die CI-Klasse „Anwendung“ [cmdb_ci_appl] und verwendet standardmäßig den Prozessgruppennamen als Anzeigename der vorgeschlagenen CI-Klasse.
2. Die auf Fingerabdrücken basierte Erkennung erstellt einen Prozessklassifizierer für die Anwendungsgruppe, die erkannt werden soll. ADM verwendet den neuen Prozessklassifizierer, um das für die CI-Klasse erstellte neue Muster auszulösen. Die Priorität des Klassifizierers ist niedriger, um sicherzustellen, dass das System zuerst die mit ITOM-Transparenz verfügbaren Standardmuster oder benutzerdefinierte Muster verwendet.
3. Die auf Fingerabdrücken basierte Erkennung erstellt ein Erkennungsmuster des Anwendungstyps für die neue CI-Klasse. **Prozessklassifizierung erzwingen** ist aktiviert, um sicherzustellen, dass der MID-Server dieses Muster nur ausführt, wenn der für ein CI identifizierte Prozess den Klassifizierungskriterien für dieses Muster entspricht.

   Hinweis: Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

4. ADM verwendet den Klassifizierer, um die horizontale Erkennung des Anwendungs-CI auszulösen.
5. ADM löst die Erkennung mit dem neuen Muster aus.
6. Nachdem das Muster die Erkennung abgeschlossen hat, wird das erkannte Anwendungs-CI in die entsprechende Tabelle der CMDB geschrieben.

Die auf Fingerabdrücken basierte Erkennung ist standardmäßig aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**an.
2. Klicken Sie auf **Fingerabdrücke der Anwendung**.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Zeigen Sie vorgeschlagene Anwendungen auf eine der folgenden Arten an:
   - Zeigen Sie im Tortendiagramm mit den **häufigsten Vorschlägen** die wichtigsten Vorschläge an, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen. Die Prozessanzahl spiegelt sich in der Größe des jeweiligen Diagrammsegments wider. Klicken Sie auf das Segment, um die entsprechenden Vorschläge in einer gefilterten Liste anzuzeigen. Klicken Sie zum Ausblenden eines Vorschlags aus dem Diagramm auf den Namen des Vorschlags in der Diagrammlegende.
   - Um nur Vorschläge für Anwendungsserver anzuzeigen, klicken Sie auf die **Kachel für vorgeschlagene Anwendungsserver**. Die gefilterte Liste mit Vorschlägen für Anwendungsserver wird angezeigt.
   - Sie können auch **alle Vorschläge** anzeigen. Die ungefilterte Liste mit allen Vorschlägen wird angezeigt.
4. Klicken Sie unter **Vorgeschlagener Gruppenname** auf den entsprechenden Vorschlag, zum Beispiel **Python**.
   Die Vorschlagsdetails werden im Formular **Anwendungsvorschlag** geöffnet.
5. Überprüfen Sie die Vorschlagsdetails unter Beachtung der folgenden Parameter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorgeschlagener Gruppenname	Der Name ITOM-Transparenz, der für den Vorschlag generiert wird. Dieses Feld ist bereits ausgefüllt, Sie können es jedoch bei Bedarf ändern.
Erweiterter Gruppenname	Die 10 wichtigsten Stichwörter, die weitere Informationen zum Prozess liefern. Predictive Intelligence extrahiert diese Stichwörter aus dem Prozess.
Vorgeschlagene CMDB CI-Klasse	Der Name der von ADM erstellten CMDB-CI-Klasse, wenn Sie sich für die Erkennung der vorgeschlagenen Anwendung entscheiden
Prozessanzahl	Die Anzahl der erkannten Prozesse, auf denen dieser Vorschlag basiert
Prozesse anzeigen	Klicken Sie, um die Beispielprozesse anzuzeigen, auf denen dieser Vorschlag basiert. Die Gesamtanzahl der Prozesse kann größer sein und beginnt bei 1000. Standardmäßig können 100 Beispielprozesse angezeigt werden.
Genauigkeit	Ein Validierungsalgorithmus überprüft die Qualität der Vorhersage. Der Algorithmus analysiert den Parameter des regulären Ausdrucks (ReGex) der Prozesse in diesem Vorschlag und in anderen Vorschlägen (Anwendungsgruppen). Wählen Sie Vorschläge mit höherer Regelgenauigkeit aus. Wenn die Genauigkeit niedrig ist, können Sie die ReGex-Definition des Prozesses manuell einstellen (siehe Beschreibung in Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen) **Hinweis:** Ändern Sie den Genauigkeitswert nicht manuell.
Prozessklassifizierer	Der vorgeschlagene reguläre Ausdruck, der im Klassifizierer verwendet wird. Falls definiert, verwendet ADM diesen regulären Ausdruck während der horizontalen Erkennung.
Regel ignorieren	Der Name des Prozesses, der mit der Aktion **Ignorieren** von der Erkennung ausgeschlossen wurde

6. **Wahlweise:** Wenn dieser Vorschlag nicht relevant ist und Sie ihn nicht für die Erkennung verwenden möchten, führen Sie eine der folgenden Aktionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

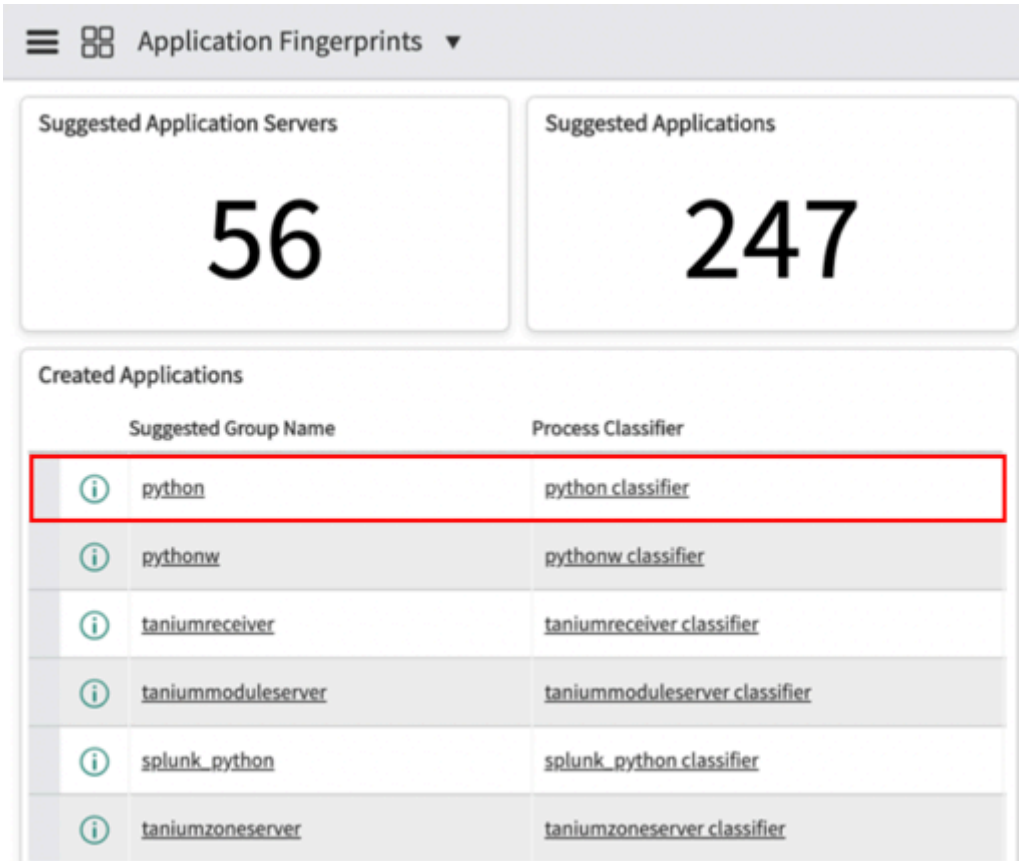
- Klicken Sie auf **Ignorieren**, um Prozesse von der horizontalen Erkennung auszuschließen.

  Dieser Prozess wird der Tabelle „Prozesshandler“ [discovery_proc_handler] hinzugefügt, wobei der `Classify parameter` auf „false“ gesetzt wird. Discovery beendet die Überprüfung des Klassifizierers auf den ausgeschlossenen Prozess und führt keine Erkennung des CI durch, für das diese Prozesse ausgeführt werden.

- Klicken Sie auf **Löschen**, um diesen Vorschlag aus der Vorschlagsliste zu entfernen.

  Der Vorschlag wird aus der Liste entfernt. Wenn Predictive Intelligence einem gelöschten Vorschlag neue Prozesse hinzufügt, wird er erneut in dieser Liste angezeigt.

7. Klicken Sie auf **Anwendung erkennen**.
   Die auf Fingerabdrücken basierte Erkennung erkennt ein Anwendungs-CI für den ausgewählten Vorschlag.
8. Überprüfen Sie im Dashboard **Fingerabdrücke der Anwendung**, ob die erkannte Anwendung unter **Created Applications (Erstellte Anwendungen)** angezeigt wird.

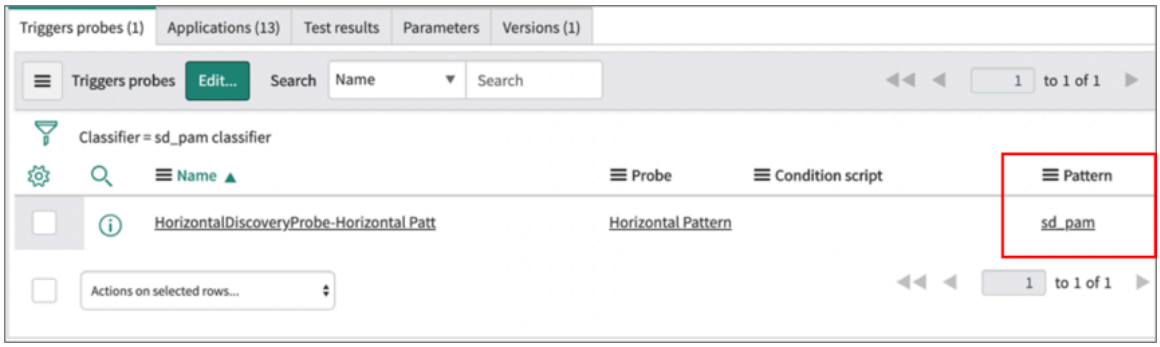


9. Konfigurieren Sie die Ausführungsreihenfolge für das automatisch erstellte Muster:

   a. Klicken Sie auf den Prozessklassifizierer neben der neuen Anwendung.
   Das Formular „Prozessklassifizierung“ wird geöffnet.

   b. Klicken Sie auf der Registerkarte „Auslösertests“ auf den Link für das Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Musterformular wird geöffnet.

c. Wählen Sie die Reihenfolge aus, in der dieses Muster immer ausgeführt wird:

- **Vor**
- **Nach**

d. Wählen Sie dann das andere zutreffende Muster aus.

> **Hinweis:** Wenn Sie sich nicht sicher sind, was die richtige Reihenfolge ist, oder wenn Sie dieses automatisch generierte Muster für die Erkennung von oben nach unten nicht verwenden möchten, konfigurieren Sie die Ausführungsreihenfolge als **After All (Nach allen)**.

e. Klicken Sie auf **Speichern**.

10. **Wahlweise:** Klicken Sie auf den Prozessklassifizierer neben der neuen Anwendung, um den Klassifizierer und das Muster anzuzeigen, das die auf Fingerabdrücken basierte Erkennung für dieses Anwendungs-CI erstellt.
11. **Wahlweise:** Wenn das Erkennungsergebnis nicht zufriedenstellend ist, kalibrieren Sie die Funktion der auf Fingerabdrücken basierten Erkennung.

Zugehörige Informationen

Predictive Intelligence

Dashboard „Fingerabdrücke der Anwendung“

Auf Fingerabdrücken basierte Erkennung kalibrieren

Nehmen Sie die Feineinstellung der Erkennung von Anwendungen auf Basis von Prozessen vor, wenn die Erkennungsergebnisse nicht zufriedenstellend sind.

Ändern Sie die Standardeinstellungen für die auf Fingerabdrücken basierte Erkennung, wenn diese Funktion überhaupt keine Vorschläge generiert. Darüber hinaus können Sie die generierten Vorschläge feinabstimmen, um sie relevant und nützlich zu machen.

Sicherstellen, dass die auf Fingerabdrücken basierte Erkennung Vorschläge generiert

Die auf Fingerabdrücken basierte Erkennung stützt sich auf die Predictive Intelligence zum Generieren von Vorschlägen für die Erkennung. Wenn das Dashboard **Fingerabdrücke der Anwendung** keine Vorschläge anzeigt, stellen Sie sicher, dass die Predictive Intelligence korrekt konfiguriert ist.

Vorbereitungen

Bestätigen Sie, dass die auf Fingerabdrücken basierende Discovery aktiviert bleibt, da sie standardmäßig aktiviert ist. Navigieren Sie zum Überprüfen zu **Alle** > **System Eigenschaft S** > **Alle Eigenschaften**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie, ob *sys_property process.clustering.appfingerprint.enabled*Eigenschaft wird nicht in der Liste angezeigt.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Dashboard **Fingerabdrücke der Anwendung** keine Vorschläge anzeigt, gehen Sie wie folgt vor. Überprüfen Sie nach jeder Aktion, ob das Problem weiterhin besteht.

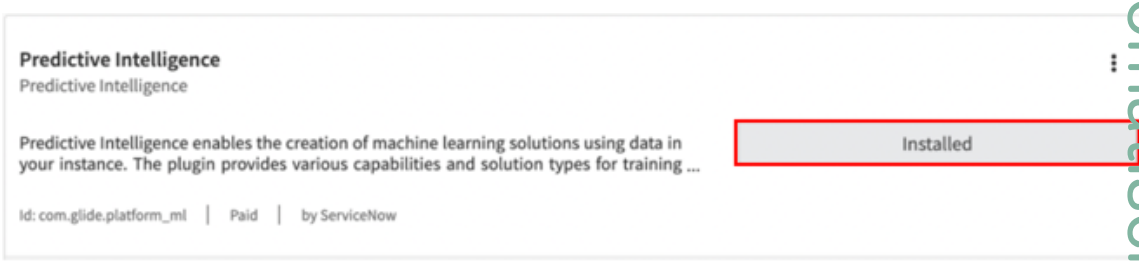
Prozedur

1. Stellen Sie sicher, dass Predictive Intelligence installiert und aktiv ist.

   a. Navigieren zu **Systemdefinition** > **Plugins**an.

   b. Suchen Sie nach **Predictive Intelligence**.

   c. Stellen Sie sicher, dass das Plugin Predictive Intelligence installiert ist.

   Wenn Predictive Intelligence nicht installiert ist, klicken Sie auf die Schaltfläche **Installieren**.

   d. Klicken Sie auf die Kachel **Predictive Intelligence**.

   e. Stellen Sie im Formular „Predictive Intelligence“ sicher, dass der **Status** gleich **Aktiv** ist.
   Wenn der Status **Inaktiv** ist, klicken Sie unter **Zugehörige Links** auf den Link **Aktivieren/ Reparieren**.

2. Stellen Sie sicher, dass der regelmäßige Auftrag zur Steuerung der auf Fingerabdrücken basierten Erkennung aktiviert und ordnungsgemäß konfiguriert ist.

   a. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**an.

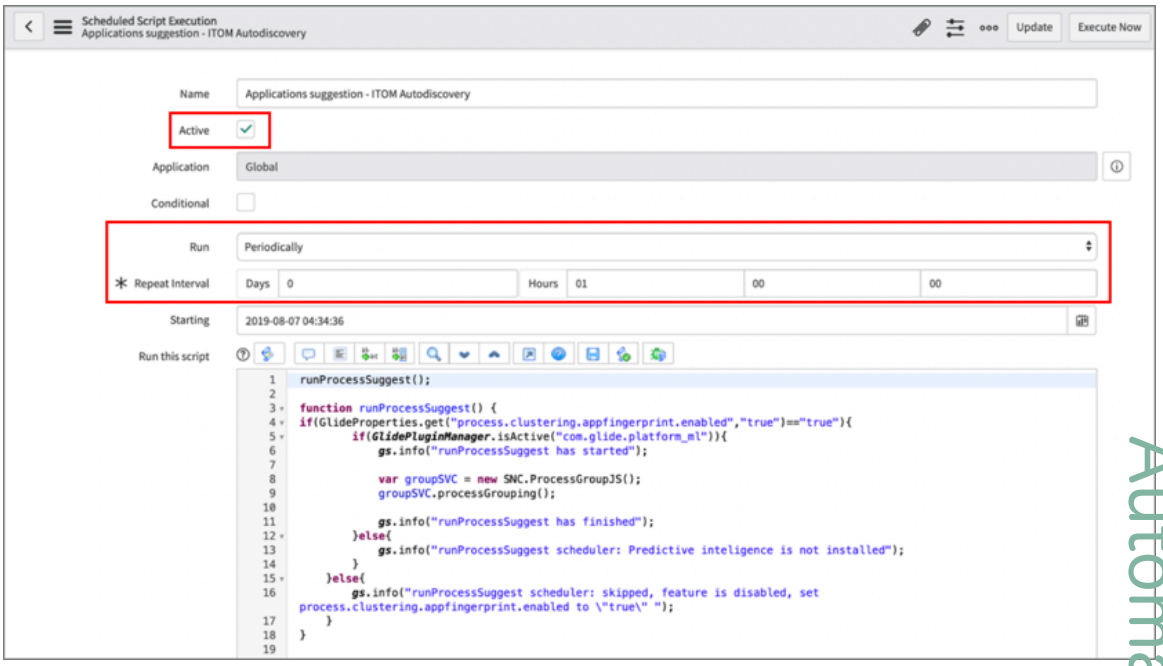
   b. Wählen Sie die regelmäßige Aufgabe *Applications suggestion - ITOM Autodisco* in der Liste aus.

   c. Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** aktiviert ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Überprüfen Sie, ob die Erkennungshäufigkeit wie im folgenden Beispiel auf eine Stunde festgelegt ist:

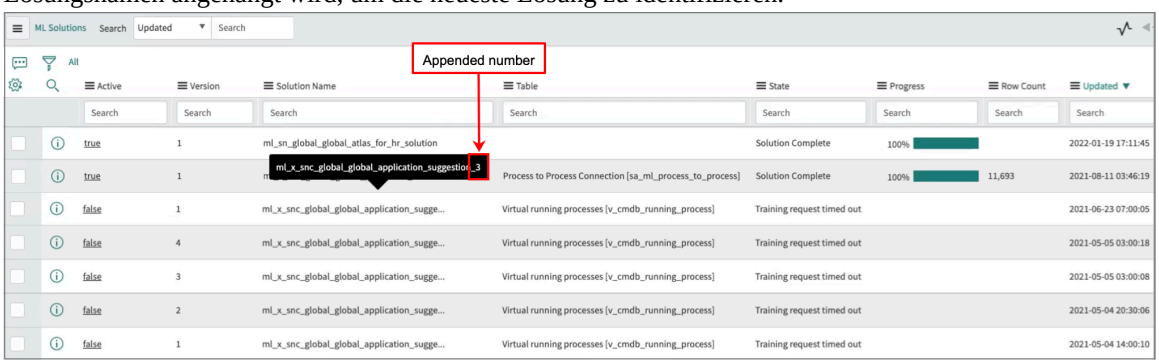


3. Prüfen Sie, ob die für die Gruppierung von Prozessen in Vorschlägen verantwortliche Clustering-Lösung aktiv ist.

a. Geben Sie Ein ml_solution.list In **Filternavigator** Feld von **Navigation** Bereich.
Auf der Registerkarte **ML-Lösungen** werden alle Lösungen angezeigt, einschließlich Clusterlösungen.

b. Identifizieren Sie Clusterlösungen, indem Sie die Spalte **Tabelle** überprüfen.
Vom System werden Clusterlösungen in der Tabelle „Virtuelle laufende Prozesse“ [v_cmdb_running_process] gespeichert.

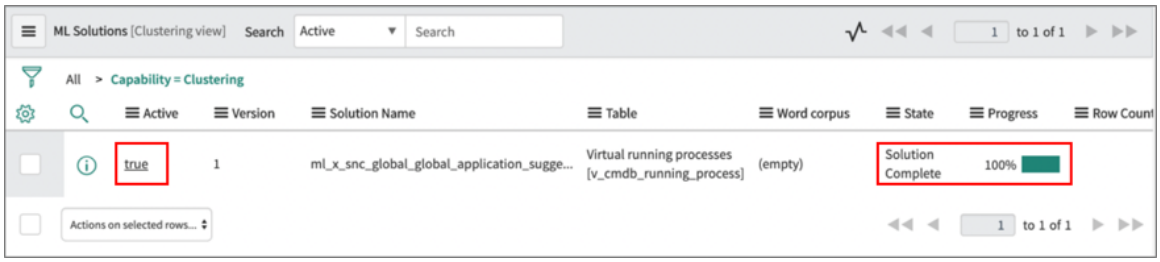
c. Wenn mehrere Clusterlösungen vorhanden sind, identifizieren Sie die neueste Lösung anhand des Zeitstempels in der Spalte **Aktualisieren**.
Alternativ dazu können Sie die Nummer verwenden, die vom System an den Lösungsnamen angehängt wird, um die neueste Lösung zu identifizieren.



d. Stellen Sie sicher, dass **Status** den Wert **Lösung abgeschlossen** und **Fortschritt** den Wert **100 %** aufweist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wenn der Statuswert nicht „Lösung abgeschlossen“ ist, konfigurieren Sie Predictive Intelligence Wie in beschrieben Konfigurationstipps für Predictive Intelligence .

4. Prüfen Sie, ob die Clustering-Lösung genügend Prozessgruppen erstellt hat, die zu Vorschlägen werden.
   a. Navigieren zu **Systemdefinition** > **Tabellen** Und suchen Sie die Tabelle virtuelle laufende Prozesse [V_cmdb_running_Process].
   b. Überprüfen Sie, ob diese Tabelle mehr als 1000 Datensätze enthält.
   c. Wenn weniger als 1000 Prozesse vorhanden sind, erkennen Sie weitere Prozesse, indem Sie eine horizontale Erkennung für zusätzliche IP-Bereiche oder Subnetze ausführen.
   d. Wenn nach der Erkennung zusätzlicher IP-Bereiche oder Subnetze immer noch weniger als 1000 Prozesse vorhanden sind, deaktivieren Sie die auf Fingerabdrücken basierte Erkennung.
5. Überprüfen Sie, ob **Anwendungsvorschlag – ITOM Autodisco** Transaktion wird nicht langsam geladen, wie in beschrieben Zeigen Sie aktive Transaktion an, und beenden Sie sie .
   Wenn diese Transaktion übermäßig lange ausgeführt wird, beenden Sie sie.

Feinabstimmung der Vorschläge der auf Fingerabdrücken basierten Erkennung

Passen Sie die Definitionen prozessbasierter Vorschläge an, bevor Sie die Erkennung starten. Normalerweise müssen Sie automatisch generierte Vorschläge optimieren, wenn die Genauigkeit weniger als 100 % beträgt. Predictive Intelligence Erstellt Vorschläge und stellt die Genauigkeitsschätzung für jeden Vorschlag bereit. Die mangelnde Genauigkeit kann dazu führen, dass erforderliche Anwendungen nicht erkannt werden oder dass zusätzlich zu den richtig erkannten Anwendungen falsche Anwendungen erkannt werden.

Vorbereitungen

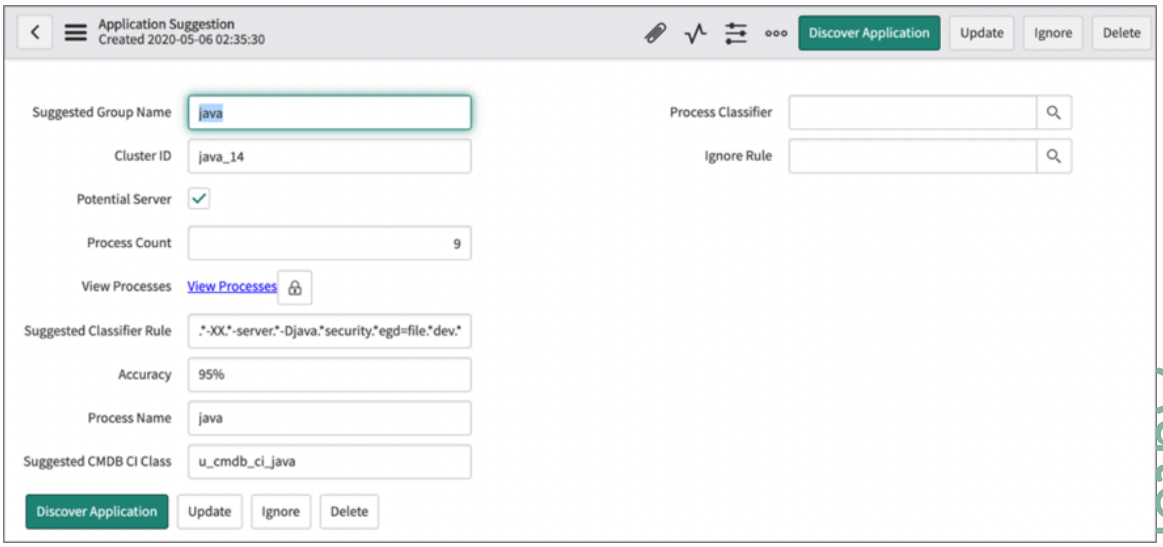
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**an.
2. Klicken Sie auf **Fingerabdrücke der Anwendung**.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Navigieren Sie mit einer der folgenden Methoden zur Liste der Vorschläge:
   - Zeigen Sie im Tortendiagramm mit den **häufigsten Vorschlägen** die wichtigsten Vorschläge an, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen.
   - Um nur Vorschläge für Anwendungsserver anzuzeigen, klicken Sie auf die **Kachel für vorgeschlagene Anwendungsserver**. Die gefilterte Liste mit Vorschlägen für Anwendungsserver wird angezeigt. Diese Liste ist auch so gefiltert, dass nur Vorschläge mit einer Genauigkeit von 100 % angezeigt werden.
   - Sie können auch **alle Vorschläge** anzeigen. Die ungefilterte Liste mit allen Vorschlägen wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie in der Liste „Anwendungsvorschläge“ auf den relevanten Vorschlag in der Spalte **Vorgeschlagener Gruppenname**.
   Das Formular „Anwendungsvorschlag“ wird geöffnet.



5. Um den Namen zu ändern, der für die auf Fingerabdrücken basierte Erkennung verwendet wird, geben Sie den gewünschten Namen in das Feld **Name** ein.
   Beispielsweise führen viele Anwendungen Java-Prozesse aus. Der vorgeschlagene Gruppenname für diese Gruppen lautet dann **Java**. Sie können einen Namen zuweisen, der die Anwendung, die Sie mithilfe dieses Vorschlags erkennen möchten, besser beschreibt (zum Beispiel `java_myweblogic`).
6. Um den für die CI-Klasse verwendeten Namen zu ändern, geben Sie den Namen der bevorzugten CI-Klasse in das Feld **Vorgeschlagene CMDB CI-Klasse** ein.
7. Um die Klassifiziererregel zu verfeinern, ändern Sie die regulären Ausdrücke im Feld **Vorgeschlagene Klassifiziererregel**.
   Fügen Sie dem regulären Ausdruck für die Erkennung einer Tomcat-Anwendung beispielsweise Versionsinformationen hinzu: `.*tomcat.* -Dopss.*version=12.1.3.*`
8. Klicken Sie auf **Aktualisieren**.
9. Wenn Sie nicht sicher sind, wie die Klassifiziererregel geändert werden kann, nehmen Sie nach der ersten Erkennung eine Feinabstimmung vor, wie unter Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen beschrieben.

Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen

Optimieren Sie den regulären Ausdruck in der Klassifiziererregel, um Discovery-Ergebnisse zu präzisieren. Predictive Intelligence extrahiert reguläre Ausdrücke aus Prozessen und weist sie Klassifiziererregeln als Teil der Erstellung von Vorschlägen zu. Wenn Sie mit den Erkennungsergebnissen nicht zufrieden sind oder die Vorschlagsgenauigkeit weniger als 100 % beträgt, ändern Sie den regulären Ausdruck.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

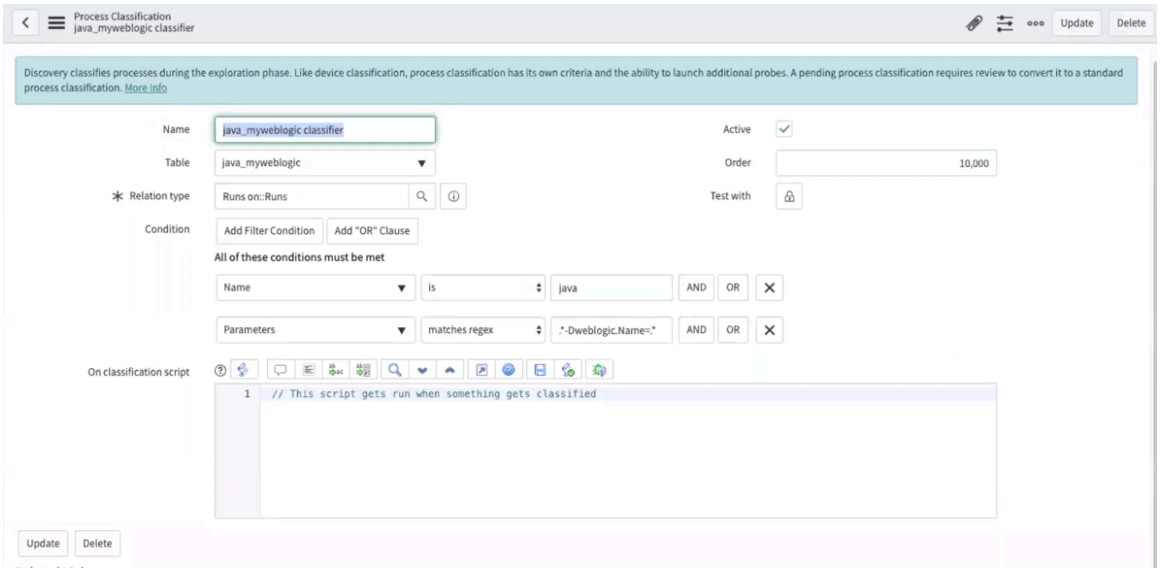
1. Navigieren zu **Alle** > **Anwendung** > **Modul**an.
2. Klicken Sie auf **Anwendung erkennen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die auf Fingerabdrücken basierte Erkennung findet die Anwendung und erstellt eine CI-Klasse, einen Klassifizierer und ein Muster.

3. Klicken Sie in der Liste **Anwendungsvorschläge** auf den neu erstellten Prozessklassifizierer.
   Das Formular „Prozessklassifizierung“ wird geöffnet.



4. Beachten Sie den regulären Ausdruck im Wertfeld **Parameter** unter **Bedingung**, der von Predictive Intelligence automatisch ausgewählt wird.
   In diesem Beispiel lautet der Wert **.*-DweblogicName=.***

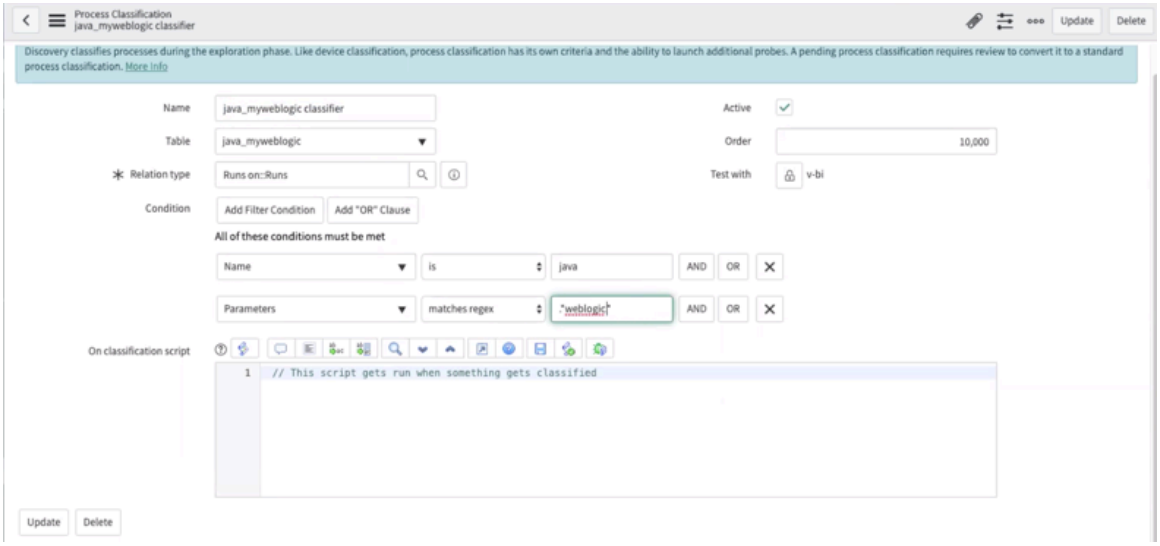
5. Klicken Sie auf das **Vorhängeschloss**-Symbol neben **Testen mit**.

6. Klicken Sie auf das **Suchsymbol**, um den Server auszuwählen, auf dem Sie zusätzliche reguläre Ausdrücke testen möchten.
   Eine Liste mit allen erkannten Servern wird geöffnet.

7. Wählen Sie den Server aus, der die Anwendung ausführt, die Sie mithilfe des benutzerdefinierten Klassifizierers erkennen möchten.
   Der ausgewählte Server wird im Feld **Testen mit** angezeigt.

8. Klicken Sie mit der rechten Maustaste in den Header des Prozessklassifizierungsformulars, und wählen Sie **Speichern** aus.
   Das System führt einen Test aus und zeigt die Ergebnisse auf der Registerkarte **Testergebnisse** unten auf der Seite an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Überprüfen Sie auf der Registerkarte „Testergebnisse“ die Prozesse, die mithilfe der für diesen Klassifizierer konfigurierten regulären Ausdrücke erkannt wurden.
10. Passen Sie den regulären Ausdruck im Wertfeld „Parameter“ unter **Bedingungen** an.
    Beispiel: Formulieren Sie ihn allgemeiner: `".*weblogic.*"`
11. Klicken Sie mit der rechten Maustaste in den Header des Prozessklassifizierungsformulars, und wählen Sie **Speichern** aus.
    Das System führt den Test erneut aus und zeigt die Ergebnisse auf der Registerkarte **Testergebnisse** unten auf der Seite an.
12. Überprüfen Sie auf der Registerkarte „Testergebnisse“, ob die Fingerabdruckerkennung die Anwendungen wie erwartet erkannt hat.

Auf Fingerabdrücken basierte Erkennung deaktivieren

Die auf Fingerabdrücken basierte Erkennung ist standardmäßig aktiviert. Deaktivieren Sie die prozessbasierte Anwendungserkennung, wenn Predictive Intelligence nicht genügend Prozesse generiert.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Fügen Sie die Systemeigenschaft hinzu `sys_property` `process.clustering.appfingerprint.enabled`Wie in beschrieben Fügen Sie eine Systemeigenschaft hinzu .
2. Um die Erkennung zu deaktivieren, geben Sie `false` in das Feld **Wert** ein.
3. Um die auf Fingerabdrücken basierte Erkennung wieder zu aktivieren, ändern Sie das Feld **Wert** in `true`.

Zugehörige Informationen

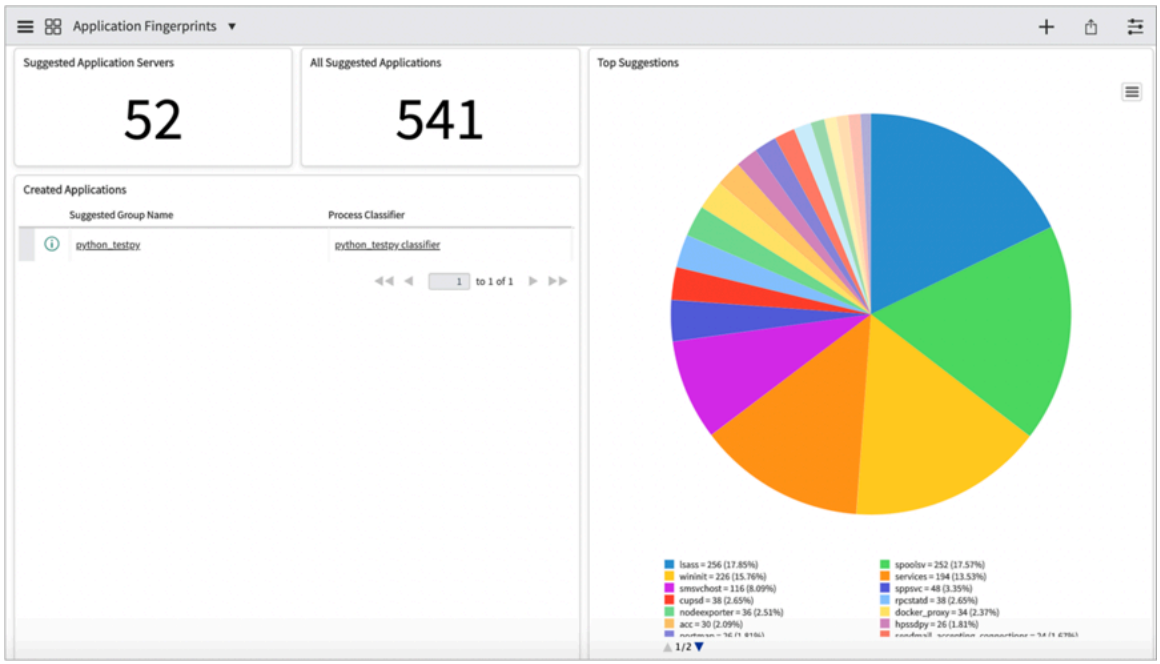
KB0826261: Advanced configuration and troubleshooting of fingerprint-based discovery (Erweiterte Konfiguration und Problembehandlung bei der auf Fingerabdrücken basierten Erkennung)

Leitfaden zur Fehlerbehebung für ML-Verbindungsvorschläge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Fingerabdrücke der Anwendung“

ITOM-Transparenz nutzt Predictive Intelligence zur ersten Analyse erkannter Prozesse und empfiehlt Anwendungen, für die eine Erkennung durchgeführt werden sollte. Mit dieser Methode erstellt ITOM-Transparenz automatisch eine CI-Klasse für die Configuration Management Database (CMDB), einen Klassifizierer oder ein Muster für die neue Anwendungs-CI-Klasse. Verwenden Sie das Dashboard „Fingerabdrücke der Anwendung“, um vorgeschlagene Anwendungen zu überprüfen.



Erforderliche ServiceNow AI Platform-Rollen

discovery_admin, führt die horizontale Erkennung mit Discovery aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Administrator, der die horizontale Erkennung des IT-Netzwerks der Organisation durchführt	Überprüfen Sie Anwendungsvorschläge, und entscheiden Sie, welche Anwendungen anhand von Fingerabdrücken erkannt werden sollen. Durch Ausführen dieser Aktion werden die Ergebnisse der grundlegenden horizontalen Erkennung verbessert.

Indikatoren

Vorgeschlagene Anwendungsserver

Die gefilterte Liste mit Vorschlägen für Anwendungsserver wird angezeigt.

Vorgeschlagene Anwendungen

Die vollständige Liste mit Vorschlägen für Anwendungen wird angezeigt.

Erstellte Anwendungen

Die Liste der Anwendungen, die das System basierend auf Fingerabdrücken erkannt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
Häufigste Vorschläge	Kreisdiagramm	Anwendungsvorschlag [cmdb_process_groups]	Ein Tortendiagrammbericht mit den häufigsten Vorschlägen, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen. Die Prozessanzahl spiegelt sich in der Größe des jeweiligen Diagrammsegments wider. Klicken Sie auf das Segment, um die entsprechenden Vorschläge in einer gefilterten Liste anzuzeigen. Klicken Sie zum Ausblenden eines Vorschlags aus dem Diagramm auf den Namen des Vorschlags in der Diagrammlegende.

Netzwerk-Discovery

Bei der Netzwerkerkennung mit Discovery werden die internen IP-Netzwerke und Subnetze innerhalb Ihrer Organisation erkannt.

Hinweis: Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung mit Discovery nicht erforderlich. Diese Erkennung ist für Organisationen konzipiert, die die für Discovery in ihren Netzwerken verfügbaren IP-Adressen nicht vollständig kennen.

Funktionsweise der Netzwerkerkennung

Mit den erfassten Informationen aktualisiert Discovery Router und Layer-3-Switches in der CMDB. Ein einzelner MID Server, der mit dem Scannen in einer konfigurierbaren Liste von Startroutern (oder *Seed*-Routern) beginnt, führt die Netzwerk-Discovery aus. Normalerweise entsprechen die Startrouter den Standardroutern, die von allen MID Server-Hostcomputern im Netzwerk verwendet werden. Es können jedoch auch beliebige Router festgelegt werden. Der MID Server verwendet die Routertabellen der Startrouter, um andere Router im Netzwerk zu erkennen. Der MID Server breitet sich dann über das Netzwerk aus und verwendet gefundene Routertabellen, um andere Router zu erkennen. Dies wird solange fortgesetzt, bis die Erkundung aller Router und Switches abgeschlossen ist.

Konvertieren Sie nach der Netzwerkerkennung mit Discovery die gefundenen IP-Netzwerke in Range Sets von IP-Adressen, die Sie in Erkennungszeitplänen zum Erkennen von Konfigurationselementen (CI) verwenden.

Konfigurieren SNMP-Anmeldeinformationen , Und lassen Sie Port 161 für SNMP-Zugriff geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Netzwerkerkennung

Die Standardwerte können für die meisten Erkennungen verwendet werden. Navigieren zu **Discovery-Definitionen** > **Eigenschaften** Zum Bearbeiten der Eigenschaften.

Feld	Beschreibung
glide.discovery.bgp_router_disable	BGP-Routererkundung deaktiviert: Deaktivierung der Ausführung des Probe **SNMP – Routing** oder des Musters, wenn ein Router erkannt wird, von dem das BGP-Protokoll ausgeführt wird. Normalerweise IST diese Exploration inaktiv, da BGP-Routingtabellen sehr groß sind und solche Router im Allgemeinen nur an der Peripherie großer Netzwerke arbeiten, in denen eine weitere Netzwerk-Discovery irrelevant wäre. Dieser Wert könnte auf „falsch“ gesetzt werden, wenn Ihr Unternehmen nur BGP-Router als Edge-Router zwischen relativ kleinen Netzwerken (z. B. zwischen Gebäuden auf einem einzelnen Campus) verwendet. Wenn Sie die Tabelle [Discovery_device_neighbors] während der Erkennung der horizontalen Ebene 2 der bgp-fähigen Geräte ausfüllen müssen, legen Sie fest **BGP-Routererkundung deaktiviert** Eigenschaft bis **Nein** . Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen mit zu wenig Arbeitsspeicher auf dem MID-Server. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.network_discovery	Debugging der Netzwerkerkennung: Ermöglicht die umfassende Protokollierung aller Netzwerk-Discovery-Aktivitäten auf der Instanz. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Monitoring von Erkennungen und Problemlösung
glide.discovery.discoverable.network.max.netmask.bits	Maximale Netzmaskengröße für auffindbare Netzwerke (Bits): Die maximale Anzahl von Bits in einer regulären Netzmaske für Netzwerke, die von einer Netzwerk-Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erkannt werden. Eine *reguläre* Netzmaske ist eine Netzmaske, die binär als eine Zeichenfolge von Einsen, gefolgt von einer Zeichenfolge von Nullen, ausgedrückt werden kann. Beispiel: 255.255.255.0 ist regulär, und 255.255.255.64 ist irregulär. Reguläre Netzwerke werden im Allgemeinen wie folgt ausgedrückt: 10.0.0.0/24, d. h. eine Netzwerkadresse von 10.0.0.0 mit einer Netzmaske von 255.255.255.0. Größere Bitzahlen bedeuten Netzwerke mit einer kleineren Anzahl von Adressen. Beispielsweise enthält das Netzwerk 10.128.0.128/30 vier Adressen: eine Netzwerkadresse (10.128.0.128), eine Broadcast-Adresse (10.128.0.131) und zwei verwendbare Adressen (10.128.0.129 und 10.128.0.130). Kleine Netzwerke werden normalerweise in Netzwerkgeräten konfiguriert, damit Loopback-Adressen oder Netzwerke bereitgestellt werden können, die ausschließlich von Punkt-zu-Punkt-Verbindungen verwendet werden. Da diese Arten von Netzwerken im Allgemeinen nicht von Netzwerk Discovery entdeckt werden müssen, wäre es nützlich, sie herauszufiltern. Wenn Sie diese Eigenschaft auf einen Wert von 1 bis 32 festlegen, können Sie die Größe der erkannten regulären Netzwerke begrenzen. Wenn Sie einen anderen Wert festlegen, werden alle Netzwerke erkannt. Unregelmäßige Netzwerke werden immer entdeckt. Der Standardwert ist 28, was bedeutet, dass reguläre Netzwerke mit 8 oder weniger Adressen nicht erkannt werden können. • **Typ**: Ganzzahl • **Standardwert**: 28
glide.discovery.network_owner_method	Auswahlmethode für Netzwerkrouter: Diese Eigenschaft steuert die Methode, die zur Entscheidung verwendet wird (während Netzwerk Discovery) welcher Router als Router ausgewählt werden soll, der einem bestimmten IP-Netzwerk zugeordnet werden soll. Die möglichen Werte sind: • **Erster Router** : Der erste Router, der das Netzwerk erkennt, ist zugeordnet • **Letzter Router** : Der letzte Router, der das Netzwerk erkennt, ist zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Die Meisten Netzwerke** : Der Router mit den am häufigsten angeschlossenen Netzwerken ist zugeordnet • **Geringste Netzwerke** : Der Router mit den am wenigsten angeschlossenen Netzwerken ist zugeordnet • **Typ**: Auswahlliste • **Standardwert**: Die meisten Netzwerke • **Zusatzoptionen**: Erster Router, Letzter Router, Die wenigsten Netzwerke
glide.discovery.physical_interface_types	Physikalische Schnittstellentypen: Eine durch Kommas getrennte Liste von Schnittstellentypen, die für die Netzwerkerkennung als *physisch* angesehen werden. Wenn ein Router (oder ein weiterleitungsfähiges Gerät) über eine Schnittstelle dieses Typs verfügt, werden die mit dieser Schnittstelle verbundenen Netzwerke als lokal mit diesem Gerät verbunden angesehen. Die Standardschnittstellentypen umfassen die Typen Ethernet, 802.11 und Token Ring. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Zeichenfolge • **Standardwert**: 6,117,9,71,209
glide.discovery.switch_interface_types	Switch-Schnittstellentypen: Kommagetrennte Liste von Schnittstellentypen, die berücksichtigt werden. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. Geräte mit beliebigen Schnittstellentypen, die NICHT in dieser Liste angezeigt werden, werden als Router klassifiziert, wenn sie über Weiterleitungsfunktionen verfügen. Eine vollständige Liste der Schnittstellentypnummern finden Sie auf der IANA-Website im Abschnitt „ifType-Definitionen.“ • **Typ**: Zeichenfolge • **Standardwert**: 7,8,9,26,53,62,69,71,78,115,117,209

Mehr erfahren

Was ist Netzwerk-Discovery?

Netzwerkerkennung ausführen

Konfigurieren Sie die Netzwerkennung mit Discovery über einen Discovery-Zeitplan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Konfigurieren SNMP-Anmeldeinformationen , Und lassen Sie Port 161 für SNMP-Zugriff geöffnet.

Erforderliche Rolle: keine

Prozedur

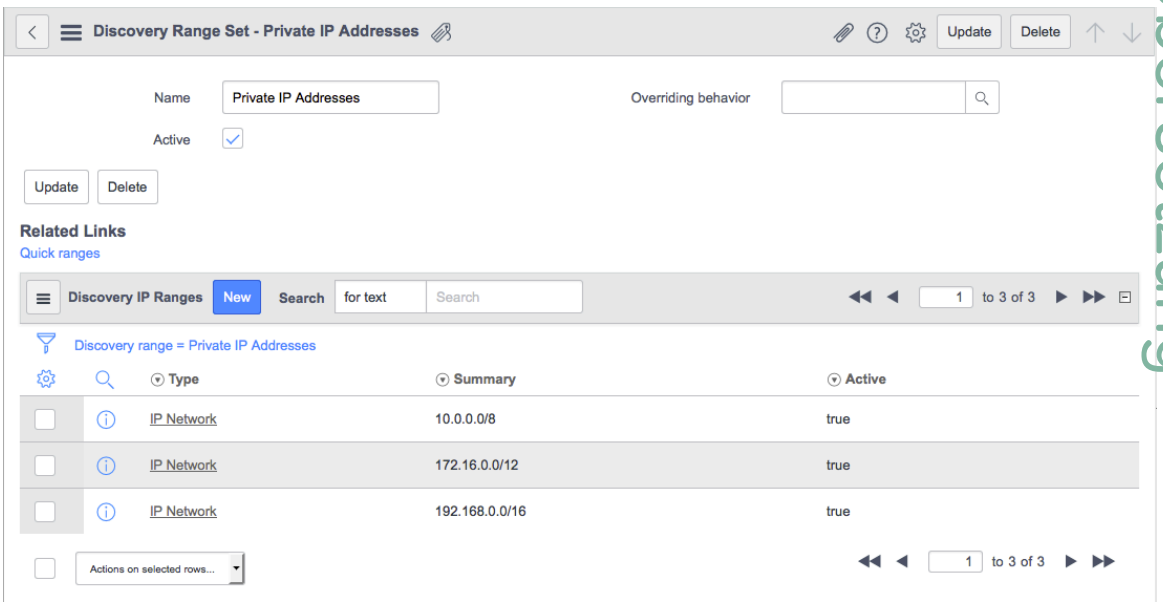
1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**, und wählen Sie **Netzwerke** aus der Liste im Feld *Erkennen* aus.
3. Wählen Sie einen MID Server aus.

   Dieses Feld ist ein Pflichtfeld.
4. Füllen Sie das Formular einschließlich der Planungsfelder aus.
5. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

   Der Bereich **Zugehörige Links** wird mit zugehörigen Listen angezeigt.
6. Klicken Sie unter „Zugehörige Links“ auf **Private Netzwerk-Discovery-IPs**, um die Liste der standardmäßigen privaten IP-Netzwerke in der zugehörigen Liste *Discovery-IP-Bereiche* anzuzeigen.

   Die Standard-IP-Netzwerke in dieser Liste sind für jede von Ihnen durchgeführte Netzwerkerkennung mit Discovery verfügbar und für die meisten Erkennungen ausreichend.
7. Wenn Ihre Organisation über zusätzliche private IP-Adressen verfügt, klicken Sie auf **Neu**, um sie hinzuzufügen.

Private IP-Adressen

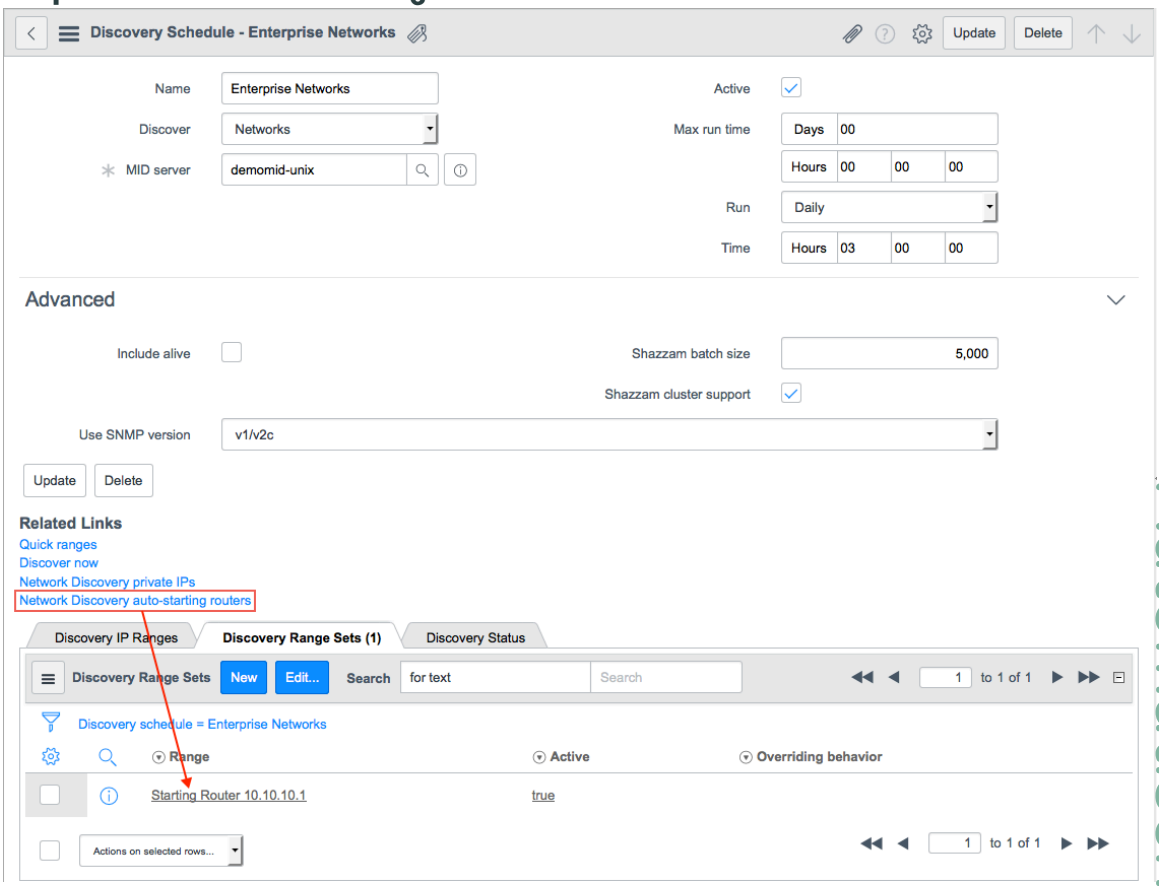


8. Fügen Sie dem Zeitplan in der Liste *Discovery-Range Sets* Startrouter hinzu.
   a. Klicken Sie auf den Link **Netzwerk-Discovery-Auto-Start-Router**, um die Liste mit dem Startrouter für jeden MID Server in Ihrem Netzwerk zu füllen.
   b. Klicken Sie auf **Bearbeiten**, um der Liste Router hinzuzufügen bzw. daraus zu löschen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitplan der Netzwerkerkennung



9. Führen Sie die Discovery manuell oder über den Zeitplaner aus.

IP-Netzwerke in Discovery-Range Sets konvertieren

Nachdem Sie mit Discovery eine Netzwerkerkennung ausgeführt haben, müssen Sie die erkannten IP-Netzwerke in Range Sets konvertieren, um sie zur Erkennung anderer Geräte nutzen zu können.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Ausgabe und Artefakte** > **IP-Netzwerke**an.

2. Klicken Sie auf **Neu**, um ein IP-Netzwerk hinzuzufügen.

3. Stellen Sie sicher, dass die folgenden Feldwerte bereitgestellt werden:

- **Status**: *Bereit*
- **Erkennen**: *Aktiviert (true)*
- **Router**: Wählen Sie in der Liste einen Router aus. Dieses Feld darf nicht leer sein.

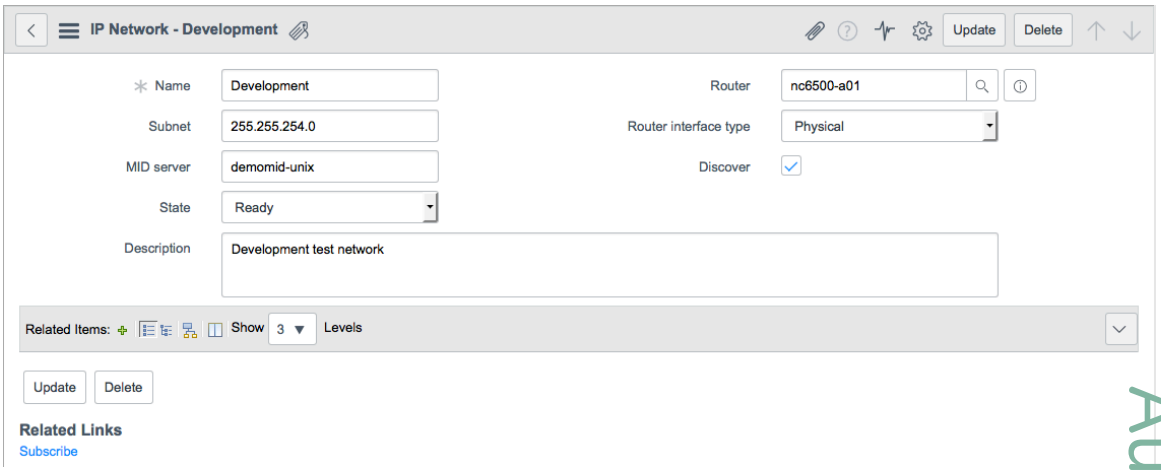
  Wenn Ihre IP-Netzwerke über eine Netzwerkerkennung mit Discovery erstellt wurden, werden diese Felder in der zugehörigen Liste *IP-Netzwerke* automatisch gefüllt. Wenn Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die IP-Netzwerke jedoch manuell eingegeben haben und Sie Ihre IP-Netzwerke manuell in Range Sets konvertieren möchten, müssen Sie die Felder entsprechend bearbeiten.

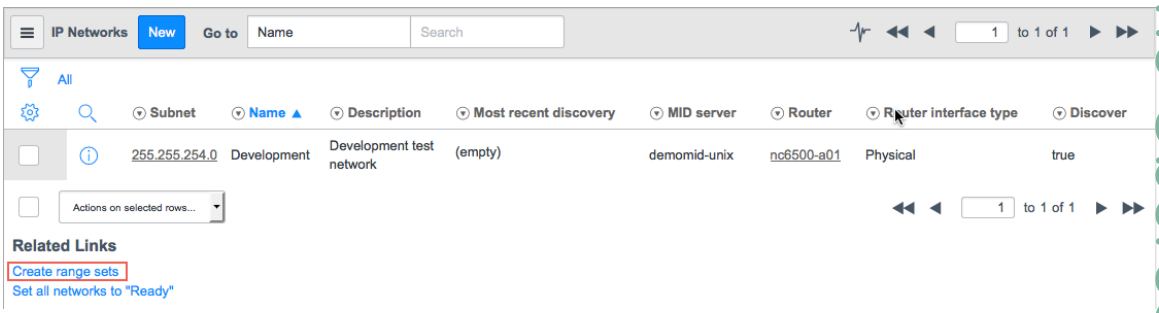
Formular „IP-Netzwerk“



4. Klicken Sie auf **Aktualisieren**, um zur Liste der IP-Netzwerke zurückzukehren.
5. Klicken Sie unter **Zugehörige Links** auf **Range Sets erstellen**.

   Verwenden Sie diese Funktion, um alle IP-Netzwerke in der Liste in Range Sets zu konvertieren.

Liste der IP-Netzwerke



   Die Seite Discovery-Status wird eingeblendet und zeigt den Fortschritt der Konvertierung an. Unter **Gestartet** und **Abgeschlossen** erhöht sich die Anzahl der IP-Netzwerke, bis alle Netzwerke konvertiert wurden.

Nächste Maßnahme

Fügen Sie Erkennungszeitplänen Discovery-Range Sets hinzu.

Einem Erkennungszeitplan Discovery-Range Sets hinzufügen

Nachdem Sie mithilfe einer Netzwerkerkennung Discovery-Range Sets erzeugt haben, fügen Sie diese Sätze einem Erkennungszeitplan hinzu. Dieser Prozess schränkt den Bereich der IP-Adressen ein, die Shazzam-Probes scannen können. Sie können auch ein Verhalten hinzufügen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie einen Erkennungszeitplan.
2. Klicken Sie in der zugehörigen Liste **Discovery-Range Sets** auf **Bearbeiten**, um ein vorhandenes Range Set hinzuzufügen, und verwenden Sie den Slushbucket, um das Range Set hinzuzufügen.
3. Klicken Sie im Formular **Discovery-Zeitplan** in der Spalte **Bereich** der zugehörigen Liste **Discovery-Range Sets** auf den Namen des Range Set.
4. Fügen Sie im Formular **Discovery Bereich** ein Discovery-Verhalten hinzu.
   Sie können auch das für diesen Zeitplan festgelegte Range Set aktivieren oder deaktivieren.
5. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Speichern** aus.

Serverlose Erkennung

Discovery kann Anwendungen auf Hostcomputern suchen, ohne zunächst den Host erkennen zu müssen. Diese Art von Erkennung wird als *serverlose* Discovery bezeichnet.

Die serverlose Erkennung basiert auf Infrastrukturmustern zum Untersuchen von CIs auf einem Host. Bei dieser Art von Erkennung werden die Scanphase und Klassifizierungsphase der Erkennung übersprungen. Es gibt zwei Arten der serverlosen Erkennung: standardmäßig und hostbasiert. Beide Typen erfordern ein Infrastrukturmuster.

Standardmäßige serverlose Discovery

Bei der standardmäßigen serverlosen Erkennung werden CIs von Remoteanwendungen erkannt, die sich auf einem unbekannten Host befinden. Bei dieser Art der serverlosen Erkennung werden für die Suche nach CIs Protokolle wie REST und HTTP verwendet. Die IP-Adresse des Hostcomputers ist nicht erforderlich. Sie definieren Eingabeparameter in einem Infrastrukturmuster, um eine Verbindung zu einer Remoteressource herzustellen. Verwenden Sie diese Art der Erkennung, wenn Sie webbasierte Anwendungen erkennen möchten.

Hostbasierte serverlose Erkennung

Mit der hostbasierten serverlosen Erkennung kann nach CIs gesucht werden, die sich auf einem bereits erkannten Hostcomputer befinden. Der Host fungiert als Proxy, über den Sie andere CIs finden. Sie führen Discovery nicht tatsächlich für den Host aus. Verwenden Sie diese Art von Erkennung in folgenden Fällen:

- Sie kennen die IP-Adresse der CIs nicht, die erkannt werden sollen, oder die CIs haben gar keine IP-Adressen.
- Die CIs befinden sich auf einem bereits erkannten Host-CI.

Für diese Art von Erkennung benötigen Sie auch ein Infrastrukturmuster, müssen aber keine Eingabeparameter wie bei der standardmäßigen serverlosen Erkennung definieren. Das Muster kann Vorgänge angeben, zum Beispiel eine WMI-Abfrage, die Abfragen auf einem Host ausführt. Nachdem Discovery eine Verbindung zum Host hergestellt hat, werden die Anmeldeinformationen des Hosts verwendet, um die Erkennung der CIs durchzuführen, die Sie im Muster erkunden. Sie müssen keine zusätzlichen Anmeldeinformationen angeben. Wenn Sie für das Muster den Debug-Modus ausführen, werden unter **Vorübergehende Variablen** Details zum Muster angezeigt. Sie können dann Mustervorgänge erstellen, die API-Aufrufe vom Host an die CIs tätigen, die Sie erkennen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serverlose Erkennungszeitpläne

Die Infrastrukturmuster, die durch die serverlose Erkennung verwendet werden, werden durch einen Erkennungszeitplan und nicht durch einen Klassifizierer ausgelöst. Bei der serverlosen Erkennung werden Klassifizierer ignoriert. Verwenden Sie einen serverlosen Zeitplantyp für beide Arten der serverlosen Erkennung. Im serverlosen Zeitplan können Sie Folgendes angeben:

- Werte für Eingabeparameter im Muster, wenn Sie die standardmäßige serverlose Erkennung verwenden. Anweisungen dazu finden Sie unter Zeitplan für standardmäßige serverlose Erkennung erstellen.
- Ein Host-CI, wenn Sie eine Proxy-Host-basierte Erkennung verwenden. Weitere Informationen finden Sie unter Zeitplan für hostbasierte serverlose Erkennung erstellen.

Muster und Zeitplan für standardmäßige serverlose Erkennung erstellen

Um Anwendungs-CIs auf einem unbekannten Host zu erkennen, erstellen Sie ein Infrastrukturmuster für die standardmäßige serverlose Erkennung. Nachdem Sie das Muster erstellt haben, erstellen Sie einen Erkennungszeitplan, der das Muster auslöst.

Vorbereitungen

Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Zur Erkundung des CI müssen Sie im Muster Eingabeparameter angeben.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie ein Muster vom Typ **Infrastruktur** mit dem richtigen CI-Typ an, der für die CIs gilt, die Sie erkennen möchten.
   Unter Muster erstellen oder anpassen werden alle Formularfelder erläutert.
4. Erstellen Sie einen Identifizierungsabschnitt, und speichern Sie das Muster.
5. Klicken Sie auf die Registerkarte **Eingabeparameter** und dann auf **Neu**.
6. Geben Sie die Parameter ein, die zum Erreichen der serverlosen CIs erforderlich sind.
   Beispielsweise können Sie eine URL eingeben, um eine Remoteressource über eine HTTP-Anforderung zu erreichen.

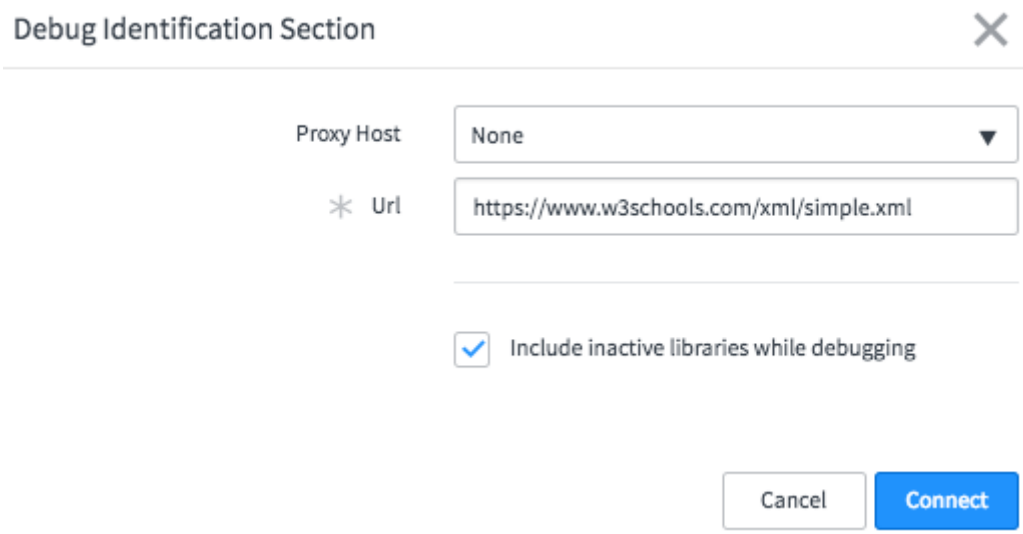
   Hinweis: In einem serverlosen Erkennungszeitplan geben Sie die tatsächliche URL an.

7. Speichern Sie das Muster.
8. Wählen Sie die Registerkarte **Standard** aus, und klicken Sie dann auf den Namen des Identifizierungsabschnitts, um den Musterdesigner zu öffnen.
9. Erstellen Sie die erforderlichen Schritte zur Erkundung serverloser CIs.
   Erstellen Sie beispielsweise einen Vorgang vom Typ **HTTP Get-Aufruf**, um eine Remoteressource über eine URL zu erreichen. In diesem Fall geben Sie den Parameter $url im Feld **URL** an.
10. Um das Muster zu testen, klicken Sie auf **Debug-Modus**, und geben Sie Werte für die Eingabeparameter ein.
    Sie müssen keinen Wert für **Proxy-Host** eingeben. In diesem Beispiel stellen wir eine Verbindung zu einer Website her, die eine XML-Datei bereitstellt. Die Analysemethode für XML-Dateien ist bereits im HTTP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Get-Aufruf definiert. Um den Mustervorgang zu testen, klicken Sie auf **Debug-Modus**, geben die URL ein, und klicken auf **Verbinden**.

Beispiel für Debugging eines HTTP Get-Aufrufs



11. Nachdem Sie eine Verbindung hergestellt und den Vorgang ausgeführt haben, wird der Inhalt im Feld **Ausgabe** angezeigt.

Zeitplan für standardmäßige serverlose Erkennung erstellen

Nachdem Sie ein Muster für die standardmäßige serverlose Erkennung erstellt haben, erstellen Sie einen Erkennungszeitplan und geben das Muster an. Discovery löst das Muster aus dem Zeitplan und nicht über den Klassifizierer aus.

Vorbereitungen

Stellen Sie sicher, dass Sie haben Anmeldeinformationen für Standardauthentifizierung Für HTTP-Aufrufe im Muster.

Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können diesen Zeitplan erneut verwenden, um dasselbe Muster mit anderen Parametern auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Ohne Server** im Feld **Discovery** aus.
   Unter Horizontale Erkennung planen werden die anderen Felder erläutert.
4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Klicken Sie in der zugehörigen Liste **Ausführungsmuster ohne Server** auf **Neu**.
6. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Muster	Wählen Sie das Muster aus, das Sie für die standardmäßige serverlose Erkennung oder für die Proxy-Host-basierte Erkennung erstellt haben.
Proxy-Host	Lassen Sie dieses Feld leer. Dieses Feld bezieht sich auf das Proxy-Host-basierte Szenario.
Aktiv	Lassen Sie dieses Kontrollkästchen aktiviert, um die Musterausführungsdefinition zu verwenden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. In **Startprogramm-Parameter Für Discovery-Muster** Zugehörige Liste, fügen Sie die für das Muster erforderlichen Parameter hinzu, und geben Sie einen Wert für jeden in der an **Wert** Spalte.
9. Klicken Sie auf **Absenden**.
10. Definieren Sie so viele Datensätze für serverlose Ausführungsmuster wie erforderlich.
    Sie können dasselbe Muster starten, es muss jedoch jeweils unterschiedliche Parameter aufweisen.
11. Führen Sie die Erkennung aus, indem Sie auf **Discovery starten** klicken, oder warten Sie, bis die Erkennung durch den Zeitplan ausgelöst wird.

Ergebnis

Überprüfen Sie Discovery Status, um anzuzeigen Discovery Protokoll, die Geräteliste, die die erkannten CIs enthält, und die ECC-Warteschlangendatensätze. Beachten Sie, dass die Shazzam-Probe und nicht gestartet wurde Discovery Es wurden keine Klassifizierungsprobes ausgelöst.

Zugehörige Informationen

Discovery-Status

Muster und Zeitplan für hostbasierte serverlose Erkennung erstellen

Um Anwendungs-CIs auf einem in der CMDB bekannten Host zu erkennen, erstellen Sie ein Infrastrukturmuster für die hostbasierte serverlose Erkennung. Nachdem Sie das Muster erstellt haben, erstellen Sie einen Erkennungszeitplan, der das Muster auslöst.

Vorbereitungen

Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie ein Muster vom Typ **Infrastruktur** mit dem richtigen CI-Typ an, der für die CIs gilt, die Sie erkennen möchten.
   Unter Muster erstellen oder anpassen werden alle Formularfelder erläutert.
4. Erstellen Sie einen Identifizierungsabschnitt, und speichern Sie das Muster.
5. Fügen Sie dem Muster Vorgänge hinzu, um das CI zu erkennen, auf das Sie über den Host zugreifen können.
6. Zum Testen des Musters klicken Sie auf **Debug-Modus**, und geben Sie die IP-Adresse des Hosts ein.

Zeitplan für hostbasierte serverlose Erkennung erstellen

Discovery löst das Muster für die hostbasierte serverlose Erkennung aus dem Zeitplan und nicht über den Klassifizierer aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Sie über Anmeldeinformationen für das Hostgerät verfügen, das als Proxy fungiert.

Erforderliche Rolle: Cloud_admin, Service_Mapping_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Ohne Server** im Feld „Discovery“ aus.
   Unter Horizontale Erkennung planen werden die anderen Felder erläutert.
4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Klicken Sie in der zugehörigen Liste **Ausführungsmuster ohne Server** auf **Neu**.
6. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Muster	Wählen Sie das Muster aus, das Sie für die hostbasierte Erkennung erstellt haben.
Proxy-Host	Wenn Sie die hostbasierte Erkennung verwenden, geben Sie ein vorhandenes CMDB-CI an. Discovery verwendet die Anmeldeinformationen dieses CI bei der Erkundung der CIs auf dem Host.
Aktiv	Lassen Sie dieses Kontrollkästchen aktiviert, um die Musterausführungsdefinition zu verwenden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

   Definieren Sie so viele Datensätze für serverlose Ausführungsmuster wie erforderlich. Sie können dasselbe Muster starten, es muss jedoch jeweils unterschiedliche Parameter aufweisen.

   Hinweis: Sie müssen keine Einträge in der zugehörigen Liste **Startprogrammparameter für Discovery-Muster** erstellen.

8. Führen Sie die Erkennung aus, indem Sie auf **Discovery starten** klicken, oder warten Sie, bis die Erkennung durch den Zeitplan ausgelöst wird.

Ergebnis

Überprüfen Sie Discovery Status, um anzuzeigen Discovery Protokoll, die Geräteliste, die die erkannten CIs enthält, und die ECC-Warteschlangendatensätze. Beachten Sie, dass die Shazzam-Probe und nicht gestartet wurde Discovery Es wurden keine Klassifizierungsprobes ausgelöst.

Discovery-Probes und -Sensoren

Discovery-Probes und -Sensoren führen die Datenerfassung durch und aktualisieren die CMDB.

Mit jeder Version ersetzen Muster viele Sonden und Sensoren für Discovery. Erwägen Sie das Erstellen neuer Muster oder das Bearbeiten vorhandener Muster, wenn Sie anpassen möchten, was Discovery finden kann. Die Informationen zu Sonden und Sensoren sind für Kunden gedacht, die noch keine Muster verwenden, und für Kunden, die bereits

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

benutzerdefinierte Sonden haben, die beim Upgrade beibehalten werden. Siehe Muster und horizontale Erkennung für weitere Informationen zu Mustern.

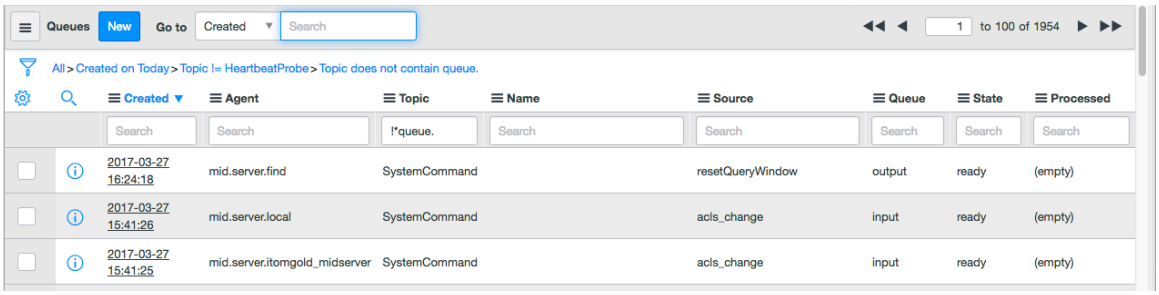
Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Erkennungsphasen

Discovery verwendet während der ersten beiden Erkennungsphasen (*Scan-Phase* und *Klassifizierungsphase*) stets Probes und Sensoren. Für die letzten beiden Phasen, *Identifizierungsphase* und *Erkundungsphase*, kann Discovery Probes und Sensoren oder Muster verwenden. Dieses Thema bezieht sich nur auf Probes und Sensoren. Erläuterungen der einzelnen Phasen finden Sie unter Discovery erkunden. Siehe Muster und horizontale Erkennung für weitere Informationen zu Mustern.

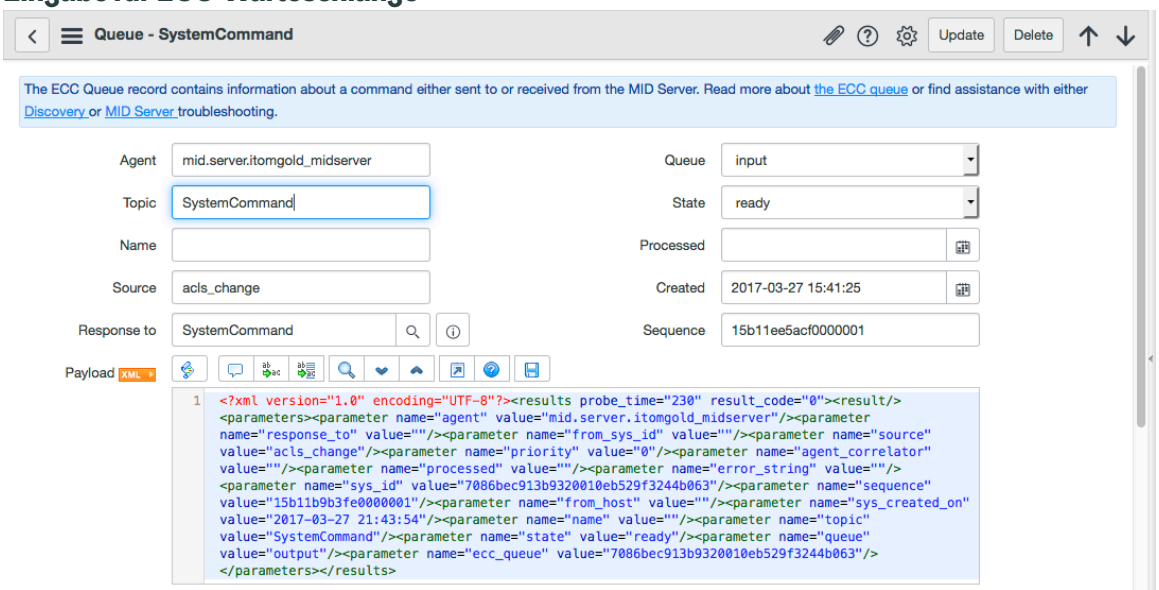
Probes, Sensoren und ECC-Warteschlange

Die Probe erfasst Informationen, die vom Sensor verarbeitet werden. Beide erhalten ihre Anweisungen aus der ECC-Warteschlange. Ein Arbeiterauftrag auf dem MID Server überwacht die Warteschlange auf Arbeit. Die Überwachung sucht nach Einträgen, bei denen das Feld *Warteschlange* den Wert *Ausgabe* und das Feld *Status* den Wert *Bereit* aufweist.



Der MID Server verarbeitet dann alle ausgegebenen ECC-Nachrichten, führt die erforderlichen Probes aus und gibt die Probe-Ergebnisse an die ECC-Warteschlange zurück. Diese Ergebnisse werden als Einträge vom Typ *Eingabe* in der ECC-Warteschlange abgelegt.

Eingabe für ECC-Warteschlange



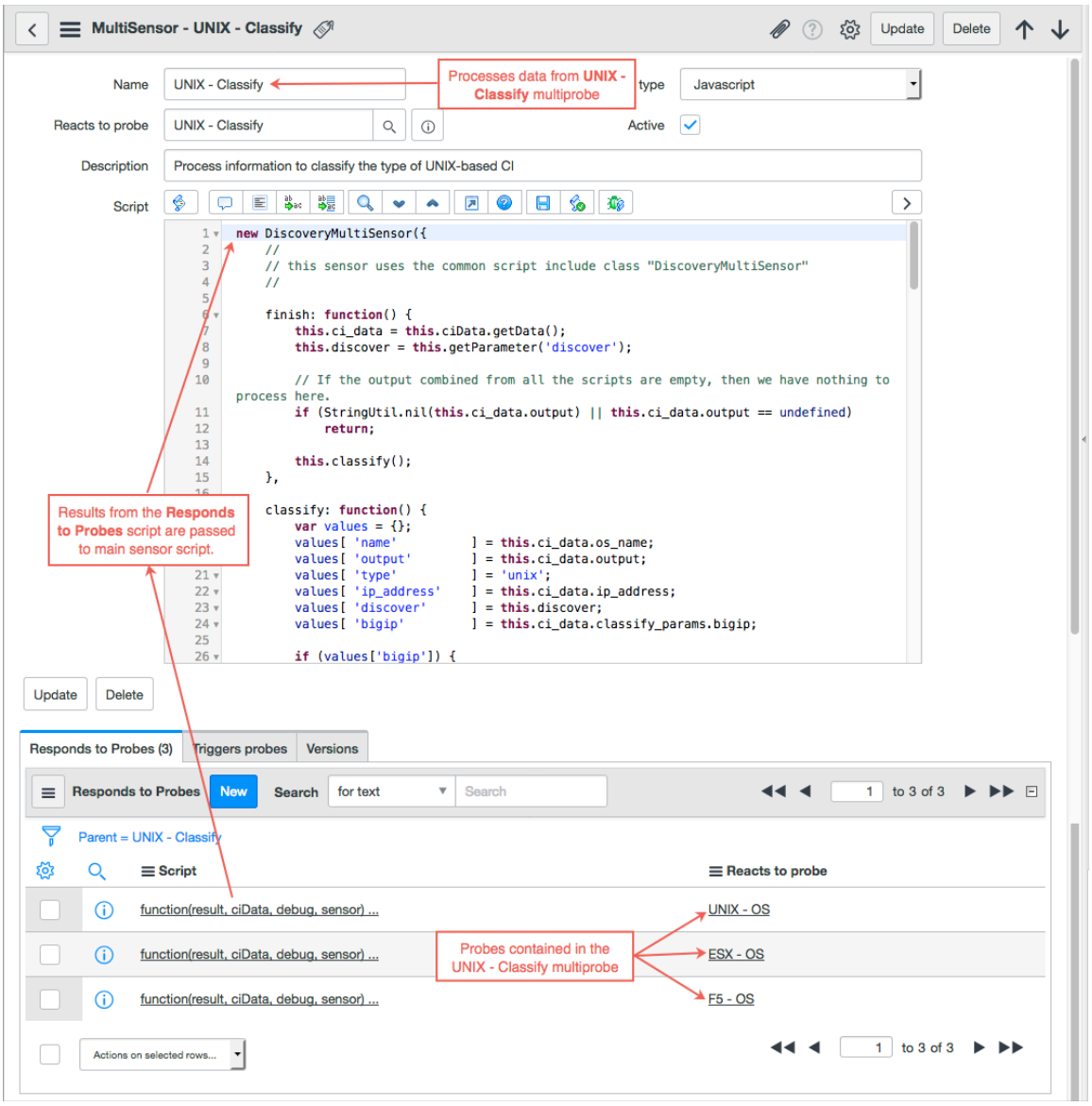
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem ein Eintrag in die Tabelle der ECC-Warteschlange eingefügt wurde, wird eine Geschäftsregel ausgelöst (beim Einfügen), die diese Informationen aufnimmt und sie durch einen *Sensorprozessor* verarbeiten lässt. Die Aufgabe des Sensorprozessors besteht darin, alle für diese eingegebenen Daten relevanten Sensoren zu ermitteln und zur Verarbeitung weiterzuleiten. Diese Sensoren aktualisieren letztlich die CMDB.

Funktionsweise der Zusammenarbeit von Probes und Sensoren

Der MID Server startet Probes, um Informationen über ein Gerät zu erfassen. Die Probe sendet die Informationen zur Verarbeitung an den Sensor zurück. Wenn für die Probe ein Nachverarbeitungsskript definiert ist, führt das Nachverarbeitungsskript einige Schritte zur Datenverarbeitung auf dem MID Server aus, bevor Daten an den Sensor in der ServiceNow-Instanz zurückgesendet werden. Andernfalls senden die Probes alle erfassten Daten zurück, und der Sensor erledigt die Datenverarbeitung. In beiden Fällen aktualisiert der Sensor die CMDB.

Eine Multi-Probe ist eine Probe, die mehrere Probes enthält. *Multisensoren* verarbeiten die Daten von Multi-Probes. Zur Verarbeitung der Daten von Multi-Probes enthalten Multisensoren einzelne Skripts, mit denen die Daten von jeder in einer Multi-Probe enthaltenen Probe verarbeitet werden, sowie ein Multisensor-Hauptskript. Die einzelnen Skripts übergeben die von ihnen verarbeiteten Daten an das Multisensor-Hauptskript.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe-Typen

Gerät	Probe-Typ
Windows Computer und Server	WMI-Remoteabfragen, Shell-Befehle
UNIX- und Linux-Server	Shell-Befehl (über SSH-Protokoll, Version 2). Discovery unterstützt alle Bourne-kompatiblen Shells.
Speicher	CIM-/WBEM-Abfragen
Drucker	SNMP-Abfragen
Netzwerkgeräte (Switches, Router usw.)	SNMP-Abfragen
Webserver	HTTP-Headerprüfung
Unterbrechungsfreie Stromversorgungen (USV)	SNMP-Abfragen

Liste der Discovery-Probes

Für Discovery ist eine Vielzahl von Probes zur Erkennung von Elementen in Ihrem Netzwerk verfügbar.

Die folgenden Probes sind in Discovery enthalten.

Die Bezeichnung des *PPP-Skripts* in der Tabelle gibt an, ob eine Probe ein PPP-Skript (Probe Post-Processing) enthält, das auf dem MID Server ausgeführt wird. Das PPP-Skript wandelt Probe-Ergebnisse in eine JSON-Zeichenfolge um und gibt die Zeichenfolge zur Sensorverarbeitung an die ServiceNow-Instanz zurück.

Um Probes und ihre Beschreibungen anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Probes**an.

Die CIM-Probe

Die CIM-Probe verwendet WBEM-Protokolle, um einen bestimmten CIM-Server, den CIM Object Manager, nach einer Reihe von Datenobjekten und Eigenschaften abzufragen.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die CIM-Probe übergeben werden:

CIM-Test

Parameter	Beschreibung	Standardwert
Quelle	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll	Keine
port	Der Port, zu dem eine Verbindung hergestellt werden soll. Wenn der Wert leer ist, wird er durch den Parameter „schema“ bestimmt: http = 5988, https = 5989.	5988 oder 5989

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIM-Test (Fortsetzung)

Parameter	Beschreibung	Standardwert
schema	[Erforderlich] Das zu verwendende Schema: „http“ oder „https“.	http
namespace	[Erforderlich] Der CIM-Namespace. Kann durch eine Abfrage überschrieben werden.	Keine
queries	[Erforderlich] Eine durch Semikolon getrennte Liste von Abfragen der CIM-Probe, für die Ergebnisse verarbeitet und zurückgegeben werden sollen	Keine
Wiederholungen	Die Anzahl der Wiederholungsversuche, wenn eine Abfrage aufgrund von Problemen mit der Netzwerkverbindung fehlschlägt	2
connection_timeout	Die Anzahl von Millisekunden, die eine Probe zum Herstellen einer Verbindung mit einem Server benötigt	5000
socket_timeout	Die Anzahl von Millisekunden, die eine Probe Daten lesen muss	5000

In CIM Intermediate Query Language (CimIQL) werden Schlüssel, Filter und Dot-Walking verwendet, um CIM-Schemen zu durchlaufen.

Parametererweiterung

Die Abfragesprache CIM unterstützt die mit Standard-SNC vorverarbeitete Erweiterung von Probe-Parametern. Platzieren Sie Variablen in Abfragen, indem Sie wie folgt ihren Namen einkapseln:

```
${foobar}.CIM_RunningOS[0].Name
CIM_ComputerSystem.${barfoo}
```

Der Text ${foobar} wird durch den Inhalt des an die CIM-Probe übergebenen Probe-Parameters foobar ersetzt. Dasselbe gilt für barfoo.

CIMIQL

CimIQL (CIM Intermediate Query Language) ist eine Zwischensprache, die darauf ausgelegt ist, den Prozess der Abfrage von CIM-Providern zu vereinfachen.

CimIQL unterstützt derzeit den standardmäßigen WBEM-Protokollstapel (Web-Based Enterprise Management). In Zukunft können jedoch weitere wie Web Services-Management (WS-MAN) hinzugefügt werden. Die Syntax der Abfragesprache leiht sich Elemente der Abfragesprache WMI von Microsoft und des wbemcli-Befehls von UNIX. Die Bibliothek CimIQL ist eine reine Java-Implementierung.

Hinweis: CimIQL wird „simicle“ ausgesprochen.

CimIQL-Syntax

Die CimIQL-Syntax umfasst zahlreiche Elemente, darunter eine Abfrage und verschiedene Token.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibungen der Elemente der CimIQL-Syntax

Element	Beschreibung
Erklärung	Das grundlegendste Element von CimIQL ist gültig . Anweisungen enthalten mehrere durch einen Punkt (.) getrennte Abfragen.
Abfrage	A Stellt eine einzelne protokollunabhängige Anforderung auf allgemeiner Ebene dar. Jede Abfrage besteht aus verschachtelten Sprachkomponenten und Unterkomponenten, die als Token bezeichnet werden.
Token	A Beschreibt einen bestimmten lexikalischen Aspekt der CimIQL-Syntax.
Vorgangstoken	Das erste Token jeder Abfrage muss ein sein , Der den gesamten auszuführenden logischen Vorgang darstellt.
Komponententoken	A Ist eine Unterkomponente eines Vorgangs-Tokens.
Ergebnis	Jede Abfrage wird mit einem Ergebnis kombiniert, das dann als Eingabe für die nächste Abfrage in der Anweisung bereitgestellt wird. A Besteht aus einer Reihe von Objekten und ihren Eigenschaften.

CimIQL-Vorgangstoken

Die CimIQL-Probe erfordert Vorgangstoken.

Jeder der folgenden Kernvorgänge besitzt ein entsprechendes Gegenstück im Standard CIM Operations over HTTP .

CimIQL-Vorgangstoken – Übersicht

Rückgabewert	Details	Äquivalent CIM Operation over HTTP
Klassenobjekt	Get Object Ruft ein einzelnes Objekt einer bestimmten Klasse ab, indem alle eindeutigen Schlüssel (als Schlüsseltoken) und alle optionalen Parametertoken getrennt durch Kommata angegeben werden	GetInstance
Klassenobjekt	Enumerate Objects Ruft Objekte ab, die mit einem Satz von Bedingungstoken und Parametertoken übereinstimmen	EnumerateInstances
Klassenobjekt	Enumerate Associated Objects Ruft Objekte ab, die den einzelnen Ergebnissen der vorherigen Abfrage zugeordnet sind	Assoziationen
Anweisungsergebnisse	Substitution Ein no-op-Token, das die Ergebnisse einer zuvor benannten Anweisung als Eingabe für die nächste Abfrage der eigenen Anweisung verwendet	Referenz auf Ergebnisse einer benannten Anweisung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Token „Get Object“

<Klassenname>{<Schlüsseltoken>,<Parametertoken>,...}

- Ruft ein einzelnes Objekt einer bestimmten Klasse ab, indem alle seine eindeutigen Schlüssel (als Schlüsseltoken) angegeben werden Schlüssel-Token) Und alle optionalen Parameter-Token , Durch Kommas getrennt. Dieses Token wird auch als bezeichnet .
- <Klassenname> entspricht dem CIM-Klassennamen (Groß-/Kleinschreibung beachten) des gewünschten Objekts. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.
- Schlüssel- und Parametertoken sind von einem Paar geschweiften Klammern { ... } eingeschlossen.
- Dieses Token darf nur als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runtime'}.*
```

Token „Enumerate Objects“

<Klassenname>{{<Bedingungstoken>,<Parametertoken>,...}}<Array-Index-Token> ODER <Klassenname><Array-Index-Token>

- Ruft Objekte ab, die mit einem Satz von Bedingungstoken und Parametertoken übereinstimmen Dieses Token wird auch als bezeichnet .
- Bedingungstoken und Parametertoken sind von zwei Paar geschweiften Klammern {{ ... }} eingeschlossen. Die geschweiften Klammern sind optional, wenn keine Bedingungen oder Parameter erforderlich sind.
- <Klassenname> entspricht dem CIM-Klassennamen (Groß-/Kleinschreibung beachten) der gewünschten Objekte. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.
- Das Indextoken ist optional.
- Dieses Token darf nur als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{{Name!='runtime'}}.*
```

Token „Enumerate Associated Objects“

<Name der Assoziationsklasse>{{<Eigenschaftenfiltertoken>,<Parametertoken>,...}}<Array-Index-Token> ODER <Name der Assoziationsklasse><Array-Index-Token>

- Ruft Objekte ab, die den einzelnen Ergebnissen der vorherigen Abfrage zugeordnet sind
- Bedingungstoken und Parametertoken sind von zwei Paar geschweiften Klammern {{ ... }} eingeschlossen. Die geschweiften Klammern sind optional, wenn keine Eigenschaftenfilter oder Parameter erforderlich sind.
- Der <Name der Assoziationsklasse> ist der Name der M:N- oder 1:N-Klasse, die zwei Objekte miteinander verknüpft. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das <Parametertoken> ResultClass kann angegeben werden, um Ergebnisse basierend auf dem Klassennamen des resultierenden Objekts zu filtern.
- Das Indextoken ist optional.
- Dieses Token darf nicht als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{{Name='runtime'}}[2].*
```

Substitutionstoken

${<Anweisungsname>}

- Ein no-op-Token, das die Ergebnisse einer zuvor benannten Anweisung als Eingabe für die nächste Abfrage der eigenen Anweisung verwendet
- Rückgabe: keine
- Beispiel:

```
$(lastComputer).ElementName
```

CimIQL-Komponententoken

Die CimIQL-Probe erfordert Komponententoken, die Unterkomponenten von operativen Token sind.

Die folgenden Token sind Unterkomponenten von Vorgangstoken.

CimIQL-Komponententoken – Übersicht

Token	Details
Eigenschaften-Token	* ODER <Eigenschaftsname>,<Eigenschaftsname>,... Gibt an, welche Eigenschaften für jedes Objekt des endgültigen Ergebnissatzes zurückgegeben werden müssen
Abfragetrennzeichen-Token	an. (Punkt) Trennt Abfragen
Index-Token	[Index] Verringert die Ergebnisse einer vorhergehenden Abfrage auf ein einzelnes Objekt am angegebenen Ganzzahlindex
Schlüssel-Token	<Schlüsselname>='<Wert>' Gleicht eine Objekteigenschaft, die als Schlüssel festgelegt ist, mit einem genauen Wert ab
Bedingungstoken	<Eigenschaftsname><Bedingungsoperator><eingeschlossener Wert> Gleicht eine einzelne Eigenschaft eines Objekts basierend auf der angegebenen Bedingung ab
Parameter-Token	<Parametername>:'<Wert>'

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Komponententoken – Übersicht (Fortsetzung)

Token	Details
	Übergibt einen Parameter nach <Parametername> an den aufgerufenen Vorgang. Der Parameter kann je nach Parameter während der CimIQL-Vorverarbeitung oder vom CIMOM auf Anforderung verwendet werden.

Eigenschaftstoken

* ODER <Eigenschaftsname>,<Eigenschaftsname>,...

- Gibt an, welche Eigenschaften für jedes Objekt des endgültigen Ergebnissatzes zurückgegeben werden müssen
- Mit dem Platzhalter * werden alle verfügbaren Eigenschaften zurückgegeben. Andernfalls wird jeder gewünschte Eigenschaftsname in einer kommagetrennten Liste bereitgestellt.
- Dieses Token ist am Ende jeder Anweisung erforderlich.
- Beispiel:

```
CIM_ComputerSystem[0].*
```

Abfragebegrenzertoken

an. (Punkt)

- Trennt Abfragen
- Beispiel:

```
CIM_ComputerSystem.PrimaryOwnerContact
```

Indextoken

[Index]

- Verringert die Ergebnisse einer vorhergehenden Abfrage auf ein einzelnes Objekt am angegebenen Ganzzahlindex
- Dieses Token ist immer optional.
- Beispiel:

```
CIM_ComputerSystem[0].*
```

Schlüsseltoken

<Schlüsselname>='<Wert>'

- Gleicht eine Objekteigenschaft, die als Schlüssel festgelegt ist, mit einem genauen Wert ab
- <Schlüsseltoken> entspricht dem Namen der als Schlüssel verwendeten Eigenschaft.
- Beispiel:

```
CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runtime'}.*
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungstoken

<Eigenschaftsname><Bedingungsoperator><eingeschlossener Wert>

- Gleicht eine einzelne Eigenschaft eines Objekts basierend auf der angegebenen Bedingung ab
- <Eigenschaftsname> entspricht dem Namen der Eigenschaft für den Abgleich.
- Der <Bedingungsoperator> legt fest, wie der tatsächliche Wert einer Eigenschaft mit dem erwarteten Wert verglichen wird. Die verfügbaren Operatoren sind *gleich* (=) und *ungleich* (!=).
- Der <eingeschlossene Wert> muss einer der folgenden Möglichkeiten entsprechen:
  - Literaler Wert, in einfachen Anführungszeichen '...' Beispiel: foo='bar'
  - Regulärer Ausdruck, zwischen Schrägstrichen /.../ Beispiel: foo=/bar.*/
- Beispiel:

```
CIM_ComputerSystem{{Name!='runtime'}}.*
```

Parametertoken

<Parametername>:'<Wert>'

- Übergibt einen Parameter nach <Parametername> an den aufgerufenen Vorgang. Der Parameter kann je nach Parameter während der CimIQL-Vorverarbeitung oder vom CIMOM (Common Information Model Object Manager) auf Anforderung verwendet werden.
- Beispiel:

```
CIM_ComputerSystem.CIM_RunningOS{{ResultClass:'Win32_ComputerSystem'}}.*
```

CimIQL-Tutorial

Dies ist ein Tutorial anhand von Beispielen, bei dem jedes Beispiel auf dem vorherigen Beispiel aufbaut.

CimIQL-Tutorial

Reihenfolge	CimIQL-Anweisung	Ergebnis
1	CIM_ComputerSystem[0].*	Ruft das erste Ergebni aller Instanzen von CIM_ComputerSysten und dessen untergeord Elemente ab. Ruft alle Eigenschaften ab
2	CIM_ComputerSystem.PrimaryOwnerContact	Ruft alle Instanzen vo CIM_ComputerSysten und deren untergeordn Elemente ab. Ruft nur eine Eigenschaft ab: PrimaryOwnerContact
3	CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runtime'}.*	Ruft eine einzelne eindeutige Instanz vo CIM_ComputerSysten und deren untergeordn

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Tutorial (Fortsetzung)

Reihenfolge	CimIQL-Anweisung	Ergebnis
		Elemente ab. Alle Schlüsseltoken müsse Identitätstoken angege werden.
4	CIM_ComputerSystem{{Name!='runtime'}}.*	Ruft alle Instanzen und untergeordnet Elemente von CIM_ComputerSys ab, die nicht die Name-Eigenschaft „runtime" aufweise Das Filtertoken {{ }} filtert Instanzen heraus, die nicht a der angegebenen Eigenschaften/Sch enthalten.
5	CIM_ComputerSystem{{Name=/^run.*$/}}.*	Ruft alle Instanzen und untergeordnet Elemente von CIM_ComputerSys ab, deren Wert dem regulären Ausdruck zwische den Schrägstriche entspricht. **Hinweis:** Der reguläre Ausdruck erforde keine einfachen Anführungszeich Das Filtertoken {{ }} filtert Instanzen heraus, die nicht a der angegebenen Eigenschaften/Sch enthalten.
6	CIM_ComputerSystem{{Name='runtime'}}[2].*	Ruft das zweite Erg aller Instanzen vor CIM_ComputerSys und dessen untergeordnete Elemente ab, wobei Instanzen die Nam

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Tutorial (Fortsetzung)

Reihenfolge	CimIQL-Anweisung	Ergebnis
		Eigenschaft „runti aufweisen. Die Reihenfolge de Vorgänge entspric der Abfragesyntax **1.** Server auf alle CIM_ComputerS und untergeordr Elemente abfrage **2.** Ergebnisse basie auf der Name-Eigenschaft filter **3.** Zweite Instanz abfra die den Filter durchlaufen hat
7	CIM_ComputerSystem.CIM_RunningOS[0].Name	Ruft die Eigenscha Name für die erste CIM_OperatingSys Instanz jeder CIM_ComputerSys Instanz ab. Das mittlere Token CIM_RunningOS, ist der Name der Assoziationsklasse, ni das Endergebnis.
8	CIM_ComputerSystem.CIM_RunningOS{{Name=/CentOS/}}[0].Name	Ruft die Eigenschaft Name für die erste CIM_OperatingSystem Instanz von jeder CIM_ComputerSystem Instanz ab, wobei alle CIM_OperatingSystem Instanzen eine Name-Eigenschaft haben, die „CentOS“ enthält.

CimIQL-Ergebnisse

Ergebnisse der CIM-Probe werden als XML-Dokument eingebettet im <output>-Element an den Probe-Sensor übergeben.

Im Folgenden finden Sie ein kommentiertes Beispiel für ein CimQuery-Batch-Ergebnis.

```
<!-- document root -->
 <cimqueryset>
 <!-- A single query and query result. Multiple <cimquery> tags may be provided. -->
 <cimquery>
```

Autorisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  <!-- The original query, enclosed by CDATA. -->
  <query><!CDATA[[>CIM_ComputerSystem[0].PrimaryOwnerContact<! ]]></query>
  <!-- The resulting data is enclosed within a single <result> tag. -->
  <result>
   <!-- A single class instance result. Multiple <instance> tags may be provided.
      Special tags are prefixed with an underscore character. -->
   <instance>
    <!-- The instance's CIM classname -->
    <_classname>Linux_ComputerSystem</_classname>
    <!-- A set of this instances identifying keys. Always provided, regardless of property filters.
       Within here, each key is provided as <KeyName>VALUE</KeyName> with the VALUE
enclosed as CDATA. -->
    <_key>
     <CreationClassName><![CDATA[Linux_ComputerSystem]]></CreationClassName>
     <Name><![CDATA[runtime]]></Name>
    </_key>
    <!-- Each property that matches the query's property filter will be provided here, in the
same format as keys;
       As <PropertyName>VALUE<PropertyName> where VALUE is enclosed as CDATA -->
    <PrimaryOwnerContact><![CDATA[root@runtime]]></PrimaryOwnerContact>
   </instance>
  </result>
</cimquery>
</cimqueryset>
```

DNS probe

DNS-Probes bestimmen die DNS-Namen für Konfigurationselemente (CI).

Die standardmäßige Probe „DNS Name Resolver“ ist eine ressourcenschonende und schnelle Probe. Er erreicht seine Geschwindigkeit dadurch, dass er parallel auf dem MID Server ausgeführt wird. Die Probe nutzt eine DNS-Suche des MID Server-Host-BS, um den verwalteten DNS-Cache zu verwenden. Die Probe verwendet auch die Datei „hosts“ des Betriebssystems.

Diese Leistungsverbesserungen können deaktiviert werden, indem die veraltete DNS-Probe entweder mit MID Server-Eigenschaften oder -Parametern wiederhergestellt wird. Die Namen der MID Server-Eigenschaften/-Parameter lauten [mid.probe.use_veralteter_forward_dns] und [mid.probe.use_legacy_reverse_dns]. Weitere Informationen finden Sie unter MID-Server-Parameter Und MID-Server-Eigenschaften .

Definitionen von DNS-Probes

Probe	Beschreibung
DNS	Bestimmt DNS-Namen von Geräten. Besitzt den Parameter ip_addresses
DNSLookupProbe	Löst die IP-Adresse eines Hosts auf
DNSNameResolver	Löst den DNS-Namen einer IP-Adresse auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Port-Sonden

Probe	Beschreibung
dns	Ausgelöst durch „dns“. Verwendet den Scanner „DNS Name Resolver“ und die Klassifizierung „Prozessklassifizierung“ [discovery_classy_proc]

Probe „Horizontal Pattern“

Von Discovery wird die Probe für horizontale Muster dafür verwendet, Muster für die horizontale Erkennung zu starten.

Die Probe „Horizontal Pattern“ arbeitet mit dem Sensor „Horizontal Discovery“, damit Discovery Muster für die Erkennung verwenden kann. Wenn Nachrichten von dieser Probe in der ECC-Warteschlange angezeigt werden, werden sie mit dem Namen der ECC-Warteschlange `Pattern Launcher` gefolgt vom Namen des Musters angezeigt. Die Probe enthält den Sensor `Horizontal Discovery Sensor`, der die tatsächlichen Aktualisierungen der CMDB basierend auf Identifizierungsregeln durchführt.

Wenn Sie Ihren eigenen Geräte- oder Prozessklassifizierer erstellen und Muster für die Erkennung verwenden möchten, müssen Sie diese Probe im Klassifiziererdatensatz angeben. Sie müssen diese Probe oder den Sensor „Horizontal Discovery“ nicht ändern.

Nutzlast aufteilen

Wenn Discovery Muster verwendet, um bestimmte Geräte wie Lastenausgleichsmodule zu finden, können große Datenmengen an die ECC-Warteschlange gesendet werden. Um große Datenmengen besser verarbeiten zu können, kann die Probe „Horizontal Pattern“ die Nutzlast in Blöcke aufteilen und dann mehrere ECC-Warteschlangen-Datensätze erstellen.

Steuern Sie mithilfe von Eigenschaften, wie der MID Server Nutzlasten aufteilt und verarbeitet. Siehe MID-Server-Eigenschaften Weitere Informationen finden Sie unter .

PowerShell-Probe

Die PowerShell-Probe führt PowerShell V2-Skripts auf dem MID Server-Host aus.

PowerShell-Skripts sind als Probe-Parameter mit dem Dateinamen als Parameternamen definiert. Es ist als Probe-Typ „Probe“ verfügbar, indem „PowerShell“ als ECC-Warteschlangenthema der Probe angegeben wird.

PowerShell-Probe-Parameter

Parametername	Beschreibung
Quelle	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll **Standardwert:** Keine
<script name>.ps1	[Erforderlich] Der Dateiname des auszuführenden PowerShell-Skripts. Ersetzen Sie `<script name>` durch ein gültiges Dateinamenpräfix. **Standardwert:** Keine
powershell_command_parameter_passing	Gibt an, ob Skriptparameter in der Befehlszeile übergeben werden sollen. Unabhängig vom

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Beschreibung
	Wert dieses Parameters macht ServiceNow alle Skriptparameter in der Befehlszeile automatisch für PowerShell-Skripts als Umgebungsvariablen verfügbar. **Standardwert:** false
powershell_param_<script parameter name>	Übergibt zusätzliche Parameter an das auszuführende PowerShell-Skript. Jeder Parameter wird dem Skript als Umgebungsvariable im Format *$env:SNC_<script parameter name>* angezeigt. Parameter mit diesem Präfix gelten nicht als verschlüsselt und werden unverändert an das Skript übergeben. Stellen Sie sicher, dass Sie den entsprechenden Parameter zwischen *powershell_param_<script parameter name>* und *powershell_<script parameter name>* auswählen. Die Verwendung des falschen Präfix führt zu Fehlern in der PowerShell-Ausführung, die an die Instanz in der ECC-Warteschlangeneingabe zurückgegeben werden. **Standardwert:** Keine
powershell_<script parameter name>	Übergibt zusätzliche Parameter an das auszuführende PowerShell-Skript. Jeder Parameter wird dem Skript als Umgebungsvariable im Format *$env:SNC_<script parameter name>* angezeigt. Der MID Server geht davon aus, dass alle Parameter mit diesem Präfix verschlüsselt sind, und versucht, sie zu entschlüsseln. Stellen Sie sicher, dass Sie den entsprechenden Parameter zwischen *powershell_param_<script parameter name>* und *powershell_<script parameter name>* auswählen. Die Verwendung des falschen Präfix führt zu Fehlern in der PowerShell-Ausführung, die an die Instanz in der ECC-Warteschlangeneingabe zurückgegeben werden. **Standardwert:** Keine
debug	Aktiviert die Debug-Protokollausgabe während der Ausführung der Probe. **Standardwert:** false
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange ausgegeben, auch wenn die Anmeldeinformationen erfolgreich sind. **Standardwert:** false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skripting-Anforderungen

Alle benutzerdefinierten PowerShell-Skripts müssen Umgebungsvariablen verwenden, um nichtboolesche Befehlszeilenparameter zu übergeben. Ersetzen Sie nichtboolesche Parameter im Abschnitt `Param()` des Skripts durch Skriptvariablen mit demselben Namen. Definieren Sie die Skriptvariable als Teil der Umgebung mit einem SNC_-Präfix. Dadurch wird ein Zeichenfolgenparameter wie der folgende:

```
Param([string]$paramName)
```

zu einer Skriptvariablen wie der folgenden:

```
if(test-path env:\SNC_paramName) {
   $paramName = $env:SNC_paramName
}
```

Beispielsweise enthält diese Parameterdefinition aus dem Skript PSScript.ps1 mehrere Zeichenfolgenparameter, die als Skriptvariablen neu definiert werden müssen:

```
Param([string]$computer, [string]$script, [string]$user, [string]$password, [boolean]$useCred,
 [boolean]$isDiscovery, [boolean]$debug)
```

Das Definieren der nichtbooleschen Parameter als Skriptvariablen führt zu folgendem Skripttyp:

```
Param([boolean]$useCred, [boolean]$isDiscovery, [boolean]$debug)

# Copy the environment variables to the params
if(test-path env:\SNC_computer) {
  $computer=$env:SNC_computer
}

if(test-path env:\SNC_script) {
  $script=$env:SNC_script
}

if(test-path env:\SNC_user) {
  $user=$env:SNC_user
  $password=$env:SNC_password
}
```

Benutzerdefinierte PowerShell-Probe erstellen

Sie können Ihre eigene PowerShell-Probe erstellen und Probe-Parameter konfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**an.
2. Klicken Sie auf **Neu**.
3. Tragen Sie die folgenden Werte ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Name**: Beliebiger eindeutiger Name
- **Probe**-Typ: Probe
- **ecc_queue_topic**: Powershell

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.
5. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf **Neu**.
6. Erstellen Sie einen Probe-Parameterdatensatz für jeden Parameter.
7. Klicken Sie auf **Absenden**.

Probe „SCPRelay“

Die *Probe „SCP Relay“* kopiert eine einzelne Datei oder den Inhalt eines Verzeichnisses von einem Host auf einen anderen und verwendet dabei den MID-Server als Relay.

Die Probe „SCP Relay“ verwendet dieselben Parameter wie die Probe „SSHCommand“. Die Befehle können innerhalb bzw. außerhalb des Kontexts eines Terminals (tty) und mit bzw. ohne sudo gesendet werden (für Befehle wie lsof, die im Kontext von root ausgeführt werden müssen, um die benötigten Informationen auszugeben). Wenn Befehle im Kontext eines Terminals gesendet werden, wird der Pfad automatisch erweitert, um eine Reihe von Standardpfaden einzubeziehen (dafür kann der Parameter path_override verwendet werden). Wenn der Zielcomputer der lokale Computer ist, wird SSH nicht verwendet. Stattdessen wird eine lokale Shell ausgeführt, um den Befehl auszuführen.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die *Probe „SCP Relay“* übergeben werden:

Parameter

Parameter	Beschreibung	Standardwert
debug	Aktiviert die Debug-Protokollierung	false
debug_ssh	Aktiviert die J2SSH-Debug-Protokollierung **agent.log** **Hinweis:** Diese Protokolldatei kann schnell größer werden und sollte deaktiviert werden, wenn sie nicht benötigt wird.	false
timeout	Legt den Verbindungstimeout für Socket-Verbindungen in ms fest	60000
path_override	Überschreibt die Standardpfade, die vor der Ausführung eines Befehls festgelegt wurden.	keine
keyboard_interactive	Bei „true“ wird die Verwendung des SSH-Anmeldemodus „keyboard_interactive“ erzwungen.	false
must_sudo	Bei „true“ wird die Ausführung des Befehls über sudo erzwungen.	false
run_in_terminal	Bei „false“ wird die Ausführung von SSH-Befehlen in einem SSH-Terminal deaktiviert (viele Befehle werden dadurch unwirksam).	Wahr
long_runner	Falls vorhanden, wird dadurch ein SSH-Befehl mit langer Ausführungszeit angegeben.	false
set_path	Bei „false“ wird die Festlegung der Umgebungsvariablen für den Pfad vor der Ausführung des Befehls deaktiviert.	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter (Fortsetzung)

Parameter	Beschreibung	Standardwert
rm_override	Falls vorhanden, wird der standardmäßige rm-Befehl ("/sbin/rm -f") mit dem angegebenen Wert überschrieben.	keine
Quelle	Host oder IP als Quelle des Kopiervogangs	erforderlich
source_port	SSH-Port der Quelle (standardmäßig 22)	erforderlich
from_file	Name der Datei, die aus der Quelle kopiert werden soll	erforderlich
target	Host oder IP als Ziel des Kopiervogangs	erforderlich
target_port	SSH-Port des Ziels (standardmäßig 22)	erforderlich
to_file	Name der Datei, die auf das Ziel kopiert werden soll	erforderlich

SNMP-Probes

SNMP-Probes verwenden das SNMP-Protokoll, um ein bestimmtes Gerät nach einer Liste von OIDs abzufragen, die dann durchlaufen und deren Ergebnisse an die Sensoren zurückgegeben werden. MID Servers bieten standardmäßig Unterstützung für alle SNMP-Protokollversionen. Sie können einen MID-Server so einstellen, dass er nur bestimmte Versionen von SNMP unterstützt.

Discovery bietet Unterstützung für die SNMP-Versionen 1, 2c und 3. Der Standardwert ist ALLE. Wenn Sie eine der Versionen auswählen, aber nicht über die Anmeldeinformationen dieser Version verfügen, wird die Option „SNMP-Version verwenden“ auf ALLE zurückgesetzt.

Hinweis: Anmeldeinformationen für die SNMP-Version müssen „active=true“ sein. Wenn eine bestimmte Version inaktiv ist, wird die Einstellung ebenfalls auf ALLE zurückgesetzt. Es wird eine Nachricht ähnlich der folgenden angezeigt: --- In dieser Instanz sind keine SNMP-Anmeldeinformationen vom Typ „snmpv3“ aktiv. „SNMP-Version verwenden“ zurück auf „Alle“ setzen.

SNMP-Muster

Das Muster „Network Router“ ersetzt die verschiedenen SNMP-bezogenen Probes zur Erkennung von Routern und Switches. Siehe Verfügbare Discovery-Muster Für eine Liste von Mustern.

SNMP-Probe-Parameter

Dies ist die Liste der Parameter, die an SNMP-Probes übergeben werden kann.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Parameter	Beschreibung	Standardwert
oid_spec_list	Eine Liste mit OID-Spezifikationen, eine pro Zeile. Jede Spezifikation muss eines der folgenden beiden Formate aufweisen:	erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	• *walk {OID}*: Durchläuft die OID und alle untergeordneten Elemente • *table {OID} {OID Children}*: Durchläuft alle Einträge in der Tabelle und gibt nur die angegebenen untergeordneten Elemente zurück (zum Beispiel „iso.org.dod.internet“) {OID Child} bezieht sich auf eine kommagetrennte Liste von untergeordneten Knoten in den Einträgen für die angegebene Tabelle. Beispiel: „ifEntry.ifIndex,ifEntry.ifDescr,ifEntry.ifType“ sind untergeordnete OID-Elemente der Tabelle „iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable“. Der Einfachheit halber kann das Präfix des Tabelleneintrags weggelassen werden. (Die vorherigen untergeordneten Elemente können als „ifIndex,ifDescr,ifType“ angegeben werden.) Alle untergeordneten Elemente können einen Filterqualifizierer in Klammern einschließen. Beispiel: Das untergeordnete Element „entPhysicalContainedIn(=0)“ gibt zurückgegebene Tabelleneinträge nur an, wenn der Wert von „entPhysicalContainedIn“ gleich 0 ist. Die im Ausdruck unterstützten Operatoren lauten wie folgt: • `=` : Ist gleich • `!=` : Ist nicht gleich • `#` : Enthält Wenn mehrere untergeordnete Elemente über einen Filterausdruck verfügen, wird der Eintrag bei einer Übereinstimmung mit einem der untergeordneten Elemente gelesen. Alle Inhalte einschließlich und hinter „//“ werden ignoriert (Kommentare). Alle OIDs, die nicht mit „1.3.6.1“ oder „iso.org.dod.internet“ beginnen, beginnen der Einfachheit halber automatisch mit „1.3.6.1“.	
Quelle	IP-Adresse oder Hostname des Geräts, auf dem SNMP abgefragt werden soll	erforderlich
index	Der nach der Community-Zeichenfolge anzuwendende Index zur Indizierung der Community-Zeichenfolge im Cisco-Stil (für VLAN-Abfrage)	0
credential_id	Die sys_id einer bestimmten Anmeldeinformation, die bevorzugt zu verwenden ist. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	keine
credential_tag	Das Anmeldeinformations-Tag, das verwendet werden muss. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	keine
timeout	Zeitüberschreitungswert (in Millisekunden) für die Wartezeit auf eine Antwort anstelle des Standardwerts.	1500

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	Sie können diesen Parameter verwenden, um den Konfigurationsparameter *mid.snmp.request.timeout* des SNMP-MID Servers zu überschreiben. **Hinweis:** Wenn *use_getbulk* auf *true* festgelegt ist, gilt der Zeitüberschreitungswert für eine einzelne GETBULK-Anforderung.	
established_session_timeout	Intervall (in Millisekunden), über das auf eine Antwort gewartet wird, nachdem mindestens eine Antwort empfangen wurde. Längere Werte können zur Erfassung vollständiger und genauer Daten nützlich sein. Sie können diesen Parameter verwenden, um den Konfigurationsparameter *mid.snmp.session.timeout* des SNMP-MID Servers zu überschreiben.	500
debug	Aktiviert die Debug-Protokollierung Legen Sie diesen Parameter für den Debug-Modus auf „true“ fest.	false
request_interval	Intervall (in Millisekunden) zwischen aufeinanderfolgenden Anforderungen für eine OID, wenn keine Antwort empfangen wurde, bis der Zeitüberschreitungswert (oder established_session_timeout) erreicht wird. Wenn dieser Wert mindestens auf den Wert für die Zeitüberschreitung (oder established_session_timeout) festgelegt ist, wird nur eine einzelne Anforderung für eine bestimmte OID gesendet. Wenn Sie den Wert für die Zeitüberschreitung (oder established_session_timeout) ändern, passen Sie request_interval gleichzeitig an, um zu vermeiden, dass zu viele oder zu wenige Anforderungen für dieselbe OID gesendet werden, je nachdem, was für eine bestimmte Umgebung angemessen ist.	400
request_delay	Intervall (in Millisekunden) zwischen dem Empfang einer Antwort und der Übertragung der nächsten Anforderung. Der Standardwert ist 0 (keine Verzögerung). Dieser Wert kann festgelegt werden, um die Gesamtrate einer SNMP-Abfrage zu verlangsamen.	0
result_format	Gibt JSON-formatierte Nutzlasten für die folgenden Probes zurück: • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System • SNMP - Routing Dieser Parameter gibt Daten in einem kompakteren Format zurück, um Sensorausfälle oder Speicherprobleme auf einem Knoten zu verhindern, wenn die Nutzlast groß wird. Ändern Sie diesen Wert nicht, und löschen Sie diesen Parameter nicht. **Warnung:** Die Verwendung dieses Parameters mit anderen Probes führt zum Ausfall des Sensors.	JSON
use_getbulk	Aktiviert die Verwendung von SNMP GETBULK-Anforderungen zum Abrufen von tabellarischen Daten von SNMP-Geräten, anstatt mehrere SNMP GETNEXT-Anforderungen zu verwenden. Für tabellarische Daten ist GETBULK effizienter. Unabhängig vom Anforderungstyp geben bestimmte Geräte möglicherweise keine Ergebnisse	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	zurück, wenn sie mit anderen Aufgaben beschäftigt sind. Dieser Parameter wird zur Konfiguration auf Probe-Ebene verwendet. GETBULK kann auch für einen einzelnen MID Server oder global für alle MID Server festgelegt werden. Einstellungen werden in ihrer Prioritätsfolge aufgelistet: • Parameter für SNMP-Probes • MID Server-Konfigurationsparameter • MID Server-Eigenschaften Die Parameter *established_session_timeout*, *request_interval*, und *request_delay* werden ignoriert, wenn *use_getbulk* auf **true** festgelegt ist. Stattdessen ist der Parameter *retries* verfügbar. Die Konfiguration der Zeitüberschreitung ist identisch mit *use_getscalar*. Standardmäßig verwenden die folgenden Probes GETBULK-Anforderungen (Parameterwert gleich *true*). • SNMP - Switch - Vlan • SNMP - Switch - BridgePortTable • SNMP - Switch - ForwardingTable • SNMP - Switch - SpanningTreeTable • SNMP - Network - ArpTable • SNMP - Layer 2 Protocol Caches • SNMP - F5 BIG IP - System (nur für Service Mapping-Kunden) **Hinweis:** Der *timeout*-Wert dieser Probes beträgt 5000.	
use_getscalar	Ermöglicht das vereinfachten Abrufen und Verarbeiten von skalaren Werten von SNMP-Geräten. Die Parameter *established_session_timeout*, *request_interval* und *request_delay* werden ignoriert, wenn *use_getscalar* auf **true** festgelegt ist. Stattdessen sind die Parameter *retries* und *timeout* verfügbar. Die Konfiguration der Zeitüberschreitung ist identisch mit *use_getbulk*.	false
Wiederholungen	Die Anzahl der zusätzlichen Versuche, die Discovery unternimmt, um eine einzelne GETBULK-Anforderung (siehe *use_getbulk*) oder eine GETNEXT-Anforderung abzuschließen, wenn der Parameter *use_getscalar* auf **true** festgelegt ist.	2

MIB-Modul laden

Sie können ein zusätzliches MIB-Modul (Management Information Base) laden, indem Sie einen neuen ecc_Agent_mib-Datensatz erstellen und die tatsächliche MIB-Datei an den Datensatz anhängen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
MIBs werden nur während des Starts von MID Servern geladen. Beim Hochfahren DES MID-Servers werden die folgenden MIB-Module geladen:

- Module, die mit der MID Server-Software gebündelt sind. Diese MIBs sind definierte Branchenstandards.
- Module, die in jeder Instanz enthalten sind. Diese MIBs werden vom Hersteller für Discovery bereitgestellt, um bestimmte Informationen von einem Gerät zu extrahieren.

Sie können alle Fehler im Zusammenhang mit dem Laden von MIB-Modulen im Agent-Protokoll anzeigen.

Hinweis: Durch das Hinzufügen einer MIB-Datei können Sie OID-Werte zusätzlich zur numerischen Schreibweise mit der Zeichenfolge/ASN-Schreibweise anfordern, es wird jedoch nicht garantiert, dass zusätzliche Informationen abgerufen werden. Es bietet einfach eine andere Möglichkeit, neue OIDs zu definieren, die Sie möglicherweise erkennen möchten.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **SNMP-MIBs**an.
2. Überprüfen Sie, ob Abhängigkeiten erfüllt sind.
   Wenn die neue MIB Abhängigkeiten von anderen MIBs aufweist, muss die MIB, die die Abhängigkeit füllt, vorhanden sein, bevor Sie den neuen Datensatz erstellen. Durchsuchen Sie die vorhandenen MIBs, um sicherzustellen, dass die erforderlichen MIBs bereits geladen sind. Ist dies nicht der Fall, führen Sie das folgende Verfahren aus, um sie der Instanz ebenfalls hinzuzufügen.
3. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
   Das Formular „MIB-Datei für MID Server“ wird geöffnet, um einen neuen ecc_agent_mib-Datensatz zu erstellen.
4. Verwenden Sie die folgenden Informationen, um das Formular auszufüllen:
   - **Name**: Name der MIB
   - **Version**: Version der MIB
   - **Quelle**: Geben Sie in diesem Feld an, wo die MIB abgerufen wurde, zum Beispiel eine URL.
   - **Beschreibung**: Die Beschreibung, die in der Tabelle ecc_agent_mib angezeigt wird
   - **Aktiv**: Dieses Kontrollkästchen gibt an, ob das MIB-Modul in der Instanz aktiviert oder deaktiviert ist.
5. Klicken Sie auf das Symbol „Anlage hinzufügen“ ( ) oben rechts, um die tatsächliche MIB-Datei an den neuen Datensatz anzuhängen.
   Der MIB-Name muss mit einem alphabetischen Zeichen beginnen. Die verbleibenden Zeichen müssen eines der folgenden sein: alphanumerisch, Bindestrich (-) oder Unterstrich (_). Der Dateiname darf keine Erweiterung aufweisen. Sie können die vorhandenen MIBs für Beispiele referenzieren. Verwenden Sie den tatsächlichen Namen der MIB sowohl für den Namen des MIB-Datensatzes als auch für den Namen des Anhangs. Dies ist jedoch nicht erforderlich.
6. Wählen Sie **Absenden**.

Nächste Maßnahme
Aktualisieren Sie das entsprechende Muster oder die Probe, um die spezifischen OID-Werte abzufragen, die in der neuen MIB definiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMP Probe MIB Module

Ein MIB-Modul (Management Information Base) ist eine Datenbank zur Verwaltung von Elementen in einem Netzwerk.

Ihre Instanz enthält Objektdefinitionen aus den gängigsten MIB-Dateien (Management Information Base). Prüfen Sie vor dem Hinzufügen einer neuen Objektdefinition die Liste der MIB-Module, um sicherzustellen, dass die Objektdefinitionen noch nicht verfügbar sind. Die Instanz enthält Objektdefinitionen aus den gängigsten MIB-Dateien (Management Information Base). Die Tabelle „MIB-Datei für MID Server“ [ecc_agent_mib] ist nach Domänen getrennt. Sie können Versionen dieser Richtlinien erstellen, die nur ein MID-Server aus derselben Domäne verwenden kann. Anweisungen finden Sie unter Richten Sie die Domänentrennung für MID-Server ein .

Die folgende Tabelle enthält die MIBs, die automatisch geladen werden. Die mit dem MID Server gebündelten MIBs sind in der Instanz nicht sichtbar. Die MIBs, die sich in der Tabelle „ecc_Agent_mib“ befinden, sind standardmäßig in der Instanz enthalten und können in angezeigt werden **MID-Server** > **SNMP-MIBs** Modul.

Wichtig: MIB-Dateien in einer ServiceNow-Instanz besitzen keine Dateierweiterung. Wenn die Systemeigenschaft **glide.attachment.extensions** in Ihrer Instanz eine Liste mit für den Import zulässigen Dateierweiterungen enthält, werden MIB-Dateien nicht geladen. Um sicherzustellen, dass MIB-Dateien geladen werden können, fügen Sie den Dateien vor dem Laden eine temporäre Erweiterung hinzu, zum Beispiel **.mib**, und listen Sie diese Erweiterung dann in der Eigenschaft **glide.attachment.extensions** auf. Wenn Sie die Datei laden, entfernt eine Geschäftsregel, die die **Compliance der MIB-Dateinamen** sicherstellt, diese Erweiterung aus der Datei, bevor sie den Datensatz in die Tabelle ecc_agent_mib einfügt.

MIB-Modul (Management Information Base)

Gebündelt mit dem MID Server	Enthalten in der Instanz
ATM-MIB	A10 AX MIB
BRIDGE-MIB	A10 COMMONS MIB
DISMAN-EVENT-MIB	CISCO-SMI
ENTITY-MIB	CISCO-STACK-MIB
EtherLike-MIB	CISCO-TC
FRAME-RELAY-DTE-MIB	CISCO-VTP-MIB
HOST-RESOURCES-MIB	F5-BIGIP-COMMON-MIB
HOST-RESOURCES-TYPES	F5-BIGIP-LOCAL-MIB
IANA-ADDRESS-FAMILY-NUMBERS-MIB	F5-BIGIP-SYSTEM-MIB
IANAifType-MIB	FOUNDRY-SN-AGENT-MIB
IP-MIB	FOUNDRY-SN-ROOT-MIB
IP-FORWARD-MIB	LanMgr-Mib-II-MIB
IPMROUTE-STD-MIB	MSFT-MIB
IPV6-MIB	NetWare-Host-Ext-MIB
ISDN-MIB	NetWare-Server-MIB
RFC-1212	PowerNet-MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MIB-Modul (Management Information Base) (Fortsetzung)

Gebündelt mit dem MID Server	Enthalten in der Instanz
RFC-1215	QMS-MIB
RFC1155-SMI	
RFC1213-MIB	
RFC1398-MIB	
RFC1406-MIB	
RMON2-MIB	
RSVP-MIB	
SNMPv2-SMI	
SNMPv2-TC	
UPS-MIB	

Probe „SSHCommand“

Eine Probe mit *SSHCommand* als Name für das ECC-Warteschlangenthema führt einen Shell-Befehl auf dem Zielhost aus und gibt die resultierende Ausgabe an den Sensor zurück.

Discovery unterstützt sh- und bash-Befehle (Bourne-Shell und Bourne-again-Shell). Geben Sie Shell-Skriptbefehle in das Feld *ECC-Warteschlangenname* der Probe ein. Das Shell-Skript kann Variablen und Dateivorgänge verwenden, die von der UNIX-Ziel-Shell unterstützt werden.

- Die SSH-Engine ist bei neuen Instanzen standardmäßig aktiviert.
- Kunden mit aktualisierten Instanzen können ServiceNow SSH für eine bestimmte Probe manuell aktivieren, indem sie den Parameter use_snc_ssh auf „true“ setzen. Alternativ können Sie SSH für alle Probes auf dem MID Server aktivieren, indem Sie den MID Server-Parameter mid.ssh.use_snc auf „true“ setzen.

Hinweis: Um Netzwerkgeräte wie Router und Switches zu erkennen, verwenden Sie SNMP-Anmeldeinformationen Anmeldeinformationen, keine SSH-Anmeldeinformationen.

Parameter für SSHCommand

Für die Probe „SSHCommand“ sind mehrere Parameter verfügbar.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Parametertabelle

Parameter	Beschreibung
allow_unsupported_shells	Ermöglicht einem Probe-Designer, einen Befehl auf einem Gerät ohne unterstützte Shell auszuführen. Ohne Shell gilt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	• Es können keine Pfadinformationen angegeben werden. • Es können keine Skripts ausgeführt werden, da keine Möglichkeit besteht, Skriptparameter zu verarbeiten. • Der im Feld **ECC-Warteschlangenname** des Probe-Formulars angegebene Text ist der Rohbefehl, der auf dem Gerät ausgeführt wird. Beispielsweise können Sie eine Probe entwerfen, um die Version eines Cisco-Switch anzuzeigen, auf dem NX-OS ausgeführt wird. Der Befehl, den der Switch versteht, lautet `show version`. Um dies zu erreichen, fügen Sie den Befehl `show version` in das Feld **ECC-Warteschlangenname** ein und fügen den Parameternamen `allow_unsupported_shells` mit dem Wert **true** hinzu. Dieser Parameter ist nur für `sncssh` wirksam. Für j2ssh wird er nicht unterstützt. Die derzeit unterstützten Shells lauten sh, bash, ksh, csh und tcsh. • Typ: Zeichenfolge, „true“ oder „false“ • Standardwert: false
Quelle	[Erforderlich] Gibt den ersten Host an, zu dem eine Verbindung hergestellt werden soll • Typ: Zeichenfolge (URL) • Standardwert: keiner
port	Gibt den Zielport für die Verbindung an • Typ: Ganzzahl (Port) • Standardwert: 22
debug	Gibt an, ob SSH-Debug-Informationen in die Protokolldatei geschrieben werden sollen. Die Parameterverwendung hängt davon ab, ob der ServiceNow-SSH-Client aktiviert ist. Wenn der SSH-Client von ServiceNow aktiviert ist, funktioniert dieser Parameter wie folgt: • Typ: Zeichenfolge • Standardwert: false Die folgenden Zeichenfolgenwerte sind für den SSH-Client von ServiceNow gültig: ○ true: Aktiviert SSH-Debug-Informationen in der Protokolldatei. ○ false: Deaktiviert SSH-Debug-Informationen in der Protokolldatei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	○ <IP-Adressen>: Gibt an, für welche IP-Bereiche SSH-Debug-Informationen in der Protokolldatei aktiviert werden sollen. Sie können IP-Adressen in den folgenden Formaten eingeben: ▪ Ein IP-Bereich, der durch einen Schrägstrich und die Anzahl der Bits im Subnetz definiert ist. Beispielsweise durchsucht der String 10.10.10.0/24 24-Bit-IP-Adressen von 10.10.10.0 bis 10.10.10.254. ▪ Ein IP-Bereich, der durch einen Bindestrich definiert wird. Der String 10.10.11.0-10.10.11.165 durchsucht beispielsweise die IP-Adressen von 10.10.11.0 bis 10.10.11.165. ▪ Eine durch Kommas getrennte Liste bestimmter IP-Adressen. Zum Beispiel durchsucht der String 10.10.11.200.10.10.11.235 die IP-Adressen 10.10.11.200 und 10.10.11.235. ○ deferred: Gibt an, dass SSH-Debug-Informationen im Speicher protokolliert werden sollen, sofern keine Fehler oder Warnungen auftreten. Wenn ein Fehler oder eine Warnung auftritt, veröffentlicht die Plattform die Debug-Informationen in der Protokolldatei. Dadurch wird sichergestellt, dass nur der Teil der Protokolldatei aufgezeichnet wird, der sich auf den Fehler oder die Warnung bezieht. Wenn kein Fehler oder keine Warnung erkannt wird, löscht die Plattform die nicht verwendeten Protokolldaten aus dem Speicher, sobald die Sitzung geschlossen wird. In jeder Sitzung werden bis zu 1000 Protokollnachrichten gespeichert. Wenn die Sitzung 1000 Protokollnachrichten überschreitet, verwirft das verzögerte Protokoll die älteste Protokollnachricht, um Platz für die neueste Protokollnachricht zu schaffen. Wenn der SSH-Client von ServiceNow deaktiviert ist, aktiviert bzw. deaktiviert dieser Parameter SSH-Debug-Informationen in der Protokolldatei: • Typ: true | false • Standardwert: false
debug_ssh	Gibt an, ob der veraltete SSH-Client Debug-Informationen in die Protokolldatei agent/logs/agent.log schreibt. **Hinweis:** Diese Protokolldatei kann schnell größer werden und sollte deaktiviert werden, wenn sie nicht benötigt wird. Der ServiceNow-SSH-Client verwendet diesen Parameter nicht. • Typ: true | false • Standardwert: false
timeout	Legt den Socket-Verbindungstimeout für den veralteten SSH-Client fest. Der ServiceNow-SSH-Client verwendet diesen Parameter nicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	• Typ: Ganzzahl (Millisekunden) • Standardwert: 60.000
path_override	Gibt an, wie die Standardpfade geändert werden können, die vor der Ausführung eines Befehls festgelegt wurden. Geben Sie einen oder mehrere durch Doppelpunkt (:) getrennte Überschreibungspfade ein. Der Standardpfad ist /usr/sbin: /usr/bin:/bin:/sbin. Der SSH-Client von ServiceNow akzeptiert die folgenden Präfixe vor dem Wert path_overide. • append: Hängt den Überschreibungspfad an das Ende des Hostpfads an. Dies ist das Standardverhalten. • replace: Ersetzt den Hostpfad durch den Wert path_overide. • prepend: Stellt den Überschreibungspfad dem Hostpfad voran. • Typ: Zeichenfolge (eine durch Doppelpunkte getrennte Liste von Verzeichnissen) • Standardwert: keiner
keyboard_interactive	Bestimmt, ob der SSH-Anmeldemodus keyboard_interactive erzwungen wird • Typ: true | false • Standardwert: false
must_sudo	Bestimmt, ob SSH-Befehle über sudo ausgeführt werden **Hinweis:** Der Probe-Parameter „must_sudo“ wirkt sich auf alle Muster aus. Auf Unix- oder Linux-Hosts kann die Musterausführung viele verschiedene Befehle ausführen, einige sollten nicht sudo angehängt sein. • Typ: Wahr | Falsch • Standardwert: false

run_in_terminal	Bestimmt, ob SSH-Befehle in einem SSH-Terminal ausgeführt werden
	• Typ: true | false
	• Standardwert:
	  ○ SSH-Client von ServiceNow: false
	  ○ Veralteter SSH-Client: true

set_path	Bestimmt, ob die Probe die PATH-Variable der Sitzung ändern darf. Standardmäßig wird die PATH-Variable während des Sitzungs-Setup auf `/usr/sbin:/usr/bin:/bin:/sbin` festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	• Typ: true | false • Standardwert: true
rm_override	Überschreibt den Standardbefehl zum Entfernen (`/bin/rm -f`) mit dem angegebenen Wert • Typ: Zeichenfolge • Standardwert: keiner
use_snc_ssh	Aktiviert den SSH-Client von ServiceNow. Der SSH-Client von ServiceNow ist bei neuen Instanzen standardmäßig aktiviert. Durch das Aktivieren des SSH-Clients von ServiceNow wird der veraltete SSH-Client deaktiviert. • Typ: true | false • Standardwert: true
command_timeout_ms	Anzahl von Millisekunden, die ein SSH-Befehl ausgeführt werden darf, bevor eine Zeitüberschreitung auftritt (Standardeinstellung pro MID Server konfigurierbar). Der veraltete SSH-Client verwendet diesen Parameter nicht. • Typ: Ganzzahl • Standardwert: Wert des MID Server-Parameters mid.ssh.command_timeout_ms
channel_timeout_ms	Gibt den Zeitraum in Millisekunden an, die ein MID Server während der Verarbeitung eines SSH-Befehls auf Aktivität wartet. Wenn der MID Server im angegebenen Zeitüberschreitungsfenster keine Aktivität erkennt, beendet dieser Parameter den Befehl. • Typ: Ganzzahl (Millisekunden) • Standardwert: 300000 (5 Minuten)
preserve_sudo_environment	Gibt an, ob Sudo verwendet werden soll, um die Umwelt für SSH zu erhalten. Dieser Parameter ist nur wirksam, wenn die sudo-Umgebung auf dem geprüften Host den Schalter `-E` unterstützt. • Typ: true | false • Standardwert: false
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange ausgegeben, auch wenn die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	Anmeldeinformationen erfolgreich sind. Siehe Fehlerbehebung Bei Anmeldeinformationen Weitere Informationen finden Sie unter .

Pfad für SSHCommand

Die Probe „SSHCommand“ berechnet den Standardpfad aus den folgenden Quellen.

- MID Server-Parameter: mid.ssh.path_override
- Parameter für die Probe „SSH Command“: path_override
- Standardpfad des Benutzers: Shell-Konfigurationsdatei

Wenn Sie den Parameter zum Überschreiben des MID Server-Pfads festlegen, hängt Discovery diesen Pfad an den Standardpfad an. Wenn Sie den Probe-Pfadparameter festlegen, verwendet Discovery diesen Pfad anstelle des Standardpfads. Discovery hängt den Standardausführungspfad eines Benutzers stets an die MID Server- und Probe-Parameterpfade an.

Standardpfad

Standardmäßig sucht der MID Server unter den folgenden Pfaden nach SSH-Befehlen:

- /usr/sbin
- /usr/bin
- /bin
- /sbin

Shell-Skriptoptionen

Die Probe „SSHCommand“ unterstützt die folgenden Skripting-Optionen im Feld *ECC-Warteschlangenname*.

Tabelle der Shell-Skripting-Optionen

Summary	Syntax	Beschreibung
Variable	${variable}	Ersetzt das Token durch den Wert der Variablen. Beispielsweise gibt ${catalina_home} den Installationsort eines Tomcat-Servers an.
Datei einschließen	${File:file_name.sh}	Behandelt den Inhalt der angegebenen Datei als Shell-Skript. Beispielsweise führt ${File:findcat.sh} das Shell-Skript findcat aus.

SSH-Befehle, die während der probenbasierten Discovery keinen privilegierten Anwender erfordern

In diesen Tabellen werden die von ausgeführten SSH-Befehle angezeigt Discovery Probes auf Zielgeräten während der horizontalen Discovery. Diese SSH-Befehle erfordern keine erhöhten Berechtigungen zur Ausführung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssysteme

Informationen zu den von Service-Mapping während der Erkennung von oben nach unten verwendeten Befehlen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern und Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

AIX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
lsattr	*-El sys0 -a modelname -F value*
lslpp	*-Lc*
/etc/ifconfig	*-au; netstat -in*
instfix	*-i | grep AIX_ML*
oslevel	*-r*
echo `lsattr	*-El sys0 -a systemid | cut ...*
rmsock	
Lsdev	• *-C -F 'name,status' -c memory|grep '^mem'* • *-C -F 'name,status' -c processor -S a*
ps	*-aef -o "pid,ppid,args"*

Linux-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
arp	*-n*
bash	*variable*
cat	• */sys/hypervisor/compilation/compiled_by* • */sys/devices/virtual/dmi/id/product_uuid* • */etc/*release* • */proc/cpuinfo* • */var/lib/dpkg/status* • */proc/mounts* • */proc/scsi/scsi* • */etc/iscsi/initiatorname.iscsi* • */sys/hypervisor/compilation/compiled_by*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Befehle (Fortsetzung)

Befehl (ECC-Warteschlangenname)	Parameter
grep MemTotal	*/proc/meminfo*
ifconfig	*-a && route -n*
sh	*variable*
U/min	*-q -a --qf*
ls	• *-d /sys/block/* | grep '^/sys/block/\(dm-|sd|sr\)'* • */sys/class/scsi_host/host*/protocol 2> /dev/null* • */sys/class/scsi_host/host*/info 2> /dev/null* • *-d /sys/class/fc_host/host**
Shoptieren	*-s extglob*
Gefunden	*-L -n -o SOURCE,TARGET 2>/dev/null*
find	*/sys/class/iscsi_session -maxdepth 1 -type l*
Fcoeadm	*-i*
ip	• *neighbor 2> /dev/null* • *address show && ip route*
hostname	*-f 2> /dev/null*
Dnsdomainname	*2> /dev/null*
grep	• *^[[:space:]]*domain /etc/resolv.conf* • *^[[:space:]]*search /etc/resolv.conf*
wget	• *--spider -t 1 -T 1* • *-qO-*
Wellung	*--connect-timeout 1*
python	*-c*
Sudo-Kat	*/sys/devices/virtual/dmi/id/product_uuid*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HP-UX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
ps	*-elx*
echo itick_per_usec/D	*| adb -k /stand/vm...*
sh	*variable*
model	
uname	• *-i* • *-r*
swlist	*-l product | grep -v 'PH._'*
echo 'memory_installed_in_machine/D'	*| a...*
netstat	*-in | grep -v Name*
Lanscan	*-ia*
Typesatz	*-i2*
Ioscan	*-fnkC processor | grep PROCESSOR | wc -l*

Solaris-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
kstat	*cpu_info*
pkginfo	*-l | egrep 'PKGINST|NAME|CATEGO...*
prtconf	• *| grep Memory* • *| grep 'System Configuration:'* • *-pv 2>/dev/null*
ifconfig	*-a; netstat -pnr -f inet*
arp	*-an*
showrev	*-p*
sneep	*-T*
bash	*variable*
Paket	*list*
iostat	*-En | awk '/^c/'*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Solaris-Befehle (Fortsetzung)

Befehl (ECC-Warteschlangenname)	Parameter
Zpool	• *list* • *status | awk '$1 == "NAME", $1 == ""'*
df	*-k*
fcinfo	*hba-port*
Zonenname	
zoneadm	
Zonencode	*-z*
Host-ID	
uname	*-r*
Nawk	
ps	• *-o pid,ppid* • *-awwx*
pfiles	

Mac-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
system_profiler	• *SPHardwareDataType SPMemoryDataType -xml* • *SPSerialATADataType SPSASDataType SPFireWireDataType -xml* • *SPNetworkDataType -xml;ifconfig | grep '\Winet6\W'* • *SPSoftwareDataType -xml* • *SPHardwareDataType -xml* • *SPApplicationsDataType -xml*
Zuletzt	*| grep -m 1 console*
hostname	*2> /dev/null*
grep	• *'^[\s]*domain' /etc/resolv.conf* • *'^[\s]*search' /etc/resolv.conf*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
ps	• *awwxo pid,ppid,command | sed -n '/<defunct>/!p'* • *-ef*
sh	*variable*
cat	*variable*
Variable	*-version*
uname	*-a*
df	*-kP*
uptime;env	*LC_ALL=C date '+%a %b %e %H:%M %Z %Y'*
echo	*\echo `uname -I` `hostname` `uname -Iv`.`uname -Ir` 2>&1``*
awk	
grep	
find	
Uuencode	*-m*
base64	*-w 0*
wc	*-c*
Nohup	
vmware	*-v 2>&1*
Systemctl	*status cloudian-s3 2>&1*

HMC-BS-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
echo	*\lshmc -V 2>&1``*

Webserver

Apache-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
httpd_command	*-V*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tomcat-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
cat	*variable*
find -L ${dirname}	*-name web.xml -print 2>/dev/null*

NGINX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	• *get-nginxcfg* • *get-nginx-ver*

Datenbanken

Oracle-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
lsnrctl	*status*

SQL-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
cat	*variable*
Variable	*-V*

HBase-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
cat	*variable*
sh	*variable*
Variable	*-lv | grep ^${processID}*
echo	*"version" | hbase shell*

Anwendungen

ESX - OS-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

F5 - OS-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
Tmsh	*show sys version 2>&1*

HAProxy-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
Variable	*-v*

JBoss-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
find	*-name web.xml -print*
cat	*variable*

KVM-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
virsh	*Various capabilities*

Puppet-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
puppet	• *--version* • *config print*
hostname	*--fqdn*

Speicher

Befehl (ECC-Warteschlangenname)	Parameter
Purehw	*list --all --nvp --type ch*
Vxprint	*-AQmb*
Vxdisk	*path*
Sudo vxdisk	*list | awk 'NR > 1'*
Püreblade	*list 2>&1*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Discovery Befehle für Probes und Muster

SSH-Befehle, die während der probenbasierten Discovery einen privilegierten Anwender erfordern

In diesen Tabellen werden die von ausgeführten SSH-Befehle angezeigt Discovery Proben während der horizontalen Discovery. Diese SSH-Befehle erfordern erhöhte Berechtigungen zur Ausführung.

Betriebssystembefehle, die erweiterte Rechte erfordern

Diese Beispiele setzen voraus, dass der Benutzername **Disco** lautet. Ersetzen Sie den tatsächlichen Anwendernamen, und überprüfen Sie, ob die Pfade für die Befehle mit den Pfaden im System übereinstimmen.

Hinweis: Sudo-Befehle funktionieren nicht mit Anmeldeinformationen für privaten Schlüssel, da für den sudo-Befehl kein Passwort angegeben werden kann. Eine Lösung ist das Hinzufügen der Option *NOPASSWD* zur Sudo-Konfiguration. Zum Beispiel könnten Sie Folgendes eingeben: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

Informationen zu Befehlen, die keine erhöhten Rechte erfordern, finden Sie unter SSH-Befehle, die während der probenbasierten Discovery keinen privilegierten Anwender erfordern.

Informationen zu den von Service-Mapping während der Erkennung von oben nach unten verwendeten Befehlen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern und Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

SSH-Schlüssel nicht validiert

Wenn MID-Server Stellt eine Verbindung zu einem System her, der MID-Server Führt keine Hostschlüsselvalidierung für dieses System durch und behandelt es daher als nicht vertrauenswürdig. Wenn ein Angreifer einen man-in-the-Middle-Angriff ausführt und den Datenverkehr an einen böswilligen SSH-Service umleitet, kann er alle über die Verbindung gesendeten Daten abfangen oder ändern.

Beschränken Sie daher alle vertraulichen Informationen, die zwischen ausgetauscht werden MID-Server Und der Ziel-SSH-Server. Verwenden Sie nur Schlüssel oder Zertifikate für die SSH-Authentifizierung, und vermeiden Sie das Senden von Systemanmeldeinformationen. Konfigurieren *NOPASSWD* In der Datei „sudoers“ für die erforderlichen privilegierten Befehle.

HP-UX

Befehl	Zweck
adb	Erfasst CPU-Geschwindigkeit und Speicher. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/adb`

Alle Linux

Befehl	Zweck
dmidecode	Sammelt Informationen über die Hardware, einschließlich der Seriennummer des Motherboard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Linux (Fortsetzung)

Befehl	Zweck
	Zeilenbeispiel „/etc/sudoers“ : `Disco ALL=(root) /sbin/dmidecode`
fdisk	Sammelt die Informationen über Datenträger und Größen im System. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/fdisk -l`
multipath	Erfasst Gerätezuordnungen für Multipath-Eingabeausgabe (MPIO). **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/multipath -ll`

Linux und Solaris

Befehl	Zweck
dmsetup	Untersucht ein niedriges Volume. **Beispiel für die Zeile „/etc/sudoers“** • `Disco ALL=(root) /usr/bin/dmsetup table *` • `Disco ALL=(root) /usr/bin/dmsetup ls`

Alle UNIX Versionen

Befehl	Zweck
lsof	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /sbin/lsof`
oratab	Gewährt Lesezugriff auf die Oratab-Datei zum Auffinden von Oracle Startseite und pfile.
netstat	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(Stamm) /bin/netstat`
ss	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /sbin/ss`

Solaris

Befehl	Zweck
iscsiadm	Ruft qualifizierte iSCSI-Namen (IQNs) ab. **Zeilenbeispiel „/etc/sudoers“** : `${sudo:iscsiadm-Listenziel – S}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Solaris (Fortsetzung)

Befehl	Zweck
`fcinfo`	Ruft World Wide Port-Namen (WWPNs) für Ports ab. **Zeilenbeispiel „/etc/sudoers“** : `${sudo:fcinfo Remote-Port -sl -p $Port}`
`prtvtoc`	Liefert Informationen zu Datenträgerpartitionen. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/prtvtoc`
`/usr/bin/ps`	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff die Rolle proc_owner.sola hinzu. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/ps`
`/usr/ucb/ps`	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. Die Verwendung von `/Usr/ucb/ps` Befehl ist ab veraltet Solaris11. Weil Discovery Erfordert die Verwendung dieses Befehls für alle Solaris Versionen, müssen Sie das ucb-Dienstprogramm manuell auf installieren Solaris11 Systeme. Anweisungen dazu finden Sie in KB0564262 . **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/ucb/ps`
`Pgrep`	Ruft eine Liste von Prozess-IDs (PIDs) mit Socket-Informationen ab. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/pgrep`
`pfiles`	Ruft für jede PID die Ausgabe für S_IFSOCK ab und verarbeitet sie. **Zeilenbeispiel „/etc/sudoers“** : `Disco ALL=(root) /usr/bin/pfiles`

Zugehörige Informationen

Discovery Befehle für Probes und Muster

vCenter-Probes und Probe-Parameter

vCenter-Probes scannen virtuelle Computer mit der Produkt-Suite vSphere von VMware. Jede Probe scannt nach verschiedenen Arten von Daten wie Netzwerke, NICs und Tags. Die Unterstützung für die Probe „VMware - vCenter“, die in früheren Releases alle vCenter-Objekte erkannte, wurde ab dem Istanbul-Release eingestellt, und sie wurde durch mehrere Probes ersetzt.

Upgradebedingte Änderungen

In upgegradeten Systemen sind der Prozessklassifizierer vCenter und die Port-Probe vmapp so konfiguriert, dass sie den Probe „VMware -vCenter Datacenters“ auslösen. Diese Probe löst dann die Probes aus, die einzelne vCenter-Objekte wie Hosts, Speicher und Datenspeicher erkennen. Die veraltete Probe „VMware - vCenter“ befindet sich noch im System, wird jedoch in der aktualisierten Instanz nicht mehr ausgelöst.

Automatische Übersetzung

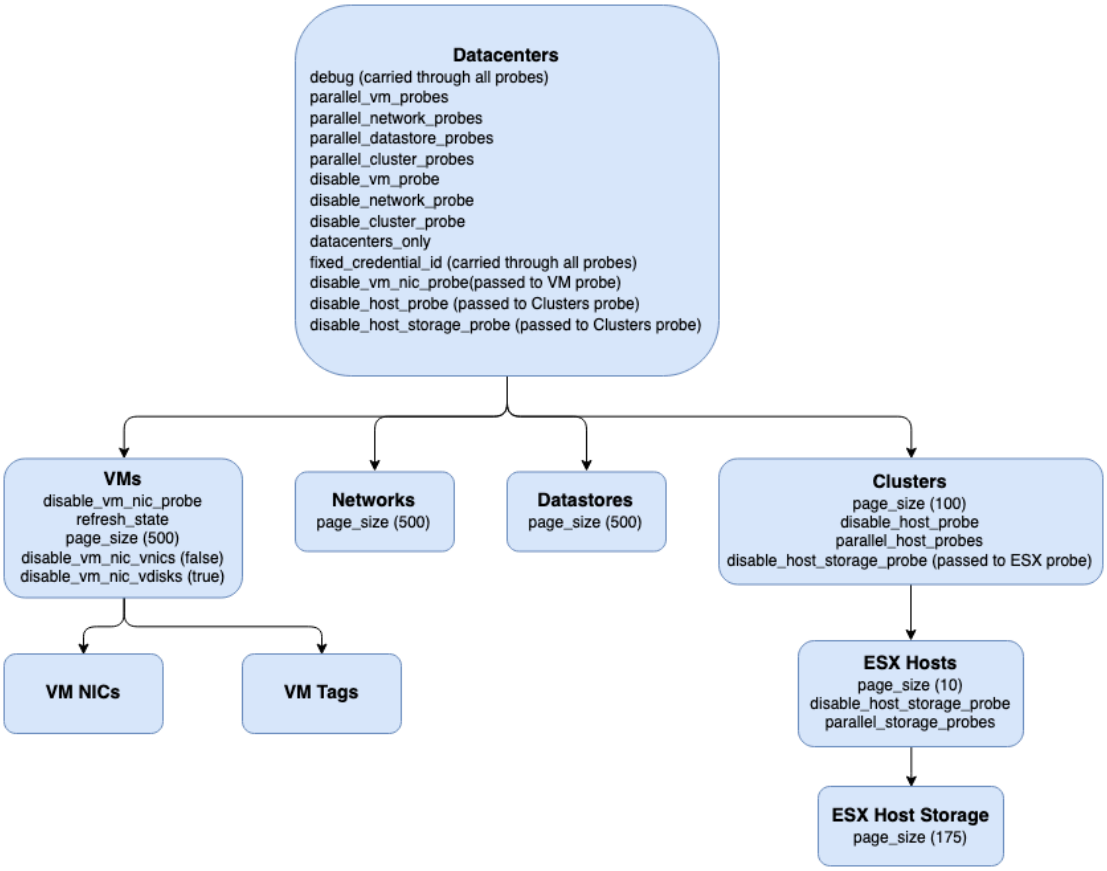
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare vCenter-Probes und Probe-Parameter

Mit vCenter-Probe-Parametern können Sie die Probes für die Objekte deaktivieren, an deren Erkennung Sie nicht interessiert sind. Sie können auch die Größe der Nutzlast einer Probe reduzieren, indem Sie eine Seitengröße angeben.

Wichtig: Beachten Sie vor dem Deaktivieren einer Probe mögliche Abhängigkeiten der Probe. Wenn die Probe, die Sie deaktivieren, eine andere Probe auslöst, wird auch die abhängige Probe deaktiviert und kann keine Daten erfassen.

Beziehung von vCenter-Elementen zu Probe-Parametern



Die folgenden Parameter sind für vCenter-Probes verfügbar.

Hinweis: Sofern nicht anders angegeben, werden diese Parameter in der Plattform standardmäßig nicht festgelegt.

vCenter-Probe-Parameter

Probe	Parameter
VMware – vCenter-Rechenzentren	• datacenter_only (Cloud Provisioning and Governance) • debuggen • disable_vm_probe • disable_network_probe • disable_datastore_probe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Probe-Parameter (Fortsetzung)

Probe	Parameter
	• disable_cluster_probe • datacenters_only • fixed_credential_id (Cloud Provisioning and Governance) • disable_vm_nic_probe • disable_host_probe • disable_host_storage_probe • vcenter_timeout: Standard 10.000 Millisekunden (10 Sekunden)
VMWare – vCenter-VMs	• disable_vm_nic_probe • disable_vm_nic_vnics (auf **false** gesetzt) • disable_vm_nic_vdisks (auf **wahr** – nur für Discovery – und **falsch** festgelegt, wenn Cloud Provisioning and Governance aktiviert ist) • disable_vm_tags_probe • refresh_state (Cloud Provisioning and Governance) • page_size (100) **Hinweis:** Bei den Einstellungen für die Parameter „vnics“ und „vdisks“ wird das Standardverhalten von vCenter Discovery beibehalten.
VMware – vCenter-VM-Tags*	keine
VMware – vCenter-VM-NICs	keine
VMware – vCenter-Netzwerke	page_size (500)
VMware – vCenter-Datenspeicher	page_size (500)
VMware – vCenter-Cluster	• disable_host_probe • disable_host_storage_probe • page_size (1000)
VMware – vCenter-ESX-Hosts	• disable_host_storage_probe • page_size (10)
VMware – vCenter-ESX-Host-Speicher	page_size (175)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Probe-Parameter (Fortsetzung)

Probe	Parameter
VMware – vCenter-ESX-Host-Lizenz	keine
VMware vCenter-VM-Leistung	Diese Probe stützt sich auf die für vCenter konfigurierten Statistikintervalle. Standardmäßig sind die folgenden Intervalle verfügbar: • 5 Minuten (300 Sekunden) – diese Daten werden 24 Stunden lang gespeichert. • 30 Minuten (1.800 Sekunden) – diese Daten werden eine Woche lang gespeichert. • 2 Stunden (7.200 Sekunden) – diese Daten werden einen Monat lang gespeichert. • 24 Stunden (86.400 Sekunden) – diese Daten werden ein Jahr lang gespeichert. Die folgenden Eigenschaften unterstützen diese Probe: • data_sampling_weeks_frame: Zeitraum, für den die Daten von der Probe abgerufen werden, in Wochen • data_sampling_minutes: Zeit zwischen der Entnahme der Datenstichproben • Metriken: erfasste Metriken (CPU/ Arbeitsspeicher/Netzwerk/Laufwerk) Diese Probe wird nur von Bewertung der Cloud-Migration verwendet. **Wichtig:** Um die Standardwerte für diese Probe zu ändern, stimmen Sie sich mit dem Administrator ab, der für die vCenter-Verwaltung verantwortlich ist. Weitere Informationen finden Sie in der VMware-Dokumentation .

* Weitere Informationen finden Sie unter VMware-Tags.

Beachten Sie beim Festlegen dieser Parameter Folgendes:

- **Deaktivierung**: Sie deaktivieren Probes, indem Sie den Parameter in der auslösenden Probe festlegen. Beispiel: Wenn Sie an der Erkennung von Speicher nicht interessiert sind, legen Sie den Parameter *disable_host_storage_probe* in der Probe „VMWare - vCenter ESX Hosts“ auf **true** fest.
- **Seitengröße**: Der Parameter für die Seitengröße steuert die Anzahl der mit einer einzelnen Probe zu erkennenden CIs. Verwenden Sie diesen Parameter, um die Größe der Nutzlast zu begrenzen, indem die Anzahl der vCenter-Elemente reduziert wird, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von einer Probe gleichzeitig erkannt werden. Die in Klammern angegebene Seitengröße entspricht der Standardeinstellung im Basissystem.

- **Debugging:** Legen Sie den Parameter debug in der Probe „VMWare - vCenter Datacenters“ fest, um Debugging für alle vCenter-Probes zu ermöglichen. Beim Debugging werden die vCenter-Rohdaten in jeder Probe-Nutzlast zurückgegeben.

Benutzerdefinierte Probes mit der Discovery-Erweiterung für vCenter auslösen

Mit der Discovery-Erweiterung für vCenter können Sie zusätzliche Attribute von derzeit erkannten CI-Typen oder Attribute neuer CI-Typen erfassen, indem Sie benutzerdefinierte Probes von einem vorhandenen Sensor auslösen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Datensätze des vCenter-Sensors unterstützen die Auslösung benutzerdefinierter Probes. Diese verwenden bedingte Skripts zur Erfassung von Daten, die Discovery normalerweise nicht erfasst, oder zur Erkennung von selbst erstellten CI-Typen.

Wichtig: Die vCenter-Erweiterung dient zum Erstellen einer einzelnen benutzerdefinierten Probe, die die vorhandene Discovery-Funktionalität erweitert. Sofern Sie als Benutzer nicht mit erweitertem Skripting vertraut sind, versuchen Sie nicht, Ihre neue Probe/Ihren neuen Sensor so zu konfigurieren, dass eine zusätzliche Probe gestartet wird.

Prozedur

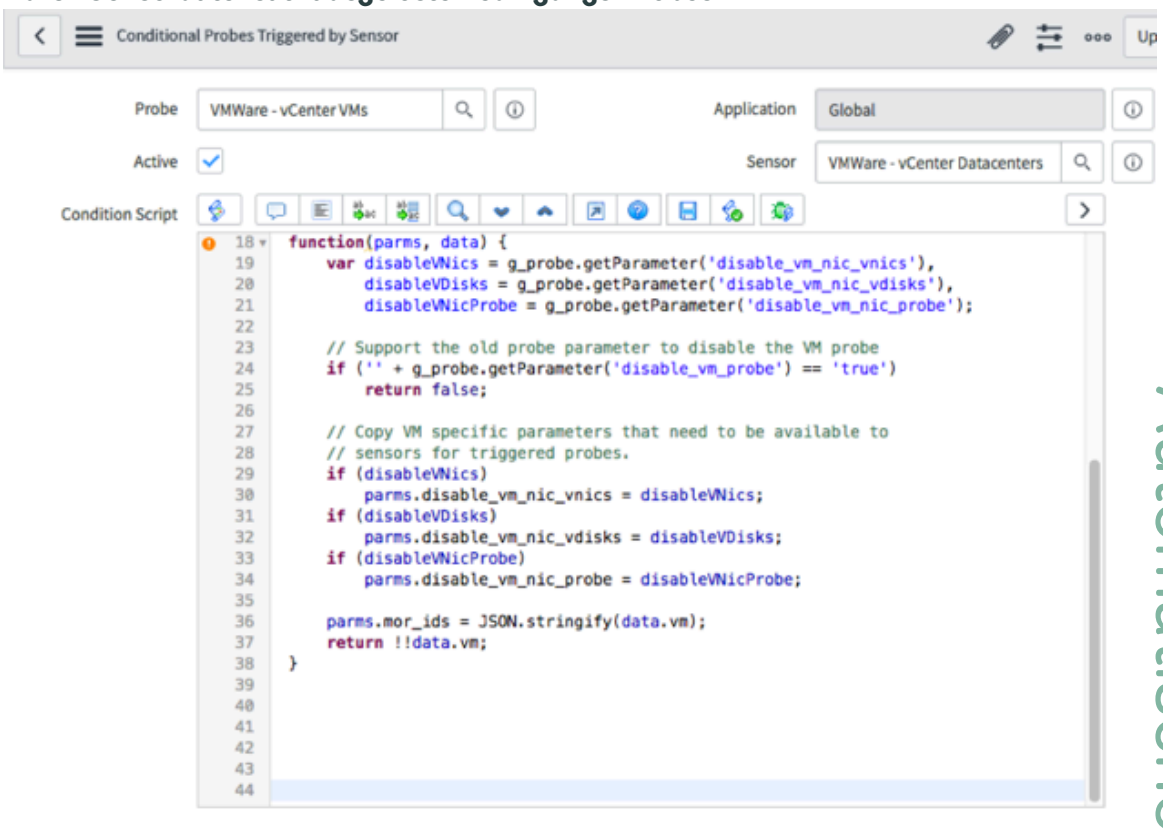
1. Navigieren zu **Alle** > **Discovery-Definition** > **Sensoren**an.
2. Wählen Sie einen vCenter-Sensordatensatz aus.
   Es ist wichtig, eine neue Probe zum richtigen Zeitpunkt auszulösen. Wenn Sie beispielsweise zusätzliche Informationen über virtuelle Computer in Ihrem Netzwerk erkennen möchten, lösen Sie Ihre Probe über den Sensor „VMware - vCenter VMs“ aus. Wenn Sie Ihre benutzerdefinierte Probe über den Sensor „VMware - vCenter Datacenters“ auslösen, werden die neue Probe und die vorhandene VM-Probe parallel ausgeführt. Dadurch kann die Erstellung oder Aktualisierung von VM-Datensätzen verhindert werden.
3. Klicken Sie auf die zugehörige Liste **Auslösertests**.
4. Klicken Sie auf **Neu**, um eine neue Probe zu erstellen, die von diesem Sensor ausgelöst werden soll, oder auf **Bearbeiten**, um der Liste eine vorhandene Probe hinzuzufügen.
   Sie können auch einen vorhandenen Probe-Datensatz als Vorlage für eine eigene neue Probe verwenden, indem Sie den Datensatz öffnen und im Kontextmenü die Option **Einfügen und beibehalten** auswählen.
5. Klicken Sie auf das Informationssymbol rechts neben dem Probe-Namen, um den Datensatz **Durch Sensor ausgelöste Bedingungs-Probes** zu öffnen.
6. Zeigen Sie das Skript an.
   Das Skript übergibt die Argumente **parms** und **data** an die Funktion und verwendet dabei Werte, die vom auslösenden Sensor an sie übergeben wurden. Das Skript konfiguriert das Objekt **parms**, aus dem die Probe-Parameter abgeleitet werden. Das Skript gibt **true** zurück, um die Probe auszulösen, oder **false**, um sie abzubrechen.

   In diesem Beispiel sind die **parms**-Argumente des Sensors „VMware - vCenter Datacenters“ allesamt Probe-Parameter, die von der Probe „Datacenters“ unterstützt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Das Argument **data** ist ein Objekt, das bis zu 4 Arrays mit den Namen **vm**, **datastore**, **network** und **cluster** enthält.

Durch Sensordatensatz ausgelöste Bedingungs-Probes



Windows Probes und Berechtigungen

Discovery Greift auf Geräte und Software zu, indem Befehle als bestimmter Anwender auf ausgeführt werden Windows Computer.

Die meisten Probes erfordern Zugriff auf Windows-Klassen, -Eigenschaften und -Registrierungseinträgen. Bestimmte Probes erfordern zudem zusätzlichen Zugriff auf Windows-Verzeichnisse und -Ressourcen. Sicherheitsrichtlinien variieren je nach Organisation, daher gibt es keine bestimmte Rolle oder kein Recht, die gewährt werden kann. Überprüfen Sie, ob Windows Anwender hat Lokaler Administrator Berechtigung für diese Windows Komponenten.

Administrative Freigaben

Windows Administrative Freigaben sind ausgeblendete Serverressourcen, die Discovery Dient zum vorübergehenden Speichern der Ergebnisse von Prozessen, die von bestimmten Probes ausgeführt werden. Die MID-Server Skriptdatei *`LaunchProc.psm1`*Startet den Prozess, schreibt seine Ausgabe in die administrative Freigabe auf dem Computer und ruft dann die Ergebnisse für ab MID-Server. Der Zugriff auf administrative Freigaben ist auf Anwender mit Administratorrechten für das Ziel beschränkt. Beispiel: Anwender, lokal oder in der Domäne, die zur lokalen Administratorgruppe gehören.

Mit New York Release, alle Windows Probes, die das WMI-Protokoll verwenden, rufen den auf *`LaunchProc.psm1`*Skriptdatei und als Standard in den Admin$-Freigabeordner schreiben. Ob jeweils eine andere Netzwerkfreigabe bereitgestellt ist Windows Ziel, kann der Ordner durch Aktualisieren von geändert werden MID-Server-Eigenschaft *`mid.powershell.target_base_dir`*.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen

Die meisten Windows-Probes greifen auf Windows-Klassen und -Eigenschaften zu, die in diesen Klassen enthalten sind. Einige Windows Klassen geben keinen Dateinamespace-Pfad an. Wenn kein expliziter Pfad angegeben ist, ServiceNow Verwendet Stamm\cimv2\<Class> Standardmäßig.

Hinweis: Discovery von Cluster-VIP wird nicht unterstützt.

Windows Klassen

Probe	Windows Klasse	Eigenschaft
Hyper-V - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Antecedent**
Hyper-V - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Abhängig**
Hyper-V - Cluster	root\MSCluster\MSCluster_Resource	**Typ**
Hyper-V - Resource Pools	root\virtualization\Msvm_ResourcePool	**AllocationUnits**
Hyper-V - Resource Pools	root\virtualization\Msvm_ResourcePool	**Kapazität**
Hyper-V - Resource Pools	root\virtualization\Msvm_ResourcePool	**InstanceID**
Hyper-V - Resource Pools	root\virtualization\Msvm_ResourcePool	**Name**
Hyper-V - Resource Pools	root\virtualization\Msvm_ResourcePool	**ResourceSubType**
Hyper-V - Resource Pools	Stamm\Virtualisierung \v2\Msvm_ResourcePool	**AllocationUnits**
Hyper-V - Resource Pools	Stamm\Virtualisierung \v2\Msvm_ResourcePool	**Kapazität**
Hyper-V - Resource Pools	Stamm\Virtualisierung \v2\Msvm_ResourcePool	**InstanceID**
Hyper-V - Resource Pools	Stamm\Virtualisierung \v2\Msvm_ResourcePool	**Name**
Hyper-V - Resource Pools	Stamm\Virtualisierung \v2\Msvm_ResourcePool	**ResourceSubType**
Hyper-V - Virtual Machines	root\virtualization\Msvm_ComputerSystem	**Beschreibung**
Hyper-V - Virtual Machines	root\virtualization\Msvm_ComputerSystem	**ElementName**
Hyper-V - Virtual Machines	root\virtualization\Msvm_ComputerSystem	**EnabledState**
Hyper-V - Virtual Machines	root\virtualization\Msvm_ComputerSystem	**Name**
Hyper-V - Virtual Machines	root\virtualization\Msvm_ComputerSystem	**TimeOfLastStateChange**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**BlockSize**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**ElementName**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**NumberOfBlocks**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**SystemName**
Hyper-V - Virtual Machines	root\virtualization \Msvm_MemorySettingData	**AllocationUnits**
Hyper-V - Virtual Machines	root\virtualization \Msvm_MemorySettingData	**InstanceID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_MemorySettingData	**VirtualQuantity**
Hyper-V - Virtual Machines	root\virtualization \Msvm_ProcessorSettingData	**InstanceID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_ProcessorSettingData	**VirtualQuantity**
Hyper-V - Virtual Machines	root\virtualization \Msvm_SyntheticEthernetPortSettingData	**ElementName**
Hyper-V - Virtual Machines	root\virtualization \Msvm_SyntheticEthernetPortSettingData	**InstanceID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BaseBoardSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BIOSGUID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BIOSSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**ChassisSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**InstanceID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**SystemName**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_Computersystem	**Beschreibung**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_Computersystem	**ElementName**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_Computersystem	**EnabledState**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_Computersystem	**Name**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_Computersystem	**TimeOfLastStateChange**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_LogicalDisk	**BlockSize**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_LogicalDisk	**ElementName**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_LogicalDisk	**NumberOfBlocks**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_LogicalDisk	**SystemName**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_MemorySettingData	**AllocationUnits**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_MemorySettingData	**InstanceID**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_MemorySettingData	**VirtualQuantity**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_ProcessorSettingData	**InstanceID**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_ProcessorSettingData	**VirtualQuantity**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_SyntheticEthernetPortSettingData	**ElementName**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_SyntheticEthernetPortSettingData	**InstanceID**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**BaseBoardSerialNumber**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**BIOSGUID**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**BIOSSerialNumber**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**ChassisSerialNumber**
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**InstanceID**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Hyper-V - Virtual Machines	Stamm\Virtualisierung \v2\Msvm_VirtualSystemSettingData	**SystemName**
Hyper-V - Virtual Networks	root\virtualization\Msvm_ActiveConnection	**Antecedent**
Hyper-V - Virtual Networks	root\virtualization\Msvm_ActiveConnection	**Abhängig**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \Msvm_VirtualEthernetSwitch	**ElementName**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \Msvm_VirtualEthernetSwitch	**Name**
Hyper-V - Virtual Networks	root\virtualization\Msvm_VirtualSwitch	**ElementName**
Hyper-V - Virtual Networks	root\virtualization\Msvm_VirtualSwitch	**Name**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_ActiveConnection	**Antecedent**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_ActiveConnection	**Abhängig**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_VirtualEthernetSwitch	**ElementName**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_VirtualEthernetSwitch	**Name**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_VirtualSwitch	**ElementName**
Hyper-V - Virtual Networks	Stamm\Virtualisierung \v2\Msvm_VirtualSwitch	**Name**
Windows: Sitzung Mit Aktiven Verbindungen	Win32_OperatingSystem	**Name**
Windows - Active Processes	Win32_Process	**Beschriftung**
Windows - Active Processes	Win32_Process	**CommandLine**
Windows - Active Processes	Win32_Process	**CreationDate**
Windows - Active Processes	Win32_Prozess	**Beschreibung**
Windows - Active Processes	Win32_Process	**ExecutablePath**
Windows - Active Processes	Win32_Process	**Name**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Active Processes	Win32_Process	**ParentProcessId**
Windows - Active Processes	Win32_Process	**Priorität**
Windows - Active Processes	Win32_Process	**ProcessId**
Windows: Amazon EC2	Win32_ComputerSystemProduct	**UUID**
Windows: Azure-Beziehung	Win32_ComputerSystemProduct	**UUID**
Windows - Classify	root\MSCluster\MSCluster_Cluster	**Name**
Windows - Classify	root\MSCluster\MSCluster_ClusterToNode	**Antecedent**
Windows - Classify	root\MSCluster\MSCluster_ClusterToNode	**Abhängig**
Windows - Classify	root\MSCluster \MSCluster_ClusterToResource	**GroupComponent**
Windows - Classify	root\MSCluster \MSCluster_ClusterToResource	**PartComponent**
Windows - Classify	root\MSCluster\MSCluster_Node	**Name**
Windows - Classify	root\MSCluster\MSCluster_Resource	**Name**
Windows - Classify	root\MSCluster\MSCluster_Resource	**PrivateProperties**
Windows - Classify	root\MSCluster\MSCluster_Resource	**Typ**
Windows - Classify	root\virtualization\Msvm_ComputerSystem	**Name**
Windows - Classify	Stamm\Virtualisierung \v2\Msvm_Computersystem	**Name**
Windows - Classify	Win32_ComputerSystem	**Domäne**
Windows - Classify	Win32_ComputerSystem	**Name**
Windows - Classify	Win32_OperatingSystem	**Beschriftung**
Windows - Classify	Win32_OperatingSystem	**Version**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Beschriftung**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Status**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetwork	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetwork	**PartComponent**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetworkInterface	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetworkInterface	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Antecedent**
Windows - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Abhängig**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToQuorumResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToQuorumResource	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResource	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResourceGroup	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResourceGroup	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Event	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Event	**Typ**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Adresse**
Windows - Cluster	root\MSCluster\MSCluster_Network	**AddressMask**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Name**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Adresse**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**DeviceID**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Name**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Netzwerk**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Beschriftung**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Characteristics**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Cluster	root\MSCluster\MSCluster_Node	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Flags**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Node	**NodeInstanceID**
Windows - Cluster	root\MSCluster\MSCluster_Node	**PrivateProperties**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Status**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Status**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveGroup	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveGroup	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveResource	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToNetworkInterface	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToNetworkInterface	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Beschriftung**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**PrivateProperties**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Status**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Typ**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Name**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**PrivateProperties**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Status**
Windows - Cluster	root\MSCluster \MSCluster_ResourceGroupToResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceGroupToResource	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToDependentResource	**Antecedent**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Cluster	root\MSCluster \MSCluster_ResourceToDependentResource	**Abhängig**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToPossibleOwner	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToPossibleOwner	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**DisplayName**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**Name**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**PrivateProperties**
Windows - Cluster	root\MSCluster \MSCluster_ResourceTypeToResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceTypeToResource	**PartComponent**
Windows - Cluster	Win32_NetworkAdapterConfiguration	**IPAddress**
Windows - Cluster	Win32_NetworkAdapterConfiguration	**IPEnabled**
Windows - CPU / Memory	Win32_PhysicalMemory	**BankLabel**
Windows - CPU / Memory	Win32_PhysicalMemory	**Kapazität**
Windows - CPU / Memory	Win32_PhysicalMemory	**DataWidth**
Windows - CPU / Memory	Win32_PhysicalMemory	**DeviceLocator**
Windows - CPU / Memory	Win32_PhysicalMemory	**FormFactor**
Windows - CPU / Memory	Win32_PhysicalMemory	**Hersteller**
Windows - CPU / Memory	Win32_PhysicalMemory	**MemoryType**
Windows - CPU / Memory	Win32_PhysicalMemory	**PartNumber**
Windows - CPU / Memory	Win32_PhysicalMemory	**SerialNumber**
Windows - CPU / Memory	Win32_PhysicalMemory	**Geschwindigkeit**
Windows - CPU / Memory	Win32_PhysicalMemory	**Status**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - CPU / Memory	Win32_PhysicalMemory	**Tag**
Windows - CPU / Memory	Win32_PhysicalMemory	**TotalWidth**
Windows - CPU / Memory	Win32_PhysicalMemory	**TypeDetail**
Windows - CPU / Memory	Win32_Processor	**Hersteller**
Windows - CPU / Memory	Win32_Processor	**MaxClockSpeed**
Windows - CPU / Memory	Win32_Processor	**Name**
Windows - CPU / Memory	Win32_Processor	**NumberOfCores**
Windows - CPU / Memory	Win32_Processor	**NumberOfLogicalProcessors**
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebServerSetting	**LogFileDirectory**
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebServerSetting	**Name**
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebServerSetting	**SecureBindings**
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebServerSetting	**ServerBindings**
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebServerSetting	**ServerComment**
Windows - Get IIS Information	Stamm\WebAdministration\Site	**Bindungen**
Windows - Get IIS Information	Stamm\WebAdministration\Site	**ID**
Windows - Get IIS Information	Stamm\WebAdministration\Site	**Protokolldatei**
Windows - Get IIS Information	Stamm\WebAdministration\Site	**Name**
Windows: Ruft die physische Adresse für VIP ab	root\MSCluster \MSCluster_NetworkInterface	**Adresse**
Windows: Ruft die physische Adresse für VIP ab	Win32_NetworkAdapterConfiguration	**IPAddress**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows: Ruft die physische Adresse für VIP ab	Win32_NetworkAdapterConfiguration	**IPEnabled**
Windows - Hardware Information	Win32_BaseBoard	**SerialNumber**
Windows - Hardware Information	Win32_BIOS	**SerialNumber**
Windows - Hardware Information	Win32_ComputerSystemProduct	**IdentifyingNumber**
Windows - Hardware Information	Win32_ComputerSystemProduct	**UUID**
Windows - Hardware Information	Win32_SystemEnclosure	**ChassisTypes**
Windows - Hardware Information	Win32_SystemEnclosure	**SerialNumber**
Windows: Hardware- Und Netzwerkinformationen	Win32_BaseBoard	**SerialNumber**
Windows: Hardware- Und Netzwerkinformationen	Win32_BIOS	**SerialNumber**
Windows: Hardware- Und Netzwerkinformationen	Win32_ComputerSystemProduct	**IdentifyingNumber**
Windows: Hardware- Und Netzwerkinformationen	Win32_ComputerSystemProduct	**UUID**
Windows: Hardware- Und Netzwerkinformationen	Win32_IP4RouteTable	**Ziel**
Windows: Hardware- Und Netzwerkinformationen	Win32_IP4RouteTable	**Maske**
Windows: Hardware- Und Netzwerkinformationen	Win32_IP4RouteTable	**NextHop**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapter	**Index**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapter	**Hersteller**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapter	**NetConnectionID**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**Beschriftung**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**DefaultIPGateway**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**DHCPEnabled**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**Index**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**IPAddress**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**IPEnabled**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**IPSubnet**
Windows: Hardware- Und Netzwerkinformationen	Win32_NetworkAdapterConfiguration	**MACAddress**
Windows: Hardware- Und Netzwerkinformationen	Win32_SystemEnclosure	**ChassisTypes**
Windows: Hardware- Und Netzwerkinformationen	Win32_SystemEnclosure	**SerialNumber**
Windows - Network	Win32_IP4RouteTable	**Ziel**
Windows - Network	Win32_IP4RouteTable	**Maske**
Windows - Network	Win32_IP4RouteTable	**NextHop**
Windows - Network	Win32_NetworkAdapterConfiguration	**Beschriftung**
Windows - Network	Win32_NetworkAdapter	**Index**
Windows - Network	Win32_NetworkAdapter	**Hersteller**
Windows - Network	Win32_NetworkAdapter	**NetConnectionID**
Windows - Network	Win32_NetworkAdapterConfiguration	**DefaultIPGateway**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Network	Win32_NetworkAdapterConfiguration	**DHCPEnabled**
Windows - Network	Win32_NetworkAdapterConfiguration	**Index**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPAddress**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPEnabled**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPSubnet**
Windows - Network	Win32_NetworkAdapterConfiguration	**MACAddress**
Windows - OS Information	Win32_ComputerSystem	**Hersteller**
Windows - OS Information	Win32_ComputerSystem	**Modell**
Windows - OS Information	Win32_ComputerSystem	**UserName**
Windows - OS Information	Win32_OperatingSystem	**CSDVersion**
Windows - OS Information	Win32_OperatingSystem	**Beschreibung**
Windows - OS Information	Win32_OperatingSystem	**Version**
Windows - OS Information	Win32_Processor	**AddressWidth**
Windows - Printers	Win32_TCPIPPrinterPort	**HostAddress**
Windows - Printers	Win32_Printer	**DeviceID**
Windows - Printers	Win32_TCPIPPrinterPort	**Name**
Windows - Printers	Win32_Printer	**Name**
Windows - Printers	Win32_Printer	**PortName**
Windows - Services	Win32_Service	**AcceptPause**
Windows - Services	Win32_Service	**AcceptStop**
Windows - Services	Win32_Service	**DesktopInteract**
Windows - Services	Win32_Service	**DisplayName**
Windows - Services	Win32_Service	**Name**
Windows - Services	Win32_Service	**PathName**
Windows - Services	Win32_Service	**ProcessId**
Windows - Services	Win32_Service	**ServiceType**
Windows - Services	Win32_Service	**StartMode**
Windows - Services	Win32_Service	**StartName**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows - Services	Win32_Service	**Status**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Beschriftung**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**DeviceID**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Index**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**InterfaceType**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Hersteller**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Modell**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**SCSIBus**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**SCSILogicalUnit**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**SCSIPort**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**SCSITargetId**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**SerialNumber**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Größe**
Windows – Speicher 2008 – WMI	Win32_DiskDrive	**Status**
Windows – Speicher 2008 – WMI	Win32_DiskPartition	**DiskIndex**
Windows – Speicher 2008 – WMI	Win32_DiskPartition	**Index**
Windows – Speicher 2008 – WMI	Win32_DiskPartition	**Größe**
Windows – Speicher 2008 – WMI	Win32_DiskPartition	**Startversatz**
Windows – Speicher 2008 – WMI	Win32_LogicalDisk	**DeviceID**
Windows – Speicher 2008 – WMI	Win32_LogicalDisk	**VolumeSerialNumber**
Windows – Speicher 2008 – WMI	Win32_LogicalDiskToPartition	**Antecedent**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows – Speicher 2008 – WMI	Win32_LogicalDiskToPartition	**Abhängig**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**Beschreibung**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**DeviceID**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**DriveType**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**FileSystem**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**FreeSpace**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**ProviderName**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**Größe**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**VolumeName**
Windows – Speicher 2008 – WMI	Win32_MappedLogicalDisk	**VolumeSerialNumber**
Windows – Speicher 2008 – WMI	Win32_mountpoint	**Verzeichnis**
Windows – Speicher 2008 – WMI	Win32_mountpoint	**Volumen**
Windows – Speicher 2008 – WMI	Win32_Volume	**Kapazität**
Windows – Speicher 2008 – WMI	Win32_Volume	**DeviceID**
Windows – Speicher 2008 – WMI	Win32_Volume	**Driveletter**
Windows – Speicher 2008 – WMI	Win32_Volume	**DriveType**
Windows – Speicher 2008 – WMI	Win32_Volume	**FileSystem**
Windows – Speicher 2008 – WMI	Win32_Volume	**FreeSpace**
Windows – Speicher 2008 – WMI	Win32_Volume	**Bezeichnung**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Zugeteilte Größe**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**BusType**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**FreundlichName**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Hersteller**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Modell**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Nummer**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**ObjectId**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Betriebsstatus**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**SerialNumber**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Disk	**Größe**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_DiskToPartition	**Datenträger**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_DiskToPartition	**Partition**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_iSCSISession	**InitiatorNodeAddress**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_iSCSISession	**SessionIdentifier**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_iSCSISession	**TargetNodeAddress**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_iSCSISessionToDisk	**Datenträger**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_iSCSISessionToDisk	**ISCSISession**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**AccessPaths**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**DiskId**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**ObjectId**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**Offset**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**Betriebsstatus**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**PartitionNumber**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Partition	**Größe**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_PartitionToVolume	**Partition**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_PartitionToVolume	**Volumen**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**Driveletter**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**DriveType**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**FileSystem**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**FileSystembezeichnung**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**ObjectId**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**Größe**
Windows – Speicher 2012 – WMI	Stamm\microsoft\Windows\Storage \MSFT_Volume	**GrößenNeuerstellung**
Windows – Speicher 2012 – WMI	Win32_DiskDrive	**Name**
Windows – Speicher 2012 – WMI	Win32_DiskDrive	**SCSIBus**
Windows – Speicher 2012 – WMI	Win32_DiskDrive	**SCSILogicalUnit**
Windows – Speicher 2012 – WMI	Win32_DiskDrive	**SCSIPort**
Windows – Speicher 2012 – WMI	Win32_DiskDrive	**SCSITargetId**
Windows – Speicher 2012 – WMI	Win32_LogicalDisk	**DeviceID**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows Klasse	Eigenschaft
Windows – Speicher 2012 – WMI	Win32_LogicalDisk	**VolumeSerialNumber**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**Beschreibung**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**DeviceID**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**DriveType**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**FileSystem**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**FreeSpace**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**ProviderName**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**Größe**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**VolumeName**
Windows – Speicher 2012 – WMI	Win32_MappedLogicalDisk	**VolumeSerialNumber**
Windows – Speicher 2012 – WMI	Win32_mountpoint	**Verzeichnis**
Windows – Speicher 2012 – WMI	Win32_mountpoint	**Volumen**

Windows Registrierungseinträge

Mehrere Windows Registrierungseinträge sind für verfügbar Discovery Windows Probes.

Hinweis: Der Sensor „Windows - Installierte Software“ wendet einen Zeitstempel von 00:00:00 auf den in der Registrierung abgerufenen Wert „install_date“ ab. Die Installationszeit aller Windows Software ist unabhängig von der Zeitzone und wird auf Mitternacht des Tages festgelegt, an dem sie installiert wurde. Zum Beispiel ein Installationsdatum von **2.19.2017** In Windows Registrierung wird als angezeigt **2.19.2017 00:00:00** In CMDB.

Probe	Windows Registrierungseinträge
Windows: Sitzung Mit Aktiven Verbindungen	HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Hostname
Windows - Classify	HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Hostname
Windows - Classify	HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Domain

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	Windows Registrierungseinträge
Windows - Get IIS Information	HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/InetStp/MajorVersion
Windows - Get IIS Information	HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/InetStp/MinorVersion
Windows - Find APD File Location	HKEY_LOCAL_MACHINE/SOFTWARE/APD/APD/CONFIGPATH
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/ParentDisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/UninstallString
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/Version
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Office/*/Registration/*/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/ProductID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	Windows Registrierungseinträge
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Office/*/Registration/*/DigitalProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/UninstallString
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Office/*/Registration/*/DigitalProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/Registration/ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/svcVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Office/*/Registration/*/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/ParentDisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/DigitalProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Package_*_KB*/InstallName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Paket_*_KB*/InstallTimeHigh
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Paket_*_KB*/InstallTimeLow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	Windows Registrierungseinträge
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Package_for_RollupFix*/InstallLocation
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Package_for_RollupFix*/InstallName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Package_for_RollupFix*/InstallTimeHigh
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/komponentenbasierte Services/Pakete/Package_for_RollupFix*/InstallTimeLow
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/products/*/InstallProperties/InstallLocation
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Deinstallation/*/InstallLocation
Windows - Installed Software	HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Microsoft/InetStp/SetupString
Windows - Installed Software	HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Microsoft/InetStp/VersionString
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/InstallLocation
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Adobe/Adobe Acrobat/DC/AVEntitlement/iEntitlementLevel
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayName
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Microsoft/Windows/CurrentVersion/Deinstallieren/*/DisplayVersion
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall/*/ParentDisplayName
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall/*/Publisher
Windows - Installed Software	HKEY_USERS/*/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall/*/UninstallString

Zugehörige Informationen

Discovery Befehle für Probes und Muster

Probe „WMIRunner“

„WMI Runner“ ist ein Probe-Typ, der über die Schnittstelle WMI (Windows Management Instrumentation) Daten aus Windows-Betriebssystemen abruft. IPv6 bietet Unterstützung für WMI Runner.

Die Probe verarbeitet mehrere benutzerspezifische WMI-Pfade, die abgefragt werden sollen, mit einem Basisformat einer nativen WMI-Abfrage. Alle zu prüfenden Felder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

müssen eindeutig benannt sein (innerhalb der Domäne der Probe). Die an den Sensor zurückgegebenen Probe-Ergebnisse liefern die für jedes abgefragte Feld gefundenen Daten, indiziert nach dem Namen.

Beim Erstellen einer WMI-Probe müssen der Probe-Typ auf „WMI-Probe“ und das ECC-Warteschlangenthema auf „WMIRunner“ festgelegt werden.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die WMI-Probe übergeben werden:

Parameter für die Probe „WMIRunner“

Parameter	Beschreibung	Standardwert
Quelle	Host, zu dem eine Verbindung hergestellt werden soll	
port	Port, zu dem eine Verbindung hergestellt werden soll	
debug	Aktiviert die Debug-Protokollierung	false
wmi_timeout	Zeitüberschreitung für die tatsächliche WMI-Probe in Sekunden. Mit diesem Parameter können Sie das Zeitüberschreitungsintervall für einzelne Windows-Probes ändern. Dieser Wert überschreibt den Wert im MID Server-Parameter windows_probe_timeout, der eine Zeitüberschreitung für alle von einem bestimmten MID Server gestarteten Probes festlegt. Die Probe „Windows - Installed Software“ ist mit einem Zeitüberschreitungswert von 15 Minuten konfiguriert.	300 (Sekunden)
process_timeout	Zeitüberschreitung für den das Skript ausführenden Prozess in Sekunden. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	wmi_timeout + 10 (Sekunden)
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für die Probe „WMIRunner“ (Fortsetzung)

Parameter	Beschreibung	Standardwert
	ausgegeben, auch wenn die Anmeldeinformationen erfolgreich sind. Siehe Fehlerbehebung bei Anmeldeinformationen Weitere Informationen finden Sie unter .	

Hinweis: Die Standardzeitüberschreitung für WMI/PowerShell beträgt 5 Minuten. Nur die Probe „Windows - Installed Software“ hat einen Standardzeitüberschreitungswert von 15 Minuten. Wenn Sie einem Probe-Parameter `wmi_timeout` hinzufügen, kann dies die Standardzeitüberschreitung eines Windows-Probe ändern.

Port-Sonden

Port-Probes werden in Discovery von der Shazzam-Probe verwendet, um Protokollaktivitäten an offenen Ports auf gefundenen Geräten zu erkennen.

Wenn eine Port-Probe auf ein Protokoll stößt, das verwendet wird, überprüft der Shazzam-Sensor den Port-Probe-Datensatz, um zu bestimmen, welche Klassifizierungs-Probe gestartet werden soll. Die gängigen Protokolle WMI, SSH, SNMP und HTTP im Basissystem besitzen Prioritätszahlen, die die Reihenfolge steuern, in der sie gestartet werden.

Die Priorität lautet wie folgt:

- 1 - WMI
- 2 - SSH
- 3 - SNMP
- 4 - HTTP

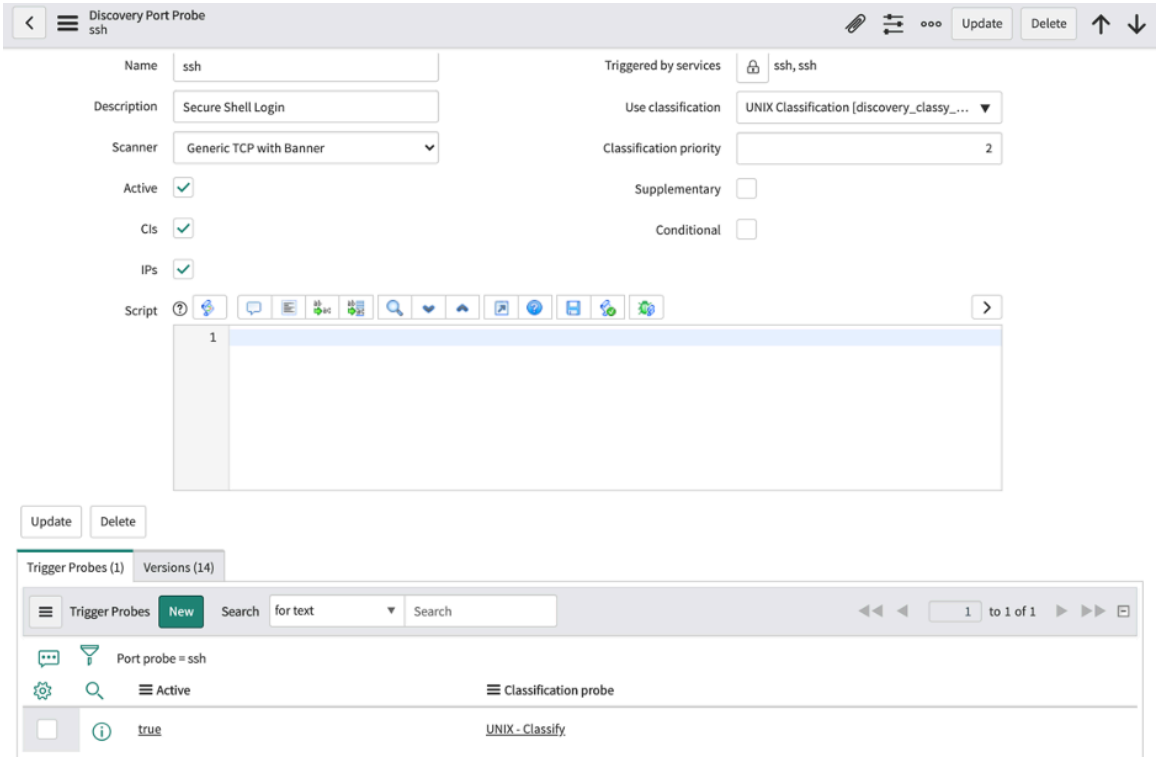
Im Basissystem wird die WMI-Probe immer zuerst gestartet. Wenn sie auf einem Gerät erfolgreich ist, werden keine anderen Port-Probes für dieses Gerät gestartet. Wenn die WMI-Probe nicht erfolgreich ist, wird die SSH-Probe gestartet, um Informationen über das Gerät zu erfassen. Wenn diese nicht erfolgreich ist, wird die SNMP-Probe gestartet. Mit dieser Methode kann Discovery Geräte ordnungsgemäß klassifizieren, wenn darauf mehrere Protokolle ausgeführt werden (zum Beispiel SSH, SNMP und HTTP).

Formular „Discovery-Anschlussprobe“

Um auf das Formular „Port-Probe“ zuzugreifen, navigieren Sie zu **Discovery-Definition** > **Anschlussprobes**an.

Um einer Port-Probe mehrere Klassifizierungs-Probes hinzuzufügen, erstellen Sie eine Verknüpfung zwischen der Port-Probe und der eigentlichen Klassifizierungs-Probe. Unten im Formular können Sie weitere Auslöser-Probes hinzufügen. Auf diese Weise wirkt sich eine fehlgeschlagene Klassifizierung nicht auf die anderen aus, sodass die Discovery-Leistung verbessert werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Formular „Anschlussprobe“ enthält die folgenden Felder:

Port-Sonden

Feld	Eingabewert
Name	Einfacher Name der Port-Probe, der ihre Funktionalität widerspiegelt (zum Beispiel SNMP)
Beschreibung	Definition des Akronyms für das Protokoll. (SSH steht zum Beispiel für Secure Shell Login.)
Scanner	Shazzam-Techniken zur Erkundung von Ports. Einige davon sind protokollspezifisch, andere generisch. Für eine WMI-Port-Probe wird beispielsweise der Scanner-Wert „Generic TCP“ und für die SNMP-Port-Probe der Wert „SNMP“ verwendet.
Aktiv	Gibt an, ob diese Port-Probe aktiviert oder deaktiviert ist
CIs	Gibt an, ob diese Port-Probe für die Erkennung von Konfigurationselementen aktiviert oder deaktiviert ist
IPs	Gibt an, ob diese Port-Probe für die Erkennung von IP-Adressen aktiviert oder deaktiviert ist
Durch Services ausgelöst	Gibt an, welche Services die Portnutzung definieren. Verwenden Sie diese Einstellung, um eine nicht standardmäßige Portnutzung zu definieren und die Portnummer an das Protokoll zu koppeln.
Klassifizierung verwenden	Benennt die entsprechende Klassifizierungstabelle basierend auf dem untersuchten Protokoll
Klassifizierungspriorität	Legt die Priorität fest, mit der die jeweilige Port-Probe ausgeführt wird. Wenn die erste Port-Probe fehlschlägt, wird die nächste Probe auf dem Gerät ausgeführt usw., bis die richtigen Daten zurückgegeben werden. Dies ermöglicht die richtige Klassifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Port-Sonden (Fortsetzung)

Feld	Eingabewert
	eines Geräts, auf dem zwei Protokolle wie SSH und SNMP ausgeführt werden. Die Standardprioritäten für die Discovery-Protokolle lauten: • 1 - WMI • 2 - SSH • 3 - SNMP • 4 - HTTP
Ergänzend	Startet zusätzliche Klassifizierungen in der Reihenfolge ihrer Priorität, nachdem eine Identifizierung mit höherer Priorität erfolgreich ausgeführt wurde
Bedingt	Führt diese Port-Probe aus, wenn eine der nicht bedingten Probes einen offenen Port zurückgibt. Die bedingten Port-Probes im Basissystem versuchen, die Namen von Windows-Geräten und DNS-Namen aufzulösen. Diese Port-Probes benötigen zusätzliche Ressourcen und werden nur verwendet, wenn Aktivität an offenen Ports erkannt wurde.
Skript	Auszuführendes Skript.

Shazzam-Probe, Port-Probes und Protokolle

Port-Scans ist der erste Schritt im Discovery-Prozess. Die Shazzam-Probe führt Port-Scans durch, und zwar unabhängig davon, ob Sie Muster für die horizontale Erkennung verwenden. In der folgenden Tabelle sind die bekannten Ports und Protokolle aufgeführt, die von verwendet werden Discovery.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (August 2024 Store), können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Und verwenden Sie das erweiterte Dashboard.

Im Basissystem sind mehrere Port-Probes verfügbar. Jede Port-Probe verwendet einen IP-Service, einen Datensatz, der angibt Discovery Welcher Port für ein bestimmtes Protokoll verwendet werden soll. Prüfen Sie diese Tabelle, bevor Sie Ports mit einer Firewall blockieren.

Wichtig: Stellen Sie sicher, dass Sie keine Ports blockieren, die Discovery Benötigt.

Standard-Port-Probes und -IP-Services

Name der Standard-Port-Probe	Geräteklassifizierung	Standard-IP-Service und -Port
dns	Prozessklassifizierung [discovery_classy_proc]	dns (Port 53)
http	HTTP-Klassifizierung [discovery_classy_http]	http (Port 80) und https (Port 443)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Port-Probes und -IP-Services (Fortsetzung)

Name der Standard-Port-Probe	Geräteklassifizierung	Standard-IP-Service und -Port
ip_phone	SNMP-Klassifizierung [discovery_classy_snmp]	sip (Port 5060)
osx	Applikationsklassifizierung-Ergebnisse scannen [discovery_classy_scan_app]	afp (Port 548)
Drucker	Applikationsklassifizierung-Ergebnisse scannen [discovery_classy_scan_app]	hp-pdl-datastr (Port 9100) und printer (Port 515)
slp	Prozessklassifizierung [discovery_classy_proc]	slp (Port 427)
snmp	SNMP-Klassifizierung [discovery_classy_snmp]	snmp (Port 161)
ssh	UNIX-Klassifizierung [discovery_classy_unix]	ssh (Port 22)
tls_ssl_certs		tls_ssl_certs • SSL-Ports: 443, 8443, 9443, 636 (ldaps), 993 (imaps), 995 (popssl), 989, 990 • StartTLS-Ports: 25 (smtp), 110, 143, 389, 21, 587 (smtp)
vmapp	Anwendungsklassifizierung [discovery_classy_appl]	vmapp_https (Port 5480) und vmapp6_https (Port 9443)
wbem	CIM-Klassifizierung [discovery_classy_cim]	wbem_https (Port 5989)
winrm	Windows-Klassifizierung [discovery_classy_windows]	winrm (Port 5985) und winrm_ssl (Port 5986)
wins	Prozessklassifizierung [discovery_classy_proc]	ms-nb-ns (Port 137)
wmi	Windows-Klassifizierung [discovery_classy_windows]	epmap (Port 135)

Diese Tabelle zeigt andere gängige Ports und Protokolle, die Discovery Verwendet.

Discovery-Ports und -Protokolle

Name	Servicename	Port	Details	Erstellen/ Einfügungen	Protokoll
afp	Apple File Protocol	548			TCP
BEA-Weblogik		7001		cmdb_ci_app_server	TCP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Ports und -Protokolle (Fortsetzung)

Name	Servicename	Port	Details	Erstellen/ Einfügungen	Protokoll
dns	Domain Name Service	53	Zum Auflösen des Namens jeder IP-Adresse		TCP/ UDP
epmap	Microsoft RPC (WMI, DCOM)	135	Windows-Systeme		TCP
ftp		21			TCP
hp-pdl-datastr	Printer PDL Data Stream	9100	HP-Drucker		TCP
http	HyperText Transfer Protocol	80	Webserver	cmdb_ci_web_server	TCP
https	HyperText Transfer Protocol over Secure Socket	443	Sichere Webserver	cmdb_ci_web_server	TCP
IBM DB2		50000			TCP
IBM MQSeries		1414			TCP
IBM Websphere		9080			TCP
IBM Web sphere SSL		9443			TCP
IMAPS		993			TCP
pip (Internet Print Protocol)	IP Phone/ Session Initiation Protocol	5060			TCP
LDAP		389			TCP
LDAPs		636			TCP
Microsoft NetBIOS		139			TCP
Microsoft-ds		445			TCP
ms-nb-ns		137			UDP
Microsoft SQL server		1433			TCP
MySQL		3306			TCP
Nagios NRPE		5666			TCP
NFS		2049			TCP/ UDP
Oracle TNS		1521			TCP
POP3		110			TCP
postgresql		5432		cmdb_ci_database	TCP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Ports und -Protokolle (Fortsetzung)

Name	Servicename	Port	Details	Erstellen/ Einfügungen	Protokoll
Drucker	Drucker	515	Drucker		TCP
sip	SIP (Session Initiation Protocol)	5060			TCP
slp	Service Location Protocol (SLP)	427			TCP/ UDP
smtp	TCP	25			
smux (SNMP Multiplexing)		199			
snmp	Simple Network Management Protocol	161	Netzwerkgeräte		UDP
snmptrap		162			UDP
ssh	Secure Shell Service	22	Unix-Systeme		TCP
sunrpc		111			TCP
telnet		23			TCP
TIBCO Rendezvous		7500			TCP
Tomcat HTTP		8080			TCP
vmapp6_https		9443			TCP
vmapp_https	vCenter Server Appliance Web Interface mit https	5480			TCP
wbem_https	CIM-XML über HTTPS (WBEM)	5989	CIM-Klassifizierung		TCP
wins	Windows Internet Name Service	137	NetBIOS-Namensauflöser		UDP

Windows Und dynamische Ports

Unterstützt Windows Computer können dynamische Portbereiche aufweisen: 49152-65535 für TCP und UDP.

Shazzam-Probe konfigurieren

Wenn Sie Discovery ausführen, erkennt die Shazzam-Probe Ihre aktiven Netzwerkgeräte, indem sie bestimmte Ports in bestimmten IP-Adressbereichen scannt. Wenn die Liste der zu scannenden IP-Bereiche groß ist, können Sie die Shazzam-Nutzlast für die JSON-Codierung konfigurieren, um ihre Größe zu reduzieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können das Verhalten einzelner Shazzam-Probes mit grundlegenden und erweiterten Parametern steuern. Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Shazzam-Nutzlast wird durch Folgendes gesteuert MID-Server-Eigenschaften . Diese Eigenschaften müssen dem MID Server nicht hinzugefügt werden. Die Shazzam-Probe greift auf ihre Standardwerte zurück.

- Die Eigenschaft **shazzam.chunk_size** steuert die maximale Anzahl von IP-Adressen, die Shazzam parallel scannen kann.
- Die Eigenschaft **mid.shazzam.regulator.interval_ms** legt das Intervall fest, in dem Shazzam Pakete starten kann.
- Die Eigenschaft **mid.shazzam.regulator.packets_per_interval** legt die Anzahl von Paketen fest, die Shazzam im Zeitintervall starten kann.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**an.
2. Wählen Sie **Shazzam** aus.
3. Fügen Sie der zugehörigen Liste **Probe Parameter** Parameter hinzu, oder bearbeiten Sie sie.
4. Konfigurieren Sie die Shazzam-Parameter.
   Zur Feinabstimmung der Shazzam-Probe stehen die folgenden Parameter zur Verfügung. Die folgenden Werte sind nur im Probe-Datensatz definiert.

Erweiterte Shazzam-Parameter

Parameter	Beschreibung
BannerTCP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner BannerTCP auf die Herstellung einer Verbindung wartet **Standardwert**: 1500
debug	Aktiviert bei Einstellung auf **true** die Debug-Protokollierung **Standardwert:** false
delay_wbem	Verzögert die Klassifizierung von Systemen mit einem offenen WBEM-Port bis zum endgültigen Shazzam-Sensorauftrag. Bei einem umfangreichen Zeitplan, der viele WBEM-Ports erkennt, kann die Verzögerung der Klassifizierung bis zum letzten Sensorauftrag dazu führen, dass dem Knoten nicht mehr genügend Arbeitsspeicher zur Verfügung steht. Wenn Sie diesen Parameter auf **false** setzen, kann die Klassifizierung dieser Systeme für alle Shazzam-Sensoraufträge erfolgen. **Standard**: true
DNS_alternativePort	Überholt
DNS_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner DNS auf eine Antwort wartet **Standardwert**: 1000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
GenericTCP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner GenericTCP auf die Herstellung einer Verbindung wartet **Standardwert**: 1000
HTTP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner HTTP auf die Herstellung einer Verbindung wartet **Standardwert**: 500
HTTP_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner HTTP auf eine Antwort wartet **Standardwert**: 500
NBT_alternativePort	Überholt
NBT_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner NBT auf eine Antwort wartet **Standardwert**: 500
Shazzam_Report_inactive	Bei **true** werden Geräte gemeldet, die zwar eingeschaltet, aber inaktiv sind. Beispiel: Ein Gerät weist keine offenen Ports auf, lehnt jedoch mindestens eine Portverbindungsanforderung ab. **Standard**: true
scanner_log	Aktiviert bei Einstellung auf **true** die Scannerprotokollierung Diese Protokollierungsinformationen werden in der Antwort der Shazzam-Probe angezeigt. **Standardwert:** false
shazzam_report_dead	Bei **true** werden Geräte mit inaktiven IP-Adressen gemeldet. Etwa ein Gerät, bei dem alle Ports geschlossen sind **Standardwert:** false
SNMP_alternativePort	Überholt
SNMP_tapIntervalMS	Legt die Anzahl von Millisekunden fest, die der Scanner SNMP zwischen Taps wartet **Standardwert**: 1000
SNMP_taps	Legt die Anzahl der Taps (Anforderungen) fest, die der Scanner SNMP versucht **Standardwert**: 2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
SNMP_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner SNMP nach dem letzten Tap auf eine Antwort wartet **Standardwert**: 1000
TLS_keepOriginalCertificate	Wenn Discovery bei der Einstellung **true** ausgeführt wird, wird das Feld certificate_file in cmdb_ci_certificate mit dem ursprünglichen Zertifikat gefüllt. Beachten Sie, dass sich dadurch die Nutzlastgröße erhöhen kann. **Standardwert:** false

Shazzam-Nutzlastgröße steuern

Eine Systemeigenschaft konvertiert Shazzam-Nutzlasten in JSON-Zeichenfolgen, wodurch deren Größe erheblich reduziert wird. Diese Einstellung verhindert, dass Knoten bei der Erkennung einer große Anzahl von IP-Bereichen durch einen einzelnen Zeitplan der Arbeitsspeicher ausgeht.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Eigenschaft glide.discovery.shazzam_ranges_json wird für neue Instanzen auf true gesetzt. Diese Einstellung codiert die Nutzlast als JSON-Zeichenfolge. Die Eigenschaft kann von Administratoren konfiguriert werden und ist in verfügbar **Discovery-Definition** > **Eigenschaften** Modul. Die Eigenschaftsbezeichnung im Modul lautet **Verwenden Sie JSON für IP-Bereiche in Shazzam**.

In upgegradeten Instanzen ist diese Eigenschaft auf false festgelegt und standardmäßig nicht sichtbar. Durch das manuelle Hinzufügen der Eigenschaft zu Ihrer aktualisierten Instanz wird die Funktion aktiviert, aber nicht zu hinzugefügt **Discovery-Definition** > **Eigenschaften** Modul. Um die JSON-Codierung zu aktivieren und dem Modul hinzuzufügen, importieren Sie den Update Set, das Sie über KB0687626 erhalten.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein, und drücken Sie die Eingabetaste.
2. Klicken Sie in der Liste der Systemeigenschaften auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Feldwerten aus:
   - **Name**: glide.discovery.shazzam_ranges_json
   - **Beschreibung**: Codiert die Shazzam-Nutzlast in JSON
   - **Wert**: true
4. Klicken Sie auf **Absenden**.

Discovery-Sensoren

Jede Probe in Discovery muss über einen entsprechenden Sensor zur Verarbeitung der zurückgegebenen Daten verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wenn eingehende Daten das Ergebnis einer WMI-Probe sind, wird der WMI-Sensor zur Verarbeitung der Nutzlast ausgelöst.

Hinweis: Wenn Sie eine Multi-Probe erstellen, müssen Sie einen Multisensor erstellen, um die von dieser Probe zurückgegebenen Daten zu verarbeiten. Weitere Informationen finden Sie unter Multi-Probes und Multisensoren.

Navigieren zu **Discovery** > **Discovery-Definition** > **Sensoren** Und bearbeiten oder erstellen Sie einen Sensor.

Tabelle der Sensorfelder

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Probe-Namen ein.
Reagiert auf Probe	Wählen Sie die Probe aus, deren Nutzlast dieser Sensor verarbeiten muss.
Sensorklasse [sys_class_name]	Wählen Sie den Typ des zu erstellenden Sensors aus: • Import-Export-Zuordnung: Diese Option wird derzeit nicht verwendet. • MultiSensor: Multisensoren verarbeiten die Daten, die von Multi-Probes zurückgegeben werden. Wählen Sie diesen Typ aus, um einen Multisensor zu erstellen, der auf die in einer Multi-Probe verwendeten einfachen Probes antwortet. • Sensor: Wählen Sie diesen Typ aus, wenn es sich bei dem Sensor um einen einfachen Sensor handelt, der auf eine einfache Probe antwortet.
Beschreibung	Geben Sie eine optionale Beschreibung der Sensorfunktion ein.
Sensortyp [sensor_type]	Geben Sie an, wie die Ergebnisse der Probe verarbeitet werden. • Klassifizierung: Dieses Feld wird derzeit nicht verwendet. • Java: Dieses Feld wird derzeit nicht verwendet. • Javascript: Von einer Probe zurückgegebene Daten werden außerhalb der Anwendung im Sensor selbst verarbeitet und sind für den Benutzer sichtbar. Dies ist der gängigste Sensortyp. • Mehrzeiliger Text: Dieses Feld wird derzeit nicht verwendet. • XML: Die XML-Daten der Probe sind in Teile zerstückelt. Einige Teile können zum Starten anderer Probes verwendet werden, die der ursprüngliche Sensor benötigt, um alle erforderlichen Informationen über ein Gerät zu füllen.
Aktiv	Wählen Sie diese Option aus, um den Sensor zu aktivieren oder zu deaktivieren.
Skript	Geben Sie das Skript ein, das bei der Verarbeitung der Probe ausgeführt werden soll. Sie können in einem Sensorskript die Hashmap g_probe_parameters verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispielsweise wird durch diesen Code der Parameter *node_port* für alle ausgelösten Probes auf 16001 festgelegt. `g_probe_parameters['node_port']=16001;`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle der Sensorfelder (Fortsetzung)

Feld	Beschreibung
Reagiert auf Probes	Verwenden Sie diese zugehörige Liste, um die einfache Probe in einer Multi-Probe anzugeben, deren Nutzlast dieser Multisensor verarbeiten muss. Diese Liste ist nur für Multisensoren verfügbar.
Auslösertests	Verwenden Sie diese zugehörige Liste, um anzugeben, welche Probes dieser Sensor für zusätzliche Erkundungen starten kann.
Die folgenden Felder können durch Konfiguration des Formulars hinzugefügt werden:	
Feld	Beschreibung
Agent	Geben Sie den ECC-Warteschlangentyp ein, mit dem dieser Sensor abgeglichen werden soll.
Standardeinstellungen übernehmen	Wählen Sie diese Option aus, um die Standardwerte des Sensors zu übernehmen.
Klassifizierungstyp	Wählen Sie den Klassifizierungstyp aus, der dem Sensor zugeordnet ist.
Zusammenfügen	Geben Sie das Feld für den Abgleich ein, anhand dem bestimmt wird, ob eine Zusammenfügung erfolgen soll.
Bedingungsskript	Erstellen Sie eine vordefinierte Anforderung für die Ausführung dieses Sensors.
Datenoption	Wählen Sie aus, wie importierte Sensordaten behandelt werden sollen. Verfügbare Optionen: • Einfügen und Aktualisieren • Nur einfügen • Nur aktualisieren
Externe Namen	Geben Sie einen Namen ein, um die Sensordaten zu kennzeichnen.

Sensortransaktion abhängig von der Dauer abbrechen

Standardmäßig bricht diese Regel die Sensortransaktion ab, wenn die Ausführung länger als 20 Minuten dauert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Ausführung der Discovery-Sensortransaktion länger als 20 Minuten dauert, werden die folgenden Aktionen ausgeführt:

- Der zugeordnete Eingabedatensatz der ECC-Warteschlange wird auf den Fehlerstatus festgelegt.
- Die *`Anzahl der Erkennungen mit abgeschlossenem Status`* wird aktualisiert.
- Fehlermeldungen werden protokolliert, zum Beispiel:

```
Sensor error when processing Linux - Storage: Transaction cancelled: maximum execution time exceeded
```

- Die Erkennung wird fortgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Verhalten ist die Folge der Transaktionsmengenregel für Discovery-Sensoren. Diese Regel ist standardmäßig aktiviert.

Sie können die Regel deaktivieren, und Sie können die Zeitspanne ändern, die verstreichen soll, bevor die Regel in Kraft tritt. Für den Zugriff auf diesen Datensatz ist die Administratorrolle erforderlich.

Prozedur

1. Um die Regel zu deaktivieren, navigieren Sie zu **Systemdefinition** > **Mengenregeln**an.
   Das Plugin **Transaction Quotas** muss aktiv sein.
2. Suchen Sie nach dem Namen `*Discovery`, um die Regelliste zu filtern.
3. Klicken Sie in der Namensspalte auf **Discovery-Sensoren**.
4. Um die Zeitspanne zu ändern, bearbeiten Sie das Feld **Höchstdauer** für die Regel.
   Der Wert wird in Sekunden angegeben.

Erkennungs-Probes verwalten

In Discovery sind zahlreiche Erkennungs-Probes und zugehörige Sensoren enthalten. Probes oder Sensoren müssen nur selten geändert werden. Möglicherweise müssen Sie jedoch Parameter festlegen, um das Verhalten einer bestimmten Probe zu steuern oder Versionen benutzerdefinierter Probes ausrichten.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Vorgehensweise

Mit Probes und Sensoren sind folgende Aktionen möglich:

Probes des Basissystems überprüfen

Informationen über im Basissystem vorhandene Probes finden Sie in der Liste der Discovery-Probes. Probes müssen für Klassifizierer aktiv sein, damit Discovery die Probes auslösen kann. Allerdings sind nicht alle Probes für Klassifizierer aktiv, da Probes und Sensoren durch immer mehr Muster ersetzt werden. Eine Liste von Mustern finden Sie unter Verfügbare Discovery-Muster .

Probes erstellen oder ändern

Sie können eine neue Probe erstellen, um zusätzliche CIs zu erkennen, die Discovery mit den Probes oder Mustern des Basissystems nicht erkennen kann. Sie können aber auch vorhandene Probes ändern, um zusätzliche Informationen zum CI-Typ zu sammeln. Nachdem Sie eine Probe erstellt oder geändert haben, testen Sie sie. Sie können auch Multi-Probes und Multisensoren erstellen. Weitere Informationen finden Sie unter Discovery-Multi-Probe erstellen.

Upgrade auf die neueste Version einer Probe oder eines Sensors durchführen

Wenn Sie Ihre Instanz upgraden, wird auch Discovery zusammen mit Komponenten wie Probes und Sensoren aktualisiert. Probes und Sensoren, die Sie angepasst haben, werden jedoch nicht aktualisiert. Sie müssen die Anpassungen in eine Textdatei kopieren, die Probes und Sensoren aktualisieren und danach die Anpassungen erneut anwenden. Weitere Informationen finden Sie unter Versionen benutzerdefinierter Probes und Sensoren angleichen.

Probe-Parameter festlegen

Probe-Parameter steuern verschiedene Aspekte der Funktionsweise von Probes. Da alle Probes im Basissystem bereitgestellt werden, sind bestimmte Parameter zulässig. Diese sind in der Liste der Discovery-Probes angegeben. Unter Probe-Parameter festlegen finden Sie Anweisungen zum Festlegen von Parametern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe-Berechtigungen prüfen

Für bestimmte Probes sind Berechtigungen erforderlich, damit Sie für die Zielcomputer und CIs ausgeführt werden können, die zur Erkennung vorgesehen sind. Weitere Informationen finden Sie unter Berechtigungen für Discovery-Probes.

Probes erstellen oder ändern

Erstellen Sie eine neue Probe zur Erkennung zusätzlicher CIs, oder ändern Sie eine vorhandene Probe, um zusätzliche Informationen zu erfassen. Nachdem Sie eine Probe erstellt oder geändert haben, testen Sie sie.

Vorbereitungen

Erforderliche Rolle: Administrator

Wichtig: Sie benötigen fortgeschrittene Skriptkenntnisse, um Sonden oder die zugehörigen Sensoren zu modifizieren. Viele vorhandene Sonden bieten Parameter, die Sie einstellen können, anstatt die Sonde selbst zu ändern. Weitere Informationen finden Sie unter Probe-Parameter festlegen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Probes**an.
2. Klicken Sie auf den Namen der Probe, die Sie ändern möchten.
3. Ändern Sie die Formularfelder (siehe Tabelle).

Feld	Beschreibung
Klasse	Wählen Sie die Probe für das Betriebssystem des abzufragenden Geräts aus. ○ AWS-Test: Wählen Sie diese Klasse aus, um Ihre Ressourcen in einer AWS-Cloud abzufragen. ○ **CIM-Test**: Wählen Sie diesen Probe-Typ aus, um einen CIM-Server mit WBEM-Protokollen abzufragen. ○ **Mehrfachprobe**: Wählen Sie diesen Probe-Typ aus, um eine oder mehrere einfache Probes eines beliebigen Typs auszuführen oder Probes verschiedener Typen zu mischen. Dieser Probe-Typ kann mehrere Abfragen gleichzeitig ausführen, die alle Ergebnisse gleichzeitig zurückgeben. Es ist nicht möglich, Multi-Probes zu anderen Multi-Probes hinzuzufügen. ○ **Probe**: Wählen Sie diesen generischen Typ aus, um eine Probe-Klasse zu definieren. Geben Sie den Namen der Probe-Klasse im Feld *ECC-Warteschlangenthema* an. ○ **SNMP-Probe**: Wählen Sie diesen Probe-Typ für Netzwerkgeräte wie Router aus. ○ **WMI-Probe**: Wählen Sie diesen Probe-Typ für Windows-Geräte aus.
ECC-Warteschlangenthema	Geben Sie einen beschreibenden Begriff für die Funktionsweise der Probe ein. Die Probe verwendet diese Bezeichnung als Feld **Thema** für eingehende ECC-Warteschlangennachrichten. Der Begriff muss nicht eindeutig sein. Beispielsweise können alle UNIX-Probes für das ECC-Warteschlangenthema den Wert **SSHCommand** aufweisen. Standardmäßig verwenden Probes die folgenden ECC-Warteschlangenthemen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ CimProbe ◦ Multi-Probe ◦ PowerShell-Probe ◦ SCPRelay ◦ SSHCommand ◦ SNMP ◦ WMIRunner
ECC-Warteschlangenname	Geben Sie entweder einen beschreibenden, für Benutzer verständlichen Namen oder den tatsächlichen Befehl ein, den die Probe ausführen soll. Beispiel: Wenn der Wert im Feld für das ECC-Warteschlangenthema **SSHCommand** lautet, geben Sie den tatsächlichen Shell-Befehl zur Ausführung in dieses Feld ein.
Cache-Ergebnisse	Wählen Sie diese Option aus, um die Ergebnisse dieser Probe zwischenzuspeichern und die Erkennungsleistung insgesamt zu verbessern. Der Cache für Probe-Ergebnisse sollte nur für die Probes und Sensoren aktiviert werden, deren Ausgabe sich wahrscheinlich nicht ändert. Beispielsweise werden Ergebnisse des Sensors „Linux - CPU“ zwischengespeichert, da sich CPU-Informationen nur selten ändern. Der Cache ist standardmäßig für Probes und Sensoren im Basissystem aktiviert, deren Ausgabe sich wahrscheinlich nicht ändert. ⚠ **Warnung:** Aktivieren Sie den Cache weder für Klassifizierungs-Probes noch für Identifizierungs-Probes. Darüber hinaus sollten Sie den Cache nicht für Probes aktivieren, die zusätzliche Probes auslösen, da deren Auslösung dadurch möglicherweise verhindert wird.
Klassischer Modus	Wählen Sie diese Option aus, um die Ergebnisse dieser Probe zwischenzuspeichern. Wählen Sie diese Option aus, um das Nachverarbeitungsskript auf der ServiceNow-Instanz anstatt auf dem MID Server zu debuggen. Dieser Modus ist nur gültig, wenn ein Postprozessorskript vorhanden ist. Verwenden Sie den klassischen Modus zum Debuggen von Nachverarbeitungsskripts in der Testumgebung. Von der Verwendung des klassischen Modus in der Produktionsumgebung rät ServiceNow ab.
Postprozessorskript	Definieren Sie ein optionales Nachverarbeitungsskript, das auf dem MID Server ausgeführt wird. Das Skript akzeptiert Probe-Ergebnisse als Eingabe und gibt eine JSON-Zeichenfolge aus, die an die Instanz zurückgesendet wird, damit sie von Sensoren als Eingabe verwendet werden kann. Verwenden Sie diese Art von Skript, um Aufgaben wie das Analysieren von Daten durchzuführen. Alle Probe-Nachverarbeitungsskripts und deren zugehörigen Sensoren haben Zugriff auf die folgenden globalen Variablen: ◦ `current`: Legt das Attribut als aktuell fest. Dieselbe Funktionalität ist auch für Sensoren verfügbar. Dabei handelt es sich um Attribute des erkannten Geräts. ◦ `related_data`: Alle zusätzlichen Daten, die von den Nachverarbeitungsskripts der Probes übergeben werden sollen, zum Beispiel `related_list` Alle Probe-Nachverarbeitungsskripts und deren zugehörigen Sensoren haben Zugriff auf die folgenden Methoden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ log(string): Protokolliert die Zeichenfolge zum MID Server und zu den ServiceNow-Instanzprotokolldateien ○ getParameter(param): Ruft den Parameter aus der Nutzlast der ECC-Warteschlange ab

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Ändern Sie diese zugehörigen Listen bei Bedarf.

Zugehörige Liste	Beschreibung
Probe Parameter	Parameter, die die Funktionalität von Probes steuern. Anweisungen dazu finden Sie unter Probe-Parameter festlegen.
Sensoren, die auf diese Probe reagieren	Die Sensoren, die von dieser Probe verwendet werden
Enthalten in MultiProbe	Gibt an, ob diese Probe mit anderen Probes als Multi-Probe enthalten ist
MultiSensor-Skripts	Skripts, die für mehrere Sensoren ausgeführt werden
Versionen	Die Version der Probe. Wenn **Status** auf **Aktuell** festgelegt ist, stellt die Probe die aktuelle Version der Instanz dar. Andernfalls haben Sie nicht die aktuelle Version und müssen möglicherweise eine Neuausrichtung durchführen. Anweisungen dazu finden Sie unter Versionen benutzerdefinierter Probes und Sensoren angleichen.

6. Klicken Sie auf **Probe testen**.
7. Geben Sie im Fenster „Probe testen“ die IP-Adresse des Ziels ein, und wählen Sie den MID Server aus. Nur MID Server, die den Status **In Betrieb** und **Validiert** aufweisen, können ausgewählt werden.
8. Klicken Sie auf **OK**.
9. Prüfen Sie die ECC-Warteschlange für den MID Server, und zeigen Sie die Ergebnisse an.

Nächste Maßnahme

Fügen Sie der zugehörigen Liste **Löst Probe aus** die Probe des entsprechenden Klassifizierers hinzu. Unter Discovery-CI-Klassifizierung erstellen finden Sie Beschreibungen der Felder und zugehörigen Listen im Klassifiziererformular.

Berechtigungen für Discovery-Probes

Zur Ausführung diverser Probes sind zusätzliche Berechtigungen erforderlich.

Aktive Verbindungen erkennen

Discovery verwendet die Probe „Windows - Active Connections“, um Informationen über aktive Verbindungen abzurufen. Für die Funktion Application Dependency Mapping muss diese Probe funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktive Verbindungen erkennen

Probes	Zusätzliche Berechtigungen
Windows - Active Connections	Fähigkeit zum Aufrufen des Objekts *\root\CIMV2:Win32_Process* Lese- und Schreibzugriff auf die Freigabe $admin

Anwendungsprofile erkennen

Discovery verwendet die folgenden Probes für den Zugriff auf Informationen über Anwendungsprofile.

Anwendungsprofile erkennen

Probes	Zusätzliche Berechtigungen
Windows - Get APD Environment Files Windows - Get APD Env File Content Windows - Get APD Version File Content	Fähigkeit zum Aufrufen des Objekts *\root\CIMV2:Win32_Process* Lese- und Schreibzugriff auf die Freigabe $admin Schreibzugriff auf das Verzeichnis %SystemRoot%\temp

VMware-Workstations erkennen

Discovery verwendet die Probe **Windows - Get VMware Workstation**, um Informationen über unter Windows installierte virtuelle VMware-Computer abzurufen.

VMware-Workstations erkennen

Probes	Zusätzliche Berechtigungen
Windows - Get VMware Workstation	Fähigkeit zum Aufrufen des Objekts *\root\CIMV2:Win32_Process* Lese- und Schreibzugriff auf die *admin$ share* Schreibzugriff auf das Verzeichnis *%SystemRoot%\temp* Konfigurieren Sie die **PATH**-Variable so, dass sie den Pfad zum Befehl vmrun.exe enthält. Dieser Befehl befindet sich normalerweise im Installationsverzeichnis der VMware-Workstation.

MSSQL erkennen

Discovery verwendet die Probe „Windows - MSSQL“, um Informationen über unter Windows installierte Microsoft SQL Server abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSSQL erkennen

Probes	Zusätzliche Berechtigungen
Windows - MSSQL	• Zugriff auf das Objekt *Win32_Process* • Zugriff auf das Objekt *Win32_Service* • Zugriff auf das Objekt *Win32_NetworkAdapterConfiguration* • Zugriff auf das Objekt *Microsoft.SqlServer.Management.Smo* • Berechtigung zum Ausführen des Befehls *nbtstat* • Zugriff auf HKLM\SOFTWARE\Microsoft\Microsoft SQL Server \InstalledInstances • Zugriff auf HKLM\SOFTWARE\Microsoft\MSSQLServer\$instanceName \SuperSocketNetLib\Tcp\TcpPort, wobei *$instanceName* einem Array möglicher Werte entspricht.

Zugehörige Informationen

Discovery Befehle für Probes und Muster

Probe-Parameter festlegen

Verwenden Sie Probe-Parameter, um das Verhalten einer bestimmten Probe bei jeder Auslösung zu steuern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Parameter sind für alle Probe-Typen verfügbar:

Parameter	Beschreibung
Quelle	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll • Typ: Zeichenfolge (URL) • Standardwert: keiner

Prozedur

1. Erstellen Sie die Probe, oder wählen Sie diejenige, für die Sie Parameter festlegen möchten.
2. Klicken Sie in der zugehörigen Liste *Probe Parameter* auf **Neu**.
3. Füllen Sie die Felder entsprechend aus (siehe Tabelle).

Das Formular „Probe Parameter“ enthält die folgenden Felder.

Felder im Formular „Probe Parameter“

Feld	Beschreibung
Name	Geben Sie den Parameternamen ein. Jeder Probe-Typ besitzt eine eigene Liste verfügbarer Parameter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wert	Geben Sie den Parameterwert oder das Skript gemäß den Anforderungen des Parameters ein.
Wertskript	[Optional] Geben Sie das Skript ein, das der Parameter ausführen soll, wenn Sie im Feld *Wert* noch kein Skript angegeben haben.
Probe	Zeigt die Probe an, auf die sich dieser Parameter bezieht.

Versionen benutzerdefinierter Probes und Sensoren angleichen

Wenn Sie eine Probe oder einen Sensor angepasst und auf eine neue Version einer Instanz aktualisiert haben, müssen Sie die Versionen der/des benutzerdefinierten Probe und Sensors auf die aktuelle Version angleichen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Probes und Sensoren weisen eine Haupt- und eine Nebenversion auf.

Hauptversion

Eine umfassende Versionsänderung spiegelt eine Änderung in der erwarteten Ausgabe einer Probe wider, zum Beispiel das Hinzufügen oder Entfernen eines Zielattributs, eine Formatänderung, zum Beispiel XML oder JSON, oder eine Änderung eines Probe-Parameterskripts.

Nebenversion

Eine geringfügige Versionsänderung bezieht sich auf kleine Korrekturen, die sich nicht auf das Ergebnis oder die Verarbeitung der Daten auswirken.

Ein Sensor und die entsprechende Probe müssen dieselbe Hauptversion aufweisen. Es wird empfohlen, dass sie auch dieselbe Nebenversion haben. Durch diesen Versionsabgleich wird sichergestellt, dass die von der Probe zurückgesendeten Daten vom Sensor verstanden und ordnungsgemäß verarbeitet werden. Alle Mitglieder eines Multi-Probe-Bündels müssen dieselbe Haupt- und Nebenversion aufweisen.

Standardmäßig verfolgt Discovery schwerwiegende Versionsabweichungen und zeigt Versionsabweichungen im Abschnitt aktive Discovery-Fehler an In Discovery-Protokoll . Sie können festlegen, ob Discovery Nichtübereinstimmungen der Nebenversion nachverfolgt, indem Sie die Discovery-Eigenschaft **Bei geringfügigen Versionskonflikten warnen** (glide.discovery.warn_minor_version) aktivieren. Nichtübereinstimmungen der Nebenversion werden im Discovery-Protokoll nachverfolgt, aber nicht im Discovery-Dashboard angezeigt.

Versionen für Multi-Probes und Multisensoren werden wie folgt geprüft:

- Die Versionen der einzelnen Probes, die in Multi-Probes enthalten sind, werden mit den „Reagiert auf Probes“-Skripts verglichen, die ihre Daten verarbeiten.
- Die Versionen der „Reagiert auf Probes“-Skripts und des Multisensor-Hauptskripts werden verglichen.

Wenn eine Probe und der entsprechende Sensor nicht dieselbe Hauptversion besitzen, verarbeitet der Sensor während einer Erkennung keine Informationen, sondern sendet Fehlermeldungen an die Protokolldatei. Fehler werden auch im Discovery-Dashboard angezeigt, wenn Sie einen Erkennungsauftrag ausführen. Wenn die Hauptversion identisch ist, die Nebenversion jedoch nicht, werden von einem Sensor während einer Erkennung Informationen verarbeitet.

So verwenden Sie die aktuellste Version einer Probe, die verfügbar ist:

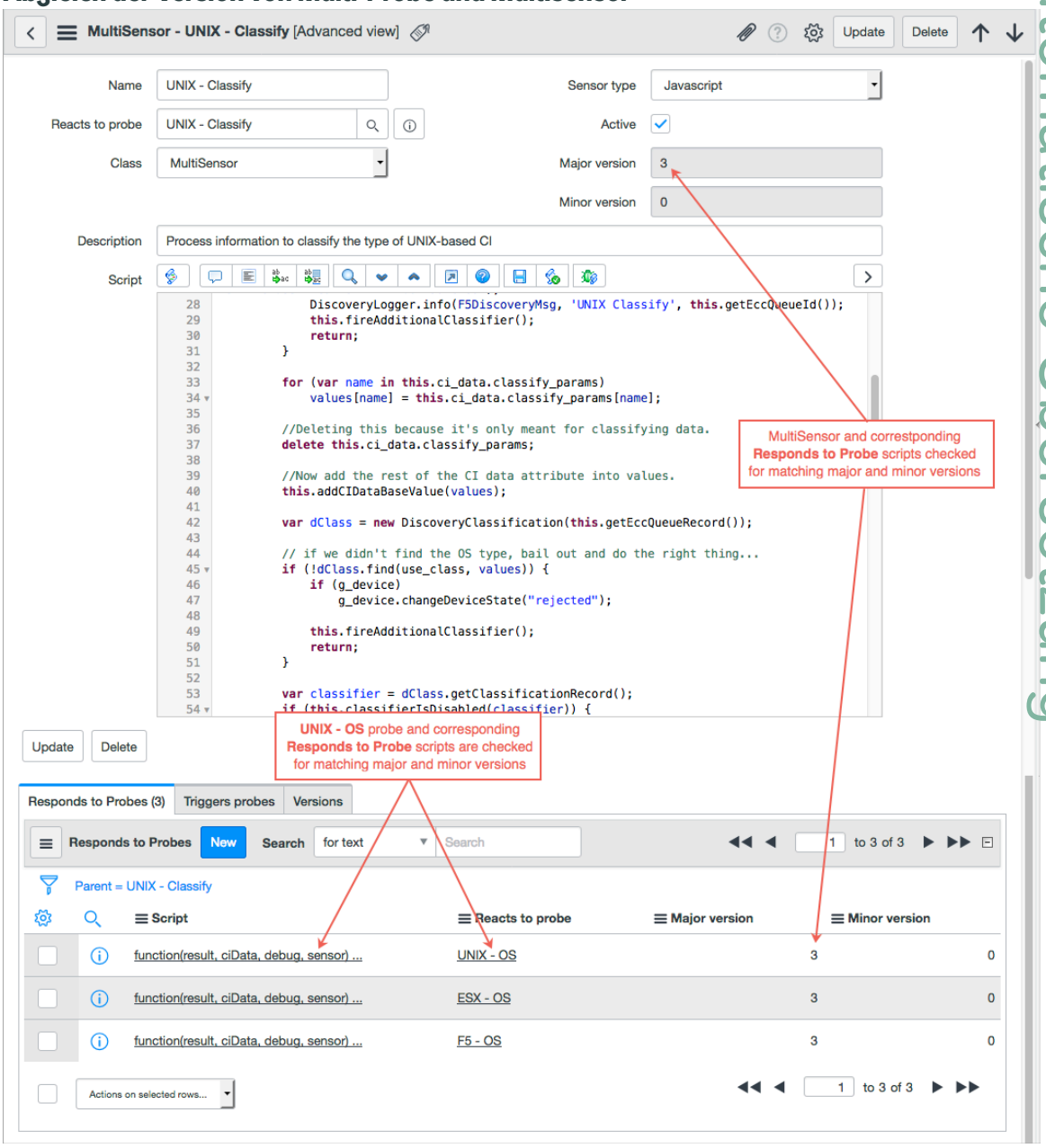
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Speichern Sie die Anpassungen, die Sie an einer Probe/einem Sensor vorgenommen haben, in einer Textdatei, um sie später erneut anwenden zu können.
2. Navigieren zu **Discovery** > **Dashboard**an.
3. Suchen Sie im Abschnitt **Aktive Discovery-Fehler** nach Versionskonflikten, und notieren Sie die Probe oder den Sensor, die/der den Fehler verursacht hat.
4. Navigieren zu **Discovery-Definition** > **Probes** oder **Discovery-Definition** > **Sensoren** Und wählen Sie die Probe oder den Sensor aus, die bzw. den Sie aktualisieren möchten.
5. Fügen Sie dem Formular die Felder **Hauptversion** und **Nebenversion** hinzu, wenn Sie die Versionen im Formular anzeigen möchten.
6. In einem Multisensor können Sie die Hauptversion anhand der Versionen der Probes in der zugehörigen Liste **Reagiert auf Probes** überprüfen, die den Sensor verwenden.

Abgleich der Version von Multi-Probe und Multisensor



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf die zugehörige Liste **Versionen**.
8. Suchen Sie nach einer Version, deren **Status** gleich **Zurück** und deren **Quelle** gleich **System-Upgrades** ist.
9. Klicken Sie auf den Datumslink in der Spalte **Erstellt** für diese Version, um den Versionsdatensatz zu öffnen.
10. Klicken Sie auf **Diese Version wiederherstellen**.
11. Navigieren Sie zurück zum Formular für die Probe oder den Sensor, und überprüfen Sie, ob die Hauptversion korrekt ist.
12. Wenden Sie Ihre Anpassungen erneut auf die Probe oder den Sensor an.
13. Stellen Sie sicher, dass Ihre Anpassungen für die neue Version der Probe oder des Sensors gültig sind, indem Sie eine Erkennung in Ihrer Testumgebung ausführen.

Discovery-Multi-Probes und -Multisensoren

Multi-Probes enthalten mindestens eine einfache Probe, die dafür konfiguriert ist, bestimmte Informationen von verwaltbaren Geräten zu extrahieren, indem mehrere Abfragen mit einer einzelnen Authentifizierung ausgeführt werden.

Sie können Multi-Probes so planen, dass sie jederzeit im Erkennungsprozess ausgeführt werden können, um die Erkundung effizienter zu gestalten. Multi-Probes werden häufig als Identitäts-Probes verwendet. Identitäts-Probes fragen für Geräte Informationen wie Name und Seriennummer ab und verwenden dann die Ergebnisse dieser Abfragen, um vorhandene CIs in der CMDB zu aktualisieren.

Zum Verarbeiten der von einer Multi-Probe zurückgegebenen Daten müssen Sie Multisensoren erstellen, die Skripts ausführen, die die von den Multi-Probes zurückgegebenen Daten verarbeiten. Multisensoren heißen in der Regel genauso wie ihre entsprechenden Multi-Probes.

Hinweis: Die entsprechenden Multisensoren tragen in der Regel denselben Namen wie die Multi-Probes.

Die folgenden Multi-Probes sind im Basissystem enthalten.

Multi-Probe	Enthaltene Probes
AIX - ADM	• AIX - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
AIX - Identity	• AIX - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs • AIX - Serial Number: Ruft AIX-Seriennummern ab
CIM - Identity	CIM - Computer System: Ruft CIM-Computersysteme über SMI-S ab
CIM - Identity - WBEM Service	CIM - CIMOM: Untersucht den WBEM-Service, CIMOM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Probe	Enthaltene Probes
HP-UX - ADM	• HP-UX - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
HP-UX - Identity	• HP-UX - Hardware Serial Number: Ruft HP-UX-Seriennummern ab • HP-UX - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs
Linux - Identity	• Linux - Hardware Information: Ruft DMI-(BIOS-)Informationen ab • Linux - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs
Mac OS X - Identity	• Mac OS X - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs • Mac OS X - CPU/Memory: Ruft CPU- und Speicherinformationen ab
SNMP - A10 - Identity	• SNMP - A10 - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des A10-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - ACE - Identity	• SNMP - Identity Info: Identifiziert ein SNMP-Gerät • SNMP - ACE - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des ACE Load Balancers verwendet wird
SNMP - Alteon - Identity	• SNMP - Alteon - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des Alteon-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - AppDirector - Identity	• SNMP - AppDirector - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des AppDirector-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - F5 BIG-IP - Identity	• SNMP - F5 BIG-IP - Identity - Serial: Ruft die für diesen Lieferanten global eindeutige Seriennummer des BIG-IP-Gehäuses ab • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - Identity	SNMP - Identity Info: Identifiziert Drucker-CIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Probe	Enthaltene Probes
SNMP - Load Balancer - Identity	• SNMP - F5 BIG-IP - Identity - Serial: Ruft die für diesen Lieferanten global eindeutigen Seriennummern des BIG-IP-Gehäuses ab • SNMP - Identity Info: Identifiziert SNMP-Geräte
SNMP - Netscaler - Identity	• SNMP - Netscaler - Identity - Serial: Ruft die für diesen Lieferanten global eindeutige Seriennummer des Netscaler-Gehäuses ab • SNMP - Identity Info: Identifiziert SNMP-Geräte
Solaris - ADM	• Solaris - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
Solaris - Identity	• Solaris - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs. • Solaris - Serial Number: Ruft Seriennummern für Solaris-Geräte ab †
Unix - ADM	• Unix - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
UNIX - Classify	• ESX - OS: Identifiziert ESX-Computer • UNIX - OS: Wird nach der Probe „ESX - OS“ ausgeführt, um das Betriebssystem für SSH-Geräte zu bestimmen, die nicht als ESX identifiziert wurden
Windows - ADM	• Windows - Active Processes: Ruft aktive laufende Prozesse ab • Windows - Active Connections: Ruft Informationen über aktive Verbindungen ab
Windows - Identity	• Windows - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs. • Windows - OS/Hardware Information: Sucht auf einem Windows-Computer nach WMI-Informationen
Windows - Storage 2008	• Windows - Storage 2008 - PS: Ruft Datenträger- und Dateisysteminformationen für Windows 2008 und frühere Versionen ab • Windows - Storage 2008 - WMI: Ruft Datenträger- und Dateisysteminformationen für Windows 2008 und frühere Versionen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Probe	Enthaltene Probes
Windows - Storage 2012	• Windows - Storage 2012 - WMI: Ruft Datenträger- und Dateisysteminformationen für Windows 2012 und höher ab • Windows - Storage 2012 - PS: Ruft Datenträger- und Dateisysteminformationen für Windows 2012 und höher ab

Hinweis: † Für diese Probe ist die Installation eines Befehlszeilentools von Oracle namens SNEEP erforderlich. Melden Sie sich zum Herunterladen und Installieren dieses Tools auf der Oracle-Website an. Nach der Installation dieses Tools wird die Probe **Solaris - Serial Number** automatisch ausgeführt, wenn Discovery ein Solaris-Gerät erkennt. Für Fujitsu PRIMEPOWER-Geräte müssen Sie diese Probe mit Root-Anmeldeinformationen ausführen.

Einer Multi-Probe eine einfache Probe hinzufügen

Sie können einer Multi-Probe über die zugehörige Liste *Enthält Probes* einfache Probes hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

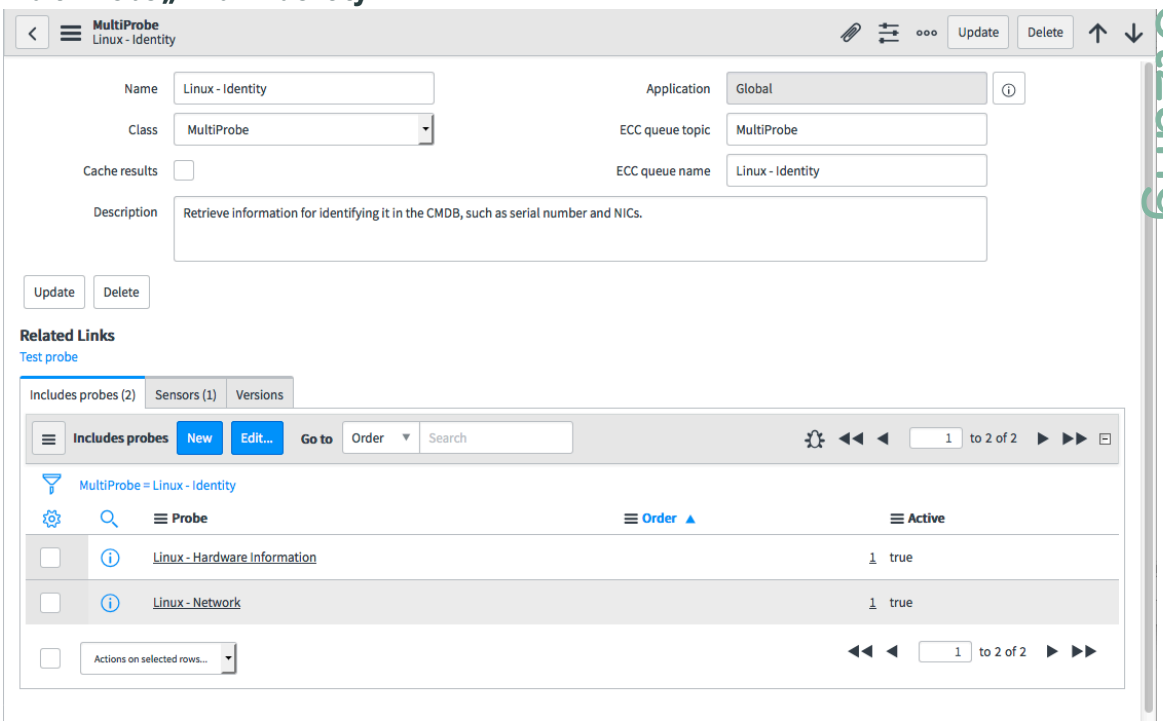
Sie können einer Multi-Probe einfache Probes beliebiger Typen hinzufügen und bei Bedarf Probe-Typen mischen.

Warnung: Fügen Sie der zugehörigen Liste *Enthält Probes* keine Multi-Probe hinzu.

Prozedur

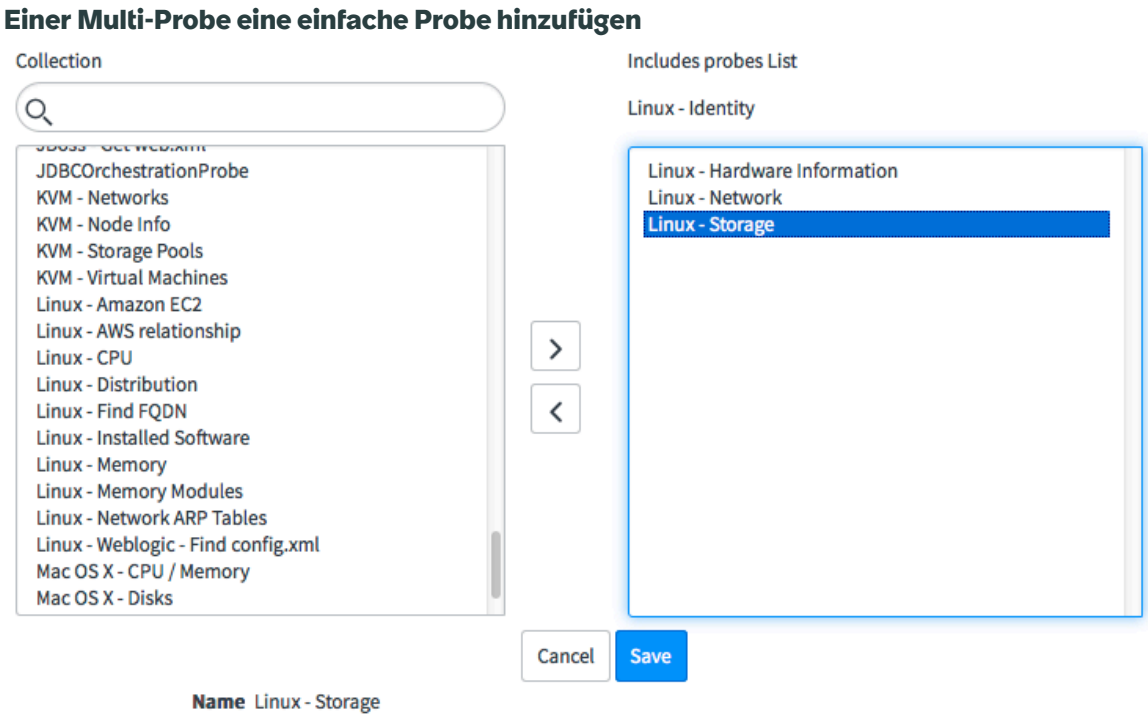
1. Navigieren zu **Alle** > **Discovery-Definitionen** > **Probes**an.
2. Öffnen Sie eine Multi-Probe aus der Liste.
   Die Multi-Probe-Bezeichnung wird in der Spalte **ECC-Warteschlangenthema** angezeigt.

Multi-Probe „Linux - Identity“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im Multi-Probe-Datensatz in der zugehörigen Liste **Enthält Probes** auf **Neu**.
4. Wählen Sie in der Erfassungsliste in der linken Spalte eine einfache Probe aus, und verschieben Sie sie in die Liste der enthaltenen Probes.



5. Klicken Sie auf **Speichern**.

Discovery-Multi-Probe erstellen

Sie können die in der Plattform bereitgestellten standardmäßigen Multi-Probes und Multisensoren verwenden oder eigene erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Probes**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Einstellungen aus:
   - Probe-Typ: Multi-Probe
   - ECC-Warteschlangenthema: Multi-Probe
4. In der zugehörigen Liste *Enthält Probes* können Sie die Probes hinzufügen, die Sie in der Multi-Probe einschließen möchten.
5. Klicken Sie auf **Speichern**.

Discovery-Multisensor erstellen

Erstellen Sie einen Multisensor, um die Daten zu verarbeiten, die von einer Multi-Probe zurückgegeben werden.

Automatische Übersetzung

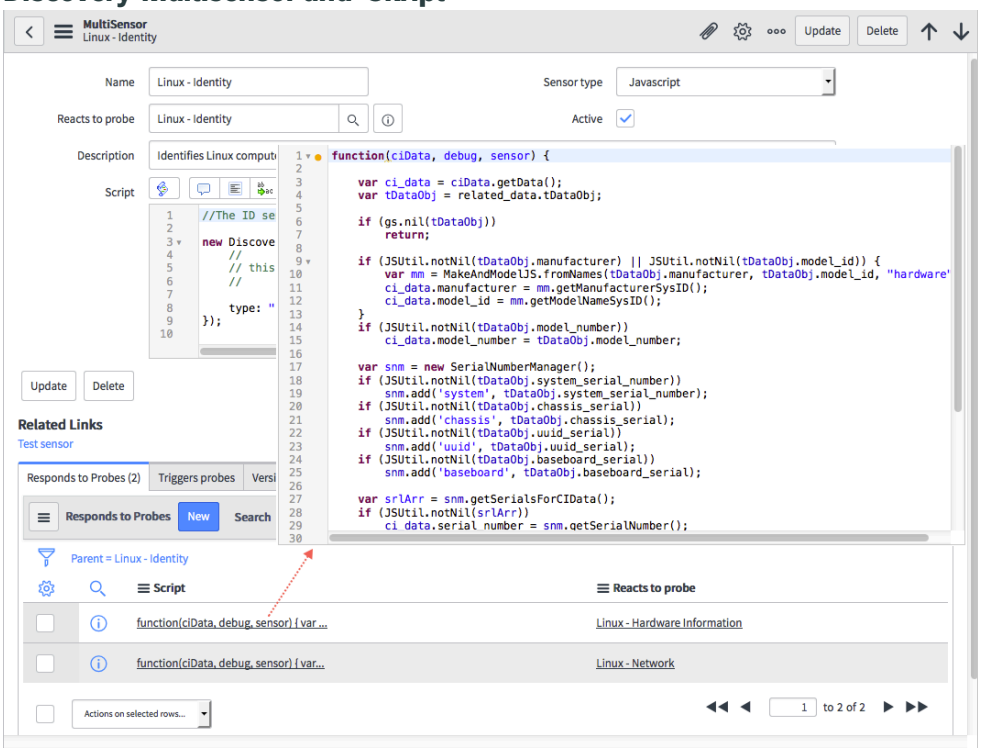
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Discovery-Multisensor und -Skript



Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Sensoren**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Einstellungen aus:
   - *Sensortyp*: Multisensor
   - *ECC-Warteschlangenthema*: Multisensor
   - *Reagiert auf Probe*: Wählen Sie die Probe aus, deren Nutzlast dieser Sensor verarbeiten muss.
   - *Sensortyp*: Wählen Sie eine der folgenden Optionen aus.
     - *Javascript*: Von einer Probe zurückgegebene Daten werden außerhalb der Anwendung im Sensor selbst verarbeitet und sind für den Benutzer sichtbar. Dies ist der gängigste Sensortyp.
     - *XML*: Die XML-Daten der Probe sind in Teile zerstückelt. Einige Teile können zum Starten anderer Probes verwendet werden, die der ursprüngliche Sensor benötigt, um alle erforderlichen Informationen über ein Gerät zu füllen.
4. Klicken Sie mit der rechten Maustaste auf den Formularheader und wählen Sie **Speichern** aus.
5. Klicken Sie in der zugehörigen Liste *Reagiert auf Probes* auf **Neu**.
6. Füllen Sie das Formular mit den folgenden Einstellungen aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *Reagiert auf Probe*: Wählen Sie die Probe in der Multi-Probe aus, auf die dieser Sensor reagiert. Der Sensor muss funktional mit der Probe verknüpft sein, etwa über die Netzwerk-ID oder Seriennummer.
- *Skript*: Geben Sie ein Skript ein, das vor dem Skript im Multisensor ausgeführt werden soll. Dieses Skript definiert, wie die von jeder Probe zurückgegebenen Daten verarbeitet werden sollen.

7. Klicken Sie auf **Speichern**.

Beispiel für benutzerdefinierte Discovery-Probe und -Sensor: CI mit Textdateiwerten füllen

Mithilfe dieser benutzerdefinierten Discovery-Probe können Sie eine Textdatei von einem Windows-Computer lesen und ein CI in der CMDB mit den Werten aus der Datei füllen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel wollte der Benutzer von *BGinfo* erstellte Dateien lesen.

Hinweis: Wenn Sie die Probe und den Sensor abgeschlossen haben, platzieren Sie die Probe in der entsprechenden Windows-Klassifizierung unter **Discovery-Definition** > **CI-Klassifizierung** > **Windows**an.

Prozedur

1. Navigieren zu **Discovery-Definition** > **Probes**, Und klicken Sie dann auf **Neu** .
2. Füllen Sie die folgenden Felder aus:
   - *Name*: Eindeutiger und beschreibender Name für die Probe
   - *Probe-Typ*: Wählen Sie **Probe** aus.
   - *Beschreibung*: Beschreiben Sie die Funktionalität dieser Probe.
   - *Verwendet von Discovery*: Aktivieren Sie dieses Kontrollkästchen.
   - *ECC-Warteschlangenthema*: Der Name der Probe, die der MID Server ausführen soll. In diesem Beispiel wird *WMIRunner* verwendet.
   - *ECC-Warteschlangenname*: In diesem Beispiel wird der beschreibende Name *WMI: BGInfo files* verwendet.
3. yxcvbnm,ooiuztreq12345tKlicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern** aus dem Kontextmenü.
4. Wechseln Sie im Probe-Formular zur Registerkarte „Probe Parameter“, und klicken Sie auf **Neu**.
5. Geben Sie `WMI_GetFiles.js` als Namen für diesen Parameter ein.
6. Kopieren Sie das folgende Skript in das Feld *Skript*, und bearbeiten Sie es nach Bedarf.
7. Klicken Sie auf **Absenden**.

```
//
 // Use ServiceNow WMIAPI to gather stats
 //
 var CMD_RETRIES = 3;
 var scanner = getScanner();
 if (scanner) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  var output = "";
  for(var i = 0; i < CMD_RETRIES; i++) {
     output = scanner.winExec("%SystemRoot%\\system32\\cmd.exe /C type
\\\"C:\\Information Systems\\BgInfo\\*.txt\\\"");
     if (output)
        break;
  }
  scanner.appendToRoot("output", output);
}
```

8. Navigieren zu **Discovery-Definition** > **Sensoren**, Und klicken Sie dann auf **Neu** .

   Füllen Sie die folgenden Felder aus:

   - *Name*: Verwenden Sie den Namen der entsprechenden Probe. In diesem Beispiel wird *Windows - Get BGInfo files* verwendet.
   - *Reagiert auf Probe*: Der Name der im vorherigen Verfahren erstellten Probe: *Windows - Get BGInfo files*
   - *Sensortyp*: Wählen Sie den Typ des zu erstellenden Sensors aus, in diesem Beispiel *Sensor*.
   - *Beschreibung*: Beschreibt die Funktion dieses Sensors
   - *Skript*: Kopieren Sie das folgende Skript in das Feld *Skript*, und bearbeiten Sie es nach Bedarf.
   - *Sensortyp*: Bestimmt, wie die Antwort der Probe verarbeitet wird - in diesem Beispiel *JavaScript*

9. Klicken Sie auf **Absenden**.

```
new DiscoverySensor({ data: {}, process: function(result) {

      this.parseOutput(result.output);
      this.update(this.data);
   },

 parseOutput: function(output) {
      var currentFile;
      var files = {};

 if (output.startsWith("<wmi")) {
          var bgout = new XMLHelper(output).toObject();
          if (!bgout)
             return;

 output = bgout.output;
      }

 var lines = output.split(/\n/);

 for(var i = 0; i < lines.length; i++) {
          var line = lines[i];
          if (line.startsWith("C:\\Information Systems\\BgInfo\\")) {
             currentFile = line.substr(30);
             files[currentFile] = "";
          } else if (currentFile) {
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            var newLine = line.trim();
            if (newLine)
               files[currentFile] += (files[currentFile]? "\n" : "") + newLine;
         }
      }

this.data['u_jack_id'] = files['JackID.txt'];
this.data['warranty_expiration'] = files['Warranty.txt'];
this.data['po_number'] = files['Ponum.txt'];},
type: "DiscoverySensor"

});
```

Muster und horizontale Erkennung

Ein Muster entspricht einer Reihe von Vorgängen, die Discovery mitteilen, welche CIs in Ihrem Netzwerk zu finden sind, welche Anmeldeinformationen verwendet werden sollen und welche Tabellen in der CMDB gefüllt werden sollen.

Dieses Thema setzt voraus, dass Ihnen die Phasen der horizontalen Erkennung bekannt sind. Wenn Sie den Prozess der horizontalen Erkennung für Probes und Muster wiederholen möchten, konsultieren Sie die folgenden Themen:

- Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren
- Prozess-Flow der horizontalen Erkennung mit Mustern

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Nutzung von Mustern durch Discovery

Ein Muster erfüllt die gleiche Funktion wie eine Probe: es identifiziert und erkundet ein Ziel-CI. Discovery verwendet Muster nur während der letzten beiden Erkennungsphasen: Identifizierung und Erkundung.

Wenn Sie die horizontale Erkennung mit Mustern starten, werden die Phasen „Scannen“ und „Klassifizierung“ so ausgeführt, als würden Sie keine Muster verwenden (nur mit Probes und Sensoren). Nach Abschluss der Klassifizierungsphase überprüft Discovery die Auslöser-Probes im Klassifizierer, um zu sehen, welche Probe zu starten ist. Wenn die Probe *`Horizontal Pattern`* als Auslöser-Probe angegeben ist, startet Discovery sowohl die Probe *`Horizontal Pattern`* als auch das von ihr angegebene Muster.

Unterschiede zwischen Probes und Mustern

Die wichtigsten Unterschiede zwischen der Verwendung von Mustern für die horizontale Erkennung und der Durchführung der horizontalen Erkennung nur mit Probes sind in der folgenden Tabelle aufgeführt:

Thema	Horizontale Erkennung mit Probes	Horizontale Erkennung mit Mustern
Erkennungsphasen	Probes werden während aller vier Erkennungsphasen ausgeführt.	Muster werden nur während der Identifizierungs- und Erkundungsphase ausgeführt. Discovery verwendet dennoch die Shazzam-Probe und die Port-Probes, um die Erkennung zu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Horizontale Erkennung mit Probes	Horizontale Erkennung mit Mustern
Erkennung neuer CIs	Discovery stellt mehrere sofort einsatzbereite Probes und Sensoren bereit. Wenn Sie jedoch neue CIs erkennen oder die Daten ändern möchten, die Discovery in die CMDB füllt, müssen Sie neue Probes und Sensoren erstellen oder die vorhandenen anpassen. Dazu benötigen Sie Kenntnisse in Java und JavaScript und müssen wissen, wie Probes mit anderen Probes und Sensoren zusammenarbeiten.	Discovery stellt in jedem Hauptrelease und im ServiceNow App Store weitere Muster bereit. Wenn Sie ein neues Muster erstellen oder ein vorhandenes anpassen möchten, können Sie den Musterdesigner verwenden, eine benutzerfreundliche Oberfläche, mit der Sie Schritte erstellen und Werte eingeben können.
Funktionsunterstützung	Unterstützt alle standardmäßigen Netzwerk- und CI-Erkennungen. Bestimmte Anwendungen werden ohne Muster nicht unterstützt. Unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte finden Sie eine vollständige Liste.	Zusätzlich zu allen standardmäßigen Erkennungsverfahren unterstützen Muster Folgendes: • Cloud Discovery • Nachverfolgung von Konfigurationsdateien • CI-Löschungsstrategien
ECC-Warteschlange und Problembehandlung	Je nachdem, wie viele Probes gestartet werden, erstellt Discovery mehrere Datensätze in der ECC-Warteschlange. Zum Beheben von Problemen mit der horizontalen Erkennung müssen Sie mehrere Datensätze der ECC-Warteschlange analysieren, um die von Discovery abgerufenen Daten anzuzeigen.	Discovery erstellt für das Muster nur einen zusätzlichen ECC-Warteschlangen-Datensatz. Zur Behebung von Problemen mit der horizontalen Erkennung während der Identifizierung und Erkundung müssen Sie für das Muster nur einen ECC-Warteschlangen-Datensatz analysieren.
Performance	Je nachdem, welche Art von Ziel-CI Sie identifizieren und erkunden möchten, kann Discovery während der Identifizierungsphase mehrere Probes und dann während der Erkennungsphase zusätzliche Probes auslösen. Es ist möglich, dass die horizontale Erkennung mit Probes aufgrund des zusätzlichen Overhead beim Auslösen und Verarbeiten vieler Probes länger dauern kann.	Discovery löst ein Muster während der Identifizierungs- und Erkundungsphase aus. Alle Vorgänge, die Discovery ausführen muss, befinden sich im Muster. Discovery kann sie der Reihe nach ausführen, bis das Muster abgeschlossen ist. Daher kann die Mustererkennung zu einer schnelleren Leistung führen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

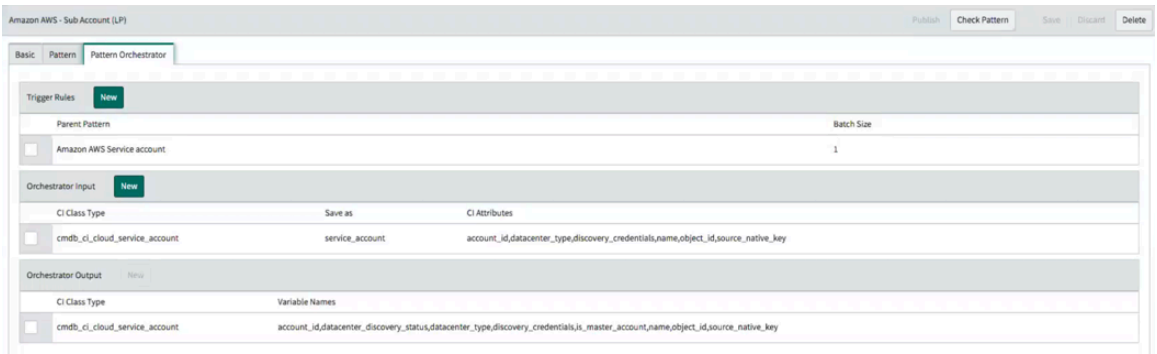
Muster für die Erkennung von oben nach unten sowie für die horizontale Erkennung

Sowohl Discovery als auch Service Mapping können dasselbe Muster für die horizontale Erkennung und die Erkennung von oben nach unten verwenden. Sie werden jedoch unterschiedlich bearbeitet. Unter Muster erstellen oder anpassen finden Sie Informationen zu den einzelnen Schritten. Wenn Sie ein Muster verwenden, das ausschließlich für die Erkennung von oben nach unten verwendet wurde, und es für die horizontale Erkennung verwenden möchten, müssen Sie einige Änderungen vornehmen. Anweisungen dazu finden Sie unter Muster für horizontale Erkennung verwenden.

Muster-Orchestrator

Der Muster-Orchestrator ist ein Prozess, mit dem eine Erkennung mehrere Muster im Zusammenhang mit einer Datensammlung hierarchisch auslösen kann. Dies dient der Behebung von Problemen mit großen Datensätzen (oder großen Nutzlasten), die langsame Erkennungen und OOM-Probleme (Out-of-Memory) auf einem MID Server verursachen können.

Auf den Muster-Orchestrator wird über die Registerkarte **Pattern Orchestrator (Muster-Orchestrator)** im **Musterdesigner** zugegriffen. Die Registerkarte enthält drei neue Tabellen: **Auslöserregeln**, **Orchestrator-Eingabe** und **Orchestrator-Ausgabe**.



Die Tabelle **Auslöserregeln** gibt das übergeordnete Muster im Feld **Übergeordnetes Muster** an. Das Feld **Batchgröße** gibt an, wie viele Elemente vom übergeordneten Muster bis zum untergeordneten Muster ausgelöst werden sollen. Für **Batchgröße** sind die Optionen **Count (Anzahl)**, **Alle** und **Use Parent Context Only (Nur übergeordneten Kontext verwenden)** verfügbar.

- **Count (Anzahl)** muss eine Zahl für **Anzahl der Batch-Größen** angeben. Das untergeordnete Muster wird jedes Mal ausgelöst, wenn das übergeordnete Muster die angegebene Anzahl von CIs sendet.
- **Alle** verwendet alle vom übergeordneten Muster gesendeten CIs und löst das untergeordnete Element einmal aus.
- **Use Parent Context Only (Nur übergeordneten Kontext verwenden)** stützt sich auf die Ausgabeeinstellungen des übergeordneten Musters, um festzulegen, welches untergeordnete Muster ausgelöst werden soll. Dies ist nützlich, wenn zwei Muster dasselbe übergeordnete Element haben, Sie aber eines vor dem anderen auslösen müssen.

Die **Orchestrator-Eingabe** verwendet das Feld **CI-Typ**, um CI-Typen aus dem übergeordneten Muster oder dem übergeordneten Muster des übergeordneten Elements zu akzeptieren. Das Feld **Gespeichert als** speichert den Namen des CI-Typs, der im Muster verwendet werden soll. Servicekonten sind ein Sonderfall und müssen den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Namen service_account aufweisen. Das Feld **CI-Attribute** verwendet alle Ausgaben des übergeordneten Musters, um die zu verwendenden Attribute auszuwählen.

Die **Orchestrator-Ausgabe** steuert, welche Daten an nachfolgende Muster gesendet werden. Sie besitzt die Felder **CI-Klassentyp**, wobei es sich um den Typ des CI handelt, das erkannt wird, und **Variablennamen**, das die Variablen angibt, die als Eingaben für untergeordnete Muster übergeben werden sollen. Variablen, die nicht in **Variablennamen** angegeben sind, werden nicht an untergeordnete Muster gesendet. Die Variable **source_native_key** kann manuell hinzugefügt werden, indem Sie im Feld **Variablennamen** nach ihr suchen.

Nativer Schlüssel der Quelle

In einigen Situationen kann ein Muster partielle Informationen über ein CI abrufen, während ein anderes Muster partielle Informationen über dasselbe CI abruft. Anstatt redundante Datensätze zu erstellen oder partielle Informationen zu verwerfen, werden die Informationen in der Tabelle „CMDB-IRE – teilweise Payloads“ [cmdb_ire_partial_payloads_list] gespeichert. Nachdem genügend Muster partielle Informationen gesammelt haben, können diese Daten korreliert werden, um vollständige Informationen über das CI bereitzustellen.

Paginierung

Eine weitere Möglichkeit, den Arbeitsspeicher des MID Servers zu entlasten, besteht in der Paginierung. Die Paginierung unterteilt eine große Nutzlast in kleinere, geordnete Segmente, die als Seiten bezeichnet werden. Die Paginierung begrenzt die maximale Größe empfangener Elemente und generiert ein Token. Sobald diese Seite verarbeitet wurde, wird das Token jeweils an die nächste Seite übergeben, die dann verarbeitet wird, bis alle Seiten abgeschlossen sind.

Die Paginierung wird über die Tabelle „Benutzerdefinierte Vorgänge“ [sa_custom_operation] gesteuert. Das Feld **Ist paginierungsfähig** ist im Formular standardmäßig ausgeblendet und kann dem Formular mit den Steuerelementen für **Formular personalisieren** hinzugefügt werden. Sobald dies auf „true“ gesetzt ist, enthält das zugeordnete Muster im Musterdesigner das Feld **Paginiert**. Indem Sie das Feld **Paginiert** auf „true“ einstellen, wird dieser Schritt im Muster mit Paginierung ausgeführt.

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Zur Verwendung eines Musters für die Identifizierungs- und Erkundungsphase der horizontalen Erkennung müssen Sie den Klassifizierern für die zu erkennenden CIs die Probe „Horizontal Pattern“ hinzufügen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

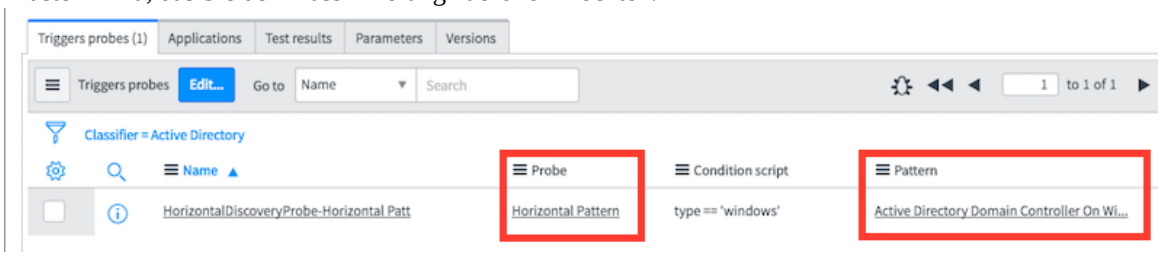
Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Dieses Verfahren ist nur für benutzerdefinierte Klassifiziererdatensätze oder solche gedacht, die standardmäßig kein Muster enthalten. Wenn Sie Ihre CMDB jedoch bereits mithilfe von Probes aus diesem Klassifizierer mit Daten gefüllt haben und dann zur Verwendung von Mustern wechseln, werden von Discovery möglicherweise doppelte CIs erstellt. Führen Sie dieses Verfahren deshalb nur aus, wenn Sie Discovery nie mit Probes für diesen Klassifiziertyp ausgeführt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **{Klassifizierungstyp}**an.
2. Öffnen Sie den Klassifiziererdatensatz.
3. Klicken Sie auf die zugehörige Liste **Löst Probe aus**.
4. Deaktivieren Sie die vorhandenen Identifizierungs- und Erkundungs-Probes.
5. Klicken Sie auf **Bearbeiten**, und fügen Sie die Probe **Horizontal Pattern** hinzu.
   Die Probe wird in der zugehörigen Liste angezeigt.
6. Doppelklicken Sie in der zugehörigen Listenansicht in das Feld unter der Spalte **Muster**, und fügen Sie das Muster hinzu, das Sie der Klassifizierung zuordnen möchten.



7. Entfernen Sie die anderen Probes aus der zugehörigen Liste **Löst Probe aus**, bzw. deaktivieren Sie sie.

> **Hinweis:** Wenn Sie ein Muster löschen, wird die Probe „Horizontal Pattern“ nicht automatisch aus dem Klassifizierer entfernt. Sie müssen für die horizontale Probe ein anderes Muster auswählen, oder Sie können wieder zur Verwendung von Identifizierungs- und Erkundungs-Probes wechseln, die für den Klassifizierer spezifisch sind. Wenn Sie die horizontale Probe ohne angegebenes Muster verwenden, wird die Erkundung nach der Klassifizierungsphase beendet.

Muster für horizontale Erkennung verwenden

Wenn Sie ein neues Muster verwenden möchten oder bereits über ein Muster verfügen, das Sie für die Erkennung von oben nach unten verwendet haben, können Sie das Muster für die horizontale Erkennung mit einigen Änderungen am entsprechenden Klassifizierer verwenden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

> **Warnung:** Dieses Verfahren ist nur für benutzerdefinierte Klassifiziererdatensätze oder solche gedacht, die standardmäßig kein Muster enthalten. Wenn Sie Ihre CMDB jedoch bereits mithilfe von Probes aus diesem Klassifizierer mit Daten gefüllt haben und dann zur Verwendung von Mustern wechseln, werden von Discovery möglicherweise doppelte CIs erstellt. Führen Sie dieses Verfahren deshalb nur aus, wenn Sie Discovery nie mit Probes für diesen Klassifizierertyp ausgeführt haben.

Prozedur

1. Stellen Sie sicher, dass Discovery das Muster verwenden kann:

   a. Navigieren zu **Musterdesigner** > **Discovery-Muster**an.

   b. Öffnen Sie das Muster.
   Anwendungsmuster, die von Service Mapping verwendet werden, sind als Typ **1: Anwendung** angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Stellen Sie in den **Identifizierungsabschnitten** auf der Registerkarte, **Standard** sicher, dass mindestens ein Bereich verfügbar ist, der einen Einstiegspunkt der Art **TCP** oder **Alle** ermöglicht. Erstellen Sie andernfalls einen entsprechenden Bereich. Den Identifizierungsschritten können Sie weitere Informationen zum Erstellen eines neuen Musters entnehmen.

d. Speichern Sie das Muster.

2. Erstellen oder ändern Sie in der Instanz die Klassifizierung für den CI-Typ, den Sie erkennen möchten. Konfigurieren Sie den Klassifizierer wie folgt:

a. Navigieren zu **Discovery-Definition** > **CI-Klassifizierung** > **{Klassifizierungstyp}**an.

b. Öffnen Sie den relevanten Klassifizierer.

c. Konfigurieren Sie den Klassifizierer wie folgt:

- **Beziehungstyp**: Wählen Sie **Wird ausgeführt auf::Wird ausgeführt** aus (nur für Prozessklassifizierer).
- **Bedingung**: Konfigurieren Sie dieselbe Bedingung, die Sie im Muster definiert haben.
- Zugehörige Liste **Auslösertests**: Fügen Sie die Probe „Horizontal Pattern“ hinzu, und fügen Sie dann der Spalte **Muster** das verwendete Muster hinzu.

Unter Discovery-CI-Klassifizierung erstellen finden Sie eine Beschreibung der anderen Felder im Klassifizierer.

Nächste Maßnahme

Führen Sie das Muster im Debug-Modus aus, um es zu testen. Wenn Sie sicher sind, dass das Muster funktioniert, können Sie die Erkennung ausführen, indem Sie einen Erkennungszeitplan einrichten oder eine Erkennung bei Bedarf ausführen. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Discovery Ressourcennutzung

Standardtransaktionen für Windows Und UNIX Generieren Sie verschiedene Mengen von Netzwerkverkehr, je nachdem, was erkannt wird.

Diese Tabellen zeigen den Bandbreitenverbrauch für jedes Daten-Flow-Segment einer typischen Discovery mithilfe von Probes und Mustern über verschiedene Betriebssysteme.

Discovery-Bandbreite über verschiedene Betriebssysteme (in Megabyte)

Gerätetyp	MID > Instanz	Instanz > MID	MID > Ziel	Ziel > MID	Gesamt
Windows 2016	0.104966	0.101271	0.77739	2.364353	3.34798
Windows 2012	0.126327	0.07928	1.177146	3.70751	5.089804
Windows 2008	0.141816	0.104674	1.032673	3.594784	4.873947
Windows 10	0.091466	0.075601	0.642313	2.221103	3.030483
Linux CentOS	0.164232	0.111376	0.148742	0.690117	1.114467
Mac OSX	0.103707	0.068302	0.021681	0.461365	0.655055
HP-UX	0.120358	0.106676	0.042669	0.101149	0.370852

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Bandbreite über verschiedene Betriebssysteme (in Megabyte) (Fortsetzung)

Gerätetyp	MID > Instanz	Instanz > MID	MID > Ziel	Ziel > MID	Gesamt
Solaris	0.130551	0.099414	0.060243	0.346605	0.636813
Cisco UCS-Switch	0.029655	0.027465	0.094918	0.097444	0.249492
F5 Load Balancer	0.043935	0.03689	0.017179	0.012132	0.110136
A10-Lastenausgleichsmodul	0.046631	0.032266	0.018313	0.03182	0.12903
EMC-Speicher	0.4776	0.373828	1.215954	4.741926	6.809308

Die folgende Tabelle zeigt den Bandbreitenvergleich zwischen einer ersten Discovery für dreistufige Anwendungen und für jede nachfolgende Discovery. Die Bandbreite ist in die drei Stufen unterteilt: UI (Apache), Anwendung (Websphere) und Daten (Oracle). Dies misst die Gesamtdatentransfers für jede Discovery-Ausführung einmal für eine Geräteklasse.

Discovery-Bandbreite für dreistufige Anwendungen (in Megabyte)

Gerätetyp	MID > Instanz	Instanz > MID	MID > Ziel	Ziel > MID	Gesamt
Dreistufige Anwendung: Erste Discovery	0.712829	0.678862	7.084678	9.430181	17.90655
F5 Load Balancer				0,017179	0,012132
Apache auf Linux				0.540161	1.107108
WebSphere ein Linux				0.729403	1.165112
Oracle auf Windows				5.797935	7.145829
Dreistufige Anwendung: Nachfolgende Discovery	0.150882	0.107409	2.536535	0.560122	3.354948
F5-Lastenausgleichsmodul				0.001347	0,012132
Apache auf Linux				0.136366	0.79392
WebSphere ein Linux				0.341042	0.11365
Oracle auf Windows				2.05778	0.354948

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Tabelle zeigt die Erkennung verschiedener Betriebssystemtypen, die Muster nutzen. Dies misst in Megabyte die Gesamtmenge der erstellten Daten und die Gesamtmenge der Daten in nachfolgenden Scans für jedes Gerät.

Discovery-Bandbreite für Muster über verschiedene Betriebssystemtypen (in Megabyte)

Gerät		MID > Instanz	Instanz > MID	MID > Ziel	Ziel > MID	Gesamt
Linux	Erstellen	0.39	0.486	0.098	0.273	1.247
	Aktualisieren	0.382	0.499	0.093	0.264	1.238
Windows Server	Erstellen	0.289	0.316	5.628	8.508	14.741
	Aktualisieren	0,273	0.306	5.621	8.458	14.658
Solaris	Erstellen	1.222	1.4	0.383	0.917	3.922
	Aktualisieren	1,24	1.42	.399	.675	3.734
HP-UX	Erstellen	0.176	0.222	0.063	0.13	0.591
	Aktualisieren	0.178	0.247	0.062	0.128	0.615
Citrix Netscaler	Erstellen	0.424	1.919	0.019	0.042	2.404
	Aktualisieren	0.355	0.619	0.016	0.041	1.031
F5	Erstellen	0.087	0.135	0.026	0.047	0.295
	Aktualisieren	0.132	0.171	0,026	0,047	0.376
L3-Switch	Erstellen	0.172	0.125	0.282	0.478	1.057
	Aktualisieren	0,178	0.126	0,282	0.479	1.065

Hinweis: Diese Messungen wurden mit grundlegenden Betriebskonfigurationen durchgeführt. Die Ergebnisse Ihres lokalen Systems können abweichen.

Beispiele für CPU-Auslastung

Beispiele für die CPU-Nutzung variieren je nach Matrix von Tausenden von Kombinationen von Betriebssystemen, Chipsätzen und spezifischen Lasten für jedes System.

Ihre Mischung dieser Variablen bestimmt Ihren eindeutigen CPU-Verbrauch.

Sie können eindeutige Builds mithilfe interner Vorlagen identifizieren und erkennen, indem Sie die Auswirkungen auf die Leistung oder die mangelnde Leistung Ihres Discovery-Tools auf Ihr System beobachten.

Monitoring von Erkennungen und Problemlösung

Erfahren Sie, wie Sie den Fortschritt Ihrer Erkennungen überwachen und das System konfigurieren, um Leistungsmetriken zu aggregieren, die wichtig für Sie sind. Hier finden Sie Beschreibungen der angezeigten Fehlermeldungen sowie mögliche Schritte zur Lösung von Problemen. Die Hi-Knowledge Base enthält mehrere Artikel, die Sie bei der Behandlung von Problemen mit Erkennungen unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID Server-Übersicht	

Discovery-Homepage

Öffnen Sie den Discovery-Manager, um Zeitpläne für IP-basierte und cloudbasierte Erkennungen zu erstellen oder zu bearbeiten. Zeigen Sie die von Ihren Zeitplänen erkannten CIs und Cloud-Ressourcen an, und verfolgen Sie dann alle aufgetretenen Fehler nach.

Leitfaden zur Discovery-Fehlerbehebung

Lesen Sie den Leitfaden zur Discovery-Fehlerbehebung in der Knowledge Base, wenn bei Ihnen Unregelmäßigkeiten auftreten, etwa wenn Discovery den erkannten Host nicht klassifizieren kann oder wenn die Shazzam-Probe bestimmte Gerätetypen nicht findet.

KB0657528: Fehlerbehebung bei Anmeldeinformationen und Berechtigungen bei Discovery, Service-Mapping und Orchestration

Discovery-Probleme können durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht werden. Erfahren Sie, wie Sie fehlende Anmeldeinformationen oder Berechtigungen identifizieren und konfigurieren können.

Discovery-Fehlermeldungen

Zeigen Sie die Liste der allgemeinen Fehlermeldungen und möglichen Lösungen an.

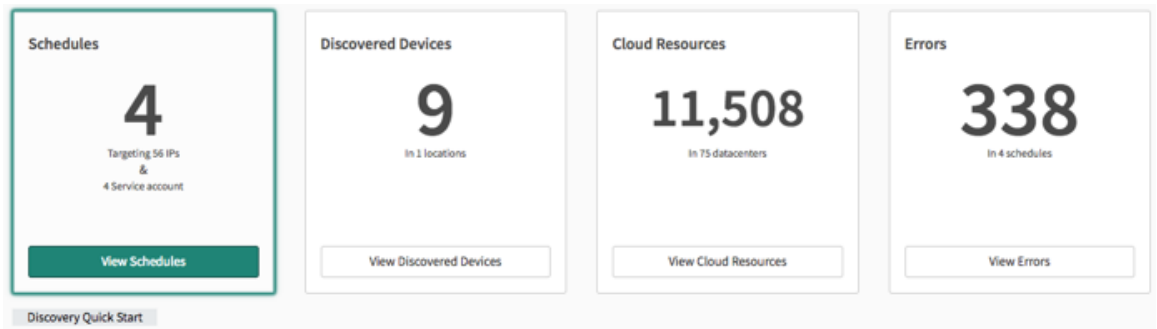
Leistungsmetriken zu Erkennungen

Zeigen Sie Leistungsmetriken zu Probe-/Muster- und Sensorverarbeitungszeiten an. Sie können Rollup-Daten verwenden, um die Leistung bestimmter Erkennungen zu überwachen oder um die Leistung zwischen Versionen nach einem Upgrade zu vergleichen.

Discovery-Homepage

Auf der Seite Discovery-Startseite finden Sie eine Zusammenfassung der Erkennungen, die durch Cloud- und Nicht-Cloud-Zeitpläne ausgelöst worden sind. Sie können alle Fehler anzeigen, die während einer Discovery aufgetreten sind, und Vorschläge zur Fehlerkorrektur einsehen. Verwenden Sie die Ansicht „Homepage“, um die für die in einem Cloud-Zeitplan ausgewählten Servicekonten erkannten Cloud-Ressourcen zu untersuchen.

Um zu öffnen Discovery-Startseite Seite, navigieren Sie zu **Discovery** > **Startseite**an. Auf der Homepage werden Discovery-Summen für die folgenden Kategorien angezeigt. Klicken Sie auf eine Kachel, um Details zu dieser Kategorie anzuzeigen.



Element	Beschreibung
Zeitpläne	Die Anzahl der Discovery-Zeitpläne, die zur Erkennung von Cloud-Ressourcen und virtuellen Computern (IP-Adressen) konfiguriert sind. Klicken Sie auf **Zeitpläne anzeigen**, um die CI-Zeitplanansicht zu öffnen, in der spezifische Informationen über die einzelnen CI-

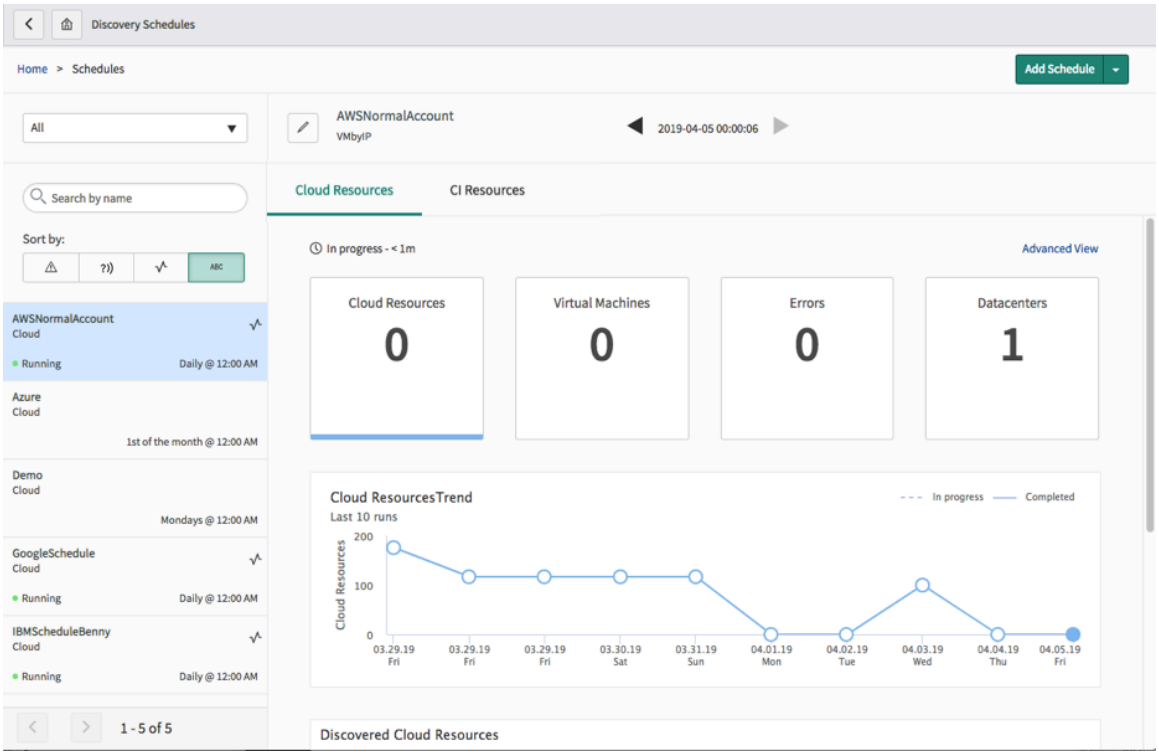
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Zeitpläne separat angezeigt werden. Zeigen Sie die Ergebnisse Ihrer Cloud- oder IP-Adresszeitpläne an, und erstellen Sie neue Zeitpläne.
Erkannte Geräte	Die Gesamtanzahl der erkannten Geräte-CIs. Geräte umfassen alle CIs in Tabellen, die die Tabelle „Hardware“ [cmdb_ci_hardware] erweitern, zum Beispiel „Computer“ [cmdb_ci_computer] und „Cisco-UCS-Zubehör“ [cmdb_ci_ucs_equipment].
Cloud-Ressourcen	Die Gesamtanzahl der für die ausgewählten Servicekonten erkannten Ressourcen (virtuellen Computer). Unter Erkennung von virtuellen Maschinen aktivieren finden Sie Details zum Einrichten von Discovery für Ihre Cloud-Ressourcen. Klicken Sie auf **Cloudressourcen anzeigen**, um eine Liste der erkannten Cloud-Ressourcen nach Typ zu öffnen.
Fehler	Die Gesamtanzahl der während der Erkennung aufgetretenen, nicht gelösten Fehler. Klicken Sie auf **Fehler anzeigen**, um einen Drilldown zu bestimmten Fehlertypen durchzuführen.

Alle Zeitpläne anzeigen

In der Zeitplanansicht werden Details zu jedem Zeitplan angezeigt, der für den ausgewählten Filter ausgeführt wurde. Standardmäßig sind in der Liste alle Erkennungszeitpläne in alphabetischer Reihenfolge aufgeführt, unabhängig vom aktuellen Ausführungsstatus.



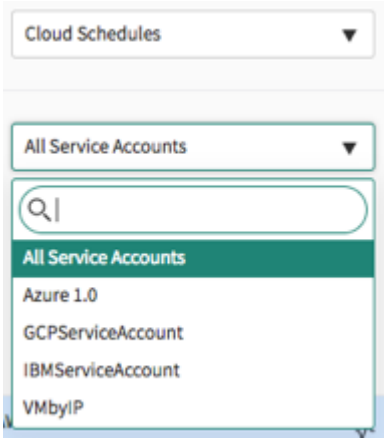
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgenden Steuerelemente, um Discovery-Ergebnisse nach Zeitplänen zu filtern:

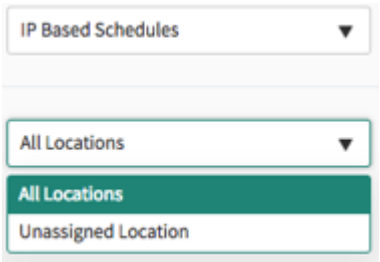
Zeitplanfilter

Folgende Filter sind zur Auswahl verfügbar:

- **Alle**: Ergebnisse aller Erkennungszeitpläne, die ausgeführt wurden. Das ist der Standardfilter.
- **Cloud-Zeitpläne**: Ergebnisse aller Cloud-Erkennungszeitpläne, die ausgeführt wurden. Wenn Sie diesen Filter auswählen, wird ein zweiter Filter eingeblendet, mit dem Sie Cloud-Zeitpläne nach **Servicekonto** anzeigen können.



- **IP-basierte Zeitpläne**: Ergebnisse aller Erkennungszeitpläne, die für Konfigurationselemente (CI) unter Verwendung von IP-Bereichen ausgeführt wurden. Wenn Sie diesen Filter auswählen, wird ein zweiter Filter angezeigt, mit dem Sie die CI-Zeitpläne nach einem bestimmten Standort oder allen Standorten anzeigen können.



Zeitplansortierer

Wählen Sie in der Zeitplanauswahl im linken Bereich von links nach rechts eines der folgenden Sortierkriterien aus:

- Fehler für alle aufgelisteten Zeitpläne
- Nicht identifizierte IP-Adressen
- Letzte Aktivität, durch die die derzeit zuerst ausgeführten Zeitpläne auflistet werden
- Alphabetische Liste der Zeitpläne

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitplanliste

Liste der verfügbaren Erkennungszeitpläne. Wählen Sie einen Zeitplan aus, um dessen Details anzuzeigen. Klicken Sie oben auf der Seite auf das Stiftsymbol, um den Zeitplan zu bearbeiten.

Datum-/Uhrzeitanzeige

Datum und Uhrzeit des Zeitpunkts, an dem der ausgewählte Zeitplan ausgeführt wurde

Zeitplanthemen

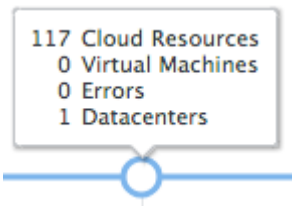
Kacheln, die die Kategorien für Erkennungsergebnisse für den ausgewählten Zeitplan anzeigen. Klicken Sie auf eine Kachel, um weitere Details dazu anzuzeigen.

- **Cloud-Ressourcen**: Zeigt die Gesamtanzahl der für diesen Filter aktualisierten oder erstellten CIs an
- **Virtuelle Computer**: Zeigt die Gesamtanzahl der mit dem ausgewählten Zeitplan erkannten virtuellen Computer an
- **Fehler**: Zeigt die Gesamtanzahl der Fehler an, die beim Ausführen des ausgewählten Zeitplans aufgetreten sind
- **Datacenter**: Zeigt die Anzahl der Rechenzentren an, die bei der Erstellung des Erkennungszeitplans ausgewählt wurden

Trenddiagramm für Cloud-Ressourcen

Dies ist ein Trenddiagramm für den ausgewählten Zeitplan. Jeder Kreis im Diagramm stellt eine bestimmte Discovery-Ausführung dar.

Platzieren Sie den Cursor auf einem beliebigen Kreis, um eine Zusammenfassung dieser Erkennung anzuzeigen.



Klicken Sie auf einen Kreis, um die Werte zu filtern, die in den Discovery-Themen angezeigt werden. Die Ergebnisse füllen die entsprechenden Kacheln über dem Diagramm.

Fehler nach Kategorie

Dies sind die Kategoriekacheln für die während der Erkennung aufgetretenen Fehler für den ausgewählten Zeitplan. Klicken Sie auf eine Kachel, um die Fehler in dieser Kategorie anzuzeigen und empfohlene Aktionen zur Fehlerkorrektur anzuzeigen. Weitere Einzelheiten erhalten Sie unter Discovery-Fehlermeldungen.

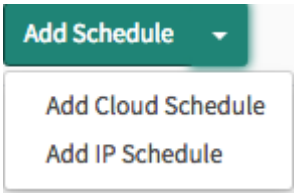
Erkannte Cloud-Ressourcen

Aufgliederung der für den ausgewählten Zeitplan erkannten Cloud-Ressourcen, dargestellt in einem horizontalen Balkendiagramm

Zeitpläne hinzufügen

Typen der hinzufügbaren Zeitpläne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



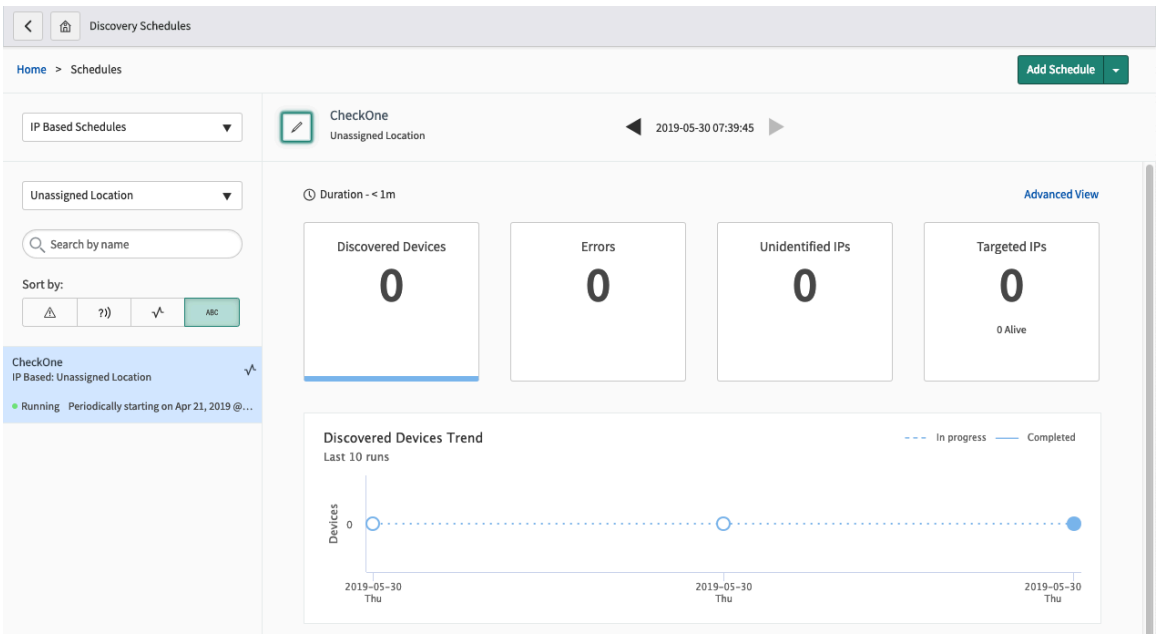
Erweiterte Ansicht

Zeigt den Discovery-Statusdatensatz für den ausgewählten Zeitplan an. Über diesen Link können Sie die Ergebnisse des Zeitplans in der ECC-Warteschlange und im Discovery-Protokoll überprüfen.

IP-basierte Zeitpläne anzeigen

Wählen Sie zum Anzeigen der Ergebnisse von IP-Bereichserkennungen im primären Filter die Option **IP-basierte Zeitpläne** aus. Verwenden Sie das eingeblendete sekundäre Feld, um die Suchergebnisse nach **Standort** zu filtern. Daraufhin zeigen die Kacheln die Ergebniskategorien für den ausgewählten IP-basierten Zeitplan an. Klicken Sie auf eine Kachel, um weitere Details dazu anzuzeigen.

- **Erkannte Geräte**: Gesamtanzahl der vom IP-basierten Zeitplan erkannten virtuellen Computer, einschließlich Ziel-IP-Adressen und nicht identifizierter IP-Adressen
- **Fehler**: Zeigt die Gesamtanzahl der Fehler an, die beim Ausführen des ausgewählten IP-basierten Zeitplans aufgetreten sind
- **Nicht identifizierte IPs**: Anzahl der nicht identifizierten CIs, die vom IP-basierten Zeitplan erkannt wurden
- **Ziel-IP-Adressen**: Anzahl der gefundenen CIs, die im IP-basierten Zeitplan konfiguriert waren



Fehler im CI-Erkennungszeitplan beheben

Auf der ServiceNow-Homepage können Sie die während einer Erkennung aufgetretenen Discovery-Fehler anzeigen und erhalten Vorschläge zur Lösung dieser Fehler. Sie können die Fehler für alle Zeitpläne oder für einen einzelnen Zeitplan anzeigen.

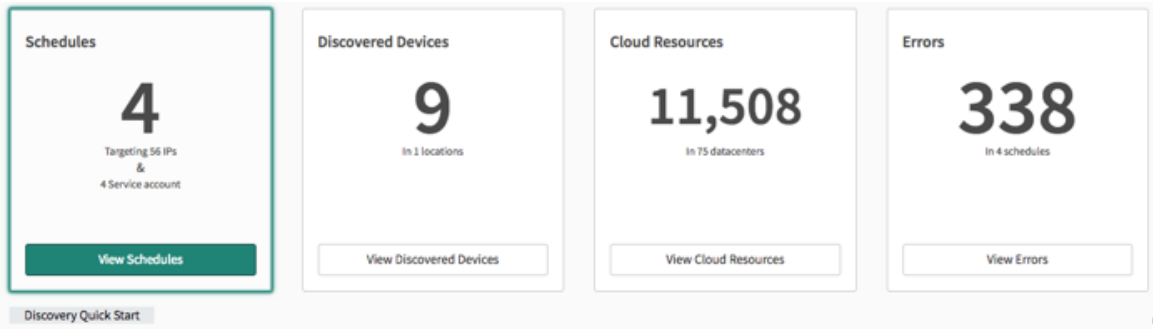
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: discovery_admin

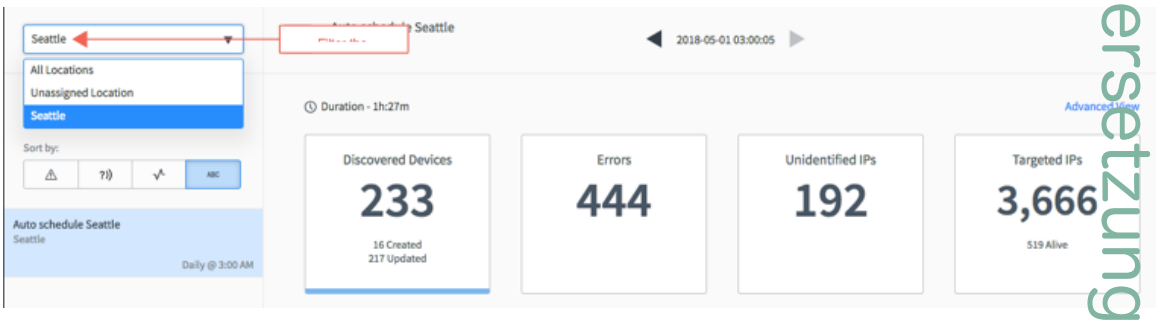
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**an.
   Die Zusammenfassungsseite für alle Zeitpläne wird angezeigt.



2. Zeigen Sie die Fehler mit einer der folgenden Methoden an:
   - Klicken Sie auf die Kachel **Fehler**, um die Fehler nach Kategorie für alle CI-Erkennungszeitpläne anzuzeigen.
   - Klicken Sie auf die Kachel **Zeitpläne**, um die Fehler für einen einzelnen Zeitplan anzuzeigen.
     a. Wählen Sie auf dem Zusammenfassungsbildschirm den Zeitplan aus, den Sie auf Fehler untersuchen möchten.

     Wenn Sie über zahlreiche Zeitpläne verfügen, können Sie sie über die Dropdown-Liste „Standort“ nach dem Standort oder über das Feld **Nach Namen suchen** nach dem Zeitplannamen filtern.

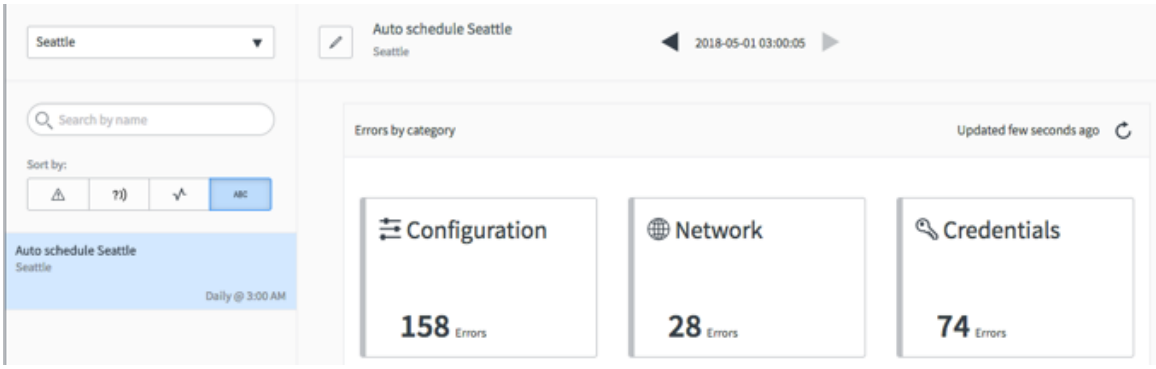


     b. Nachdem Sie den Zeitplan ausgewählt haben, klicken Sie auf die Kachel **Fehler**.

Automatische Übersetzung

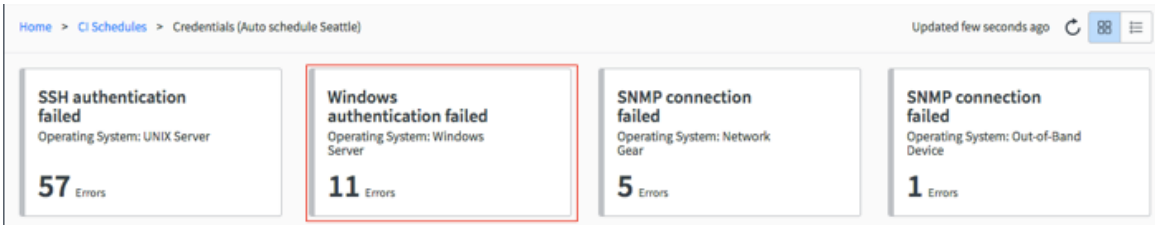
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Scrollen Sie nach unten, um die Fehler nach Kategorie anzuzeigen.



3. Klicken Sie auf eine Kategoriekachel, um die spezifischen Fehlercodes anzuzeigen, die in dieser Kategorie aufgetreten sind.

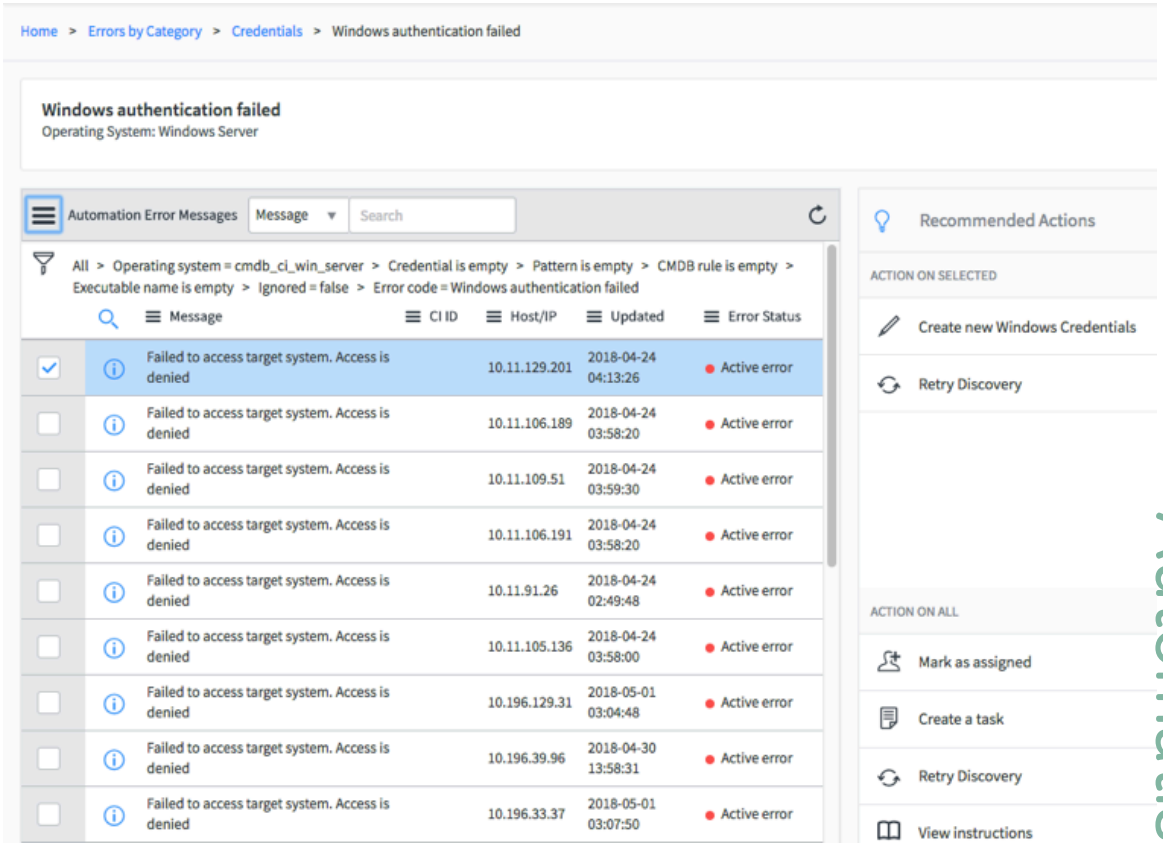
4. Klicken Sie auf die Kachel für den Fehlercode, den Sie untersuchen möchten.



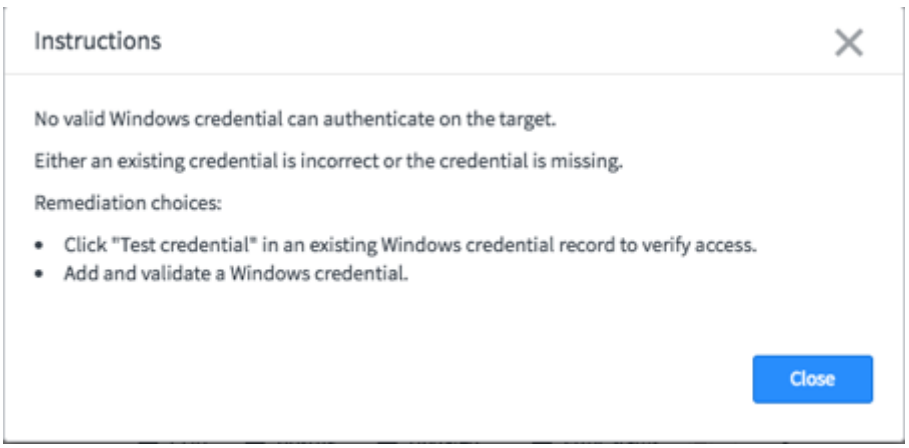
Die Liste zeigt alle Vorkommen dieses Fehlercodes an, entweder für einen einzelnen CI-Zeitplan oder für alle Zeitpläne, und zwar abhängig vom Pfad, den Sie zum Anzeigen der Fehler ausgewählt haben. Die Liste zeigt die IP-Adresse jeder Instanz an, bei der der Fehler aufgetreten ist, und den Fehlerstatus **Aktiver Fehler**. Der Bereich **Recommended Actions** auf der rechten Seite enthält die empfohlene Aktion für den ausgewählten Fehler. Der Bereich **AKTION FÜR ALLE** enthält Vorgänge, die Sie für alle Fehler in der Liste ausführen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

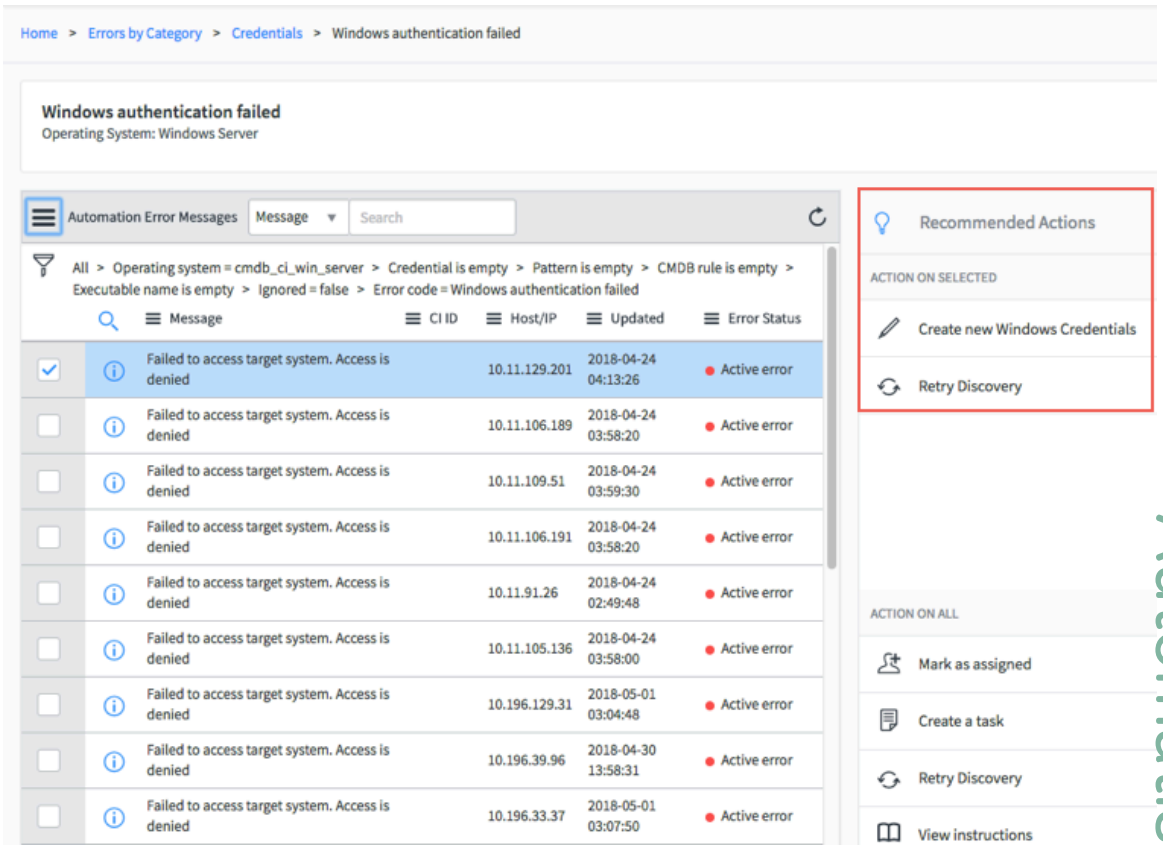


5. Klicken Sie auf **Anweisungen anzeigen**, um Details und Vorschläge zur Fehlerkorrektur für den Fehlercode anzuzeigen.

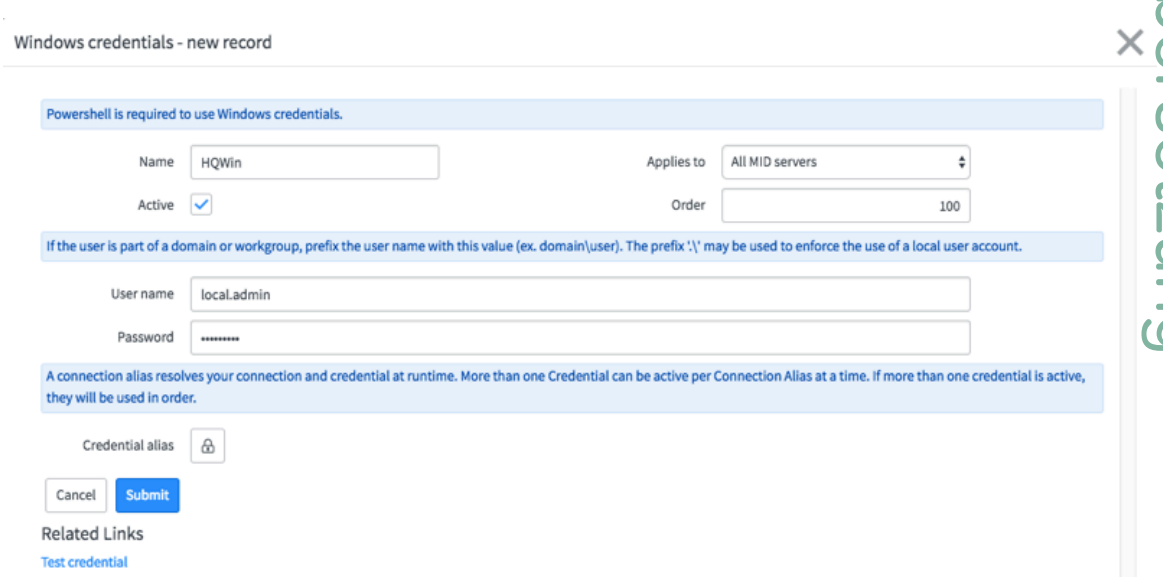


6. Um mit der Arbeit zu beginnen, aktivieren Sie entweder das Kontrollkästchen neben einem Fehler, um diesen Fehler zu beheben, oder wählen Sie eine Aktion für **ALLE** aus, um diesen Fehlercode für alle Instanzen dieses Fehlers zu beheben.
   In diesem Beispiel empfiehlt das System, zur Behebung dieses Fehlercodes neue Windows-Anmeldeinformationen zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Schließen Sie die vorgeschlagenen Aufgaben zur Fehlerkorrektur ab, bevor Sie die Erkennung erneut versuchen.
   In diesem Beispiel wird über den Link **Neue Windows-Anmeldeinformationen erstellen** ein Formular zum Erstellen und Testen neuer Windows-Anmeldeinformationen geöffnet.



8. Nachdem Sie alle empfohlenen Aufgaben abgeschlossen haben, klicken Sie auf **Discovery wiederholen**.
   Eine mögliche Vorgehensweise besteht darin, die Discovery für **ALLE** Instanzen nach dem Erstellen der Anmeldeinformationen zu wiederholen. Möglicherweise stellen die neuen Anmeldeinformationen die Lösung des Problems für alle Instanzen dar, bei denen dieser Fehlercode auftritt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Überprüfen Sie die Spalte **Fehlerstatus**, um die Ergebnisse Ihrer Maßnahmen zur Fehlerkorrektur anzuzeigen.
   Einzelne Wiederholungsversuche werden schnell abgeschlossen. Neuversuche für eine große Anzahl von IP-Adressen können mehrere Minuten dauern.

   Fehler können einen der folgenden Status aufweisen:

   - **Aktiver Fehler**: Der Fehler ist nicht gelöst. Das ist der Standardstatus aller neuen Fehler.
   - **Gelöst**: Der Fehler ist behoben. Für die empfohlenen Aktionen wird *Fehler erfolgreich gelöst* angezeigt.
   - **Zugewiesen**: Zur Behebung dieses Fehlers ist eine Aufgabe zugewiesen. Klicken Sie auf **Eine Aufgabe erstellen**, um einen Benutzer für alle aktiven Fehler einer Aufgabe zuzuweisen. Zugewiesene Fehler gelten als **Aktive Fehler**, für die noch Aktionen ausgeführt werden können.
   - **Ausstehende Erkennung**: Es wird darauf gewartet, dass die Erkennung gestartet wird, nachdem Sie die Aktion **Discovery wiederholen** für alle Fehler ausgeführt haben.
   - **In Erkennung**: Die Erkennung ist derzeit aktiv.

Zugehörige Informationen

Discovery-Status

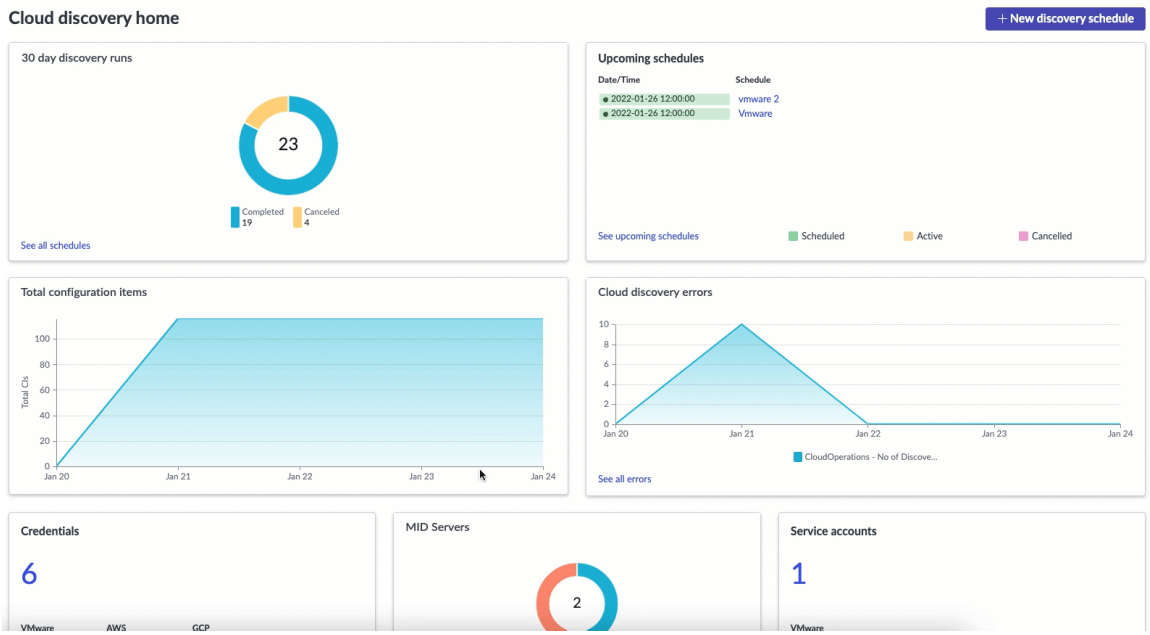
Protokolle für horizontale Erkennung prüfen

ECC-Warteschlange für Discovery

Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Cloud-Discovery Homepage in Cloud Operations Workspace

Die Cloud-Discovery-Homepage bietet eine Zusammenfassung der Discovery-Vorgänge, die durch einen Discovery-Zeitplan ausgelöst wurden. Sie können die Anzahl der im Laufe der Zeit erkannten CIs und aufgetretenen Fehler anzeigen. Außerdem können Sie einen beliebigen Dashboard-Bericht auswählen, um zusätzliche Informationen anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche ServiceNow AI Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin

Greifen Sie auf zu Cloud-Discovery Homepage

Um das Dashboard zu öffnen, wechseln Sie zu: **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Dashboard**an.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	Der sn_cloud_ops_ws.cloud_ops_admin kann die folgenden Informationen im Cloud-Discovery-Dashboard überprüfen: • 30-tägige Discovery-Ausführungen • Bevorstehende Zeitpläne • Total configuration items (Gesamte Konfigurationselemente) • Cloud-Discovery-Fehler • Anmeldeinformationen • MID Servers • Servicekonto • Cloud-VMs nach Rechenzentrum

Indikatoren

Anmeldeinformationen

Dieser Indikator zeigt die Gesamtanzahl der im System definierten Anmeldeinformationen und ihre Aufgliederung nach Cloud-Anbieter an.

Wählen Sie die unter einem beliebigen Anmeldeinformationstyp angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Anmeldeinformationen anzuzeigen.

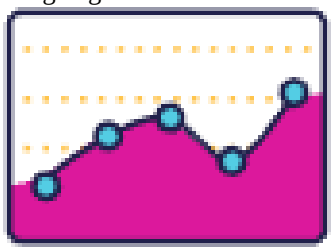
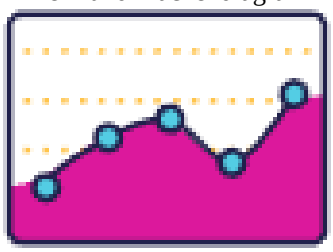
Service-Accounts

Dieser Indikator zeigt die Gesamtanzahl der im System definierten Service-Accounts und ihre Aufgliederung nach Cloud-Provider an.

Wählen Sie die unter einem beliebigen Cloud-Provider angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Servicekonten anzuzeigen.

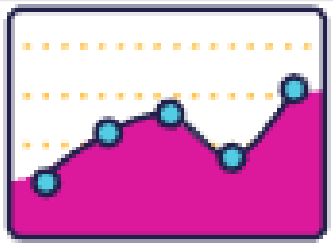
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Discovery-Ausführungen für 30 Tage	Ringdiagramm 	discovery_status	In diesem Bericht werden Anzahl und Status der Discovery-Ausführungen in den letzten 30 Tagen angezeigt. Von Cloud-Discovery werden die folgenden Status im Bericht angezeigt: • Aktiv • Abgebrochen • Abgeschlossen Wählen Sie den Bericht aus, um die Liste aller Erkennungen anzuzeigen.
Bevorstehende Zeitpläne	Liste	discovery_schedule	In diesem Bericht werden Informationen über bis zu acht bevorstehende geplante Erkennungen angezeigt. Wählen Sie einen Zeitplan aus, um die Details anzuzeigen.
Total configuration items (Gesamte Konfigurationselemente)	Linien- und Flächendiagramm 	cmdb_ci	In diesem Bericht wird die Anzahl der im Laufe der Zeit erkannten CIs angezeigt. Wählen Sie den Bericht aus, um die Liste aller bisher erkannten Konfigurationselemente anzuzeigen. Sie können einen beliebigen CI-Datensatz auswählen, um weitere Informationen zum CI und den zugehörigen Daten aus mehreren Quellen anzuzeigen, falls verfügbar.
Cloud-Discovery-Fehler	Linien- und Flächendiagramm	discovery_log	In diesem Bericht wird die Anzahl der Cloud-Discovery-Fehler im Zeitverlauf angezeigt. Wählen Sie den Bericht aus, um die Liste

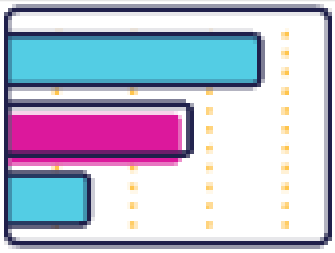
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			aller Cloud-Discovery-Fehler im Discovery-Protokoll anzuzeigen. Alternativ können Sie auf diese Informationen zugreifen, indem Sie zu navigieren **Diagnosen** > **Discovery-Protokoll**an.
Anmeldeinformationen	Indikator	discovery_credential	In diesem Bericht wird die Gesamtanzahl der im System definierten Anmeldeinformationen und ihre Aufgliederung nach Cloud Provider angezeigt. Wählen Sie die unter einem beliebigen Anmeldeinformationstyp angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Anmeldeinformationen anzuzeigen.
MID Server verwenden	Ringdiagramm 	ecc_agent	In diesem Bericht wird die Gesamtanzahl der MID Servers und ihr Status angezeigt.
Servicekonto	Indikator	cmdb_ci_cloud_service_account	In diesem Bericht wird die Gesamtanzahl der im System definierten Servicekonten und ihre Aufgliederung nach Cloud Provider angezeigt. Wählen Sie die unter einem beliebigen Cloud-Provider angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Servicekonten anzuzeigen.
Cloud-VMs nach Rechenzentrum	Horizontales Balkendiagramm	sn_disco_cd_vm_analytics	In diesem Bericht wird die Anzahl der pro

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Rechenzentrum erkannten VMs angezeigt. Von Cloud-Discovery wird dieser Bericht nur für Microsoft Azure-, Amazon Web Services(AWS)- und vCenter-Rechenzentren angezeigt.

Cloud-Discovery Zeitpläne-Dashboard in Cloud Operations Workspace

Das Zeitplan-Dashboard von Cloud-Discovery zeigt Informationen zur ausgewählten Discovery-Ausführung an.

Erforderliche ServiceNow AI Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin

Greifen Sie auf zu Cloud-Discovery Zeitpläne-Dashboard

Um das Dashboard zu öffnen, wechseln Sie zu: **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Zeitpläne**an.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Zeigen Sie die Ressourcenanzahl aus den letzten Discovery-Ausführungen an. • Zeigen Sie die für die letzten Discovery-Ausführungen benötigte Zeit an. • Zeigen Sie die Liste der neu erkannten CIs an. • Zeigen Sie die Liste der CIs an, die gegenüber der vorherigen Discovery-Ausführung fehlen. • Zeigen Sie die Anzahl der während der ausgewählten Discovery-Ausführung erkannten CIs an. • Zeigen Sie die Anzahl von Erkennungsfehlern an, die während der ausgewählten Discovery-Ausführung aufgetreten sind.

Indikatoren

Gesamtzahl der Ressourcen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Indikator zeigt die Gesamtanzahl der während der ausgewählten Discovery-Ausführung erkannten Configuration Items (CI) an.

Neu erkannt

Der Indikator zeigt die Anzahl der neuen CIs an, die während der ausgewählten Discovery-Ausführung erkannt wurden.

Abwesend vom letzten

Der Indikator zeigt die Anzahl der in der ausgewählten Discovery-Ausführung fehlenden CIs an. Das heißt, CIs wurden während der vorherigen Discovery-Ausführung erkannt, fehlen jedoch in der ausgewählten Discovery-Ausführung.

Fehler

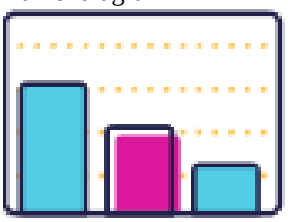
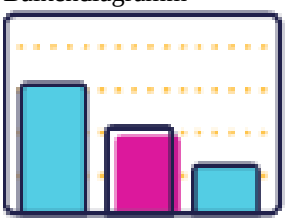
Der Indikator zeigt die Anzahl von Erkennungsfehlern, die während der ausgewählten Discovery-Ausführung aufgetreten sind.

Dauer

Der Indikator zeigt die Zeit an, die zum Abschließen der ausgewählten Discovery-Ausführung benötigt wurde.

Hinweis: Cloud-Discovery berechnet die Indikatoren **Neu erkannt** und **Abwesend vom letzten** nur für die musterbasierten Erkennungen.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Ressourcenanzahl laut letzten Discovery-Ausführungen	Balkendiagramm 	discovery_cloud_results	In diesem Bericht wird die Anzahl der CIs angezeigt, die während der letzten 10 Ausführungen des ausgewählten Discovery-Zeitplans erkannt wurden.
Zeit für letzte Discovery-Ausführungen	Balkendiagramm 	discovery_status	In diesem Bericht wird die Zeit angezeigt, die die letzten 10 Ausführungen des ausgewählten Discovery-Zeitplans bis zum Abschluss benötigt haben. Dieser Bericht umfasst sowohl abgeschlossene als auch abgebrochene Discovery-Durchläufe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter

Name	Typ	Beschreibung
Zeitplanfilter	Auswahlbasierter Filter	Standardmäßig sind in der Liste alle Cloud-Discovery-Zeitpläne in alphabetischer Reihenfolge aufgeführt, unabhängig vom aktuellen Ausführungsstatus. Verwenden Sie den Zeitplanfilter, um die Cloud-Discovery-Zeitpläne zu filtern. Sie können die Zeitpläne nach Cloud-Provider, Zeitplanname oder beidem filtern. Sie können die gefilterte Liste auch nach einem der folgenden Kriterien sortieren: • **Alphabetisch**: Sortieren Sie die Zeitplannamen alphabetisch. • **Fehler**: Sortieren Sie nach der Anzahl der während der Erkennung aufgetretenen Fehler. • **Discovery wird ausgeführt**: Sortieren Sie nach Status der Erkennung. Wählen Sie nach dem Filtern des Zeitplans die Discovery-Ausführung aus der Dropdown-Liste „Bericht“ aus, um ihre Daten im Zeitplan-Dashboard anzuzeigen, das auf der Registerkarte **Ergebnisse** angezeigt wird. **Hinweis:** Nur die letzten 10 Discovery-Ausführungen werden in der Dropdown-Liste „Bericht“ angezeigt.

Leistungsmetriken zu Erkennungen

Diese Discovery-Erweiterung sammelt Leistungsmetriken über die Probe-/Muster- und Sensorverarbeitungszeit und aggregiert diese Daten über die Zeit. Sie können Rollup-Daten verwenden, um die Leistung bestimmter Erkennungen zu überwachen oder um die Leistung zwischen Versionen nach einem Upgrade zu vergleichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken

Discovery stellt die folgenden einzelnen Leistungsmetriken bereit:

- Probe-Verarbeitungszeit und Musterverarbeitungszeit
- Sensorverarbeitungszeit
- Verarbeitungszeit der Identification and Reconciliation Engine (IRE) für Discovery-Muster. Diese Verarbeitungszeit ist bereits in der Sensorverarbeitungszeit enthalten, wird hier jedoch isoliert, um mehr Einblicke in Identifizierung und Abgleich von Musternutzlasten zu erhalten.

Discovery kann einzelne Metriken für diese Attribute zusammenfassen:

- Builds/Versionen
- Discovery-Status
- Ziel-IP-Adresse

Metrikzusammenfassungen auslösen

Metrik-Rollups werden wie folgt gestartet:

- **Nach Build zusammengefasst**: Implementiert durch die reguläre Aufgabe **Aggregate Discovery Probe And Sensor Metrics By Build (Metriken für Discovery-Probes und -Sensoren nach Build zusammenfassen)**. Diese Aufgabe wird um 02:00 Uhr Ortszeit ausgeführt.
- **Nach Status zusammengefasst**: Implementiert durch die Skriptaktion **Rollup Probe/Sensor Metrics by Status (Rollup-Probe-/Sensormetriken nach Status)**, die durch die registrierten Ereignisse **discovery.complete** und **discovery.cancelled** ausgelöst wird
- **Nach Ziel zusammengefasst**: Implementiert durch die Skriptaktion **Rollup Probe/Sensor Metrics by Target (Rollup-Probe-/Sensormetriken nach Ziel)**, die durch das registrierte Ereignis **discovery.device.complete** ausgelöst wird

Hinweis: Wenn die Discovery-Ausführung abgebrochen wird, bevor sie abgeschlossen ist, kann Discovery die Zusammenfassungstabelle der IP-Zielmetriken nicht aktualisieren. Das liegt daran, dass das Ereignis `discovery.device.complete`, das die Zusammenfassung auslöst, nicht ausgeführt wird. IP-Zieldaten für eine unterbrochene Erkennung werden erfasst, wenn nachfolgende Erkennungen erfolgreich auf dem Ziel ausgeführt werden. Das Abbrechen der Discovery-Ausführung wirkt sich nicht auf die Zusammenfassung anderer Metriken aus, die anders ausgelöst werden.

Tabellen

Discovery-Leistungsmetrikdaten werden in den folgenden Tabellen gespeichert:

Tabelle	Beschreibung
Probe- und Sensormetriken (einzeln) [discovery_perf_metric_probe_sensor]	Speichert die einzelnen Leistungsmetriken für Probe-/Muster-, Sensor- und IRE-Verarbeitungszeiten
Probe- und Sensormetriken (Zusammenfassung) [discovery_perf_metric_probe_sensor_rollup]	Dies ist die Basistabelle der Metrikzusammenfassung. Darin werden keine Daten gespeichert. Die drei Rollup-Tabellen „Nach Build“, „Nach Status“ und „Nach Ziel“ erweitern allesamt diese Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Probe- und Sensormetriken (nach Build zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_build]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach Build und Version
Probe- und Sensormetriken (nach Status zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_status]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach Discovery-Status
Probe- und Sensormetriken (nach Ziel zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_target]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach IP-Adresse

Discovery-Eigenschaften

Die Eigenschaften von Leistungsmetriken steuern, ob eine Zusammenfassung erfolgt, aber nicht, welche Daten in der Zusammenfassung enthalten sind. Status- und IP-Zieldaten werden wie folgt erfasst:

- Rollups für Status enthalten immer neue Daten. Discovery erfasst während der Erkennung kontinuierlich Daten für alle Probes und Sensoren für diesen Discovery-Status und speichert sie in der Tabelle „Probe- und Sensormetriken (einzeln)“ [discovery_perf_metric_probe_sensor]. Die Zusammenfassung fasst alle Probe-Daten und Sensordaten für diesen bestimmten Status zusammen, nachdem die Ereignisse `discovery.cancel` und `discovery.complete` für diesen Status ausgelöst wurden, jedoch nur, wenn die Zusammenfügungseigenschaft für Status-Rollups aktiviert ist.
- Discovery erfasst kontinuierlich Daten für IP-Ziele und speichert sie in der Tabelle „Probe- und Sensormetriken (einzeln)“ [discovery_perf_metric_probe_sensor]. Die Zusammenfassung führt für alle vorhandenen IP-Zieldaten einen Rollup durch, nachdem die Eigenschaft `glide.discovery.perf.metrics.rollup_by_target` aktiviert wurde, und erstellt Datensätze in der Tabelle „Probe- und Sensormetriken (nach Ziel zusammengefasst)“ [discovery_perf_metric_probe_sensor_rollup_by_target].

Die folgenden Eigenschaften steuern die Erfassung von Metriken für Probes und Sensoren:

Eigenschaft	Beschreibung
glide.discovery.perf.metrics.enable_collection	Aktiviert die Erfassung von Leistungsmetriken • **Typ**: true | false • **Standard**: true
glide.discovery.perf.metrics.rollup_by_build	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Build gruppiert ist • **Typ**: true | false • **Standard**: true
glide.discovery.perf.metrics.rollup_by_status	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Status gruppiert ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: true | false • **Standardwert:** false
glide.discovery.perf.metrics.rollup_by_target	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Ziel-IP-Adresse gruppiert ist. Standardmäßig erfasst Discovery kontinuierlich einzelne IP-Adressmetriken, auch wenn die Zusammenfassung nach Ziel-IP deaktiviert ist. Wenn Sie die Zusammenfassung für IP-Ziele aktivieren, schließt Discovery alle Zielmetriken in die Zusammenfassungstabelle ein. • **Typ**: true | false • **Standardwert:** false

Discovery-Leistungsmetriken für Probes, Sensoren und Muster anzeigen

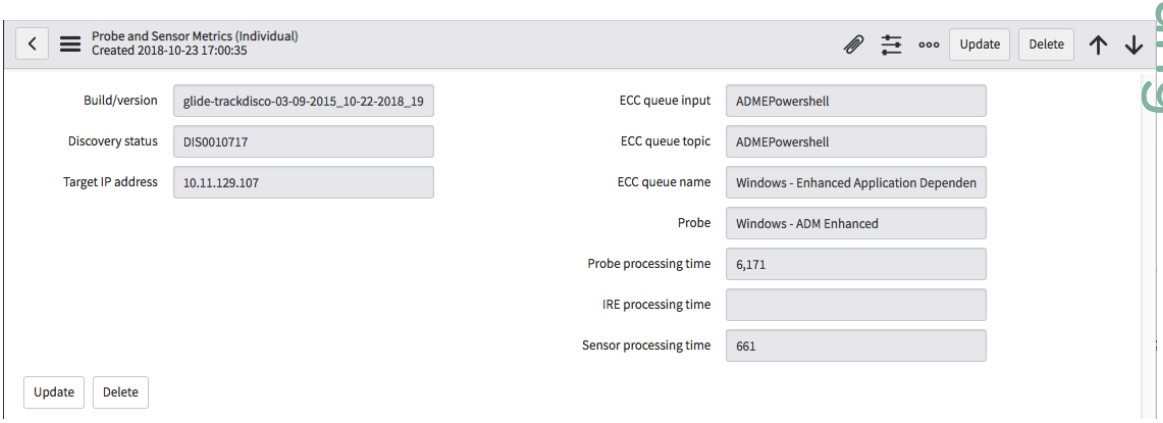
Standardmäßig verfolgt Discovery die Leistung einzelner Probes, Sensoren und Muster durch Messung der Verarbeitungszeit. Bei Verwendung von Mustern misst Discovery die Verarbeitungszeit der Identification and Reconciliation Engine (IRE).

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Leistungsmetriken** > **Probe/Sensor (Einzeln)**an.
2. Sortieren Sie die Liste nach dem Discovery-Status, um die Liste der Probes und Muster anzuzeigen, die in einer bestimmten Erkennung ausgeführt wurden.
3. Sie können die Metriken für jede Probe, jeden Sensor oder jedes Muster in der Liste anzeigen oder den Datensatz öffnen.
   Alle Metrikdaten für Probes und Sensoren sind schreibgeschützt.



Das Formular „Probe- und Sensormetriken (einzeln)“ enthält folgende Felder:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
Build/Version	build_version	Build, in dem die Erkennung ausgeführt wurde
Discovery-Status	discovery_status	ID-Nummer des Discovery-Status, von dem die Metriken erfasst wurden
Ziel-IP-Adresse	target_ip	IP-Adresse des Ziels für diese Erkennung
Eingabe für ECC-Warteschlange	ecc_queue_input	Identifiziert einen bestimmten ECC-Eingabedatensatz in der ECC-Warteschlangentabelle
ECC-Warteschlangenthema*	ecc_queue_topic	Identifiziert die Java-Klasse auf dem MID Server, der die Probe ausführt
ECC-Warteschlangenname*	ecc_queue_name	Identifiziert die Probe/das Muster, deren/dessen Leistung durch diese Zusammenfassung ausgewertet wurde
Probe*	probe	Name der für diese Erkennung verwendeten Probe
Probe-Verarbeitungszeit	probe_time	Interaktionszeit des MID Servers mit dem Ziel, einschließlich Erstellung der Nutzlast, die an die Instanz zurückgesendet wird. Die Zeit wird in Millisekunden angegeben.
IRE-Verarbeitungszeit	ire_time	Zeit, die für die Verarbeitung der Musternutzlast für die Instanz durch die Identification and Reconciliation Engine (IRE) erforderlich ist. Die IRE-Zeit ist nützlich, da sie den Teil der vom Muster verwendeten Sensorzeit anzeigt. Die Zeit wird in Millisekunden angegeben.
Sensorverarbeitungszeit	sensor_time	Zeit, die der Sensor zur Verarbeitung der Nutzlast für die Instanz für eine Erkennung benötigt hat. Die Zeit wird in Millisekunden angegeben.

*Wird zur eindeutigen Identifizierung einer Probe/eines Musters und des zugehörigen Sensors beim Erfassen von Metriken für eine Erkennung verwendet

Nach Build zusammengefasste Discovery-Leistungsmetriken anzeigen

Verwenden Sie die Rollup-Daten nach Build, um sicherzustellen, dass die Verarbeitungszeiten für Discovery-Komponenten für Erkennungen in einem 24-Stunden-Zeitraum konsistent bleiben. Zeigen Sie

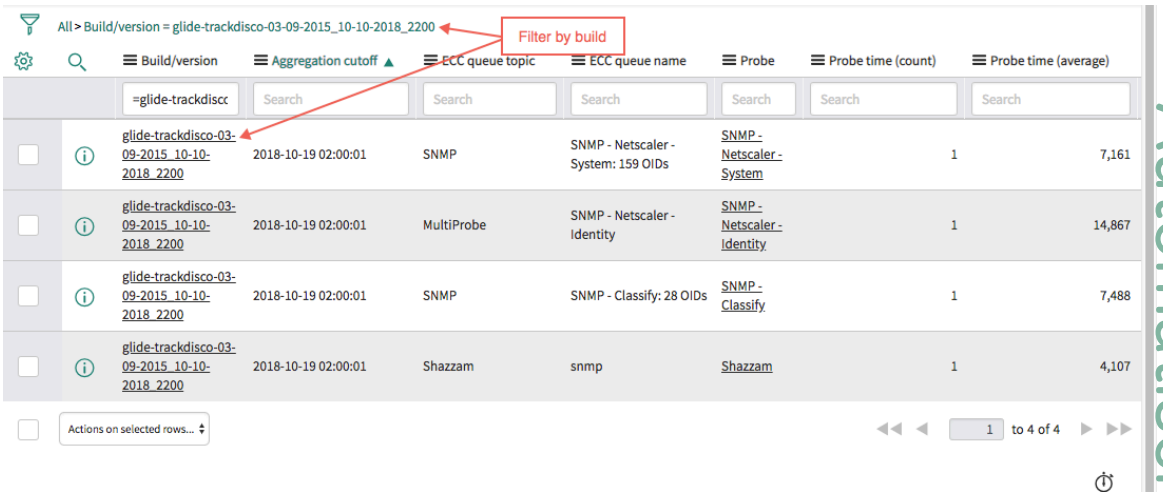
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zusammengefasste Build-Daten vor und nach einem Upgrade an, um die Leistung der alten und der neuen Version zu vergleichen. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Leistungsmetriken** > **Probe/Sensor (Rollup nach Build)**an.
2. Sortieren Sie die Liste nach **Build/Version**.



3. Filtern Sie nach einem bestimmten Build, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die eine Erkennung für diesen Build durchgeführt haben.
4. Öffnen Sie einen Datensatz, um die Statistiken für Probes/Muster für den ausgewählten Build anzuzeigen. Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollup-Berechnungen beziehen sich auf einen 24-Stunden-Zeitraum und beginnen jede Nacht um 02:00 Uhr.
5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Build angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Nach Status zusammengefasste Discovery-Leistungsmetriken anzeigen

Verwenden Sie die Rollup-Daten nach Status, um sicherzustellen, dass die Verarbeitungszeiten für Probes, Muster und Sensoren für eine bestimmte Erkennung konsistent bleiben. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

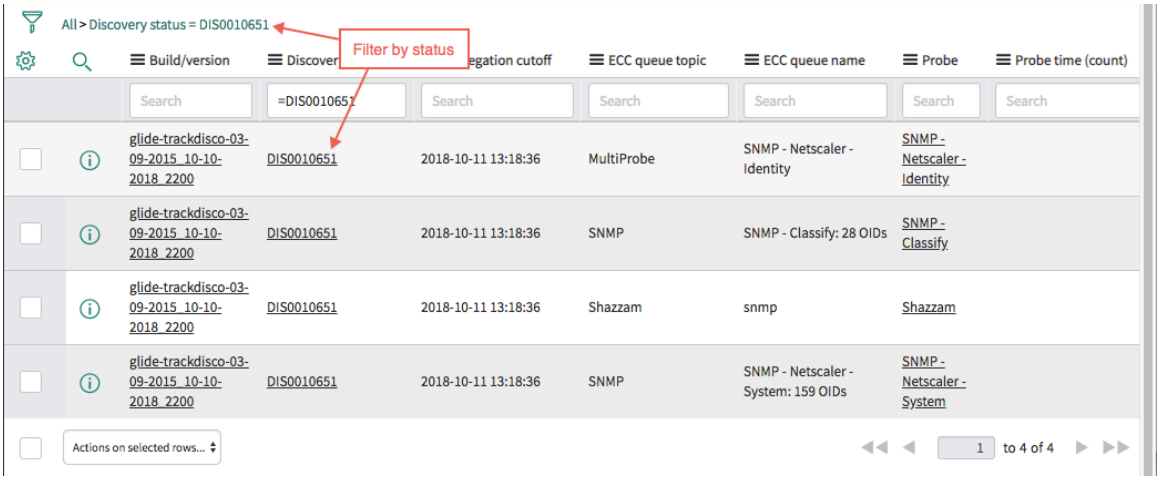
Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Leistungsmetriken** > **Probe/Sensor (Rollup nach Status)**an.
2. Sortieren Sie die Liste nach **Discovery-Status**, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die in einer bestimmten Erkennung ausgeführt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Filtern Sie nach einem bestimmten Status, um für in diesem Status ausgeführte Probes und Muster verfügbare Metriken anzuzeigen.
4. Öffnen Sie einen Datensatz, um die Statistiken für Probes/Muster für den ausgewählten Status anzuzeigen. Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollups werden nur für den Status „Abgeschlossen“ oder „Abgebrochen“ erstellt.
5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Status angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Nach IP-Adresse zusammengefasste Discovery-Leistungsmetriken anzeigen

Verwenden Sie die Rollup-Daten nach Ziel, um sicherzustellen, dass die Verarbeitungszeiten für Probes, Muster und Sensoren für jede Erkennung einer bestimmten IP-Adresse konsistent bleiben. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

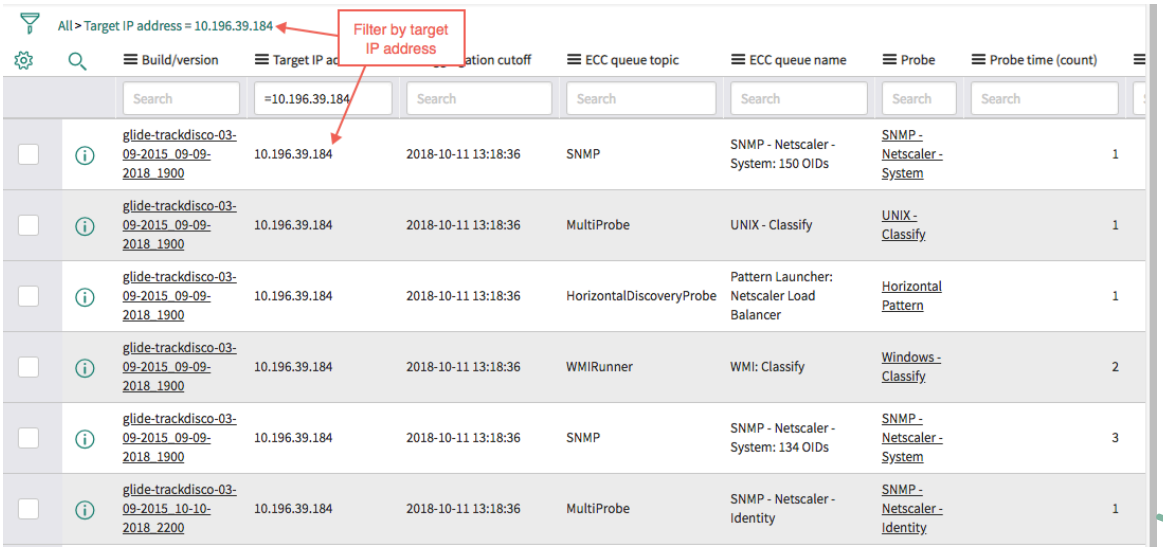
Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Leistungsmetriken** > **Probe/Sensor (Rollup nach Ziel)**an.
2. Sortieren Sie die Liste nach **Ziel-IP-Adresse**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Filtern Sie nach einer bestimmten IP-Adresse, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die eine Erkennung für diese IP-Adresse durchgeführt haben.
4. Öffnen Sie einen Datensatz, um die Statistiken für die/das ausgewählte Probe/Muster für die spezifische IP-Adresse anzuzeigen.
   Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollups werden durchgeführt, nachdem IP Discovery erfolgreich abgeschlossen wurde.
5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Ziel angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Zusammengefasste Daten für Discovery-Leistungsmetriken

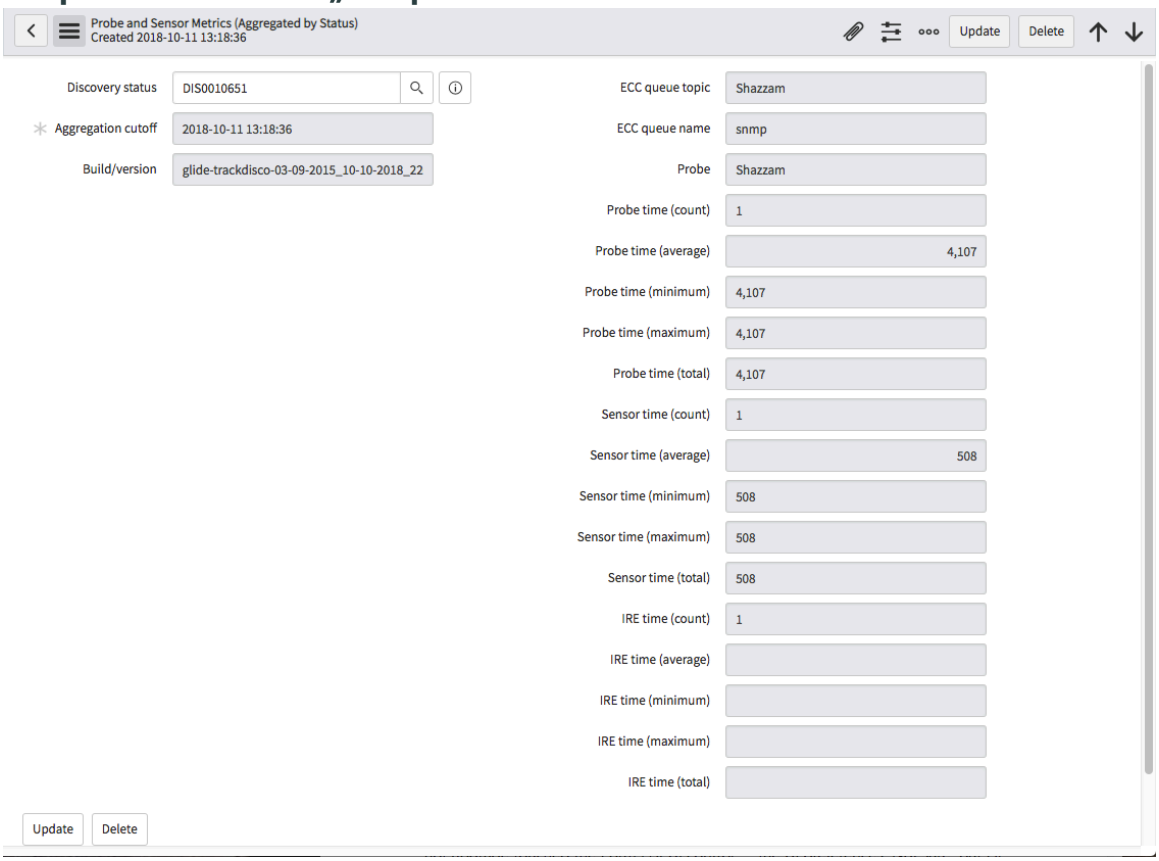
Discovery-Leistungsmetriken können bei jeder Discovery-Ausführung Daten für Probes, Muster und Sensoren zusammentragen. Discovery berechnet die Verarbeitungszeiten und erhöht die Anzahl der Ausführungen einer Komponente für jedes Rollup-Profil: Status, Ziel oder Build. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

Beispiel für Rollup-Formular

Dies ist ein Beispiel für einen Zusammenfassungsdatensatz für Metriken über Probes und Sensoren. Die hier angezeigten Metrikfelder werden für jede Zusammenfassung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für das Formular „Rollup nach Status“



Zusammengefasste Daten für Leistungs-Framework

Sofern nicht anders angegeben, gelten diese Felder für alle Zusammenfassungsdatensätze.

Feldbezeichnung	Feldname	Beschreibung
Build/Version	build_version	Der Name des Build, der auf der Instanz ausgeführt wird. Dieser Name identifiziert Version, Patch-Ebene und Release-Datum von ServiceNow Platform.
Discovery-Status	discovery_status	ID-Nummer des Discovery-Statusdatensatzes für diese Zusammenfassung **Hinweis:** Dieses Feld wird nur im Formular für Rollups nach Status angezeigt.
Ziel-IP-Adresse	target_ip_address	IP-Adresse des Ziels für diese Erkennung **Hinweis:** Dieses Feld wird nur im Formular für Rollups nach Ziel angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
Ende der Zusammenfassung	aggregation_cutoff	Der Endzeitpunkt variiert je nach Rollup-Profil. • **Nach Build**: Standardmäßig täglich um 02:00 Uhr • **Nach Status**: Abschlusszeit der letzten Zusammenfassung für diesen Discovery-Status, der möglicherweise ausgeführt wurde, als **discovery.complete** oder **discovery.cancelled** für diesen Status ausgeführt wurde • **Nach Ziel**: Abschlusszeit der letzten Zusammenfassung für diese Ziel-IP-Adresse, die möglicherweise ausgeführt wurde, als **discovery.device.complete** für diese IP-Adresse ausgeführt wurde
ECC-Warteschlangenthema*	ecc_queue_topic	Identifiziert die Java-Klasse auf dem MID Server, der die Probe ausführt
ECC-Warteschlangenname*	ecc_queue_name	Identifiziert die Probe/das Muster, deren/dessen Leistung durch diese Zusammenfassung ausgewertet wurde
Probe*	probe	Name der für diese Erkennung verwendeten Probe
Probe-Zeit (Anzahl)	probe_time_count	Anzahl der Ausführungen einer Probe für ein bestimmtes Rollup-Profil
Probe-Zeit (Durchschnitt)	probe_time_average	Durchschnittliche Zeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Probe-Zeit (Minimum)	probe_time_min	Minimale Zeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Probe-Zeit (Maximum)	probe_time_max	Maximale Zeit, die eine Probe benötigt hat, um Daten zu einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
		Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Probe-Zeit (gesamt)	probe_time_total	Gesamtzeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Sensorzeit (Anzahl)	sensor_time_count	Anzahl der Verarbeitungen von Nutzlasten durch einen Sensor für ein bestimmtes Rollup-Profil
Sensorzeit (Durchschnitt)	sensor_time_average	Durchschnittliche Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (Minimum)	sensor_time_min	Minimale Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (Maximum)	sensor_time_max	Maximale Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (gesamt)	sensor_time_total	Gesamtzeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Anzahl)	ire_time_count	Anzahl der Verarbeitungen der Nutzlast eines Musters durch die Identification and Reconciliation Engine (IRE) für ein bestimmtes Rollup-Profil
IRE-Zeit (Durchschnitt)	ire_time_average	Durchschnittliche Zeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Minimum)	ire_time_min	Minimale Zeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Maximum)	ire_time_max	Maximale Zeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (gesamt)	ire_time_total	Gesamtzeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

* Zusammen identifizieren diese Werte eindeutig ein für eine Erkennung verwendetes Probe/Sensor-Paar (eine „Probe-Ausführung“).

Discovery-Fehlermeldungen

Im System werden Fehlermeldungen und Warnungen dokumentiert, damit Benutzer Probleme erkennen und Maßnahmen ergreifen können, um diese zu beheben.

Allgemeine Fehlermeldungen

Eingabe-/Ausgabefehler

- CONNECTION_FAILED
- CONNECTION_TIMEOUT
- CONNECTION_REFUSED
- CONNECTION_CIPHER_UNSUPPORTED
- CONNECTION_PROTOCOL_UNSUPPORTED
- CONNECTION_LOST
- INVALID_CONNECTION_PARAMETER
- FILE_NOT_FOUND
- IO_ERROR

Authentifizierungsfehler

- NO_CREDENTIALS
- AUTHENTICATION_FAILED
- INVALID_CREDENTIALS_TYPE

SSH-Fehler

- SSH_SHELL_UNSUPPORTED
- SSH_SCRIPT_TRANSFER_FAILED
- SSH_INVALID_SESSION

Windows-Fehler

POWER_SHELL_VERSION_UNSUPPORTED

Befehlsfehler

- COMMAND_TIMEOUT
- INVALID_COMMAND
- COMMAND_FILTER_ERROR
- COMMAND_PARSER_ERROR
- COMMAND_KEY_MAPPER_ERROR
- COMMAND_VALUE_NORMALIZER_ERROR
- TERMINAL_SESSION_LOST_ERROR
- TERMINAL_SESSION_ENVIRONMENT_MODIFICATION_ERROR

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Generische Komponentenfehler

- INVALID_COMPONENT
- INVALID_COMPONENT_PARAMETER
- INVALID_OPERATION

Allgemeine Fehlermeldungen

Nachricht: org.xml.sax.SAXParseException: The entity name must immediately follow the '&' in the entity reference

Eine Version dieser Nachricht wird angezeigt, wenn Sie Sonderzeichen in einem Passwort verwendet haben, das in einer XML-Datei gespeichert ist.

Nachricht: Identified, ignored extra IP

Diese Nachricht kann am Ende der Klassifizierungsphase von Discovery angezeigt werden, wenn eine Ziel-IP-Adresse zu einem Gerät gehört, das gleichzeitig erkannt wird.

Beispiel: Ein Windows-Server verfügt über zwei NIC-Karten mit zwei IP-Adressen. Beide IP-Adressen liegen im selben Erkennungszeitplan innerhalb des Zielbereichs von Discovery. Diese Nachricht wird generiert, um darauf hinzuweisen, dass die zweite IP-Adresse ignoriert wird, da dasselbe CI innerhalb einer Discovery-Ausführung nicht zweimal aktualisiert werden soll.

Diese Nachricht ist eine zu erwartende Warnung. Es ist keine Aktion erforderlich.

Nachricht: Authentication failures

Der Erkennungsprozess konnte das CI nicht erkennen, da die Erkennungsanwendung nicht authentifiziert werden konnte. Um diesen Fehler zu beheben, fügen Sie der Tabelle „Discovery-Anmeldeinformationen“ die Anmeldeinformationen dieses Computers hinzu.

Nachricht: Identified, not updating CI, now finished

Keine Übereinstimmung mit einem der CI-Bezeichner

Nachricht: The impersonation of user failed

Diese Nachricht stammt aus der PowerShell. Überprüfen Sie, ob die Domäne zusammen mit dem Benutzernamen in den Anmeldeinformationen angegeben ist.

Nachricht: Connection failed to WMI service. Error: Permission denied

Diese Nachricht stammt aus WMI. Überprüfen Sie, ob der MID-Server-Service mit den richtigen Anmeldeinformationen ausgeführt wird und Zugriff auf das Zielgerät hat.

Um dies zu überprüfen, führen Sie auf dem MID-Server-Host in der Eingabeaufforderung den folgenden Befehl aus:

```
wmic /node:target /user:user /password:password path win32_operatingsystem
target = IP address of target device
user = user account used by the mid server service
password = password used by the mid server service
```

Nachricht: Connection failed to WMI service. Error: The remote server machine does not exist or is unavailable

Diese Nachricht stammt aus WMI. Überprüfen Sie, ob das MID-Server-Servicekonto Zugriff auf den Zielcomputer hat. Überprüfen Sie, ob als MID-Server-Servicekonto ein Domänenadministratorkonto verwendet wird. Überprüfen Sie, ob vorhandene Firewalls für die Verbindung geöffnet sind. Um dies zu überprüfen, führen Sie auf dem MID-Server-Host in der Eingabeaufforderung den folgenden Befehl aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie ihn aus für runner_type = WMI:

```
wmic /node:"<target>" /user:"<user>" /password:"<password>" path
 win32_operatingsystem
From within a Powershell console on the mid server host, execute for
 runner_type=Powershell:
gwmi win32_operatingsystem -computer <ip> -credential '<username>'
```

Nachricht: Provider is not capable of the attempted operation

Das WMI-Repository wurde beschädigt. Durch Befolgen der Anweisungen im Artikel „WMI: Repository Corruption, or Not?“ (WMI: Beschädigung des Repository: ja oder nein?) auf der Microsoft TechNet-Website lässt sich das Problem beheben.

Nachricht: The result file can't be fetched because it doesn't exist

PRB581515 - Powershell does not work when customer has locked down write rights to admin share (Powershell funktioniert nicht, wenn der Kunde Schreibrechte für Administratorfreigabe gesperrt hat)

Nachricht: Please run sneep as root to ensure correct serial number from fserial data source

Damit die Probe „Solaris - Serial Number“ ordnungsgemäß funktioniert, muss das Oracle-Befehlszeilentool **Sneep** installiert sein. Es gibt eine bekannte Einschränkung bei Fujitsu PRIMEPOWER-Geräten. Um diese Einschränkung zu umgehen, führen Sie die Solaris-Erkennung mit Root-Anmeldeinformationen aus.

Discovery-Fehlermeldungen für Sensoren

Nachricht: The multisensor will not process because its major version = X while probe_name responding script's major version = Y

Die obige Fehlermeldung zeigt an, dass eine Nichtübereinstimmung der Hauptversion vorliegt.

Nachricht: Nutzlastlänge überschreitet den Grenzwert von 5000000

Die obige Fehlermeldung zeigt an, dass die Discovery-Probe-Ergebnisse den Grenzwert überschreiten. Die MID-Server Verwerfen die Ergebnisse und gibt eine Warnmeldung zurück. Legen Sie zum Lösen den Wert von fest `mid.discovery.max_payload_size` MID-Server Eigenschaft für eine beliebige negative Zahl (z. B. -1), um das Nutzlastlimit zu deaktivieren und zu ermöglichen, dass Nutzlasten beliebiger Größe an die Instanz gesendet werden können.

Nachricht: The multisensor will not process because its responding script's major version = X while its referenced probe probe_name major version = Y

Die obige Fehlermeldung zeigt an, dass eine Nichtübereinstimmung der Hauptversion vorliegt.

Nachricht: sensor_name sensor's major version = X while its related probe's major version = Y

Die obige Fehlermeldung zeigt an, dass die Probe- und Sensorversionen eine Nichtübereinstimmung der Hauptversion aufweisen. Der Sensor stoppt die Verarbeitung, bis diese Bedingung gelöst ist.

Message: sensor_name multisensor's minor version = X while probe_name responding script's minor version = Y

Die obige Fehlermeldung zeigt an, dass eine geringfügige Versionsabweichung vorliegt.

Nachricht: sensor_name multisensor's responding script's minor version = X while its referenced probe probe_name minor version = Y

Die obige Fehlermeldung zeigt an, dass eine geringfügige Versionsabweichung vorliegt.

Nachricht: sensor_name sensor's minor version = X while its related probe's minor version = Y

Die obige Fehlermeldung zeigt an, dass die Probe- und Sensorversionen nicht übereinstimmen. Die Verarbeitung wird fortgesetzt, Sie können diese Bedingung jedoch lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Meldung: Sensorfehler bei der Verarbeitung von . . . : Keine Sensoren definiert

Jede aktive Probe sucht nach einem entsprechenden Sensor, um die von der Probe erfassten Daten zu verarbeiten. Die obige Fehlermeldung zeigt an, dass der entsprechende Sensor für die Probe fehlt oder inaktiv ist.

Meldung: Sensorfehler bei der Verarbeitung von . . . : TypeError: . . .

Die obige Fehlermeldung gibt an, dass der Sensor einen der Kernfehlerkonstruktoren in JavaScript hat.

Meldung: Sensorfehler bei der Verarbeitung von ...: Ausnahme beim Verarbeiten des Sensors: XML-Analyseproblem: ![CDATA]

Dieser XML-Analysefehler tritt auf, wenn der Discovery-Sensor die Nutzlast der ECC-Eingabewarteschlange nicht analysieren kann. Die Nutzlast ist nicht gemäß XML-Spezifikationen formatiert. Mögliche Lösungen:

- Verwenden Sie für problematische Zeichen Maskierungszeichen. Ändern Sie beispielsweise **<** in **&lt** und **&** in **&amp**.
- Verwenden Sie Maskierungszeichen für ganze Textblöcke mit CDATA-Abschnitten oder Codierungsdeklarationen am Anfang des Texts.
- Entfernen Sie alle Leerzeichen (Leerzeichen, Tabulatorzeichen, Zeilenumbrüche) vor XML-Deklarationen.

Meldung: Sensorfehler bei der Verarbeitung von Linux – Netzwerk-ARP-Tabellen: Ausnahme beim Ausführen des Probe-Nachverarbeitungsskripts: Keine XML-Daten

Das System zeigt den Fehler „No XML data (Keine XML-Daten)“ an, wenn der XML-Sensorprozessor in der Probe-Ausgabe nicht die erwarteten XML-Daten findet. Während der Sensorverarbeitung versucht Discovery, die Probe-Ergebnisse abzurufen, die Probe-Ausgabe ist jedoch leer. Prüfen Sie, ob die Probe die richtige Ausgabe für die Verarbeitung durch den Sensor zurückgibt.

Meldung: Sensorfehler bei der Verarbeitung von Shazzam: Ausnahme beim Ausführen des Nachverarbeitungsskripts für Probe: Probe nicht gefunden: Null

Der Fehler „Probe not found (Probe nicht gefunden)“ tritt auf, wenn der Sensorprozessor den vermeintlich mit dem Sensor verknüpften Probe-Datensatz nicht findet. Während der Sensorverarbeitung ruft Discovery den Probe-Datensatz aus dem Probe-Cache ab und speichert ihn zur späteren Referenz. Der Fehler „Probe not found (Probe nicht gefunden)“ tritt auf, wenn die sys_id der Probe nicht gefunden werden kann oder wenn ein Problem mit dem Probe-Cache vorliegt.

Weitere Informationen finden Sie unter Nach Ursache für Fehler „Probe not found (Probe nicht gefunden)“ suchen.

Suche nach der Ursache einer Sensorfehlermeldung

Verwenden Sie dieses Verfahren, um einen Discovery-Sensorfehler zu identifizieren.

Vorbereitungen

Erforderliche Rolle: sn_Cloud_OPS_WS.Cloud_OPS_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Prozess müssen Sie Folgendes identifizieren:

- Den Fehler
- Den Namen des Sensors, bei dem der Fehler aufgetreten ist
- Den Datumsstempel des Fehlers
- Den zugeordneten Stack Trace des Fehlers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Führen Sie je nach verwendeter Anwendung eine der folgenden Aktionen aus:
   - Um anzuzeigen **Discovery-Protokoll** In Cloud Operations Workspace, Navigieren Sie zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Discovery-Protokoll**an.
   - Um anzuzeigen **Discovery-Protokoll** In Discovery, Navigieren Sie zu **Alle** > **Discovery** > **Discovery-Protokoll**an.
2. Um den Fehler zu finden, filtern Sie nach dem **Ebenennamen** des **Fehlers**.
   Wenn Sie Discovery verwenden, können Sie auch den Fehler und den Datumsstempel im Fehlerbericht anzeigen. Der Bericht ist im Discovery-Dashboard verfügbar.
3. Beachten Sie das Feld **Erstellt** im Fehlerdatensatz.
   Dieser Zeitstempel wird verwendet, um den richtigen Stack Trace zu finden.
4. Beachten Sie das Feld **Kurznachricht** im Fehlerdatensatz.
   Dieses Feld zeigt den Namen des Sensors, bei dem der Fehler aufgetreten ist.
5. Navigieren Sie zu , um die Stapelverfolgung zu suchen **Systemprotokolle** > **Fehler**an.
6. Suchen Sie nach Datum und Uhrzeit, die dem Wert in entsprechen **Erstellt** Feld des Fehlerdatensatzes in Discovery Protokoll.
7. Das Feld **Nachricht** dieses Eintrags enthält den vollständigen Stack Trace des Fehlers.
   Der Stack Trace enthält die Fehlermeldung, die sys_id des Skripts und die Nummer der Zeile, in der der Fehler aufgetreten ist.
8. Nachdem Sie die Fehlerdetails ermittelt haben, können Sie die JavaScript-Datei reparieren.

Suchen Sie die Ursache der Fehlermeldung „kein Sensor definiert“

Jede aktive Probe sucht nach einem entsprechenden Sensor, um die von der Probe erfassten Daten zu verarbeiten. Die Meldung „keine Sensoren definiert“ gibt an, dass der entsprechende Sensor für die Probe fehlt oder inaktiv ist.

Vorbereitungen

Erforderliche Rolle: sn_Cloud_OPS_WS.Cloud_OPS_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Um die Ursache dieses Fehlers zu finden, identifizieren Sie **Kurznachricht** Feld des Fehlerdatensatzes. Dieses Feld zeigt den Namen der Probe an, für die der Sensor fehlt.

Prozedur

1. Führen Sie je nach verwendeter Anwendung einen der folgenden Schritte aus:
   - Um die Ursache des Fehlers mit zu identifizieren Cloud Operations Workspace, Navigieren Sie zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Diagnosen** > **Discovery-Protokoll**an.
   - Um die Ursache des Fehlers mit zu identifizieren Discovery, Navigieren Sie zu **Alle** > **Discovery** > **Ausgabe und Artefakte** > **Discovery-Protokoll**an.
2. Filtern Sie **Ebene** Spalte nach **Fehler** .
   Wenn Sie Discovery verwenden, finden Sie den Fehlerbericht auch im Discovery-Dashboard.
3. Beachten Sie das Feld **Kurznachricht** im Fehlerdatensatz.
   Dieses Feld zeigt den Namen des Sensors, bei dem der Fehler aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ursache einer Sensorfehlermeldung beheben

Zum Beheben einer Discovery-Sensorfehlermeldung müssen Sie die JavaScript-Datei korrigieren, die den Code enthält, der den Fehler generiert hat.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

So korrigieren Sie die JavaScript-Datei:

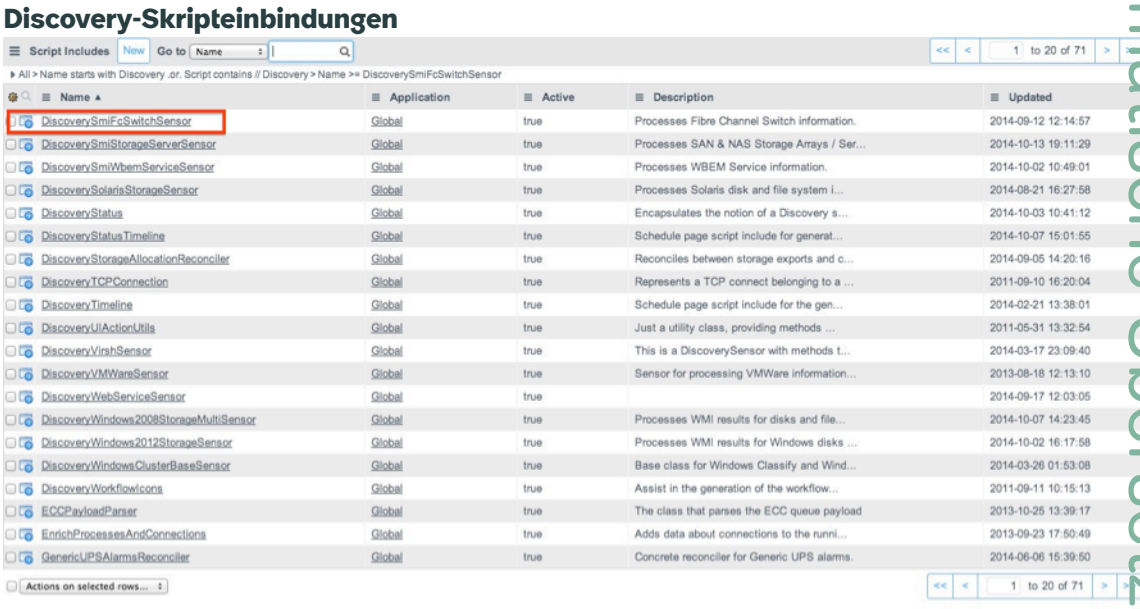
Prozedur

1. Navigieren Sie in Discovery zu dem Modul, in dem der Fehler aufgetreten ist.

   Navigieren Sie in diesem Beispiel zu **Discovery-Definition** > **Skripteinbindungen**an.

2. Korrigieren Sie den Fehler.

   a. In diesem Beispiel suchen Sie nach DiscoverySmiFcSwitchSensor im Feld **Name**.



   b. Klicken Sie auf den Link, um zur Detailseite für diese Skripteinbindung zu wechseln.

   c. Ändern Sie das JavaScript-Skript auf dieser Seite, um den angegebenen Fehler zu beheben.

   d. Klicken Sie auf **Aktualisieren**.

Nach Ursache für Fehler „Probe not found (Probe nicht gefunden)“ suchen

Überprüfen Sie die korrekte sys_id der Probe, die dem Parameter *probe* in der Nutzlast des Datensatzes für die ECC-Warteschlangeneingabe zugeordnet ist.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Notieren Sie sich die sys_id der Probe, die in der Nutzlast der ECC-Warteschlange angezeigt wird.

Nutzlastbeispiel für ECC-Warteschlange

```
▼<parameters>
    <parameter name="port" value="22"/>
    <parameter name="probe" value="10e0eebd0a0a0b4f61f46a5027df7fb6"/>
    <parameter name="priority" value="0"/>
    <parameter name="use_class" value="discovery_classy_unix"/>
```

2. Navigieren zu **Discovery-Definition** > **Probes** Und öffnen Sie den Datensatz für die Probe, die Sie überprüfen möchten.
3. Klicken Sie mit der rechten Maustaste auf den Header des Datensatzes.
4. Wählen Sie im Kontextmenü **sys_id kopieren**.
   Befolgen Sie die Anweisungen des Browsers, um die sys_id zu kopieren, falls die Sicherheitsmaßnahmen des Browsers diese Funktion einschränken.
5. Vergleichen Sie diesen Wert mit der sys_id der Probe aus der Nutzlast.
   Wenn die sys_id des Probe-Datensatzes nicht mit dem Wert in der Nutzlast übereinstimmt, versuchen Sie, die Ursache für den falschen Wert zu ermitteln.

Cloud-Discovery-Fehler in Cloud Operations Workspace beheben

Zeigen Sie die während der Erkennung aufgetretenen Cloud-Discovery-Fehler an und beheben Sie sie. Sie können die Fehler für alle Cloud-Discovery-Ausführungen oder eine einzelne Cloud-Discovery-Ausführung anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_cloud_ops_ws.cloud_ops_admin

Prozedur

1. Navigieren zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery**an.
2. Wählen Sie **Fehler** aus.
   Die Registerkarte **Status** des Moduls „Zeitpläne“ zeigt die Liste der Fehler für die ausgewählte Discovery-Ausführung an.
3. Wählen Sie eine Kategoriekachel aus, um die spezifischen Fehlercodes anzuzeigen, die in dieser Kategorie aufgetreten sind.
4. Wählen Sie die Kachel für den Fehlercode aus, den Sie untersuchen möchten.
   In der Liste werden alle Vorkommen dieses Fehlercodes für alle Cloud-Discovery-Zeitpläne angezeigt. Die Liste zeigt die Fehlermeldung, die ID des Configuration Item (CI), die IP-Adresse jeder Instanz, bei der der Fehler aufgetreten ist, und den Fehlerstatus an.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die spezifischen Fehler aus und wählen Sie dann die entsprechende Aktion im Abschnitt **Selected errors** (Ausgewählte Fehler) aus.
   - Wählen Sie die entsprechende Aktion im Abschnitt **Alle Fehler** aus.

     Von Cloud-Discovery wird die ausgewählte Aktion auf alle Fehler in der Liste angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Aktionen

Aktion	Beschreibung
Aufgabe erstellen	Sie können eine Fehleraufgabe erstellen und einem Benutzer zur Lösung zuweisen. Zugewiesene Fehler gelten als **Aktive Fehler**, für die noch Aktionen ausgeführt werden können. Cloud-Discovery zeigt die Nummer der Fehleraufgabe auf der Fehlercode-Kachel an.
Erkennung wiederholen	Cloud-Discovery versucht erneut eine IP-basierte Erkennung. Wenn Sie **Discovery wiederholen** auswählen, wird diese Aktion von Cloud-Discovery für alle aktiven Fehler ausgeführt, die in der Liste verfügbar sind. Sie können die Erkennung nur wiederholen, wenn das Plugin „ServiceNow® IP-based Discovery“ (com.snc.discovery.ip_based) in der Instanz installiert und aktiviert ist.
Ignorieren	Cloud-Discovery ignoriert den Fehler.

6. Überprüfen Sie die Spalte **Fehlerstatus**, um die Ergebnisse der Fehlerkorrektur anzuzeigen.
   Einzelne Wiederholungsversuche werden schnell abgeschlossen. Neuversuche für eine große Anzahl von IP-Adressen können mehrere Minuten dauern.

   Fehler können einen der folgenden Status aufweisen:

   - **Aktiver Fehler**: Der Fehler ist nicht gelöst. Das ist der Standardstatus aller neuen Fehler.
   - **Gelöst**: Der Fehler ist behoben.
   - **Zugewiesen**: Zur Behebung dieses Fehlers ist eine Aufgabe zugewiesen.
   - **Ausstehende Erkennung**: Es wird darauf gewartet, dass Discovery gestartet wird, nachdem Sie die Aktion **Discovery wiederholen** für alle Fehler ausgeführt haben.
   - **In Erkennung**: Discovery ist derzeit aktiv.

Discovery – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Discovery-Listen und -Formularen.

Cloud-Discovery-Referenz

Referenzthemen enthalten zusätzliche Informationen zu den in verwendeten Listen, Formularen und Cloud-Einstellungen Cloud-Discovery.

Cloud-Discovery Referenz des Service-Account-Formulars

Das Cloud-Discovery-Formular „Servicekonto“ zeigt detaillierte Informationen zum ausgewählten Cloud-Provider an. Die Cloud-Discovery Das Formular „Service-Account“ ist in verfügbar Cloud Operations Workspace.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Web Services (AWS) – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen.
Account-ID	12-stellige IAM-Kontonummer (Identity and Access Management)
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die AWS-Erkennung erstellt haben. Wenn der Account ein Mitgliedsaccount einer AWS-Organisation ist und Sie den zugeordneten Verwaltungsaccount mit Anmeldeinformationen konfiguriert haben, lassen Sie dieses Feld leer. Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für AWS finden Sie unter Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren.
URL	URL des Rechenzentrums. Geben Sie dieses Feld nur für ein AWS GovCloud (USA) und AWS Accounts der Region China.
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.
Select account for access (Konto für Zugriff auswählen)	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, die keine permanenten AWS-Anmeldeinformationen verwenden und für den Zugriff IAM-Rollen ausnutzen.

Felder des Microsoft Azure-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Microsoft Azure-Abonnements
Subscription ID (Abonnement-ID)/ Management group ID (Verwaltungsgruppen-ID)	Microsoft Azure-Abonnement-ID
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die Microsoft Azure-Erkennung erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des Microsoft Azure-Servicekontos (Fortsetzung)

Feld	Beschreibung
	Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars „Azure-Service-Prinzipal“ finden Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern.
URL	URL des Rechenzentrums. Die Konfiguration dieses Felds ist für erforderlich Azure GovCloud (USA)-Accounts. Fügen Sie die erforderliche URL hinzu.
Ereignisse Abrufen	Option, um in der ServiceNow AI Platform das Sammeln von Informationen über Ressourcen-Changes aus der Microsoft Azure-Cloud zu aktivieren. Die ServiceNow AI Platform verwendet die Informationen über Ressourcen-Changes zur Aktualisierung der Configuration Management Database (CMDB). Weitere Informationen zu den unterstützten Azure-Ressourcentypen finden Sie unter Azure Change-Verarbeitung. Wenn Sie das Kontrollkästchen Ereignisse abrufen für eine Verwaltungsgruppe aktivieren, wird die aktiviert ServiceNow AI Platform Aktiviert Azure Change-Verarbeitung für alle Abonnements in der Verwaltungsgruppe.

Felder des Google Cloud Platform-Servicekontos

Feld	Beschreibung
Service-Account	Projekt-ID des Google Cloud Platform (GCP)-Projekts, dessen Ressourcen Sie erkennen möchten. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Projekt-ID des Google Cloud Platform (GCP)-Projekts.
Project ID (Projekt-ID)/Folder ID (Ordner-ID)	Projekt-ID des Google-Projekts
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die GCP-Erkennung erstellt haben. Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit API-Anmeldeinformationen für Google finden Sie unter Erkennung von Google Cloud Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des Google Cloud Platform-Servicekontos (Fortsetzung)

Feld	Beschreibung
Ereignisse Abrufen	Option zum Aktivieren der eventgesteuerten ServiceNow®-Erkennung zum Sammeln von Events für die in den Google-Projekt-LDCs gehosteten Ressourcentypen.

Felder des IBM-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die IBM-Erkennung erstellt haben. Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für IBM finden Sie unter Erkennung von IBM-Clouds.
Account-ID	IBM-Software-Anwendernummer, die in der Instanz für den Zugriff auf die IBM Cloud-Konsole verwendet werden soll

Oracle Cloud Infrastructure – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Account-ID	OCI-Compartment-ID
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die Erkennung der Oracle Cloud Infrastructure (OCI) erstellt haben. Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit API-Anmeldeinformationen für Oracle finden Sie unter Oracle Cloud Infrastructure (OCI)-Discovery.
Rechenzentrums-URL	Rechenzentrumswert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Cloud Infrastructure – Servicekonto-Felder (Fortsetzung)

Feld	Beschreibung
	Beispiel: https://$service.ap-mumbai-1.oraclecloud.com

OpenStack – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
OpenStack account ID (OpenStack-Konto-ID)	Projekt-ID des OpenStack-Projekts, das erkannt werden soll
Account credentials (Kontoanmeldeinformationen)	Name der Anmeldeinformationen, die Sie für die OpenStack-Discovery erstellt haben Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für OpenStack finden Sie unter OpenStack-Ressourcenerkennung.
Cloud URL	OpenStack-Identitätsservice-Endpunkt. Beispiel: https://<openstack dns>:<port>.

Red Hat Virtualization (RHV) – Servicekonto-Felder

Feld	Beschreibung
Servicekonto	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Manager URL	Konto-ID, zu der diese Anmeldeinformationen gehören. Geben Sie die API-URL der RHV-M-Instanz an, einschließlich des Ports. Beispiel: https://my-manager-instance.com:443
Manager credentials (Manager-Anmeldeinformationen)	Name der Anmeldeinformationen, die Sie für die RHV-Discovery erstellt haben Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Red Hat Virtualization (RHV) – Servicekonto-Felder (Fortsetzung)

Feld	Beschreibung
	„Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für RHV finden Sie unter Oracle Linux Virtualisierungsmanager und Red hat Virtualization Discovery.

Felder des VMware-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
UUID	Universeller eindeutiger Bezeichner (Universal Unique Identifier, UUID) der Instanz. So greifen Sie auf die UUID zu: 1. Öffnen Sie den Browser für verwaltete Objekte (Managed Object Browser, MOB) für vCenter. 2. Auswahlvorgang **Inhalt** > **Über**an. 3. Fügen Sie den Wert der Instanz-UUID-Eigenschaft in dieses Feld ein.
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die VMware-Erkennung erstellt haben. Um in ServiceNow AI Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für VMware finden Sie unter VMware-Anmeldeinformationen .
URL	Vollständige vCenter-URL

Formularreferenz für Einstellungen bearbeiten

Das Formular „Einstellungen bearbeiten“ zeigt Informationen zu an Amazon Web Services(AWS) Einstellungen, die zum Aufzeichnen und Bereitstellen von verwendet werden AWS Ereignisse zum Abhörendpunkt.

Formular „Einstellungen bearbeiten“

Feld	Beschreibung
Allgemeine Einstellungen	
Ressourcentypen, die aufgezeichnet werden sollen	Ressourcentypen, für die Sie die Konfigurationsänderung aufzeichnen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Einstellungen bearbeiten“ (Fortsetzung)

Feld	Beschreibung
	Geben Sie auch an, ob Sie die Konfigurationsänderung für globale Ressourcen wie erfassen möchten AWS AMI-Ressourcen. Weitere Informationen finden Sie unter Auswählen der AWS-Konfigurationsdatensätze für Ressourcen Thema in AWS Dokumentation.
Datenaufbewahrungszeitraum	(Optional) Aufbewahrungsrichtlinie für die aufgezeichneten Ereignisse.
AWS Konfigurationsrolle	Eine AWS-Rolle, die auf die folgenden Services und Ressourcen zugreifen kann: • Simple Notification Service (SNS) • AWS-Konfigurationsservice • Ressourcentypen, für die Sie die Konfigurationsänderung nachverfolgen möchten
Liefermethode	
AWS S3-Bucket	Ein AWS S3-Bucket zum Speichern der aufgezeichneten Ereignisse. Erstellen Sie einen AWS S3-Bucket, oder wählen Sie einen vorhandenen aus AWS S3-Bucket, auf den Sie Zugriff haben.
Streamen Sie Konfigurationsänderungen und -Benachrichtigungen an einen Amazon SNS-Thema	Option zum Veröffentlichen der Ereignisbenachrichtigungen im SNS-Thema.
Amazon SNS-Thema	Amazon SNS-Thema, zu dem AWS Der Konfigurationsservice muss die Ereignisse veröffentlichen. 1. Wählen Sie aus **Wählen Sie ein Thema aus Ihrem Account aus** Option. 2. Wählen Sie aus Amazon SNS-Thema in Schritt erstellt 3 Aus der Dropdownliste SNS-Themenname.

Formular „Befehlsvalidierungsaufgaben“ für musterbasierte Discovery

Aufgaben Zur Befehlsvalidierung Das Formular zeigt die Felder an, die Sie ausfüllen müssen, wenn Sie eine Aufgabe zum Testen eines Musterbefehls erstellen oder ändern.

Weitere Informationen zum Testen von Musterbefehlen finden Sie unter Validiert Befehle, die in der musterbasierten Discovery verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Nummer	Die Aufgabennummer wird automatisch vom System erstellt.
Methode für MID Server-Auswahl	Wählen Sie die relevante Methode aus: • **Spezifischer MID Server**: Zum Definieren des MID Servers für diesen Test. • **Automatische MID-Auswahl** – Zur Verwendung eines MID-Servers, der dem IP-Bereich oder IP-Netzwerk zugewiesen ist, den Sie für den Test verwenden möchten. Wählen Sie diese Methode nur aus, wenn Sie einen MID-Server mit IP-Bereichen konfiguriert haben oder als Standard-MID-Server für Discovery. • **Try All Eligible MID Servers** (Alle berechtigten MID Server testen): Zur Verwendung eines beliebigen MID Servers, der für den IP-Bereich oder das IP-Netzwerk verfügbar ist, den/das Sie für den Test verwenden möchten. Wählen Sie diese Methode nur aus, wenn Sie einen MID-Server mit IP-Bereichen konfiguriert haben oder als Standard-MID-Server für Discovery.
MID Server	Name des MID-Server s. Dieses Feld wird nur angezeigt, wenn unter **Methoden für MID Server-Auswahl** die Option **Spezifischer MID Server** ausgewählt ist.
Alle Musterbefehle validieren	Das Kontrollkästchen zum gleichzeitigen Validieren aller Befehle, die von einem bestimmten Muster verwendet werden.
Betriebssystemklasse	CI-Klasse, die die Server darstellt, auf denen Sie diese Validierungsaufgabe ausführen.
Befehlstyp	Befehlstyp, der von der Art des Servers abhängt: • **Shell-Befehl** • **WMI-Abfrage** • **SNMP-Abfrage** (tabellarisch und skalar) • **SNMP-Walk** • **HTTP GET** (für Anmeldeinformationen für Standardauthentifizierung, nicht für Token)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld ist nur verfügbar, wenn **Validiert AI-Musterbefehle** Ist nicht ausgewählt.
IP-Adressen	Beliebige Kombination aus IP v4-Adressen, IP-Bereichen oder IP-Netzwerken. Zum Beispiel: • 10.196.39.12, 10.196.39.12: Kommagetrennte IP-Adressen für eine Liste eigenständiger Adressen. • 1.1.1.1-1.1.1.100: Durch Bindestriche getrennte IP-Adressen für einen IP-Bereich. • 1.1.1.1/28: Schrägstrichschreibweise für ein IP-Netzwerk. **Hinweis:** Vergewissern Sie sich, dass Sie die Skripteinbindung ParseIPRanges installiert haben, wenn Sie einen IP-Bereich oder ein IP-Netzwerk verwenden möchten. Weitere Informationen finden Sie unter KB1123625: Tool zur Befehlsvalidierung .
Befehle	Die Befehle, für die Sie Anmeldeinformationen testen möchten. Normalerweise handelt es sich dabei um einen Befehl, der vom Discovery-Prozess nicht ausgeführt werden konnte. Beispiel: **/api/v1/pods?limit=50** oder **sudo dmidecode**. Sie können nur Befehle aus der Liste der verfügbaren Befehle auswählen. Dieses Feld ist nur verfügbar, wenn **Validiert Alle Musterbefehle** Ist nicht ausgewählt.
Muster	Der Name des Musters, für das Sie die Befehle validieren möchten. Dieses Feld ist nur verfügbar, wenn **Validiert Alle Musterbefehle** Ist nicht ausgewählt.

Zugehörige Informationen

Befehlslistenformular für musterbasierte Discovery

Discovery Befehle für Probes und Muster

Befehlslistenformular für musterbasierte Discovery

Die **Befehlsliste** Das Formular enthält alle in der Discovery verwendeten Befehle nach Infrastruktur- oder Anwendungstypmustern.

Informationen zum Anzeigen einer Liste von Befehlen, die von einem Muster verwendet werden, finden Sie unter Zeigen Sie Befehle an, die in der musterbasierten Discovery verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Befehlsliste

Attribut	Beschreibung
Anwendbare Betriebssystemklasse	Der Befehl soll auf dieser BS-Klasse ausgeführt werden.
CI-Typ	Das Muster, das diesen Befehl enthält, ist diesem CI-Typ zugewiesen. **Hinweis:** Einige ServiceNow-Anwendungen bezeichnen CI-Typen als CI-Klassen.
Befehl	Der Discovery-Befehl.
Befehlstyp	Typ des Befehls: • **Shell-Befehl** • **WMI-Abfrage** • **SNMP-Abfrage** (tabellarisch und skalar) • **SNMP-Walk** • **HTTP GET** (für Anmeldeinformationen für Standardauthentifizierung, nicht für Token)
Ist Failover-Schritt	Dieser Befehl wird in einem Failover-Schritt innerhalb eines Musters verwendet. Mögliche Werte sind „wahr“ oder „falsch“.
Veraltet	Dieses Feld ist zur internen Verwendung vorgesehen. Mögliche Werte sind „wahr“ oder „falsch“.
Muster	Der Befehl ist Teil dieses Discovery-Musters.
Schrittname	Name des Schritts, der diesen Befehl enthält.
Domäne	Der Befehl wird für die Erkennung von CIs in dieser Domäne validiert. Dieses Feld gilt für eine domänengetrennte Umgebung.

Zugehörige Informationen

Formular „Befehlsvalidierungsaufgaben“ für musterbasierte Discovery

Discovery Befehle für Probes und Muster

Details zu Discovery-Protokollen

Discovery-Protokolle enthalten Informationen zum horizontalen Discovery-Prozess basierend auf Probes und Mustern.

Zugehörige Liste „Discovery-Protokoll“

Die zugehörige Liste „Discovery-Protokoll“ enthält Informationen zur horizontalen Erkennung basierend auf Probes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Discovery-Protokoll enthält die folgenden Informationen:

Feld	Eingabewert
Erstellt	Zeitstempel der Discovery Aktivität. Jeder Zeitstempel definiert die ungefähre Zeit der Aktivität. Mehrere Discovery Ereignisse können in zufälliger Reihenfolge innerhalb einer Sekunde auftreten.
Ebene	Klassifiziert die Aktivität in eine der folgenden Ebenen für die allgemeine Sortierung: • Fehler • Informationen • Warnung
Kurznachricht	Informative Nachricht, in der das Ergebnis der Aktivität oder der Discovery-Fortschritt angezeigt wird. Suchen Sie hier nach dem Ergebnis eines Klassifizierungs-Tests oder nach einem Authentifizierungsfehler.
Eingabe für ECC-Warteschlange	Der zugehörige Eingabedatensatz aus der ECC-Queue für diese Ermittlung. Sie können diese Datensätze auch in der verwandten Liste **ECC-Queue** anzeigen.
CI	Benennt ein Gerät, für das in der CMDB ein übereinstimmendes CI gefunden wurde. Wählen Sie den Link aus, um den CI-Datensatz für das Gerät anzuzeigen.
Quelle	Benennt die bestimmte Aktivität, z. B. die Shazzam-Sonde oder eine UNIX-Klassifizierungs-Sonde.
Gerät	Listet die IP-Adresse des erkannten CI auf. Alle durch die IP-Adresse identifizierten Geräte werden im Protokoll angezeigt, auch wenn sie alle Einladungen zur Kommunikation abgelehnt haben. Jede Portaktivität von einem Gerät speichert sie in das Protokoll, auch wenn alle nachfolgenden Versuche zur Identifizierung fehlschlagen. Wählen Sie die IP-Adresse des Geräts aus, um die Ereignisse anzuzeigen, die mit der Erkennung dieses Geräts verknüpft sind.

Horizontales Discovery-Protokoll

Das Fenster „Horizontales Discovery-Protokoll“ enthält Informationen zur musterbasierten horizontalen Erkennung.

Discovery-Protokollelement	Beschreibung
Pre Pattern Execution	Aktionen, die vor dem Start des Musters ausgeführt wurden
Selecting Pattern for Execution	Das Muster, das für die Erkennung ausgeführt wurde
{Identification Section name}	Zeigt die Ergebnisse der Vorgänge im Muster an. Erweitern Sie den Namen, um die einzelnen Vorgänge anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Protokollelement	Beschreibung
Pre Payload Processing Scripts	Die Ergebnisse der Skripts, die ausgeführt wurden, bevor die Nutzlast empfangen wurde
Payload Processing	Details zur Nutzlast und ihrer Verarbeitung. Suchen Sie nach Fehlern, die möglicherweise bei verschiedenen Aktivitäten aufgetreten sind, zum Beispiel beim Ausführen von Identifizierungsregeln und Aktualisierungen der CMDB.
Post Payload Processing Scripts	Die Ergebnisse der Skripts, die ausgeführt wurden, nachdem die Nutzlast empfangen wurde

Formularreferenz für Discovery-Zeitplan

Das Formular „Discovery-Zeitplan“ enthält Details zu den Konfigurationselementen (Configuration Items, CIs), die für die Discovery bestimmt sind, den zugehörigen MID-Server und die Zeitplaneinstellungen, wann und wie die Discovery ausgeführt wird.

Anweisungen zu diesem Verfahren finden Sie unter Horizontale Erkennung planen.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen, beschreibenden Namen für den Zeitplan ein.
Erkennen	Wählen Sie einen der folgenden Scantypen aus: • **Konfigurationselemente**: Verwendet Discovery-Bezeichner dazu, Geräte mit CIs in der CMDB abzugleichen und die CMDB entsprechend zu aktualisieren. Führen Sie eine einfache Erkennung durch, indem Sie einen bestimmten MID-Server auswählen, um nach allen Protokollen (SSH, WMI und SNMP) zu scannen. Oder führen Sie erweiterte Erkennungen anhand von Discovery-Verhalten durch. Wenn Sie ein Verhalten auswählen, wird *MID-Server* Feld ist nicht verfügbar. **Hinweis:** Ein IPv6-Adresslistenscan ist auf aktiviert Discovery Zeitplan für Konfigurationselemente. • **IP-Adressen**: Scannt Geräte, ohne Anmeldeinformationen zu benutzen. Diese Scans erkennen alle aktiven IP-Adressen im angegebenen Bereich und erstellen Geräteverlaufsdatensätze, aktualisieren jedoch nicht CMDB. Bei Scans von IP-Adressen werden auch mehrere IP-Adressen angezeigt, die auf einem einzelnen Gerät ausgeführt werden. Identifizieren Sie Geräte nach Klasse und Typ, zum Beispiel Windows-Computer und Cisco-Netzwerkgeräte. Die Eigenschaft *Max. Bereichsgröße* der Shazzam-Probe bestimmt die maximale Anzahl von IP-Adressen, die von Shazzam gescannt werden. Details siehe Shazzam-Probe konfigurieren. • **Netzwerke**: Erkennt IP-Netzwerke (Router und Switches). Ergebnisse dieser Suche werden verwendet, um die Tabelle „IP-Netzwerk“ [cmdb_ci_ip_Network] in auszufüllen **Discovery** > **IP-Netzwerke** Mit einer Liste von IP-Adressen und Netzwerkmasken. Netzwerkscans aktualisieren Router und Layer-3-Switches in der CMDB. • **Service**: Es werden Services für die Anwendung Service-Mapping erkannt. Anweisungen dazu finden Sie unter Erkennung von oben nach unten mithilfe von Service-Mapping planen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“ (Fortsetzung)

Feld	Beschreibung
	• **Ohne Server**: CIs werden gefunden, ohne dass eine Erkennung eines Hosts oder von CIs auf einem Proxy-Host ausgeführt werden muss, der sich bereits in der CMDB befindet. Weitere Informationen finden Sie unter Serverlose Erkennung. • **Cloud-Applikation**: Erkennt nur die Cloud-Ressourcen für die von Ihnen angegebenen Muster. Anweisungen dazu finden Sie unter Cloud-Discovery erkunden. • **Cloud-Ressourcen**: Erkennt Ressourcen für einen der unterstützten Cloud Provider. Diese Option wird nur angezeigt, wenn Sie Discovery unter einem Cloud-Servicekonto ausführen. Sie können es nicht aus einem neuen auswählen Discovery Zeitplan. • **Zertifikate**: Erkennt Zertifikate basierend auf URLs. Durch Auswahl dieser Option wird das Feld „Typ der Zertifikaterkennung“: „URL-Zertifikaterkennung“ hinzugefügt. Weitere Informationen finden Sie unter Zertifikaterkennung über individuelle URL-Scans ausführen.
Methode für MID-Server-Auswahl	Wählen Sie die Methode aus, die von Discovery zur MID-Server-Auswahl verwendet wird: • **MID-Server automatisch auswählen** : Aktivieren Discovery Um auszuwählen MID-Server Automatisch basierend auf den von Ihnen konfigurierten Discovery-IP-Bereichen. Um einen passenden MID-Server zu finden, müssen Sie MID Servers so konfigurieren, dass Folgendes verwendet wird: ◦ Die Discovery-Anwendung oder ALLE Anwendungen. Diese Einstellung gewährt Discovery Zugriff auf den MID-Server. ◦ Der IP-Bereich, der die Bereiche enthält, die Sie im Discovery-Zeitplan konfigurieren. **Hinweis:** MID-Server Die automatische Auswahl wird mit IPv6 nicht unterstützt. • **Spezifischer MID Server-Cluster**: Verwenden Sie einen vorkonfigurierten Cluster von MID Servers n. Wählen Sie das Cluster aus. Sie müssen kein Mitglied des Clusters angeben. Die MID-Server Kann nicht Teil mehrerer Cluster sein, z. B. eines, der den Lastenausgleich und eines, der Failover unterstützt. Sie können einen beliebigen Cluster hinzufügen, unabhängig von der Anwendung, der die MID Servers zugewiesen sind. Wenn Sie den Cluster auswählen, wird die **Discovery** Anwendung wird automatisch hinzugefügt, wenn sie für nicht vorhanden ist MID Servers Im Cluster. • **Spezifischer MID Server**: Verwenden Sie nur einen MID-Server. Wenn dieser MID-Server Teil eines Clusters ist, wird nur dieser MID-Server verwendet. Der Cluster wird nicht verwendet. Sie können beliebige hinzufügen MID-Server Unabhängig von der Anwendung, der sie zugewiesen ist. Die **Discovery** Anwendung wird automatisch hinzugefügt, wenn sie nicht bereits für zugewiesen ist MID-Server Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“ (Fortsetzung)

Feld	Beschreibung
	wählen aus. Sie können einen spezifischen MID-Server für alle Arten von Discovery-Scans außer **Service** zuweisen. • **Verhalten verwenden**: Verwenden Sie ein Verhalten, wenn für einen einzelnen Zeitplan die Verwendung mehrerer MID Servers erforderlich ist, damit eine der folgenden Aktivitäten ausgeführt werden kann: ◦ Scans, die mehrere Windows-Anmeldeinformationen erfordern ◦ Ein Zeitplan, der mindestens zwei bestimmte Protokolle (SNMP, SSH oder WMI) mit mehr als einem MID-Server ausführen muss. ◦ Lastenausgleich für umfangreiche Erkennungen, bei denen ein einzelner MID-Server nicht ausreicht. ◦ Scannen mehrerer Domänen **Hinweis:** Der Discovery-Zeitplan erzwingt die Domänentrennung. Die zur Auswahl verfügbaren MID Servers müssen sich in derselben Domäne wie der Benutzer befinden, der den Zeitplan konfiguriert. Weitere Informationen finden Sie unter MID Server-Auswahlreihenfolge für Erkennungszeitpläne.
MID-Server	Wählen Sie den MID-Server für diesen Zeitplan aus. Dieses Feld ist verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Spezifischer MID Server* festgelegt ist oder wenn eine Erkennung von IP-Adressen, Netzwerken oder Webservices durchgeführt wird. Um zu überprüfen, dass MID-Server Sie haben ausgewählt, ist aktiv und validiert. Sehen Sie sich die an MID-Server-Dashboard .
MID-Server-Cluster	Wählen Sie den MID-Server-Cluster für diesen Zeitplan aus. Dieses Feld ist verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Spezieller MID Server-Cluster* festgelegt ist.
Verhalten	Wählen Sie ein Verhalten aus, das für die MID Servers in Ihrem Netzwerk konfiguriert ist. Dieses Feld ist nur verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Verhalten verwenden* festgelegt ist.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diesen Zeitplan zu aktivieren. Wenn Sie das Kontrollkästchen deaktivieren, ist der Zeitplan inaktiv, Sie können eine Discovery jedoch weiterhin manuell über dieses Formular mithilfe der konfigurierten Werte ausführen.
Standort	Wählen Sie ein Verzeichnis aus, das den vom Zeitplan erkannten CIs zugewiesen werden soll. Wenn dieses Feld leer ist, wird kein Standort zugewiesen.
Max. Ausführungszeit	Legen Sie eine Zeitbegrenzung für die Ausführung dieses Zeitplans fest. Wenn die konfigurierte Zeit verstrichen ist, werden die verbleibenden Aufgaben für die Discovery abgebrochen, auch wenn der Scan nicht abgeschlossen ist. Verwenden Sie dieses Feld, um die Systemlast auf ein gewünschtes Zeitfenster zu beschränken. Wenn in dieses Feld kein Wert eingegeben wird, wird dieser Zeitplan solange ausgeführt, bis er abgeschlossen ist.
Max. Leerlaufzeit	Legen Sie eine Zeitgrenze für Inaktivität während der Discovery fest, um verzögerte Prozesse automatisch abzubrechen und das Ereignis zu protokollieren. Eine Discovery wird nur dann als inaktiv betrachtet, wenn keine Eingabedatensätze verarbeitet werden und nichts im Verarbeitungsstatus verbleibt. Die Leerlaufzeit wird vom letzten Change

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“ (Fortsetzung)

Feld	Beschreibung
	zu einem ECC-Warteschlangendatensatz gemessen. Die konfigurierte Leerlaufzeit wird zu Beginn der Discovery festgelegt und spiegelt bis zur nächsten Ausführung keine Änderungen wider. Wenn in dieses Feld kein Wert eingegeben wird, wird dieser Zeitplan bis zum Abschluss oder Abbruch ausgeführt.
„Ausführen“ und zugehörige Felder	Bestimmt den Ausführungszeitplan der Erkennung. Konfigurieren Sie die Häufigkeit im Feld **Ausführen** und in den anderen Feldern, die angezeigt werden, um eine genaue Zeit anzugeben. **Hinweis:** Die Laufzeit verwendet die Systemzeitzone. Wenn Sie das optionale Feld **Als tz ausführen** hinzufügen, hat dies keine Auswirkungen auf die tatsächliche Ausführungszeit.
Statusänderungen protokollieren	Aktivieren Sie dieses Kontrollkästchen, um immer dann einen Protokolleintrag zu erstellen, wenn sich der Status während einer Erkennung ändert, zum Beispiel wenn sich die Einstellung für ein Gerät von *Aktiv* zu *Classifying (Wird klassifiziert)* ändert. Zeigen Sie die Discovery-status aus der zugehörigen Liste Discovery-Geräte im Formular Discovery-Status an. Die Felder *Abgeschlossene Aktivität* und *Aktuelle Aktivität* zeigen die Status an.
Shazzam-Batch-Größe	Geben Sie die Anzahl der IP-Adressen ein, die jede Shazzam-Probe scannen kann. Die Aufteilung der IP-Adressen in Batches verbessert die Leistung, indem die Klassifizierung für jeden Batch nach Abschluss des Batches beginnt und nicht nach dem Scannen aller IP-Adressen. Die Probes werden sequenziell ausgeführt. Beispiel: Der Wert ist auf 1.000 festgelegt, und bei einer Erkennung werden 10.000 IP-Adressen mit einem einzelnen MID-Server gescannt. Es werden 10 Shazzam-Probes erstellt, wobei jede Probe 1000 IP-Adressen scannt. Standardmäßig beträgt die Batch-Größe 1000. Eine UI-Richtlinie erzwingt eine minimale Batch-Größe von 256, da Batch-Größen unter 256 IP-Adressen nicht vom Clustering profitieren. Die Richtlinie konvertiert einen beliebigen Wert unter 256 in den Wert 0. Der Wert für dieses Feld darf den in der Eigenschaft „maximale Bereichsgröße“ für die Shazzam-Probe definierten Wert nicht überschreiten.
Discovery Service Desk-Mitarbeiter	Wählen Sie den Service Desk-Mitarbeiter aus, um diese Discovery durchzuführen: • **AWS-MID** : Verwenden AWS SSM zum Durchführen der Discovery. • **MID** : Verwenden Sie MID-Server Dient zum Durchführen der Discovery. Standardmäßig ist Discovery Agent ist auf MID festgelegt. Dieses Feld ist nur verfügbar, wenn die Systemeigenschaft vorhanden ist `glide.discovery.enable_ssm`lst aktiviert, die **Erkennen** Typ ist auf festgelegt **Konfigurationselemente** , Und **Ausführen nach** Das Feld ist so konfiguriert, dass es einem Zeitplan für Cloud-Ressourcen folgt.
Shazzam-Cluster-Unterstützung	Aktivieren Sie das Kontrollkästchen, um die Shazzam-Verarbeitung auf mehrere MID Servers in einem Cluster zu verteilen und die Leistung zu verbessern. Diese Einstellung wird mit der Shazzam-Batch-Größe verwendet. Beispielsweise wird ein Zeitplan erstellt, um 100.000 IP-Adressen mit 10 zu scannen MID ServersZugewiesen, um die Arbeit auszuführen. Jedem MID-Server sind 10.000 IP-Adressen zum Scannen zugewiesen. Wenn die Shazzam-Batch-Größe auf 5.000 IP-Adressen pro Probe festgelegt ist, führt der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“ (Fortsetzung)

Feld	Beschreibung
	Zeitplan zwei Shazzam-Probes pro MID-Server (10.000 IP-Adressen/5.000 pro Batch) aus. Diese Probes werden nacheinander und nicht gleichzeitig ausgeführt.
SNMP-Version verwenden	Verwenden Sie dieses Feld, um die SNMP-Version anzugeben, die für diese Erkennung verwendet werden soll. Der Standardwert lautet **ALLE**. Sie können diesen Wert in ändern **v1** , **V2c** , Oder **V3** .
Batch-Größe für URL-Zertifikat	Definieren Sie die Anzahl der URLs, die pro Batch während der Discovery erkannt werden sollen. Lassen Sie die Batch-Größe unverändert. Ändern Sie sie nur, wenn dies empfohlen wird.
Kurzbereiche	Definieren Sie zu scannende IP-Adressen und Adressbereiche, indem Sie IP-Adressen in mehreren Formaten (Netzwerk, Bereich oder Liste) in einer einzelnen kommagetrennten Zeichenfolge eingeben. Weitere Informationen finden Sie unter Erstellen Sie einen schnellen IP-Bereich für einen Discovery Zeitplan.
Discovery starten	Verwenden Sie diesen Link, um diese Discovery sofort zu starten.
Zugehörige Listen	
IP-Bereiche	Diese zugehörige Liste definiert die IP-Adressbereiche, die mit diesem Zeitplan gescannt werden sollen. Wenn Sie einen einfachen CI-Scan verwenden (kein Verhalten), verwenden Sie diese zugehörige Liste, um die zu erkennenden IP-Adressen zu definieren. **Hinweis:** Um die Sicherheit zu verbessern, beschränken Sie den Bereich der Erkennungsziele, indem Sie unnötige Netzwerke und Geräte ausschließen.
Discovery Bereiche	Diese zugehörige Liste definiert jedes Range Set, das in einem Zeitplan zur Überprüfung durch mindestens eine Shazzam-Probe festgelegt ist.
Discovery-Status	Diese zugehörige Liste zeigt die Ergebnisse aktueller und vergangener Ausführungen des Zeitplans an.
Zertifikat-URLs	Diese zugehörige Liste zeigt die URLs an, die mit diesem Zeitplan erkannt werden. Sie können URLs dieser Liste hinzufügen oder daraus löschen.

Erstellen Sie einen neuen Discovery-Zeitplan-Formularreferenz

Das Formular Neuen Discovery-Zeitplan erstellen zeigt Informationen zum Zeitplan und zum Ziel-Cloud-Anbieter an. Das Formular Neuen Discovery-Zeitplan erstellen ist in verfügbar Cloud Operations Workspace.

Anweisungen zu diesem Verfahren finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Anbieterformular auswählen

Feld	Beschreibung
Name des Discovery-Zeitplans	Name des Discovery-Zeitplans.
Cloud-Anbieter	Name des Cloud-Anbieters, der die zu erkennenden Ressourcen hostet.
MID-Auswahltypen	MID-Server oder MID-Cluster, den Sie zum Erkennen der Cloud-Ressourcen verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anbieterformular auswählen (Fortsetzung)

Feld	Beschreibung
	Die folgenden Optionen sind verfügbar: • MID-Server automatisch auswählen: Discovery verwendet automatisch einen geeigneten MID-Server. • Spezifischer MID-Server-Cluster: Discovery verwendet den im Feld „MID-Cluster“ angegebenen MID-Cluster. • Spezifischer MID-Server: Discovery verwendet den im MID-Server-Feld angegebenen MID-Server. Wenn der ausgewählte MID-Server Teil eines MID-Clusters ist, werden die Aufträge gleichmäßig auf alle MID Servers dieses Clusters verteilt. Dieses Feld wird nur angezeigt, wenn einer der folgenden Werte im Feld „Cloud-Anbieter“ ausgewählt ist: • AWS • Azure • Google
MID-Cluster	MID-Cluster, die Sie mit dem Cloud-Discovery-Zeitplan verwenden möchten. Dieses Feld wird nur angezeigt, wenn im Feld „MID-Auswahltypen“ der Wert „Spezifischer MID-Server-Cluster“ ausgewählt ist.
Discovery ohne Anmeldeinformationen	Option zur Verwendung der Discovery ohne Anmeldeinformationen. Um die MID Servers anzuzeigen und zu filtern, die eine IAM-Rolle annehmen können, um die Cloud-Ressourcen zu erkennen, schieben Sie den Schalter **Discovery ohne Anmeldeinformationen** nach rechts.
MID Servers	MID Servers, die Sie mit dem Cloud-Discovery-Zeitplan verwenden möchten. Dieses Feld wird nur angezeigt, wenn im Feld „MID-Auswahltypen“ der Wert „Spezifischer MID-Server“ ausgewählt ist.

Discovery-Administratorarbeitsbereich – Referenz

Referenzthemen enthalten zusätzliche Informationen zu den in verwendeten Listen, Formularen und Einstellungen Discovery-Administratorarbeitsbereich.

Discovery-Administratorarbeitsbereich Support-Tools

Die **Support-Tools** Die Registerkarte enthält Tools zum Untersuchen und Beheben von Problemen mit Ihrer Instanz.

Verfügbare Tools

Tool	Beschreibung
CAPI zu Mustern	Migriert Ihren Cloud-Discovery Von Cloud-API-REST-Aufrufe (CAPI) zu Mustern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Tools (Fortsetzung)

Tool	Beschreibung
Migration von Probes zu Muster	Migriert ältere Probes zu neuen, flexiblen und effizienten Mustern.
Protokolle abrufen	Ruft Diagnoseprotokolle ab, um die Identifizierung zu erleichtern ITOM-Transparenz Und Discovery Probleme.
Erkennen Sie häufig erkannte CIs	Zeigt an, welche CIs häufiger erkannt werden als andere.
Muster für Anpassungsprüfung	Bestimmt, ob eine Anpassung ein Muster brechen könnte.
IRE-Nutzlast-Explorer	Identifiziert die zugrunde liegende Schlüsselkomponente bei Identifikation und Abgleich (IRE) für verschiedene Datenquellen.
Discovery-Anpassungsbericht	Erkennt Probe, Sensor, Klassifizierer und Mustercode, die anhand der Basissystemeinstellungen geändert wurden.
Dateien aus Store-Updates übersprungen	Untersucht alle Dateinamen aus Muster-Plugins, die bei Store-Updates übersprungen wurden.
Aufgabe zur Befehlsvalidierung	Führt Befehle für einen Bereich von IP-Adressen aus und validiert sie.
Fehlende IPs in Zeitplänen	Gibt an, welche Discovery In Zeitplänen fehlen IPs und fügt sie dem Zeitplan hinzu.
SNMP-OID-Daten fehlen	Überprüft auf fehlende SNMP-Geräte-OIDs aus den SNMP-Daten, die dazu führen, dass die Geräte falsch klassifiziert werden.
SaCmdManager	Sucht nach Informationen, die beim Erstellen möglicherweise benötigt werden Discovery Muster.

Formular „Vorschlag für Fingerabdruck der Anwendung“

Wenn Sie Vorschläge basierend auf Fingerabdrücken der Anwendung anzeigen, überprüfen Sie die Informationen im Formular „Vorschlag für Anwendungsfingerabdrücke“.

Daten des Formulars „Fingerabdruckvorschlag für Anwendung“

Feld	Beschreibung
Name des Discovery-Musters	Der Name des Musters.
Vorgeschlagene CMDB-CI-Klasse	Der Name der CMDB-CI-Klasse. Dieses Feld ist vorab ausgefüllt, Sie können es jedoch als Administrator bei Bedarf ändern.
Vorgeschlagene Klassifizierungsregel	Der Name des Prozesses, der mit der Aktion „Ignorieren“ von der Discovery ausgeschlossen wurde.
Genauigkeit in Prozent	Ein Prozentsatz, der auf einem Validierungsalgorithmus basiert und die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten des Formulars „Fingerabdruckvorschlag für Anwendung“ (Fortsetzung)

Feld	Beschreibung
	Qualität der Vorhersage überprüft. Wählen Sie Vorschläge mit höherer Genauigkeit aus. Sie können dieses Feld nicht ändern.
Vorgeschlagener Gruppenname	Der Name ITOM-Transparenz, der für den Vorschlag generiert wird. Dieses Feld ist bereits ausgefüllt, Sie können es jedoch bei Bedarf ändern.
Prozessanzahl	Die Anzahl der erkannten Prozesse, auf denen dieser Vorschlag basiert
Erweiterter Gruppenname	Die 10 wichtigsten Stichwörter, die weitere Informationen zum Prozess liefern. Predictive Intelligence extrahiert diese Stichwörter aus dem Prozess. Dieses Feld ist vorab ausgefüllt, und Sie können es nicht ändern.

Discovery-Administratorarbeitsbereich Datenvisualisierungen

Die **Übersicht** Die Registerkarte enthält Visualisierungen, die detaillierte Informationen zu enthalten Discovery Zeitplan. Diese Visualisierungen bieten einen umfassenden Überblick über die Leistung und den Status des Zeitplans und zeigen wichtige Metriken wie die Anzahl der abgeschlossenen Erkennungen, die Erfolgsquote und die aufgetretenen Fehler an.

Datenvisualisierungen

Berichtstitel	Typ	Beschreibung
Gesamtanzahl der Ausführungen	Indikator	Gesamtzahl der Male Discovery Zeitplan wurde in einem bestimmten Zeitraum ausgeführt.
Fehleraufgaben	Indikator	Anzahl der aktiven (in Bearbeitung befindlichen oder ausstehenden) Fehleraufgaben, die in einem bestimmten Zeitraum geöffnet wurden.
Zeitleiste der Ereignisse während der Zeitplanausführung	Zeitachse	Ereignisse, die während der Zeitplanausführungen aufgetreten sind.
CIs insgesamt	Indikator	Anzahl der bei der letzten Ausführung erkannten CIs.
Erkannte Anzahl von CIs	Liniendiagramm	Trends der erkannten CI-Attribute dafür Discovery Planen Sie für die im Ausführungsverlauf aufgeführten Status. Der Trend des Anomalieschwellenwerts spiegelt die schwerste Anomalie für diesen Zeitplan wider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen (Fortsetzung)

Berichtstitel	Typ	Beschreibung
		Wichtig: Der Anomalieschwellenwert wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.
Fehler	Indikator	Gesamtzahl der bei der letzten Ausführung erkannten Fehler.
Fehleranzahl	Liniendiagramm	Fehlertrends hierfür Discovery Planen Sie für die im Ausführungsverlauf aufgeführten Status. Der Trend des Anomalieschwellenwerts spiegelt die schwerste Anomalie für diesen Zeitplan wider. **Wichtig:** Der Anomalieschwellenwert wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.
Dauer in Min.	Indikator	Dauer in Minuten, die zuletzt benötigt wurde Discovery Zur Ausführung.
Discovery-Laufzeit	Liniendiagramm	Laufzeittrends dafür Discovery Planen Sie für die im Ausführungsverlauf aufgeführten Status. Der Trend des Anomalieschwellenwerts spiegelt die schwerste Anomalie für diesen Zeitplan wider. **Wichtig:** Der Anomalieschwellenwert wird nur angezeigt, wenn die Anomalieerkennung aktiviert ist. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich-Einstellungen.

Referenz des Formulars für Warteschlangenregistrierung

Im Formular „Warteschlangenregistrierung“ werden die Felder angezeigt, die beim Erstellen oder Ändern einer Warteschlange verfügbar sind.

Formular „Warteschlangenregistrierung“

Feld	Beschreibung
Warteschlange	Name der Warteschlange.
Anwendung	Umfang der Anwendung.
Automatische Aufgabenplanung	Option zum Aktivieren der automatischen Auftragsplanung. Wenn diese Option ausgewählt ist, wechselt die Warteschlange zur automatischen Auftragsplanung, und das System verarbeitet alle Auftragskonfigurationen.
Reihenfolge der Ereignisverarbeitung	Methode zum Verarbeiten von Ereignissen. Verfügbare Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Warteschlangenregistrierung“ (Fortsetzung)

Feld	Beschreibung
	• Parallel: Verarbeiten Sie mehrere Ereignisse gleichzeitig . • Sequenziell: Verarbeiten Sie jeweils nur ein Ereignis. Die Ereignisse sind voneinander abhängig und können erst verarbeitet werden, nachdem das vorherige Ereignis abgeschlossen ist. **Hinweis:** Nachdem Sie die Verarbeitungsreihenfolge konfiguriert und die Warteschlange übermittelt haben, kann sie nicht bearbeitet werden. Stattdessen müssen Sie die Warteschlange löschen und eine weitere Warteschlange erstellen.
Aufgabenkonfigurationstyp	Typ der Auftragskonfiguration. Verfügbare Optionen: • Konstante Anzahl: Erstellt die erforderliche Anzahl von Aufträgen. • Mit Knoten skalieren: Erstellt mehrere Aufträge basierend auf der Anzahl der Knoten. Wählen Sie diese Option aus, wenn Sie die Anzahl der verfügbaren Knoten nicht kennen. **Hinweis:** Dieses Feld wird automatisch auf eine konstante Zahl festgelegt, wenn das Feld Ereignisverarbeitungsreihenfolge auf sequenziell festgelegt ist.
Skalierungsfaktor	Gesamtanzahl der Aufträge, die basierend auf dem Wert von berechnet wird **Auftragskonfigurationstyp** Feld.
Abfrageintervall	Wie häufig Aufträge Ereignisse in dieser Warteschlange abfragen und verarbeiten sollen.
Beschreibung	Beschreibung der Warteschlange.

Schnellstarttest für IP-Discovery

Schnellstarttest für IP-Discovery validiert Konfigurationselemente (CI) und ihre Beziehungen.

IP-Discovery-Schnellstarttest

Test	Beschreibung
Testen Sie IPDiscovery	IP-Discovery wird für eine IP-Eingabe vom Anwender ausgeführt. Nach der Discovery werden das CI und die Beziehungen in den Tabellen „cmdb_ci“ und „rel_ci“ erstellt. Dieser Test validiert die erstellten CIs und Beziehungen sowie Ausgabe-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Discovery-Schnellstarttest (Fortsetzung)

Test	Beschreibung
	und Discovery-Fehler während der Discovery-Ausführung.

Weitere Informationen zur IP-Discovery finden Sie unter Horizontale Erkennung planen.

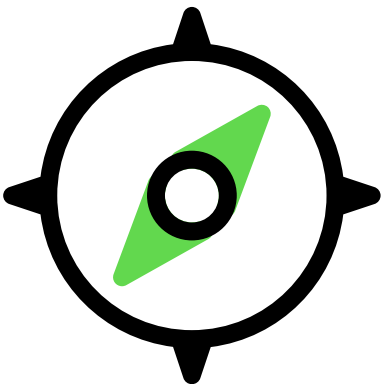
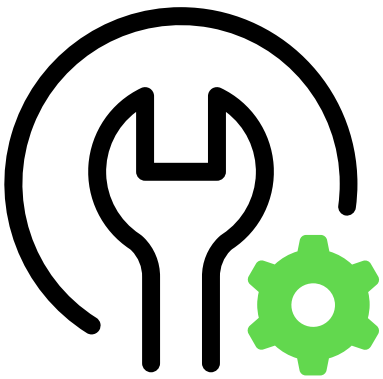
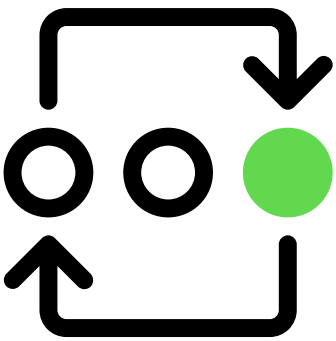
Zugehörige Informationen

Schnellstarttests

Firewall-Audits und Reporting

Verwenden Sie Firewall-Audits und Reporting Anwendung zum Erkunden und Erstellen eines Bestands Ihrer Firewall-Sicherheitsrichtlinien, Geräte, Gerätegruppen und Managerinformationen. Darüber hinaus können Sie Anforderungen für neue Firewall-Regeln über initiieren Servicekatalog Anwendung und Durchführung von Audits von Firewall-Sicherheitsrichtlinien innerhalb der angegebenen Zeitrahmen.

Erste Schritte

Firewall-Audits und Reporting erkunden	Firewall-Audits und Reporting verwalten	Firewall-Audits und Reporting – Referenz
		
Nutzen Firewall-Audits und Reporting Dient zum Erstellen von Bestand	Erfahren Sie, wie Sie den Firewall-Bestand einrichten	Machen Sie sich mit Dashboards und der Berichtskalibrierung vertraut

Problembehandlung und Hilfe

- Was ist ein Firewall-Audit?
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Firewall-Audits und Reporting erkunden

Mit Firewall-Audits und Reporting, Sie haben die Möglichkeit, Ihre Firewall-Sicherheitsrichtlinien, Geräte, Gerätegruppen und Managerinformationen zu erkunden und zu inventarisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darüber hinaus können Sie sie verwenden, um Anforderungen für neue Firewall-Regeln und Audit-Sicherheitsrichtlinien innerhalb eines angegebenen Zeitrahmens zu übermitteln.

Firewall-Audits und Reporting – Übersicht

Ein Firewall-Gerät fungiert als Netzwerksicherheitssystem, das den Datenverkehr basierend auf bestimmten Richtlinien überwacht und steuert. Es schafft eine Schutzbarriere zwischen vertrauenswürdigen internen und nicht vertrauenswürdigen externen Netzwerken und umfasst mehrere Sicherheitsrichtlinien zum Schutz vor Bedrohungen. Laufende Wartung und Audits sind wichtig, wenn sich Sicherheitsrichtlinien entwickeln und potenzielle Schlupflöcher verhindern. Der Firewall-Audit-Prozess optimiert die Regelnachverfolgung und -Aktualisierung und stellt die Ausrichtung an den Sicherheitsrichtlinien des Unternehmens sicher. Firewall-Lieferanten, einschließlich Panorama, bieten zentrale Manager für eine effiziente Kontrolle über Geräte und Richtlinien.

Firewall-Audits und Reporting – Workflow

Die Anwendung Firewall-Audits und Reporting ermöglicht dem ServiceNow Discovery-Prozess die Erkennung von Firewalls (derzeit Palo Alto Networks-Firewalls), CMDB-CIs für die Firewall-Geräte, Firewall-Managern, Firewall-Gerätegruppen und Firewall-Richtlinien mithilfe von serverlosen Mustern. Auditaufgaben für Firewall-Richtlinien werden von Firewall-Managern oder -Geräten generiert. Über Servicekatalog können Sie zudem neue Firewall-Sicherheitsrichtlinien anfordern und ältere Firewall-Regelanforderungen, Auditanforderungen und Auditaufgaben archivieren, um die Systemperformance zu verbessern. Weitere Informationen finden Sie unter Transparenz des Firewall-Bestands. Informationen zum Anzeigen verschiedener Berichte zur Nachverfolgung erkannter Richtlinien und Audit-Aufgaben finden Sie unter Firewall-Administratorarbeitsbereich-Dashboard.

Firewall-Audits und Reporting – Vorteile

Vorteil	Funktion	Anwender
Aktuelle Bestandsaufnahme von Firewall-Sicherheitsrichtlinien, Geräten, Gerätegruppen und Managerinformationen, indem Daten dauerhaft in gespeichert werden CMDB Durch regelmäßige Abfragen an einen Firewall-Manager.	Transparenz des Firewall-Bestands	Firewall-Administrator [sn_Disco_Firewall.Firewall_admin]
Möglichkeit der Anforderung einer neuen Firewall-Regel mithilfe von Servicekatalog	Firewall-Regelanforderungen	Firewall-anfordernde Person [sn_Disco_Firewall.Firewall_anfordernde Person]
Möglichkeit der Überwachung von Firewall-Sicherheitsrichtlinien für einen bestimmten Zeitraum	Firewall-Administratorarbeitsbereich-Dashboard	Firewall-Anwender [sn_Disco_Firewall.Firewall_user]

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Firewall-Audits und Reporting Rollen und Verantwortlichkeiten

Bestimmte Anwender und Rollen zur Optimierung der Überwachung und Nachverfolgung von Anforderungen für neue Firewall-Regeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Konfigurationseinstellungen werden abhängig von den zugewiesenen Rollen aktiviert oder deaktiviert.

Rolle	Verantwortlichkeiten
Firewall-Administrator [sn_Disco_Firewall.Firewall_admin]	Verantwortlich für die Bearbeitung von Konfigurationselement-(CI-)Attributen, die nicht von Discovery ausgefüllt werden, einschließlich „assigned_to“ und anderer. Firewall-Administratoren verfügen über die Fähigkeit, die Liste der Firewall-Manager mit spezifischen Details für jeden Manager anzuzeigen. Darüber hinaus sind sie berechtigt, das Dashboard anzuzeigen und zu bearbeiten, Audits über die Detailseite des Firewall-Managers zu initiieren, Richtlinien zu erstellen, zu ändern und anzuzeigen, Audit-Aufgaben zu bearbeiten, und fordern Sie Richtlinienänderungen an. **Hinweis:** Die Rolle „Firewall-Administrator“ enthält die Rolle „Firewall-Anwender“. Diese Rolle wird nicht automatisch mit der Rolle „Discovery_admin“ gewährt und muss dem Anwender explizit zugewiesen werden.
Firewall-Anwender [sn_Disco_Firewall.Firewall_user]	Verantwortlich für die Anzeige von Firewall-Dashboards und -Richtlinien in schreibgeschützter Kapazität. **Hinweis:** Diese Rolle enthält die Rolle „Firewall-anfordernde Person“.
Firewall-Anfordernde Person [sn_Disco_Firewall.Firewall_Anforderer]	Verantwortlich für die Anforderung neuer Firewall-Regeln über die Servicekatalog.

Firewall-Audits und Reporting konfigurieren

Richten Sie den Prozess ein, um Einblicke in die Erkennung und Zusammenstellung eines Bestands von Firewall-Sicherheitsrichtlinien, Geräten, Gerätegruppen und Managerinformationen zu erhalten.

Konfiguration – Übersicht

Vor der Verwendung Firewall-Audits und Reporting, Es ist wichtig, die erforderlichen Plugins einzurichten, die Aktivierung sicherzustellen, Ihre Instanz auf die neueste Version zu aktualisieren und herunterzuladen Firewall-Audits und Reporting Anwendung von ServiceNow Store. Weitere Informationen finden Sie unter Erste Schritte mit Firewall-Audits und Reporting.

Nachdem die Voraussetzungen erfüllt sind, können Sie mit den folgenden Aufgaben fortfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Audits und Reporting-Aufgaben

Aufgabe	Beschreibung
Firewall-Richtlinien erkennen	Erkennen Sie Firewall-Richtlinien, die das Aufdecken von Firewall-Geräten, Richtlinien und Besitzergruppen umfassen, um eine zentrale Ansicht der Stellfläche sicherzustellen.
Firewall-Audits und Reporting anpassen	Anpassen Firewall-Audits und Reporting Durch Ändern Discovery Eigenschaften zur Anpassung bestimmter Aspekte.
Firewall-Regelaudits, Regelanforderungen und Auditaufgaben archivieren	Verbessern Sie die Systemleistung, indem Sie Firewall-Regelanforderungen, Audit-Anforderungen und Audit-Aufgaben archivieren, die älter als ein angegebener Zeitraum sind.
Auditanforderung initiieren	Initiieren Sie Audits für einen angegebenen Firewall-Manager oder -Gerät, um die Einhaltung der Sicherheitsrichtlinien der Organisation sicherzustellen.

Erste Schritte mit Firewall-Audits und Reporting

Vor dem Eintauchen in Firewall-Audits und Reporting-Funktionalität erfüllen Sie die erforderlichen Anforderungen, indem Sie das -Plugin installieren und aktivieren, Ihre -Instanz aktualisieren und die -Anwendung von beziehen ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Prozedur

1. Stellen Sie sicher, dass die folgenden Plugins installiert und aktiviert sind.
   - ITOM-Transparenz [com.snc.itom.vis.license]-Plugin
   - Plugin Discovery [com.snc.discovery]
   - Configuration Management for Scoped Apps (CMDB) Plugin [com.snc.cmdb.scope]
2. Bestätigen Sie, dass Ihr System auf aktualisiert wurde Zurich Oder eine neuere Version.
   Während des Upgradeprozesses wird Firewall-Audits und Reporting Das Plugin [com.sn_Disco_Firewall] wird automatisch installiert, wenn der ITOM-Transparenz[com.snc.itom.vis.license] und Discovery[Com.snc.Discovery] Plugins sind bereits installiert.
3. Laden Sie herunter Firewall-Audits und Reporting Anwendung von ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transparenz des Firewall-Bestands

Mit der Anwendung Firewall-Audits und Reporting können Sie Ihre Firewall-Sicherheitsrichtlinien, -Geräte, -Gerätegruppen und -Managerinformationen erkennen und inventarisieren.

ServiceNow Platform hilft Unternehmen dabei, mithilfe der zentralisierten Configuration Management Database (CMDB) den Überblick über ihre IT-Ressourcen zu behalten und Workflows für Anforderungs- und Change-Management-Prozesse zu automatisieren. Die Anwendung Firewall-Audits und Reporting ermöglicht Sicherheitsteams, alle Firewalls zusammen mit den zugehörigen Richtlinien, Firmware-Versionen und anderen Hardwareattributen zu erkennen. Das Serviceportal von ITSM hilft Kunden, Workflows zu digitalisieren, wenn sie neue Firewall-Regeln anfordern. In Kombination mit Incident Management- und Change-Management-Workflows von ITSM ermöglicht diese Lösung Transparenz im Erfüllungsprozess. Um Teams die Arbeit zu erleichtern, sind der Systembenutzer und die Systemgruppen in der ServiceNow Platform für Richtlinien verantwortlich. Ein zentrales Dashboard bietet den Überblick über die Firewall-Umgebung und umfassende Transparenz über den Zustrom von Anforderungsdatensätzen, die in der Erfüllungswarteschlange des Firewall-Administrators landen.

Derzeit arbeitet ServiceNow mit Palo Alto Networks Panorama. In zukünftigen Versionen werden weitere Firewall-Anbieter hinzugefügt. Die Integration verwendet XML-APIs und SNMP, um die Verbindung mit herzustellen Firewall-Audits und Reporting Anwendung für Firewall-Bestands- und Firewall-Richtlinien.

Firewall-Richtlinien erkennen

Als Mitglied eines Sicherheitsteams können Sie Firewall-Geräte, -Richtlinien und -Besitzergruppen erkennen und erhalten so einen zentralen Überblick über den Footprint. Diese Daten werden in der ServiceNow CMDB aktualisiert. Richten Sie einen Zeitplan ein, um Ihre Firewall-Richtlinien zu erkennen, damit Sie die wertvollen Informationen Ihres Unternehmens im Auge behalten können.

Vorbereitungen

Für die Panorama-Integration benötigen Sie eine Superuser-Rolle (schreibgeschützt).

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Administratoren, die für verantwortlich sind Discovery Kann einen wiederkehrenden Zeitplan für einrichten Palo Alto Networks Firewall-Richtlinien-Discovery. Dieser Zeitplan verwendet das serverlose Muster, das eine Verbindung mit dem Palo Alto Firewall Manager herstellt, um Informationen für die folgenden vier Configuration Items (CIs) in zu erkennen und zu aktualisieren CMDB.

- Panorama-Firewall-Manager [cmdb_ci_Firewall_Manager_Panorama]
- Palo Alto-Firewall-Geräte [cmdb_ci_Firewall_device_palo_alto]
- Panorama-Firewall-Gerätegruppe [cmdb_ci_Firewall_device_Group_Panorama]
- Panorama-Firewall-Sicherheitsrichtlinien [cmdb_ci_Firewall_sec_Policy_Panorama]

Prozedur

1. Erstellen Sie einen neuen Anmeldeinformationsalias vom Typ **API-Schlüssel-Anmeldeinformationen** Und **Übermitteln** Die Anmeldeinformationen.
2. Geben Sie den API-Schlüssel für Panorama ein.
   Weitere Informationen finden Sie unter Anmeldeinformationsaliasse für Discovery .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Zum Erstellen von Discovery Planen Sie, führen Sie die folgenden Schritte aus.
   a. Wählen Sie Aus **Erkennen: Serverlos** .
   b. Wählen Sie die entsprechende aus **MID-Server** .
   c. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
   Weitere Informationen zu finden Discovery Zeitplan, siehe Planen Sie eine horizontale Discovery .
4. Wählen Sie auf der Registerkarte unten im Bildschirm das Muster serverlose Ausführung aus, und wählen Sie dann aus **Neu** .
5. Führen Sie im Muster „serverlose Ausführung“ die folgenden Schritte aus.
   a. Geben Sie einen Namen ein.
   b. Wählen Sie Aus **PaloAlto: Firewall-Manager** .
   c. Wählen Sie Aus **Untergeordnete Muster Ausführen** .
   d. Wählen Sie **Absenden**.
6. Navigieren Sie zu **Startprogramm-Parameter Für Discovery-Muster** Und legen Sie die folgenden drei Parameter fest.
   - Anmeldeinformationsalias: Geben Sie den neuen Aliasnamen für Anmeldeinformationen an, der in Schritt 1 erstellt wurde.
   - TrustInsecureHosts: Auf festlegen **Wahr** Um die Überprüfung des Hostnamens zu deaktivieren und zu aktivieren, dass selbstsignierte Zertifikate als vertrauenswürdig akzeptiert werden.
   - url: Geben Sie die Basis-URL des Panorama-Geräts ein.

     Beispiel: https://<PANORAMA_HOST>/api
7. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

Firewall-Audits und Reporting anpassen

Ändern Sie die Discovery-Eigenschaften, um einige Aspekte von Firewall-Audits und Reporting anzupassen.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Discovery-Eigenschaften Verwalten Sie verschiedene Aspekte des horizontalen Discovery-Prozesses. In diesem Verfahren wird erläutert, wie Sie standardmäßige Richtlinienbesitzergruppen- und Genehmigungsgruppennamen für die Genehmigung von Firewall-Regelaufgaben zuweisen.

Prozedur
1. Zum Bearbeiten Discovery-Eigenschaften , Navigieren Sie zu **Alle** > **Discovery-Definition** > **Eigenschaften**an.
   Weitere Informationen zu Eigenschaften finden Sie unter Discovery-Eigenschaften .
   - sn_disco_firewall.default.rule.task.policy.owner.group: Name Ihrer standardmäßigen Aufgabenbesitzergruppe
   - sn_disco_firewall.default.rule.task.approval.group: Name Ihrer standardmäßigen Genehmigungsgruppe
2. Bearbeiten Sie die Eigenschaften nach Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_disco_firewall.default.rule.task.policy.owner.group: Name Ihrer standardmäßigen Aufgabenbesitzergruppe
- sn_disco_firewall.default.rule.task.approval.group: Name Ihrer standardmäßigen Genehmigungsgruppe

Diese Funktion spart Zeit, indem Sie Ihre Standardbesitzergruppe und Ihre Genehmigungsgruppe automatisch in Anforderungen ausfüllen.

Firewall-Regelaudits, Regelanforderungen und Auditaufgaben archivieren

Archivieren Sie Firewall-Regelanforderungen, Auditanforderungen und Auditaufgaben, die älter als ein bestimmter Zeitraum sind, um die Systemperformance zu verbessern. Sie können sie zu einem späteren Zeitpunkt vollständig aus der Archivtabelle löschen, um die Größe dieser Tabelle zu verringern.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Datenarchiver“ [com.glide.auxdb] aktiviert und aktiviert ist.

Erforderliche Rolle: firewall_admin

Prozedur

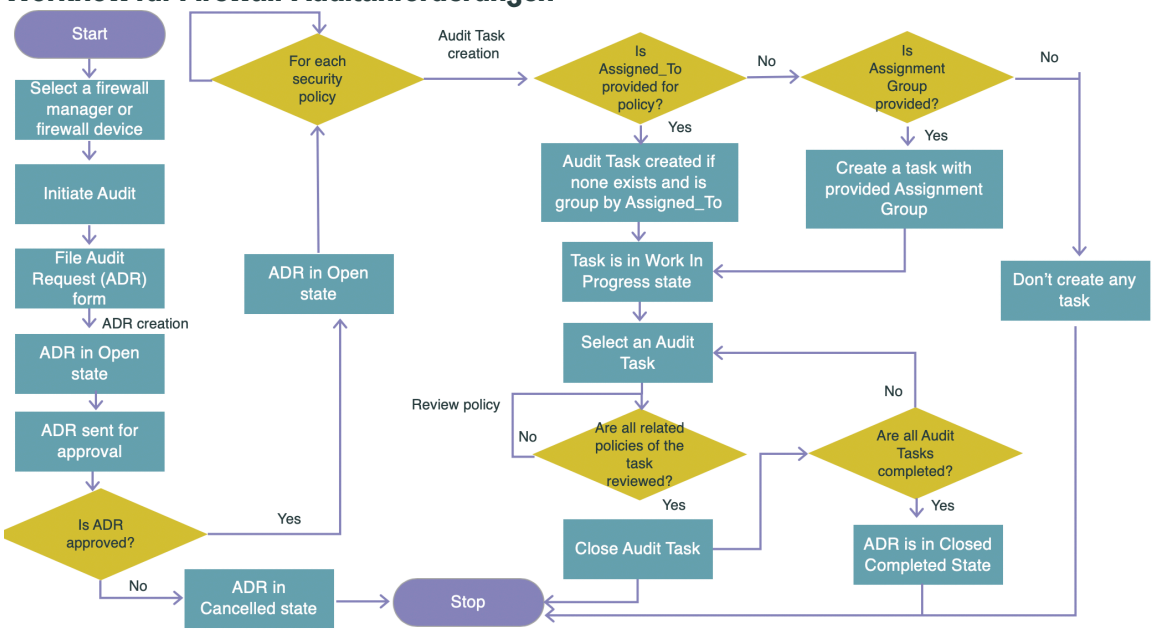
1. Aktivieren Sie mindestens eine **Firewall-Archivierungsregel**.
   Die folgenden Archivierungsregeln gehören zum Lieferumfang der Anwendung Firewall-Audits und Reporting, sind jedoch standardmäßig inaktiv. Um Regeln zu verwenden, müssen Sie sie aktivieren.
   - Archive Firewall Audit Request
   - Archival Firewall Audit Request Security Policy M2M
   - Archive Firewall Audit Task
   - Archival Firewall Audit Task Security Policy M2M
   - Archive Firewall Rule Task
   - Archival Firewall Rule Task Security Policy M2M
2. Navigieren zu **Archivregeln** > **Wählen Sie eine Firewall-Archivierungsregel aus**an.
3. Aktivieren Sie die Checkbox **Aktiv**.
   Das Plugin „Data Archiver“ [com.glide.auxdb] verschiebt täglich nicht mehr benötigte Daten aus primären Tabellen in einen Satz von Archivtabellen. Es sucht und archiviert Anforderungen und Aufgaben basierend auf der aktivierten und ausgewählten Archivierungsregel. Die Regel archiviert Daten aus der Primärtabelle, wenn die folgenden beiden Bedingungen erfüllt sind:
   - Status „Geschlossen - vollständig“
   - Aktualisiert vor mehr als 12 Monaten

Firewall-Audits

Firewall-Audits und Reporting Bietet ein flexibles Audit-Framework, um Ihren Besitz für die Firewall-Richtlinie und die Notwendigkeit einer Firewall-Richtlinie nachzuverfolgen. Sie können ein zufälliges Audit auslösen, um Ihre Sicherheitshygiene in Bezug auf die Firewall-Richtlinie und den Besitz zu messen und regelmäßig proaktive Audits durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für Firewall-Auditanforderungen



Auditanforderung initiieren

Initiieren Sie Audits für einen angegebenen Firewall-Manager oder -Gerät, um eine ordnungsgemäße Konfiguration gemäß den Sicherheitsrichtlinien Ihrer Organisation sicherzustellen.

Vorbereitungen

Erforderliche Rolle: firewall_admin

Prozedur

1. Um alle erkannten Firewall-Manager in Ihrem Netzwerk aufzulisten, navigieren Sie zu **Alle** > **Firewall-Audits und Reporting** > **Datensätze** > **Geräte oder Manager**an.
2. Wählen Sie in der Liste den CI-Datensatz eines Firewall-Managers oder einen Gerätedatensatz aus.
3. Wählen Sie Aus **Audit-Anforderung Initiieren** .
4. Füllen Sie die Pflichtfelder im Formular aus.
5. Wählen Sie **Absenden**.

Nächste Maßnahme

Das Verfahren initiiert ein Audit für den Firewall-Manager, validiert es und übermittelt die Audit-Aufgabe. Firewall-Audit-Aufgaben werden basierend auf dem zugewiesenen Anwender für die Firewall-Sicherheitsrichtlinie generiert. Wenn für die Richtlinie ein bestimmter Anwender fehlt, wird für diese Sicherheitsrichtlinie keine Audit-Aufgabe erstellt und in platziert *`Excluded Policy List`*Für Audit-Anforderungen.

Daraufhin wird ein Audit für den Firewall-Manager angefordert, validiert und übermittelt. Firewall-Auditaufgaben werden auf Grundlage eines zugewiesenen Benutzers für die Firewall-Sicherheitsrichtlinie erstellt. Wenn die Richtlinie keinem Benutzer zugewiesen ist, wird keine Auditaufgabe für diese Sicherheitsrichtlinie erstellt, und sie wird der *`Excluded Policy List`* der Auditanforderungen hinzugefügt.

- Wenn *`Assigned To`*Wird angegeben, wird die Audit-Aufgabe vom zugewiesenen Anwender erstellt und gruppiert.
- Wenn *`Assigned To`*lst nicht angegeben, und *`sn_disco_firewall.default.rule.task.policy.owner.group`*Discovery-Eigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ist nicht festgelegt, die Richtlinie wird hinzugefügt *Excluded Policies*Liste, und es wird keine Audit-Aufgabe generiert.

- Wenn *Assigned To*lst nicht angegeben, aber *sn_disco_firewall.default.rule.task.policy.owner.group*Die Discovery-Eigenschaft ist konfiguriert, die Audit-Aufgabe wird erstellt und nach gruppiert **Zuweisungsgruppe** .

Um zu überprüfen, ob die Audit-Aufgabe angefordert wurde, navigieren Sie zu **Audits** > **Auditanforderung**an. Ihre Aufgabe sollte in der Liste angezeigt werden. Die Erstellung von Auditaufgaben findet im Hintergrund mit Subflows statt. Je nach Anzahl der Richtlinien müssen Sie möglicherweise warten, bis Auditaufgaben erstellt werden.

Die *Assigned To*-Person prüft alle in der zugehörigen Liste enthaltenen Richtlinien. Sie wählt die Aktion für jede Richtlinie aus und markiert die Aufgabe als *Close Complete*.

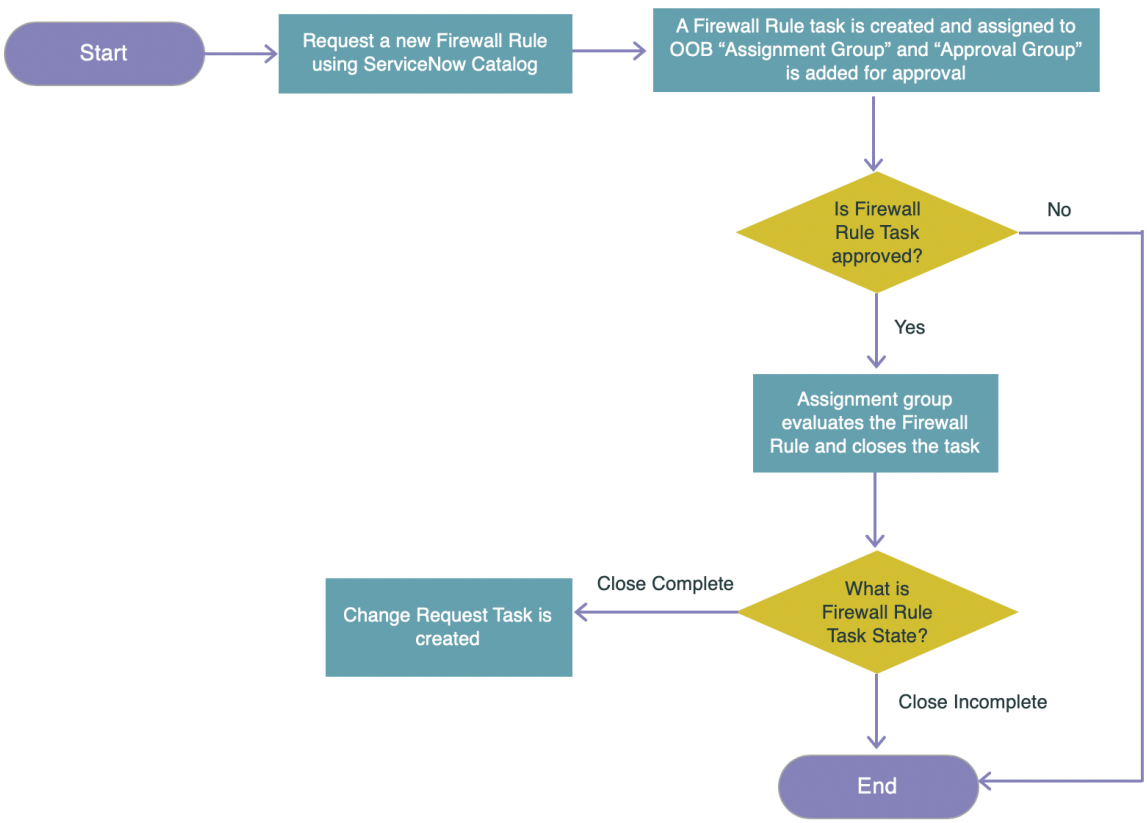
Firewall-Audits und Reporting verwenden

Firewall-Audits und Reporting Ist eine leistungsstarke Anwendung zum anfordern neuer Firewall-Regeln, die die Verwaltung von IP-Adressen optimieren.

Firewall-Regelanforderungen

Verwenden Servicekatalog Zum anfordern neuer Firewall-Richtlinien und -Regeln.

Workflow für Firewall-Regelanforderung



Neue Firewall-Regel anfordern

Fordern Sie mit eine neue Firewall-Regel an Servicekatalog Zur Verwaltung verschiedener IP-Adressen, zur Verbesserung der Netzwerksicherheit und zur Anpassung an sich ändernde Geschäftsanforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass der Katalog für Firewall-Audits und Berichterstellung aktiviert ist.

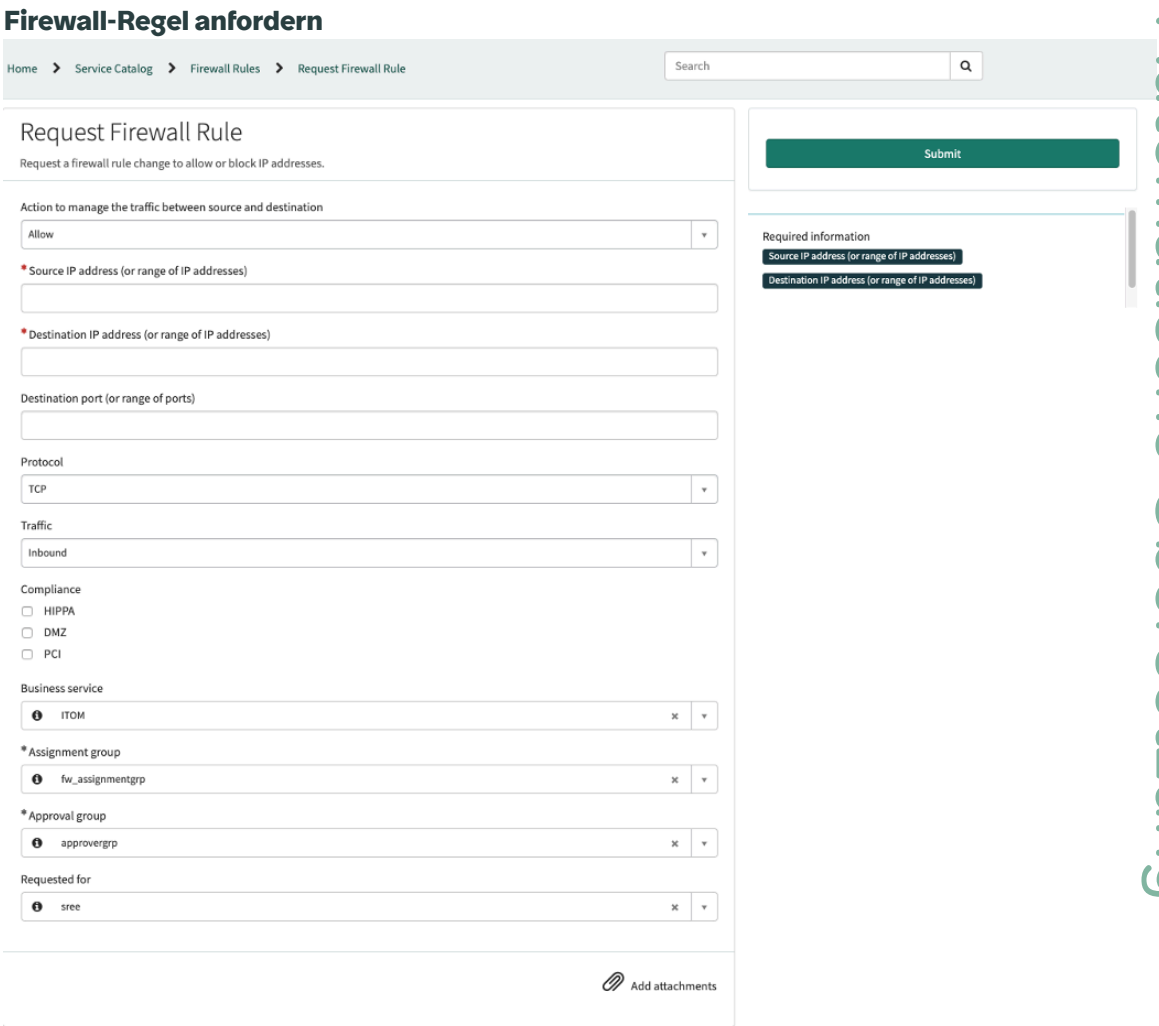
Erforderliche Rolle: firewall_admin

Warum und wann dieser Vorgang ausgeführt wird

Administratoren initiieren Aufgaben, die automatisch zur Bewertung und Genehmigung an das Risikoteam weitergeleitet werden. Nach der Genehmigung implementieren Firewall-Administratoren Changes reibungslos, alle durch automatisierte Workflows orchestriert.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Firewall-Regeln**an.
2. Wählen Sie Aus **Firewall-Regel Anfordern** .



3. Geben Sie die entsprechenden Informationen für die folgenden Pflichtfelder ein.

- Source IP address (Quell-IP-Adresse)
- Destination IP address (Ziel-IP-Adresse)
- Zuweisungsgruppe

  Muss haben *sn_disco_firewall.firewall_user*Rolle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Genehmigungsgruppe

  Muss haben *approver_user*Rolle.

4. Geben Sie die erforderlichen Details ein, oder wählen Sie sie aus.
5. Wählen Sie **Absenden**.
   Die Firewall-Regelaufgabe wird erstellt.

Nächste Maßnahme

Navigieren Sie zu , um die neue Regelaufgabe zu überprüfen **Regelanforderungen** > **Regelanforderungsaufgabe**an. Ihre Anforderung muss in der Liste sichtbar sein.

Firewall-Anforderungen genehmigen

Die Genehmigung von Firewall-Anforderungen stellt kontrollierten Zugriff und Compliance sicher, wobei Mitglieder der Genehmigergruppe befugt sind, Firewall-Audits und neue Firewall-Anforderungen zu überprüfen und zu genehmigen.

Vorbereitungen

Erforderliche Rolle: Mitglieder der angegebenen Genehmigergruppe **Approval_Group** Die in der Regelaufgabe angegeben ist. Bei Bedarf kann der Administratoranwender die Liste der Genehmiger in der Regelanforderungsaufgabe bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Meine Genehmigungen**an.
2. Wählen Sie das grüne Häkchen aus, um zu genehmigen.

Ergebnis

- Die Zuweisungsgruppe bearbeitet dann die Anforderung und markiert sie als *Close Complete*.
- Sobald die assignment_group die Anforderung als *Close Complete* markiert hat, wird ein Subflow im Hintergrund ausgeführt, um eine Change-Anforderung zu erstellen, falls das Plugin „Change Request“ aktiviert ist.

  Hinweis: Die Change-Anforderung wird nur erstellt, wenn die Regelaufgabe *Approved* ist und den Status *Close Complete* aufweist.

Die Sicherheitsrichtlinie M2M für die Firewall-Regelaufgabe entspricht der zugehörigen Liste *Security policies*In *Rule task*. Firewall-Administratoren können die Felder *description* und *tag* in einer Sicherheitsrichtlinie auf einem Panorama-Gerät hinzufügen. Sie können beim Erstellen oder Ändern von Sicherheitsrichtlinien in Panorama auch Firewall-Regelaufgabennummern und Change-Anforderungsnummern hinzufügen. Wenn die nächste Erkennung ausgeführt wird, füllt die M2M-Tabelle die Zuordnung zwischen:

- Firewall-Regelaufgabe und Firewall-Sicherheitsrichtlinie
- Firewall-Sicherheitsrichtlinie und Business Service, wenn der Business Service während der Firewall-Regelaufgabenanforderung bereitgestellt wird

Firewall-Audits und Reporting – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Firewall-Audits und Reporting Komponenten, einschließlich Dashboards und Berichtskalibrierung.

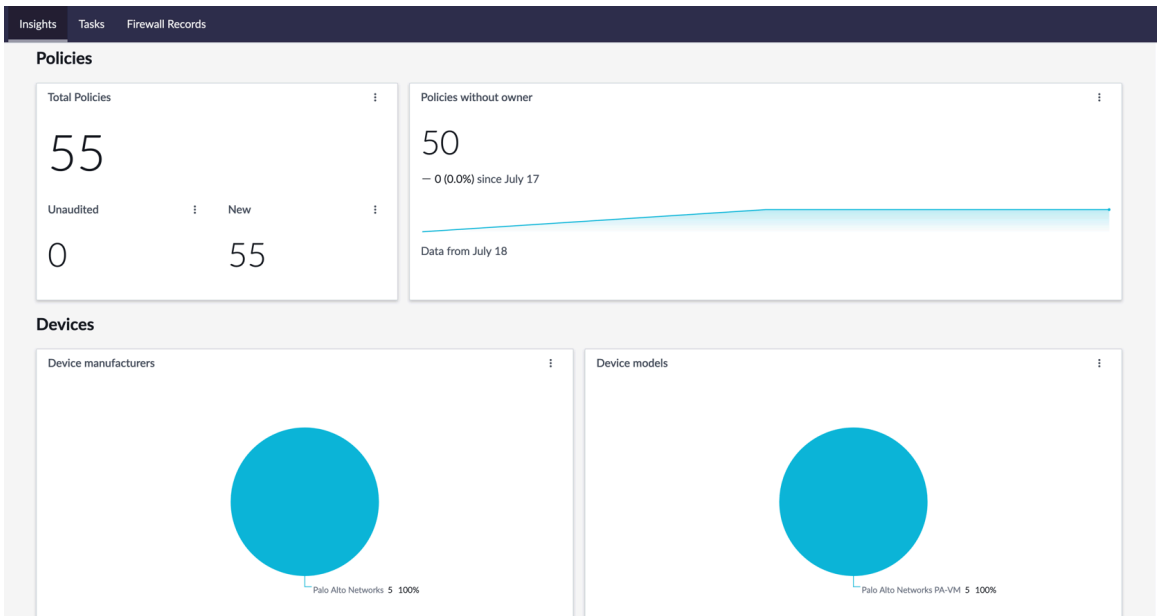
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Administratorarbeitsbereich-Dashboard

Das einheitliche Dashboard ermöglicht Sicherheits- und Risikoteams die Überwachung von Aufgaben, Change-Anforderungen und den gesamten Lebenszyklus des Firewall-Bestands mit täglichen oder manuellen Updates für genaue und aktuelle Informationen.

Registerkarte „Firewall Insights (Firewall-Erkenntnisse)“

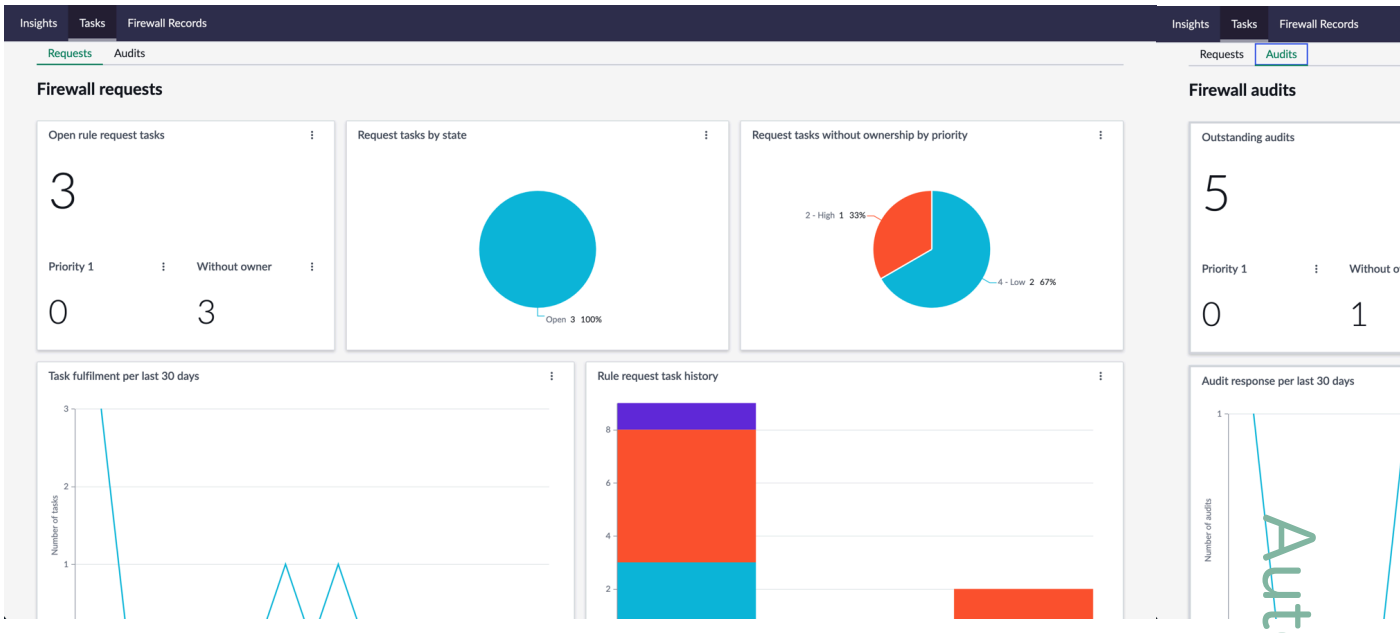
Die **Einblicke** Die Registerkarte bietet einen Snapshot von Firewall-Richtlinien und zugehörigen Geräten und zeigt Trends in Richtlinien ohne Besitzer im Laufe der Zeit. Verfolgen Sie neue und nicht auditierte Richtlinien, und zeigen Sie die Verteilung der Gerätehersteller und -Modelle im Netzwerk an.



Registerkarte „Requests and Audits (Anforderungen und Audits)“

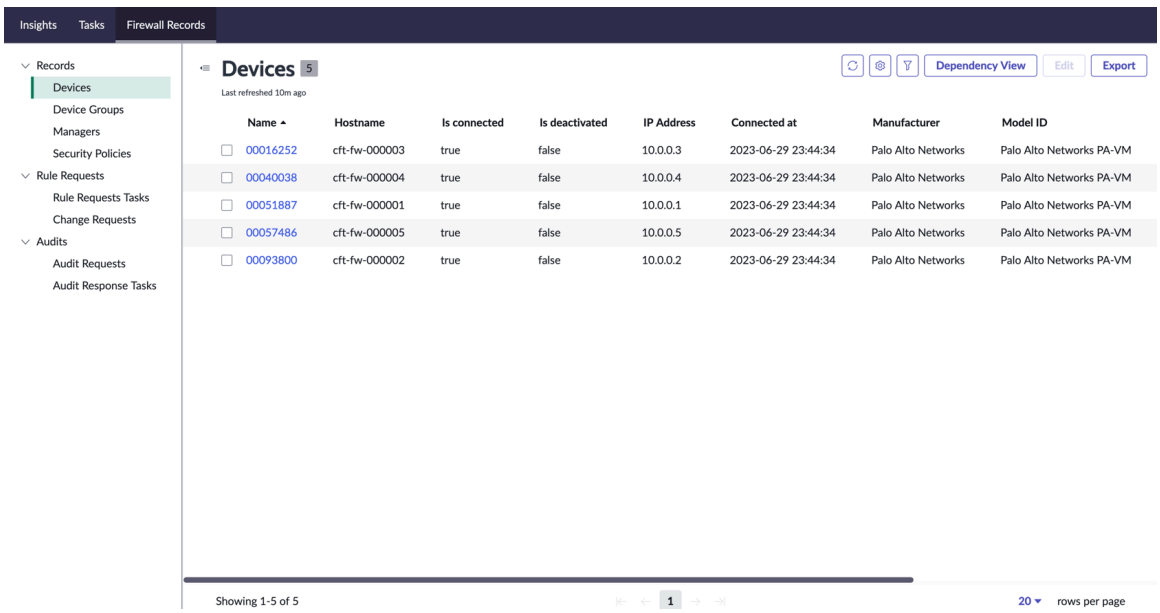
Innerhalb von **Aufgaben** Registerkarte erkunden Sie **Anforderungen** Und **Audits** Unterregisterkarten. Die **Anforderungen** Die Registerkarte bietet Aufgliederungen der Anforderungsaufgaben nach Status und Besitz sowie Erfüllungstrends im Zeitverlauf. Ebenso wird **Audits** Auf der Registerkarte werden ausstehende Audits nach Status und Besitz sowie Antworttrends im Zeitverlauf angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registerkarte „Firewall-Datensätze“

Die **Firewall-Datensätze** Die Registerkarte bietet konsolidierten Zugriff auf die Tabellen „Datensätze“, „Regelanforderungen“ und „Audits“. Anwender können einzelne oder Gruppen von Datensätzen filtern, bearbeiten und exportieren. Die **Geräte** Und **Sicherheitsrichtlinie** Unterregisterkarten enthalten eine Abhängigkeitsanzeige für ausgewählte Datensätze.



Endanwender und Rollen

Endanwender und Ziel	Erforderliche Rolle
Risikoteams	firewall_admin oder firewall_user
Sicherheit	firewall_admin oder firewall_user

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfall

Um das Dashboard manuell zu aktualisieren, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge** Und wählen Sie aus **Geplante Firewall-Aufgabe** . Öffnen Sie den Datensatz, und wählen Sie aus **Jetzt Ausführen** Um die Dashboard-Elemente mit den neuesten Informationen zu aktualisieren.

Kalibrierung von Firewall-Audits und Reporting

Erkunden Sie weitere Details zu Firewall-Audits und Reporting Kalibrierung durch Überprüfung des bereitgestellten Materials.

Firewall-Audits und Reporting pattern

Palo Alto Firewall Manager

Dieses serverlose Muster verwendet die Funktion „große Nutzlast“ zum Beibehalten von Sicherheitsrichtlinien. Discovery-Administratoren können mithilfe dieses Musters einen Zeitplan einrichten. Wenn **Untergeordnete Muster Ausführen** Ist aktiviert, werden die folgenden untergeordneten Muster automatisch in der angegebenen Reihenfolge ausgeführt:

- Palo Alto Firewall Manager
- Palo Alto Firewall Devices
- Palo Alto Firewall Device groups
- Palo Alto Panorama Security policies

Schnellstarttest für Firewall-Audits und Reporting

Schnellstarttest für Firewall-Audits und Reporting Dient zum Validieren von Konfigurationselementen (CI) und ihren Beziehungen.

Firewall-Audits und Reporting Schnellstart-Test

Test	Beschreibung
Firewall-Discovery	Firewall-Discovery wird auf einem Firewall-Endpunkt ausgeführt. Discovery bringt den Firewall-Manager, Richtlinien und Geräte und behält sie in den Tabellen „cmdb_ci“ bei. Dieser Test validiert die Firewall-Manager-, Richtlinien- und Gerätedaten in den Tabellen „cmdb_ci“ sowie Ausgabe- und Discovery-Fehler während der Discovery-Ausführung.

Weitere Informationen finden Sie unter Firewall-Audits und Reporting.

Zugehörige Informationen

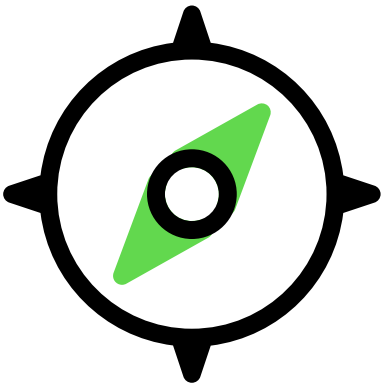
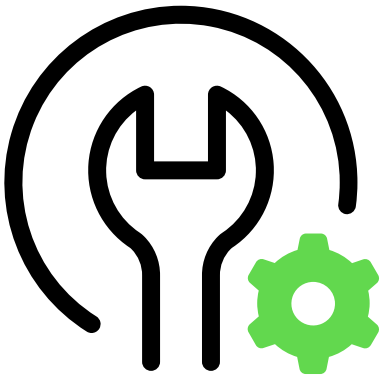
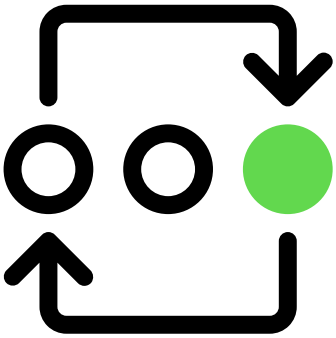
Schnellstarttests

Zertifikatsbestand-Management

Mit Zertifikatsbestand-Management, Können Sie alle TLS-Zertifikate erkennen, eine Bestandsaufnahme durchführen und proaktiv verwalten. Zertifikatsbestand-Management Unterstützt IPv6 und bietet eine umfassende Abdeckung für Ihre Zertifikatverwaltungsanforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Verwalten	Zertifikatsbestand-Management – Referenz
Zertifikatsbestand-Management	Zertifikatsbestand-Management	
		
Nutzen Zertifikatsbestand-Management Dient zum Erstellen und Verwalten von Zertifikaten	Erfahren Sie, wie Sie einrichten Zertifikatsbestand-Management	Machen Sie sich mit Dashboards, Tabellen, Mustern und Begriffen vertraut

Problembehandlung und Hilfe

- Was ist Zertifikatverwaltung?
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Zertifikatsbestand-Management erkunden

Zertifikatsbestand-Management Dient als zentralisierte und automatisierte Lösung zur Handhabung der Komplexität der Zertifikatverwaltung. Es verbessert die Sicherheit, stellt Compliance sicher und bietet einen optimierten Ansatz für die Verwaltung des Lebenszyklus digitaler Zertifikate in einer Organisation.

Zertifikatsbestand-Management – Übersicht

Zertifikatsbestand-Management Ist eine zentrale und automatisierte Lösung, die die Nachverfolgung und Verwaltung digitaler Zertifikate in einer IT-Infrastruktur optimiert. Durch Automatisierung der Discovery-, Bestands- und Überwachungsprozesse Zertifikatsbestand-Management Ermöglicht Organisationen die Verwaltung eines umfassenden Datensatzes von Zertifikaten, einschließlich wichtiger Details wie Ablaufdaten und Aussteller.

Das System erleichtert die Nachverfolgung in Echtzeit, automatisiert Routineaufgaben wie Verlängerungen und unterstützt die Anpassung an bestimmte organisatorische Anforderungen. Mit Integrationsfunktionen in vorhandene CI-basierte Discovery Zeitpläne und Support für IPv6, Zertifikatsbestand-Management Bietet Flexibilität und Effizienz bei der Verwaltung des gesamten Lebenszyklus von Zertifikaten. Die rollenbasierte Zugriffssteuerung sorgt für eine sichere und maßgeschneiderte Nutzung, während Warnungen und Benachrichtigungen Administratoren über kritische Ereignisse auf dem

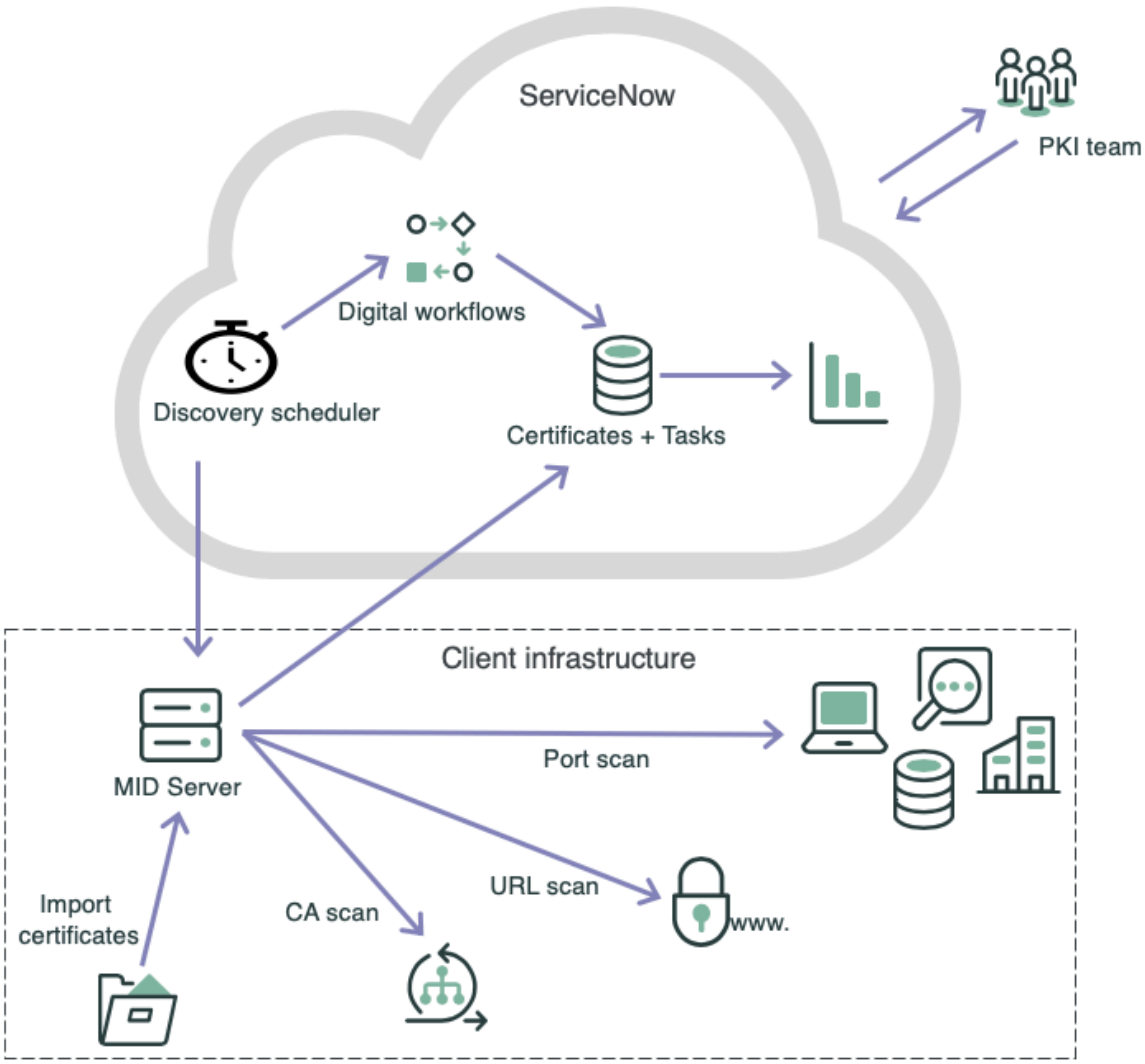
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laufenden halten und zu mehr Sicherheit, Compliance und betrieblicher Effizienz bei der Zertifikatverwaltung beitragen.

Zertifikatsbestand-Management – Workflow

Zertifikatsbestand-Management Optimiert den Prozess des Scans nach Zertifikaten, indem sie über Ihr festgelegtes Configuration Item (CI) automatisch an bestimmten Ports erkannt werden Discovery Zeitpläne. Darüber Hinaus Zertifikatsbestand-Management Ermöglicht Anwendern die Flexibilität, neue zu generieren Discovery Zeitpläne, die auf das Scannen einzelner URLs zugeschnitten sind. Dieser dynamische Ansatz stellt eine robuste und anpassungsfähige Methode für die Erkennung und Verwaltung von Zertifikaten sicher und trägt zu einer sicheren und gut organisierten IT-Infrastruktur bei.

Prozess-Flow-Diagramm



Um weitere Informationen dazu zu erhalten Zertifikatsbestand-Management Funktioniert, siehe Prozess-Flow in Zertifikatsbestand-Management.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management – Vorteile

Vorteil	Funktion	Anwender
Verwaltung von TLS-Zertifikaten durch Verwaltung eines zentralen Bestands, Priorisierung von Zertifikaten und Nutzung von Verlängerungs-Workflows, um kostspielige Ausfälle zu verhindern und eine sichere Umgebung sicherzustellen.	Zertifikatsbestand-Management konfigurieren	Zertifikatadministrator [sn_Disco_certmgmt.pki_admin]
Automatisierte Funktionen zur Optimierung der Nachverfolgung, um die manuelle Überwachung eines großen Volumens von Zertifikaten zu verhindern. Nutzen Sie einen proaktiven Ansatz, indem Sie über bevorstehende Ablaufzeiten auf dem Laufenden bleiben und zu einer gut verwalteten und sicheren Zertifikatumgebung beitragen.	Automatisierte Zertifikatverlängerung	Zertifikatanwender [sn_Disco_certmgmt.pki_user]
Eine sichere und konforme Zertifikatumgebung wird gepflegt, indem erforderliche Aktionen im Zusammenhang mit Zertifikataufgaben und -Flows überwacht, genehmigt, validiert und autorisiert werden. Dieser umfassende Ansatz stellt sicher, dass Zertifikatverlängerungsaufgaben und Incidents für abgelaufene Zertifikate angemessen behandelt werden, was zu einem robusten Sicherheits-Framework beiträgt.	Zertifizierungsaufgaben genehmigen	Zertifikatgenehmiger [pki_Approver]

Prozess-Flow in Zertifikatsbestand-Management

Zertifikatsbestand-Management Erlaubt Discovery Dient zum automatischen Scannen nach Zertifikaten für bestimmte Ports über Ihr vorhandenes CI-basiert Discovery Zeitpläne. Darüber hinaus können Sie neue Discovery-Zeitpläne zum Scannen einzelner URLs erstellen.

Funktionsweise von Zertifikatsbestand-Management

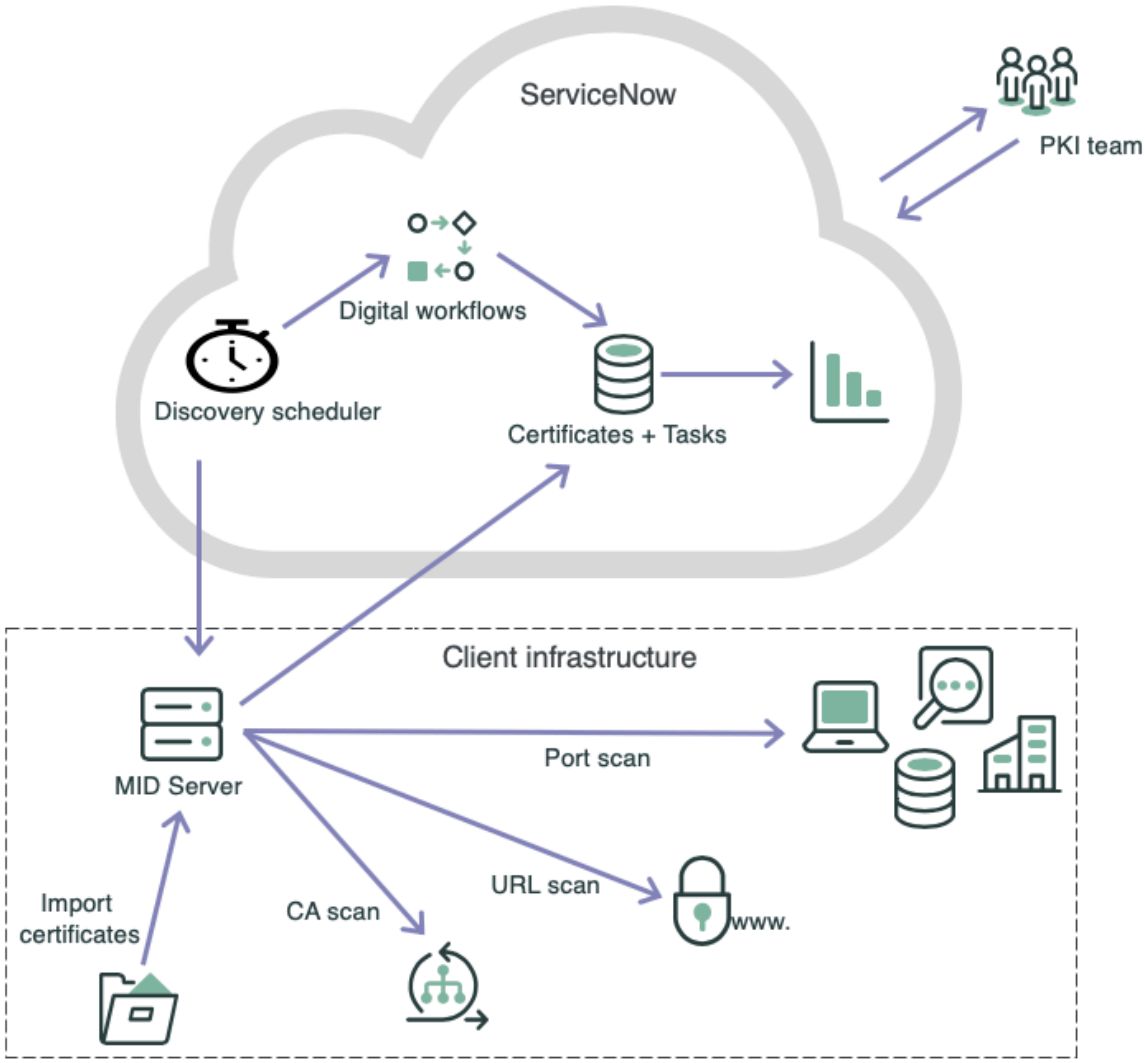
In Version 1.1.7 von Zertifikatsbestand-Management können Sie auch nach Zertifizierungsstellen suchen und Zertifikate aus Dateien importieren.

Mit dem Zurich-Release können Sie Version 1.2.0 von Zertifikatsbestand-Management herunterladen. Sie können in der Tabelle „HTTP(S)-Endpunkt“ [cmdb_ci_endpoint_http] verwendete Zertifikate erkennen und in einem Massenvorgang eine Liste von SSL-Zertifikaten importieren. Sie können Ereignisse und Warnungen für ablaufende und abgelaufene Zertifikate erstellen und sich in Slack über ablaufende und abgelaufene Zertifikate benachrichtigen lassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess-Flow-Diagramm



Die Zertifikatsbestand-Management Der Prozess-Flow ist in zwei verschiedene Phasen segmentiert:

- Phase vor der Discovery: Das anfängliche Segment des Prozesses variiert je nach Quelle der Zertifikat-Discovery. Diese Phase konzentriert sich auf Aktionen, die zum Identifizieren von Zertifikaten aus verschiedenen Quellen innerhalb der IT-Infrastruktur erforderlich sind.
- Phase nach der Discovery: Diese Phase umfasst nachfolgende Aktionen, die ausgeführt werden, nachdem die Zertifikate erfolgreich erkannt wurden. Es umfasst Prozesse wie Katalogisierung, Nachverfolgung und Verwaltung von Zertifikaten, um ihre sichere und effiziente Integration in das System sicherzustellen.

Phase vor der Discovery

Die Phase vor der Discovery umfasst vorbereitende Schritte, z. B. das Definieren von Scanparametern und das Konfigurieren von Anmeldeinformationsdetails, um eine reibungslose Initiierung des Zertifikaterkennungsprozesses sicherzustellen.

Discovery über Ports

Die Port-Probe [tls_ssl_certs] scannt automatisch 14 standardmäßig vorautorisierte Ports.
Die Port-Probe [tls_ssl_certs] scannt automatisch 14 standardmäßig vorautorisierte Ports.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Typische Ports für SSL: 443, 8443, 9443, 636 (ldaps), 993 (imaps), 995 (popssl), 989, 990
- StartTLS-Ports: 25 (smtp), 110, 143, 389, 21, 587 (smtp)

Als Teil des CI Discovery Während Shazzam verarbeiten, die MID-Server Verwendet Scanner, um Zertifikatketteninformationen von der IP-Portnummer zu erfassen und verschiedene Attribute zu erfassen, einschließlich der Zertifikathierarchie. Die MID-Server Wandelt diese Zertifikate dann in eine XML-Nutzlast um, die sie für die Instanz freigibt. Der Shazzam-Sensor erkennt wiederum den ECC-Warteschlangeneintrag und fügt einen neuen Datensatz in die Tabelle „erkanntes Zertifikat“ [sn_Disco_certmgmt_certificate_history] ein.

Die folgenden Felder werden aus der XML-Nutzlast abgerufen und in Java-Code aus der Shazzam TLS-Portprobe für erkannte Zertifikate verifiziert: Zertifikat-ID, Revocation_Status, Betreff, Aussteller, sans/, is_Self_signed, is_CA, valid_from, valid_to, Signature_Algorithmus, Fingerprint_Algorithmus, key_size, Serial_number und Version.

Discovery über URL

Die Tabelle „Zertifikat-URL“ [sn_disco_certmgmt_cert_url] enthält eine Liste von URLs, die Ziele der Zertifikaterkennung darstellen. Jeder Datensatz enthält auch einen optionalen Verweis auf die Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate], um anzugeben, welches Zertifikat mit der angegebenen URL-Definition verknüpft ist. Die erforderlichen Parameter aus dem Discovery Zeitpläne werden kombiniert, um zu erstellen und zu initialisieren Discovery Status. Die Probe [CertificateDiscoveryFromURLScan] erkennt die Zertifikatkette für jede der URLs im Batch und gibt eine XML-Nutzlast aus, die die Zertifikatkette für jedes Zertifikat enthält. Er fügt auch einen neuen Datensatz in die Tabelle „Erkanntes Zertifikat“ [sn_disco_certmgmt_certificate_history] ein.

Discovery Über Importieren von Zertifikaten (Version 1.1.7 Zertifikatbestand und -Verwaltung)

Die Importzertifikate werden über das Muster „SSL-Zertifikat importieren“ erkannt, das auf den folgenden Parametern basiert.

- Hostname/IP, auf dem die Zertifikate gehostet werden
- Ordner, in dem sich Zertifikate befinden
- TLS_keepOriginalCertificate: Wenn Sie diesen Parameter auf „wahr“ festlegen, kann dies zu einer erhöhten Nutzlastgröße führen, was möglicherweise zu Problemen mit zu wenig Arbeitsspeicher führen kann.
- Mid_Temp_folder: Der temporäre Ordner auf der MID-Server Wo Dateien vorübergehend kopiert werden.

Hinweis: Automatische Auswahl MID-Server Option wird für MID-Kombinationen von Windows und Linux NICHT unterstützt. Wenn der MID-Server zum Speichern der ursprünglichen Zertifikatdateien verwendet wird, müssen Hostname/IP leer oder localhost sein, und der spezifische MID-Server für den Discovery-Zeitplan muss ausgewählt sein.

Discovery Über CA-Behörde (Version 1.1.7 Zertifikatbestand und -Verwaltung)

Sobald die Anmeldeinformationen für Zertifikatbestand und -Verwaltung mit GoDaddy, DigiCert, Entrust oder Sectigo Certificate Authority und eingerichtet wurden Discovery Zeitplanausführungen, das spezifische CA-Muster führt REST-API-Aufrufe an (GoDaddy, DigiCert, Entrust oder Sectigo) durch, erfasst Zertifikatinformationen, ruft die Liste der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikate ab und speichert sie in den Tabellen [cmdb_ci_certificate], [certificate_Domain] und [sys_attachment].

CA_api_url und CA_api_Version sind optionale Parameter. Wenn diese Parameter in Musterparametern leer gelassen werden, werden Standardwerte verwendet. Die Standardwerte umfassen:

- DigiCert – Zertifikatverwaltung (CA_api_Version = v2, CA_api_url = https://www.digicert.com/services/)
- Entrust – Zertifikatverwaltung (ca_api_Version = v2, ca_api_url = https://api.entrust.net/enterprise/)
- GoDaddy – Zertifikatverwaltung (ca_api_Version = v1, ca_api_url = https://api.godaddy.com/)
- Sectigo – Zertifikatverwaltung (ca_api_Version = v1, ca_api_url = https://cert-manager.com/api/ssl/)

Die Argumente für GoDaddy-, DigiCert-, Entrust- und Sectigo-Muster lauten wie folgt. Ab Version 1,2 haben Sie die Möglichkeit, Sectigo zu scannen und Zertifizierungsstellen (CAS) zu vertrauen.

- Start_Offset: Die Offsetposition zum Lesen von Zertifikaten von CA-Behörden mit einem Standardwert von 0.
- Grenzwert: Die Anzahl der Zertifikate, die aus dem Start_Offset gelesen werden sollen, mit einem Standardwert von 1500.
- Anmeldeinformationsalias: Der Name des Anmeldeinformationsalias oder Tags, der mit den ZERTIFIZIERUNGSSTELLEN-Anmeldeinformationen verknüpft ist und in der serverlosen Ausführungsmusterkonfiguration hinzugefügt wurde.

  Wenn der Parameter „TLS_keepOriginalCertificate“ auf „wahr“ festgelegt ist, wird die Zertifikatdatei an das Zertifikat-CI angehängt. Dies kann die Nutzlastgröße erhöhen, was möglicherweise zu Problemen mit zu wenig Arbeitsspeicher führen kann.

- IncludeCertStatus: Ein Parameter zum Angeben zusätzlicher zu erkennender zertifikatstatus zusätzlich zu den Standardwerten.

zertifikatstatus nach Zertifizierungsstellen

Zertifizierungsstelle	Standardstatus Erkannt
Sectigo	○ Ausgegeben ○ Abgelaufen
DigiCert und GoDaddy	○ Aktiv ○ Abgelaufen ○ Widerrufen ○ Abgebrochen
Entrust	○ Aktiv ○ Abgelaufen ○ Widerrufen

Sie können mehrere Zertifikatstatus einschließen, indem Sie sie durch Kommas trennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die **status** Das Feld in der Tabelle „eindeutiges Zertifikat“ [cmdb_ci_certificate] gibt den Lebenszyklusstatus des Zertifikats an, nicht den Rohstatus aus der API. Wenn die API status wie „ausgestellt“, „gültig“, „abgelaufen“ oder „Abgebrochen“ zurückgibt, werden sie als „ausgestellt“ in der Tabelle „eindeutiges Zertifikat“ [cmdb_ci_certificate] gespeichert.

Sobald die Phase vor der Discovery abgeschlossen ist, fahren Sie mit fort Phase nach der Discovery .

Phase nach der Discovery

Nach der Discovery-Phase verwaltet das System TLS-Zertifikate, bietet Flexibilität für manuelle und automatisierte Anforderungsoptionen und erfüllt verschiedene zertifikatbezogene Aufgaben und Prozesse.

Die von der Zertifizierungsstelle und dem Stamm signierten TLS-Zertifikatketten füllen die eindeutigen Tabellen „Zertifikat“ [cmdb_ci_certificate] und „installiertes Zertifikat“ [sn_Disco_certmgmt_cmdb_installed_certificate] aus. Anschließend überprüft eine geplante Aufgabe die eindeutige Zertifikattabelle für ablaufende und abgelaufene Zertifikate und initiiert die Erstellung und Zuweisung von Zertifikataufgaben und Incidents.

Sie haben die Möglichkeit, neue Zertifikate manuell anzufordern und vorhandene zu verlängern. Weitere Informationen finden Sie unter Manueller Flow für Zertifikatanforderungen.

In Version 1,3 wurde die Möglichkeit eingeführt, Anforderungen für neue Zertifikate, Verlängerungen oder Widerrufen von Zertifikaten zu automatisieren. Weitere Informationen finden Sie unter Automatisierte Zertifikatverwaltung für TLS-Zertifikate.

Um die Systemleistung zu optimieren, entfernt eine Tabellenbereinigung alte Zertifikatdatensätze nach einer angegebenen Anzahl von Tagen automatisch aus diesen beiden Tabellen:

- Tabelle „Erkanntes Zertifikat“ [sn_disco_certmgmt_certificate_history]: älter als 30 Tage
- Tabelle „Installiertes Zertifikat“ [sn_disco_certmgmt_cmdb_installed_certificate]: älter als 90 Tage

Hinweis: Sie können verschiedene Verhaltensweisen im Zusammenhang mit umschalten Zertifikatsbestand-Management Abhängig von Ihren Anforderungen verwenden Sie bestimmte Zertifikateigenschaften, wie in gezeigt Discovery-Eigenschaften Und Systemeigenschaften .

Das System sucht nach Zertifikaten, die länger als sechs Monate abgelaufen oder archiviert wurden. Wenn ein Ersatzzertifikat vorhanden ist, entfernt das System ausstehende Aufgaben für diese veralteten Zertifikate.

Dieselbe sechsmonatige Nachfrist gilt für abgelaufene und archivierte Zertifikate und Zertifikataufgaben in *`failed`*status.

Zertifikatsbestand-Management Rollen und Verantwortlichkeiten

Dedizierte Anwender mit speziellen Rollen werden zugewiesen, um die Überwachung und Nachverfolgung von Anforderungen für neue und verlängernde Zertifikate zu optimieren.

Die Zertifikatsbestand-Management Dashboard- und Zertifikatkonfigurationseinstellungen werden abhängig von den zugewiesenen Rollen aktiviert oder deaktiviert.

Rolle	Verantwortlichkeiten
Zertifikatadministrator	Der Headless-Anwender (ein Account, der nicht an einen bestimmten Anwender gebunden ist) ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Verantwortlichkeiten
[sn_Disco_certmgmt.pki_admin]	im Basissystem enthalten und mit ausgestattet *sn_disco_certmgmt.pki_admin*Rolle. Es dient als Anrufer für automatisch generierte Verlängerungszertifikataufgaben und Incidents. Um diesen Anwender anzupassen, passen Sie die Anwender-ID mithilfe der Discovery-Eigenschaft an: *glide.discovery.certs.cert_admin_user_id*Anstatt sie als standardmäßigen Headless-Anwender zu belassen. Diese Rolle ist für die Änderung nicht standardmäßiger Attribute im ursprünglichen Zertifikatdatensatz verantwortlich. Sie kann Attribute wie Status, Status, Zugewiesen an, Zuweisungsgruppe, Verlängerungsnachverfolgung ändern. und Servicetyp. Die inhärenten Attribute des Zertifikats bleiben unverändert. Der Standardstatus für erkannte Zertifikate ist installiert, diese Rolle kann ihn jedoch manuell an andere status anpassen, z. B. „ausgestellt“, „installiert“, „widerrufen“ und „stillgelegt“. Darüber hinaus haben Anwender mit dieser Rolle die Möglichkeit, verschiedene Dashboards anzuzeigen und Lese-/Schreibzugriff auf Zertifikate und Zertifikataufgaben zu haben, die dem Zertifikat zugeordnet sind Discovery. **Hinweis:** • Die Rolle sn_disco_certmgmt.pki_admin enthält die Rolle sn_disco_certmgmt.pki_user. • Alle Benutzer mit der Rolle pki_admin können dem Genehmigerfeld im Zertifikatanforderungsformular hinzugefügt werden. Benutzern mit der Rolle pki_admin sollte die Rolle approved_admin manuell zugewiesen werden, um Anforderungen aus dem Zertifikataufgabenformular zu genehmigen oder abzulehnen. Dieser Genehmiger muss sich nicht anmelden, um die Aufgabe zu genehmigen. In einem Zertifikataufgabenformular oder einer zugehörigen Liste kann der Systemadministrator oder ein Benutzer mit der Rolle approved_admin oder pki_admin mehrere Genehmiger hinzufügen oder den vorhandenen Genehmiger bearbeiten. • Die Rolle approver_user ist erforderlich, wenn der Benutzer eine Anforderung genehmigen möchte, indem er sich anmeldet. Ohne die Rolle approver_user kann ein Benutzer nicht zu **Meine Genehmigungen** navigieren, um die Anforderungen zu genehmigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Verantwortlichkeiten
Zertifikatanwender [sn_Disco_certmgmt.pki_user]	Diese Rolle, die für die Überwachung der Zertifikat-Discovery verantwortlich ist, hat Zugriff auf verschiedene Dashboards und verfügt über Lese-/Schreibberechtigungen für Zertifikate und zugehörige Zertifikataufgaben.
Zertifikatgenehmiger [sn_Disco_certmgmt.pki_Approver]	Ein Anwender mit dieser Rolle (normaler Anwender), der für Zertifikatanforderungen verantwortlich ist, kann Zertifikatanforderungen über initiieren Servicekatalog Formular.
Zertifikatanforderer [sn_Disco_certmgmt.certificate_requester]	Diese Rolle, die für die Übermittlung von Zertifikatanforderungen verantwortlich ist, hat die Möglichkeit, Zertifikate von anzufordern und zu verlängern Servicekatalog.

Zertifikatsbestand-Management konfigurieren

Richten Sie einen optimierten Prozess ein, um Einblicke in die Zertifikatbestandsverwaltung zu erhalten, der wichtige Aspekte wie Zertifikaterkennung, Massenupload-Funktionalität, Wartung von Zertifikatkettenbeziehungen, Konfiguration von Anmeldeinformationsbezeichnern, Anpassung des Systems, Erstellung neuer Anforderungen/Verlängerungsanforderungen, Archivierungsaufgaben, Automatisierung der TLS-Zertifikatverwaltung, Integration mit Ereignismanagement, Slack-Benachrichtigungen für Warnungen und Nutzung von Cert-Manager für eine effiziente Zertifikatgenerierung abdeckt.

Konfiguration – Übersicht

Vor der Verwendung Zertifikatsbestand-Management, Es ist wichtig, die erforderlichen Plugins einzurichten, die Aktivierung sicherzustellen, Ihre Instanz auf die neueste Version zu aktualisieren und herunterzuladen Zertifikatsbestand-Management Anwendung von ServiceNow Store. Weitere Informationen finden Sie unter Erste Schritte mit Zertifikatsbestand-Management.

Nachdem die Voraussetzungen erfüllt sind, können Sie mit den folgenden Aufgaben fortfahren.

Zertifikatsbestand-Management-Aufgaben

Aufgabe	Beschreibung
Transparenz von TLS-Zertifikaten	Richten Sie ein effizientes Zertifikatbestandsverwaltungssystem ein, indem Sie die Zertifikat-Discovery konfigurieren, Massenzertifikathochladungen ermöglichen, Kettenbeziehungen verwalten, sicheren Zugriff konfigurieren und das System an bestimmte organisatorische Anforderungen anpassen.
Manueller Flow für Zertifikatanforderungen	Ermöglichen Sie die Erstellung neuer Zertifikatanforderungen oder Zertifikatverlängerungen im System unter Einhaltung definierter Richtlinien. Implementieren Sie einen Prozess zum Archivieren abgeschlossener Zertifikataufgaben, um einen Verlaufsdatensatz für Audits- und Compliance-Zwecke zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management-Aufgaben (Fortsetzung)

Aufgabe	Beschreibung
Automatisierte Zertifikatverwaltung für TLS-Zertifikate	Richten Sie Automatisierungsprozesse ein, um TLS-Zertifikate zu verwalten, einschließlich Erneuerung, Updates und Widerruf nach Bedarf.
Zertifikatintegrationen und -benachrichtigungen	Richten Sie die Integration zwischen Ereignismanagementsystemen und Zertifikatbestandsverwaltung für die Echtzeitüberwachung und Reaktion auf zertifikatbezogene Ereignisse ein. Konfigurieren Sie Benachrichtigungen, die an Slack-Kanäle gesendet werden sollen, und halten Sie Stakeholder über kritische Zertifikatereignisse und -Änderungen auf dem Laufenden.
Zertifikatgenerierung über die Zertifizierung-Manager-Integration	Verwenden Sie Cert-Manager oder ein ähnliches Tool, um den Zertifikatgenerierungsprozess zu automatisieren und eine effiziente und sichere Ausgabe basierend auf vordefinierten Richtlinien sicherzustellen.

Erste Schritte mit Zertifikatsbestand-Management

Vor dem Eintauchen in Zertifikatsbestand-Management Die Funktionalität der Anwendung erfüllt die erforderlichen Anforderungen, indem Sie das Plugin installieren und aktivieren, Ihre Instanz aktualisieren und erhalten Zertifikatsbestand-Management Anwendung aus dem ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Prozedur

1. Stellen Sie sicher, dass die folgenden Plugins installiert und aktiviert sind.
   - ITOM-Transparenz [com.snc.itom.vis.license]-Plugin
   - Plugin Discovery [com.snc.discovery]
   - Configuration Management for Scoped Apps (CMDB) Plugin [com.snc.cmdb.scope]
2. Bestätigen Sie, dass Ihr System auf aktualisiert wurde Zurich Oder eine neuere Version.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Upgradeprozesses wird Zertifikatsbestand-Management Das Plugin [com.sn_Disco_certmgmt] wird automatisch installiert, wenn der ITOM-Transparenz[com.snc.itom.vis.license] und Discovery[Com.snc.Discovery] Plugins sind bereits installiert.

3. Laden Sie herunter Zertifikatsbestand-Management Anwendung von ServiceNow Store.

Ergebnis

Sie sind bereit, mit zu beginnen Zertifikatsbestand-Management.

Hinweis: Die MID-Server Benötigt basierend auf Ihrem Anwendungsfall Zugriff auf die folgenden Endpunkte:

- Entrust: Zertifikat-URL erkennen: `https://api.entrust.net/enterprise/`
- Entrust-Download-Stammzertifikat-URL: `https://web.entrust.com/root-certificates/`
- DigiCert: `https://www.digicert.com/services/`
- Sectigo: `https://cert-manager.com/api/ssl/`
- GoDaddy: `https://api.godaddy.com/`

Transparenz von TLS-Zertifikaten

Die Anwendung Zertifikatsbestand-Management ermöglicht Discovery die automatische Suche nach Zertifikaten an bestimmten Ports über Ihre vorhandenen CI-basierten Discovery-Zeitpläne. Darüber hinaus können Sie Discovery-Zeitpläne zum Scannen einzelner URLs erstellen.

Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

In Zertifikatsbestand-Management, Sie können eine Liste der importierten Zertifikate zu hinzufügen Zertifikaterkennung über Zertifikatdateiimport ausführen, Und scannen Sie nach Zertifikaten von Ihrer Zertifizierungsstelle (Certificate Authority, CA), z. B. GoDaddy und DigiCert. Sie können Sectigo und Entrust CAS auch scannen.

Die vorhandenen Muster für Zertifizierungsstellen für DigiCert zum Sammeln der folgenden Felder als Teil der Discovery des CA-Trust-Zertifikats. Diese Felder sind erforderlich, um einen automatisierten Flow (Anforderung, Verlängerung oder Widerruf) für Zertifikate zu erstellen, die von der DigiCert CA Discovery erkannt wurden, und werden in der Tabelle „Zertifikaterweiterungen“ [sn_Disco_certmgmt_certificate_Extension] gespeichert.

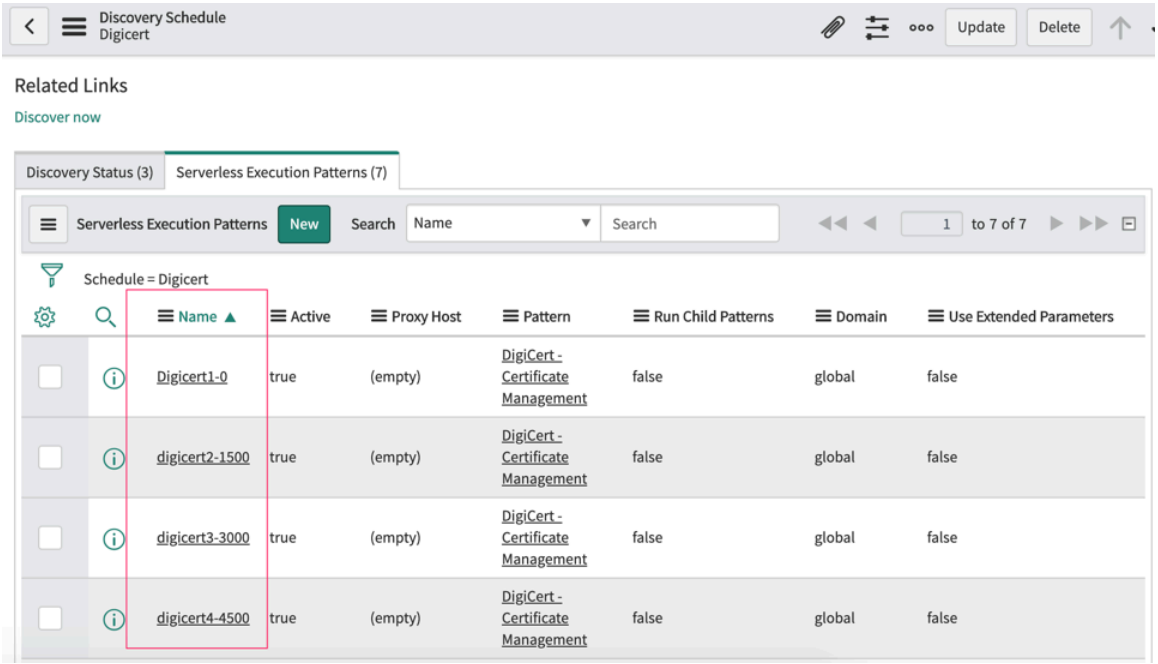
- Zertifikat-ID
- Auftrags-ID
- Fingerabdruck
- Seriennummer
- Zertifikatstatus

Mit Zertifikatsbestand-Management, Können Sie Wenn über Port-Scans ausführen. Sie können auch Zertifikaterkennung über individuelle URL-Scans ausführen.

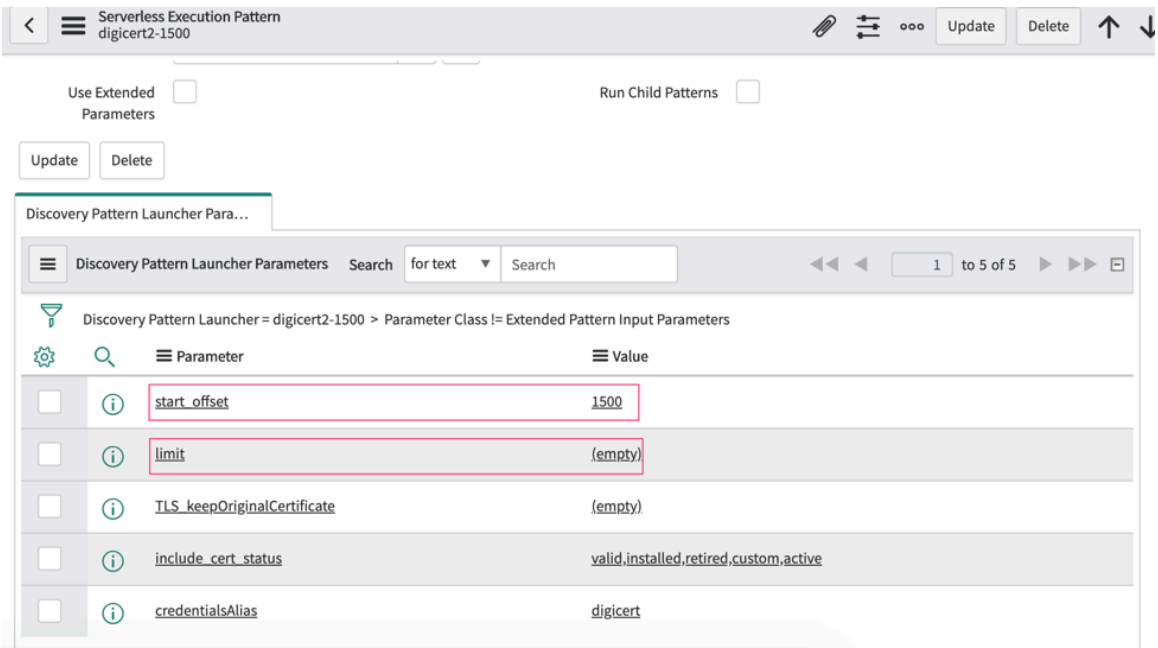
Um Zertifikate zu importieren oder die Vertrauensstellung einer Zertifizierungsstelle mit mehr als 1500 Zertifikaten zu erkennen, erstellen Sie einen Erkennungszeitplan mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mehreren konfigurierten serverlosen Mustern. Jede Musterausführung unterstützt die Erkennung von maximal 1500 Zertifikaten.



Zum Erkennen aller Zertifikate müssen „limit“ (Standardwert: 1500) und „start_offset“ (Standardwert: 0) entsprechend konfiguriert werden. Um beispielsweise bis zu 6.000 Zertifikate abzurufen, fügen Sie vier serverlose Muster mit Start_Offset 0, 1500, 3000 und 4500 hinzu. Die Parameter „start_offset“ and „limit“ werden wie dargestellt konfiguriert.



Wenn über Port-Scans ausführen

Wenn die TLS-Port-Probe [tls_ssl_certes] aktiviert ist, Discovery Scannt automatisch 14 vorautorisierte Ports als Teil Ihres vorhandenen CI Discovery Zeitpläne.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie die Port-Probe „TLS“ [tls_ssl_certs].
   a. Navigieren zu **Discovery-Definition** > **Anschlussprobes**an.
   b. Öffnen Sie **tls_ssl_certs**.
   c. Um die Probe zu aktivieren, wählen Sie aus **Aktiv** Kontrollkästchen.

      Standardmäßig ist das Kontrollkästchen für jede neue Installation deaktiviert.

   d. Speichern Sie die Änderungen.
2. Fügen Sie einen IP-Service hinzu, um die Port-Probe „TLS“ zu konfigurieren.
   a. Navigieren zu **Discovery-Definition** > **IP-Services**an.
   b. Erstellen Sie einen neuen IP-Service mit einem Port.
3. Konfigurieren Sie die Port-Probe „TLS“.

   Bearbeiten Sie die Port-Probe-Definition, um bis zu 138 zusätzliche Ports hinzuzufügen oder vorhandene zu entfernen.

   a. Navigieren zu **Discovery-Definition** > **Anschlussprobes**an.
   b. Öffnen Sie **tls_ssl_certs**.
   c. Entsperren Sie **Ausgelöst durch Services** Durch Auswahl des Schlosssymbols daneben.
   d. Entfernen Sie alle Ports aus der Liste, oder fügen Sie zusätzliche Ports aus dem Suchbereich hinzu.
   e. Speichern Sie die Änderungen.

Ergebnis

Ihre vorhandenen Discovery-Zeitpläne sollten an den angegebenen Ports dann automatisch nach Zertifikaten scannen.

Zertifikaterkennung über individuelle URL-Scans ausführen

Um die Zertifikat-Discovery durch URL-Scans zu initiieren, müssen Sie einzelne URLs manuell einbeziehen und ein neues Zertifikat konfigurieren Discovery Zeitplan.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Nur die Zertifikate, die während URL-Scans auf dem Server verfügbar sind, können erkannt werden. Verwenden Sie den folgenden Befehl, um die verfügbaren Zertifikate zu bestätigen:

```
openssl s_Client -Showcerts -Connect <URL>:<PORT> </dev/null
```

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Zertifikat-Discovery-Quell-URLS**an.
2. Um der Tabelle einzelne URLs hinzuzufügen, wählen Sie aus **Neu** .
   Stellen Sie genaue Ergebnisse sicher, indem Sie URLs im folgenden Format eingeben: Schema://Host:Port. Der Port ist optional, und wenn nicht angegeben, werden Standardwerte verwendet. Beispiele: https://www.servicenow.com oder https://servicenow.com:443, ldaps://myldap.com oder ldaps://myldap.com:636.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von finden Sie Discovery Zeitpläne, siehe Planen Sie eine horizontale Discovery .

   a. Wählen Sie Aus **Discovery** : **Zertifikate** .

   b. Wählen Sie **Typ der Zertifikaterkennung**:**URL-Zertifikaterkennung** aus.

      Behalten Sie die Batchgröße unverändert bei, es sei denn, es gibt eine bestimmte Empfehlung zum Ändern.

4. Zum Hinzufügen oder Löschen anderer URLs aus der **Zertifikat-URLs** Wählen Sie die Registerkarte aus **Bearbeiten** .
5. Wählen Sie **Absenden**.
6. Aktivieren Sie das Kontrollkästchen, um URLs aus der Tabelle „HTTP(s)-Endpunkt“ [cmdb_ci_endpoint_http] in den Discovery-Prozess einzubeziehen.

Ergebnis

Wenn Ihr Discovery-Zeitplan ausgeführt wird, wird in den angegebenen URLs automatisch nach Zertifikaten gescannt, und alle URLs werden aus der Tabelle cmdb_ci_endpoint_http abgerufen. Anschließend wird eine Zuordnung zwischen der URL und dem Zeitplan in *`sn_disco_certmgmt_cert_url_sched_m2m`* erstellt.

Wenn Service-Mapping aktiviert ist, wird standardmäßig eine Beziehung zwischen dem HTTP-Endpunkt und der Anwendung erstellt, wenn ein Eintrag in cmdb_ci_endpoint_http erstellt wird. Beispielsweise wird die Anwendung Amazon automatisch mit amazon.com verknüpft.

Die Beziehung lautet: cmdb_ci_endpoint_http[übergeordnet] --> [Endpunkt implementieren in::Endpunkt implementieren von] --> cmdb_ci_appl[untergeordnet].

Wenn die obige Beziehung vorhanden ist, erstellt die URL-Zertifikaterkennung eine zusätzliche Beziehung zwischen dem Zertifikat und der Anwendung. Diese Beziehung lautet: cmdb_ci_appl[übergeordnet] --> [Verwendet::Verwendet von] --> cmdb_ci_certificate[untergeordnet].

Hinweis: URL-Discovery-Zeitpläne generieren keine Serverkonfigurationselemente (CIs).

Massen-Upload von Zertifikaten verwenden

In Zertifikatsbestand-Management Ab Version 1.2.0 haben Sie die Möglichkeit, SSL-Zertifikate effizient als Massenimport zu importieren, sodass Sie bis zu 5000 Zertifikate in einer einzigen XLSX-Datei hochladen können, um Zeit- und Ressourceneinsparungen zu erzielen.

Vorbereitungen

Erforderliche Rolle: pki_user oder pki_admin

Dem Standardadministrator werden sowohl die Rollen pki_user als auch pki_admin zugewiesen. Die Anwender mit den folgenden Rollen haben Zugriff auf das Hochladen von Massenzertifikaten.

- sn_disco_certmgmt.pki_user
- sn_disco_certmgmt.pki_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Massen-Upload von Zertifikaten durchführen**an.
2. Wählen Sie auf der Seite „Massen-Upload“ die Option aus **Laden Sie Die Vorlagendatei Herunter** (.xlsx) Link zum Herunterladen von sample_cmdb_ci_certificate.xlsx Datei.
3. Öffnen Sie die heruntergeladene sample_cmdb_ci_certificate.xlsx Datei.
4. Sehen Sie sich die Beispielwerte in den Spalten als Leitfaden an, und fügen Sie die Eigenschaften des SSL-Zertifikats den entsprechenden Spalten hinzu.

   Jeder Eintrag im Excel-Blatt entspricht einem CI-Zertifikat. Stellen Sie sicher, dass die folgenden obligatorischen Spalten ausgefüllt sind.

   - root_issuer
   - issuer
   - subject_common_name
   - issuer_common_name
   - fingerprint
   - issuer_distinguished_name
   - subject_distinguished_name
   - fingerprint_algorithm
   - valid_to: Darf nicht kleiner als valid_fom sein. In Millisekunden. Beispiel: 1586789478000 stellt den 13. April 2020, 14:51:18 Uhr dar.
   - valid_from: In Millisekunden. Beispiel: 1586789478000 stellt den 13. April 2020, 14:51:18 Uhr dar.
   - signature_algorithm
   - key_size
   - Zustand: ausgegeben, installiert, widerrufen, deaktiviert oder sonstige

   Hinweis: Zur Aufrechterhaltung der Kettenbeziehung des Zertifikats muss jedes Zertifikat den Fingerabdruck seines Stammzertifikats im aufweisen **Root_issuer** Spalte und der Fingerabdruck des Ausstellers in **Aussteller** Spalte. Für selbstsignierte Zertifikate beides **Root_issuer** Und **Aussteller** Muss den Wert des Fingerabdrucks des Zertifikats aufweisen.

5. Speichern Sie sample_cmdb_ci_certificate.xlsx Datei.
6. Navigieren zu **Zertifikatverwaltung** > **Massen-Upload von Zertifikaten durchführen**an.
7. Wählen Sie Aus **Datei Durchsuchen** Und wählen Sie „Abgeschlossen“ sample_cmdb_ci_certificate.xlsx Datei.
8. Wählen Sie **Hochladen** aus.

Ergebnis

Wenn beim Upload Fehler auftreten, werden eine Warnmeldung und ein Link zu den Fehlerprotokollen angezeigt. Nur Benutzer mit der Administratorrolle können diese Protokolle anzeigen. Fehler können auftreten, wenn ein Pflichtfeld leer gelassen wird oder wenn ein valid_from-Epochenwert größer als valid_to ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem die Datei erfolgreich hochgeladen wurde, wird eine Erfolgsmeldung mit einem Umleitungslink `View All` angezeigt. Sie können eine Liste der Zertifikate anzeigen, die der Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate] hinzugefügt wurden.

Zertifikaterkennung über Zertifikatdateiimport ausführen

In Zertifikatsbestand-Management, Sie können Zertifikate erkennen, indem Sie Zertifikatdateien mithilfe der musterbasierten Discovery in das System importieren.

Vorbereitungen

Stellen Sie sicher **TLS_keepOriginalZertifikat** Ist auf festgelegt `False`.

Stellen Sie sicher, dass das Zertifikat in einem der folgenden Formate vorliegt: .Cert, .pem, .txt, .der.

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Die Importzertifikate werden mithilfe des Musters „SSL-Zertifikat importieren“ erkannt, das auf den folgenden Parametern basiert:

- Server: Der Hostname oder die IP-Adresse, auf der die Zertifikate gehostet werden. Wenn aus importiert wird MID-Server, Geben Sie localhost an, und lassen Sie temp_certificate_folder leer.
- Server_certificates_folder: Der Ordnerpfad auf dem Server, der die Zertifikate enthält.
- Parameter „TLS_keepOriginalCertificate“: Auf „falsch“ festlegen, um potenzielle Probleme mit Arbeitsspeicher aufgrund einer erhöhten Nutzlastgröße zu vermeiden.
- Temp_certificates_folder: Temporärer Ordner auf dem MID-Server Wohin die Dateien kopiert werden.

Prozedur

1. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von finden Sie Discovery Zeitpläne, siehe Planen Sie eine horizontale Discovery .
   a. Wählen Sie **Discovery**: **Zertifikate importieren** aus.
   b. Wählen Sie **Typ der Zertifikaterkennung**: **Zertifikate importieren** aus.
   c. Wählen Sie **Methode für MID Server-Auswahl**: **Spezifischer MID Server** aus.
   d. Wählen Sie Aus **MID-Server** : Wählen Sie den bevorzugten MID-Server aus.
   e. Fügen Sie die Anmeldeinformationen für hinzu Windows Oder Linux Hostcomputer, auf dem sich die Zertifikate befinden.
   f. Füllen Sie alle anderen erforderlichen Felder aus.
   g. Wählen Sie **Speichern**.
2. Um das Muster „SSL-Zertifikat importieren“ aus hinzuzufügen **Serverloses Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .

Ergebnis

Wenn Ihr Discovery-Zeitplan ausgeführt wird, werden Ihre Dateien automatisch gescannt.

Verbinden Sie ein Zwischenzertifikat mit seinem Stammzertifikat

Verbinden Sie Zwischenzertifikate mit kürzlich importierten Zertifikaten oder mit Stammzertifikaten außerhalb der Server, um die Zertifikatvertrauenskette abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wenn sich Ihr Stammzertifikat außerhalb Ihres Servers befindet, müssen Sie zuerst Erkennen Sie Stammzertifikate, die außerhalb Ihres Servers gehostet werden. Wenn Sie Zertifikatdateien importieren müssen, Zertifikaterkennung über Zertifikatdateiimport ausführen.

Hinweis: Wenn sich Ihre Stammzertifikate bereits auf Ihren Servern befinden, werden sie erkannt und mithilfe des Standards mit der Zertifikatkette verbunden Discovery Auf Ihren Servern bereitgestellte Probes.

Erforderliche Rolle: Admin, Discovery_admin, Zertifikatadministrator

Warum und wann dieser Vorgang ausgeführt wird

Ihr Zwischenzertifikat und Ihr Endentitätszertifikat befinden sich auf Ihrem Server. Discovery Scannt und richtet eine Zertifikatvertrauenskette für diese Zertifikate ein. Wenn Ihr Stammzertifikat außerhalb Ihres Servers gespeichert wird, führen Sie einen speziellen aus Discovery Darauf und verbinden Sie es mit Ihrem Zwischenzertifikat. Ein Fehler beim Herstellen der Verbindung kann dazu führen, dass Zwischenzertifikate als Stammzertifikat identifiziert werden.

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Wählen Sie Aus **sn_Disco_certmgmt.find_and_attach_root_certificate** .
3. Legen Sie den Wert auf fest **Wahr** Im Systemeigenschaftsdatensatz.
4. Speichern Sie den Datensatz, indem Sie auswählen **Aktualisieren** .
5. Führen Sie die Zertifikat-Discovery erneut aus
   Sie können die Discovery mit einer Portprobe oder einer URL erneut ausführen Discovery.

Ergebnis

Ihr Zwischenzertifikat identifiziert sein Stammzertifikat. Wird abgeschlossen Discovery Ihrer Zertifikatvertrauenskette.

Verwalten von Zertifikatketten-Beziehungen über Zertifikatimport

Die Aufrechterhaltung von Zertifikatkettenbeziehungen über den Zertifikatimport stellt die Integrität und Sicherheit digitaler Zertifikate sicher und validiert ihre Authentizität in einem System.

Zur Verwaltung von Zertifikatkettenbeziehungen wird als Erweiterung der Branchenstandard .txt verwendet. Zertifikatkettenbeziehungen werden nicht mit anderen Dateierweiterungen verwaltet. Die erwartete Reihenfolge von Zertifikaten in einer TXT-Zertifikatkettendatei lautet: Serverzertifikat, Zwischenzertifikat und Stammzertifikat.

Anwendungsfälle:

- Wenn zwei oder mehr Zertifikate gefunden werden, die Formate wie .cert und .pem aufweisen, wird nur das erste Zertifikat berücksichtigt. Die anderen Zertifikate werden nicht verarbeitet, und es werden keine Zertifikatkettenbeziehungen verwaltet.
- Wenn eine TXT-Erweiterung vorhanden ist, die nur ein Zertifikat enthält, wird sie als Serverzertifikat betrachtet, und es werden keine Zertifikatbeziehungen verwaltet.
- Wenn eine TXT-Erweiterung vorhanden ist, die zwei Zertifikate enthält, wird das erste Zertifikat als Serverzertifikat und das zweite Zertifikat als Stammzertifikat betrachtet (keine Zwischenzertifikate).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Zertifikatketten-Beziehung hängt von der letzten URL/IP-Discovery-Ausführung ab. Durch das Importieren einer Datei ohne Zertifikatketten-Beziehungen werden vorhandene Kettenbeziehungen unterbrochen, die demselben Zertifikat (Fingerabdruck) zugeordnet sind.

Bezeichner für Anmeldeinformationen für Anmeldeinformationstyp Zertifikatverwaltung konfigurieren

Stellen Sie eine eindeutige Identifizierung und effektive Verwaltung von Anmeldeinformationen sicher, indem Sie den Anmeldeinformationsbezeichner für konfigurieren Zertifikatsbestand-Management.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um die Unterstützung von Anmeldeinformationen für externen Speicher für die TLS-Zertifikat-Discovery von CA-Typen wie GoDaddy, DigiCert und Sectigo zu aktivieren, richten Sie den Anmeldeinformationsbezeichner in der Instanz für den jeweiligen Anmeldeinformationstyp Zertifikatverwaltung ein.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie einen Anmeldeinformationstyp mit der Bezeichnung aus **Zertifikatverwaltungs-Anmeldeinformationen** .
4. Wählen Sie im Formular „Anmeldeinformationen“ die aus **Externer Anmeldeinformationsspeicher** Kontrollkästchen.
5. Füllen Sie die Felder **Anmeldeinformationsalias** und **Nachweis-ID** aus.
   Stellen Sie sicher, dass die Anmeldeinformations-ID und Arg_ID in der Datei „Resolver für Anmeldeinformationen“ übereinstimmen.
6. Wählen Sie **Absenden**.

Führen Sie die Zertifikat-Discovery über die Abfrage der Zertifizierungsstelle aus

Die Ausführung der Zertifikat-Discovery über die Abfrage der Zertifizierungsstelle ermöglicht die systematische Identifizierung und den Import von TLS-Zertifikaten von bestimmten Zertifizierungsstellen und stellt eine umfassende Nachverfolgung, Verwaltung und Sicherheit des Zertifikatbestands sicher. Erkennen Sie TLS-Zertifikate von Zertifizierungsstellen (CA) mit Zertifikatsbestand-Management, Mit Mustern für verschiedene Zertifizierungsstellen-Lieferanten.

Vorbereitungen
Erforderliche Rolle: pki_admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
In der Zertifikat-Discovery verwendet das Muster Certificate Authorties (CA) bestimmte API-Elemente. Der Anwender, der den Instanzanmeldeinformationen hinzugefügt wurde, benötigt Berechtigungen für diese Abfragen. Weitere Informationen zum Muster für Zertifizierungsstellen (CA) und den zugehörigen API-Elementen finden Sie unter API-Elemente und -Berechtigungen für Zertifizierungsstellen-Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Generieren Sie bei Bedarf einen Anmeldeinformationsalias.
   Weitere Informationen finden Sie unter Anmeldeinformationsaliasse für Discovery . Erstellen Sie für neue Anmeldeinformationen einen neuen Anmeldeinformationsalias. Wenn mehrere Anmeldeinformationen denselben Alias teilen, Discovery Priorisiert die Anmeldeinformationen und initiiert den Prozess.
2. Erstellen Sie einen neuen Anmeldeinformationstyp, der für die Zertifizierungsstelle (Certificate Authority, CA) spezifisch ist.

   a. Navigieren zu **Discovery** > **Anmeldeinformationen** Wählen Sie dann aus **Neu** .

   b. Wählen Sie **Anmeldeinformationen für Zertifikatverwaltung** aus.

   c. Zum Entsperren von **Aliasliste für Anmeldeinformationen** , Wählen Sie das Schlosssymbol.
   Der Alias ist den Anmeldeinformationen zugeordnet.

   d. Wählen Sie **Typ angeben**: **Anmeldeinformationen** aus.

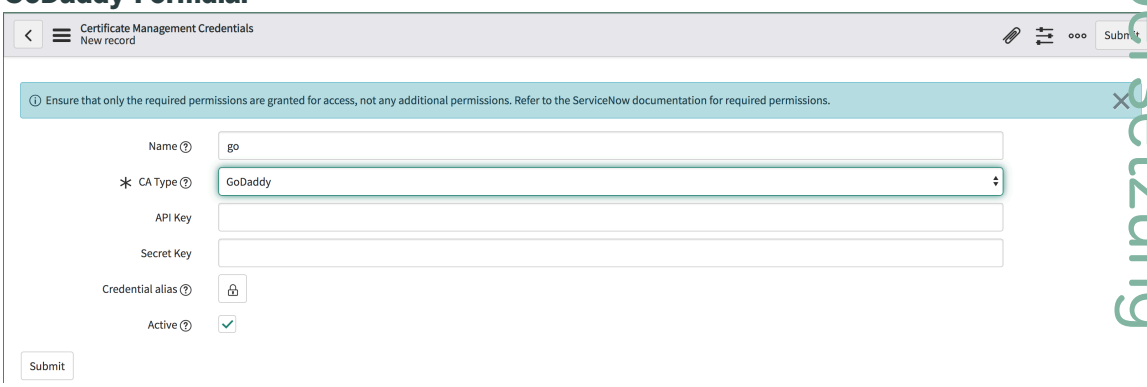
   e. Wählen Sie Aus **CA-Typ** .
   Die verfügbaren CA-Typen sind: GoDaddy, DigiCert, Entrust oder Sectigo.

   f. Füllen Sie die Felder für den ausgewählten CA-Typ aus.

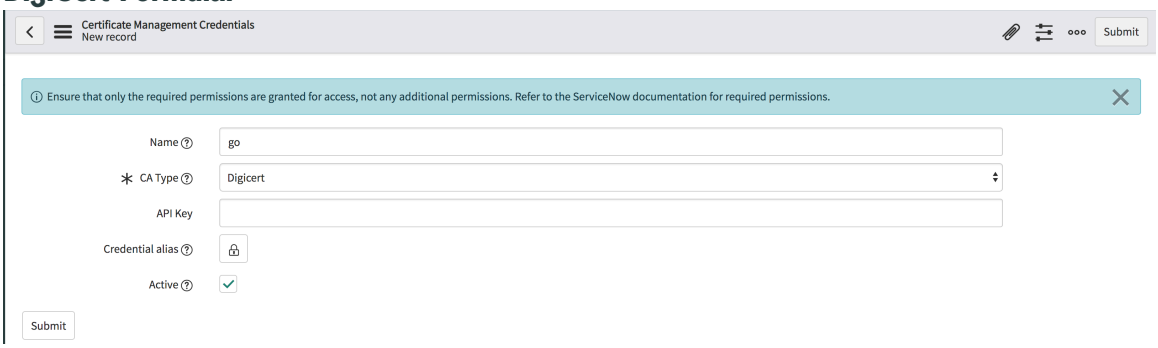
   Jede Zertifizierungsstelle (Certificate Authority, CA) erfordert bestimmte Formularfeldeinträge. Weitere Informationen finden Sie unter API-Schlüssel-Anmeldeinformationen .

   Sehen Sie sich die folgenden Beispiele für Formulare für jede CA an.

GoDaddy-Formular



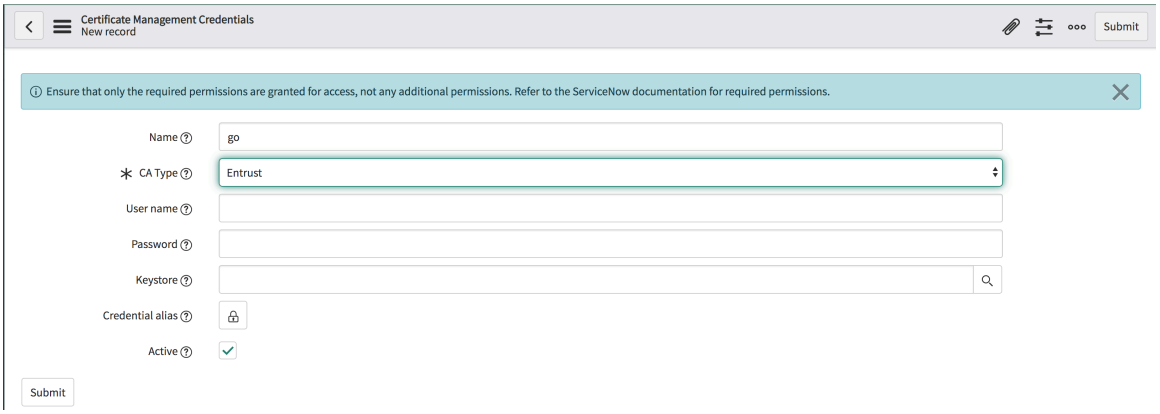
DigiCert-Formular



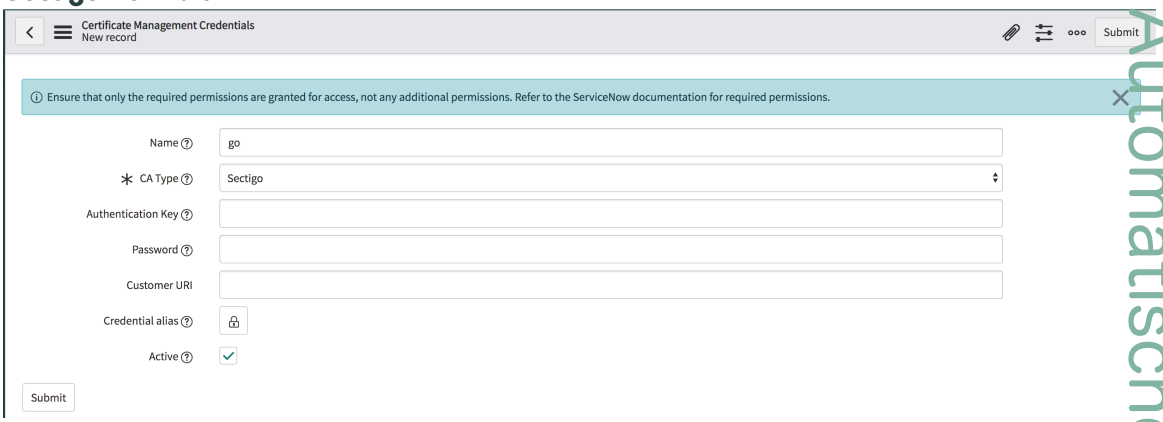
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entrust-Formular



Sectigo-Formular



Automatische Übersetzung

3. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von finden Sie Discovery Zeitpläne, siehe Planen Sie eine horizontale Discovery .
   a. Wählen Sie Aus **Discovery** : **Zertifikate** .
   b. Wählen Sie **Typ der Zertifikaterkennung**: **CA Trust Discovery (Erkennung der CA-Vertrauensstellung)** aus.
   c. Wählen Sie **Methode für MID Server-Auswahl**: **Automatische Auswahl** oder **Spezifischer MID Server** aus.
   d. Füllen Sie alle anderen erforderlichen Felder aus.
   e. Wählen Sie **Speichern**.
4. Zum Hinzufügen eines benötigten CA-Musters über die **Serverloses Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .
   Wenn Sie aktivieren **Zertifikatstatus einschließen** Option können Sie mehrere Zertifikatstatus angeben, indem Sie sie durch Kommas trennen.
5. Wählen Sie **Absenden**.

Ergebnis

Wenn Ihr Discovery-Zeitplan ausgeführt wird, werden Ihre Dateien automatisch gescannt.

Erkennen Sie Stammzertifikate, die außerhalb Ihres Servers gehostet werden

Sammeln Sie Informationen zu Stammzertifikaten, die außerhalb Ihres Servers gespeichert sind. Erstellen Sie einen spezialisierten Discovery Zeitplan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Admin, Discovery_admin, Zertifikatadministrator

Warum und wann dieser Vorgang ausgeführt wird
Um Stammzertifikate zu erkennen, die außerhalb Ihres Servers gespeichert sind, erstellen Sie ein spezielles Discovery Planen Sie, um sie als Ziel festzulegen.

Prozedur
1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Von Discovery Seite „Zeitplan“ auswählen **Neu** .
3. Füllen Sie die Felder im Formular „Discovery-Zeitplan“ aus.
   Eine Beschreibung der Feldwerte finden Sie unter Discovery Formulartabelle planen.
4. Speichern Sie diesen Datensatz, indem Sie auswählen **Aktualisieren** .
5. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
6. Erstellen Sie ein serverloses Ausführungsmuster.
   a. Wählen Sie **Neu**.
   b. Wählen Sie auf der Seite „neuer Datensatz“ das Suchsymbol ( ) In **Muster** Feld.
   c. Füllen Sie aus **Name** Feld.
   d. Suchen und auswählen **SSL-Zertifikat importieren** .
   e. Wählen Sie **Absenden**.
      Sie werden zurück zu weitergeleitet Discovery Zeitplanseite, die in Schritt 4 erstellt wurde.
7. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
8. Wählen Sie aus **Name** Des neuen Musters, das Sie gerade erstellt haben.
9. Wählen Sie aus **(Leer)** Wertfeld und fügen Sie für jeden Parameter einen Wert hinzu.
   Anleitungen dazu, welche Werte festgelegt werden sollen, finden Sie unter Zertifikaterkennung über Zertifikatdateiimport ausführen.
10. Sammeln Sie Informationen zu Ihrem Stammzertifikat, indem Sie eine eindeutige Zertifikatdatei erstellen.
    a. Navigieren Sie zu **Discovery-Zeitplan** Datensatz, den Sie erstellt haben.
    b. Wählen Sie den Link aus **Entdecken Sie jetzt** Um zu beginnen Discovery Das Ihr Stammzertifikat sammelt.
11. Navigieren zu **Alle** > **Eindeutige Zertifikate**an.
12. Nach Discovery Ist abgeschlossen. Suchen Sie Ihr Stammzertifikat, um zu bestätigen, dass es vorhanden ist.

Ergebnis
Ihr Discovery Sammelt Informationen zu Ihrem Stammzertifikat, das sich außerhalb eines Servers befindet.

Nächste Maßnahme
Verbinden Sie ein Zwischenzertifikat mit seinem Stammzertifikat Um Ihre Zertifikatkette abzuschließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management anpassen

Passen Sie verschiedene Aspekte in an Zertifikatsbestand-Management Verwenden Discovery Eigenschaften, mit denen Sie die Lösung an Ihre spezifischen Anforderungen anpassen und die Gesamtverwaltung von TLS-Zertifikaten verbessern können.

Vorbereitungen
Erforderliche Rolle: discovery_admin oder admin

Prozedur

Zum Bearbeiten Discovery-Eigenschaften , Navigieren Sie zu **Alle** > **Discovery-Definition** > **Eigenschaften**an.

- glide.discovery.certs.cert_admin_user_id
- glide.discovery.certs.days_before_expiration_to_create_renewal_task
- glide.discovery.certs.en_incident_creation_for_expired_certipts
- glide.discovery.certs.enable_renewal_task_creation_for_discovered_certipts
- glide.discovery.certs.slack_channel_id

Manueller Flow für Zertifikatanforderungen

Anforderungen und Incidents zur Zertifikatverlängerung werden automatisch erstellt, wenn Zertifikate bald ablaufen oder abgelaufen sind. Sie können Anforderungen auch manuell mit erstellen Servicekatalog.

Eine geplante Aufgabe untersucht täglich die Tabelle „eindeutige Zertifikate“ [cmdb_ci_certificate] und löst Verlängerungsaufgaben aus, wenn ein Zertifikat abgelaufen ist oder kurz vor dem Ablauf steht.

Wichtige Überlegungen zur Erneuerung von Zertifikaten:

- Aufgaben für Zertifikatverlängerungen werden 60 Tage vor Ablauf automatisch generiert. Um den Zeitrahmen zu ändern, aktualisieren Sie Discovery-Eigenschaft : `glide.discovery.certs.days_before_expiration_to_create_renewal_task`.
- Zertifikataufgaben werden automatisch die Priorität 3 – Mittel zugewiesen. Ändern Sie die Priorität, indem Sie die Aufgabe bei Bedarf öffnen.
- Wenn für das aktuelle Zertifikat bereits eine Zertifikataufgabe vorhanden ist, werden keine zusätzlichen Aufgaben erstellt.
- Für Verlängerungszertifikataufgaben und Incidents werden basierend auf dem Zertifikat-CI verschiedene Felder automatisch vorab ausgefüllt.
- Wenn ein Zertifikat abläuft und nicht ersetzt wird, wird ein neuer Incident erstellt. Für jedes abgelaufene Zertifikat wird jedoch nur ein Incident generiert.
- Um die Liste der Zertifikat-Incidents anzuzeigen, navigieren Sie zu **Service Desk** > **Incidents**an.

Neue Zertifikatanforderungen erstellen

Erstellen Sie neue Zertifikatanforderungen manuell über Servicekatalog Für eine personalisierte und effiziente Beschaffung von Zertifikaten, die mehr Flexibilität und Kontrolle bietet.

Vorbereitungen
Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: pki_admin

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**an.
2. Wählen Sie Aus **Neues Zertifikat Anfordern** .
3. Geben Sie die erforderlichen Informationen für die folgenden Pflichtfelder an.
   - **Zertifikatsignierungsanforderung**
   - **Zertifizierungsstelle**
   - **Zertifikattyp**
   - **Gültigkeitszeitraum**
   - **Genehmiger**
4. Geben Sie nach Bedarf zusätzliche Details im Formular ein, oder wählen Sie sie aus.
5. Wählen Sie **Absenden**.

Ergebnis

Die Zertifikataufgabe wird generiert und zur Genehmigung übermittelt. Das Genehmigungsfeld ist schreibgeschützt für pki_user und kann für pki_admin bearbeitet werden.

Anforderung zur Verlängerung von Zertifikaten erstellen

Initiieren Sie Verlängerungsanforderungen für Zertifikate manuell mit Servicekatalog Für zusätzliche Flexibilität und Kontrolle.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist.

Erforderliche Rolle: pki_admin

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**an.
2. Wählen Sie Aus **Zertifikat Verlängern** .
3. Wählen Sie ein Zertifikat-CI aus.
4. Geben Sie die erforderlichen Informationen für die folgenden Pflichtfelder an.
   - **Zertifikatsignierungsanforderung**
   - **Angefordert für**
   - **Genehmiger**
5. Geben Sie nach Bedarf zusätzliche Details im Formular ein, oder wählen Sie sie aus.
6. Wählen Sie **Absenden**.

Ergebnis

Die Zertifikataufgabe wird generiert und zur Genehmigung übermittelt. Das Genehmigungsfeld ist schreibgeschützt für pki_user und kann für pki_admin bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Benachrichtigungsprozess für die Zertifikatverlängerung unterstützt ausschließlich den manuellen Flow und erfordert keine automatisierte Zertifikatverwaltung. Für CSR-Informationen müssen Sie die automatisierte Zertifikatverwaltung verwenden.

Wenn beim Überwachen des Status eines Zertifikatauftrags ein konfigurationsbezogenes Problem auftritt, kann die Aufgabe in „in Arbeit“ stecken bleiben. Der PKI-Administrator ist für die Lösung solcher Probleme verantwortlich. Beispiel: Wenn MID-Server Während der geplanten Aufgabe, die den Status der Zertifikatreihenfolge nachverfolgt, ausfällt, wartet das System auf die nächste geplante Aufgabe, anstatt einen Fehler zu protokollieren. Wenn MID-Server Wird vor dem nachfolgenden Auftrag wieder hochgefahren, wird der Zertifikatabruf entsprechend fortgesetzt.

Zertifikataufgaben archivieren

In Version 1.1.7 Zertifikatsbestand-Management, Führt das Plugin „Datenarchiver“ [com.glide.auxdb] tägliche Vorgänge durch, um Daten, die nicht mehr aus primären Tabellen benötigt werden, in einen festgelegten Satz von Archivtabellen zu übertragen.

Vorbereitungen
Erforderliche Rolle: pki_user oder pki_admin

Warum und wann dieser Vorgang ausgeführt wird
Zertifikatsbestand-Management Überprüft und archiviert aktiv Zertifikataufgaben, die ein Jahr älter sind. Um dies zu erleichtern, muss das entsprechende Plugin aktiviert und aktiviert sein, damit die geplanten Archivierungsaufgaben ausgeführt werden können. Es ist wichtig zu beachten, dass die Zertifikataufgaben-Archivierungsregel, die im enthalten ist Zertifikatsbestand-Management Anwendung, ist standardmäßig inaktiv.

Prozedur

1. Aktivieren **Zertifikataufgabenregel** .
2. Navigieren zu **Archivregeln** > **Archiv Der Zertifikataufgabe**an.
3. Aktivieren Sie die Checkbox **Aktiv**.

Ergebnis
Nach der Aktivierung archiviert diese Regel Daten aus der Zertifikataufgabentabelle [sn_Disco_certmgmt_certificate_Task] unter den folgenden Bedingungen:

- Status „Geschlossen - vollständig“
- Das letzte Update ist mehr als zwölf Monate her

Automatisierte Zertifikatverwaltung für TLS-Zertifikate

Von Zertifikatsbestand-Management Version 1,3.8. Sie können den Anforderungs-Flow für neue Zertifikate, Verlängerungen und Widerrufen von Zertifikaten automatisch amtieren.

Zertifikatsbestand-Management Ruft automatisch Zertifikate von Zertifizierungsstellen (Certificate Authorties, CAS) ab, ohne dass ein manuelles Eingreifen des PKI-Teams erforderlich ist. Ab Version 2,1 unterstützt diese Funktion DigiCert und Entrust CA Gateway für nahtlose automatische Erfüllungs-Flows mit der Einschränkung, dass nur OV-DigiCert-Zertifikate angefordert werden können. Version 2.3.2 führt Unterstützung für die Microsoft CA ein. Weitere Informationen finden Sie in der Dokumentation des jeweiligen Anbieters. Für automatisierte Flows mit DigiCert oder Entrust CA Gateway in Zertifikatbestand und -Verwaltung müssen Sie über Berechtigungen zum anfordern, verlängern und Widerrufen von Zertifikaten verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Microsoft CA-Anwender benötigt die folgenden Berechtigungen:

Microsoft Gateway-Anwenderberechtigungen

Berechtigung	Aktion
CredSSP auf CA, Zwischenserver und MID-Server	Richten Sie CredSSP auf CA, Zwischenserver und ein MID-Server. Informationen zu CredSSP-Konfigurationsschritten finden Sie in der Now Support Knowledge Base, die im KB-artikel dokumentiert ist KB1632624 .
Mitgliedschaft bei Enterprise-Administratoren	Stellen Sie sicher, dass der Anwender die Mitgliedschaft in der Enterprise-Administratorgruppe hat.
Sicherheitsgruppeneinschluss für Vorlage	Stellen Sie sicher, dass der Anwender in der Sicherheitsgruppe der Vorlage enthalten ist.
Bestimmte Berechtigungen in CA	Gewähren Sie den Anwendern Berechtigungen: Zertifikate lesen, ausstellen und verwalten, CA verwalten und Zertifikate anfordern in der CA.

Automatisierte Flows für die Zertifikatverwaltung verwenden

Certificate and Management optimiert Ihre TLS-Zertifikatprozesse und bietet Vorteile wie verbesserte Effizienz und erhöhte Sicherheit. Die Automatisierung der Zertifikatverwaltung stellt eine rechtzeitige Erneuerung von Zertifikaten sicher, wodurch das Risiko abgelaufener Zertifikate minimiert wird.

Vorbereitungen

Zur Verwendung von Microsoft Automatisierter Flow der Zertifizierungsstelle. Sie müssen installieren **ServiceNow IntegrationHub-Aktionsschritt – PowerShell** Plugin und muss über ein Integration Hub-Abonnement verfügen. Weitere Informationen finden Sie unter IntegrationHub Nutzung und Abonnement .

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Legen Sie die Systemeigenschaft *sn_disco_certmgmt.cert_task_default_approval_group* auf den Standardnamen der Genehmigungsgruppe fest.
   Wenn die Zertifikatanforderung in den manuellen Modus wechselt, wird der Name der Genehmigungsgruppe als Standardgruppe verwendet. Beispielsweise wird die Standardgruppe verwendet, wenn keine übereinstimmende Richtlinie oder mehr als zwei übereinstimmende Richtlinien vorhanden sind. Sie können mehrere durch Kommata getrennte Genehmigungsgruppen hinzufügen. Die erste Gruppe in der Liste, die zur Aufgabendomäne gehört, wird zur Genehmigung verwendet. Wenn keine domänenspezifische Gruppe gefunden wird, wird der erste Name in der globalen Domänenliste verwendet.
2. Aktualisieren Sie die Systemeigenschaft, um den Gültigkeitszeitraum des Zertifikatauftrags festzulegen *sn_disco_certmgmt.default_cert_order_validity_period*.
   Der Standardwert ist 730 Tage (2 Jahre).
3. Fügen Sie die IP von hinzu Microsoft CA-Server.
   - Fügen Sie hinzu *ca_host_ip*Feld der Weiterleitungsrichtlinie.
   - Fügen Sie die IP eines Zwischenservers in hinzu *ca_host_ip*Feld der Weiterleitungsrichtlinie.

   Der Zwischenserver kann beliebig sein Windows Server in derselben Domäne wie Microsoft CA-Server und hat Zugriff auf die in Powershell verfügbaren Befehle certutil und certreq. Wenn ein Zwischenserver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet wird, wird MID-Server Führt ein Powershell-Skript auf dem Zwischenserver mithilfe von „invoke-Command“ aus. Dieser Befehl verwendet einen Remote Procedure Call (RPC), um die certutil- und certreq-Befehle auf dem CA-Server auszuführen.

4. Erstellen Sie die Zertifikatanmeldeinformationen, und ordnen Sie diese dem Anmeldeinformationsalias zu. Jede Anmeldeinformation sollte mit einem eindeutigen Anmeldeinformationsalias zugeordnet werden. Weitere Informationen finden Sie unter Anmeldeinformationsalias für Discovery .

5. Bestätigen Sie, dass sich die Informationen zu Zertifikat und Zertifikat-URL in den Tabellen „Zertifizierungsstelle“ [sn_Disco_certmgmt_CA] und „API-URL der Zertifizierungsstelle“ [sn_Disco_certmgmt_ca_api_url] befinden.
Die Standard-URL für DigiCert und Entrust CA Gateway stellt alle Validierungstyp-URLs bereit. Sie können auch zusätzliche URLs hinzufügen.

6. Legen Sie die Aufgabenpriorität fest.

   Die Priorität und der Typ der Change-Anforderungen werden basierend auf der Priorität der Aufgabe zugeordnet. Change-Anforderungen haben die gleiche Priorität wie eine Aufgabenpriorität, außer dass eine Change-Anforderung keine P5 hat, daher wird sie in diesem Fall P4 zugeordnet.

   Um den Typ von Change-Anforderungen zu ändern, die Eigenschaft „Change-Management“ *`com.snc.change_management.change_model.type_compatibility`*Muss auf „wahr“ festgelegt werden. Der Standardwert ist False.

   a. Legen Sie bei Bedarf die Aufgabe fest, und ändern Sie die Systemeigenschaft *`sn_disco_certmgmt.default_cert_task_priority`*Zum Konfigurieren der Prioritäten „Neu“ und „Verlängerungsaufgabe“.
   Die Priorität ist standardmäßig P3. Die möglichen Werte sind 1, 2, 3, 4, 5. Wenn der Wert 1 ist, wird die Priorität auf P1 festgelegt usw. Wenn ein ungültiger Wert angegeben ist, wird die Priorität auf den Standardwert P3 zurückgesetzt.

   b. Legen Sie bei Bedarf die Aufgabe fest, und ändern Sie die Systemeigenschaft *`sn_disco_certmgmt.default_revoke_cert_task_priority`*Dient zum Konfigurieren von Prioritäten für Widerrufsaufgaben.
   Die Priorität ist standardmäßig P1. Die möglichen Werte sind 1, 2, 3, 4, 5. Wenn der Wert 1 ist, wird die Priorität auf P1 festgelegt usw. Wenn ein ungültiger Wert angegeben ist, wird die Priorität auf den Standardwert P1 zurückgesetzt.

7. **Wahlweise:** Installieren Sie das Plugin „Integration Hub“ [com.glide.hub.integrations].

   (Optional) Das Plugin [com.glide.hub.integrations] ist nicht erforderlich, um das DigiCert- oder Entrust-CA-Gateway-Zertifikat anzufordern und den Status der Zertifikatbestellung nachzuverfolgen. Wenn Sie jedoch die Zertifikat-Subflow-Aktionen debuggen oder Ihren eigenen Anpassungs-Flow für DigiCert oder Entrust CA Gateway hinzufügen möchten, installieren Sie dieses Plugin.

Routing-Richtlinien für die automatisierte Zertifikatverwaltung einrichten

Richten Sie eine Weiterleitungsrichtlinie ein, um Ihre Zertifikatbestands- und -Verwaltung zu automatisieren. Das Erstellen einer Richtlinie basierend auf Zertifizierungsstelle (CA), Umgebung und anderen Funktionen stellt eine effiziente TLS-Zertifikatverwaltung sicher.

Vorbereitungen
Erforderliche Rolle: pki_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die Routing-Richtlinie entscheidet, welche Zertifizierungsstelle für Zertifikatvorgänge kontaktiert werden muss. Sie enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR. Die Routing-Richtlinie löst den Flow zum Anfordern von Zertifikaten für bestimmte Zertifizierungsstellen aus.

Hinweis: Eine Zertifikatanforderung gilt als Duplikat, wenn eine weitere Zertifikataufgabe mit demselben Domänennamen vorhanden ist, die noch ausgeführt wird. Doppelte Zertifikatanforderungen sind nicht zulässig. Sie können diese Einstellung jedoch überschreiben, indem Sie das Kontrollkästchen „Allow duplicate requests“ (Duplizierte Anforderungen zulassen) aktivieren. Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**an.
2. Wählen Sie **Neu**, und füllen Sie die erforderlichen Felder im Formular aus.
   Während Anforderungen für neue Zertifikate und die Erneuerung von Zertifikaten automatisiert werden können, bevorzugen viele PKI-Teams eine persönliche Validierung vor der Erfüllung. Wenn ja, wählen Sie aus **Genehmigung erforderlich** Kontrollkästchen.

   Hinweis:

   Organisation, Organisationseinheit, Ort, Bundesland, Land und E-Mail akzeptieren kommagetrennte Werte. * wird als beliebig betrachtet. Der allgemeine Antragstellername und der alternative Antragstellername werden mit einem regulären Ausdruck unterstützt. Das RegEx-Format weist die folgenden Einschränkungen auf:

   - Darf keine Kommas enthalten.
   - Sie darf nicht mit einem Schrägstrich (/) beginnen und enden und * entspricht einem.
   - Weitere Informationen zu den Feldern und Werten in einem Weiterleitungsrichtlinienformular finden Sie unter .

3. Die folgenden CSR-Attribute stimmen mit den Einträgen in der Tabelle „Routing-Richtlinie“ [sn_disco_certmgmt_routing_policy] überein:
   - Organisation
   - Organisationseinheit
   - Ort
   - Status
   - Land
   - E-Mail
   - Umgebung
   - Zertifikatzweck (intern/extern)
   - Allgemeiner Antragstellername
   - Alternativer Antragstellername

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Für Entrust CA Gateway gibt es auch diese Felder: „Bezeichner der Zertifizierungsstelle“, „Zertifikatprofil“ und „Zertifikatformat“. Für Microsoft CA verwendet auch diese Felder: Zertifizierungsstelle, CA-Vorlagenname, CA-Host-IP, Anmeldeinformationen und CSR-Attribute. Für DigiCert erfordert die Weiterleitungsrichtlinie auch ein URL-Feld der Zertifizierungsstellen-API, um automatisierte Prozesse und Widerrufs-Flows zu verarbeiten.

4. Die folgenden Optionen können auftreten.

Option	Bezeichnung
Wenn eine einzelne Routing-Richtlinie übereinstimmt	Überprüfen Sie die folgenden Bedingungen: ○ Validieren Sie den allgemeinen Antragstellernamen mit dem Muster des regulären Ausdrucks, das in der Tabelle „Routing-Richtlinie“, dem Domänennamen oder * angegeben ist. ○ Überprüfen Sie, ob der Gültigkeitszeitraum der Zertifikatanforderung den maximalen Gültigkeitszeitraum in der Tabelle „Routing-Richtlinie“ nicht überschreitet. ○ Prüfen Sie auf die Kennzeichnung für zulässige duplizierte Zertifikatanforderungen in der Tabelle „Routing-Richtlinie“.
Wenn mehrere Routing-Richtlinien in Frage kommen	Die Aufgabe wird der Standardgenehmigergruppe zugewiesen.
Wenn keine Routing-Richtlinie gefunden wurde	Die Aufgabe wird der Standardgenehmigergruppe zugewiesen.
Wenn eine einzelne Richtlinie übereinstimmt und die Kennzeichnung „Genehmigung erforderlich“ auf „true“ gesetzt ist	Die Aufgabe wird der Aufgabengenehmigungsgruppe zugewiesen, die in der Routing-Richtlinie definiert ist.

Ergebnis

Die Genehmigungsgruppe ist der Routing-Richtlinie zugewiesen und enthält die Rolle pki_approver und mindestens eines der aktiven Gruppenmitglieder, die in dieser Gruppe verfügbar sind. Wenn die Routing-Richtlinie eine manuelle Genehmigung erfordert, wird die Genehmigung von den Personen in der Genehmigungsgruppe angefordert.

Nächste Maßnahme

Die folgenden Knowledge Base-Artikel führen Sie durch den Prozess der Erstellung der erforderlichen Anmeldeinformationen und der Konfiguration von Weiterleitungsrichtlinien für verschiedene Zertifizierungsstellen:

Informationen zu DigiCert finden Sie unter [DigiCert] automatisierte Zertifikatverwaltung für TLS-Zertifikate konfigurieren [KB2166364] .

Informationen zu Entrust finden Sie unter [Entrust] automatisierte Zertifikatverwaltung für TLS-Zertifikate konfigurieren [KB2173533] .

Informationen zu „Let's Encrypt“ finden Sie unter [Verschlüsseln – ACME] automatisierte Zertifikatverwaltung für TLS-Zertifikate konfigurieren [KB2197962] .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu Microsoft CA finden Sie unter [Microsoft CA] automatisierte Zertifikatverwaltung für TLS-Zertifikate konfigurieren [KB2198094] .

Routing-Richtliniendetails

Weiterleitungsrichtlinien sind für die automatisierte Zertifikatverwaltung in TLS-Zertifikaten wichtig, da sie bestimmte Kriterien definieren, z. B. CA und Umgebung, um eine effiziente Verarbeitung verschiedener Szenarien während des Zertifikatlebenszyklus zu ermöglichen.

Es gibt drei verschiedene Szenarien zur Funktionsweise von Routing-Richtlinien für die automatisierten Zertifikatverwaltung für TLS-Zertifikate.

- Szenario 1: Eine einzelne Routing-Richtlinie stimmt überein, und eine manuelle Genehmigung ist erforderlich. Der Genehmiger kann die Aufgabendetails überprüfen und die Zertifikatanforderung genehmigen. Nach der Genehmigung wird der automatisierte Flow ausgelöst.
- Szenario 2: Keine Routing-Richtlinie stimmt überein ODER es sind mehrere Routing-Richtlinien vorhanden, die übereinstimmen. Der Genehmiger kann die Aufgabendetails überprüfen und „Weiterleitungsrichtlinie wählen und genehmigen“ auswählen. Der Genehmiger muss die Weiterleitungsrichtlinie manuell auswählen. Die aktualisierte Routing-Richtlinie wird dann angezeigt. Der Genehmiger wählt die Routing-Richtlinie aus, die dann den automatisierten Flow auslöst.
- Szenario 3: Eine einzelne Routing-Richtlinie stimmt überein, eine manuelle Genehmigung ist nicht erforderlich, und die Kennzeichnung „Genehmigung erforderlich“ ist inaktiv. Dadurch wird der automatische Flow ausgelöst.

Hinweis:

Wenn der Genehmiger die Zertifikatanforderungsaufgabe abgelehnt hat, wird die Aufgabe als „Fehlgeschlagen“ markiert. Eine einzige Genehmigung reicht aus, um den Fortschritt des automatisierten Flows auszulösen.

Neue Zertifikate mit der automatisierten Zertifikatverwaltung anfordern

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung mithilfe der automatisierten Zertifikatverwaltung automatisch ab. Zertifikatsbestand-Management Version 2.1.0 bietet Unterstützung für die Anforderung von Zertifikaten von DigiCert und Entrust CA Gateway. Version 2.3.2 unterstützt auch Microsoft CA.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und dass eine Weiterleitungsrichtlinie erstellt wird.

Nur für DigiCert: Sie müssen den API-Schlüssel aus DigiCert abrufen, dessen Domäne bereits von DigiCert validiert wurde. Wenn Sie eine Zertifikatanforderung mit einer neuen Domäne übermitteln, die nicht von DigiCert validiert wurde, wird die Anforderung als Ausstehend angezeigt, der automatisierte Flow kann die Zertifikatinformationen nicht abrufen, und die Anforderung wird als Fehlgeschlagen markiert.

Erforderliche Rolle: Anfordernde Person des Zertifikats, PKI-Administrator, PKI-Anwender oder Administrator

Zertifikatanforderer sind Benutzer, die nicht über die Rolle „PKI-Administrator“ oder „PKI-Benutzer“ verfügen.

Hinweis: Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**an.
2. Wählen Sie Aus **Neues Zertifikat anfordern: Automatisierter Flow** .
3. Geben Sie Details für die Pflichtfelder an: **CSR** Und **Gültigkeitszeitraum** .
4. Füllen Sie das Formular aus, oder wählen Sie zusätzliche Informationen aus, und klicken Sie dann auf **Übermitteln** Um mit der Bestellung fortzufahren.

   Die Tabelle „Routing-Richtlinie“ [sn_disco_certmgmt_routing_policy] hilft beim Abrufen der Routing-Richtlinien-ID für die Zertifizierungsstelle. Wenn keine einzelne Routing-Richtlinien-ID zurückgegeben wird, muss der Genehmiger die Routing-Richtlinie auswählen und die Aufgabe genehmigen. Weitere Informationen finden Sie unter Genehmigen Sie Zertifikataufgaben .

   Dadurch wird eine neue Zertifikataufgabe erstellt, die dann den automatisierten Flow auslöst. Wenn in der Routing-Richtlinie das Feld „Genehmigung erforderlich“ aktiviert wurde, muss die Aufgabe genehmigt werden, bevor der automatisierte Flow beginnt.

Ergebnis

- Sobald die Anforderung übermittelt wurde, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.

  Hinweis: PowerShell-Schritt wird für verwendet Microsoft CA. Dies erfordert das Plugin com.Glide.Hub.action_STEP.powershell.

- Ein Datensatz wird in der Tabelle „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] erstellt, sobald das Zertifikat erfolgreich abgerufen wurde.
- Alle 30 Minuten wird die regelmäßige Aufgabe „DigiCert – Status der Zertifikatbestellung verfolgen“ ausgeführt, und der Status wird überprüft.

  Hinweis: Es sind keine geplanten Aufgaben für Entrust CA Gateway und vorhanden Microsoft CA.

- Wenn das Zertifikat verfügbar ist, wird es an die Zertifikataufgabe angehängt.
- Die Zertifikataufgabe wird dann als „Abgeschlossen“ markiert und eine Change-Anforderung wird erstellt.
- Wenn mehrere Aufgaben für dieselbe CSR erstellt werden und „Allow Duplication“ (Duplizierung zulassen) in der Routing-Richtlinie nicht aktiviert ist, schlägt die Aufgabe fehl.
- Wenn der Gültigkeitszeitraum den Gültigkeitszeitraum der übereinstimmenden Routing-Richtlinie überschreitet, schlägt die Aufgabe fehl.

Generieren Sie automatisch eine Zertifikatsignierungsanforderung

Sie können eine Certificate Signing Request (CSR) für die Instanz generieren, indem Sie die erforderlichen Informationen im Katalogformular angeben.

Das manuelle Erstellen einer CSR kann ein umständlicher und fehleranfälliger Prozess sein. Die automatische CSR-Generierung kann auf aktiviert werden **Neues Zertifikat Anfordern** Und **Neues Zertifikat Anfordern (Automatisiert)** Formulare. Diese Funktion ist aus Sicherheitsgründen standardmäßig deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die automatische CSR-Generierung zu aktivieren, legen Sie die Systemeigenschaft fest **sn_Disco_certmgmt.enable_csr_Generation** Auf „wahr“. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Nach der Aktivierung wird ein **Möchten Sie CSR generieren?** Das Kontrollkästchen wird im Zertifikatanforderungsformular angezeigt. Wenn Sie das Kontrollkästchen aktivieren, können die erforderlichen Eingabefelder die CSR generieren. Geben Sie die erforderlichen Informationen an, und wählen Sie aus **Generieren** . Die Eingabedaten werden validiert, und die CSR wird entsprechend formatiert.

Die CSR wird in generiert **Zertifikatsignierungsanforderung (CSR)** Und ein privater Schlüssel wird in generiert **Privater Schlüssel** Feld. Wählen Sie aus **Herunterladen** Link zum Speichern des privaten Schlüssels zur späteren Verwendung. Standardmäßig beträgt die Größe des privaten Schlüssels 2048, kann jedoch mithilfe der Systemeigenschaft geändert werden **sn_Disco_certmgmt.private_key_size** . Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Bei Auswahl von **Übermitteln** , Das Formular enthält eine Warnung zum Herunterladen und Speichern des privaten Schlüssels. Aus Sicherheitsgründen speichert ServiceNow keine privaten Schlüssel. Daher muss der private Schlüssel gespeichert werden, bevor das Formular verlassen wird, andernfalls geht er verloren.

Zertifizierungsaufgaben genehmigen

Manchmal müssen Sie eine Zertifikataufgabe manuell genehmigen, um die Gültigkeit und Sicherheit von TLS-Zertifikaten sicherzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Genehmigung für eine Routing-Richtlinie angefordert wird, wählen Sie die erstellte Routing-Richtlinie aus. Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Meine Genehmigung**an.
2. Öffnen Sie die automatisch erstellte Genehmigungsaufgabe.
3. Überprüfen Sie die neuen Zertifikatdetails, und wählen Sie **Weiterleitungsrichtlinie wählen und genehmigen** aus.

Ergebnis

1. Der automatisierte Flow zum anfordern eines neuen Zertifikats wird initiiert.
2. Sie können die Zertifikataufgabe öffnen, indem Sie zu navigieren **Zertifikatverwaltung** > **Aufgabe „Neues Zertifikat“**an.
3. Stellen Sie sicher, dass der automatisierte Flow ausgelöst wird.
4. Wenn die ZERTIFIZIERUNGSSTELLE die Zertifikatanforderung genehmigt, werden sowohl die Auftrags-ID als auch die Zertifikat-ID für das neu angeforderte Zertifikat abgerufen. Wenn die CA nicht genehmigt, wird nur die Auftrags-ID abgerufen.

> **Hinweis:** Für Entrust CA Gateway werden die Zertifikatseriennummer und die Registrierungs-ID abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verlängern Sie ein Zertifikat mithilfe der automatisierten Zertifikatverwaltung

Fordern Sie die Erneuerung eines Zertifikats an und rufen Sie das Zertifikat für eine Anwendung automatisch ab. Dadurch werden sichere und unterbrechungsfreie Services verwaltet, während Sie die Gültigkeitsdauer des Zertifikats verlängern, wodurch potenzielle Serviceunterbrechungen aufgrund abgelaufener Zertifikate verhindert werden.

Vorbereitungen

Routing-Richtlinien für die automatisierte Zertifikatverwaltung einrichten Um sicherzustellen, dass der Zertifikatverwaltungskatalog aktiviert ist.

Um ein vorhandenes Zertifikat zu verlängern, stellen Sie sicher, dass die Erweiterungsdetails für das Zertifikat in der Tabelle [sn_Disco_certmgmt_certificate_Extension] ausgefüllt sind. Derzeit werden diese Details automatisch von ausgefüllt Discovery DigiCert-CA-Muster oder für alle Zertifikate, die über den automatisierten Flow erstellt wurden. Bei Entrust-Zertifikaten funktioniert dies jedoch nur, wenn Sie Neue Zertifikate mit der automatisierten Zertifikatverwaltung anfordern.

Erforderliche Rolle: PKI-Administrator, Administrator, Zertifikatbesitzer oder Benutzer, die Teil der Zertifikatbesitzer-Gruppe sind.

Die Zertifikatbesitzer- und Zertifikatbesitzergruppe enthält die Rolle „Zertifikatanforderer“ (minimale Rolle).

Hinweis: Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Um ein vorhandenes Zertifikat zu verlängern, fordern Sie ein neues Zertifikat mit denselben Details wie das ursprüngliche Zertifikat an. Derzeit ist keine Verlängerungs-API für Entrust CA Gateway und verfügbar Microsoft CA-Zertifikate. Während einer Verlängerungsanforderung wird intern ein neues Zertifikat mit denselben Attributen wie das ausgewählte Zertifikat generiert.

Für die Verlängerung eines vorhandenen Zertifikats ist eine CSR obligatorisch. Die anfordernde Person kann eine vorhandene CSR verwenden, falls verfügbar, oder eine neue CSR verwenden. Wenn Sie eine vorhandene CSR verwenden möchten, verwenden Sie dieselbe CSR, um ein neues Zertifikat von der CA anzufordern. Wenn Felder mit Tresor- und Java-APIs eingegeben werden, wird die CSR generiert.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**an.
2. Klicken Sie auf **Zertifikat verlängern – Automatisierter Flow**.
3. Geben Sie Details für die Pflichtfelder an: **CSR** Und **Gültigkeitszeitraum** .
4. Füllen Sie das Formular aus, oder wählen Sie zusätzliche Informationen aus, und klicken Sie dann auf **Übermitteln** Um mit der Bestellung fortzufahren.

Ergebnis

1. Die Tabelle „Weiterleitungsrichtlinie“ [sn_Disco_certmgmt_Routing_Policy] hilft beim Abrufen der ID DER CA-Weiterleitungsrichtlinie.
   - Wenn eine einzelne Weiterleitungsrichtlinie nicht übereinstimmt, muss der Genehmiger die CA auswählen und den Flow auslösen.
   - Wenn die CSR einen anderen Domänennamen als den ausgegebenen Zertifikatdomänennamen enthält, fordert die Aufgabe die Genehmigung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine einzelne Weiterleitungsrichtlinie übereinstimmt, aber in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] keine Informationen zum Verlängerungszertifikat verfügbar sind, erfordert die Aufgabe eine Genehmigung.
- Zertifikate können nicht verlängert werden, wenn die Details der Zertifizierungsstelle und der Auftrags-ID oder des Fingerabdrucks für das Zertifikat in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] fehlen. Erkennen Sie das Zertifikat über Abfrage der Zertifizierungsstelle Zum Ausfüllen der erforderlichen Details in der Zertifikaterweiterungstabelle. Wählen Sie nach Discovery die Routing-Richtlinie aus, und genehmigen Sie die Aufgabe.

2. Dadurch wird eine Aufgabe für das bestellte Zertifikat erstellt, die den Flow zum anfordern von Verlängerungszertifikaten auslöst.
3. Sobald die Anforderung übermittelt wurde, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.

   Hinweis: PowerShell-Schritt wird für verwendet Microsoft CA. Dies erfordert das Plugin com.Glide.Hub.action_STEP.powershell.

4. Die Auftrags-ID wird in der Tabelle „Zertifikataufgabe“ [sn_Disco_certmgmt_certificate_Task] und in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] gespeichert.

   Hinweis: Für Entrust CA Gateway werden die Zertifikatseriennummer und die Registrierungs-ID abgerufen. Die Seriennummer wird in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] gespeichert.

5. Alle 30 Minuten wird die geplante Aufgabe „DigiCert – Status der Zertifikatbestellung verfolgen“ ausgeführt und der Status wird überprüft.

Hinweis:

Das System ruft Details zum ausgewählten Zertifikat aus der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] ab und stellt die Anforderung an die CA, das Zertifikat zu verlängern. Zertifikate können nicht verlängert werden, wenn die Zertifizierungsstelle, die Auftrags-ID oder der Fingerabdruck in dieser Tabelle fehlen. Wenn zusätzliche Details zum verlängern des Zertifikats fehlen, protokolliert das System eine Nachricht und schlägt vor, was zu tun ist. In diesem Fall müssen Sie die Erkennung für das Zertifikat mithilfe der CA-basierten Erkennung durchführen. Weitere Informationen finden Sie unter Führen Sie die Zertifikat-Discovery über die Abfrage der Zertifizierungsstelle aus Um diese Details in die Zertifikaterweiterungstabelle auszufüllen.

Widerrufen Sie ein Zertifikat mithilfe der automatisierten Zertifikatverwaltung

Widerrufen Sie das Zertifikat für eine Anwendung. Für den Widerruf ist keine Genehmigung erforderlich, wenn `order Id`Und `certificate Id`Sind in der Zertifikaterweiterungstabelle vorhanden. Wenn `order Id`Und `certificate Id`Sind in der Zertifikaterweiterungstabelle nicht vorhanden, benötigen Sie eine Genehmigung.

Vorbereitungen

Routing-Richtlinien für die automatisierte Zertifikatverwaltung einrichten Um sicherzustellen, dass der Zertifikatverwaltungskatalog aktiviert ist.

Um ein vorhandenes Zertifikat zu widerrufen, stellen Sie sicher, dass die Erweiterungsdetails für das Zertifikat in der Tabelle [sn_Disco_certmgmt_certificate_Extension] ausgefüllt sind. Sie müssen keine Endpunkt-URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angeben. Das System codiert die Widerrufs-URLs für die Discovery automatisch. Derzeit werden diese Details automatisch von ausgefüllt Discovery DigiCert-CA-Muster oder für alle Zertifikate, die über den automatisierten Flow erstellt wurden. Bei Entrust-Zertifikaten funktioniert dies jedoch nur, wenn Sie Neue Zertifikate mit der automatisierten Zertifikatverwaltung anfordern.

Erforderliche Rolle: pki_admin oder admin

Hinweis: Derzeit werden Genehmigungen nur in der Erfüller-Genehmigungs-Experience unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**an.
2. Wählen Sie Aus **Zertifikat widerrufen: Automatisierter Flow** .
3. Fügen Sie das ausgestellte Zertifikat ein, das Sie widerrufen möchten (z. B. www.undefined.com). Mehrere Zertifikate können zum Widerrufen ausgewählt werden.
4. Geben Sie einen ausreichenden Grund für den Widerruf des Zertifikats an.
   Für Microsoft CA der Grund muss eine Ganzzahl sein. Wenn ein anderer Wert angegeben wird, wird der Standardwert 0 verwendet, was bedeutet, dass nicht angegeben ist.
5. Wählen Sie aus, um den Widerrufsauftrag aufzugeben **Übermitteln** .
6. Wählen Sie im Bestätigungs-Popup die Option aus **OK** .

Ergebnis

1. Wenn Sie einen Widerruf anfordern, wird automatisch eine Aufgabe wird erstellt.
   - Wenn *`order Id`*Und *`certificate Id`*Sind in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] vorhanden, für den Widerruf ist keine Genehmigung erforderlich.
   - Wenn *`order Id`*Und *`certificate Id`*Sind in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] nicht vorhanden, fordert die Aufgabe die Genehmigung an.
   - Wenn die Seriennummer für das Entrust CA-Gateway in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] nicht vorhanden ist, fordert die Aufgabe die Genehmigung an.
2. Sobald das PKI-Team die Genehmigung erteilt hat, erfolgt die Zuordnung zwischen dem Zertifikat und der Zertifizierungsstelle basierend auf der ausgewählten Routing-Richtlinie.
3. Dadurch wird der Widerrufvorgang für die ausgewählte Zertifizierungsstelle ausgelöst, die die Zertifizierungsstellen-APIs verwendet.
4. Details werden in der Zertifikaterweiterungstabelle gespeichert.
5. Alle 30 Minuten wird die regelmäßige Aufgabe „DigiCert – Status der Zertifikatbestellung verfolgen“ ausgeführt, und der Status wird überprüft.

   Hinweis: Es sind keine geplanten Aufgaben für Entrust CA Gateway und vorhanden Microsoft CA.

6. Der Status des Zertifikats wird als widerrufen markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Zertifikate können nicht widerrufen werden, wenn Details zur Zertifizierungsstelle oder Zertifikat-ID in der Tabelle „Zertifikaterweiterung“ [sn_Disco_certmgmt_certificate_Extension] fehlen. Für Entrust CA-Gateway können Zertifikate nicht widerrufen werden, wenn die Seriennummer fehlt. Erkennen Sie das Zertifikat über Abfrage der Zertifizierungsstelle Zum Ausfüllen der erforderlichen Details in der Zertifikaterweiterungstabelle. Anschließend wählt Discovery die Routing-Richtlinie aus und genehmigen die Aufgabe.

Widerrufen Sie die Anforderung der Zertifikat-API. Wenn „Skip_Approval“ auf „wahr“ festgelegt ist, wird der Widerrufsprozess schneller abgeschlossen. Wenn „skip_approval“ auf „false“ festgelegt ist, wird der Widerrufsprozess abgeschlossen, sobald der DigiCert- oder Entrust CA Gateway-Administrator die Anforderung zum Widerrufen genehmigt oder abgelehnt hat. Um den Genehmigungsschritt zu überspringen, muss der API-Schlüssel über Administratorrechte verfügen.

Zertifikatintegrationen und -benachrichtigungen

Ab Version 1.2.0 Zertifikatsbestand-Management Nahtlose Integration mit Ereignismanagement, Bietet eine einheitliche Lösung für optimierte Vorgänge. Diese Integration ermöglicht die Generierung von Ereignissen und Benachrichtigungen mit der zusätzlichen Fähigkeit, Warnungen an Slack zu senden, und verbessert so die Kommunikations- und Warnungsmechanismen innerhalb von Zertifikatsbestand-Management System.

Ereignismanagement mit Zertifikatsbestand-Management integrieren

In Zertifikatsbestand-Management Version 1.2.0 und höher, Ereignismanagement Kann Ereignisse und Warnungen für ablaufende und abgelaufene Zertifikate erstellen, wodurch die Überwachungsfunktionen des Systems verbessert werden.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Store-Anwendung ist installiert.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die -Integration nutzt Flow Designer Funktion zum Initiieren von Ereignissen. Es wird täglich eine bereits vorhandene verwendet Discovery Zeitplan zur Identifizierung abgelaufener oder ablaufender Zertifikate, wodurch ein Subflow aktiviert wird. Bei der Subflow-Aktivierung wird die Installation von überprüft Ereignismanagement Store-Anwendung. Wenn die Anwendung installiert ist, generiert der Subflow ein Ereignis für ablaufende oder abgelaufene Zertifikate.

Prozedur

1. Um alle generierten Warnungen oder Ereignisse anzuzeigen, navigieren Sie zu **Alle** > **Ereignismanagement** > **Alle Warnungen** oder **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
2. Um bestimmte Zertifikatereignisse auszuschließen und Warnungsauslöser zu verhindern, navigieren Sie zu **Ereignismanagement** > **Bedingungen** > **Ereignisregeln** Und führen Sie die folgenden Schritte aus.
   a. Wählen Sie aus **Zertifikat Abgelaufen/Ablaufende Ereignisse** Regel.
   b. Wählen Sie aus **Ereignisfilter** Registerkarte.
   c. Wählen Sie **Events ignorieren, die diesem Filter entsprechen** aus.
   d. Fügen Sie nach Bedarf weitere erforderliche Details hinzu.
   e. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatbenachrichtigungen in Slack erhalten

In Version 1.2.0 von Zertifikatsbestand-Management, Einrichten Slack Benachrichtigungen, um über ablaufende und abgelaufene Zertifikate auf dem Laufenden zu bleiben. Erhalten Sie detaillierte Warnungen mit praktischen URL-Links, um zusätzliche Informationen zu erhalten.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Eine geplante Aufgabe in Zertifikatsbestand-ManagementÜberprüft regelmäßig die Ablaufdaten von Zertifikaten, die im Feld „valid_to“ der Tabelle „cmdb_ci_certificate“ gespeichert sind. Wenn Zertifikate abgelaufen sind oder kurz vor dem Ablauf stehen, initiiert der Auftrag den Subflow Process Slack Message, der anschließend Benachrichtigungen an den angegebenen sendet Slack Kanal.

Prozedur

1. Richten Sie die Slack-Spoke ein .
2. Erstellen Sie einen Slack-Bot , und fügen Sie ihn einem Slack-Kanal hinzu.
3. Konfigurieren Sie Standard-Slack-Anmeldeinformationen .
4. Konfigurieren Sie anwenderdefinierte Slack-Anmeldeinformationen .

   Wenn Ihr Slack Spoke-Version ist 1,2.0. Sie können den nächsten Schritt zum Abrufen der Kanal-ID umgehen.

5. Rufen Sie die ID für ab Slack Kanal.
   a. Wechseln Sie zu **Slack**.
   b. Klicken Sie mit der rechten Maustaste auf den Kanal.
   c. Auswahlvorgang **Weitere Optionen** > **Link kopieren**an.
   d. Kopieren Sie über den bereitgestellten Link die Zeichenfolge nach <archive/>.
6. Konfigurieren Sie Slack Kanal-ID-Eigenschaft.
   a. Navigieren zu **Discovery** > **Eigenschaften**an.
   b. Geben Sie einen Wert in ein Slack Kanal-ID-Eigenschaft `glide.discovery.certs.slack_channel_id`.
7. Wählen Sie **Speichern**.

Ergebnis
Benachrichtigungen werden an weitergeleitet Slack Kanal in angegeben Discovery Eigenschaften. Wenn einem Anwender ein Zertifikat zugewiesen ist und seine konfigurierte E-Mail-Adresse mit übereinstimmt Slack E-Mail, wird der Anwender in getaggt Slack Nachricht. Die Slack Die geplante Aufgabe wird wöchentlich ausgeführt, und Sie können ihre Häufigkeit anpassen, indem Sie die Einstellungen für die geplante Aufgabe „Zertifikatbenachrichtigung“ ändern.

Zertifikatgenerierung über die Zertifizierung-Manager-Integration

Fordern Sie ein Zertifikat über an Kubernetes cert-Manager mit ServiceNow Externer Aussteller (sn-externer Aussteller) und speichern Sie das Zertifikat und die zugehörigen Informationen sicher im Kubernetes Cluster als Geheimnis. In Kubernetes, Ein Geheimnis ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein Objekt, mit dem Sie vertrauliche Informationen wie Passwörter, API-Schlüssel und Zertifikate speichern und verwalten können.

Informationen zum Erstellen eines externen Ausstellers finden Sie unter Erstellen und Bereitstellen eines externen Ausstellers für die Zertifikatverwaltung [KB1435392] .

Bereitstellungsanforderungen

- Stellen Sie den Zertifizierungsmanager in bereit Kubernetes Umgebung. Aktualisieren **manager.yaml** Mit Instanz-URL, Zertifikatbesitzergruppe, Zertifikatbesitzer, Umgebung und Verlängerungsnachverfolgung.
- Stellen Sie bereit ServiceNow Externer Aussteller (sn-external-issuer) in Ihrem Kubernetes Umgebung. Erstellen Sie einen Kubernetes Geheimnis *`clusterissuer-servicenow-credentials`*Mit Anwendername und Passwort der Instanz, um sicherzustellen, dass der Anwender über die erforderlichen Rollen verfügt, um ein Zertifikat anzufordern.

ServiceNow Externer Aussteller (sn-externer Aussteller)

- Externe Aussteller erweitern die Zertifikatmanager-Funktionalität, um Zertifikate über nicht-Core-APIs und -Services auszustellen.
- Die ServiceNow Externer Aussteller ist eine ServiceNow-spezifische Implementierung eines externen Ausstellers.
- Wenn eine neue Zertifikataufgabe erstellt wird, werden ihre Zertifikatanforderungs-UID und die Zertifikataufgaben-SYS-ID im lokalen JSON-Cache und die Tabelle „Zertifikatanforderungs-UID zu Aufgabenzuordnung“ in der Instanz gespeichert.
- Die ServiceNow Externer Aussteller fragt die Instanz ab, um den Status der Zertifikataufgabe zu überwachen.
- Wenn sich die Zertifikataufgabe in befindet **In Arbeit** status, seine Zertifikatanforderungs-UID und die SYS-ID der Zertifikataufgabe werden der Tabelle „UID-Zuordnung externer Aussteller“ in der Instanz und dem lokalen JSON-Cache hinzugefügt. Während dieser Zeit versucht der Zertifizierungsmanager automatisch, das Zertifikat anzufordern.
- Nach Erhalt einer Zertifikatanforderung sucht der Zertifizierungsmanager im lokalen JSON-Cache nach einer übereinstimmenden Aufgabe. Wenn gefunden, wird dieselbe Aufgabe abgefragt. Andernfalls fragt sie die Instanz nach Datensätzen aus der Tabelle „UID-Zuordnung des externen Ausstellers“ ab und füllt den lokalen JSON-Cache aus.
- Sobald die Aufgabe als abgeschlossen markiert wurde und das Zertifikat generiert wurde, wird der ServiceNow Der externe Aussteller sendet eine weitere Anforderung an die Instanz, lädt den Zertifikatanhang herunter und aktualisiert die Zertifikatressource und das entsprechende Geheimnis in Kubernetes.

Bereitstellung des externen Ausstellers von ServiceNow in Kubernetes

Bereitstellung des externen Ausstellers von ServiceNow in Kubernetes Umfasst die folgenden Schritte:

1. Rufen Sie auf der Downloadseite der ServiceNow-Instanz das Helm Chart oder das YAML-ZIP-Paket ab.
2. Passen Sie an manager.yaml Oder Werte.yaml Dateien nach Bedarf für Ihren spezifischen Anwendungsfall. Diese Dateien können wichtige Informationen wie die Instanz-URL und die Zertifikatbesitzergruppe enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie einen Kubernetes Geheimer Name `Clusteraussteller-servicenow-Anmeldeinformationen` Mit Anwendername und Passwort der Instanz.

   Beispielbefehl:

   - Erstellen Sie einen Kubernetes Geheimer Name `Clusteraussteller-servicenow-Anmeldeinformationen` Mit Anwendername und Passwort der Instanz. Beispielbefehl:

     ```
     kubectl create secret generic clusterissuer-servicenow-credentials
              --from-literal=user=<user_name> --from-literal=password=<password> -n
             system
     ```

   - Stellen Sie sicher, dass der Anwender über die erforderlichen Rollen verfügt, um Zertifikate anzufordern.

4. Führen Sie die folgenden Befehle für die Bereitstellung aus.

   ```
   kubectl create ns system
   kubectl apply -f crd
   kubectl apply -f rbac
   kubectl apply -f issuers
   kubectl apply -f manager/manager.yaml
   ```

5. (Optional) Passen Sie zusätzliche Konfigurationen in den Dateien an Ihre spezifischen Anforderungen an.
6. Stellen Sie sicher, dass die Bereitstellung erfolgreich ist und der externe ServiceNow-Aussteller hochgefahren ist und ausgeführt wird.

Flow „Neues Zertifikat anfordern“

Übermitteln Sie nach der Bereitstellung eine Zertifikatressource mit den folgenden Informationen in einer Datei mit dem Namen `Certificate_clusterissuer.yaml` .

- IssuerRef: Clusteraussteller-servicenow
- Aussteller: Aussteller-servicenow
- Art: ClusterIssuer
- IssuerRef: servicenow-issuer.servicenow.com

Hier ist eine Beispiel-Zertifikatressource:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
name: certificate-by-clusterissuer
spec:
commonName: certificate-by-clusterissuer.servicenow.com
secretName: certificate-by-clusterissuer
dnsNames:
- servicenow.com
- foo.servicenow.com
issuerRef:
name: clusterissuer-servicenow
group: servicenow-issuer.servicenow.com
kind: ClusterIssuer
```

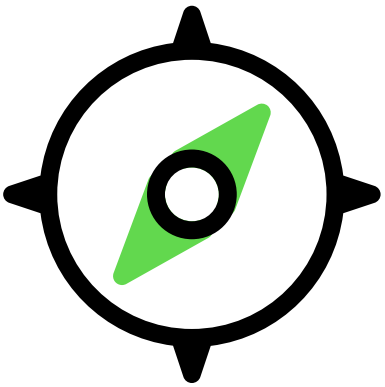
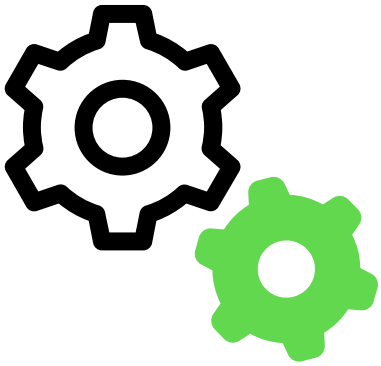
Wenden Sie die Zertifikatressource mit an `Kubectl Apply -f certificate_clusterissuer.yaml`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisierte Zertifikatverwaltungsumgebung

Automated Certificate Management Environment (ACME) ist ein Protokoll zur Automatisierung der Verwaltung von SSL-/TLS-Zertifikaten.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über ACME und seine Vorteile.	Einrichtung Und konfigurieren Sie ACME.	Verwenden Sie ACME, um die Interaktion zwischen einem zu automatisieren Zertifizierungsstelle Und einem Server.

ACME erkunden

Die Automated Certificate Management Environment (ACME) ist ein Kommunikationsprotokoll, das die Interaktion zwischen einer Zertifizierungsstelle (Certificate Authority, CA) und einem Server automatisiert. Sie optimiert die Prozesse zum anfordern, verlängern und Widerrufen von SSL-/TLS-Zertifikaten.

ACME Übersicht

ACME verwendet JSON-formatierte Nachrichten, die über eine sichere HTTPS-Verbindung übertragen werden. Diese Kommunikation ermöglicht die automatisierte Verwaltung des Lebenszyklus von Zertifikaten, wodurch manuelle Eingriffe und das Fehlerrisiko reduziert werden.

ACME ist ein weit verbreiteter Standard, der von Administratoren öffentlicher Schlüsselinfrastruktur, Geschäftsbereichsbesitzern, Zertifikatverwaltungsanwendern, Administratoren, Account-Besitzern und Teammanagern verwendet wird.

ACME Vorteile

Beim anfordern, verlängern oder Widerrufen von SSL-/TLS-Zertifikaten bietet ACME erhebliche Vorteile:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Es automatisiert Aufgaben im Zusammenhang mit der Zertifikatverwaltung und reduziert den Verwaltungsaufwand für IT-Teams.
- Es hilft, sicherzustellen, dass die Zertifikate gültig und aktuell sind.
- Manuelle Zertifikatverwaltungsaufgaben entfallen, wodurch die Gesamtkosten gesenkt werden.

ACME wird konfiguriert

Durch die Konfiguration der Automated Certificate Management Environment (ACME) können Sie SSL/TLS-Zertifikate automatisch für Webserver konfigurieren, wodurch die Sicherheit verbessert und die Verwaltung vereinfacht wird.

Erstellen Sie die Anmeldeinformationen für die ACME-Zertifizierungsstelle

Erstellen Sie ACME-Anmeldeinformationen auf der Website oder API der ACME-Zertifizierungsstelle. Die Anmeldeinformationen werden von Ihrer ACME-Client-Software verwendet, um mit der ACME Certificate Authority (CA) zu interagieren, um Zertifikate anzufordern, zu verlängern oder zu widerrufen.

Vorbereitungen

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Auf der **Welche Art von Anmeldeinformationen möchten Sie erstellen?** Seite auswählen **Zertifikatmanagement-Anmeldeinformationen** .
4. Füllen Sie im Formular die Felder aus.

Formular für Anmeldeinformationen für Zertifikatverwaltung

Feld	Beschreibung
Name	Name für die Anmeldeinformation
Anmeldeinformationsalias	Anmeldeinformationsalias, der mit den ANMELDEINFORMATIONEN DER CA verknüpft ist.
CA-Typ	Typ der Zertifizierungsstelle (z. B. Verschlüsseln oder Entrust).
ACME	Option zum Aktivieren des ACME-Flows für den Entrust CA-Typ. **Hinweis:** Für den CA-Typ **Verschlüsseln wir** , Diese Option ist standardmäßig ausgewählt.
Privater Schlüssel	Erstellen Sie einen privaten Schlüssel, oder generieren Sie einen Account mit Let's Encrypt oder Entrust. Geben Sie einen privaten Schlüssel mit dem Schlüsseltyp RSA oder ECDSA an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie RSA verwenden, müssen Sie Kryptografiestandards für öffentliche Schlüssel im PKCS#1-Format verwenden. OpenSSL erstellt das PKCS#1-Format mit dem folgenden Befehl: `openssl-Genrsa: Traditionell`
Schlüsseltyp	Verschlüsselungsalgorithmus für den privaten Schlüssel (z. B. RSA oder ECDSA).
Schlüssel-ID	Wird für die Accountbindung verwendet und von der CA bereitgestellt. **Hinweis:** Gilt für CA-Typ **Vertrauen** .
MAC-Schlüssel	Wird für die Accountbindung verwendet und von der CA bereitgestellt. **Hinweis:** Gilt für CA-Typ **Vertrauen** .

5. Wählen Sie **Aktualisieren**.

Richten Sie die Weiterleitungsrichtlinie für ACME ein

Richten Sie eine Weiterleitungsrichtlinie ein, um eine Automated Certificate Management Environment (ACME) einzurichten. Dazu gehört die Erstellung einer Richtlinie basierend auf Faktoren wie Zertifizierungsstelle (CA), Umgebung und anderen Funktionen, um eine effiziente SSL/TLS-Zertifikatverwaltung sicherzustellen.

Vorbereitungen
Erforderliche Rolle: pki_admin, Flow_Designer, action_Designer oder admin

Warum und wann dieser Vorgang ausgeführt wird
Doppelte Zertifikatanforderungen sind nicht zulässig. Sie können diese Einstellung jedoch überschreiben, indem Sie das Kontrollkästchen „Allow duplicate requests“ (Duplizierte Anforderungen zulassen) aktivieren. Eine Zertifikatanforderung gilt als Duplikat, wenn noch eine andere Zertifikataufgabe mit demselben Domänennamen ausgeführt wird.

Die Routing-Richtlinie entscheidet, welche Zertifizierungsstelle für Zertifikatvorgänge kontaktiert werden muss. Sie enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR. Die Routing-Richtlinie löst den Flow zum Anfordern von Zertifikaten für bestimmte Zertifizierungsstellen aus.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**an.
2. Wählen Sie **Neu**.
3. Auf der **Richtlinie Für Zertifikatweiterleitung** Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Beschreibung der Feldwerte finden Sie unter Formular „Zertifikatweiterleitungsrichtlinie“.

4. Wählen Sie **Aktualisieren**.

Formular „Zertifikatweiterleitungsrichtlinie“

Füllen Sie das Formular „Zertifikatweiterleitungsrichtlinie“ aus, um die Weiterleitungsrichtlinie für ACME einzurichten.

Richtlinie für Zertifikatweiterleitung

Feld	Beschreibung
Name	Name der Weiterleitungsrichtlinie.
Zertifizierungsstelle	CA, die zum Erstellen eines neuen Zertifikats oder zum verlängern oder Widerrufen von Zertifikaten verwendet wird. Basierend auf Ihren Anmeldeinformationen werden folgende CAS unterstützt: • Verschlüsseln wir • Entrust
Zuweisungsgruppe	Gruppe, der eine manuelle Zertifikataufgabe zugewiesen ist.
DNS-Abfrageaktion	Flow Designer-Option zum automatischen Lösen von DNS-Herausforderungen (z. B. Basisskript – **ACME-DNS-Herausforderung: GoDaddy**). **Hinweis:** Sie können auch eine neue Aktion erstellen, die dem Basisskript ähnlich ist, um andere DNS-Anbieter zu unterstützen. Die Rolle „Flow_Designer“ oder „action_Designer“ ist für diese Aktion erforderlich. Wenn **Keine** Ist ausgewählt, werden die Zertifikate neu oder verlängert mithilfe des manuellen ACME-Flows der DNS-Herausforderung.
Anmeldeinformationsalias	Anmeldeinformationsalias, der mit den ANMELDEINFORMATIONEN DER CA verknüpft ist.
Zweck des Zertifikats	Gibt an, ob die Zertifikatanforderung für einen internen oder externen Zweck bestimmt ist.
Aufgabengenehmigungsgruppe	Gruppe, der die Aufgabengenehmigung zugewiesen ist.
DNS-Aufgabenzuweisungsgruppe	Gruppe, der die DNS-Herausforderung für diese Aufgabe zugewiesen ist.
MID-Server	MID-Server für Zertifikataktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Zertifikatweiterleitung (Fortsetzung)

Feld	Beschreibung
Hinweis: Die **Organisation**, **Organisationseinheit**, **Ort**, **Status**, **Land**, Und **E-Mail-Adresse** Felder akzeptieren kommagetrennte Werte. Die **Allgemeiner Antragstellername** Und **Alternativer Antragstellername** Felder enthalten reguläre Ausdrücke. Das Format des regulären Ausdrucks weist die folgenden Einschränkungen auf: • Darf keine Kommas enthalten. • Darf nicht mit einem Schrägstrich (/) beginnen oder enden.	

Mit ACME

Verwenden Sie die Automated Certificate Management Environment (ACME), um SSL/TLS-Zertifikate anzufordern, zu verlängern oder zu widerrufen.

ACME bietet zwei Optionen:

- Manueller ACME-Flow der DNS-Herausforderung

  Der Anwender, der die DNS-Herausforderungen selbst ausführt.

- Automatisierter ACME-Flow der DNS-Herausforderung

  Die in der Weiterleitungsrichtlinie ausgewählte DNS-Abfrageaktion fügt den DNS-Abfragedatensatz automatisch den DNS-Datensätzen der Domäne hinzu.

Führen Sie die folgenden Aufgaben aus, um mit der Verwendung von ACME zu beginnen:

- Fordern Sie ein neues Zertifikat mit dem manuellen ACME-Flow der DNS-Herausforderung an
- Fordern Sie ein neues Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage an
- Verlängern Sie das Zertifikat mit dem manuellen ACME-Flow der DNS-Herausforderung
- Verlängern Sie das Zertifikat mit dem automatisierten ACME-Flow der DNS-Herausforderung
- Widerrufen Sie das Zertifikat mit dem automatisierten ACME-Flow

Fordern Sie ein neues Zertifikat mit dem manuellen ACME-Flow der DNS-Herausforderung an

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung mithilfe des manuellen ACME-Flows der DNS-Challenge automatisch ab.

Vorbereitungen

- Der Zertifikatverwaltungskatalog muss aktiviert sein.
- Eine Weiterleitungsrichtlinie ohne DNS-Abfrageaktion muss vorhanden sein.

Erforderliche Rolle: Anfordernde Person des Zertifikats, PKI-Administrator, PKI-Anwender oder Administrator

Hinweis:

Die anfordernde Person des Zertifikats ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf den automatisierten Flow der Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**an.
   b. Wählen Sie Aus **Zertifikatverwaltung** .
   c. Wählen Sie Aus **Automatisierter Flow** .
2. Wählen Sie Aus **Neues Zertifikat Anfordern (Automatisiert)** .
3. Füllen Sie im Formular die Felder aus.

Neues Zertifikat

Feld	Beschreibung
Zweck des Zertifikats	Gibt an, ob die Anforderung für ein internes oder externes Zertifikat gilt. Wählen Sie für CAS (z. B. Let's Encrypt) die Option aus **Extern** .
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	CSR mit den Zertifikatinformationen.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist. Für Let's Encrypt beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Eigentümer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen aus CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe erstellt und eine Aktivität zugewiesen, damit Sie die DNS-Herausforderung abschließen und als abgeschlossen markieren können.
5. Auf der **Neue Zertifikataufgabe** Seite, in **DNS-Aufgabe** Feld den Datensatz auswählen.
6. Auf der **DNS-Aufgabe** Fügen Sie einen DNS-TXT-Datensatz für die angehängte DNS-Herausforderung hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. In **DNS-Herausforderungen** Kopieren Sie den DNS-Wert.

b. Wechseln Sie im Webbrowser zur Domäne, und fügen Sie den DNS-Wert als TXT-Datensatz hinzu. Beispielsweise kann die Domäne sein **godaddy.com** > **thedisconow.com**an.

c. Füllen Sie die anderen Pflichtfelder aus.

d. Wählen Sie **Speichern**.

Hinweis: Die meisten DNS-Updates werden innerhalb einer Stunde wirksam, die Aktualisierung kann jedoch bis zu 48 Stunden dauern.

7. Auf der **DNS-Aufgabe** Ändern Sie den Status des Datensatzes in **Abgeschlossen** .
8. **Wahlweise:** Überprüfen Sie, ob der DNS-Datensatz erfolgreich propagiert wurde.
   Um zu überprüfen, ob sie erfolgreich propagiert wurde, verwenden Sie `Graben` Befehl.
9. Wählen Sie **Speichern**.

Ergebnis

- Sobald die DNS-Herausforderung abgeschlossen ist, stellt der automatisierte Flow die Anforderung an die ZERTIFIZIERUNGSSTELLE, das Zertifikat abzurufen.
- Das Zertifikat wird an die Aufgabe „Neues Zertifikat“ angehängt.
- Der Status der Zertifikataufgabe ändert sich in Abgeschlossen.

Fordern Sie ein neues Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage an

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung mithilfe eines automatisierten ACME-Flows (Automated Certificate Management Environment) der DNS-Abfrage automatisch ab.

Vorbereitungen

Stellen Sie sicher, dass Anmeldeinformationen eingerichtet wurden.

Hinweis: Die GoDaddy-Anmeldeinformationen werden im Basissystem auf der Anmeldeinformationsseite bereitgestellt.

Der Zertifikatverwaltungskatalog wurde aktiviert.

Eine Weiterleitungsrichtlinie mit einer DNS-Abfrageaktion ist vorhanden.

Erforderliche Rolle: Anfordernde Person des Zertifikats, PKI-Administrator, PKI-Anwender, Flow_Designer, action_Designer, oder -Administrator

Hinweis:

Eine Zertifikatanfordernde Person ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf den automatisierten Flow zu.
   a. Navigieren zu **Alle** > **Servicekatalog**an.
   b. Wählen Sie Aus **Zertifikatverwaltung** .
   c. Wählen Sie Aus **Automatisierter Flow** .
2. Wählen Sie Aus **Neues Zertifikat Anfordern (Automatisiert)** .
3. Füllen Sie im Formular die Felder aus.

Formular „Neues Zertifikat“

Feld	Beschreibung
Zweck des Zertifikats	Gibt an, ob die Anforderung für ein internes oder externes Zertifikat gilt. Wählen Sie für CAS wie Let's Encrypt aus **Extern** .
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	CSR mit Zertifikatinformationen.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist. Für Let's Encrypt beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Eigentümer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen aus CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe zum Abschließen der DNS-Herausforderung erstellt. Die Aufgabe wird automatisch abgeschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

- Sobald die DNS-Datensatzverbreitung nach zwei Minuten abgeschlossen ist, wird die DNS-Abfrage automatisch abgeschlossen, und der automatisierte Flow sendet eine Anforderung an die ZERTIFIZIERUNGSSTELLE, um das Zertifikat abzurufen.

  Administratoren können diese Dauer ändern, indem sie ändern *sn_disco_certmgmt.wait_time_for_dns_record_propagation*Systemeigenschaft.

- Das Zertifikat wird an die Aufgabe „Neues Zertifikat“ angehängt.
- Der Status der Aufgabe „Zertifikat anfordern“ ändert sich in „Abgeschlossen“.

Verlängern Sie das Zertifikat mit dem manuellen ACME-Flow der DNS-Herausforderung

Anforderung zur Verlängerung des Zertifikats und zum automatischen Abrufen der Zertifikate für eine Anwendung mithilfe des manuellen ACME-Flows der DNS-Herausforderung.

Vorbereitungen

- Der Zertifikatverwaltungskatalog muss aktiviert sein.
- Eine Weiterleitungsrichtlinie ohne DNS-Abfrageaktion muss vorhanden sein.

Erforderliche Rolle: Anfordernde Person des Zertifikats, PKI-Administrator, PKI-Anwender oder Administrator

Hinweis:

Die anfordernde Person des Zertifikats ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

Prozedur

1. Greifen Sie auf den automatisierten Flow der Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**an.
   b. Wählen Sie Aus **Zertifikatverwaltung** .
   c. Wählen Sie Aus **Automatisierter Flow** .
2. Wählen Sie Aus **Zertifikat Verlängern (Automatisiert)** .
3. Füllen Sie im Formular die Felder aus.

Zertifikat verlängern

Feld	Beschreibung
Ausgestelltes Zertifikat	Zu verlängerndes Zertifikat.
Zweck des Zertifikats	Fordern Sie ein internes oder externes Zertifikat an. Wählen Sie für CAS (z. B. Let's Encrypt) die Option aus **Extern** .
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	CSR mit Zertifikatinformationen.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Für Let's Encrypt beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Eigentümer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen aus CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe erstellt und eine Aktivität zugewiesen, damit Sie die DNS-Herausforderung abschließen und als abgeschlossen markieren können.
5. Auf der **Neue Zertifikataufgabe** Seite, in **DNS-Aufgabe** Feld den Datensatz auswählen.
6. Auf der **DNS-Aufgabe** Fügen Sie einen DNS-TXT-Datensatz für die angehängte DNS-Herausforderung hinzu.

   a. In **DNS-Herausforderungen** Kopieren Sie den DNS-Wert.

   b. Wechseln Sie im Webbrowser zur Domäne, und fügen Sie den DNS-Wert als TXT-Datensatz hinzu. Beispielsweise kann die Domäne sein **godaddy.com** > **thedisconow.com**an.

   c. Füllen Sie die anderen Pflichtfelder aus.

   d. Wählen Sie **Speichern**.

   Hinweis: Die meisten DNS-Updates werden innerhalb einer Stunde wirksam, die Aktualisierung kann jedoch bis zu 48 Stunden dauern.

7. Auf der **DNS-Aufgabe** Ändern Sie den Status des Datensatzes in **Abgeschlossen** .
8. **Wahlweise:** Überprüfen Sie, ob der DNS-Datensatz erfolgreich propagiert wurde.
   Um zu überprüfen, ob sie erfolgreich propagiert wurde, verwenden Sie `Graben` Befehl.
9. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

- Sobald die DNS-Herausforderung abgeschlossen ist, stellt der automatisierte Flow die Anforderung an die ZERTIFIZIERUNGSSTELLE, das Zertifikat abzurufen.
- Das Zertifikat wird an die Aufgabe „Neues Zertifikat“ angehängt.
- Der Status der Zertifikataufgabe ändert sich in Abgeschlossen.

Verlängern Sie das Zertifikat mit dem automatisierten ACME-Flow der DNS-Herausforderung

Anforderung zur Verlängerung des Zertifikats und zum automatischen Abrufen der Zertifikate für eine Anwendung mithilfe eines automatisierten Flows der DNS-Abfrage (Automated Certificate Management Environment, ACME).

Vorbereitungen

Stellen Sie sicher, dass Anmeldeinformationen eingerichtet wurden.

Hinweis: Die GoDaddy-Anmeldeinformationen werden im Basissystem auf der Anmeldeinformationsseite bereitgestellt.

Der Zertifikatverwaltungskatalog wurde aktiviert.

Eine Weiterleitungsrichtlinie mit einer DNS-Abfrageaktion ist vorhanden.

Erforderliche Rolle: Anfordernde Person des Zertifikats, PKI-Administrator, PKI-Anwender, Flow_Designer, action_Designer, oder -Administrator

Hinweis:

Eine Zertifikatanfordernde Person ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

Prozedur

1. Greifen Sie auf den automatisierten Flow „Zertifikatverlängerung“ zu.
   a. Navigieren zu **Alle** > **Servicekatalog**an.
   b. Wählen Sie Aus **Zertifikatverwaltung** .
   c. Wählen Sie Aus **Automatisierter Flow** .
2. Wählen Sie Aus **Zertifikat Verlängern (Automatisiert)** .
3. Füllen Sie im Formular die Felder aus.

Zertifikat verlängern

Feld	Beschreibung
Ausgestelltes Zertifikat	Zu verlängerndes Zertifikat.
Zweck des Zertifikats	Fordern Sie ein internes oder externes Zertifikat an. Wählen Sie für CAS (z. B. Let's Encrypt) die Option aus **Extern** .
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	CSR mit Zertifikatinformationen.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Für Let's Encrypt beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Eigentümer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen aus CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe zum Abschließen der DNS-Herausforderung erstellt. Die Aufgabe wird automatisch abgeschlossen.

Ergebnis

- Sobald die DNS-Datensatzverbreitung nach zwei Minuten abgeschlossen ist, wird die DNS-Abfrage automatisch abgeschlossen, und der automatisierte Flow sendet eine Anforderung an die ZERTIFIZIERUNGSSTELLE, um das Zertifikat abzurufen.

  Administratoren können diese Dauer ändern, indem sie ändern *sn_disco_certmgmt.wait_time_for_dns_record_propagation*Systemeigenschaft.

- Das Zertifikat wird an die Aufgabe „Neues Zertifikat“ angehängt.
- Der Status der Aufgabe „Zertifikat anfordern“ ändert sich in „Abgeschlossen“.

Widerrufen Sie das Zertifikat mit dem automatisierten ACME-Flow

Fordern Sie einen Widerruf des Zertifikat für eine Anwendung an.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und dass eine Weiterleitungsrichtlinie erstellt wird.

Erforderliche Rolle: pki_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf den automatisierten Flow der Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**an.
   b. Wählen Sie Aus **Zertifikatverwaltung** .
   c. Wählen Sie Aus **Automatisierter Flow** .
2. Wählen Sie Aus **Zertifikat Widerrufen (Automatisiert)** .
3. Entsperren Sie **Ausgestelltes Zertifikat** Feld.
4. Wählen Sie das Symbol „Suchen mit Liste“ ( ) Und wählen Sie das Zertifikat aus, das Sie widerrufen möchten.
   Sie können mehr als ein Zertifikat auswählen.
5. Geben Sie einen ausreichenden Grund für den Widerruf des Zertifikats an.
6. Geben Sie die Widerrufsreihenfolge durch Auswahl von an **Übermitteln** .
7. Wählen Sie im Bestätigungsdialogfeld aus **OK** .

Ergebnis

Es wird automatisch eine Aufgabe erstellt, die den Widerrufsvorgang auslöst. Sobald der Vorgang abgeschlossen ist, ändert sich der Status des Zertifikats in „Widerrufen“.

ACME-Integration mit KeyFactor EJBCA für automatisierte Flows

Automatisieren Sie den Flow beim anfordern, verlängern und Widerrufen Ihrer Zertifikate, indem Sie Keyfactor EJBCA mit der Automated Certificate Management Environment (ACME) integrieren.

Keyfactor-EJBCA ist eine Zertifizierungsstelle, die Ihre Zertifikate ausstellt. ACME sind eine Reihe von Protokollen und Regeln, die Ihnen eine sichere Umgebung für die Verwendung eines automatisierten Flows zur Verwaltung von Zertifikaten bieten.

Indem Sie Ihre Weiterleitungsrichtlinienfelder konfigurieren, können Sie sicherstellen, dass der Inhalt in Ihrer Certificate Signing Request (CSR) mit der richtigen Weiterleitungsrichtlinie übereinstimmt. Dies optimiert den Prozess zum anfordern, verlängern und Widerrufen Ihrer Zertifikate.

EJBCA hat zwei Arten von Anmeldeinformationen. Eine enthält External Account Binding (EAB), die andere nicht

In EJBCA werden automatisierte Zertifikat-Workflows gestartet, wenn Sie Weiterleitungsrichtlinien für EJBCA ACME-Zertifikate erstellen. Für jede Weiterleitungsrichtlinie gibt es Pflichtfelder, in denen Sie Informationen angeben müssen.

Ihre Plattform verfügt über Weiterleitungsrichtlinien, in denen Sie alle Felder der Weiterleitungsrichtlinie ausfüllen. Ihre Plattform richtet diese Informationen an jeder CSR aus, die Sie erstellen, um Zertifikate anzufordern, zu verlängern und zu widerrufen.

Weitere Informationen finden Sie unter Erstellen Sie eine Weiterleitungsrichtlinie für EJBCA-ACME-Zertifikate.

Führen Sie die folgende Aufgabe aus, um EJBCA ACME zur Automatisierung Ihres Zertifikatlebenszyklus zu verwenden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Verbindungs- und Anmeldealias erstellen
2. Konfigurieren Sie Ihre Basis-API-URL für EJBCA ACME
3. Validieren Sie Ihre EJBCA ACME-Basis-API-URL

Konfigurieren Sie Ihre Basis-API-URL für EJBCA ACME

Konfigurieren Sie Ihre Basis-API-URL für EJBCA ACME für die Stamm-URL-Adresse Ihrer Organisation.

Vorbereitungen

Erforderliche Rolle: Discovery_admin, PKI-Administrator (Public Key Infrastructure), admin

Prozedur

1. Navigieren zu **Alle** > **Zertifizierungsstellen**an.
2. Wählen Sie in der Tabelle der Zertifizierungsstellen die Option aus **EJBCA-ACME** .
3. Bearbeiten Sie den Text auf eine der folgenden Arten:
   - Wählen Sie Aus **Bearbeiten** Text.
   - Doppelklicken Sie auf (oder verwenden Sie die Tastenkombination)“ **Basis-URL** Feld.

   Hinweis: Wenn eine Warnmeldung angezeigt wird, befinden Sie sich möglicherweise in der Anwendung „Global“. Wählen Sie den Link aus, der angezeigt wird, um den Datensatz zu bearbeiten.
4. Fügen Sie Ihre eigene API-URL über dem ein [Ejbca_acme] Text innerhalb der URL.
5. Stellen Sie sicher, dass die ACME-Option ausgewählt ist.
6. Wählen Sie **Speichern**.

Ergebnis

Die Basis-API-URL für Ihre EJBCA-ACME-Umgebung ist für Ihre Systeme konfiguriert.

Erstellen Sie eine Weiterleitungsrichtlinie für EJBCA-ACME-Zertifikate

Automatisieren Sie Ihre EJBCA-ACME-Workflows, indem Sie eine Weiterleitungsrichtlinie erstellen, die an Ihren Zertifikatsignaturanforderungen (Certificate Signing Requests, CSRs) ausgerichtet ist, um Zertifikate anzufordern, zu verlängern und zu widerrufen.

Vorbereitungen

Erforderliche Rolle: Discovery_admin, PKI-Administrator (Public Key Infrastructure), admin

Warum und wann dieser Vorgang ausgeführt wird

Optimieren Sie Ihren Workflow für den Zertifikatlebenszyklus, indem Sie ein Formular für Weiterleitungsrichtlinien ausfüllen. Dieses Formular konfiguriert Ihre Weiterleitungsrichtlinienfelder, um sicherzustellen, dass Ihre Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) mit der richtigen Weiterleitungsrichtlinie der Zertifizierungsstelle (Certificate Authority, CA) übereinstimmt.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Zertifikatweiterleitungsrichtlinie“ aus.
   Eine Beschreibung der Feldwerte finden Sie unter Formulartabelle für Zertifikatweiterleitungsrichtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Warnung:** Damit Ihr automatisierter Workflow funktioniert, müssen Sie jedes Feld in Ihrem Weiterleitungsrichtlinienformular ausfüllen. Wenn nicht, erfordert Ihr CSR manuelle Schritte. Sie können alle Felder und Werte im anzeigen Formulartabelle für Zertifikatweiterleitungsrichtlinie.

4. Wählen Sie **Absenden**.

Nächste Maßnahme
Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**an.

Indem Sie Ihre Weiterleitungsrichtlinie auf der Seite „Zertifikatweiterleitungsrichtlinien“ suchen, validieren Sie Ihre EJBCA ACME-Zertifikatweiterleitungsrichtlinie.

Validieren Sie Ihre EJBCA ACME-Basis-API-URL

Validieren Sie, dass Ihre Basis-API-URL für EJBCA ACME auf die Stamm-URL-Adresse Ihrer Organisation aktualisiert wurde.

Vorbereitungen
Erforderliche Rolle: Discovery_admin, PKI-Administrator (Public Key Infrastructure), admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Zertifikatverwaltung**an.
2. Wählen Sie aus **Zertifikatdatensätze** Registerkarte.
3. Wählen Sie Aus **API-URL der Zertifizierungsstelle** .
4. Wählen Sie Aus **EJBCA-ACME** In der Tabelle.

Ergebnis
Die UI wird zum Zertifikatfeld und zur zugehörigen Basis-URL weitergeleitet.

Nächste Maßnahme
Überprüfen Sie die URL, und bestätigen Sie, dass es sich nicht um die Standardeinstellungen handelt.
Um eine Verbindung mit EJBCA herzustellen, müssen Sie die Standard-URL in Ihre spezifische Umgebungs-URL (env) ändern. Wenn die Standardeinstellung weiterhin angezeigt wird, konfigurieren Sie Ihre Basis-API-URL neu. Weitere Informationen finden Sie unter Konfigurieren Sie Ihre Basis-API-URL für EJBCA ACME.

ACME-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Automated Certificate Management Environment (ACME), einschließlich Tabellen, Mustern und Begriffen.

Um die Prozesse Ihres Zertifikatlebenszyklus zu automatisieren, müssen Sie Weiterleitungsrichtlinien ausfüllen, die in die Formulare der Zertifizierungsstelle eingetragen sind. Eine Beschreibung der Felder im Formular „Zertifizierungsstelle“ finden Sie unter Formulartabelle für Zertifikatweiterleitungsrichtlinie.

Formulartabelle für Zertifikatweiterleitungsrichtlinie

Um die Prozesse Ihres Zertifikatlebenszyklus zu automatisieren, müssen Sie ein Weiterleitungsrichtlinienformular ausfüllen, das Ihre Zertifikatsignaturanforderungen ausfüllt. Diese Tabelle zeigt die erforderlichen Felder und Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für ein Formular für eine Zertifikatweiterleitungsrichtlinie

Feld	Beschreibung
Name	Name Ihrer Weiterleitungsrichtlinie.
Zertifizierungsstelle	Zertifizierungsstelle. Um eine Liste der unterstützten Zertifizierungsstellen anzuzeigen, wählen Sie das Suchsymbol aus. Wählen Sie Aus **EJBCA-ACME** . **Hinweis:** Die Zertifizierungsstelle bestimmt, ob zusätzliche Felder für Ihre Weiterleitungsrichtlinie erforderlich sind. Füllen Sie zuerst dieses Feld aus, um zu sehen, welche Informationen Sie für dieses Formular benötigen.
Umgebung	Die Umgebung, für die Sie Ihr Zertifikat benötigen. Die Optionen sind: • Entwicklung • Notfallwiederherstellung • Produktion • Unterproduktion an.
Zuweisungsgruppe	Zuweisungsgruppe. Sie können eine Zuweisungsgruppe auswählen oder eine neue erstellen.
DNS-Abfrageaktion	Domänennamensystem-Challenge-Aktion.
Anmeldeinformationsalias	Anmeldeinformationsalias. Ihre Optionen basieren auf den Aliassen, die Sie im Formular „Anmeldeinformationen für Zertifikatverwaltung“ erstellen.
Zertifizierungszweck	Zertifizierungszweck. Die Optionen sind: • Intern • Extern
Ist aktiv	Option zum Aktivieren der Richtlinie
Doppelte Anforderung zulassen	Option, mit der mehrere Anforderungen mehrere Zertifikate erhalten können.
Freigabe erforderlich	Option, um eine Genehmigung zu erfordern.
Aufgabengenehmigungsgruppe	Aufgabengenehmigungsgruppe. Dieses Feld wird nur angezeigt, wenn **Genehmigung Erforderlich** Feld ist aktiviert.
DNS-Aufgabenzuweisungsgruppe	DNS-Aufgabenzuweisungsgruppe. Wählen Sie Aus **Zertifikatbestand und -Verwaltung**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für ein Formular für eine Zertifikatweiterleitungsrichtlinie (Fortsetzung)

Feld	Beschreibung
Domäne	Domäne der Richtlinie. Dieses Feld wird automatisch auf festgelegt `global`
MID-Server	MID-Server Sie möchten verwenden.
Allgemeiner Antragstellername	Bestimmter Entitäts- oder Domänenname, für den das Zertifikat ausgestellt wird. Geben Sie einen Namen oder ein `*` .
Alternativer Antragstellername	Domäne oder Unterdomäne, die im allgemeinen Antragstellernamen enthalten ist. Geben Sie einen alternativen Namen oder ein `*` .
Organisation	Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie die Organisation oder ein `*` .
Ort	Ort (Stadt) der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie den Ort oder ein `*` .
Land	Land der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie das Land oder ein `*` .
Organisationseinheit	Organisationseinheit, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie die Einheit oder ein `*` .
Status	Status der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie den Status oder ein `*` .
E-Mail-Adresse	E-Mail-Adresse des Administrators in der Organisation, der die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie eine E-Mail-Adresse oder ein `*` .

Automatisierte Zertifikatverlängerung

Erkennen Sie Zertifikate, die kurz vor dem Ablauf ablaufen, und verlängern Sie sie automatisch vor dem Ablauf, um Ihre digitalen Systeme sicher und kontinuierlich verfügbar zu halten.

Abgelaufene Zertifikate sind für Organisationen ein schwerwiegendes Problem.

Viele Organisationen haben aufgrund ihrer TLS-Zertifikate (Transport Layer Security), die ohne ihr Wissen ablaufen, unerwartete Ausfälle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die manuelle Nachverfolgung Ihrer digitalen TLS-Zertifikate ist eine zeitaufwändige und langwierige Aufgabe, die dazu führen kann, dass Zertifikate unbemerkt ablaufen. Wenn Sie ablaufende Zertifikate übersehen, werden Websites unsicher und gefährlich für Anwender.

Mit Service Desk-Mitarbeitern für automatische Zertifikatverlängerung können Sie Zertifikate suchen, die kurz vor dem Ablauf stehen, und sie automatisch verlängern, bevor sie ablaufen.

Sie können auch festlegen, dass ein Zertifikat automatisch verlängert wird, nachdem ein neues Zertifikat angefordert wurde.

Automatisierte Zertifikatverlängerung wird konfiguriert

Konfigurieren Sie Ihren MID-Server Und Systemeigenschaften zum automatischen verlängern von Zertifikaten, bevor sie ablaufen.

Um Ihre Zertifikate automatisch zu verlängern, bevor sie ablaufen, verwenden Sie den automatisierten Zertifikatverlängerungs-Workflow oder den Now Assist KI-Agent für Zertifikatverlängerung.

In beiden Fällen müssen Sie Ihr System zuerst für die automatische Verlängerung konfigurieren.

Die Konfiguration für die automatisierte Zertifikatverlängerung umfasst die folgenden Schritte:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server
3. Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung. Dieser Schritt ist optional, wenn Sie verwenden Now Assist KI-Agent für Zertifikatverlängerung.

Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung

Sammeln Sie Informationen zu Stammzertifikaten, die außerhalb Ihres Servers gespeichert sind. Erstellen Sie einen spezialisierten Discovery Zeitplan.

Vorbereitungen

Erforderliche Rolle: pki_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Ihren MID-Server Dient zum automatischen verlängern von Zertifikaten, indem die Konfigurationsparameter in festgelegt werden MID-Server.

Informationen zur Versionskompatibilität und zur Fehlerbehebung finden Sie unter Verlängerung von TLS-Zertifikaten mit KI-Agents für Discovery artikel aus dem Wissensmodul [KB2470998] in der Now Support Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **MID-Server**an.
2. Wählen Sie aus MID-Server Die Sie konfigurieren möchten.
3. Wählen Sie aus **Konfigurationsparameter** Registerkarte.
4. Fügen Sie einen neuen Parameter hinzu, indem Sie auswählen **Neu** .
5. Wählen Sie aus **Parametername** Feld.
6. Wählen Sie Aus **Ext.Vault.hashicorp.address**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. In **Wert** Geben Sie Ihre externe Hashicorp-Tresoradresse ein.
   Der Standardwert ist http://127.0.0.1:8200.
8. Wählen Sie **Absenden**.
9. Fügen Sie einen neuen Parameter hinzu.
   a. Wählen Sie **Neu**.
   b. Wählen Sie aus **Parametername** Feld.
   c. Wählen Sie Aus **Ext.Vault.hashicorp.path**
   d. In **Wert** Geben Sie Ihren Dateipfad im Hashicorp-Tresor ein.
   e. Wählen Sie **Absenden**.
10. Navigieren Sie zum Speicherort Ihres Hostnamens von MID-Server
    a. Navigieren Sie in zur IP-Adresse **IP-Adresse** Feld von MID-Server Datensatz.
    b. Navigieren Sie zu **MID-Server-Installationsordner** Wo Sie installiert haben MID-Server.
    c. Wählen Sie aus Service Desk-Mitarbeiter/config.xml Datei.
    d. Fügen Sie den Parameter hinzu `ext.vault.hashicorp.token`In Ihrer Datei cofig.xml.
    e. Fügen Sie den folgenden Code ein: `<parameter name="ext.valut.hashicorp.token" secure="true" value="<YOUR TOKEN VALUE>"/>`
    f. Starten Sie Ihren neu MID-Server.

Ergebnis
Ihr MID-Server Ist für die automatische Zertifikatverlängerung konfiguriert.

Nächste Maßnahme
Um den Prozess der Konfiguration für die automatische Zertifikatverlängerung abzuschließen, müssen Sie die erforderlichen Schritte bis ausführen Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server Und Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung.

Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server

Aktivieren Sie Ihren MID-Server Um Ihre Zertifikate durch Hinzufügen von automatisch zu verlängern Zertifikatsbestand-Management Und GenerateCSR-Anwendungen.

Vorbereitungen
Überprüfen Sie, ob Sie die Aufgabe abgeschlossen haben Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung.

Erforderliche Rolle: pki_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Verschieben Sie die Anwendungen Zertifikatsbestand-Management Und GenerateCSR aus Ihrer Sammlungsliste in Ihre Liste der unterstützten Anwendungen.

Prozedur
1. Navigieren zu **Alle** > **MID-Server**an.
2. Wählen Sie aus MID-Server Die Sie konfigurieren möchten.

> **Hinweis:** Die MID-Server Muss identisch sein MID-Server Die Sie für die automatisierte Zertifikatverlängerung konfiguriert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. MID-Server anpassen
   a. Wählen Sie Aus **Unterstützte Anwendungen** .
   b. Wählen Sie **Bearbeiten**.
   c. Verschieben **Zertifikatbestand und -Verwaltung** Zu **Liste Der Unterstützten Anwendungen** .
   d. Wählen Sie **Speichern**.
   Sie werden zu weitergeleitet MID-Server Seite.
4. Hinzufügen MID-Server Fähigkeiten
   a. Wählen Sie Aus **Fähigkeiten** .
   b. Wählen Sie **Bearbeiten**.
   c. Verschieben **GenerateCSR** Von der Sammlungsliste zur Liste der unterstützten Anwendungen.
   d. Wählen Sie **Speichern**.
   Sie werden zu weitergeleitet MID-Server Seite.

Ergebnis
Ihr MID-Server Unterstützt Zertifikatsbestand-Management Und GenerateCSR-Anwendungen, die eine Anforderung zum Aktivieren der automatischen Zertifikatverlängerung erfüllen.

Nächste Maßnahme
Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung, Um die Konfiguration für die automatische Zertifikatverlängerung abzuschließen.

Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung

Aktivieren Sie die Optionen für die automatische Verlängerung in Ihren Systemeigenschaften, um Ihr System so zu konfigurieren, dass TLS-Zertifikate (Transport Layer Security) automatisch verlängert werden, bevor sie ablaufen.

Vorbereitungen
Überprüfen Sie, ob Sie die Aufgaben abgeschlossen haben. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung, Und Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server.

Erforderliche Rolle: pki_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Die Konfiguration Ihrer Systemeigenschaften zum Aktivieren der automatischen Zertifikatverlängerung ist für die Verwendung des Workflows für die automatische Verlängerung und des erforderlich Now Assist Agent für KI-Zertifikatverlängerung.

Prozedur
1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach *auto_renew*.
3. Wählen Sie Aus **sn_Disco_certmgmt.enable_Auto_Renewal_options_in_Service_catalog**
4. Legen Sie fest **Wert** Feld bis **Wahr** .

Ergebnis
Ihr System ist so konfiguriert, dass Zertifikate automatisch verlängert werden, bevor sie ablaufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sie können Legen Sie ein Zertifikat so fest, dass es automatisch verlängert wird Oder verwenden Sie Now Assist KI-Agent für Zertifikatverlängerung.

Legen Sie ein Zertifikat so fest, dass es automatisch verlängert wird

Legen Sie Zertifikate so fest, dass sie automatisch verlängert werden. Geben Sie die Anzahl der Tage vor ihrem Ablauf an, sodass das Zertifikat automatisch vor diesen Tagen verlängert wird.

Vorbereitungen

Führen Sie die folgenden Aufgaben aus, um Ihr System so zu konfigurieren, dass Ihre Zertifikate automatisch verlängert werden:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server
3. Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Navigieren zu **Servicekatalog** > **Zertifikatverwaltung** > **Automatisierter Flow** > **Zertifikat verlängern (automatisiert)**an.
2. Wählen Sie das ausgestellte Zertifikat aus, das Sie verlängern möchten, indem Sie auf das Suchsymbol klicken .
3. Legen Sie fest **Automatisch Verlängern** Feld bis **Ja** .

   Hinweis: Durch Auswahl von **Ja** , Wird ein neues Feld mit dem Namen angezeigt **Wie viele Tage vor Ablauf muss dieses Zertifikat verlängert werden?** .

4. Wählen Sie die Anzahl der Tage im aus **Wie viele Tage vor Ablauf muss dieses Zertifikat verlängert werden?** Feld.
5. Wählen Sie **Absenden**.

Ergebnis

Das von Ihnen ausgewählte Zertifikat ist so festgelegt, dass die Anzahl der Tage vor Ablauf, die Sie anfordern, automatisch verlängert wird.

Fordern Sie ein neues Zertifikat an, und legen Sie es auf „automatisch verlängern“ fest

Legen Sie Ihr Zertifikat so fest, dass es automatisch verlängert wird, wenn Sie es zum ersten Mal anfordern.

Vorbereitungen

Führen Sie die folgenden Aufgaben aus, um Ihr System so zu konfigurieren, dass Ihre Zertifikate automatisch verlängert werden:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server
3. Konfigurieren Sie Systemeigenschaften für die automatische Zertifikatverlängerung

Erforderliche Rolle: pki_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Servicekatalog** > **Zertifikatverwaltung** > **Automatisierter Flow** > **Neues Zertifikat anfordern (automatisiert)**an.
2. Aktivieren Sie das Kontrollkästchen **Möchten Sie CSR generieren?**
3. Füllen Sie die Felder im Formular Neues Zertifikat anfordern aus.
   Eine Beschreibung der Feldwerte finden Sie unter Neue Zertifikatformulartabelle wird angefordert.
4. Wählen Sie Aus **Generieren** .
5. Legen Sie fest **Gültigkeitszeitraum für Zertifikat (in Tagen)** Feld bis Gültigkeitszeitraum des Zertifikats.
6. Legen Sie fest **Automatisch Verlängern** Feld bis **Ja** .

   Hinweis: Durch Auswahl von **Ja** , Wird ein neues Feld mit dem Namen angezeigt **Wie viele Tage vor Ablauf muss dieses Zertifikat verlängert werden?** .

7. Wählen Sie die Anzahl der Tage vor dem Zertifikat aus, das Sie verlängern möchten **Wie viele Tage vor Ablauf muss dieses Zertifikat verlängert werden?** Feld.
8. Wählen Sie **Absenden**.

Ergebnis
Ihr neues Zertifikat wird mit Anweisungen zur automatischen Verlängerung ausgegeben, bevor es abläuft.

Validiert den Status der automatischen Verlängerung Ihres Zertifikats

Bestätigen Sie, dass Sie Ihr Zertifikat so festlegen, dass es automatisch verlängert wird, bevor es abläuft.

Vorbereitungen
Führen Sie eine der folgenden Aufgaben aus, bevor Sie Ihr Zertifikat validieren:

- Legen Sie ein Zertifikat so fest, dass es automatisch verlängert wird
- Fordern Sie ein neues Zertifikat an, und legen Sie es auf „automatisch verlängern“ fest

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Eindeutige Zertifikate**an.
2. Wählen Sie das Zertifikat aus, das Sie validieren möchten.
3. Wählen Sie aus **Zertifikatmetadaten** Registerkarte.
4. Stellen Sie sicher, dass **Automatische Verlängerung aktiviert** Feld ist auf festgelegt **Wahr** .

   Hinweis: pki_admin kann dieses Feld auswählen und bearbeiten.

Zertifikatsbestand-Management – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Zertifikatsbestand-Management Dashboard und Komponenten, einschließlich Tabellen, Muster und Begriffe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Tabellen

Zertifikatsbestand-Management Tabellen bieten ein zentrales System zum Nachverfolgen und Verwalten digitaler Zertifikate. Sie erfassen wichtige Details, einschließlich erkannter Zertifikate, Installationsstandorte, Verlaufsdaten und zugehöriger Aufgaben wie Verlängerungen und Anforderungen. Dieses Framework stellt eine effiziente Zertifikatverwaltung sicher, unterstützt Sicherheit, Compliance und optimierte Vorgänge.

Zertifikatsbestand-Management Tabellen

Tabelle	Beschreibung
Eindeutiges Zertifikat [cmdb_ci_certificate]	Discovery füllt diese Tabelle mit einem Datensatz für jedes eindeutige Zertifikat aus, das für die Zertifikatverwaltung erkannt wird. Die Fingerabdruckspalte ist für jedes Serverzertifikat eindeutig. **Hinweis:** Sie können auch die gesamte Zertifikatkette mithilfe der zugehörigen Liste in der Tabelle „eindeutiges Zertifikat“ anzeigen.
Installiertes Zertifikat [sn_Disco_certmgmt_cmdb_installed_certificate]	Discovery füllt diese Tabelle mit allen erkannten Zertifikaten aus und zeigt alle Standorte an, an denen Zertifikate installiert sind. Sie enthält keinen Verweis auf das Server-CI, und IRE wird nicht durchlaufen. Alle Beziehungen mit dem verwalteten Zertifikat werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] gespeichert. Die Beziehungen können für Server, Anwendungen und Business Services sein.
Erkanntes Zertifikat [sn_Disco_certmgmt_certificate_history]	Erkannte Zertifikate werden zuerst als Teil des Shazzam- und URL-Erkennungssensors in dieser Tabelle gespeichert und zeigen die XML-Nutzlast aller Zertifikate mit dieser Adresse an.
Zertifikatdomäne [Certificate_Domain]	Speichert eine oder mehrere Domänen für den alternativen Antragstellernamen.
Zertifikataufgabe [sn_Disco_certmgmt_certificate_Task]	Speichert alle Zertifikatverlängerungsaufgaben und neue Zertifikatanforderungsaufgaben.
Zertifikat-URL [sn_Disco_certmgmt_cert_url]	Enthält eine Liste von URLs nach Zeile, die für die Zertifikat-Discovery als Ziel dienen sollen.
Zertifikatverwaltungs-Anmeldeinformationen [sn_Disco_certmgmt_certificate_Management_credential] (Version 1.1.7 Zertifikatbestand und -Verwaltung)	Speichert die CA-Typen, einschließlich GoDaddy und DigiCert. Andere werden basierend auf dem Skript certificate_authority gefüllt. Nur discovery_admin kann andere CA-Anmeldeinformationen erstellen. Für zukünftige Releases ist die Unterstützung von externen Anmeldeinformationen vorgesehen.
Geplante Zertifikat-URL [sn_Discovery_cert_url_sched_m2m]	Verknüpft die URLs zur Erkennung von [Discovery_cert_url] mit einem bestimmten Discovery-Zeitplan [Discovery_schedule].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Tabellen (Fortsetzung)

Tabelle	Beschreibung
Zertifizierungsstelle [sn_Disco_certmgmt_ca] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Enthält den Namen der Zertifizierungsstelle und die Basis-URL der REST API.
Zertifizierungsstellen-API-URL [sn_Disco_certmgmt_ca_api_url] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Enthält die Referenz der Zertifizierungsstelle, die Endpunkt-URL der REST API und den Zertifikatvalidierungstyp.
Routing-Richtlinie [sn_Disco_certmgmt_Routing_Policy] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Entscheidet, welche CA für Zertifikatvorgänge kontaktiert werden muss. Diese Tabelle enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR.
Automatisierte Zertifikataufgabe [sn_Disco_certmgmt_Task] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Enthält alle automatisierten Zertifikatanforderungsaufgaben (neu, verlängern und widerrufen).
Neue Zertifikataufgaben [sn_Disco_certmgmt_New_Task] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Erweitert von sn_Disco_certmgmt_Task und enthält neue Zertifikatanforderungsaufgaben.
Aufgaben „Zertifikat verlängern“ [sn_Disco_certmgmt_renew_Task] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Erweitert von sn_Disco_certmgmt_Task und enthält Aufgaben zur Anforderung von Zertifikatverlängerung.
Aufgaben „Zertifikat widerrufen“ [sn_Disco_certmgmt_revoke_Task] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Erweitert von sn_Disco_certmgmt_Task und enthält Aufgaben zur Anforderung von Zertifikatwiderrufen.
Zertifikatverlängerungen [sn_Disco_certmgmt_certificate_Extension] (Version 1.3.8 Zertifikatbestand und -Verwaltung)	Speichert Informationen für alle Serverzertifikate.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management-Muster

Zertifikatbestandsmuster optimieren die Verwaltung digitaler Zertifikate, stellen verbesserte Sicherheit, Compliance und effiziente Lebenszyklussteuerung sicher und reduzieren das Risiko von Schwachstellen. Verwalten Sie Zertifikatbestand mit optimierten Mustern effizient.

Zertifikatsbestand-Management Muster und Beschreibungen

Muster	Beschreibung
GoDaddy – Zertifikatverwaltungsmuster (Version 1.1.7 Zertifikatbestand und -Verwaltung)	Teil der Anwendung „Zertifikatbestand und -Verwaltung“. Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) GoDaddy
DigiCert – Zertifikatverwaltungsmuster (Version 1.1.7 Zertifikatbestand und -Verwaltung)	Teil der Anwendung „Zertifikatbestand und -Verwaltung“. Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) DigiCert
Entrust – Zertifikatverwaltungsmuster (Version 1.2.0 Zertifikatbestand und -Verwaltung)	Teil der Anwendung „Zertifikatbestand und -Verwaltung“. Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) Entrust
Sectigo – Zertifikatverwaltungsmuster (Version 1.2.0 Zertifikatbestand und -Verwaltung)	Teil der Anwendung „Zertifikatbestand und -Verwaltung“. Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) Sectigo
SSL-Zertifikatmuster importieren Version 1.1.7 Zertifikatbestand und -Verwaltung.	Ermöglicht Ihnen das Erkennen von Zertifikaten, indem Sie Zertifikate aus Dateien importieren. Zertifikaterkennung über Zertifikatdateiimport ausführen.
Amazon AWS: Zertifikatmanager Muster und **Amazon AWS – Zertifikate-Tags sammeln** Gemeinsame Bibliothek. Zertifikatsbestand-Management, Mindestens 3,4.0. Muster für Discovery und Service-Mapping, Mindestens 1.12.0.	Erkennt Zertifikate als Teil von AWS Cloud-Discovery. AWS Certificate Manager-Discovery.
Google Cloud Platform (GCP): Zertifikat-Manager-Zertifikate Muster und **Google Cloud Platform (GCP): Klassische Zertifikate** Muster. Zertifikatsbestand-Management, Mindestens 3,4.0. Muster für Discovery und Service-Mapping, Mindestens 1.12.0.	Erkennt Zertifikate als Teil von GCP Cloud-Discovery. GCP Certificate Manager-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Muster und Beschreibungen (Fortsetzung)

Muster	Beschreibung
Azure: Key Vault-Zertifikate Muster. Zertifikatsbestand-Management, Mindestens 3,4.0. Muster für Discovery und Service-Mapping, Mindestens 1.12.0.	Erkennt Zertifikate als Teil von Azure Cloud-Discovery. Azure Discovery des Key Vault-Zertifikats.
Java-Schlüsselspeicher und Windows-Zertifikate	Erkennt Zertifikate im Java-Schlüsselspeicher oder Windows-Zertifikatspeicher. Java-Schlüsselspeicher und Windows-Zertifikatspeicher Discovery.

AWS Certificate Manager-Discovery

Cloud-Discovery Verwendet Muster, um Zertifikatdaten zu erkennen, die die aufweisen Amazon AWS Cloud Certificate Manager (ACM) verwaltet. Die Erkennung dieser Daten erfordert die Installation und Aktualisierung Muster für Discovery und Service-Mapping Und Zertifikatsbestand-Management.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie die Konfiguration von AWS Account

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management(sn_Disco_certmgmt) Mindestens 3.4.0

Muster für Discovery und Service-Mapping(sn_itom_pattern) Mindestens 1.12.0

Verifizieren Sie das Cloud-Discovery Hat Berechtigungen zum Erkennen AWS

Führen Sie die folgenden Befehle mit aus AWS CLI zum Überprüfen der Berechtigungen und Richtlinien, die an Ihre aktive IAM-Rolle angehängt sind:

- Zertifikate auflisten

  `AWS_PAGER=„“ aws acm list-Certificates --Region <region>`

- Beschreiben Sie Zertifikate

  `AWS_PAGER=" awsacm description-certificate --certificate-arnarn:aws:acm:<region>:<accout_id>:certificate/<certificate_id>`

- Ruft Zertifikate Ab

  `AWS_PAGER=" awsacm GET-certificate --certificate-arnarn:aws:acm:<region>:<account_id>:certificate/<certificate_id>`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tags abrufen

```
AWS_PAGER='' awsresourcegroupstaggingapi get-resources --Tags-per-page 100
--resource-type-Filters 'acm:certificate'
```

Legen Sie die Konfiguration der Systemeigenschaft fest

Wenn die Systemeigenschaft *sn_itom_pattern.issuer_certificate_search_by_idn*Ist auf festgelegt **Falsch** , Discovery Verwendet die Zertifikatfingerabdrücke, um Aussteller und Stammaussteller zu finden.

Verifizieren Sie MID-Server Anforderungen

Die MID-Server Muss entweder ALLE Fähigkeiten oder AWS-Fähigkeit haben.

Überprüfen Sie die Konfiguration von Cloud-Discovery Zeitplan

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die **Amazon AWS: Zertifikatmanager** Muster und **Amazon AWS – Zertifikate-Tags sammeln** Die gemeinsame Bibliothek unterstützt die Erkennung der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Name	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: **.service-now.com*
Fingerabdruck	Hashwert des Zertifikats Beispiel: *D708c8583c78c176d5df1a4f01aac746294 e390a03038f280b0d8f5ef*
Fingerabdruck-Algorithmus	Der Algorithmus, der zum Hash des Zertifikats verwendet wird. Beispiel: Discove Fingerabdrücke vom SHA-256-Algorithmus, sodass der ausgefüllte Wert: *SHA-2*
Seriennummer	Seriennummer des Zertifikats Beispiel: *70 d8 c9 52 77 1c 2d 54 97 00 0e 21 05 e8 c1 73*
Allgemeiner Antragstellername	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: **.servi*
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der eindeutige Name des Antragstellers besteht aus folgenden Elementen • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die besitzt Domäne An die das Zertifikat a wird. • Organisationseinheit (OU): Die Organisationseinheit, die Eigentümer von ist Do das Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Der allgemeine Name des Zertifikatausstellers. Beispiel: Entrust-Zertifizierungss
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der eindeutige Name des Ausstellers besteht aus folgenden Elementen • Allgemeiner Name (CN): Die Behörde, die das Zertifikat ausgestellt hat. Beispi *`Zertifizierungsstelle`* . • Organisation (O): Die Organisation, die das Zertifikat ausgestellt hat. Beispiel: *`Inc`* . • Organisationseinheit (OU): Die Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate e sollen Discovery Legt fest **Verlängerungsnachverfolgung** Bis *`Priorität 3`* Wenn die Systemeigenschaft *`Glide.Discovery.zert.enable_Renewal_Task_Creation_for_discovered_`* Ist auf festgelegt **Wahr** .
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *`25. September 2023 10:43:0`*
Gültig Bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024 2011-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), an die das Zertifikat ausgestellt wird.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OU), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wird. Wird in einem zweistellige ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland (ST) oder die Provinz der Organisation, für die das Zertifikat ausgest mit zweistelligem Code ausgefüllt.
Antragsteller-Ort	Die Stadt, der Standort (L) der Organisation, für die das Zertifikat ausgestellt wird.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, an die das Zertifikat ausgestellt wird.
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die Referenz ist verfüg ausgestellte Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das ausgestellte Zertifikat Nutzlast ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

CI-Beziehungen

Die **Amazon AWS: Zertifikatmanager** Muster und **Amazon AWS – Zertifikate-Tags sammeln** Die gemeinsame Bibliothek unterstützt die Erkennung der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_Datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Service-Account [cmdb_ci_Cloud_Service_Account]
Schlüsselwert[cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

GCP Certificate Manager-Discovery

Cloud-Discovery Verwendet Muster, um Zertifikatdaten zu erkennen, die die aufweisen GCP Zertifikatmanager verwaltet. Die Erkennung dieser Daten erfordert die Installation und Aktualisierung Muster für Discovery und Service-Mapping Und Zertifikatsbestand-Management.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie die Konfiguration von GCP Account

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management (sn_Disco_certmgmt), mindestens 3.4.0

Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0

Überprüfen Sie die Konfiguration der Systemeigenschaft

Wenn die Systemeigenschaft *sn_itom_pattern.issuer_certificate_search_by_idn*Ist auf festgelegt **Falsch** , Discovery Verwendet die Zertifikatfingerabdrücke, um Aussteller und Stammaussteller zu finden.

Verifizieren Sie MID-Server Anforderungen

Die MID-Server Muss entweder haben **ALLE** Fähigkeit oder **GCP** Fähigkeit.

Überprüfen Sie die Konfiguration von Cloud-Discovery Zeitplan

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die **Google Cloud Platform (GCP): Zertifikat-Manager-Zertifikate** Muster und **Google Cloud Platform (GCP): Klassische Zertifikate** Muster unterstützen die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Name	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: *.service-now.com
Seriennummer	Seriennummer des Zertifikats Beispiel: 70 d8 c9 52 77 1c 2d 54 97 00 0e 21 05 e8 c1 73
Allgemeiner Antragstellername	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: *.servi
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der eindeutige Name des Antragstellers besteht aus folgenden Elementen • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Zertifik wird. • Organisationseinheit (OU): Die Organisationseinheit, die die Domäne besitzt, f Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Der allgemeine Name des Zertifikatausstellers. Beispiel: Entrust-Zertifizierungss
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der eindeutige Name des Ausstellers besteht aus folgenden Elementen • Allgemeiner Name (CN): Die Behörde, die das Zertifikat ausgestellt hat. Beispi Zertifizierungsstelle . • Organisation (O): Die Organisation, die das Zertifikat ausgestellt hat. Beispiel: Inc . • Organisationseinheit (OU): Die Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate e sollen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Discovery Legt fest **Verlängerungsnachverfolgung** Bis *Priorität 3* Wenn die Systemeigenschaft *Glide.Discovery.zert.enable_Renewal_Task_Creation_for_discovered_* Ist auf festgelegt **Wahr** .
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *25. September 2023 10:43:0*
Gültig Bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024 2011-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), an die das Zertifikat ausgestellt wird.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OU), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wird. Wird in einem zweistellige ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland (ST) oder die Provinz der Organisation, für die das Zertifikat ausgest mit zweistelligem Code ausgefüllt.
Antragsteller-Ort	Die Stadt, der Standort (L) der Organisation, für die das Zertifikat ausgestellt wird.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, an die das Zertifikat ausgestellt wird.
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die Referenz ist verfüg ausgestellte Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das ausgestellte Zertifikat Nutzlast ist.
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

CI-Beziehungen

Die **Google Cloud Platform (GCP): Zertifikat-Manager-Zertifikate** Muster und **Google Cloud Platform (GCP): Klassische Zertifikate** Muster unterstützen die Erkennung der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Google-Rechenzentrum [cmdb_ci_google_Datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Service-Account [cmdb_ci_Cloud_Service_Account]
Schlüsselwert[cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

Azure Discovery des Key Vault-Zertifikats

Cloud-Discovery Verwendet Muster zur Erkennung Azure Key Vault-Zertifikate. Die Erkennung dieser Daten erfordert die Installation und Aktualisierung Muster für Discovery und Service-Mapping Und Zertifikatsbestand-Management.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie die Konfiguration von Azure Account

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management (sn_Disco_certmgmt), mindestens 3.4.0

Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0

Überprüfen Sie die Konfiguration der Systemeigenschaft

Überprüfen Sie, ob *sn_itom_pattern.issuer_certificate_search_by_idn*Auf festlegen **Wahr** Zum Konfigurieren Discovery Dient zum Durchsuchen von Ausstellern nur nach eindeutigem Ausstellernamen. Discovery Fingerabdruck kann nicht für jedes Zertifikat in der Kette berechnet werden, da PFX-Datensätze für Schlüssel-Wert-Zertifikate keine Zertifikatketten enthalten.

Verifizieren Sie MID-Server Anforderungen

Die MID-Server Muss entweder haben **ALLE** Fähigkeit oder **Azure** Fähigkeit.

Überprüfen Sie die Konfiguration von Cloud-Discovery Zeitplan

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die **Azure: Key Vault-Zertifikate** Muster unterstützen die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Name	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: **.service-now.com*
Seriennummer	Seriennummer des Zertifikats Beispiel: *70 d8 c9 52 77 1c 2d 54 97 00 0e 21 05 e8 c1 73*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Allgemeiner Antragstellername	Der Hostname/die Domäne, die dem Zertifikat zugeordnet ist. Beispiel: *.servi
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der eindeutige Name des Antragstellers besteht aus folgenden Elementen • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Zertifik wird. • Organisationseinheit (OU): Die Organisationseinheit, die die Domäne besitzt, f Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Der allgemeine Name des Zertifikatausstellers. Beispiel: Entrust-Zertifizierungss
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der eindeutige Name des Ausstellers besteht aus folgenden Elementen • Allgemeiner Name (CN): Die Behörde, die das Zertifikat ausgestellt hat. Beispi *Zertifizierungsstelle* . • Organisation (O): Die Organisation, die das Zertifikat ausgestellt hat. Beispiel: *Inc* . • Organisationseinheit (OU): Die Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate e sollen Discovery Legt fest **Verlängerungsnachverfolgung** Bis *Priorität 3* Wenn die Systemeigenschaft *Glide.Discovery.zert.enable_Renewal_Task_Creation_for_discovered_* Ist auf festgelegt **Wahr** .
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *25. September 2023 10:43:0*
Gültig Bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024 2011-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), an die das Zertifikat ausgestellt wird.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OU), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wird. Wird in einem zweistellige ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland (ST) oder die Provinz der Organisation, für die das Zertifikat ausgest mit zweistelligem Code ausgefüllt.
Antragsteller-Ort	Die Stadt, der Standort (L) der Organisation, für die das Zertifikat ausgestellt wird.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, an die das Zertifikat ausgestellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die Referenz ist verfüg ausgestellte Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das ausgestellte Zertifikat Nutzlast ist.
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

CI-Beziehungen

Die **Azure: Key Vault-Zertifikate** Muster unterstützen die Erkennung der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Azure-Rechenzentrum [cmdb_ci_Azure_Datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Service-Account [cmdb_ci_Cloud_Service_Account]
Schlüsselwert[cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

Java-Schlüsselspeicher und Windows-Zertifikatspeicher Discovery

DiscoveryVerwendet **Sammeln Sie Zertifikate** Abschnitt „Erweiterung“ von **Linux-Server** Und **Windows-Betriebssystem: Server** Muster zum Erkennen von Zertifikaten, die im Java-Schlüsselspeicher oder gespeichert sind Windows Zertifikat Speichern. Die Erkennung der Zertifikatinformationen erfordert die Installation und Aktualisierung Muster für Discovery und Service-Mapping Und Zertifikatsbestand-Management.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Verifizieren Das Die folgenden Plugins sind aktuell

- Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0
- Zertifikatsbestand-Management (sn_Disco_certmgmt), mindestens 3.4.0

Überprüfen Sie, ob das Muster ist Aktiviert

Die **Sammeln Sie Zertifikate** Die Mustererweiterung ist standardmäßig deaktiviert. Auf der **Discovery-Muster** Liste, überprüfen Sie, ob **Sammeln Sie Zertifikate** Muster Erweiterung Hat **Aktiv** Feld auf festgelegt **Wahr** .

Überprüfen Sie die Konfiguration der Java-Schlüsselspeicher-Anmeldeinformationen

In **Discovery-Anmeldeinformationen** Modul, wählen Sie aus **jks-Anmeldeinformationen** . Stellen Sie sicher, dass Sie die Discovery-IP-Affinität konfiguriert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

haben. In **Typ** Feld , Einfügen `java_Keystore` . Weitere Informationen finden Sie unter Erste Schritte mit Anmeldeinformationen

Überprüfen Sie die Konfiguration von Die DiscoveryZeitplan

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen

Von Discovery während der horizontalen Erkennung erfasste Daten

Die **Sammeln Sie Zertifikate** Abschnitt „Erweiterung“ von **Linux-Server** Und **Windows-Betriebssystem: Server** Muster unterstützen die Erkennung der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Fingerabdruck [Fingerabdruck]	Die Fingerabdrucknummer des Zertifikats.
Seriennummer [serial_number]	Seriennummer des Zertifikats
Signaturalgorithmus [Signature_Algorithmus]	Der Signaturalgorithmus des Zertifikats.
Fingerabdruckalgorithmus [Fingerprint_Algorithmus]	Der Fingerabdruckalgorithmus des Zertifikats.
Eindeutiger Ausstellername [issuer_Distinguished_Name]	Der eindeutige Name des Zertifikatausstellers. Der eindeutige Name des Ausstellers besteht aus folgenden Elementen • Allgemeiner Name (CN): Die Behörde, die das Zertifikat ausgestellt hat. Beispiel: *`Entrust-Zertifizierungsstelle`* . • Organisation (O): Die Organisation, die das Zertifikat ausgestellt hat. Beispiel: *`„Entrust“, Inc`* . • Organisationseinheit (OU): Die Einheit, die über die gesetzlichen Rechte zum Ausstellen des Zertifikats verfügt.
Eindeutiger Antragstellername [subject_Distinguished_Name]	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der eindeutige Name des Antragstellers besteht aus folgenden Elementen • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Zertifikat ausgestellt wird. • Organisationseinheit (OU): Die Organisationseinheit, die die Domäne besitzt, für die das Zertifikat ausgestellt wird.
Allgemeiner Antragstellername [subject_common_Name]	Der dem Zertifikat zugeordnete Hostname oder Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Antragstellerland [subject_Country]	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wird. Wird in einem zweistelligen Ländercode ausgefüllt.
Antragstellerstatus [subject_State]	Die Region, das Bundesland (ST) oder die Provinz der Organisation, für die das Zertifikat ausgestellt wird. Diese Daten werden mit einem zweistelligen Code ausgefüllt.
Betrefflokalität [subject_locality]	Die Stadt, der Standort (L) der Organisation, für die das Zertifikat ausgestellt wird.
Betrefforganisationseinheit [subject_Organization_unit]	Die Organisationseinheit (OU), für die das Zertifikat ausgestellt wird.
Antragstellerorganisation [subject_Organization]	Die Organisation (O), für die das Zertifikat ausgestellt wird.
Betreff-E-Mail [subject_email]	Die E-Mail-Adresse der Organisation, für die das Zertifikat ausgestellt wird.
Gültig ab [valid_from]	Das Zertifikat ist ab diesem Datum (Wird in Ihrer Zeitzone angezeigt.). Beispiel: *25. September 2023 10:43:03*
Gültig bis [valid_to]	Das Ablaufdatum des Zertifikats (Wird in Ihrer Zeitzone angezeigt.). Beispiel: 2024 2011-09-24 10:43:03
Status [state]	Wenn Discovery Sammelt das Zertifikat, das das Feld angibt **Installiert**
Alternativer Antragstellername [subject_Alternative_Name]	Eine Liste von Verweisen auf alternative Hostnamen, die vom Server verwendet werden.
Aussteller [Aussteller]	In diesem Feld befindet sich ein Verweis auf den Zertifikatdatensatz. Der Aussteller ist die Entität, die das Zertifikat signiert und ausgestellt hat. Die Referenz ist verfügbar, wenn das ausgestellte Zertifikat Teil derselben Nutzlast ist.
Installiertes Zertifikat [sn_disco_certmgmt_cmdb_installed_certificate]	
Discovery-Methode [Discovery_method]	Wenn ein Muster dieses installierte Zertifikat erkannt hat, wird im Feld angegeben **Muster** .
Quelle [Quelle]	Die IP-Adresse des Hostservers, auf dem die Discovery ausgeführt wird.
Server [Server]	Der Java-basierte Webserver oder Windows Basierter Webserver, der das Zertifikat in Java-Schlüsselspeichern auf dem Hostcomputer speichert.
Stammaussteller [root_issuer]	Ein Verweis auf den Stammzertifikatdatensatz. Die Referenz ist verfügbar, wenn das ausgestellte Zertifikat Teil derselben Nutzlast ist.

Zertifikatsbestand-Management Begriffe

Das Glossar „Zertifikatbestandsverwaltung“ umfasst eine Reihe von präzisen Definitionen und Erklärungen für Begriffe im Zusammenhang mit der Nachverfolgung, Speicherung und Verwaltung digitaler Zertifikate in einer IT-Umgebung.

Zertifizierungsstelle (CA)

Entität, die ein digitales Zertifikat ausstellt

Zertifikatfingerabdruck

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enthält die eindeutigen Informationen des Zertifikats, zum Beispiel Metadaten

Erkennungsmethode - CA (Zertifikatsbestand-Management Version 1.1.7)

TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden von einer Zertifizierungsstelle wie GoDaddy und DigiCert erkannt.

Erkennungsmethode - Zertifikatimport (Zertifikatsbestand-Management Version 1.1.7)

TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden erkannt, indem die Dateien mithilfe der musterbasierten Erkennung in das System importiert werden.

Erkennungsmethode - Port

TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden an Listener-Ports von Remoteservern erkannt.

Erkennungsmethode - URL

TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden aus URLs erkannt.

Externes Zertifikat

Gibt an, dass das digitale Zertifikat entweder von der Stamm- oder Zwischenzertifizierungsstelle signiert ist

Internes Zertifikat oder selbstsigniert

Gibt an, dass das digitale Zertifikat von derselben Entität signiert ist, deren Identität es zertifiziert. Zum Beispiel sind interne oder selbstsignierte Zertifikate nicht von Stamm- oder Zwischen-CAs signiert.

Transport Layer Security (TLS)

Nachfolgeprotokoll zu SSL. TLS ist eine verbesserte Version von SSL. Es funktioniert ähnlich wie SSL und verwendet eine Verschlüsselung, um die Übertragung von Daten und Informationen zu schützen.

Trust-Manager

Validiert das TLS-Zertifikat

Truststore

Repository zum Speichern von CA-Zertifikaten

Eindeutige und installierte Zertifikate im Vergleich

Eindeutig: Jede eindeutige Instanz bzw. jeder eindeutige Fingerabdruck eines Zertifikats

Installiert: Zeigt an, wo jedes erkannte Zertifikat installiert ist

API-Elemente und -Berechtigungen für Zertifizierungsstellen-Muster

Erkunden Sie die Muster-API-Elemente und -Berechtigungen für Zertifizierungsstellen (CA), um umfassende Einblicke in die zugehörigen Funktionalitäten und Autorisierungsanforderungen zu erhalten.

API-Elemente und Berechtigungen

Zertifizierungsstellen	API-Element
GoDaddy	• * / v1 / Zertifikate • * /v1/certificates/{certificate_id}/download

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Elemente und Berechtigungen (Fortsetzung)

Zertifizierungsstellen	API-Element
DigiCert	• * /services/v2/order/certificate • * /services/v2/certificate/{certificate_id}/chain
Entrust	• * / v2/certificates • * / v2/certificates/{certificate_id}
Sectigo	• * /cert-manager/api/ssl/v1 • * /cert-manager/api/ssl/v1/collect/{certificate_id}/pem

In Zertifikatsbestand-Management Version 1.1.7 stehen folgende Muster zur Verfügung:

- GoDaddy
- DigitCert

In Zertifikatsbestand-Management Version 1.2.0 stehen folgende Muster zur Verfügung:

- Entrust
- Sectigo

Schnellstarttest für Zertifikatsbestand-Management

Schnellstarttest für die Zertifikat-Discovery für GoDaddy, Entrust, DigiCert, Setigo.

Zertifikatsbestand-Management – Schnellstarttest

Test	Beschreibung
Zertifikat-Discovery	Zertifikat-Discovery für GoDaddy, Entrust, DigiCert und Setigo. Discovery holt die Zertifikate und speichert sie in der Tabelle „cmdb_ci_certificate“. Dieser Test validiert die Zertifikate und CIs in den Tabellen „cmdb_ci_certificate“.

Weitere Informationen zu Zertifikatsbestand-Management finden Sie unter Zertifikatsbestand-Management .

Zugehörige Informationen

Schnellstarttests

Discovery Formulartabelle planen

Durchzuführen Discovery Für Stammzertifikate, die außerhalb Ihres Servers gespeichert sind, müssen Sie einen speziellen festlegen Discovery Zeitplan, der diese Zertifikate findet. Diese Tabelle führt Sie durch das für diese Aufgabe erforderliche Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie ein Neu fest Discovery Zeitplan für Zertifikate

Feld	Wert
Name	Name für Ihren Zeitplan.
Erkannt	**Zertifikate**: **Hinweis:** Sobald Sie das Feld Erkennen ausgefüllt haben, wird **Zertifikat-Discovery-Typ** Feld wird angezeigt.
Discovery-Typ des Zertifikats	**Importieren Sie Zertifikate** .
Methode für MID-Server-Auswahl	**Bestimmter MID-Server** .
MID-Server	Die MID-Server Sie möchten diese Discovery durchführen.
Anmeldeinformationsalias	Ihr Anmeldeinformationsalias. Wenn Sie eine einrichten müssen, Verbindungs- und Anmeldealias erstellen .

Neue Zertifikatformulartabelle wird angefordert

Eine Tabelle der Felder zum anfordern eines neuen Formulars.

Neue Zertifikatformulartabelle wird angefordert

Feld	Beschreibung
Zweck des Zertifikats	Intern | Extern Bei der Option Intern müssen Sie das Formular ausfüllen. Optionen sind **Intern** Oder **Extern** . Die Option Extern erfordert, dass Sie die Certificate Signing Request (CSR) und den privaten Schlüssel aus einer externen Quelle wie certificatetools.com importieren.
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	Die CSR wird an die Zertifizierungsstelle (Certificate Authority, CA) gesendet, um das neue Zertifikat anzufordern. Dieses Feld wird automatisch ausgefüllt, wenn Sie auswählen **Möchten Sie CSR generieren?** Kontrollkästchen.
Privater Schlüssel	Privater Schlüssel für das Zertifikat. Dieses Feld wird nur angezeigt, wenn Sie auswählen **Möchten Sie CSR generieren?** Kontrollkästchen und wird automatisch ausgefüllt.
Möchten Sie CSR generieren?	Option zum Generieren einer Zertifikatsignierungsanforderung (Certificate Signing Request, CSR). Wenn diese Option aktiviert ist, muss das CSR-Formular ausgefüllt werden.
Allgemeiner Antragstellername	Bestimmter Entitäts- oder Domänenname, für den das Zertifikat ausgestellt wird. Geben Sie einen Namen oder ein `*` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Zertifikatformulartabelle wird angefordert (Fortsetzung)

Feld	Beschreibung
Alternativer Antragstellername	Domäne oder Unterdomäne, die im allgemeinen Antragstellernamen enthalten ist. Geben Sie einen alternativen Namen oder ein * .
Organisation	Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie die Organisation oder ein * .
Organisationseinheit	Organisationseinheit, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie die Einheit oder ein * .
Ort/Stadt	Ort (Stadt) der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie den Ort oder ein * .
Provinz	Bundesland oder Kanton der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie den Status oder ein * .
Land	Land der Organisation, die die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie das Land oder ein * .
E-Mail-Adresse	E-Mail-Adresse des Administrators in der Organisation, der die Zertifikatsignierungsanforderung für den angegebenen allgemeinen Antragstellernamen stellt. Geben Sie eine E-Mail-Adresse oder ein * .
Anwendungsservices	Anwendungsservices für das Zertifikat.
Server	Server, auf denen das Zertifikat gehostet werden kann.
Anwendungsnamen	Bestimmte Anwendung, für die das Zertifikat ausgestellt wird.
Anwendungsserver	Anwendungsserver, auf denen das Zertifikat gehostet wird.
Zertifikat-Besitzergruppe	Zertifikatbesitzergruppe für das Zertifikat.
Zertifikat-Besitzer	Bestimmte Entität, für die das Zertifikat ausgestellt wird.
Umgebung	Die Umgebung, für die Sie Ihr Zertifikat benötigen. Die Optionen sind: • Entwicklung • Notfallwiederherstellung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Zertifikatformulartabelle wird angefordert (Fortsetzung)

Feld	Beschreibung
	• Produktion • Unterproduktion
Verlängerungsnachverfolgung	Option zum Aktivieren der automatischen Verlängerung Ihres Zertifikats. Diese Option gilt nur, wenn Sie nicht auswählen **Automatisch verlängern** Feld.
Automatisch Verlängern	Option zum Festlegen der Option „Zertifikat automatisch verlängern“.
Wie viele Tage vor Ablauf muss das Zertifikat verlängert werden?	Numerischer Wert. Anzahl der Tage vor Ablauf Ihres Zertifikats, sodass Sie das Zertifikat vor diesen Tagen verlängern möchten.

Service-Mapping

Die Anwendung ServiceNow® Service-Mapping erkennt alle Anwendungsservices in Ihrer Organisation und erstellt eine umfassende Zuordnung aller in diesen Anwendungsservices verwendeten Geräte, Anwendungen und Konfigurationsprofile.

Service-Mapping ist als separates Abonnement erhältlich und erfordert eine Aktivierung durch Service-Mapping-Personal.

Mit serviceorientierten Vorgängen Kontrolle gewinnen

Service-Mapping ermöglicht IT-Abteilungen von Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service bereitstellen, die Erstellung einer serviceorientierten Ansicht der Infrastruktur.

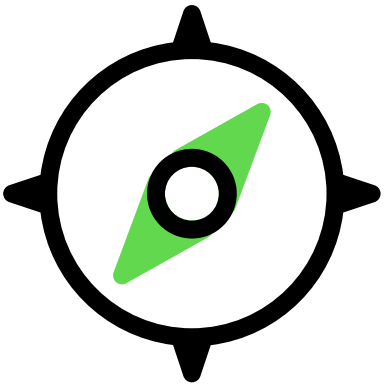
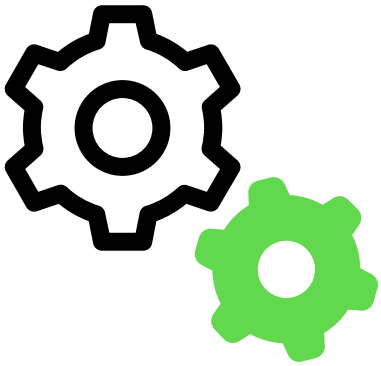
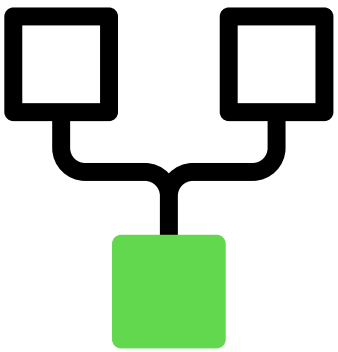
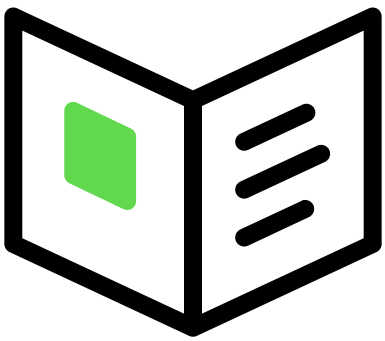
Amortisierungszeit schnell erreichen

Verkürzen Sie den Zuordnungsprozess, und optimieren Sie die Genauigkeit mit sofort einsatzbereiten Optionen. Mit Service-Mapping werden verschiedene Methoden zum Sammeln von Informationen über Konfigurationselemente (Configuration Items, CIs) und über deren Organisation in Anwendungsservices bereitgestellt. Die folgenden Zuordnungsmethoden sind verfügbar: musterbasiert, tagbasiert, datenverkehrsbasiert und erkennungsbasiert auf Basis von Predictive Intelligence.

Multi-Cloud-Strategie umsetzen

Ordnen Sie Services mit hoher Genauigkeit über dynamische cloudbasierte Provider hinweg zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen  Erfahren Sie mehr über die verschiedenen Methoden der Zuordnung von Anwendungsservices.	Konfigurieren  Planen und konfigurieren Sie Ihre Implementierung.	
Verwenden  Überprüfen Sie die Zuordnungsanwendungsservices für Analysen und Wartung.	Referenz  Rufen Sie Details zu Komponenten wie Rollen, Tabellen und Eigenschaften ab.	

Service-Mapping erkunden

Service-Mapping Erkennt alle Serviceinstanzen in Ihrer Organisation und erstellt eine umfassende Übersicht aller in diesen Serviceinstanzen verwendeten Geräte, Anwendungen und Konfigurationsprofile.

Video: Service-Mapping-Übersicht

Dieses Video bietet einen Überblick über Service-Mapping Auf der ServiceNow AI Platform.

Service-Mapping – Benutzer

Service-Mapping ermöglicht IT-Abteilungen von Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service bereitstellen, die Erstellung einer serviceorientierten Ansicht der Infrastruktur.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

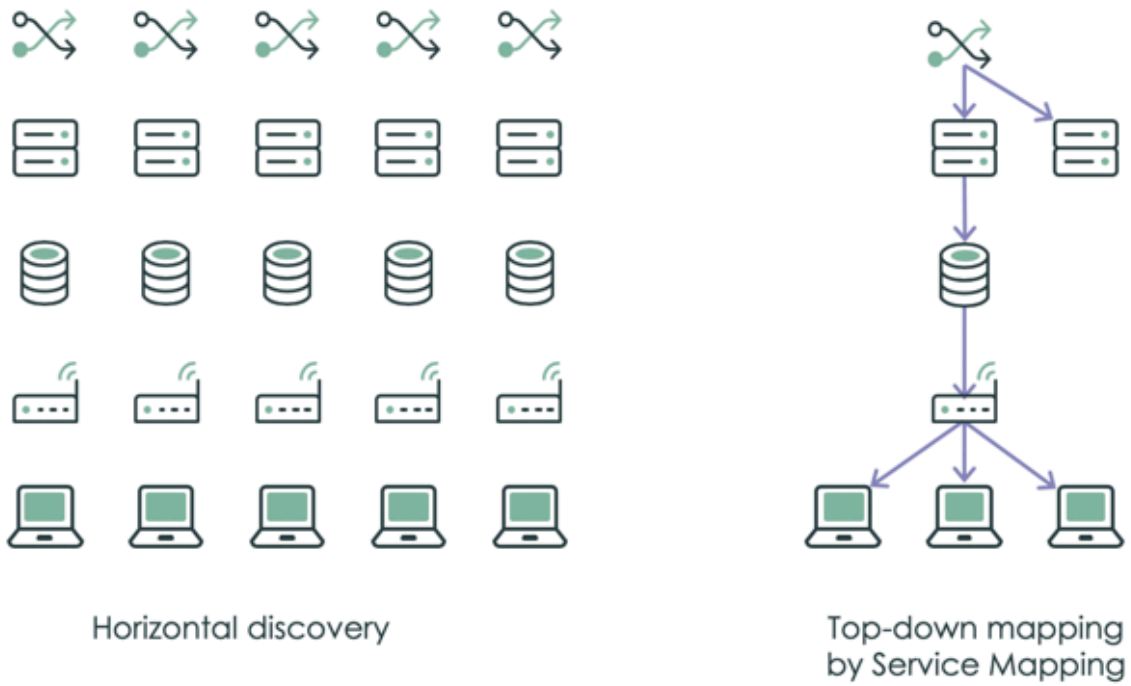
Wie verwenden Sie Service-Mapping?

Eine Serviceinstanz ist ein Satz verbundener Anwendungen und Hosts, die so konfiguriert sind, dass sie der Organisation einen Service anbieten. Serviceinstanzen können intern sein, z. B. ein Organisations-E-Mail-System, oder kundenorientiert, z. B. eine Organisationswebsite. Zum Erstellen von Finanzberichten über eine webbasierte Anwendung sind beispielsweise Computer, Webserver, Anwendungsserver, Datenbanken, Middleware und Netzwerkinfrastruktur erforderlich. Diese Anwendungen und Hosts sind alle so konfiguriert, dass sie den Dienst der Finanzberichterstattung anbieten.

Normalerweise erstellen und verwalten IT-Abteilungen einen Bestand, der Geräte und Anwendungen als eigenständige, unabhängige Objekte behandelt. Verbindungen zwischen Geräten und Anwendungen werden nicht berücksichtigt. Dies wird in der Regel als horizontale Erkennung bezeichnet. Die größte Herausforderung von IT-Abteilungen wird durch diese Methode nicht bewältigt, die darin besteht, die Verbindungen und Abhängigkeiten zwischen den einzelnen Objekten zu verstehen.

Service-Mapping Ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Die Top-Down-Zuordnung hilft Ihnen, die Auswirkungen eines problematischen Objekts auf den Rest des Serviceinstanzvorgangs sofort zu erkennen.

Vergleich der Ergebnisse der horizontalen Zuordnung und der Zuordnung von oben nach unten



Serviceinstanz-Zuordnungen zeigen Infrastrukturobjekte und semantische Verbindungen zwischen ihnen. Service-Mapping generiert Serviceinstanz -Zuordnungen regelmäßig neu, um sie aktuell und relevant zu halten. Alle fehlerhaften Objekte werden zusammen mit den betroffenen Geräten und Anwendungen angezeigt und geben so einen Überblick über den Serviceinstanz -Status.

Wie funktioniert Service-Mapping?

Service-Mapping kann unterschiedliche Methoden zum Erstellen von Anwendungsservices bereitstellen. Die Hauptmethode von Service-Mapping zum Erkennen und Zuordnen von Geräten und Anwendungen ist die Verwendung von Mustern. Ein Muster ist eine Folge von Vorgängen, die zum Erkennen der Attribute von Geräten und Anwendungen und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

deren ausgehenden Verbindungen dienen. Wenn Ihre Organisation Tags für das Asset-Management verwendet, können Sie diese Tags verwenden, um Serviceinstanzen zuzuordnen. Service-Mapping kann Geräte und Anwendungen auch durch Verfolgen der Datenverkehrsverbindungen zwischen ihnen erkennen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet. Weitere Informationen finden Sie unter Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen.

Was Sie wissen müssen, bevor Sie beginnen

Sie können Service-Mapping nur verwenden, wenn das Produkt Discovery aktiviert und eingerichtet ist.

Sie müssen Benutzer definieren und Anmeldeinformationen konfigurieren, um Service-Mapping und Discovery Zugriff auf Anwendungen und Geräte in Ihrem Unternehmensnetzwerk zu ermöglichen. Weitere Informationen finden Sie unter Service-Mapping konfigurieren.

Service-Mapping auf ServiceNow AI Platform

Service-Mapping ist auf Discovery und MID-Server, angewiesen, um Geräte und Anwendungen zu erkennen. Service-Mapping nutzt Ergebnisse der horizontalen Erkennung von Discovery. MID-Server erleichtert die Kommunikation zwischen Service-Mapping und erkannten Geräten und Anwendungen.

Von Service-Mapping gesammelte und organisierte Daten sind in Ereignismanagement, Abhängigkeitsansichten und Anwendungs-Portfoliomanagement (APM) sichtbar. Mit Ereignismanagement können Sie Events anzeigen, um Aktionen zur Wiederherstellung der Anwendungsservices Ihrer Organisation durchzuführen. Abhängigkeitsansichten zeigt Beziehungen zwischen Geräten und Anwendungen im Kontext der Anwendungsservices an, zu denen sie gehören. Wenn Service-Mapping in APM integriert ist, bietet es Informationen zu Komponenten, aus denen eine Geschäftsanwendung besteht, und hilft APM-Benutzern, die Leistung von Geschäftsanwendungen zu überwachen.

Service-Mapping unterstützt Domänentrennung. Wenn in Ihrer ServiceNow AI Platform Domänentrennung eingesetzt wird, können Administratoren und Benutzer nur Anwendungsservices sehen und verwalten, die zu ihrer eigenen Domäne gehören.

Um eine Liste von anzuzeigen Service-Mapping Plugin-Abhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Zugehörige Informationen

- Anwendungsservices
- Ereignismanagement
- Abhängigkeitsansichten

Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen

Service-Mapping stellt verschiedene Methoden zum Sammeln von Informationen über Konfigurationselemente (CIs) und zu deren Organisation in Anwendungsservices bereit. Die folgenden Zuordnungsmethoden sind verfügbar: musterbasiert, tagbasiert, datenverkehrsbasiert und erkennungsbasiert auf Basis von Predictive Intelligence. Erfahren Sie mehr über die Zuordnungsmethoden, um die Methoden auszuwählen, die den Anforderungen Ihres Unternehmens am besten entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsmethode	Beschreibung	Vorteile	Nachteile
Empfehlungen für automatisierte Services	Predictive Intelligence Wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und ordnet ihre Relevanz ein. Service-Mapping Verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Es werden auch Verbindungsvorschläge generiert Für Server und Lastenausgleichsmodule Damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen.	Auf Basis von Verbindungsregeln fügt Service-Mapping automatisch CI-Verbindungen und CIs hinzu, zu denen sie führen. Sie können die Standardverbindungsregeln ändern oder eigene erstellen, um diese Erkennungsmethode zu verbessern. Die Erkennung auf Basis von Predictive Intelligence ist für die Zuordnung mehrerer Anwendungsservices effektiv.	Wenn Sie die Erkennung auf Basis von Predictive Intelligence verwenden, um TCP-Verbindungen und -Prozesse zu identifizieren, stellen Sie sie in großen lokalen Bereitstellungen bereit. Predictive Intelligence ist eine ML-Lösung und erfordert Schulung. Um mit dieser Erkennungsmethode die besten Ergebnisse zu erzielen, müssen Sie die Erkennung wiederholt ausführen. Service-Mapping kann fälschlicherweise dynamische Verbindungen hinzufügen oder entfernen.
Musterbasierte Erkennung	Service-Mapping verwendet Muster zum Erkennen und Zuordnen von CIs. Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Ein typisches Service-Mapping-Muster besteht aus separaten Algorithmen zum Identifizieren von CIs und Ermitteln von CI-Verbindungen.	Die musterbasierte Discovery erstellt präzise und vollständige Serviceinstanzen, die die serviceorientierte Ansicht der IT-Infrastruktur Ihrer Organisation zuverlässig darstellen.	Die musterbasierte Zuordnung erfordert die Konfiguration von Anmeldeinformationen, Benutzern und Benutzerberechtigungen, damit Service-Mapping auf Anwendungen im privaten Netzwerk Ihrer Organisation zugreifen kann. Dieser Prozess kann zeitaufwändig und mühsam sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsmethode	Beschreibung	Vorteile	Nachteile
Tagbasierte Erkennung	Wenn Ihre Organisation Tags für das Asset-Management verwendet, können Sie diese Tags verwenden, um Serviceinstanzen zuzuordnen. Discovery und Cloud Provisioning and Governance erkennen mit CIs verknüpfte Tags und füllen CMDB mit diesen Daten. Service-Mapping verwendet die Tag-bezogenen Daten aus CMDB zum Zuordnen von Services.	Tags eignen sich zur effektiven Zuordnung mehrerer Anwendungsservices. Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.	Serviceinstanzen, die mithilfe von Tags zugeordnet sind, enthalten möglicherweise keine relevanten CIs, wenn diese CIs nicht über die richtigen Tags verfügen.
Datenverkehrsbasierte Erkennung	Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als Traffic-basierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Je nach Konfiguration variiert das Systemverhalten hinsichtlich der datenverkehrsbasierten Erkennung.	Die Verwendung der datenverkehrsbasierten Erkennung ist wie das Auswerfen eines feineren Netzes, mit dem von Service Mapping sogar die CIs gefunden werden, die mithilfe von Mustern nicht erkannt wurden.	Die datenverkehrsbasierte Erkennung führt zwar zu einer inklusiveren Zuordnung, kann aber auch zur Zuordnung vieler redundanter CIs führen, die den Betrieb des Anwendungsservice nicht beeinflussen. Dadurch kann ein Anwendungsservice durch irrelevante CIs unübersichtlich werden. Sie sollten die datenverkehrsbasierte Erkennung in der Anfangsphase der Erkennung eines Anwendungsservice verwenden und sie deaktivieren, sobald Erkennung und Feinabstimmung des Anwendungsservice abgeschlossen sind.

Service-Mapping mit Agent Client Collector

Agent Client Collector Aktiviert die Erkennung und Zuordnung von Anwendungsservices, ohne dass Sie Anmeldeinformationen für einrichten müssen MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Agent Client Collector, Sie können sowohl Top Down als auch maschinelles Lernen bereitstellen Service-Mapping Und profitieren Sie von einem vereinfachten Ansatz für die Zuordnung von Anwendungsservices.

Informationen zum Konfigurieren von Service-Mapping Für die Arbeit mit Agent Client Collector, Siehe Konfigurieren Agent Client Collector Zur Verwendung mit Service-Mapping.

CMDB-basierte Zuordnung

Mit Daten, die in gespeichert sind Configuration Management Database (CMDB), Sie können die Top Down-Discovery ausführen und die Anwendungsservices Ihrer Organisation zuordnen, ohne auf zugreifen zu müssen MID-Server.

Die Top Down-Discovery beginnt mit einer IP-Adresse und ruft den zugehörigen Host ab. Anschließend wird versucht, einen verfügbaren zu finden MID-Server. Wenn ein MID-Server Ist nicht verfügbar, und die CMDB-basierte Zuordnung ist aktiv, sie wird initiiert. Diese Funktion verwendet eingehenden Datenverkehr, der bereits in registriert ist CMDB Um den Zielprozess zu ermitteln, der für eine identifizierte IP-Adresse ausgeführt wird, und nach einer damit verknüpften Anwendung zu suchen. Die Anwendung wird dann als Knoten in der Servicezuordnung zugeordnet.

Wenn eine Anwendung nicht identifiziert wird, verwendet die CMDB-basierte Zuordnung die ADM-Logik (Application Dependency Mapping), um eine Anwendung zu klassifizieren und zu erstellen, die mit dem Zielprozess in verknüpft ist CMDB.

Wenn ADM die Anwendung nicht klassifizieren kann, wird eine einfache Anwendung in der Tabelle „Anwendung“ [cmdb_ci_appl] in erstellt CMDB. Weitere Informationen finden Sie unter Application Dependency Mapping (ADM) für Discovery.

Informationen zum Konfigurieren von Service-Mapping Informationen zur CMDB-basierten Zuordnung finden Sie unter Konfigurieren Service-Mapping Zum Arbeiten mit Configuration Management Database (CMDB).

Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services Vereinfacht die Verarbeitung der Zuordnung von Anwendungsservices oder des Hinzufügens zu einem vorhandenen Service, indem Anwendungsservicekandidaten mithilfe von maschinellem Lernen bereitgestellt werden. Zugeordnete Services bieten wichtige Informationen, mit denen Sie datengesteuerte Entscheidungen treffen, Services priorisieren und auf Situationen reagieren können.

Maschinelles Lernen (ML) verwenden, Service-Mapping Identifiziert schnell potenzielle Anwendungsfingerabdrücke basierend auf erkannten Prozessen. Bewertet die Beziehung zwischen diesen Fingerabdrücken und Konfigurationselementen (Configuration Items, CIs) und erstellt aussagekräftige Verbindungen. Diese Verbindungen werden verwendet, um eine Anwendungsservice-Zuordnung zu erstellen, eine visuelle Darstellung eines Service.

Empfehlungen für automatisierte Services Vereinfacht den Zuordnungsprozess weiter, indem die ML-Informationen zur Berechnung von Einstiegspunkten verwendet werden, wodurch effizient identifiziert wird, wo mit der Zuordnung eines Anwendungsservice begonnen werden soll. Außerdem wird eine Liste von Anwendungsservice-Kandidaten generiert. Jeder Kandidat enthält einen Einstiegspunkt sowie eine Reihe zuvor identifizierter Ressourcen, die in die Servicezuordnung aufgenommen werden sollen. Sie können dann einen Kandidaten auswählen, um einen neuen Anwendungsservice zu erstellen oder einem vorhandenen Service hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Fingerabdrücke

Service-Fingerabdrücke Ergänzungen Empfehlungen für automatisierte Services Durch Identifizierung eindeutiger, klassifizierter Komponenten identifizierter Anwendungsservice-Kandidaten. Die Präsentation dieser Komponenten erleichtert die Auswahl des am besten geeigneten vorgeschlagenen Anwendungsservice. Sie können Komponenten einer Anwendung in Ihrer tatsächlichen Umgebung anzeigen, einschließlich Details wie Produkt, Produktkategorie, Herausgeber und Beschreibung. Verwenden Sie diese Informationen, um nach bestimmten Komponenten zu suchen, die Sie erkennen möchten, oder um fundierte Entscheidungen darüber zu treffen, welche Kandidaten in Anwendungsservices konvertiert werden sollen.

Zu verwenden Service-Fingerabdrücke, Sie müssen herunterladen und installieren ITOM Content Service Von ServiceNow® Store Und aktivieren Sie ITOM Content Service. Weitere Informationen finden Sie unter ITOM Content Service.

Domänentrennung mit Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services Unterstützt Domänentrennung ab Version 1,9.0. Für lokale Instanzen wird derzeit kein Support angeboten. Wenden Sie sich an das Produktmanagement, um weitere Informationen zu erhalten.

Zugehörige Informationen

- Service-Mapping erkunden
- Service-Mapping Arbeitsbereich
- Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich
- Ordnen Sie Anwendungsservices basierend auf zu Empfehlungen für automatisierte Services

Erkennung auf Basis von Predictive Intelligence

Service-Mapping verwendet von Predictive Intelligence verarbeitete Daten, um Vorschläge für datenverkehrsbasierte Verbindungen zu generieren.

Mit Predictive Intelligence generierte Verbindungsvorschläge

Predictive Intelligence Wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und ordnet ihre Relevanz ein. Service-Mapping Verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Es werden auch Verbindungsvorschläge generiert Für Server und Lastenausgleichsmodule Damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen. Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist.

- **Hoch** – Diese Verbindung bezieht sich wahrscheinlich auf eine interne Komponente, die nur von dieser bestimmten Komponente oder Anwendung verwendet wird.
- **Mittel** – Diese Verbindung bezieht sich wahrscheinlich auf eine Middleware-Komponente, die von mehreren Services verwendet wird, z. B. IBM MQ oder Oracle WebLogic-Server.
- **Niedrig** – Diese Verbindung wird wahrscheinlich mit einer Anwendung verbunden, die auf zahlreichen Servern in der Organisation bereitgestellt wird, normalerweise zu Überwachungszwecken, z. B. Tivoli Enterprise Monitoring Agents oder MID-Server.
- **Sehr niedrig** – Diese Verbindung bezieht sich wahrscheinlich auf eine zentrale Anwendung, die von der gesamten Organisation verwendet wird, z. B. Microsoft Active Directory Oder Okta.

Wenn Predictive Intelligence Ist aktiviert, Service-Mapping Fügt automatisch Verbindungen zu Serviceinstanzen basierend auf Verbindungsregeln hinzu. Diese Vorschläge werden mithilfe von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verkehrsbezogenen Daten aus dem generiert Configuration Management Database (CMDB) Und die Analyse von Anwendungsfingerabdrücken, CIs und Prozessen von Predictive Intelligence.

Verbindungsregeln auf Basis von Verbindungsvorschlägen

Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

Wenn Service-Mapping eine Verbindung basierend auf Verbindungsregeln hinzufügt, werden die folgenden Aktionen ausgeführt:

1. Die Verbindungsregel wird dem Verbindungsvorschlag zugeordnet.
2. Das Attribut für *`Decision`* für den Verbindungsvorschlag wird in `Durch Regel hinzugefügt` geändert.
3. Während der erneuten Erkennung von Services wird eine Ebene der tatsächlichen CI-Verbindungen zu relevanten Anwendungsservices hinzugefügt.

Jedes Mal, wenn Anwendungsservices neu erkannt werden, fügt Service-Mapping nur eine Ebene von CI-Verbindungen hinzu. Sie können die Häufigkeit in Ihren Erkennungszeitplänen ändern, um die Zuordnung der Anwendungsservices mithilfe von Verbindungsregeln abzuschließen.

Service-Mapping wertet nur aktive Verbindungsregeln und nur für Verbindungsvorschläge aus, die das Entscheidungsattribut „Unentschieden“ besitzen. Das System wendet die Regeln mit dem folgenden Algorithmus an:

1. Service-Mapping überprüft lokale Regeln auf eine CI-Verbindung. Wenn mehrere Regeln für dieselbe CI-Verbindung relevant sind, verwendet Service-Mapping zur Bestimmung der Reihenfolge das entsprechende Attribut und wertet die Regeln vom niedrigsten zum höchsten Reihenfolgewert aus. Standardmäßig überprüft Service-Mapping nur 20 lokale Regeln.
2. Wenn ein Verbindungsvorschlag mit der Verbindungsregelbedingung übereinstimmt, fügt Service-Mapping diese Verbindung dem entsprechenden Anwendungsservice hinzu.
3. Wenn Service-Mapping keine Übereinstimmung mit lokalen Regeln findet, beginnt das System, globale Regeln in aufsteigender Reihenfolge anhand des Reihenfolgeattributs auszuwerten und anzuwenden. Standardmäßig überprüft das System nur 20 globale Regeln.
4. Wenn ein Verbindungsvorschlag mit der Regelbedingung übereinstimmt, fügt das System ihn den entsprechenden Anwendungsservices hinzu. Wenn eine Regel so konfiguriert ist, dass vorgeschlagene Verbindungen von bestimmten Services ausgeschlossen werden, wendet das System diese Regel nicht auf diese Services an.
5. Jedes Mal, wenn Service-Mapping Anwendungsservices des manuellen oder erkannten Typs neu erkennt, validiert es hinzugefügte datenverkehrsbasierte Verbindungen automatisch anhand der aktiven Verbindungsregeln. Auf diese Weise stellt das System sicher, dass Anwendungsservices nur relevante Verbindungen basierend auf den aktuellen und aktiven Verbindungsregeln enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wenn eine Regel nicht mehr gültig ist, ändert Service-Mapping das Entscheidungsattribut für den entsprechenden Verbindungsvorschlag in „Unentschieden“. Service-Mapping entfernt auch die Zuordnung zwischen der Verbindungsregel und dem Verbindungsvorschlag. Sofern Service-Mapping keine andere Verbindungsregel auf CI-Verbindungen anwenden kann, die irrelevant wurden, entfernt Service-Mapping sie aus den Anwendungsservices.

Bei Bedarf können Sie die Anzahl der lokalen oder globalen Verbindungsregeln ändern, die das System im Algorithmus verwendet (siehe Mit Service Mapping installierte Eigenschaften).

Erkennung auf Basis von Predictive Intelligence aktivieren

Die Erkennung auf Basis von Predictive Intelligence funktioniert auf Produktebene. Gesteuert wird diese Funktion mit der Eigenschaft *sa_ml.connection_suggestions.active*. Wenn die datenverkehrsbasierte Erkennung in Ihrer Bereitstellung vor Release Quebec aktiviert war und Sie damit mindestens einen Anwendungsservice erkannt haben, ist die Erkennung auf Basis von Predictive Intelligence standardmäßig deaktiviert.

Zugehörige Informationen

- CIs für mehrere Anwendungsservices mithilfe von Verbindungsregeln hinzufügen
- CIs für einzelne Anwendungsservices mithilfe von Verbindungsregeln hinzufügen
- CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen
- CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Musterbasierte Erkennung in Service-Mapping

Die musterbasierte Erkennung ist die Hauptmethode von Service-Mapping zum Sammeln von Daten über Geräte und Anwendungen, die in Anwendungsservices verwendet werden. Nachdem Service-Mapping Daten gesammelt hat, wird eine Zuordnung von Anwendungsservices erstellt und die erfassten Daten werden in CMDB gespeichert.

ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

Service-Mapping verwendet Muster zum Erkennen und Zuordnen von CIs. Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Ein typisches Service-Mapping-Muster besteht aus zwei Arten von Algorithmen zum Identifizieren von CIs und Finden von CI-Verbindungen.

Der Ausgangspunkt eines Erkennungsprozesses ist ein Einstiegspunkt. Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Um beispielsweise Ihre Instanz des E-Mail-Services zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt. Der Erkennungs- und Zuordnungsprozess beginnt mit der horizontalen Erkennung durch Discovery, um den Host zu identifizieren. Nach Abschluss der Hosterkennung startet Service-Mapping die Discovery von oben nach unten, um auf diesem Host ausgeführte Anwendungen zu finden und zuzuordnen.

Service-Mapping verwendet MID Servers, um mit CIs in Ihrer Organisation zu kommunizieren. MID Servers befinden sich in Ihrem Unternehmensnetzwerk und Service-Mapping kann mit ihnen kommunizieren, ohne Firewalls zu überwinden.

Hinweis: Mustervorgänge bieten derzeit keine Unterstützung mehrerer Sprachen. Wenn die Werte, die von Mustervorgängen zurückgegeben werden, nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Muster-Discovery schlägt fehl.

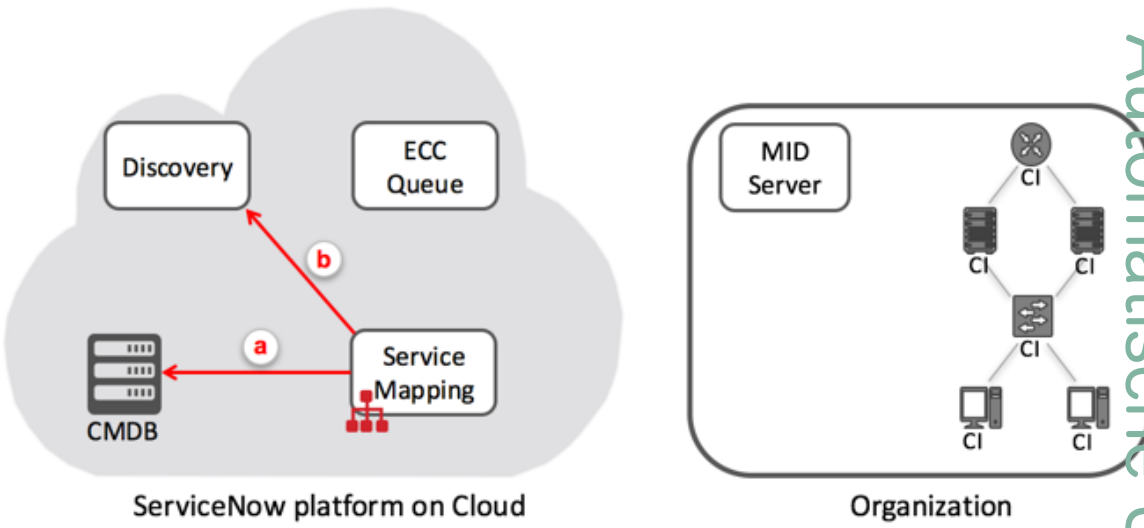
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Erkennungs- und Zuordnungsprozess besteht aus den folgenden Interaktionen:

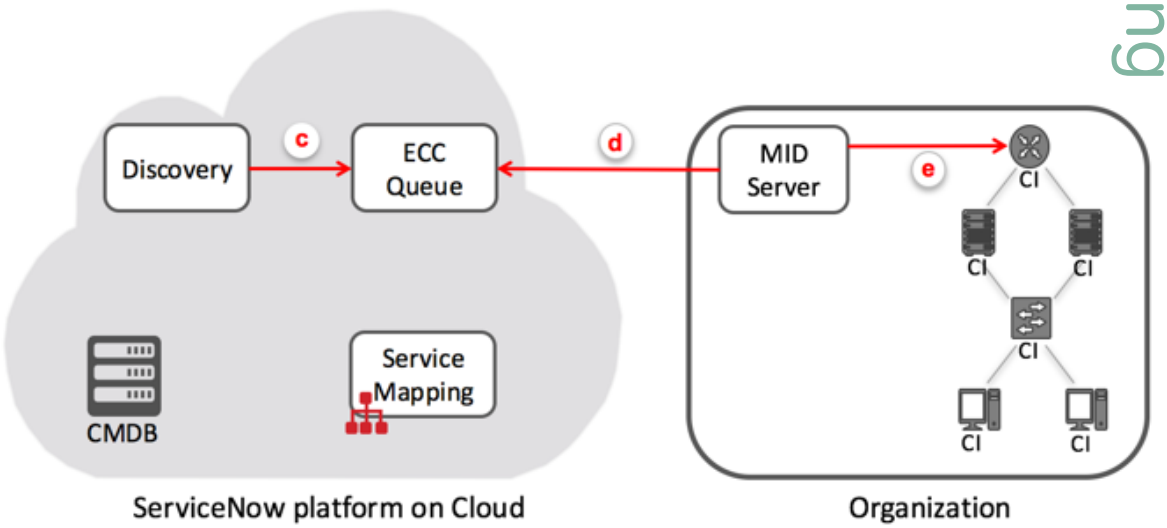
1. Ein Administrator definiert einen Serviceinstanz mit einem Einstiegspunkt für ein Anwendungs-CI.

   Service-Mapping erstellt einen Datensatz für den neuen Serviceinstanz in der Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered].

2. Das Gerät, auf dem die Anwendung gehostet wird, wird identifiziert.
   a. Service-Mapping prüft, ob das Gerät, das dieses Anwendungs-CI hostet, in der CMDB vorhanden ist .
   b. Wenn das Gerät, das diese Anwendungs-CI hostet, nicht vorhanden ist, löst Service-Mapping eine Discovery aus, um den Host zu erkennen.



   c. Discovery erstellt den ersten Satz von Probes für die Porterkennung (die sogenannten Shazzam-Probes) und platziert sie als Erkennungsanforderung in der ECC-Warteschlange (External Communication Channel).
   d. MID-Server Überprüft die ECC-Warteschlange und ruft die ihr zugewiesene Erkennungsanforderung ab.
   e. MID-Server führt die Probes für den Host aus und erkennt offene Ports.

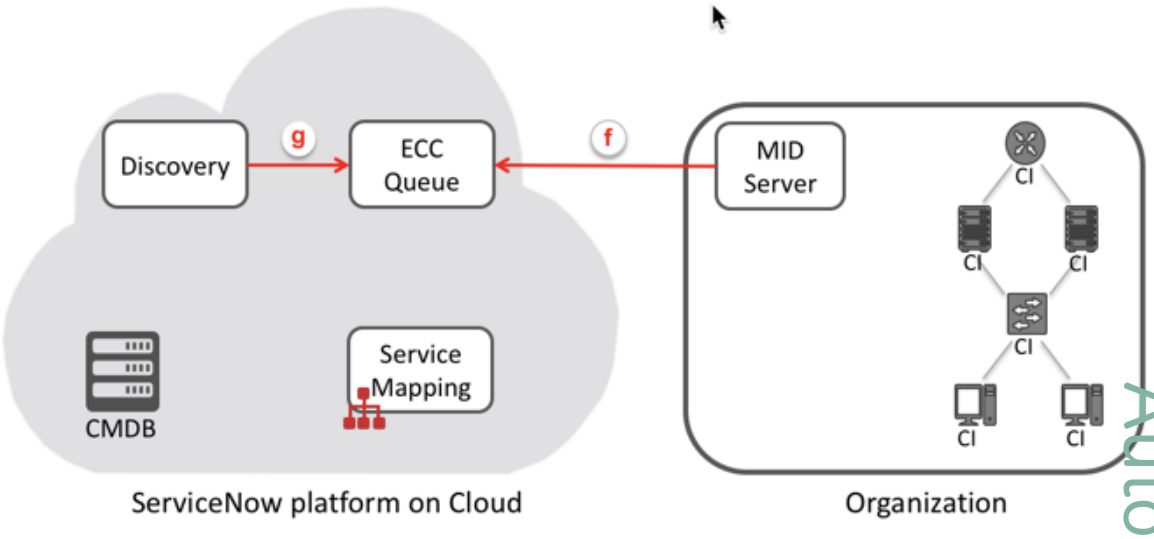


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

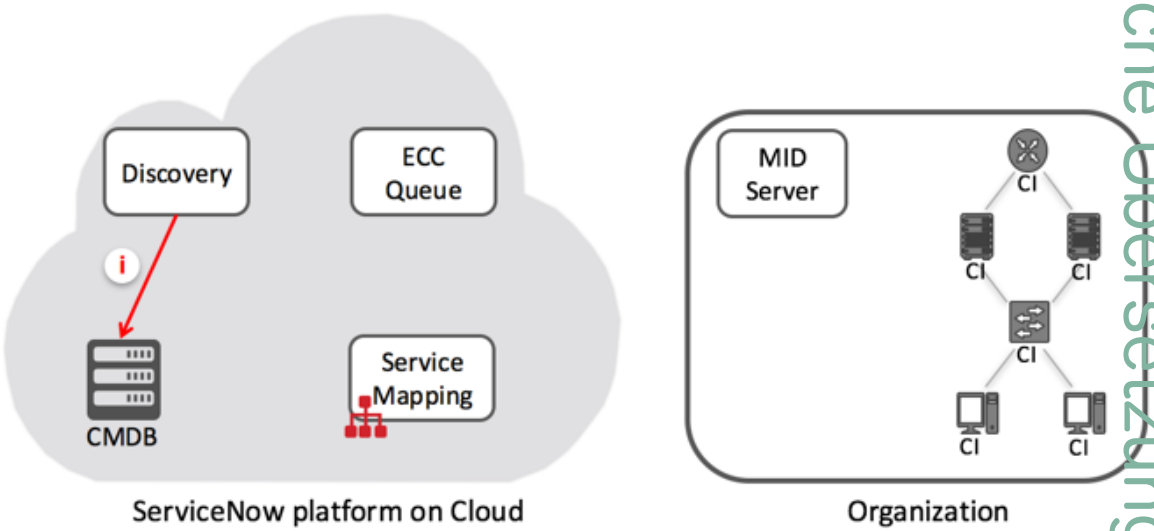
f. Der MID-Server übergibt Informationen über die Hostports an die ECC-Warteschlange.

g. Discovery prüft die ECC-Warteschlange und empfängt Informationen über die Hostports.



h. Diese Schritte werden für andere Probe-Typen wiederholt: Klassifizierung, Identifizierung und Erkundung.

i. Discovery fügt den Host der CMDB hinzu.



j. Während der Hosterkennung mit Probes prüft Service-Mapping die ECC-Warteschlange, ob dieser Prozess abgeschlossen ist. Nach Abschluss der Hosterkennung überprüft Service-Mapping, ob dieser Host in der CMDB vorhanden ist.

Hinweis: Eine detaillierte Beschreibung des Flow der horizontalen Erkennung finden Sie unter Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren.

3. Sobald der Host in CMDB gefunden wurde, erkennt Service-Mapping die auf diesem Host ausgeführte Anwendung.

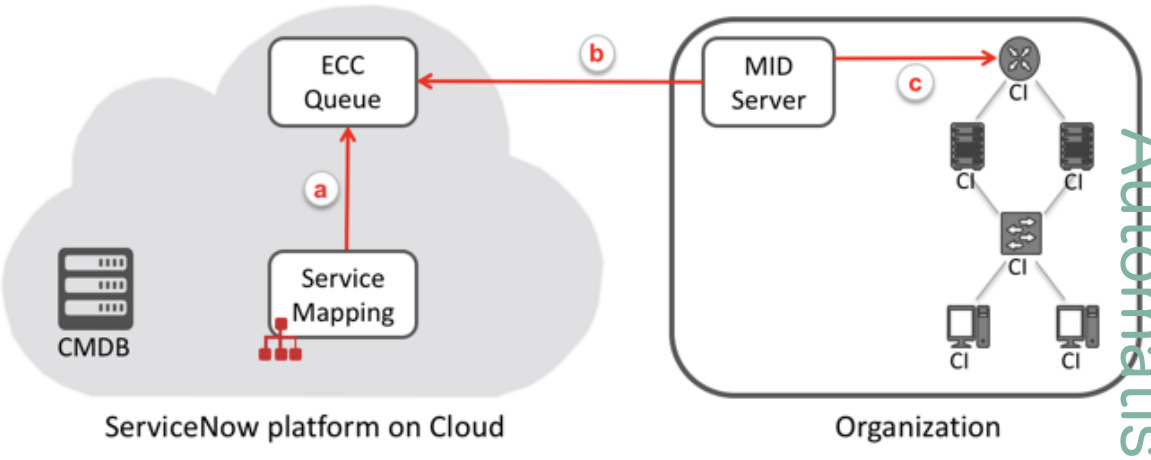
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Service-Mapping erstellt eine Anforderung zur Anwendungserkennung für die IP-Adresse des Einstiegspunkts. Anschließend wird die Anforderung in die ECC-Warteschlange geschrieben und der Anforderung ein MID-Server zugewiesen.

b. MID-Server überprüft die ECC-Warteschlange und ruft die ihr zugewiesene Erkennungsanforderung ab.

c. Der MID-Server beginnt mit der Ausführung von Identifizierungsabschnitten für die Muster, die dem Klassifizierer zugeordnet sind, um eine Übereinstimmung für den Einstiegspunkt zu finden. Wenn der Identifizierungsabschnitt mit dem Einstiegspunkt übereinstimmt, erkennt das Muster ein CI.



d. Der MID-Server beginnt mit der Ausführung von Konnektivitätsabschnitten für das Muster, um ausgehende Verbindungen des neu erkannten CI zu finden.

e. Der MID-Server übergibt Informationen über das erkannte CI und seine Attribute und Verbindungen an die ECC-Warteschlange.

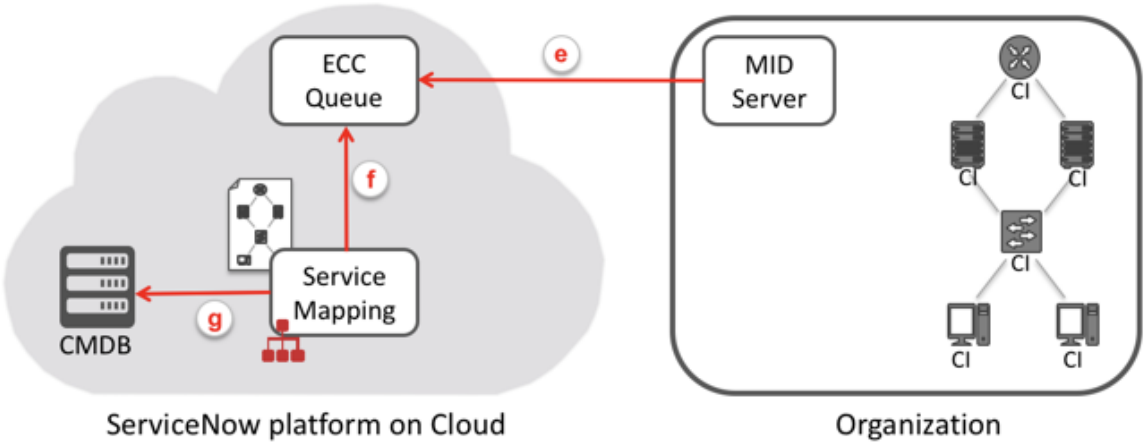
f. Service-Mapping überprüft die ECC-Warteschlange und erhält Informationen über das neu erkannte CI.

Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von den Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

g. Service-Mapping schreibt die Informationen in die CMDB und fügt dieses CI der Serviceinstanz -Zuordnung hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



h. Service-Mapping erstellt die Erkennungsanforderungen für alle Anwendungen, mit denen das neu erkannte CI eine Verbindung herstellt. Die Zuordnung ist abgeschlossen, nachdem Service-Mapping ein CI zugeordnet hat, das entweder keine ausgehenden Verbindungen aufweist oder als Grenze markiert ist. Eine Grenze bewirkt, dass Service-Mapping die Erkennung ab diesem Punkt anhält und ausgehenden Verbindungen nicht folgt.

4. Das System führt regelmäßig eine Neuberechnung des Services durch, um die CMDB nach den neuesten CI-Änderungen abzufragen, Daten für Netzwerk- und Speicherpfade hinzuzufügen und CI-Auswirkungsregeln anzuwenden.

Zugehörige Informationen

ECC-Warteschlange für Discovery

Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren

Datenverkehrsbasierte Erkennung in Service-Mapping

Tag-basierte Discovery in Service-Mapping

Wenn Ihre Organisation Tags verwendet oder sie in einem lokalen einrichtet ServiceNow Instanz können Sie diese Tags verwenden, um Anwendungsservices zuzuordnen.

Ein Tag ist eine Bezeichnung, die aus einem Schlüssel-Wert-Paar besteht. Ihre Organisation kann Tags verwenden, um ihre Assets zu kategorisieren und die Abfragefunktionen und Berichterstellungsfunktionen zu verbessern. Discovery Und Cloud Provisioning and Governance Kann Tags erkennen, die von allen wichtigen Cloud-Anbietern und Container-Ökosystemen verwendet werden. Sobald die Tags erkannt wurden, können von Service-Mapping auf Grundlage dieser Tags Anwendungsservices erstellt werden. In der Regel verwenden Unternehmen Tags in virtualisierten, hyperkonvergenten oder Multi-Cloud-Infrastrukturen.

Beispiel für die Verwendung von Tags in der Organisationsinfrastruktur

Segment	Technologieanbieter	Getaggte Objekte
Cloud	Amazon Web Services(AWS), Azure, Google Cloud Platform(GCP), IBM Cloud Platform	IaaS-, PaaS-, FaaS-, CaaS-Ressourcen
Hyperkonvergent	Nutanix	Virtuelle Maschinen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für die Verwendung von Tags in der Organisationsinfrastruktur (Fortsetzung)

Segment	Technologieanbieter	Getaggte Objekte
Container	Kubernetes, OpenShift Containerplattform, AWS ECS	Container
Virtualisierung	VMware vCenter	Virtuelle Maschinen

Im Gegensatz zu anderen Zuordnungsmethoden ist es bei der tagbasierten Zuordnung nicht notwendig, Anmeldeinformationen zu konfigurieren oder Benutzern erweiterte Rechte zu gewähren. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

Tag-basierte Discovery-Phasen

Der Tag-basierte Erkennung- und Zuordnungsprozess besteht aus den folgenden Phasen:

1. Discovery Und Cloud Provisioning and Governance Erkennen Sie Tags für Cloud- und Ressourcenkonfigurationselemente (CIs), und füllen Sie dann Daten für erkannte Tags in die Tabelle „Schlüsselwert“ [cmdb_key_value] aus.
2. Der Administrator erstellt CI-Tag-Kategorien und definiert Tag-Schlüssel, die in den Kategorien enthalten sind. Tag-Kategorien enthalten Tags mit ähnlicher Verwendung. Wenn Ihre Organisation beispielsweise über Produktions- und Bereitstellungsumgebungen verfügt, können Sie Tag-Werte „Produktion“ und „Bereitstellung“ erstellen.
3. Der Administrator erstellt eine Tag-basierte Servicefamilie und wählt Tag-Kategorien für die Zuordnung aus. CIs, denen mehrere Tags zugewiesen sind, können Teil mehrerer Services sein.
   - Nur CIs mit erkannten Tag-Schlüsseln für die ausgewählten Tag-Kategorien werden Teil von Anwendungsservices.
   - Der Administrator kann die Kriterien einschränken, indem er zusätzlich zu Tag-Kategorien bestimmte Tag-Werte definiert.
   - Service-Mapping Verwendet nur CIs mit übereinstimmenden Werten zum Erstellen von Anwendungsservices.
   - CIs, denen mehr als ein Tag zugewiesen ist, können Teil mehrerer Services sein.

   Hinweis: Wenn Sie eine Servicefamilie zur Zuordnung von Services auf der Grundlage von Tags in einer domänengetrennten Umgebung erstellen, müssen Sie den entsprechenden Endknoten auswählen.
4. Service-Mapping fragt CMDB nach CIs mit Tag-Werten ab, die den Tag-Definitionen für diese Tag-basierte Servicefamilie entsprechen.
5. Service-Mapping erstellt basierend auf den definierten Tags Servicekandidaten.

   Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.
6. Der Administrator wählt die zuzuordnenden Servicekandidaten aus und startet den Zuordnungsprozess.
7. Service-Mapping fügt der Tag-basierten Tabelle der Anwendungsservices [cmdb_ci_service_by_tags] neue Anwendungsservices hinzu.

Wichtig: Serviceinstanzen, die mithilfe von Tags zugeordnet sind, enthalten möglicherweise keine relevanten CIs, wenn diese CIs nicht über die richtigen Tags verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Service-Mapping ordnet Anwendungsservices zu, indem basierend auf CI-Beziehungen Verbindungen zwischen getaggten CIs erstellt werden. Die Tabelle „Durchsetzungsregeln für Anwendungsservices“ [svc_traversal_rules] enthält Informationen zum Erstellen von Tag-basierten Anwendungsservices.

   Hinweis: Service-Mapping enthält CIs, die Teil dieser Beziehungen sind, auch wenn diesen CIs keine Tags zugewiesen sind.

Tag-basierte Services werden erstellt

Mit können Sie einzelne Tag-basierte Anwendungsservices erstellen Gemeinsames Servicedatenmodell(CSDM) Flow wie in beschrieben Füllen Sie Anwendungsservices mithilfe von Tags aus .

Informationen zum Erstellen mehrerer Tag-basierter Services finden Sie unter Ordnen Sie Anwendungsservices mithilfe von Tags mit zu klassisch Service-Mapping.

Zugehörige Informationen

Tag-basierte Discovery-Konfiguration

Tag-Governance

Tag-basierte Discovery für Service-Mapping Arbeitsbereich

Wenn Ihre Organisation Tags für das Asset-Management verwendet, können Sie verwenden Service-Mapping Arbeitsbereich zum Verwalten dieser Tags und Erstellen von Tag-basierten Anwendungsservices.

Ein Tag ist eine Bezeichnung, die aus einem Schlüssel-Wert-Paar besteht, das zum Kategorisieren und Organisieren von Assets in Ihrer Organisation verwendet wird. Tags verbessern die Abfrage- und Berichterstellungsfunktionen und erleichtern die Verwaltung und Nachverfolgung von Ressourcen. Im Gegensatz zu anderen Zuordnungsmethoden ist es bei der tagbasierten Zuordnung nicht notwendig, Anmeldeinformationen zu konfigurieren oder Benutzern erweiterte Rechte zu gewähren. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen. Discovery Und Cloud Provisioning and Governance Kann Tags von allen wichtigen Cloud-Anbietern und Container-Ökosystemen automatisch erkennen. Sobald diese Tags erkannt wurden, Service-Mapping Kann sie nutzen, um Anwendungsservices zu erstellen und zu verwalten. Dieser Ansatz ist für das Ressourcenmanagement in virtualisierten, hyperkonvergierten und Multi-Cloud-Umgebungen nützlich.

Informationen zum traditionellen Tag-basierten Discovery-Prozess finden Sie unter Tag-basierte Discovery in Service-Mapping. Tag-basierte Discovery für Service-Mapping Arbeitsbereich funktioniert unterschiedlich und besteht aus den folgenden Phasen:

Hinweis:

Zugriff auf Tag-basierte Servicezuordnung in Service-Mapping Arbeitsbereich erfordert die Installation von Service-Mapping Plus Version 1.16.3. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

1. Discovery Und Cloud Provisioning and Governance Erkennen Sie Tags für Cloud- und Ressourcenkonfigurationselemente (CIs), und füllen Sie dann Daten für erkannte Tags in die Tabelle „Schlüsselwert“ [cmdb_key_value] aus.
2. Der Administrator erstellt CI-Tag-Kategorien und definiert Tag-Schlüssel, die in den Kategorien enthalten sind. Tag-Kategorien enthalten Tags mit ähnlicher Verwendung. Wenn Ihre Organisation beispielsweise

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

über Produktions- und Bereitstellungsumgebungen verfügt, können Sie Tag-Werte „Produktion“ und „Bereitstellung“ erstellen.

Hinweis: Ab Version 1,7.0, Tag-Governance Bietet fünf vordefinierte Kategorien, die Sie ohne Änderung verwenden können. Administratoren können diese Kategorien auch ändern oder neue hinzufügen.

3. Der Prozess beginnt mit der Auswahl einer Tag-Kategorie aus den verfügbaren Kategorien oder einer vom Administrator erstellten Kategorie.
   - Nur CIs mit erkannten Tag-Schlüsseln für die ausgewählten Tag-Kategorien werden Teil von Anwendungsservices.
   - Der Administrator kann die Kriterien einschränken, indem er zusätzlich zu Tag-Kategorien bestimmte Tag-Werte definiert.
   - Service-Mapping Verwendet nur CIs mit übereinstimmenden Werten, um Anwendungsservices mit der automatisch erstellten Servicefamilie zu erstellen.
4. Service-Mapping Fragt ab CMDB Für CIs mit Tag-Werten, die den Tag-Definitionen für die ausgewählten Kategorien entsprechen.
5. Service-Mapping erstellt basierend auf den definierten Tags Servicekandidaten.
6. Der Administrator wählt die zuzuordnenden Servicekandidaten aus, startet den Zuordnungsprozess und benennt die Tag-basierte Servicefamilie. Dieser Datensatz wird gespeichert, damit der Administrator jederzeit zurückkehren kann, um den Prozess zu überwachen oder später fortzusetzen.
7. Service-Mapping fügt der Tag-basierten Tabelle der Anwendungsservices [cmdb_ci_service_by_tags] neue Anwendungsservices hinzu.

   Wichtig: Serviceinstanzen, die mithilfe von Tags zugeordnet sind, enthalten möglicherweise keine relevanten CIs, wenn diese CIs nicht über die richtigen Tags verfügen.

8. Der Tag-basierte Serviceinhalt wird bei Bedarf berechnet, wenn die Zuordnung zum ersten Mal angezeigt oder manuell initiiert wird.

   Service-Mapping ordnet Anwendungsservices zu, indem basierend auf CI-Beziehungen Verbindungen zwischen getaggten CIs erstellt werden. Die Tabelle „Durchsetzungsregeln für Anwendungsservices“ [svc_traversal_rules] enthält Informationen zum Erstellen von Tag-basierten Anwendungsservices.

   Die Tabelle „Manuelle CI-Ausschlüsse/-Einschlüsse“ [svc_Manual_ci_Exclusions_inclusions] kann CI-Klassen herausfiltern und verhindern, dass sie durch Tags oder Durchlaufregeln hinzugefügt werden.

   Hinweis: Service-Mapping enthält CIs, die Teil dieser Beziehungen sind, auch wenn diesen CIs keine Tags zugewiesen sind.

Zugehörige Informationen

Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich

Ordnen Sie Ihre Anwendungsservices mithilfe von Tags in zu Service-Mapping Arbeitsbereich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenverkehrsbasierte Erkennung in Service-Mapping

Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als Traffic-basierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung.

Datenverkehrsbasierte Zuordnung – Definition

Die Traffic-basierte Zuordnung kann als Erweiterung der musterbasierten Zuordnung betrachtet werden. Während die musterbasierte Zuordnung zur Identifizierung von Verbindungen auf vordefinierten Regeln und Mustern basiert, analysiert die Traffic-basierte Zuordnung den Netzwerkverkehr, um Verbindungen zwischen CIs in Ihrer Umgebung automatisch zu erkennen. Dieser Ansatz ermöglicht es Service-Mapping Um die CIs zu finden, die nicht anhand von Mustern erkannt wurden.

Je nach Konfiguration kann das Verhalten der Traffic-basierten Discovery variieren.
Wenn Predictive Intelligence Ist aktiviert, Service-Mapping Fügt automatisch Verbindungen zu Serviceinstanzen basierend auf Verbindungsregeln hinzu. Diese Vorschläge werden mithilfe von verkehrsbezogenen Daten aus dem generiert Configuration Management Database (CMDB) Und die Analyse von Anwendungsfingerabdrücken, CIs und Prozessen von Predictive Intelligence.

Wenn Discovery auf basiert Predictive Intelligence Ist nicht aktiviert, Service-Mapping Fügt automatisch Traffic-basierte Verbindungen mithilfe von Daten aus dem hinzu CMDB Zu den Serviceinstanzen. Um Ihre Serviceinstanzen jedoch gut organisiert zu halten, müssen Sie möglicherweise Verbindungen zu irrelevanten CIs manuell entfernen.

Wenn die Funktion „Verbindungsvorschläge“ deaktiviert ist, verwenden Sie normalerweise die Traffic-basierte Discovery in den Anfangsphasen der Erkennung von Anwendungsservices. Um eine saubere, organisierte Servicezuordnung zu erhalten, können Sie die Traffic-basierte Discovery deaktivieren, nachdem Sie die Erkennung und Feinabstimmung Ihrer Anwendungsservices abgeschlossen haben. Weitere Informationen finden Sie unter Anwendungsservices feinabstimmen, um Eigentümeranforderungen zu implementieren.

Verbindungen, die nur über die Traffic-basierte Discovery erstellt wurden, werden nicht entfernt. Wenn jedoch die musterbasierte Discovery ausgeführt wird, nachdem die Traffic-basierte Discovery ausgeführt wurde, kann es zu doppelten Verbindungen zwischen CIs kommen. Um Duplikate zu vermeiden, entfernt das System alle Verbindungen, die durch die Traffic-basierte Discovery erstellt wurden, wenn sie auch durch die musterbasierte Discovery erstellt wurden.

Datenverkehrsbezogene Daten aus der CMDB

Im System werden Befehle und Netzwerk-Flow-Protokolle verwendet, um datenverkehrsbezogene Daten zu sammeln und in den CMDB-Tabellen zu speichern. Service-Mapping ruft diese Daten aus den Tabellen ab, um ein- und ausgehende CI-Verbindungen zu erkennen.

Tabellen, die Daten enthalten, die mit Traffic-basierten Methoden erfasst wurden

Tabelle	Quelle	Benutzt von Service-Mapping zum
Flow Connector [sa_flow_connection]	Netflow- und VPC-Protokolle	Erkennen Sie Abhängigkeiten, und fügen Sie Verbindungen während der Top Down-Discovery hinzu.
IP/Port und Statistiken für Flow-Services [sa_flow_service]	Netflow- und VPC-Protokolle	Entdecken Sie alle Services, die Ports überwachen. Im Basissystem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellen, die Daten enthalten, die mit Traffic-basierten Methoden erfasst wurden (Fortsetzung)

Tabelle	Quelle	Benutzt von Service-Mapping zum
		verwendet Service-Mapping keine Daten aus dieser Tabelle.
Ablauf-Serverkommunikation [sa_flow_server_comm]	Netflow- und VPC-Protokolle	Entdecken Sie Services, die mit anderen Services kommunizieren. Im Basissystem verwendet Service-Mapping keine Daten aus dieser Tabelle.
TCP-Verbindung [cmdb_tcp]	netstat- und lsof-Befehle	Verbindungen bei der Top Down-Discovery erkennen.

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden `netstat`, `ss`, Und `lsof`Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration.Um die Traffic-basierte Discovery zu verbessern, können Sie konfigurieren Service-Mapping Dient zum Erfassen von Daten aus NetFlow- und VPC-Protokollen. Service-Mapping Greift auch auf die TCP-Verbindungsdaten zu, die von verbessertem ADM (Application Dependency Mapping) erfasst wurden Discovery Wird als Teil der horizontalen Discovery ausgeführt. Siehe Application Dependency Mapping (ADM) für Discovery Um mehr über diesen Prozess zu erfahren.

Datenverkehrsbasierte Erkennung im System aktivieren

Die Traffic-basierte Discovery mithilfe von Befehlen ist in verfügbar Service-Mapping Zur Verwendung auf jeder Ebene. Sie können es auf verschiedenen Ebenen aktivieren, von den globalsten bis zu den spezifischsten. Weitere Informationen finden Sie unter Aktivieren Sie die Traffic-basierte Discovery für einen Anwendungsservice.

Produktebene

Standardmäßig ist die Traffic-basierte Discovery in Service-Mapping Ist deaktiviert. Die **Traffic-basierte Discovery** (`sa.traffic_based_discovery.active`) Die Eigenschaft steuert die Traffic-basierte Discovery auf dieser Ebene. Das Aktivieren der Traffic-basierten Discovery auf Produktebene erleichtert die Erkennung aller CIs in Ihrer Umgebung. Spezifischere Regeln in der sind jedoch vorhanden Serviceinstanz , CI-Typ oder bestimmte CI-Ebenen können diese Einstellungen überschreiben.

> **Wichtig:** Sie können die Traffic-basierte Discovery nicht auf anderen Ebenen aktivieren, es sei denn, sie ist auf Produktebene aktiviert.

Die Funktion für Verbindungsvorschläge funktioniert auf Produktebene. Gesteuert wird diese Funktion mit der Eigenschaft `sa_ml.connection_suggestions.active`. Wenn Sie die Traffic-basierte Discovery vor aktiviert haben Quebec Release und wurde verwendet, um mindestens einen Anwendungsservice zu erkennen. Die Funktion „Verbindungsvorschläge“ ist standardmäßig deaktiviert.

Serviceinstanz Ebene

Sie können die Traffic-basierte Discovery für eine Person aktivieren Serviceinstanz . In diesem Fall Service-Mapping Verwendet die Traffic-basierte Discovery für alle CIs, aus denen dies besteht Serviceinstanz . Wenn jedoch die Traffic-basierte Discovery für einige CI-Typen oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bestimmte CIs deaktiviert ist, werden diese CIs mit dieser Methode nicht erkannt, auch wenn dies der Fall ist Serviceinstanz Ist auf die Verwendung der Traffic-basierten Discovery festgelegt.

Sie aktivieren beispielsweise die Traffic-basierte Discovery für eine bestimmte Serviceinstanz, die eine enthält Tomcat Server, eine MySQL-Datenbank und eine Webanwendung. Service-Mapping Verwendet die Traffic-basierte Discovery, um zu erkennen Tomcat Server, MySQL-Datenbank und Webanwendung.

CI-Typebene

Sie können in einer Erkennungsregel festlegen, dass ein bestimmter CI-Typ in der datenverkehrsbasierten Erkennung ein- oder ausgeschlossen wird. Diese Regel hat Vorrang vor der Einstellung, die Sie für eine Person auswählen Serviceinstanz .

Sie aktivieren beispielsweise die Traffic-basierte Discovery für eine bestimmte Serviceinstanz, die eine enthält Tomcat Server, eine MySQL-Datenbank und eine Webanwendung. Sie erstellen eine CI-Typregel, die alle ausschließt Tomcat Server aus Traffic-basierter Discovery. Service-Mapping Verwendet die Traffic-basierte Discovery, um die MySQL-Datenbank und die Webanwendung zu erkennen, da keine Regeln zum Ausschließen vorhanden sind.

Spezifische CI-Ebene

Sie können eine Discovery-Regel erstellen, um einen bestimmten CI-Typ aus der Traffic-basierten Discovery einzubeziehen oder auszuschließen. Diese Regel hat Vorrang vor der Einstellung, die Sie für eine Person auswählen Serviceinstanz Oder beliebige Regeln für CI-Typen.

Sie aktivieren beispielsweise die Traffic-basierte Discovery für eine bestimmte Serviceinstanz, die eine enthält Tomcat Server, eine MySQL-Datenbank und eine Webanwendung. Sie erstellen eine CI-Typregel, die alle ausschließt Tomcat Server aus Traffic-basierter Discovery. Sie erstellen jedoch auch eine Discovery-Regel, die die Traffic-basierte Discovery für einen bestimmten aktiviert Tomcat Server. Service-Mapping Verwendet die Traffic-basierte Discovery, um die MySQL-Datenbank, die Webanwendung und diese spezifische zu erkennen Tomcat Trotz der CI-Typregel, die alle ausschließt Tomcat Server.

Siehe Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren Weitere Informationen zum Erstellen von Regeln für CI-Typen oder bestimmte CIs.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Nicht zu Anwendungsservices gehörende CIs entfernen

Datenerfassung und -erkennung mit Netflow

Datenerfassung und -erkennung mit VPC-Flow-Protokollen

Erkennung von Anwendungsservices in der Cloud mithilfe von Service-Mapping

Service-Mapping kann Anwendungsservices erkennen, die aus in der Cloud bereitgestellten Geräten und Anwendungen bestehen.

Es gibt zwei Arten von Cloud-Computing-Methoden, die Ihr Unternehmen verwenden kann: Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS). Service-Mapping erkennt Anwendungsservices basierend auf IaaS auf die gleiche Weise wie alle Anwendungsservices, die auf einer Infrastruktur innerhalb eines privaten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unternehmensnetzwerks basieren. Die Methode nutzt Discovery für die Suche nach Hosts, bevor Anwendungen und Verbindungen zwischen ihnen mithilfe von Mustern erkannt werden. Weitere Informationen zu diesem Discovery-Flow finden Sie unter Musterbasierte Erkennung in Service-Mapping.

Für die vollständige oder partielle Erkennung von Anwendungsservices auf Basis von PaaS wird ein anderes Paradigma benötigt. Anwendungen in solchen Bereitstellungen werden von Netzwerkgeräten in der Cloud gehostet. Um in einer solchen Bereitstellung einen Anwendungsservice zu erkennen, verwenden Sie Discovery und Service-Mapping wie folgt:

- Sie konfigurieren ein Servicekonto für die Cloud-Computing-Plattform, die den Anwendungsservice hostet. Service-Mapping und Discovery verwenden dieses Servicekonto zum Zugriff auf Geräte und Anwendungen auf dieser Plattform.
- Discovery führt die horizontale Erkennung mithilfe von Probes durch und findet die Infrastrukturgeräte in der Cloud.
- Discovery führt die horizontale Erkennung mithilfe von Mustern durch und findet in der Cloud gehostete Anwendungen und Services.
- Service-Mapping führt die Erkennung von oben nach unten durch, um Verbindungen zwischen Geräten und Anwendungen zu finden und die Zuordnung des Anwendungsservice zu erstellen.

Zugehörige Informationen

Cloud-Discovery erkunden

Service-Mapping-Flow

Erfahren Sie mehr über allgemeine Aufgaben, die Benutzer mit unterschiedlichen Rollen in Service-Mapping ausführen.

In Service-Mapping, Arbeiten Anwender zusammen, um die Anwendungsservices einer Organisation zuzuordnen, zu überprüfen und zu überwachen.

Hinweis: Eine vollständige Liste der Rollen in Service-Mapping finden Sie unter Mit Service-Mapping installierte Komponenten.

Ein typischer Service-Mapping-Workflow umfasst die folgenden Phasen:

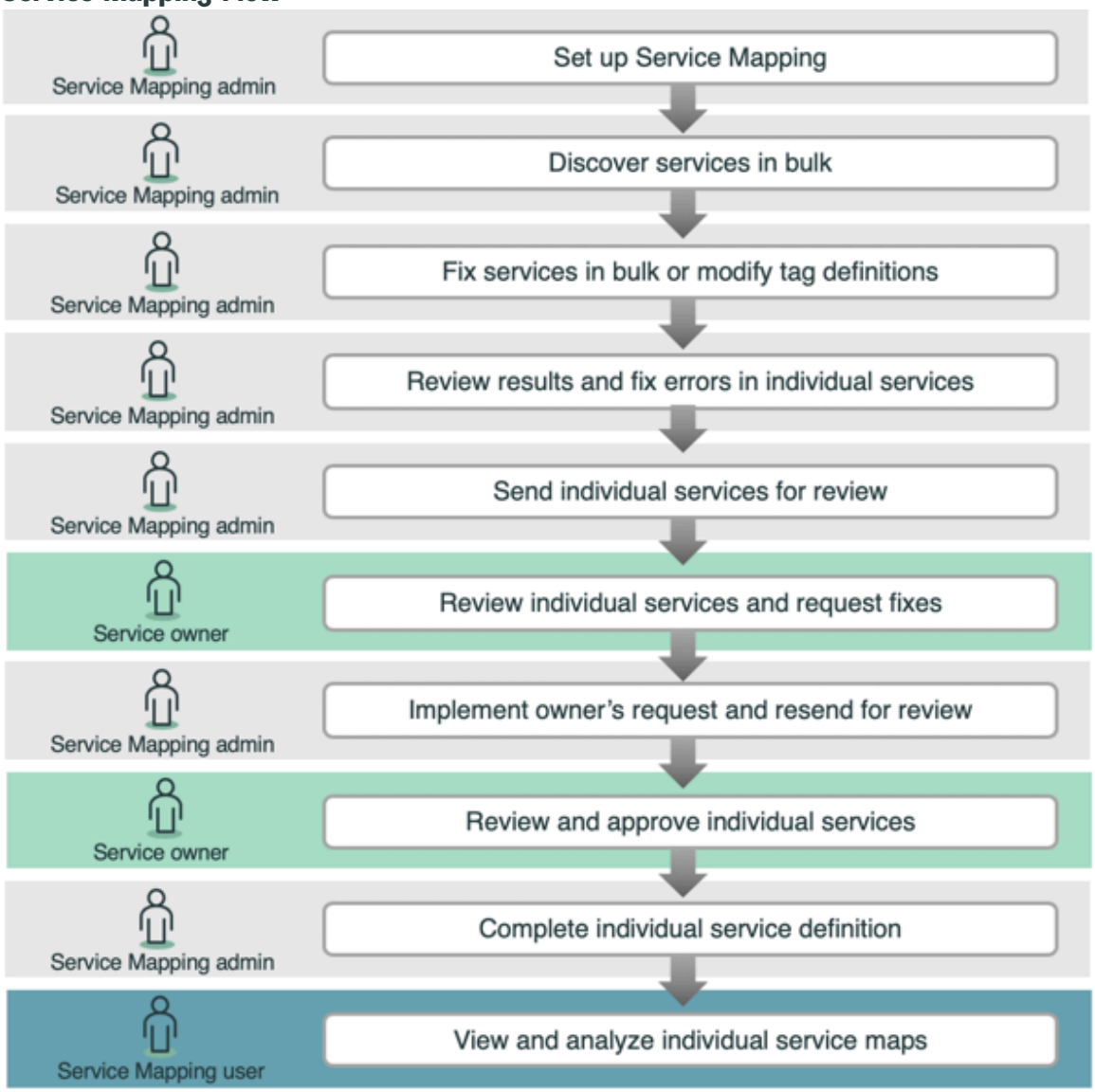
1. Der Administrator führt grundlegende obligatorische Konfigurationen für die Einrichtung durch Service-Mapping. Unter Service-Mapping konfigurieren finden Sie weitere Details.
2. Der Administrator führt die Zuordnung von Anwendungsservices der Organisation als Massenvorgang aus. Darüber hinaus kann der Administrator einige Anwendungsservices einzeln zuordnen. Siehe Ordnen Sie mehrere von vorgeschlagene Anwendungsservices zu klassisch Service-Mapping Weitere Informationen zur Massenzuordnung von Services.
3. Der Administrator behebt Anwendungsservicefehler in Massenarbeit, wie in beschrieben Fehler bei Anwendungsservices als Massenvorgang beheben.
4. Der Administrator überprüft die Ergebnisse der ersten Zuordnung und löst Fehler in einzelnen Anwendungsservices. Unter Fehler in individuellen Anwendungsservicezuordnungen beheben finden Sie weitere Details.
5. Der Administrator sendet die korrigierten Anwendungsservices zur Überprüfung an den Anwendungsservice-Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.
6. Der Besitzer der Serviceinstanz überprüft, ob die Zuordnungen der Serviceinstanz vollständig sind und alle Hauptkomponenten, aus denen sie besteht, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kommentare, die als Ablehnungsnachrichten bezeichnet werden, in Serviceinstanzzuordnungen für die Service-Mapping Zu implementierender Administrator. Siehe Anwendungsservicezuordnungen prüfen.

7. Der Administrator verwendet das Feedback des Anwendungsservice-Besitzers, um die Anwendungsservice-Zuordnungen zu optimieren, und sendet sie dann zur Überprüfung an den Besitzer weiter. Weitere Informationen zur Feinabstimmung einer Anwendungsservice-Zuordnung finden Sie unter Anwendungsservices feinabstimmen, um Eigentümeranforderungen zu implementieren.
8. Wenn die überarbeiteten Serviceinstanzzuordnungen zufriedenstellend sind, genehmigt der Serviceinstanzbesitzer sie. Wenn nicht, fordert der Verantwortliche weitere Fehlerkorrekturen an, die der Administrator umsetzen muss. Siehe Anwendungsservicezuordnungen prüfen.
9. Der Administrator schließt die Anwendungsservices ab, indem er den Zugriff konfiguriert und erweiterte Attribute wie Relevanz festlegt. Weitere Informationen finden Sie unter Fertigstellung des Anwendungsservice.
10. Nach Serviceinstanz Definition ist abgeschlossen, die Service-Mapping Anwender können Anwendungsservice-Zuordnungen anzeigen. Um mehr über die Wartung der Anwendungsservices mit zu erfahren Service-Mapping, Siehe Analyse und Wartung von Anwendungsservices mithilfe von klassisch Service-Mapping.

Service-Mapping-Flow



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzlich zu diesen Aufgaben kann es erforderlich sein, Muster anzupassen, die Service-Mapping verwendet, um Geräte und Anwendungen zu erkennen, die Anwendungsservices bilden. Anwender müssen über die Rolle pd_admin verfügen, um Muster anzupassen. Im Basissystem enthält die Rolle service_mapping_admin die pd_role. Das Anpassen von Mustern erfordert Grundkenntnisse in der Programmierung.

Zugehörige Informationen

Benutzerzugriff auf Anwendungsservices steuern

Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich

Das Dashboard „Tag-basierte Servicezuordnung“ bietet eine intuitive Möglichkeit, Tag-basierte Services zu verwalten. Verwenden Sie die Widgets, Datenvisualisierungen und die Listennavigation, um Ihre Services in wenigen Schritten zu überprüfen und zu aktualisieren oder neue Tag-basierte Services zu erstellen. Das -Dashboard verbessert die Service-Mapping Arbeitsbereich, der eine effiziente und anwenderfreundliche Oberfläche zum Organisieren und Optimieren Ihrer Servicezuordnungen bietet.

Voraussetzungen

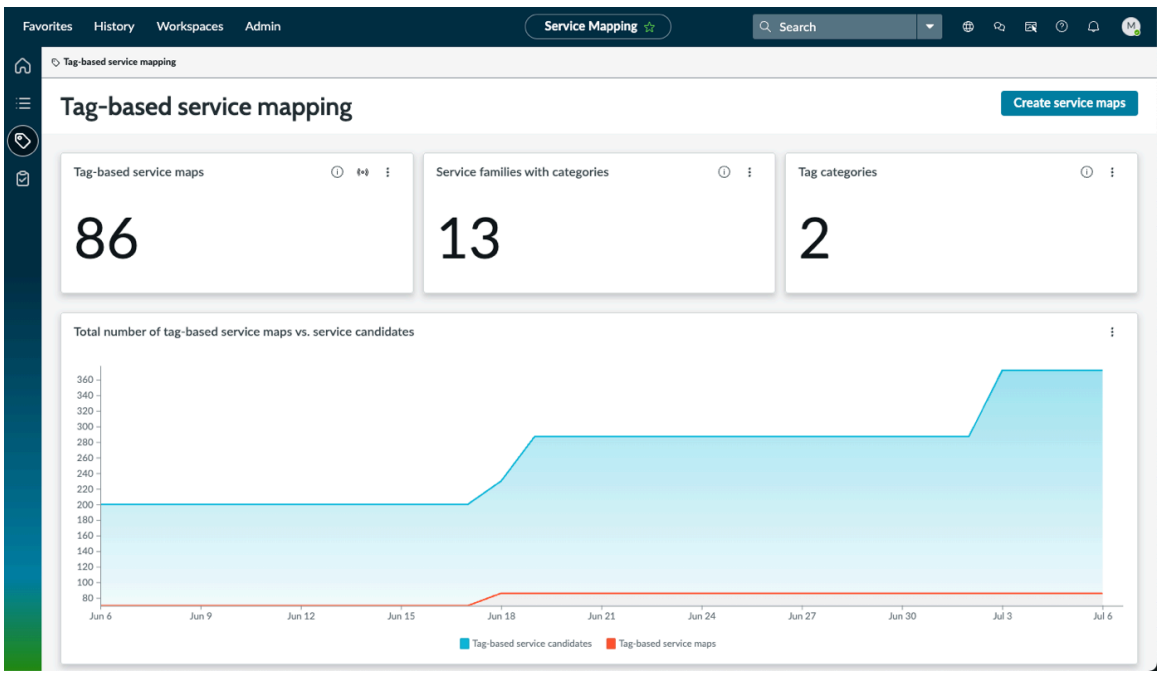
Zugriff auf Tag-basierte Servicezuordnung in Service-Mapping Arbeitsbereich erfordert die Installation von Service-Mapping Plus Version 1.16.3. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Erforderliche Rolle

service_mapping_admin

Zugriff

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Service-Mapping**, Und wählen Sie dann die Tag-basierte Servicezuordnung aus ( ) Symbol im Navigationsbereich.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselmetriken

Wenn Sie in diesem Abschnitt ein Widget auswählen, gelangen Sie zur Liste, um detailliertere Informationen zu erhalten.

Tag-basierte Servicezuordnungen

Die Anzahl der Servicezuordnungen, die mithilfe der Tag-basierten Servicezuordnung erstellt wurden.

Servicefamilien mit Kategorien

Die Anzahl der Servicefamilien, die zum Speichern von Servicekandidaten und Servicezuordnungen erstellt wurden.

Tag-Kategorien

Die Anzahl der Tag-Kategorien, die Tags gruppieren, die eine zugehörige Verwendung haben.

Bericht

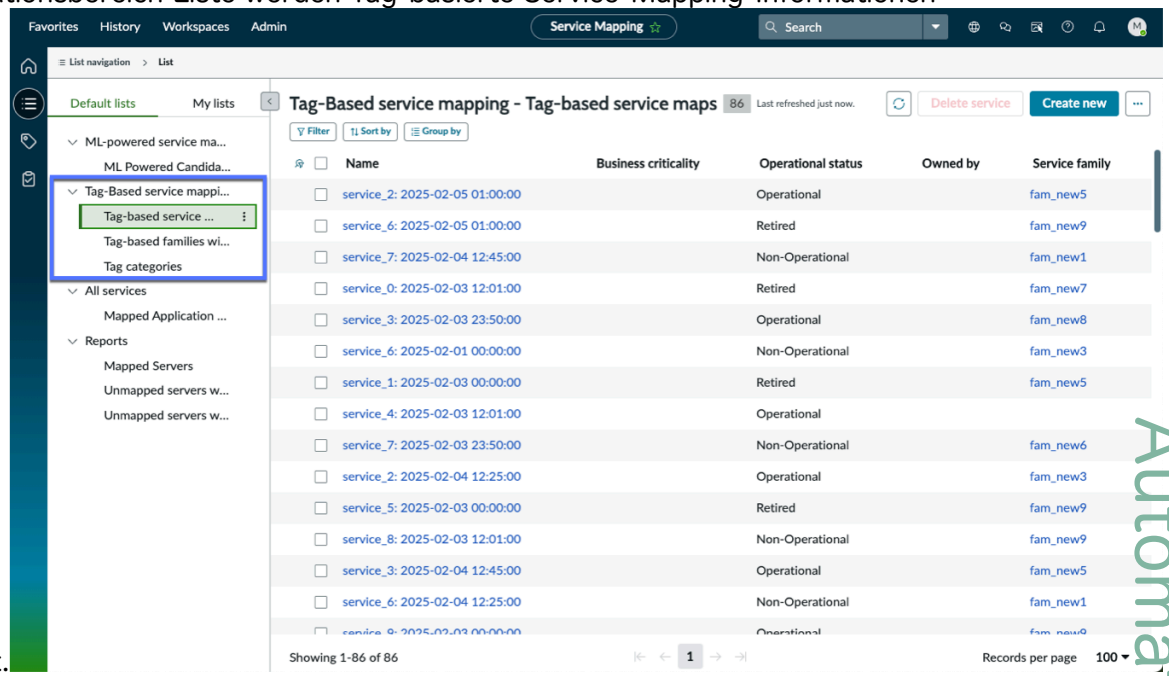
Titel	Typ	Beschreibung
Gesamtzahl der Tag-basierten Servicezuordnungen im Vergleich zu Servicekandidaten	Zweivariables Liniendiagramm	Ein Diagramm, das die Tag-basierten Servicekandidaten und die Tag-basierten Servicezuordnungen zeigt, die an einem bestimmten Tag über einen Zeitraum von 30 Tagen erstellt wurden. Verwenden Sie diese Informationen, um die tatsächliche Anzahl der zugeordneten Services im Vergleich zur Anzahl der erstellten Servicekandidaten zu bewerten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listennavigation

Im Navigationsbereich Liste werden Tag-basierte Service-Mapping-Informationen angezeigt.



Zeigen Sie auf den folgenden Seiten Tag-basierte Informationen an, und greifen Sie auf Tag-basierte Aktionen zu:

Tag-basierte Servicezuordnungen

- Zeigen Sie vorhandene Servicezuordnungen an, oder löschen Sie sie.
- Initiieren Sie den Flow, um einen Tag-basierten Service zu erstellen.

Tag-basierte Familien mit Kategorien

- Zeigen Sie Servicefamilien an, die mindestens eine ausgewählte Kategorie haben.
- Wählen Sie eine Servicefamilie aus, um detaillierte Informationen anzuzeigen, einschließlich zugeordneter Services und Servicekandidaten.
- Initiieren Sie den Flow, um einen Tag-basierten Service zu erstellen.

Tag-Kategorien

- Zeigen Sie vorhandene Tag-Kategorien an, oder löschen Sie sie.
- Wählen Sie eine Tag-Kategorie aus, um detaillierte Informationen anzuzeigen, einschließlich Tag-Schlüssel.
- Initiieren Sie den Flow, um eine Tag-Kategorie zu erstellen.

Domänentrennung

Wenn Sie eine Servicefamilie zur Zuordnung von Services auf der Grundlage von Tags in einer domänengetrennten Umgebung erstellen, müssen Sie den entsprechenden Endknoten auswählen. Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.Wenn Sie Domänentrennung ohne haben Performance Analytics Domänenunterstützung. Sie können keine Datenvisualisierung für die Gesamtzahl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Tag-basierten Servicezuordnungen vs. Servicekandidaten anzeigen. Sie werden dann zur Installation von weitergeleitet Performance Analytics Domänen-Support-Plugin.

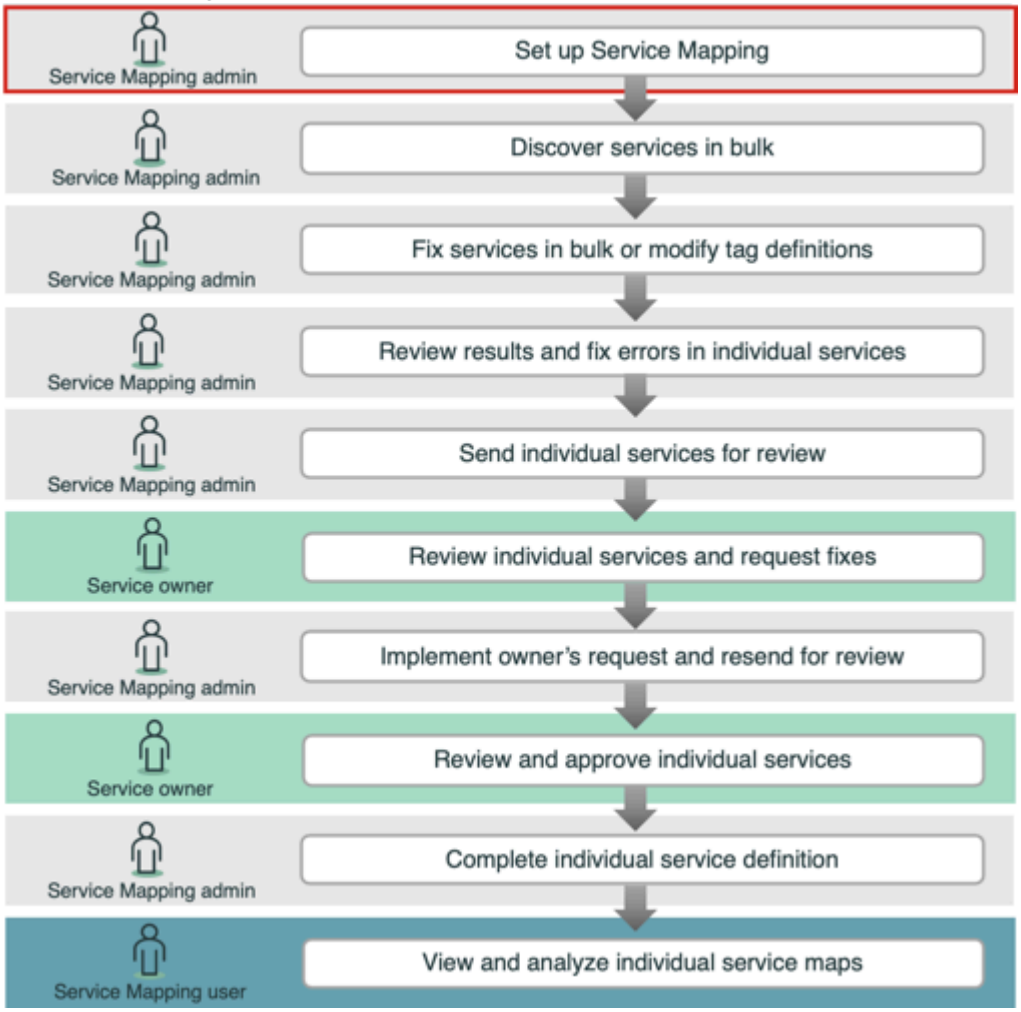
Für weitere Informationen zur Domänentrennung und Service-Mapping, Siehe Domain Separation und Service-Mapping.

Service-Mapping konfigurieren

Der erste Schritt in Service-Mapping besteht darin, Rollen, Anmeldeinformationen und MID-Server-Verbindungen zu konfigurieren.

Das Einrichten von Service-Mapping ist die erste Phase im Workflow von Service-Mapping.

Service Mapping-Workflow



Service-Mapping ist Teil von ServiceNow AI Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Service-Mapping gelten.

⚠ **Warnung:** Das Setup von Service-Mapping für den Advance Release unterscheidet sich von der Standardeinrichtung von Service-Mapping.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Service-Mapping anfordern.
2. Service-Mapping Plus installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

3. Installieren und konfigurieren Sie den MID-Server. MID Servers, die sich im privaten Netzwerk des Unternehmens befinden, erleichtern die Kommunikation zwischen Servern im Netzwerk und einigen ServiceNow-Anwendungen wie Service-Mapping und Discovery. Weitere Informationen finden Sie unter Konfiguration des MID Servers für Service-Mapping.
4. Vergewissern Sie sich, dass Discovery eingerichtet ist und die horizontale Erkennung wie erwartet ausführt.
5. Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen.
6. Konfigurieren Sie die für Service-Mapping erforderlichen Anmeldeinformationen für den Zugriff auf Anwendungen im privaten Netzwerk Ihrer Organisation. Weitere Informationen finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.
7. Wenn das Netzwerk Ihrer Organisation Lastenausgleichsmodule enthält, die auf einem Linux-Host ausgeführt werden, erzeugen Sie ein Erkennungsverhalten für Lastenausgleichsmodule.
8. Ordnen Sie relevanten Benutzern die folgenden Service-Mapping-Rollen zu:

   service_mapping_admin

   Richtet die Service-Mapping-Anwendung ein. Ordnet Serviceinstanzen zu, korrigiert und verwaltet sie. Führt auch eine erweiterte Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.

   service_mapping_user

   Zeigt Zuordnungen für operative Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität und Verfügbarkeit von Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.

   sm_app_owner

   Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_App_owner Anwendern zu, die Serviceinstanzen besitzen und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.

9. Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist an.
10. Wenn Ihre Organisation über eine ServiceNow-Bereitstellung mit benutzerdefinierten Discovery- oder CMDB-Attributen verfügt, führen Sie die zusätzliche Konfiguration durch, die in KB0647574: Preparing customized ServiceNow deployments to work with Service Mapping (Vorbereitung benutzerdefinierter ServiceNow-Bereitstellungen zur Verwendung mit Service Mapping) beschrieben ist.

Zusätzlich zu den hier beschriebenen obligatorischen Setupkonfigurationen müssen Sie möglicherweise zusätzliche Konfigurationen durchführen, nachdem Sie den ersten Zuordnungsprozess abgeschlossen haben. Weitere Informationen finden Sie unter Erweiterte Konfiguration von Service Mapping.

Service-Mapping anfordern

Service-Mapping ist im Rahmen des ITOM-Transparenz-Abonnements verfügbar und erfordert eine Aktivierung durch ServiceNow-Personal.

Vorbereitungen

Erforderliche Rolle: keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Plugins werden automatisch aktiviert, wenn das Service-Mapping-Plugin (com.snc.service-mapping) aktiviert ist:

- Discovery (com.snc.discovery)

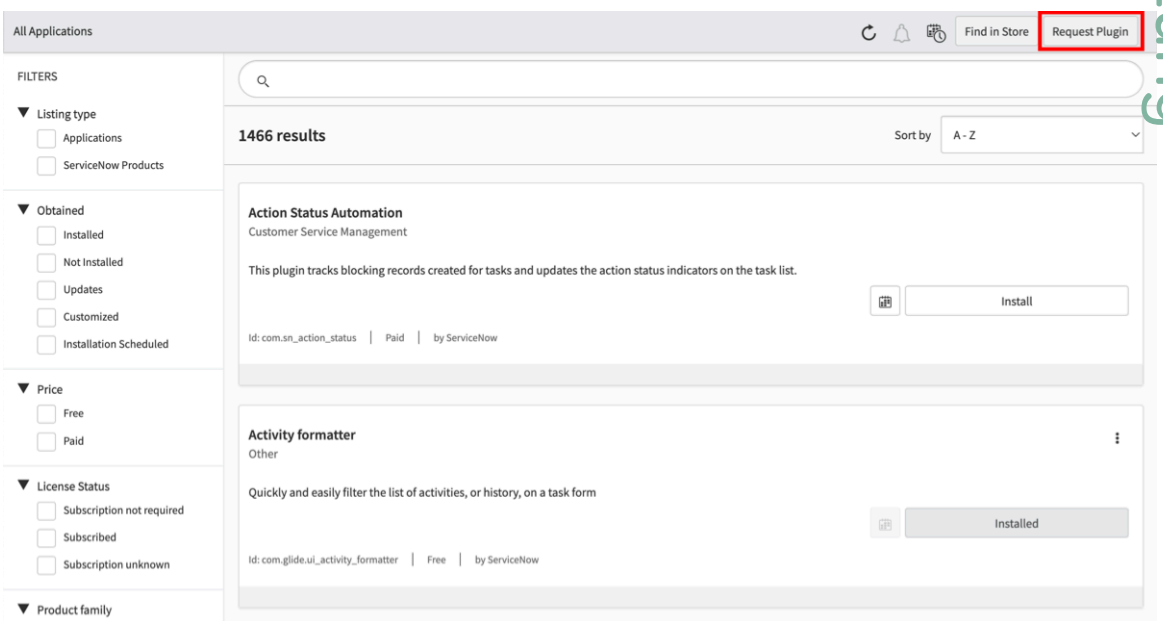
  Hinweis: Bei der erstmaligen Aktivierung des Plugins „Discovery“ im Release Zurich installieren Sie zuerst das Plugin „Discovery“ (com.snc.discovery) und anschließend das Plugin „Muster für Discovery und Service-Mapping“ (com.sn_itom_pattern) in der Version 1.0.52, damit Cloud-Discovery funktioniert. Anschließend können Sie ein Upgrade auf Zurich durchführen.

- Musterdesigner (com.snc.pattern.designer)
- Cloud Provisioning and Governance Core (com.snc.cloud.core)
- Performance Analytics – Content Pack – Service Mapping (com.snc.service-mapping.pa.content)
- Ereignismanagement und Service-Mapping Core (com.snc.service-watch)

  Hinweis: Das Plugin „Ereignismanagement und Service-Mapping Core“ (com.snc.service-watch) unterscheidet sich vom Plugin „Ereignismanagement“ (com.glideapp.itom.snac).

Prozedur

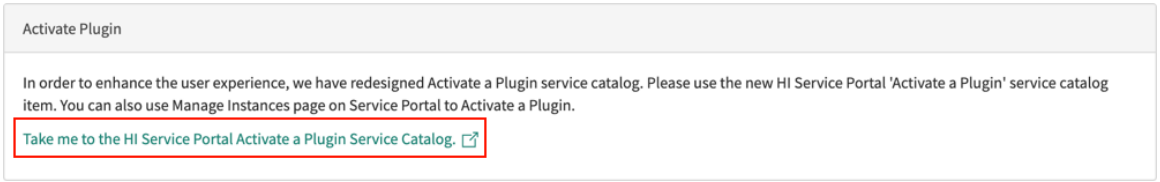
1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

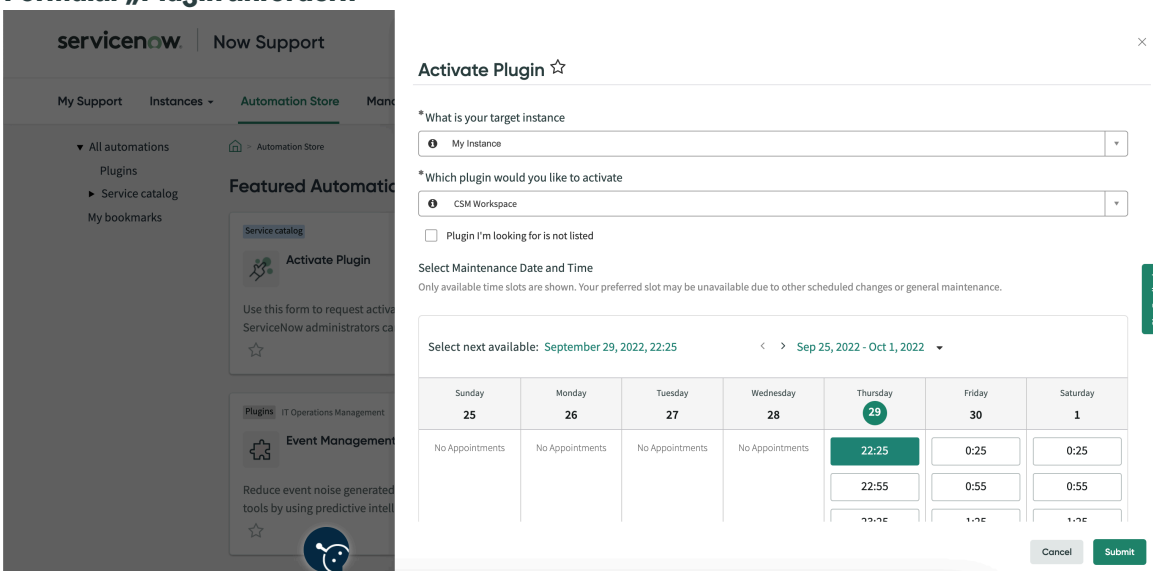
Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Zugehörige Informationen

Für die Hosterkennung erforderliche Anmeldeinformationen

Service-Mapping Plus installieren

Mit der Administratorrolle können Sie die Anwendung Service Mapping Plus (sn_sm_scoped_app) installieren. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie die Anwendungsliste im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Service-Mapping Plus installiert:

- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter Mit Service-Mapping Plus installierte Komponenten.

Um eine Liste von anzuzeigen Service-Mapping Plugin-Abhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie die Anwendung Service Mapping Plus (sn_sm_scoped_app) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Konfiguration des MID Servers für Service-Mapping

Konfigurieren Sie Service-Mapping und MID Servers so, dass sie gemeinsam funktionieren.

Was ist der MID-Server?

Der MID-Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server ausgeführt wird. MID Servers, die sich im privaten Netzwerk des Unternehmens befinden, erleichtern die Kommunikation zwischen Servern im Netzwerk und einigen ServiceNow-Anwendungen wie Service-Mapping und Discovery.

Hinweis: Wenn sowohl das Plugin „Service-Mapping“ (com.sn_itom_pattern) in der Instanz als auch ein Sprach-Plugin (z. B. Spanisch) aktiviert ist, stellen Sie sicher, dass die Sprache für den MID-Server im Benutzerdatensatz ebenfalls auf „English/None“ (Englisch/Keine) festgelegt ist.

MID-Server – Auswahlkriterien

Die meisten Umgebungen erfordern mehrere MID Servers, Mit Service-Mapping Mit dem entsprechenden MID-Server Für Discovery. MID Servers Haben die folgenden Auswahlkriterien Service-Mapping Kann verwenden, um das relevante auszuwählen MID-Server:

- Anwendung – legt fest, mit welcher Anwendung ein MID-Server arbeitet. Stellen Sie es auf Service-Mapping, um diesen MID-Server ausschließlich für Discovery-Anforderungen von Service-Mapping zu reservieren. Alternativ können Sie auf ALL setzen, damit alle ServiceNow-Anwendungen MID-Server verwenden können.

- Fähigkeit – Definiert die Netzwerkfähigkeit. Für Service-Mapping, Legen Sie diesen Parameter auf ALLE oder eine beliebige Kombination aus SSH, WMI, SNMP und fest Cloud Provisioning and Governance . Siehe Konfigurieren Sie die MID-Server-Fähigkeiten .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IP-Bereich – schränkt den Betrieb dieses MID-Server auf diesen IP-Bereich ein. Service-Mapping wählt diesen MID-Server nicht für eine Discovery-Anforderung, deren Endpunkt außerhalb dieses IP-Bereichs liegt.Siehe Konfigurieren Sie einen IP-Adressbereich für den MID-Server .

  Hinweis: Für Informationen zur Umgehung MID-Server Konfiguration basierend auf IP-Bereich, siehe Feinabstimmung Service-Mapping Mit MID-Affinität und IP-Wiederverwendung.

Service-Mapping wählt einen MID-Server mit folgendem Algorithmus aus:

- Service-Mapping wählt den MID-Server aus, dessen Auswahlkriterien am besten mit den Parametern der Discovery-Anforderung übereinstimmen.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien gibt, wählt Service-Mapping den Standard-MID-Server aus.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien und keinen Standard-MID-Server gibt, kann Service-Mapping den Discovery-Prozess nicht starten.

Standardmäßig verwendet Service-Mapping diesen Algorithmus in allen Bereitstellungen, die von Istanbul oder Jakarta aktualisiert wurden, unterstützt jedoch sowohl neue als auch veraltete Algorithmen zur Auswahl eines MID-Server s. Weitere Informationen finden Sie unter MID Server-Auswahlalgorithmus wählen.

Standard-MID Servers für Service-Mapping

Zusätzlich zu den Auswahlkriterien können Sie einen der MID Servers als Standardserver konfigurieren, der Service-Mapping nutzt. Wenn es keine MID Servers gibt, deren Anwendung, Fähigkeit oder IP-Bereich geeignet ist, verwendet Service-Mapping den standardmäßigen MID-Server. Siehe Konfigurieren Sie einen Standard-MID-Server für jede Anwendung .

PowerShell zur Erkennung nutzen

MID Servers können PowerShell für die direkte Kommunikation mit Windows-Servern verwenden, wobei sowohl WMI- als auch WinRM-Protokolle verwendet werden. Für Windows-Services, die das WinRM-Protokoll verwenden, richtet der PowerShell-Prozess eine sichere PSSession ein (PowerShell-Remoting-Sitzung) ein, bis MID-Server die Abfrage eines Windows-Servers beendet. Bei Windows-Servern, die das WMI-Protokoll verwenden, sendet der PowerShell-Prozess jeden PowerShell-Befehl mit Anmeldeinformationen.

Wenn Sie die MID Servers nicht für die Verwendung von PowerShell und PowerShell Remoting konfigurieren, verwenden die MID Servers WMI.

ServiceNow bietet jetzt Unterstützung für PowerShell 3.0 bis 5.1.

MID-Server-Erkennung ohne Anmeldeinformationen mit Nmap

Wenn MID-Server nicht über ausreichende Anmeldeinformationen verfügt, um auf ein Gerät oder eine Anwendung zuzugreifen, kann sie Nmap-Befehle (Network Mapper) ausführen, um grundlegende Informationen ohne Verwendung von Anmeldeinformationen zu erfassen. Die Discovery ohne Anmeldeinformationen mit Nmap erfordert eine zusätzliche Konfiguration, wie in Nmap auf einem MID-Server installieren und deinstallieren beschrieben ist.

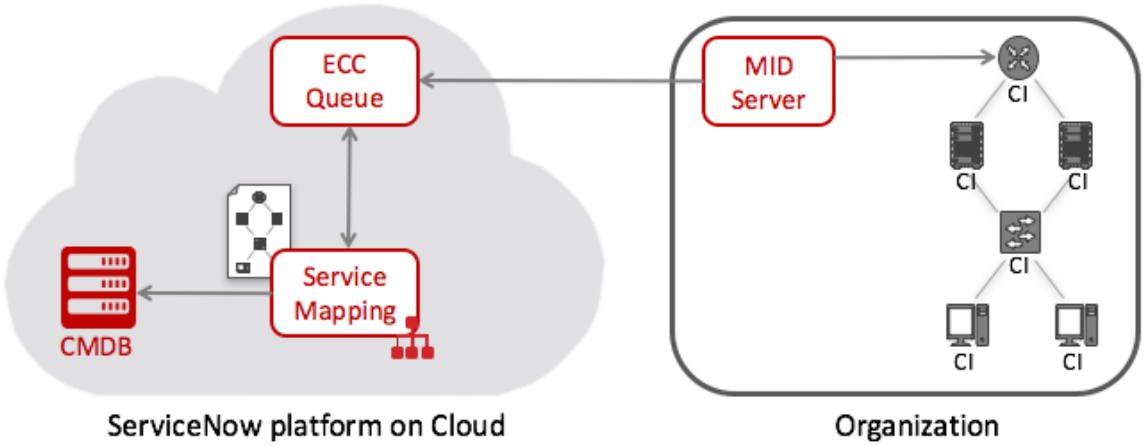
ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID Servers platzieren

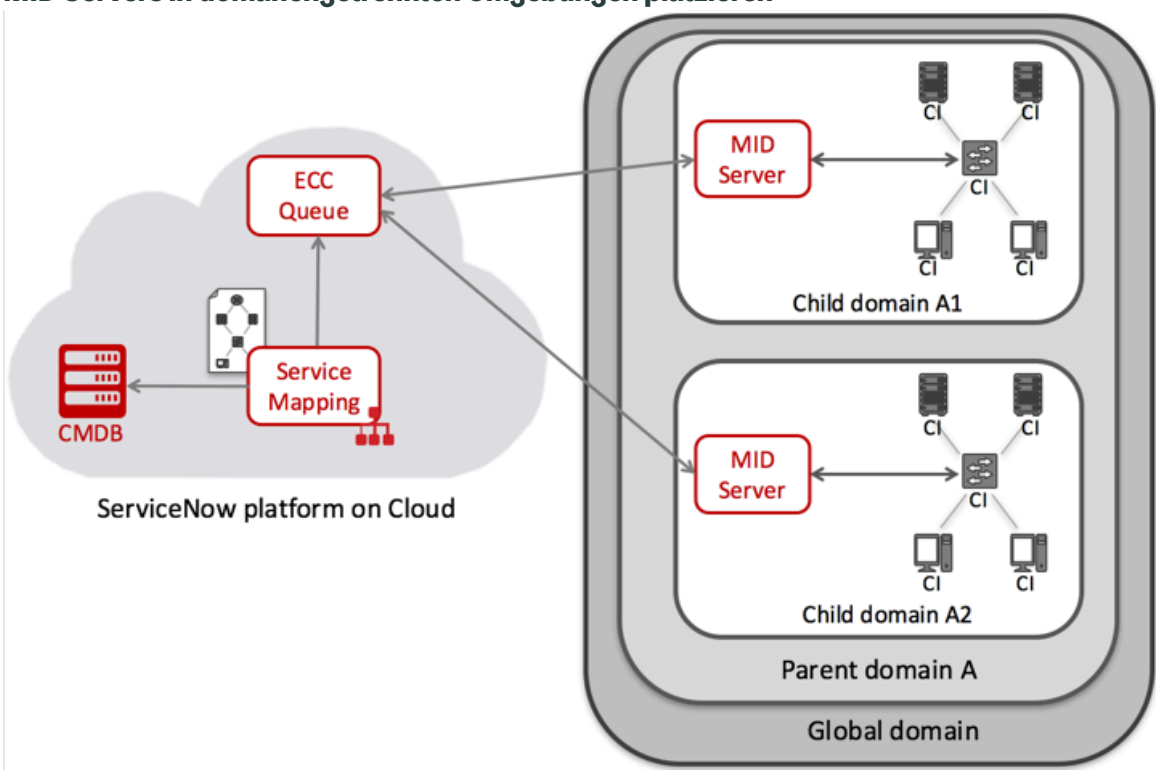
Die Anzahl der von Ihnen benötigten MID Servers hängt von den Anforderungen Ihres Unternehmens ab. Wenn Sie Geräte und Anwendungen in Ihrem privaten Netzwerk zuordnen möchten, platzieren Sie die MID Servers im privaten Netzwerk. Wenn Sie Geräte und Anwendungen in der DMZ zuordnen möchten, platzieren Sie die MID Servers sowohl in der DMZ als auch im privaten Netzwerk.

MID Servers im privaten Netzwerk platzieren



In Bereitstellungen, in denen die Domänentrennung aktiviert ist und Domänen so konfiguriert sind, dass sie eine Hierarchie bilden, müssen MID Servers auf der untersten Domänenebene, einer "Blattdomäne", platziert werden.

MID Servers in domänengetrennten Umgebungen platzieren



Einmal MID Servers MID Servers Sind installiert, konfigurieren Sie sie für die Arbeit mit Service-Mapping Für die besten Discovery-Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

MID Server-Verbindungsvoraussetzungen

Erkennung ohne Anmeldeinformationen mit Nmap

Anwendungserkennung ohne Anmeldeinformationen

Mehrere MID Server-Bereitstellungen

MID Server-Installation

MID-Server-Eigenschaften, die von Service-Mapping verwendet werden

MID Server-Auswahlalgorithmus wählen

Service-Mapping unterstützt die neuen und veralteten Algorithmen zur Auswahl eines MID-Server s für eine Erkennungsanforderung. Den zu aktivierenden Algorithmus können Sie je nach Anforderungen Ihres Unternehmens auswählen.

Vorbereitungen

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping wählt einen MID-Server mit folgendem Algorithmus aus:

- Service-Mapping wählt den MID-Server aus, dessen Auswahlkriterien am besten mit den Parametern der Discovery-Anforderung übereinstimmen.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien gibt, wählt Service-Mapping den Standard-MID-Server aus.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien und keinen Standard-MID-Server gibt, kann Service-Mapping den Discovery-Prozess nicht starten.

Standardmäßig verwendet Service-Mapping diesen Algorithmus in allen Neuinstallationen und Bereitstellungen, die von Istanbul oder Jakarta upgegradet wurden.

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mapping wählt die MID-Server deren Anwendungskriterien auf *`ServiceMapping`* oder *`ALL`* eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.
- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

Standardmäßig verwendet Service-Mapping den veralteten Algorithmus in allen Bereitstellungen, die auf Istanbul und früher upgegradet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**an.
2. So aktivieren Sie den neuen Algorithmus für Bereitstellungen, die auf Istanbul und früher upgegradet wurden:
   a. Deaktivieren Sie das Kontrollkästchen **Alten MID-Auswahlalgorithmus aktivieren**.
   b. Klicken Sie auf **Speichern**.
   c. Konfigurieren Sie die MID-Server-Auswahlkriterien (siehe Konfiguration des MID Servers für Service-Mapping).
3. So aktivieren Sie den veralteten Algorithmus für die Zurich-Bereitstellung:
   a. Aktivieren Sie das Kontrollkästchen **Alten MID-Auswahlalgorithmus aktivieren**.
   b. Klicken Sie auf **Speichern**.
   c. Konfigurieren Sie die MID-Server-Auswahlkriterien (siehe MID-Server-Konfiguration für Service-Mapping in upgegradeten Bereitstellungen).

MID-Server-Konfiguration für Service-Mapping in upgegradeten Bereitstellungen

Für ServiceNow-Bereitstellungen, die von früheren Versionen auf Istanbul upgegradet wurden, verwendet Service-Mapping den veralteten Algorithmus, um den MID-Server für eine Erkennungsanforderung auszuwählen.

MID Servers besitzen die folgenden Auswahlkriterien, anhand derer Service-Mapping in upgegradeten Bereitstellungen einen MID-Server für eine Erkennungsanforderung auswählt:

- Anwendung – legt fest, mit welcher Anwendung ein MID-Server arbeitet. Stellen Sie es auf Service-Mapping, um diesen MID-Server ausschließlich für Discovery-Anforderungen von Service-Mapping zu reservieren. Alternativ können Sie auf ALL setzen, damit alle ServiceNow-Anwendungen MID-Server verwenden können.

  In früheren Versionen konnten Sie MID Servers konfigurieren, um nur mit Service-Mapping über den Parameter `Capability` zu arbeiten. Wenn Sie bei dieser Konfiguration MID Servers hatten, wurde der Anwendungsparameter beim Upgrade auf Istanbul automatisch auf `ServiceMapping` gesetzt.

- IP-Bereich – schränkt den Betrieb dieses MID-Server auf diesen IP-Bereich ein. Service-Mapping wählt diesen MID-Server nicht für eine Discovery-Anforderung, deren Endpunkt außerhalb dieses IP-Bereichs liegt.

Zusätzlich zum IP-Bereich können Sie einen der MID Servers als Standardserver konfigurieren, der Service-Mapping nutzt. Betriebsinformationen finden Sie unter Standardmäßigen MID-Server in Service-Mapping für upgegradete Bereitstellungen konfigurieren.

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mapping wählt die MID-Server deren Anwendungskriterien auf `ServiceMapping` oder `ALL` eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

Im neuen Algorithmus für die Auswahl von MID Servers wird ein zusätzliches Auswahlkriterium verwendet: Fähigkeit. Dadurch kann Service-Mapping ein Netzwerkprotokoll berücksichtigen. Informationen über aktualisierte Auswahlkriterien und den neuen Auswahlalgorithmus für den MID-Server finden Sie unter MID Server-Auswahlalgorithmus wählen.

Standardmäßig verwendet Service-Mapping in allen upgegradeten Bereitstellungen den veralteten Algorithmus, unterstützt jedoch sowohl neue als auch veraltete Algorithmen zur Auswahl eines MID-Server s. Bei Bedarf können Sie den neuen Auswahlalgorithmus MID-Server für Ihre upgegradete Bereitstellung aktivieren. Weitere Informationen finden Sie unter MID Server-Auswahlalgorithmus wählen.

Zugehörige Informationen

IP-Adressbereich für MID Server konfigurieren

Standardmäßigen MID-Server in Service-Mapping für upgegradete Bereitstellungen konfigurieren

In Bereitstellungen, die auf Istanbul oder früher upgegradet werden, verwendet Service-Mapping den standardmäßigen MID Server, wenn kein MID Server mit dem entsprechenden IP-Bereich gefunden werden kann. Durch die Konfiguration eines standardmäßigen MID Servers wird der Erkennungsprozess verbessert.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

Führen Sie dieses Verfahren nur für Bereitstellungen aus, die auf Istanbul oder früher upgegradet wurden. Führen Sie für neue Installationen aus Konfigurieren Sie einen Standard-MID-Server für jede Anwendung .

Stellen Sie sicher, dass Sie den Namen des MID Servers kennen, den Sie als Standard für Service-Mapping konfigurieren möchten.

Warum und wann dieser Vorgang ausgeführt wird

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mapping wählt die MID-Server deren Anwendungskriterien auf *`ServiceMapping`* oder *`ALL`* eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.
- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein, um zu den Systemeigenschaften zu navigieren.
2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie die Werte für die neue Eigenschaft wie folgt:

Eigenschaft	Beschreibung
Name	Geben Sie mid.server.sm_default ein.
Beschreibung	Geben Sie eine Freitextbeschreibung für die Verwendung dieses MID Servers ein.
Typ	Wählen Sie **Zeichenfolge** aus.
Wert	Geben Sie den Namen des MID Servers ein, den Sie für Service-Mapping als Standard konfigurieren möchten.

4. Klicken Sie auf **Aktualisieren**.

Zugehörige Informationen

Konfiguration des MID Servers für Service-Mapping

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Informieren Sie sich über Anmeldeinformationen, Benutzer und Benutzerberechtigungen, die Sie konfigurieren müssen, damit Service-Mapping im privaten Netzwerk Ihrer Organisation Anwendungen erkennen und darauf zugreifen kann.

Konfigurieren Sie die relevanten Anforderungen für eine erfolgreiche Erkennung von oben nach unten:

Hostanmeldeinformationen

Service-Mapping nutzt Hostanmeldeinformationen, um auf Anwendungen zuzugreifen, die auf den entsprechenden Hosts ausgeführt werden. Normalerweise reichen Hostanmeldeinformationen für die Erkennung von oben nach unten aus. Um beispielsweise den HP Service Manager-Anwendungsserver zu erkennen, konfigurieren Sie nur Anmeldeinformationen (SSH-Anmeldeinformationen oder Windows-Anmeldeinformationen) für den Zugriff auf den Server, auf dem diese Anwendung gehostet wird.

Applicative-Anmeldeinformationen

Zur Erkennung mancher Anwendungen benötigt Service-Mapping neben den Anmeldeinformationen des Hosts, auf dem diese Anwendungen ausgeführt werden, noch weitere Anmeldeinformationen. Diese Art von Anmeldeinformationen wird in ServiceNow als Applicative-Anmeldeinformationen bezeichnet. Um beispielsweise ABAP SAP Central Services (ASCS) zu erkennen, konfigurieren Sie zusätzlich zu den Hostanmeldeinformationen auch Applicative-Anmeldeinformationen.

Erweiterte Rechte für Unix-basierte Hosts

Für auf MID Servers konfigurierte Unix-basierte Hosts müssen Sie für alle Unix-basierten Hosts in Ihrer Organisation einem Benutzer Anmeldeinformationen auf sudo-Ebene gewähren. Beispiel: Wenn der ASCS-Hostserver Unix-basiert ist, erteilen Sie einem Benutzer erweiterte Rechte, damit dieser für den Unix-basierten Server Discovery-Befehle ausführen kann.

SNMP-Community Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Berechtigungsnachweise für die SNMP-Community so, dass Service-Mapping und Discovery Netzwerkgeräte mit dem SNMP-Protokoll abfragen können. Konfigurieren Sie für Thunder ADC von A10 Networks beispielsweise SNMP-Community-Anmeldeinformationen.

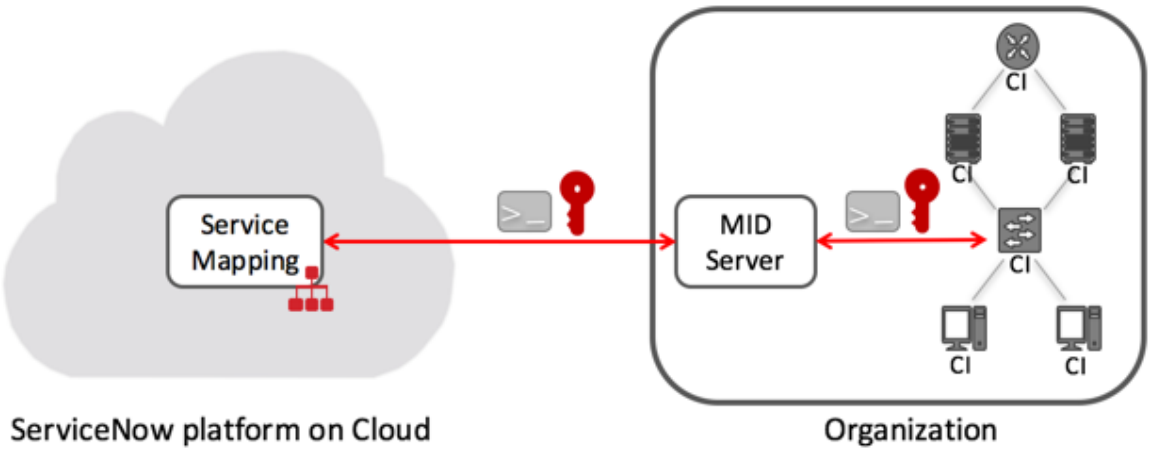
Benutzer oder Benutzerberechtigungen

Möglicherweise müssen Sie zusätzliche Benutzer oder Benutzerberechtigungen angeben, um bestimmte Befehle auszuführen oder auf bestimmte Verzeichnisse zuzugreifen. Erteilen Sie für ASCS zum Beispiel einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion:

ServiceNow AI Platform bietet eine zentralisierte Möglichkeit zum Konfigurieren von Anmeldeinformationen für Discovery, Service-Mapping und andere Anwendungen. Sie können die Anmeldeinformationen für Hosts und Anwendungen nur einmal konfigurieren. Wenn Sie bereits hostbezogene Anmeldeinformationen für eine andere Anwendung konfiguriert haben, müssen Sie dies für Service-Mapping nicht noch einmal tun.

Sie können Anmeldeinformationen bestimmten MID Servers zuweisen oder allgemeine Anmeldeinformationen beibehalten, damit sie von allen MID Servers n verwendet werden können. MID Servers rufen Befehle und Anmeldeinformationen von der ServiceNow Instanz ab und wenden sie an, um CIs im privaten Unternehmensnetzwerk zu erkennen.

Anmeldeinformationen MID-Server n zuweisen, damit diese auf CIs zugreifen können



Verwenden Sie die folgenden Richtlinien, um zu entscheiden, für welchen MID-Server Anmeldeinformationen erstellt werden:

- Wenn alle CIs des gleichen CI-Typs dieselben Anmeldeinformationen nutzen, müssen Sie keinen MID-Server für sie angeben. In diesem Fall werden sie standardmäßig für alle MID Servers verwendet.

  Hinweis: Die Angabe des MID-Server s beim Konfigurieren von Anmeldeinformationen ist optional.

- Wenn CIs desselben Typs und im gleichen Netzwerk unterschiedliche Anmeldeinformationen haben, konfigurieren Sie diese Anmeldeinformationen und definieren die Reihenfolge, in der Service-Mapping sie beim Verbindungsaufbau zu diesen CIs verwendet.

Zusätzlich zu den allgemeinen Anmeldeinformationen, die Sie für die MID Servers konfigurieren, müssen Sie auf allen Unix-basierten Hosts in Ihrer Organisation Anmeldeinformationen auf sudo-Ebene konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn MID-Server nicht über ausreichende Anmeldeinformationen verfügt, um auf ein Gerät oder eine Anwendung zuzugreifen, kann sie Nmap-Befehle (Network Mapper) ausführen, um grundlegende Informationen ohne Verwendung von Anmeldeinformationen zu erfassen. Die Discovery ohne Anmeldeinformationen mit Nmap erfordert eine zusätzliche Konfiguration, wie in Nmap auf einem MID-Server installieren und deinstallieren beschrieben ist.

Überprüfen Sie die Liste der Anmeldeinformationen, die erforderlich sind, um Hosts und Anwendungen zu erkennen, die im Basissystem unterstützt werden.

Applikation	CI-Typ	Konfigurationsschritte
Betriebssystem AIX	AIX-Server [cmdb_ci_aix_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.

IBM z/OS	IBM zOS server-Server [cmdb_ci_ibm_zos_server]	• Führen Sie den USS-Service an Port 22 des z/OS-Servers aus.
		• Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
		• Gewähren Sie dem Benutzer folgende Berechtigungen:
		  ○ Zum Schreiben in das /tmp-Verzeichnis
		  ○ Zum Anzeigen aller Benutzerprozesse
		  ○ Ausführen von REXX-Skripts.

		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
		Gewähren Sie dem Benutzer folgende Berechtigungen: • Zum Schreiben in das /tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Ausführen von REXX-Skripts.
Betriebssystem HP-UX	HPUX-Server [cmdb_ci_hpux_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
Betriebssystem Linux	Linux-Server [cmdb_ci_linux_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
Betriebssystem Solaris	Solaris-Server [cmdb_ci_solaris_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
Betriebssystem Windows	Windows Server [cmdb_ci_windows_server]	Auf der ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		Geben Sie alle unter Für die Hosterkennung erforderliche Anmeldeinformationen beschriebenen erforderlichen Anmeldeinformationen und Berechtigungen an.
A10-Lastenausgleichsmodul	A10 Load Balancer [cmdb_ci_lb_a10]	Konfigurieren Anwendbare Anmeldeinformationen .
		Konfigurieren Sie die SNMP-Anmeldeinformationen .
Windows Azure Active Directory Domain Services	Active Directory-Domänencontroller [cmdb_ci_ad_controller]	Auf der ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
AWS DynamoDB	Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	• Auf der AWS Konsole, gewähren Sie einem Anwender die folgenden Berechtigungen: AmazonDynamoDBReadOnly Access und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		AWSLambdaInvocation-DynamoDB. • Auf der ServiceNow AI Platform®, Konfigurieren AWS Anmeldeinformationen mit einem geheimen Schlüssel und einem Zugriffsschlüssel.
Amazon Web Services (AWS) – Elastic Load Balancing	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Amazon Web Services Anmeldeinformationen.
		In ServiceNow AI Platform: Erstellen Sie ein Servicekonto. Setzen Sie die Konto-ID auf die in der AWS-Managementkonsole angezeigte Konto-ID für Amazon ELB.
Amazon Web Services (AWS) – API-Gateway		Konfigurieren Amazon Web Services Anmeldeinformationen.
		In ServiceNow AI Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der das API-Gateway gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der apigateway:GET-Funktion nur für die GET-Aktion in API Gateway.
		Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.
Amazon Web Services (AWS) – Elastic Compute Cloud (EC2)	Windows-Server [cmdb_ci_windows_server] oder Linux-Server [cmdb_ci_linux_server]	(Wenn auf einem Unix-Server gehostet), auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Windows-Anmeldeinformationen .
		In ServiceNow AI Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der das API-Gateway gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Der MID-Server muss in der Amazon-Cloud platziert sein.
Amazon Web Services (AWS) – Relational Database Service (RDS)	Cloud-Datenbank [cmdb_ci_cloud_database]	Konfigurieren Amazon Web Services Anmeldeinformationen.
		In ServiceNow AI Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Der MID-Server muss in der Amazon-Cloud platziert sein.
Amazon Web Services (AWS) – Lambda	Cloud-Funktion [cmdb_ci_cloud_function]	Konfigurieren Amazon Web Services Anmeldeinformationen.
		In ServiceNow AI Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der AWS Lambda gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.
		Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der ListFunctions-API mit der Ressource: arn:aws:lambda:region:account-id: function:function-name. Gewähren Sie einem Benutzer die Berechtigung zum Ausführen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		der GetFunction-API mit der Ressource: „*“.
Apache Tomcat	Tomcat [cmdb_ci_app_server_tomcat]	Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn auf einem Unix-Server gehostet), auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf einem Windows Server) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Apache Tomcat WAR	Tomcat WAR [cmdb_ci_app_server_tomcat_war]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Wenn gehostet auf UNIX), auf der ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf einem Windows Server) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
Apache-Webserver	Apache-Webserver [cmdb_ci_apache_web_server]	(Unter UNIX) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Erteilen Sie auf dem Server mit dem Apache-Webserver die Benutzerberechtigung zur Ausführung des folgenden Befehls: $APACHEHOME/bin/httpd –V.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Stellen Sie auf dem Server mit dem Apache-Webserver sicher, dass die Datei $APACHEHOME/bin/envvar mit dem richtigen nativen Bibliothekspfad konfiguriert ist.
		(Wenn gehostet auf UNIX), auf der ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf einem Windows Server) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
App TNS-Dienst	[cmdb_ci_appl_ora_tns]	Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn gehostet auf einem Windows Server) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn gehostet auf Linux Oder UNIX), auf der ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
F5 BIG-IP Global Traffic Manager (GTM) und F5 BIG-IP Local Traffic Manager (LTM)	Load Balancer-Service [cmdb_ci_lb_service]	• Um die Mitglieder des Lastenausgleichsmodul-Pools erfolgreich zu erkennen, legen Sie fest **Servicenamen anzeigen** Option (*bigpipe.displayservicenames*) Des Lastenausgleichsmodul bis **Falsch** Auf dem F5-Lastenausgleichsmodul.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• Für F5-Lastenausgleichsmodul-Muster: ◦ Konfigurieren SNMP-Anmeldeinformationen Auf der ServiceNow AI Platform. ◦ (Optional) wenn iRules oder SNMP-Community-Anmeldeinformationen für die Erkennung ausgehender Verbindungen nicht ausreichen, konfigurieren Sie SSH-Anmeldeinformationen . **Hinweis:** Wenn Sie keine SSH-Anmeldeinformationen verwenden möchten, können Sie mit der REST API eine Verbindung zu F5-BIG-IP-Geräten herstellen. Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery. • Für SSH-Muster des F5-Lastenausgleichsmoduls: ◦ Konfigurieren Sie SSH-Anmeldeinformationen . ◦ Überprüfen Sie die Berechtigungen für die folgenden SSH-Befehle: ▪ `Autorisierungspartition aller auflisten` ▪ `Listen Sie globale SYS-Einstellungen auf`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		▪ SYS-Hardware anzeigen ▪ Listen Sie SYS-DB-Failover.State auf ▪ Listen Sie das Eigenkapital einzeilig auf ▪ SYS-mac-address | grep-Schnittstelle anzeigen ▪ Netzschnittstellenfeld-fmt anzeigen ▪ NET Self anzeigen | grep -e „Mac-Adresse“ „IP:“ ▪ ltm-Pool auflisten | grep -e „Pool“ „Modus“ ▪ ltm-Pool auflisten / <partition_name>/* | grep -e „Pool“ „Mode“ ▪ ltm-Pool anzeigen | grep -e „LTM::“ „Verbindungen insgesamt“ ▪ ltm-Pool / <partition_name>/ * |grep -e 'LTM::' 'Verbindungen insgesamt' anzeigen ▪ Listen Sie sys DB bigpipe.displayservicenames | grep-Wert auf ▪ /Net vlan anzeigen | grep -e „Schnittstellenname“ „Mac“ „Tag“ ▪ Virtuelles ltm-Detail anzeigen | grep -e „Server:“ „Status“ „Pool:“ „Ziel“ „Verbindu insgesamt“ ▪ Virtuelle ltm-Details anzeigen / <partition_name>/ * | grep -e „Server:“ „Status“ „Pool:“ „Ziel“ „Verbindu insgesamt“ ▪ gtm-Wideip anzeigen | grep -e „WideIp“ „Status“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		▪ Listenwideip a /<partition_name>/* | grep -e 'WideIp' 'Status' ▪ gtm-Wideip alle anzeigen | grep -e „WideIp“ „Status“ ▪ gtm-Widget auflisten ▪ gtm-Wideip alle auflisten • Für F5REST-Muster: ○ Für horizontale Discovery mit Discovery, Geben Sie schreibgeschützte Berechtigungen zum Ausführen der folgenden APIs an: ▪ „https://“ + $ipAddress + „/mgmt/tm/ltm/Pool“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/global-settings“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/Hardware“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/Failover“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/Self“ ▪ „https://“ + $ipAddress + „/mgmt/tm/ltm/Virtual?$select=destination,mask,vlans“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/Interface“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/interface/stats“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/Trunk“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/vlan“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		▪ „https://“ + $ipAddress + „/mgmt/tm/net/vlan/“+<vlan id> +“/interface“ ▪ „https://“ + $ipAddress + „/mgmt/tm/gtm/wideip“ ▪ „https://“ + $ipAddress + „/mgmt/tm/cm/Traffic-Group/“ ▪ „https://“ + $ipAddress + „/mgmt/tm/cm/device“ ○ Erstellen Standardauthentifizierung Anmeldeinformationen. • Für F5 REST OAuth 2,0-Authentifizierungsmuster: ○ Überprüfen Sie die schreibgeschützte Berechtigung für die folgenden APIs: ▪ „https://“ + $ipAddress + „/mgmt/Shared/authn/login“ ▪ „https://“ + $ipAddress + „/mgmt/tm/ltm/Pool“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/global-settings“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/Hardware“ ▪ „https://“ + $ipAddress + „/mgmt/tm/sys/Failover“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/Self“ ▪ „https://“ + $ipAddress + „/mgmt/tm/ltm/Virtual?$select=destination,mask,vlans“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/Interface“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/interface/stats“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		▪ „https://“ + $ipAddress + „/mgmt/tm/net/Trunk“ ▪ „https://“ + $ip_address + „/mgmt/tm/net/vlan“ ▪ „https://“ + $ipAddress + „/mgmt/tm/net/vlan/“+<vlan id> +“/interface“ ▪ „https://“ + $ipAddress + „/mgmt/tm/gtm/wideip“ ▪ „https://“ + $ipAddress + „/mgmt/tm/cm/Traffic-Group/“ ▪ „https://“ + $ipAddress + „/mgmt/tm/cm/device“ ○ Erstellen Standardauthentifizierung Anmeldeinformationen. ○ Erstellen Ein Anmeldeinformationsalias Für die Anmeldeinformationen für die Standardauthentifizierung. ○ Erstellen Sie einen serverloser Discovery-Zeitplan . • Geben Sie für die Top Down-Discovery mit Service-Mapping Berechtigungen zum Ausführen der folgenden APIs an: ○ https://" get_attr {"managementIP"}"/mgmt/tm/ltm/"get_attr {"irule"} ○ https://" get_attr {"managementIP"}"/mgmt/tm/ltm/Virtual/~Common~"get_attr {"vip_Name"} ○ https://" get_attr {"computer_system.managementIP"}"/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		mgmt/tm/ltm/pool/"get_attr {"pool_name"}"/members? • (Optional) Für die Top Down-Discovery mit Service-Mapping, konfigurieren Sie Applicative-Anmeldeinformationen . • (Optional) Für die Top Down-Discovery mit Service-Mapping, stellen Sie einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle bereit: ○ Bigpipe-Befehle (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 9) ○ Bigpipe- und Traffic Management Shell-Befehle (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10) ○ TMSH-Befehle (Traffic Management Shell) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 11) ○ Erweiterte Befehle für die Traffic Management Shell (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10, 11 und 12) ○ Der *show cm traffic-group – get command* für die Erkennung von F5 BIG-IP Device Service Clustering • (Optional) Für die Top Down-Discovery mit Service-Mapping , geben Sie dem Benutzer erhöhte Rechte, damit er Service-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
BMC CTRL-M Enterprise Manager	Control-M [cmdb_ci_appl_controlm]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn unter Linux oder gehostet UNIX Server) (optional) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
BMC CTRL-M Gateway	Control-M [cmdb_ci_appl_controlm]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn unter Linux oder gehostet UNIX Server) (optional) auf dem ServiceNow AI Platform, Konfigurieren Sie cc.
BMC IT Asset Management (ITAM)	ITAM Asset Center [cmdb_ci_appl_itam]	Auf der ServiceNow AI Platform, Konfigurieren Sie ein Windows BS-Anwender mit Berechtigungen zum Zugriff auf die ITAM-Registrierung wie in beschrieben Windows-Anmeldeinformationen .
CA Identity Manager-Bereitstellungsserver	CA Identity Manager-Bereitstellungsserver [cmdb_ci_appl_ca_id_man]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Cadebill Interconnect	Interconnect [cmdb_ci_inter_connect]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
Cadebill Interconnect-Instanz	Interconnect-Instanz [cmdb_ci_interconnect_instance]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
Cisco Application Control Engine ACE (unter Cisco CSM)	ACE [cmdb_ci_lb_ace]	Auf der ServiceNow AI Platform, Konfigurieren Anwendbare Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
		Auf der ServiceNow AI Platform, Konfigurieren Sie die SNMP-Community-Anmeldeinformationen wie in beschrieben SNMP-Anmeldeinformationen .
Cisco CallManager	Cisco CallManager [cmdb_ci_appl_cisco_call_man]	(Wenn gehostet auf einem Linux Oder UNIX Server) (optional) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf einem Windows Server) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
Cisco Global Site Selector (GSS)	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Sie die SNMP-Community-Anmeldeinformationen wie in beschrieben SNMP-Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
		Geben Sie einen Benutzer an, der zum Ausführen der Abfrage für die Domänenliste, die DNS-Regelausgabe und die VIP-Antwort

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		berechtigt ist, um die ausgehenden Verbindungen von GSS abzurufen.
Citrix Delivery Controller	Delivery Controller [cmdb_ci_appl_delivery_controler]	• Konfigurieren Sie die Windows-Anmeldeinformationen, um auf den Hostcomputer zuzugreifen. • Stellen Sie sicher, dass PowerShell für Discovery auf Ihren MID Servern installiert ist. Für die für die Citrix-Discovery verwendeten Muster müssen PowerShell-Befehle ausgeführt werden können. • Für Betriebssystembenutzer müssen Sie „Get-XDSite“ ausführen. Der Citrix Studio-Administrator muss Berechtigungen erteilen. • (Optional) Für die Top Down-Discovery mit Service-Mapping installieren Sie auf dem Citrix Delivery Controller das Modul Citrix.Broker. • (Optional) Für die Top Down-Discovery mit Service-Mapping, erstellen Sie einen Benutzer mit Berechtigung zum Ausführen von PowerShell-Befehlen. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.
Citrix-Nutzungssammler	Citrix Collector [cmdb_ci_appl_citrix_collector]	• Konfigurieren Anwendbare Anmeldeinformationen. • Konfigurieren Sie einen Benutzer mit Berechtigungen zum Ausführen von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		PowerShell-Befehlen auf dem Citrix-Server. • (Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen . **Hinweis:** Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_collector fest. • Gewähren Sie zum Erkennen von Epic die Berechtigung zum Ausführen des Befehls afarm. • Erteilen Sie einem Benutzer die Berechtigung zum Lesen und Abfragen des Citrix-Repository: ○ Bei Versionen 4.5 und höher ein PowerShell-Skript vom XenApp-Server. ○ Für Versionen vor 4.5 ein Microsoft Visual Basic Script (VBScript) vom Citrix-Präsentationsserver • (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		ServiceNow AI Platform SSH-Anmeldeinformationen . **Hinweis:** Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut `Credential alias` auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut `Credential alias` auf cmdb_ci_appl_citrix_collector fest.
Citrix Presentation Server/Citrix XenApp **Hinweis:** Citrix XenApp ist ab Release XenApp 5 der neue Name für Presentation Server.	Citrix XenAPP oder Presentation Server [cmdb_ci_appl_citrix_xenapp]	• Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren
Citrix Netscaler	Citrix Netscaler [cmdb_ci_lb_netscaler]	• Konfigurieren Sie die SNMP-Anmeldeinformationen . **Hinweis:** Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-Anmeldeinformationen angeben möchten. • Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST. Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery.
Citrix NetScaler Global Server-Lastenausgleichsmodul	Load Balancer-Service [cmdb_ci_lb_service]	• Konfigurieren Sie die SNMP-Anmeldeinformationen . **Hinweis:** Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen. • (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Anmeldeinformationen angeben möchten. • Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST.
APK verbinden	Connect-It Service [cmdb_ci_appl_connectit]	(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
EMC Documentum	Documentum DocBase [cmdb_ci_appl_doc_docbroker]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) (optional) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Epic	epicd app server [cmdb_ci_epicd_app_server] epic agent [cmdb_ci_epic_agent] epic cache [cmdb_ci_epic_cache] epicd [cmdb_ci_endpoint_epicd]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) (optional) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
FormEngine	Oracle Forms Engine [cmdb_ci_appl_ora_forms]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Google Cloud Platform	Cloud-Servicekonto [cmdb_ci_cloud_service_account]	• Stellen Sie einen leseberechtigten Benutzer bereit, der zur Verwendung der folgenden API-Elemente berechtigt ist. • Konfigurieren Sie auf der ServiceNow AI Platform Google API-Anmeldeinformationen.
HAProxy	HAProxy Load Balancer [cmdb_ci_lb_haproxy]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) (optional) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
HP Operations Manager	HP Operations Manager [cmdb_ci_appl_hp_operations]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
HP Service Manager-Anwendungsserver	HP Service Manager [cmdb_ci_appl_hp_service]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) (optional) auf dem ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
HP Service Manager-Index	HP SM-Indexserver [cmdb_ci_appl_hp_index]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf einem Linux- oder Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
HP Service Manager Knowledge Base	HP SM KnowledgeBase [cmdb_ci_appl_hp_sm_kb]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
HP Quality Center	HP Quality Center [cmdb_ci_appl_hp_qc]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
HP UCMDB	HP uCMDB [cmdb_ci_app_server_hp_ucmdb]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
IBM Cloud Platform	Cloud-Servicekonto [cmdb_ci_cloud_service_account]	Konfigurieren Sie auf der ServiceNow AI Platform die IBM-Anmeldeinformationen zum Zugriff auf das IBM-Konto.
IBM WebSphere Message Broker	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• "source " + $directory + "/mqsiprofile” • "echo $MQSI_VERSION “ • $directory + "/mqsireportbroker " + $name • $directory + "/mqsibrowse " + $name + " -t BROKERRESOURCES “ Legen Sie das Attribut *`Credential alias`* auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
IBM CTRL-M Server	Control-M [cmdb_ci_appl_controlm]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
IBM CICS Transaction Gateway CTG	IBM CTG [cmdb_ci_appl_ibm_ctg]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM Customer Information Control System (CICS)	IBM CICS [cmdb_ci_appl_ibm_cics]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM DB2	DB2-Instanz [cmdb_ci_db_db2_instance]	• (Unter Linux gehostet) Gewähren Sie dem Benutzer erweiterte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
	Hinweis: Beginnend mit CMDB CI-Klassenmodelle Version 1.69.0, die Bezeichnung wurde in umbenannt **DB2-Subsystem** .	Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann. • (Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen . Legen Sie das Tag-Attribut auf [cmdb_ci_db_db2_instance] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. (Optional) Um Verbindungen zu IBM DB2 zu erkennen, konfigurieren Sie SSH-Anmeldeinformationen für einen Benutzer, der berechtigt ist, die folgenden Befehle auszuführen: ◦ `db2 list tablespaces` ◦ "db2cmd /c /w /i db2 -tvf "+$ script_name • (Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen: ◦ Zum Schreiben in das / tmp-Verzeichnis ◦ Zum Anzeigen aller Benutzerprozesse ◦ Ausführen von REXX-Skripts. ◦ Einlesen des db2-Ordners. • (Unter z/OS gehostet) Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
IBM J2EE EAR	[cmdb_ci_app_server_ws_ear]	(Nur unter Linux) Geben Sie dem Benutzer erweiterte Rechte, damit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
IBM PowerHA SystemMirror für AIX Discovery	• Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group] • UNIX-Clusterressource [cmdb_ci_unix_cluster_resource] • UNIX-Clusterknoten [cmdb_ci_unix_cluster_node] • AIX-Server [cmdb_ci_aix_server] • UNIX-Cluster [cmdb_ci_unix_cluster] • Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Konfigurieren Sie einen UNIX-Benutzer mit Berechtigungen zum Ausführen aller in der offiziellen IBM-Dokumentation definierten Befehle.
IBM Tivoli Access Manager WebSEAL- oder IBM Security Access Manager(ISAM)-Appliance	Webseal [cmdb_ci_app_server_webseal]	(Nur für ISAM-Appliance) Konfigurieren Sie Anwendbare Anmeldeinformationen Für den Anwender mit Berechtigungen zum Ausführen der folgenden REST-Befehle: • /reverseproxy – zum Abrufen von Daten über Reverse-Proxy und -Instanzen • /wga/reverseproxy/"+ ${junctionstable[].instance}+"/junctions – zum Abrufen von Verbindungen für jede Instanz • /wga/reverseproxy/ " + $instance_name + "/junctions?junctions_id=" + $junction_name – zum Abrufen von Weiterleitungs-URLs für die Einstiegspunktverbindung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Nur für ISAM-Appliance) Stellen Sie sicher, dass im System die cURL-Befehle für die Erkennung verwendet werden können: • Definieren Sie auf dem MID-Server, der für die Erkennung der ISAM-Appliance verwendet wird, die Variable PATH, die die Installation des cURL-Pakets für die entsprechenden MID-Server-Benutzer enthält. • Konfigurieren Sie Berechtigungen zum Ausführen der Datei curl.exe für den entsprechenden MID-Server-Benutzer.
		(Wenn gehostet auf Linux) Auf ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM Virtualisierungs- und Hardwareverwaltungskonsole (HMC)	• HMC-Server • IBM-Frame • LPAR-Instanz (Logische Partition) Eine LPAR ist das Äquivalent zu einer virtuellen Maschine bei IBM. • LPAR-Ressource	• Überprüfen Sie, ob die folgenden Anwendungen aktuell sind: ○ Muster für Discovery und Service-Mapping ○ CMDB CI-Klassenmodelle • Überprüfen Sie, ob Sie über Berechtigungen für die folgenden HMC-Befehle verfügen: ○ `lssyscfg` ○ `lshmc` ○ `lshwres`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• Überprüfen Sie, ob Sie über Berechtigungen für den folgenden AIX-Befehl (LPAR) verfügen: `Lparstat: i` . **Hinweis:** Die `Lparstat: i` Der Befehl ist zusätzlich zu den für die AIX-Server-Discovery erforderlichen Befehlen. Weitere Informationen zur AIX-Server-Discovery finden Sie unter Erkennung von AIX-Servern. Eine Liste der AIX-Befehle finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. • Konfigurieren Sie SSH-Anmeldeinformationen auf dem ServiceNow AI Platform. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .
IBM WebSphere Application Server	IBM Websphere [cmdb_ci_app_server_websphere]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Unter z/OS gehostet) Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
		(Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• Zum Schreiben in das /tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Zum Ausführen von REXX-Skripts • Zum Ausführen von Befehlen mit oeconsol • Zur Ausführung des Befehls, mit dem Informationen über die WebSphere Application Server-Aufgabe abgerufen werden: `"oeconsol 'D OMVS,A=ALL' | grep "+ $taskname`. • Zum Lesen des Inhalts des WAS-Installationsordners und der Berechtigung zum Lesen von was.env.file, worin sich die Installationsvariablen befinden.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM WebSphere DataPower	DataPower [cmdb_ci_app_server_datapower]	**SNMP-Anmeldeinformationen** SNMP-Anmeldeinformationen sind für die Verwendung der folgenden SNMP-Abfragen erforderlich: • Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]: ○ 1.3.6.1.2.1.1.1 ○ 1.3.6.1.2.1.1.5 ○ 1.3.6.1.2.1.4.20.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		◦ 1.3.6.1.2.1.2.2.1 ◦ 1.3.6.1.4.1.14685.3.1.196.1 ◦ 1.3.6.1.4.1.14685.3.1.11.1 ◦ 1.3.6.1.4.1.14685.3.1.112.1 • Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]: ◦ 1.3.6.1.2.1.1.1 ◦ 1.3.6.1.2.1.1.5 ◦ 1.3.6.1.4.1.14685.3.1.11.1 **Applicative-Anmeldeinformationen** Neben SNMP-Anmeldeinformationen sind zum Erkennen von DataPower-Anwendungsdomänen auch Applicative-Anmeldeinformationen erforderlich, auch als logische CIs bekannt. Darüber hinaus werden SNMP- und Applicative-Anmeldeinformationen für die Top Down-Discovery von Anwendungsbeziehungen (entsprechende DataPower-Anwendungsdomäne) verwendet. **Benutzer mit Berechtigungen zum Ausführen von SOAP** Damit eine Top Down-Discovery für den DataPower-Webservice und die MQ-Verbindung ausgeführt werden kann, sind Berechtigungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		zum Ausführen von SOAP-Abfragen erforderlich.
IBM WebSphere Message Broker-Flow	WMB Flow [cmdb_ci_appl_wmb]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Stellen Sie einem Benutzer des IBM-Betriebssystems WebSphere Message Broker Berechtigungen zum Ausführen des WebSphere Message Broker-Service bereit.
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Wenn auf einem Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • "source " + $directory + "/mqsiprofile” • "echo $MQSI_VERSION “ • $directory + "/mqsireportbroker " + $name • $directory + "/mqsibrowse " + $name + " -t BROKERRESOURCES “ Legen Sie das Attribut `Credential alias` auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
IBM WebSphere Message Broker	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Legen Sie das Attribut `Credential alias` auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		Stellen Sie einem Benutzer des IBM-Betriebssystems WebSphere Message Broker Berechtigungen zum Ausführen des WebSphere Message Broker-Service bereit.
IBM MQ (früher IBM WebSphere MQ)	IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Anwendbare Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • (Auf Windows-Server) "echo display QMSTATUS ALL | runmqsc -e " + $queue_manager – zum Abrufen des Status des Warteschlangenmanagers (QM) • (Auf Windows-Server) "echo display QMGR ALL | runmqsc -e " + $queue_manager – for getting the complete information about QM. • (Auf Unix-Server) "echo \" display QMSTATUS ALL \" | runmqsc " + $queue_manager – zum Abrufen des Status des QM • (Auf Unix-Server) "echo \" display QMGR ALL \" | runmqsc " + $queue_manager – zum Abrufen von vollständigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Informationen über den QM • (Auf Unix-Server) "echo \" display queue(" + $entry_point.queue + ") \" | runmqsc " + $queue_manager – zum Abrufen von Informationen über die EP-Warteschlange
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Wenn auf einem Unix-Server gehostet) Konfigurieren SSH-Anmeldeinformationen . Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut `Credential alias` auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. (Optional) um IBM MQ-Verbindungen zu finden, konfigurieren Sie SSH-Anmeldeinformationen für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • "echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • "echo \" display QMSTATUS ALL \" | runmqsc "+ $queue_manager • echo \" display QMGR ALL \" | runmqsc "+ $queue_manager
		(Unter z/OS gehostet) Konfigurieren Sie auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		ServiceNow AI Platform die SSH-Anmeldeinformationen .
		(Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen: • Zum Schreiben in das / tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Zum Ausführen von REXX-Skripts • Zum Ausführen von Befehlen mit oeconsol • Zur Ausführung von MQ-Befehlen
IBM MQ-Warteschlange (früher IBM WebSphere MQ-Warteschlange)	IBM MQ-Warteschlange (früher IBM WebSphere MQ-Warteschlange) [cmdb_ci_appl_ibm_wmq_Queue]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Anwendbare Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • dspmq – zum Abrufen von Informationen über den Warteschlangenmanager • "echo \" display queue(" + $entry_point.queue + ") \" | runmqsc " + $queue_manager – zum Abrufen von Informationen über die Warteschlange • "echo \" display clusqmgr(*) conname \" | runmqsc " + $queue_manager – zum Abrufen aller Zeilen des Warteschlangenmanagers (QM) des Clusters • "echo \" display qstatus(" + $entry_point.queue + ") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc " + $queue_manager – zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Abrufen von Informationen über den Status der Warteschlange
		(Wenn auf Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • dspmq echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qcluster("+$rqmname +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" dischl(*) CHLTYPE(SDR) CONNAME XMITQ WHERE(XMITQ EQ "+$xmit_name +")\" | runmqsc "+ $queue_manager • (Optional) "echo \" display clusqmgr(*) conname \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qstatus("+ $entry_point.queue +") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc "+ $queue_manager Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut `Credential alias` auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Wenn gehostet auf Windows), auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen Für einen Anwender mit Berechtigungen zum Ausführen der folgenden Befehle: • dspmq echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qcluster("+$rqmname +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" dischl(*) CHLTYPE(SDR) CONNAME XMITQ WHERE(XMITQ EQ "+$xmit_name +")\" | runmqsc "+ $queue_manager • (Optional) "echo \" display clusqmgr(*) conname \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qstatus("+ $entry_point.queue +") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc "+ $queue_manager Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut `Credential alias` auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden..
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
IBM WebSphere Portal	WebSphere-Portal [cmdb_ci_appl_websphere_portal]	(Nur unter Linux) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Interconnect Web Service	Interconnect [cmdb_ci_inter_connect]	(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
Jboss	JBoss [cmdb_ci_app_server_jboss]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn auf Unix-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Jboss-Modul	Jboss-Modul [cmdb_ci_app_server_jb_module]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
JRun	JRun [cmdb_ci_app_server_jrun]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
JRun WAR Inc	JRun WAR [cmdb_ci_app_server_jrun_war]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
Microsoft Azure-Websites	Cloud-Webserver [cmdb_ci_cloud_webserver]	Fügen Sie in ServiceNow AI Platform einen Azure-Service-Prinzipal hinzu und richten Sie ein Cloud-Konto für Azure ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Azure-Lastenausgleichsmodul	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Sie auf der ServiceNow AI Platform einen Azure-Dienstprinzipal, und richten Sie ein Cloud-Konto für Azure ein. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Azure SQL-Datenbank	Cloud-Datenbankregel [cmdb_ci_cloud_database]	Fügen Sie in ServiceNow AI Platform einen Azure-Service-Prinzipal hinzu und richten Sie ein Cloud-Konto für Azure ein. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Dynamic CRM	Dynamische CRM-Komponente [cmdb_ci_appl_ms_dynamic_crm]	Auf der ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft BizTalk Orchestration	BizTalk Orchestration [cmdb_ci_appl_biztalk_orch]	Auf der ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft BizTalk Server	BizTalk [cmdb_ci_appl_biztalk]	Auf der ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf Windows Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Microsoft Exchange-Back-End-Server	ExchangeBackEndServer [cmdb_ci_exchange_backend]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen für einen Windows-Server.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft Exchange-Front-End-Server	ExchangeFrontEndServer [cmdb_ci_exchange_frontend]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen für einen Windows-Server.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft FAST Search Server	Fast Search [cmdb_ci_appl_fastsearch]	Erstellen Sie einen Benutzer mit der Berechtigung zum Lesen der folgenden Dateien: • install_directory+"\etc \VERSION.xml • und install_directory+"\etc \CSConfig.xml
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft Exchange Hub Transport-Server Microsoft Exchange Postfach Microsoft Exchange CAS	ExchangeHub [cmdb_ci_exchange_hub] Exchange MailBox [cmdb_ci_exchange_mailbox] Exchange-Clientzugriffsserver [cmdb_ci_exchange_cas]	• Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. Verwenden Sie als Windows-Anmeldeinformationen Anwendername und Passwort des Microsoft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Exchange Server-Administrators. Zum Beispiel Anwendername: local\administrator und Passwort: Are1300. **Hinweis:** Wenn Sie Windows-Anmeldeinformationen für einen anderen Benutzer als den Microsoft Exchange Server-Administrator konfigurieren, verwendet Service-Mapping die Traffic-basierte Discovery, die zur Zuordnung aller Microsoft Exchange-Clients führt. • (Für Exchange CAS 2010 und 2013, 2016) Konfigurieren Sie auf der ServiceNow AI Platform Applicative-Anmeldeinformationen , indem Sie den CI-Typ auf „Exchange-Postfach“ einstellen. **Warnung:** Verwechseln Sie den CI-Typ der Exchange Mailbox nicht mit dem CI-Typ des Exchange Mailbox-Servers. Service-Mapping Verwendet diese anwendbaren Anmeldeinformationen für den Zugriff auf den Ordner of/Servers/Servers.slab im Key Exchange Admin Center (EAC). Service-Mapping Verwendet auch die anwendbaren Anmeldeinformationen, um die folgenden PowerShell-Befehle für auszuführen MID Servers: ○ Get-ExchangeServer ○ Get-ExchangeServer ○ Get-Mailboxserver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		○ Get-ClusteredMailBoxServerStatus ○ Get-ExchangeServer ○ Get-StorageGroup ○ Get-MailboxDatabase • (Für Microsoft Exchange CAS 2010 und 2016) Installieren Sie das Microsoft.Exchange.Management.PowerSh Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet. • (Für Microsoft Exchange CAS 2007) Installieren Sie das Microsoft.Exchange.Management.PowerSh Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet. • (Für Microsoft Exchange CAS 2007, 2010) Laden Sie das rctrlx-Tool zum Ausführen von PowerShell-Befehlen auf ServiceNow AI Platform hoch, wie in Datei rctrlx.exe auf MID Servers hochladen beschrieben. • (Für Microsoft Exchange CAS 2007 und 2010) Statten Sie einen Exchange Mailbox-Betriebssystem-Benutzer mit den Rechten zum Ausführen von Exchange-Services unter Windows und der Berechtigung zum Abfragen des Exchange-Repositorys aus: Konfigurieren Sie auf der ServiceNow AI Platform die Windows-Anmeldeinformationen , indem Sie das Attribut `Credential alias` auf [cmdb_ci_exchange_mailbox] einstellen. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		für dieses CI später in Mustern verwenden. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren . • Vergewissern Sie sich, dass Sie den Einstiegspunkt kennen, der zum Erkennen des Microsoft Exchange-Servers erforderlich ist. Verwenden Sie die URL für den Outlook-Webzugriff im folgenden Format: http(s)://<hostname>:<port>/owa Zum Beispiel http(s)://myhost:<443>/owa
Microsoft Identity Integration Server	IIFP [cmdb_ci_directory_iifp]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
Microsoft Internet Information Services (IIS)	Microsoft IIS-Webserver [cmdb_ci_microsoft_iis_web_server]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen . (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Virtuelles Verzeichnis für Microsoft Internet Information Services (IIS)	Virtuelles IIS-Verzeichnis [cmdb_ci_iisdirectory]	Konfigurieren Sie auf der ServiceNow AI Platform die folgenden Anmeldeinformationen: • Windows-Anmeldeinformationen • Anwendbare Anmeldeinformationen Überprüfen Sie den Lesezugriff auf die folgenden Dateien: • Web.config : Mögliche Standorte $entry_Point.path + „Web.config“ Oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		$entry_Point.path + „\Web.config“ • Computer.Konfiguration : Möglicher Standort „Dir \„C:\Windows \Microsoft.NET\"
		• (Optional) Um ADO.NET-Verbindungen zu erkennen, legen Sie das Attribut *Credential alias* auf [cmdb_ci_iisdirectory] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft Message Queuing (MSMQ)	MSMQ [cmdb_ci_appl_msmq]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
Microsoft .NET Framework	.NET-Anwendung [cmdb_ci_appl_dot_net]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen . (Optional) Um ADO.NET-Verbindungen zu erkennen, legen Sie das Attribut *Credential alias* auf [cmdb_ci_iisdirectory] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		Erteilen Sie einem Betriebssystembenutzer des virtuellen IIS-Verzeichnisses Rechte zum Ausführen des IIS-Service unter Windows.
		Konfigurieren Anwendbare Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft SharePoint	SharePoint [cmdb_ci_appl_sharepoint]	Konfigurieren Sie auf der ServiceNow AI Platform die folgenden Anmeldeinformationen: • Windows-Anmeldeinformationen • Legen Sie das Attribut `Credential alias` auf [cmdb_ci_appl_sharepoint] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. • Konfigurieren Sie den WMI-Abfragezugriff auf den SharePoint-Remoteserver. • (Optional) Um Windows SharePoint-Verbindungen zu erkennen, konfigurieren Sie Windows-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der http get-Anforderung an die URL der SharePoint-Zentraladministration.
		Erteilen Sie einem SharePoint-Betriebssystemsbenutzer Berechtigungen: • Zum Ausführen von SharePoint-Services unter Windows • Zum Anmelden bei der SharePoint-Verwaltungsseite
		Um zwei separate Anmeldeinformationen mit unterschiedlichen Berechtigungen zu verwenden, konfigurieren Sie die Anmeldeinformationen wie in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		beschrieben Voraussetzungen für die Durchführung der Top Down-Discovery/Service Mapping-Discovery für das SharePoint-System [KB0813083] artikel in Now Support Knowledge Base.
Microsoft SQL-Datenbank	MySQLClusterDataNode [cmdb_ci_db_mysql_clusternode]	Stellen Sie den/die folgenden Benutzer bereit: • Zur Erkennung von Microsoft BizTalk mithilfe von SQL-Abfragen einen Benutzer und Anmeldeinformationen für Microsoft BizTalk • Zur Erkennung von Lizenzierungsinformationen für Microsoft SQL Server einen Benutzer und Anmeldeinformationen zum Zugriff auf die Microsoft SQL-Datenbank Informationen zum Betrieb finden Sie in der Produktdokumentation.
		Anmeldeinformationen für Host-Discovery wie in beschrieben Windows-Anmeldeinformationen .
		Konfigurieren Anwendbare Anmeldeinformationen .
MongoDB	Mongo-Konfigurationsserver [cmdb_ci_appl_mongo_config_serv]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschriebenen Mongo-Befehle.
MySQL Cluster MGM-Knoten	MySQLClusterMGMNode [cmdb_ci_db_mysql_clustermgnode]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		einen privilegierten Benutzer erfordern ausführen kann.
		Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
Nginx	Nginx-Webserver [cmdb_ci_nginx_web_server]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Anwendbare Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
OpenText Documentum	Documentum DocBase [cmdb_ci_appl_doc_docbase]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
Oracle-Anwendungsserver	Oracle iAS [cmdb_ci_app_server_ora_ias]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
Oracle Advanced Queue-Warteschlange	Advanced Queue-Warteschlange [cmdb_ci_appl_ora_queue]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Oracle Clusterware	UNIX-Cluster [cmdb_ci_unix_cluster], UNIX-Clusterknoten [cmdb_ci_unix_cluster_node], UNIX-Clusterressource [cmdb_ci_unix_cluster_resource], virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Weitere Informationen finden Sie unter Oracle Datenbank-Discovery.
Oracle Concurrent-Server	Oracle Concurrent Server [cmdb_ci_appl_ora_conc]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle-Datenbank	Oracle-Instanz [cmdb_ci_db_ora_instance]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle-Datenbank 12c	Oracle PDB-Instanz [cmdb_ci_db_ora_pdb_instance]	• Konfigurieren Sie Applicative-Anmeldeinformationen . • Für Windows konfigurieren Sie Windows-Anmeldeinformationen . • Für Unix konfigurieren Sie SSH-Anmeldeinformationen . • Konfigurieren Sie für die Oracle-Datenbank die Discovery von Oracle-Datenbanken. • Gewähren Sie einem Benutzer Berechtigungen zum Ausführen von Abfragen in den folgenden Tabellen: ◦ V$DATAFILE ◦ V$TEMPFILE ◦ V$LOG ◦ DBA_FREE_SPACE ◦ V$DATABASE ◦ V$PDBS ◦ V$PARAMETER
Queue für erweiterte Oracle-Datenbanken	Advanced Queue-Warteschlange [cmdb_ci_appl_ora_queue]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		ServiceNow AI Platform SSH-Anmeldeinformationen .
		Stellen Sie einen Oracle-Instanzbenutzer mit Berechtigung zur Ausführung des Befehls sqlplus bereit (siehe Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern).
Oracle Discoverer Engine	Oracle Discoverer Engine [cmdb_ci_appl_ora_disc]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Discoverer-Anwenderoberfläche	Oracle Discoverer-UI [cmdb_ci_appl_ora_disc_ui]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.
		Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle E-Business Suite	Oracle ESB [cmdb_ci_appl_ora_ebs]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Form-UI	Oracle Forms-UI [cmdb_ci_appl_ora_forms_ui]	(Wenn auf einem Windows-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren Sie einen Domänenanwender für den Zugriff auf das Windows-Betriebssystem wie in beschrieben Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Fulfillment-Server	Oracle Fulfillment Server [cmdb_ci_appl_ora_fs]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.
Oracle GlassFish Server	GlassFish [cmdb_ci_appl_glassfish] GlassFish WAR [cmdb_ci_appl_glassfish_war]	• (Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen. • (Beim Hosting auf einem Linux- oder UNIX-Server) (Optional) Konfigurieren Sie in der ServiceNow AI Platform SSH-Anmeldeinformationen. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.
Oracle HTTP-Server	Oracle-HTTP-Server [cmdb_ci_appl_ora_http]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen.
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.
Oracle iAS-Webmodul	Oracle iAS-Webmodul [cmdb_ci_app_server_ora_ias_m]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		AI Platform Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Oracle Metric-Client	Oracle Metric-Client [cmdb_ci_appl_ora_metric_client]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Oracle Metric-Server	Oracle Metric-Server [cmdb_ci_appl_ora_metric_svr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle MySQL-Server	MySQL-Instanz [cmdb_ci_db_mysql_instance]	Stellen Sie den/die folgenden Benutzer bereit: • Zur Erkennung von Microsoft BizTalk mithilfe von SQL-Abfragen einen Benutzer und Anmeldeinformationen für Microsoft BizTalk • Zur Erkennung von Lizenzierungsinformationen für Microsoft SQL Server einen Benutzer und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Anmeldeinformationen zum Zugriff auf die Microsoft SQL-Datenbank
		Konfigurieren Anwendbare Anmeldeinformationen .
		(Unter Linux gehostet) Gewähren Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn auf einem Linux-Server gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Net-Listener	Oracle Datenbank-Listener [cmdb_ci_db_ora_listener]	(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Oracle Notification Server	Oracle-Benachrichtigungsserver [cmdb_ci_appl_ora_notif_svr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
Oracle OACORE-Server	Oracle OACORE-Server [cmdb_ci_appl_ora_oacore]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Oracle OAFM-Server	Oracle OAFM-Server [cmdb_ci_appl_ora_oafm]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn auf Unix gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
Oracle PeopleSoft	Peoplesoft-Anwendungsserver [cmdb_ci_appl_peoplesoft]	(Wenn auf Unix gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		Erteilen Sie einem Benutzer die Berechtigung zum Ausführen der unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschriebenen Befehle.
Oracle Prozessmanager	Oracle-Prozessmanager [cmdb_ci_appl_ora_pm]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Reports Server	Oracle-Berichtsserver [cmdb_ci_appl_ora_report]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		AI Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Tnslsnr-Engine	Oracle TNS-Listener-Engine [cmdb_ci_appl_ora_tnslsnr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Wenn unter Linux gehostet) auf dem ServiceNow AI Platform, Konfigurieren SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
Oracle Tuxedo und Oracle Tuxedo-Portal	Tuxedo [cmdb_ci_appl_tuxedo] und Tuxedo-Portal [cmdb_ci_appl_tuxedo_portal]	• Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen . • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren . • (Wenn auf Unix gehostet wird) Geben Sie einem Benutzer die erweiterten Rechte zum Ausführen von Befehlen, die in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern beschrieben werden.
Oracle WebLogic-Modul	Oracle iAS-Webmodul [cmdb_ci_app_server_ora_ias_m]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
Oracle WebLogic-Server (Version 10.3)	Weblogic [cmdb_ci_app_server_weblogic]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.
Oracle WebLogic-On-Demand-Router-Lastenausgleichsmodul	Websphere ODR LB [cmdb_ci_app_server_ws_odr]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen.
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen.
Radware Alteon NG	Alteon Load Balancer [cmdb_ci_lb_alteon]	Auf der ServiceNow AI Platform, Konfigurieren SNMP-Anmeldeinformationen.
Radware AppDirector	Radware-Load Balancer [cmdb_ci_lb_radware]	Auf der ServiceNow AI Platform, Konfigurieren SNMP-Anmeldeinformationen.
Red Hat Cluster Suite	Virtuelle Cluster-IPs [cmdb_ci_cluster_vip] UNIX-Cluster [cmdb_ci_unix_cluster] UNIX-Clusterknoten [cmdb_ci_unix_cluster_node] UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen.
		Erteilen Sie einem Benutzer die Berechtigung zum Lesen dieser Dateien: • /etc/cluster/cluster.conf • /etc/hosts
		Erteilen Sie einem Benutzer erweiterte Rechte zur Ausführung dieses Befehls: `clustat –x`.
PostgreSQL-Datenbank	PostgreSQL-Instanz [cmdb_ci_db_postgresql_instance]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Nur unter Unix) Geben Sie diesem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Pivotal RabbitMQ	RabbitMQ-Cluster [cmdb_ci_appl_rabbitmq_cluster]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP Business Object XI Schedule	SAP BO BOXIScheduleRouter [cmdb_ci_appl_sap_bo_scheduler]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Optional) für die Erkennung mit dem WinRM-Protokoll, seew Konfigurieren Sie vertrauenswürdige WinRM-Hosts auf dem MID-Server .
SAP Crystal Management Server	SAP Business Objects CMS-Server [cmdb_ci_appl_sap_bo]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
SAP-Zentralinstanz/ SAP Central Services (SCS)/ SAP Development Infrastructure/ SAP Evaluated Receipt Settlement (ERS)/ SAP Java Connector/ SAP NetWeaver-Dialoginstanz/ ABAP SAP Central Services (ASCS)	SAP CI-Anwendung [cmdb_ci_appl_sap_ci] / SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]/ SAP DI-Anwendung [cmdb_ci_appl_sap_di]/ SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]/ SAP JC-Anwendung [cmdb_ci_appl_sap_jc]/ SAP DI-Anwendung [cmdb_ci_appl_sap_di]/ SAP ASCS-Anwendung [cmdb_ci_appl_sap_ascs]	• (Beim Hosting auf UNIX-Server) Konfigurieren Sie auf der ServiceNow AI Platform die Applicative-Anmeldeinformationen und SSH-Anmeldeinformationen. Die SSH-Anmeldeinformationen werden dazu verwendet, Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. Geben Sie dem Anwender zusätzlich erhöhte Rechte an, um Befehle ausführen zu können, die einen privilegierten Anwender erfordern: Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. • (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform die Windows-Anmeldeinformationen, um Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren. • (Optional für Discovery von oben nach unten durch Service-Mapping) Erteilen Sie einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion. • (Optional für Top Down-Discovery durch Service-Mapping) Wenn Ihre Organisation digitale SAP-Business-Services mithilfe von Webservices

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		implementiert und Sie alle verbundenen Services zuordnen möchten, führen Sie die folgenden Aktionen aus: ○ Konfigurieren Sie Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: CVERS, DBCONS und RFCONS. ○ Stellen Sie sicher, dass Sie über die Webservice-URL verfügen. Informationen zum Erstellen von Webservices finden Sie unter https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ .
SAP HANA-Datenbank	SAP HANA-Datenbank [cmdb_ci_appl_sap_hana_db]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP Sybase DB	Sybase-Instanz [cmdb_ci_db_syb_instance]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Nur unter Unix) Geben Sie diesem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SQL Server Analysis Services (SSAS)	SQL Server Analysis Services [cmdb_ci_db_mssql_analysis]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
SQL Server Integration Services-Auftrag (SSIS)	SQL Server Integration Services-Auftrag [cmdb_ci_db_mssql_int_job]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
SQL Server Integration Services (SSIS)	SQL-Server-Integrationsservices [cmdb_ci_db_mssql_integration]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SQL Server Reporting Services (SSRS)	SQL Server Reporting Services [cmdb_ci_db_mssql_reporting]	Erteilen Sie einem Benutzer des Betriebssystems SSRS Berechtigungen zum Ausführen des SSRS-Service.
		Konfigurieren Sie Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der http get-Anforderung für die Einstiegspunkt-URL.
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen . Legen Sie das Attribut *`Credential alias`* auf [cmdb_ci_db_mssql_reporting] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Konfigurieren Sie zum Erkennen von Verbindungen zu Berichtsdatenquellen Anmeldeinformationen für einen Benutzer mit der Berechtigung zum Ausführen einer http post-Anforderung für die Einstiegspunkt-URL.
		Konfigurieren Anwendbare Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Sun iPlanet Webserver	iPlanet Webserver [cmdb_ci_iplanet_web_server]	Konfigurieren Anwendbare Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
Sun Directory	Sun LDAP-Server [cmdb_ci_sun_ldap_dir_server]	Konfigurieren Anwendbare Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
Sun JES	JES [cmdb_ci_email_server_jes]	Konfigurieren Anwendbare Anmeldeinformationen .
		Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
Symantec Enterprise Vault	Enterprise Vault [cmdb_ci_email_server_ent_vault]	Auf der ServiceNow AI Platform, Konfigurieren Windows-Anmeldeinformationen .
TIBCO ActiveMatrix BusinessWorks/ TIBCO ActiveMatrix BusinessWorks-Prozess/ TIBCO EMS-Warteschlange/ TIBCO Enterprise Message Service (EMS)/	ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]/ ActiveMatrix Business Works-Prozess [cmdb_ci_appl_tibco_matrix_proc]/ EMS-Warteschlange [cmdb_ci_appl_tibco_queue]/ Tibco Enterprise Message Service [cmdb_ci_appl_tibco_message]	• (Beim Hosting auf Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Tibco EMS. • (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen . • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
TIBCO ActiveMatrix Adapter	Tibco-Adapter [cmdb_ci_appl_tibco_adapter]	(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .
Veritas Enterprise Vault	Enterprise Vault [cmdb_ci_email_server_ent_vault]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .

Lösen von Problemen im Zusammenhang mit Anmeldeinformationen

Wenn Discovery-Probleme auftreten, die durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht wurden, beheben Sie sie wie im KB-artikel erläutert: Fehlerbehebung bei Anmeldeinformationen und Berechtigungen bei Discovery, Service-Mapping, Orchestration

Für die Hosterkennung erforderliche Anmeldeinformationen

Es gibt Anmeldeinformationen und Berechtigungen, die Service-Mapping für die Erkennung von Hosts benötigt.

Vor der Erkennung von Anwendungen greift Service-Mapping auf Hosts zu, auf denen Anwendungen ausgeführt werden, und erkennt diese. Stellen Sie sicher, dass Sie alle erforderlichen Anmeldeinformationen angeben, um die Hosterkennung zu ermöglichen.

ServiceNow AI Platform bietet eine zentralisierte Möglichkeit zum Konfigurieren von Anmeldeinformationen für Discovery, Service-Mapping und andere Anwendungen. Sie können die Anmeldeinformationen für Hosts und Anwendungen nur einmal konfigurieren. Wenn Sie bereits hostbezogene Anmeldeinformationen für eine andere Anwendung konfiguriert haben, müssen Sie dies für Service-Mapping nicht noch einmal tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die Erkennung von Hosts unter UNIX oder Linux erforderliche Anmeldeinformationen

Discovery, Orchestration und IntegrationHub Erkunden UNIX Und Linux Geräte, die SSH-Anmeldeinformationen verwenden, um Befehle über Secure Shell (SSH) auszuführen.

Um ausreichende Berechtigungen zu erteilen, konfigurieren Sie eine der folgenden UNIX- oder Linux-Anmeldeinformationen:

- Nicht-Root-Benutzer und -Kennwort und Ausführung der ausgewählten Befehle als „root“ mithilfe des Dienstprogramms sudo
- Root-Benutzer und -Passwort

Informationen zu Befehlen, die Rechte auf Sudo-Ebene erfordern, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern Und Befehle, die Stammberechtigungen für Discovery und Orchestration erfordern .

Um mit Nicht-Root-Anmeldeinformationen auf Unix-basierte Hosts zuzugreifen, erteilen Sie Lesezugriff auf die folgenden Dateien und Verzeichnisse:

- /etc/*release
- /etc/bashrc
- /etc/profile
- /proc/cpuinfo
- /proc/vmware/sched/ncpus
- /var/log/dmesg
- APD-Verzeichnis

Für die Erkennung von Hosts auf Windows-Servern erforderliche Anmeldeinformationen

Um ausreichende Berechtigungen zu erteilen, konfigurieren Sie eine der folgenden Windows-Anmeldeinformationen:

- Ein Domänenbenutzer mit lokalem Administratorzugriff auf Windows-Zielhosts
- Einen Domänenadministrator

> **Hinweis:** Die Anmeldeinformationen für den Domänenadministrator benötigen Sie möglicherweise nur in einigen Fällen. Beispielsweise beim Erkennen von Domänencontrollern.

Konfigurieren Sie DEN zu verwendenden MID-Server Windows-Anmeldeinformationen .

(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Lösen von Problemen im Zusammenhang mit Anmeldeinformationen

Wenn Discovery-Probleme auftreten, die durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht wurden, beheben Sie sie wie im KB-artikel erläutert: Fehlerbehebung bei Anmeldeinformationen und Berechtigungen bei Discovery, Service-Mapping, Orchestration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern

Um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen, nutzt Service-Mapping Befehle, für die erweiterte Rechte erforderlich sind. Konfigurieren Sie nicht nur die erforderlichen Anmeldeinformationen, sondern auch die Server in Ihrer Organisation, damit Service-Mapping diese Befehle mit erweiterten Rechten ausführen kann.

Sie führen diese Befehle nicht direkt aus. Service-Mapping verwendet Befehle, die erhöhte Rechte erfordern, als Teil der folgenden Prozesse:

- Hosterkennung
- Prozessidentifikation am Port
- CIs anhand von Mustern entdecken

Einige dieser Befehle erfordern keine erweiterten Rechte, es sei denn, Verzeichnisse, auf die Service-Mapping zugreifen muss, sind geschützt. Weitere Informationen finden Sie unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

Betriebssystembefehle, die erweiterte Rechte erfordern

AIX-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
`cat`	`file-name`	Zeigt den Dateiinhalt an

`ls`	`-F-1`
	`-1HF`
	`-w 1`
	`-1`
		Listet den Verzeichnisinhalt auf

`procwdx`	`Process_id`	Ruft das Arbeitsverzeichnis eines Prozesses ab
`rmsock`	`Socketname tcpcp`	Sucht nach einem Prozess, der einen bestimmten Port abhört
`lsof`	`-Pnl +M -i`	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind
`lstat`	Verschiedene Optionen	Ruft Informationen über einen Link ab
`ps`	`eww`	Ruft Umgebungsvariablen für den Prozess unter AIX ab

HP-UX-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
`cat`	`file-name`	Zeigt den Dateiinhalt an
`ls`	`-F-1` `-1HF`	Listet den Verzeichnisinhalt auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HP-UX-Befehle, die erweiterte Rechte erfordern (Fortsetzung)

Befehl	Parameter	Beschreibung
	`-w 1` `-1`	
`pfiles`	`Process_id`	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind
`lsof`	`-Pnl +M -i`	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind

Solaris-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
`cat`	`File_name`	Zeigt den Dateiinhalt an

`ls`	`ls -F-1`
	`ls -1HF`
	`ls -w 1`
	`ls -1`
		Listet den Verzeichnisinhalt auf

	`e-l`	Ruft Dateiattribute ab, die für die Entscheidung zum Zwischenspeichern von Dateien verwendet werden
`pargs`	`-e`	Ruft das ausführbare Verzeichnis ab.
`pargs`	`-a`	Ruft den Prozess ab.
`lsof`	`-Pnl +M -i`	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.
`netstat`	`-anu`	Listet die offenen Ports auf Obligatorisch für Solaris Version 11.2 oder höher.
`Ifconfig`	`Ifconfig -a`	Zeigt Schnittstelleninformationen an (sudo zum Abrufen der MAC-Adressen erforderlich)
`pwdx`	`Process_id`	Ruft die Prozessinformationen ab
`pargs`	`-e process_id`	Ruft die Prozessinformationen ab
`ps`	`-eo user, pid, ppid, comm, args`	Ruft die Prozessliste ab
`inetadm`	`-l or without params`	Verarbeitet den Anwendungsfall mit dem inet-Daemon

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Befehle, die erweiterte Rechte erfordern

Befehle	Parameter	Beschreibung

`cat`	`File_name`
	`scsi`
	`tr '\\n'`
	`/proc`
	`/proc/cpuinfo`
	`sys`
	`sys/hypervisor`
	`sys/hypervisor/compilation`
	`sys/hypervisor/compilation/compiled by`
		Zeigt Informationen über den Inhalt der Datei an

`cut`	`-d` `-f1`	Zeigt die gesamte Ausgabe einer Datei an

`dmidecode`	`-t 17`
	`-s bios-vendor`
	`-t 1`
	`-t 2`
	`-t 3`
		Zeigt Informationen zur Hardware des Linux-Servers in einem lesbaren Format an

`lshw`		Zeigt Informationen zur Hardware des Linux-Servers in einem lesbaren Format an

`ls`	`ls -F-1`
	`ls -1HF`
	`ls -w 1`
	`ls -1`
	`ls -l`
		Listet den Verzeichnisinhalt auf

`netstat`	`-ltnup` `-ltnp`	Zeigt die offenen Netzwerkverbindungen an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Befehle, die erweiterte Rechte erfordern (Fortsetzung)

Befehle	Parameter	Beschreibung
	`-ntup` `-an`	
`Isof` **Hinweis:** Wird in einigen Fällen als Alternative zu netstat verwendet.	`-Pnl +M -i`	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.

`ss`	`-ltnup`
	`-ntup`
	`-an`
		Zeigt die offenen Netzwerkverbindungen an

`stat`	`--format="%Y"` `-L file_name`	Zeigt die Änderungszeit der Datei an
`fdisk`	`-l`	Zeigt alle Festplattenpartitionen an

Anwendungsbefehle, die erweiterte Rechte erfordern

Service-Mapping verwendet einige dieser Befehle in Mustern.

Apache-Webserver (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

Apache Tomcat (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Tomcat (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Apache Tomcat WAR (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an
version.sh/version.bat	-	Ruft die Tomcat-Version ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Dieser Befehl wird in Verbindungsabschnitten des Musters zum Erkennen von Apache Tomcat-WAR-Verbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

App TNS-Service (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BIG-IP Global Traffic Manager (GTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
`ping`	`-a -c 1 [url[1].host]`	Ruft die Host-IP ab

BMC CTRL-M Enterprise Manager (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

BMC CTRL-M Gateway (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Verbindungen zum Control M-Server verwendet. Sucht nach Datei- und Ordnerpfaden

Citrix NetScaler (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`Anzeigen`	Verschiedene Optionen	Ruft die Netscaler-IP-Adresse ab.

EMC Documentum Broker (unter UNIX)

Befehl	Parameter	Beschreibung
`find`	Verschiedene Optionen	Sucht nach Verbindungen zu Docbase

FormEngine (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	(Nur unter Unix) Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

FormEngine (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	(Nur unter Unix) Zeigt den Dateiinhalt an

IBM Customer Information Control System (CICS) (unter UNIX)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

IBM CTRL-M Server (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	(Nur für Unix) Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	(Nur für Unix) Sucht nach Datei- und Ordnerpfaden

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
`cat`	-	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Zeigt den Dateiinhalt in der Ausgabe an
`find`	Verschiedene Optionen	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM DB2 (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	*-*	Zeigt den Dateiinhalt in der Ausgabe an

IBM J2EE EAR (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner

IBM WebSphere-Anwendungsserver (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	*-*	Zeigt den Dateiinhalt an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

IBM WebSphere-Portal (auf UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	*-*	Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker-Flow (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an
ps	*-ef*	Ruft die Prozessinformationen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf

IBM WebSphere Message Broker (unter UNIX)

Befehl	Parameter	Beschreibung
ps	*-ef*	Ruft die Prozessinformationen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

IBM MQ (ein UNIX) – Früher IBM WebSphere MQ

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

IBM MQ-Warteschlange (am UNIX) – Früher IBM WebSphere MQ-Warteschlange

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

JBoss-Modul (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JBoss (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`find`	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

JRun (unter UNIX)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

JRun WAR Inc (unter UNIX)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

Microsoft Exchange-Clientzugriffsserver (CAS), Microsoft Exchange-Hub-Transport-Server, Microsoft Exchange-Postfach (unter Windows)

Befehl	Parameter	Beschreibung
`Get-ExchangeServer`	`-status -Identity "+ $hostname+"| export-clixml $env:TEMP \exchange_pwrshell_output.xml`	Extrahiert die Liste der Microsoft Exchange-Hosts und -Rollen
`Get-ExchangeServer`	`format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer`	Extrahiert die Liste der Microsoft Exchange-Hosts und -Rollen im Tabellenformat
`Get-Mailboxserver`	`format-list`	Extrahiert die Liste der Microsoft Exchange-Postfachserver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Exchange-Clientzugriffsserver (CAS), Microsoft Exchange-Hub-Transport-Server, Microsoft Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
`Get-ClusteredMailBoxServerStatus`	`format-table -Property OperationalMachines`	Extrahiert Informationen über Microsoft Exchange-Postfachcluster
`Get-ExchangeServer`	`format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer`	Extrahiert Informationen über Microsoft Exchange-Hub-Transport-Server
`Get-StorageGroup`	`-server "+$hname+" | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv`	Extrahiert Informationen über den Speicher und exportiert sie in eine Datei
`Get-MailboxDatabase`	`| select LogFolderPath | format-table -autosize -hideTableHeaders; Get-MailboxDatabase | select EdbFilePath| format-table -autosize -hideTableHeaders;Get-MailboxDatabase | select TemporaryDataFolderPath| format-table -autosize -hideTableHeaders`	Extrahiert Informationen über die Microsoft Exchange-Postfachdatenbank

MySQL-Server (unter Linux)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	(Nur unter Unix) Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`ps`	`--pid=[process.pid] --no-headers -o " %U : %p : %a”`	Ruft den Parameterwert „userid“ ab

MySQL-Cluster-MGM-Knoten (unter Linux)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`ps`	`--pid=[process.pid] --no-headers -o " %U : %p : %a”`	(Nur unter Unix) Ruft den Parameterwert „userid“ ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nginx (unter UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a"*	Ruft den Parameterwert „userid“ ab
ls	*[IncludeTabletmp[].files]*	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf
cat	*[IncludeTabletmp[].files]*	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Zeigt den Dateiinhalt an

Oracle E-Business-Suite (ein UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
export	-	Legt Variablen fest
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung mit Oracle Instanz.
awk	Verschiedene Optionen	Ändert die Ausgabe
netstat	Verschiedene Optionen	Ruft offene Ports ab

Oracle Warteschlange für erweiterte Warteschlange (ein UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Gleichzeitiger Server (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur für Unix) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
ls	Verschiedene Optionen	(Nur für Unix) Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	(Nur für Unix) Zeigt den Dateiinhalt in der Ausgabe an
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Discoverer Engine (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	-	Zeigt den Dateiinhalt an

Oracle Discoverer-Benutzeroberfläche (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	-	Zeigt den Dateiinhalt an

Oracle Form-Benutzeroberfläche (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Fulfillment Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle HTTP Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle Metric-Client (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle OACORE-Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle OAFM-Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	Zeigt den Dateiinhalt an
`ps`	`-ef`	Ruft die Prozessinformationen ab
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf.

Oracle IAS-Webmodul (ein UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene Optionen	(Nur für Unix) Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	(Nur für Unix) Zeigt den Dateiinhalt an
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf.

Oracle Prozessmanager (ein UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	Zeigt den Dateiinhalt an

Oracle Berichtsserver (auf UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`cat`	-	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle TnsIsnr-Engine (ein UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle WebLogic-Modul (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

Oracle WebLogic Server (Version 10.3) (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

Oracle Lastenausgleichsmodul für WebLogic-On-Demand-Router (ein UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Tuxedo (ein UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene	Listet Dateien und Ordner im vorgegebenen Ordner auf
`cat`	`-`	Zeigt den Dateiinhalt in der Ausgabe an
`find`	`-name`	Dieser Befehl wird nur zum Erstellen von Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
`netstat`	Verschiedene	Ruft offene Ports ab
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`ps`	`-ef`	(Nur für Unix) Ruft Prozessattribute ab

Oracle Tuxedo-Portal (unter UNIX)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene	Extrahiert Zeichenfolgen aus der Ausgabe
`ls`	Verschiedene	Listet Dateien und Ordner im vorgegebenen Ordner auf
`cat`	`-`	Zeigt den Dateiinhalt in der Ausgabe an

PostgreSQL-Datenbank (unter UNIX)

Befehl	Parameter	Beschreibung
`ls`	`[IncludeTabletmp[].files]`	Dieser Befehl wird zum Erstellen von HTTP-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf

Rabbit MQ (unter UNIX)

Befehl	Parameter	Beschreibung
`ps - ef`	`ps -ef | grep "+ $process.parentProcessId`	Ruft den übergeordneten Prozess ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rabbit MQ (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
	`+" |egrep -v -e grep -e beam`	

Red Hat Cluster Suite (unter Linux)

Befehl	Parameter	Beschreibung
`clustat`	`-x`	Zeigt die Clusterkonfiguration und den Status im XML-Format an

Befehle, für die ein privilegierter Benutzer erforderlich ist, um SAP-Anwendungen zu erkennen: ABAP, SAP Central Services (ASCS), SAP Control Instance, SAP Netweaver Dialog Instance, SAP Evaluated Receipt Settlement (ERS), SAP Java Cluster (SJC), SAP Central Services (SCS) (unter UNIX)

Befehl	Parameter	Beschreibung
`pargs`	`-e`	Ruft das ausführbare Verzeichnis ab.
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`ping`	`-c 1`	Überprüft, ob der Host antwortet
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`Isof` **Hinweis:** Wird in einigen Fällen als Alternative zu netstat verwendet.	`-Pnl +M -i`	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.
`CVERS`	-	Ruft die Version der installierten SAP-Module ab
`DBCONS`	-	Ruft die Verbindungszeichenfolgen für SAP DB ab
`RFCDES`	-	Ruft die Verbindungszeichenfolge zu Systemen ab, die in SAP integriert sind
`sapcontrol`	`-function ABAPGetComponentList`	Ruft die sysid für SAP -Anwendungen und -Komponenten ab.

Sun Directory (unter Solaris)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sun iPlanet Web Server (unter Solaris)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

Sun JES (unter Solaris)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Sybase (unter UNIX)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

TIBCO ActiveMatrix Adapter (unter UNIX)

Befehl	Parameter	Beschreibung
`cat`	-	Zeigt den Dateiinhalt an
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks (unter UNIX)

Befehl	Parameter	Beschreibung
`hostname`	-	Ruft den Hostnamen ab
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`cat`	-	Zeigt den Dateiinhalt an
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX)

Befehl	Parameter	Beschreibung
`hostname`	-	Ruft den Hostnamen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`cat`	-	Zeigt den Dateiinhalt an
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf
`cut`	Verschiedene Optionen	Teilt die Ausgabezeile auf

TIBCO EMS-Warteschlange (unter UNIX)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

TIBCO Enterprise Message Service (EMS) (unter UNIX)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

Zugehörige Informationen

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Die meisten der von Service-Mapping für Erkennung und Zuordnung verwendeten Befehle erfordern keine erweiterten Rechte.

Überprüfen Sie diese Befehlsliste, um zu verstehen, wie Service-Mapping diese verwendet, und um sicherzustellen, dass die virtuelle Sicherheit Ihres Unternehmens nicht beeinträchtigt wird.

Sie führen diese Befehle nicht direkt aus. Service-Mapping verwendet Befehle, die erhöhte Rechte erfordern, als Teil der folgenden Prozesse:

- Hosterkennung
- Prozessidentifikation am Port
- CIs anhand von Mustern entdecken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssysteme

AIX-Befehle

Befehl	Parameter	Beschreibung
`awk`	Verschiedene Optionen	Analysiert die Zeichenfolge
`istat`	`file_name`	Ruft den Zeitpunkt der letzten Änderung der Datei ab
`nslookup`	`hostname`	Löst den DNS-Hostnamen auf
`ping`	`-c count ip/host`	Pingt den Host
`arp -an`	Verschiedene Optionen	Zeigt die ARP-Tabelle an
`grep`	Zu durchsuchende Zeichenfolge	Sucht eine Zeichenfolge in der vorherigen Befehlsausgabe
`traceroute`	`-n ip_address`	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
`netstat`	`-an` `-Aan`	Zeigt offene Netzwerkverbindungen an
`ps`	`-eo user, pid, ppid, comm, args`	Ruft die Prozessliste ab
`find`	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ

HP-UX-Befehle

Befehl	Parameter	Beschreibung
`ping`	`-c count ip/host`	Pingt den Host
`arp -an`		Zeigt die ARP-Tabelle an
`grep`	Zu durchsuchende Zeichenfolge	Sucht eine Zeichenfolge in der vorherigen Befehlsausgabe
`awk`	Verschiedene Optionen	Analysiert die Zeichenfolge
`traceroute`	`-n ip_address`	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
`netstat`	`-an`	Zeigt offene Netzwerkverbindungen an
`ps`	`-eo user, pid, ppid, comm, args`	Ruft die Prozessliste ab
`find`	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM / z /OS

Befehle	Parameter	Beschreibung
sysvar	*SYSNAME*	Ruft den Systemnamen ab
hostname		Ruft den Gerätenamen ab
grep	Zu durchsuchende Zeichenfolge	Sucht nach einer Zeichenfolge in der Befehlsausgabe
hostname	*-*	Ruft den Hostnamen ab
netstat	*-g | awk '{if (NR>4) print \$1,\$3}'*	Ruft Netzwerkinformationen ab
netstat	*-r | awk '{if (NR>3) print \$1,\$2,\$5}'*	Ruft Gateway-Informationen ab
netstat	*-h | awk '{if (NR>4) print \$1}' | grep -v '127.0.0.1'*	Ruft ein IP-Array ab
netstat	*-R ALL | awk '{if (NR>1) print \$0}'*	Ruft Schnittstellen ab
netstat	*df -k | awk '{print \$1,\$2}' |sed -e s'/(//' | sed -e s'/)//' 2> /dev/null*	Ruft die Dateisysteminformationen ab
ps	*-*	Ruft die Prozessliste ab
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	*file-name*	Zeigt den Dateiinhalt an
cut	Verschiedene Optionen	Teilt die Ausgabe gemäß den eingegebenen Parametern auf
uname	*l, v, rm, s*	Ruft den Betriebssytemtyp ab

Linux

Befehle	Parameter	Beschreibung
nslookup	*hostname*	Löst den DNS-Hostnamen auf
ping	*-c count ip* *host*	Pingt den Host
arp	*-an/n*	Zeigt die ARP-Tabelle an
lp n	*-an/n*	Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge *-v*	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Befehle	Parameter	Beschreibung

	`hypervisor`
	`proc`
	`cpuinfo`
	`-i 'attached scsi'`
	`var`
	`log`
	`dmesg`
	`'SCSI device'`
	`'Disk`
	`UUID`	

`awk`	Verschiedene Optionen	Analysiert die Zeichenfolge
`netstat`	`-an`	Zeigt offene Netzwerkverbindungen an
`ss`	`-an`	Zeigt offene Netzwerkverbindungen an
`ps`	`-eo user, pid, ppid, comm, args, wwwx`	Ruft die Prozessliste ab
`egrep`	Verschiedene Optionen	Durchsucht Text in der vorherigen Befehlsausgabe
`find`	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ
`traceroute`	`-n ip_address`	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
`df`	`-kP, echo`	Extrahiert die Informationen zum Dateisystem, einschließlich der Größe in KB
`uptime`	Verschiedene Optionen	Zeigt die aktuelle Uhrzeit, die Betriebsdauer des Systems, die Anzahl der aktuell angemeldeten Benutzer und Durchschnittswerte der Systemlast der letzten 1, 5 und 15 Minuten an
`Datum`	Verschiedene Optionen	Zeigt das Datum in der Zeitzone an, in der das Betriebssystem Linux konfiguriert ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Befehle	Parameter	Beschreibung
perl	*-e 'print time*	Öffnet die Perl-Shell und gibt die Zeit aus
Befehl	*-v vxprint*	Dieser Befehl wird im Debug-Modus verwendet.
uname	*-a* *-r*	Zeigt Systeminformationen an
ipfconfig	*-a*	Zeigt die Konfiguration der Netzwerkschnittstelle an
ip	Weiterleitungsliste *-4 -o addr show* *-6 -o a* *r* Zu analysierende Zeichenfolge	Zeigt Informationen zur Netzwerkschnittstelle an, einschließlich der Weiterleitungstabelle
Route	*-n*	Zeigt die IP-Weiterleitungstabelle an
ip r		Zeigt die IP-Weiterleitungstabelle an
sed	*-n '2!p'*	Führt eine Funktion mit dem Streameditor SED aus
bash	*-c*	Führt den Befehl mit der UNIX-Shell oder der UNIX-Befehlssprache aus
waagent	*-version 2>/dev/null*	Zeigt die vom Microsoft Azure Linux-Agent extrahierten Informationen an

Solaris

Befehl	Parameter	Beschreibung
nslookup	*hostname*	Löst den DNS-Hostnamen auf
ping	*-c count ip/host*	Pingt den Host
arp	*-an*	Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Solaris (Fortsetzung)

Befehl	Parameter	Beschreibung
awk	Verschiedene Optionen	Analysiert die Zeichenfolge
traceroute	*-n ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
netstat	*-an*	Zeigt die offenen Netzwerkverbindungen an
zoneadm	*List*	Zeigt die Liste der Zonen an
egrep	Verschiedene Optionen	Durchsucht Text in der vorherigen Befehlsausgabe
find	Verzeichnis und Parameter	Sucht nach Dateien nach Name oder Typ

Windows WMI-Abfragen

Abfrage	Beschreibung
*Select * from Win32_ComputerSystem*	Ruft grundlegende Informationen zum Server wie die Seriennummer ab
Select LastModified from CIM_LogicalFile Where Name=...	Ruft den Zeitpunkt der letzten Änderung der Datei ab
Select AddressWidth from Win32_Processor	Ruft die Computerarchitektur ab (32 Bit oder 64 Bit)
*Select * From Win32_Process where (ProcessId = ?)*	Ruft die auf dem Computer ausgeführte Prozessliste ab
Select Name from CIM_LogicalDisk	Ruft die Dateisysteme auf dem Computer ab, zum Beispiel C: oder D :
Select FileName, Extension from CIM_Directory where Drive='drive' and Path='path'	Ruft die Liste der Dateien in einem bestimmten Verzeichnis ab

Windows-Befehle

Befehl	Parameter	Beschreibung
get_process_info.exe	*Process_id*	Extrahiert Informationen über die Prozesse mithilfe der von ServiceNow erstellten ausführbaren Datei
type	*File_name*	Zeigt den Inhalt der Textdatei an
nslookup	*Host_name*	DNS-Suche
arp	*-a*	Zeigt die ARP-Tabelle an
netstat	*-ano*	Zeigt die Netzwerkverbindungen an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Befehle (Fortsetzung)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe
`dir`	`/q` `/s /b`	Listet Dateien in den Verzeichnissen auf

`paping`	`--nocolor -c 1 -p`
	`port_num`
	`ip_address`
		Dienstprogramm zum Ausführen von TCP-Ping für den angegebenen Host

`ping`	`-n 1` `ip_address/host`	Pingt den Host
`tracert`	`Ip_address`	Zeigt die Layer-3-Netzwerkroute zum Zielhost an

Anwendungen

A10-Lastenausgleichsmodule

Befehl	Parameter	Beschreibung
`show partition`	Verschiedene Optionen	Ruft die konfigurierte Partition ab
`sh-run all-partitions`	Verschiedene Optionen	Ruft Details wie Informationen über virtuelle Server, Ports, Servicegruppen und Poolmitglieder ab
`show slb virtual-server all-partitions`	Verschiedene Optionen	Ruft den Status des virtuellen Servers und Details zur Trefferanzahl ab

Befehle, die keinen privilegierten Benutzer für die Erkennung von ABAP SAP Central Services (ASCS) erfordern (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`msg_server`	`-V`	Ruft die Version ab
`ping`	`-n 1`	(Nur für Windows) Überprüft, ob der Host antwortet
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehle, die keinen privilegierten Benutzer für die Erkennung von ABAP SAP Central Services (ASCS) erfordern (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
ss	Verschiedene Optionen	Listet die offenen Ports auf.

Active Directory-Domänencontroller (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Ruft offene Ports ab
ss	Verschiedene Optionen	Listet die offenen Ports auf
hostname	-	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet alle Dateien im angegebenen Ordner auf

Apache-Webserver (unter UNIX)

Befehl	Parameter	Beschreibung
httpd	*-V*	Ruft die Version ab
cut	Verschiedene Optionen	Teilt die Ausgabezeile auf
opmnctl	*status -fmt %cmp32%prt32%por40%pid* und *@farm status -noheaders -fsep "|" -fmt %cmp%prt %clu%ins%por*	Dieser Befehl wird nur zum Erkennen der OC4J-Konnektivität verwendet. Ruft den Status des OPMN CTRL-Service ab
sort	*-u*	Dieser Befehl wird nur zum Erkennen der Weblogic-Konnektivität verwendet. Sortiert die Ausgabe

Apache-Webserver (unter Windows)

Befehl	Parameter	Beschreibung
httpd.exe	*-V*	Ruft die Version ab
opmnctl	*status -fmt %cmp32%prt32%por40%pid* und *@farm status -noheaders -fsep "|" -fmt %cmp%prt %clu%ins%por*	Dieser Befehl wird nur zum Erkennen der OC4J-Konnektivität verwendet. Ruft den Status des OPMN CTRL-Service ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Tomcat (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
`find`	`-name`	Erstellt die Webserviceverbindungen. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
`version.sh/version.bat`	`-`	Ruft die Tomcat-Version ab
`java -cp " + $install_directory + "/lib/catalina.jar org.apache.catalina.util.`	`- ServerInfo`	Ruft die Tomcat-Version ab
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf
`find`	`-name`	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
`ss`	Verschiedene Optionen	(Nur für Linux) Listet die offenen Ports auf

Apache Tomcat WAR (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
`version.sh/version.bat`	`-`	Ruft die Tomcat-Version ab
`netstat`	Verschiedene Optionen	(Nur Windows) Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

App TNS-Service (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf
grep	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe

BIG-IP Global Traffic Manager (GTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
Anzeigen	*/gtm pool [wide_ip_pool_4_cmd[1].pool] members*	Dieser Befehl wird nur zum Erstellen von Verbindungen zu Poolmitgliedern verwendet. Ruft die Poolmitglieder ab
list	*/gtm server [servers_from_cmd[].server] addresses*	Dieser Befehl wird nur zum Erstellen von Verbindungen zu Poolmitgliedern verwendet. Listet die Alias-Serveradressen auf

BIG-IP Local Traffic Manager (LTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
b	*rule [rule name] list* und *virtual address [entry_point.ip_address]*	Dieser Befehl wird nur zum Erstellen von Verbindungen aus Regeln verwendet. Listet vorhandene Regeln für BIGPipe auf
list	*ltm rule [rule name]* und *data-group wts_routing_destination_prod | grep -A 1 [ep_uri]*	Dieser Befehl wird nur zum Erstellen von Verbindungen aus Regeln verwendet. Listet vorhandene Regeln für TMSH auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BIG-IP Device Service Clustering

Befehl	Parameter	Beschreibung
show cm traffic-group – get	Verschiedene Optionen	Dieser Befehl wird zum Abrufen von Datenverkehr und Clustering-Informationen verwendet.

BMC CTRL-M Enterprise Manager (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	(Nur für Windows) Listet die offenen Ports auf

BMC CTRL-M Gateway (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Verbindungen zum Control M-Server verwendet. Sucht nach Datei- und Ordnerpfaden
xargs	*grep <string>*	Dieser Befehl wird nur zum Erstellen von Verbindungen zum IBM CTRL-M-Server verwendet. Führt den Befehl an allen Listen der Ausgabe aus

BMC IT Asset Management (ITAM)

Befehl	Parameter	Beschreibung
tnsping	Verschiedene Optionen	Ruft Informationen über Oracle-Verbindungen ab

CA Identity Manager-Bereitstellungsserver (für Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra(Für UNIX)

Befehl	Parameter	Beschreibung
`find`	Verschiedene Optionen	Sucht nach dem Pfad der base init-Konfigurationsdatei.
`Suchen`	Verschiedene Optionen	Sucht nach dem Pfad der base init-Konfigurationsdatei, wenn der Befehl find fehlschlägt
`nodetool version`	Verschiedene Optionen	Ruft ab Apache Cassandra Version.
`nodetool describecluster`	Verschiedene Optionen	Ruft den Clusternamen ab
`nodetool info`	Verschiedene Optionen	Ruft Informationen über Rechenzentrum und Rack ab
`nodetool ring`	Verschiedene Optionen	Ruft die Arbeitsauslastung ab, die für ausgeführt wird Apache Cassandra.
`nodetool tablestats`	Verschiedene Optionen	Ruft eine Liste der in einem Cluster verfügbaren Keyspaces ab
`dse`	`-v`	Ruft den DataStax ab Cassandra Version.
`dsetool ring`	Verschiedene Optionen	Ruft die Arbeitsauslastung ab, die für DataStax ausgeführt wird Cassandra.

Befehlszeilenschnittstelle Cisco ACE (unter Cisco CSM)

Befehl	Parameter	Beschreibung
`Anzeigen`	`context, running`	Zeigt die angeforderten Informationen an
`include`	`-`	Extrahiert Zeichenfolgen aus der Ausgabe
`echo`	`-`	Zeigt Zeichenfolgen in der Ausgabe an

Cisco Global Site Selector (unter Cisco CSM)

Befehl	Parameter	Beschreibung
`Anzeigen`	`gslb-config domain-list`	Zeigt die Domänenliste an
`Anzeigen`	`gslb-config dns rule`	Zeigt die DNS-Regelausgabe an
`Anzeigen`	`gslb-config answer-group`	Zeigt die VIP-Antwort an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Citrix Delivery Controller (unter Windows)

Befehl	Parameter	Beschreibung
powershell	*Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerApplication -Name [entry_point.name]| select Name, CommandLineExecutable,CommandLineArguments, WorkingDirectory, ApplicationType, BrowserName| Format-List* und *Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerApplication -Name [entry_point.name] | select Name,CommandLineExecutable,CommandLineArguments,WorkingDirecto | Format-List* Und *Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerMachine -DesktopGroupName ‘ [delivery_groups[1].name]*	Ruft die von diesem Delivery Controller verwalteten Anwendungen ab

Citrix Usage Collector (unter Windows)

Befehl	Parameter	Beschreibung
qfarm		Erkennt Epic-Symbole

Citrix XenApp (unter Windows)

Befehl	Parameter	Beschreibung
get_xenapp_apps.ps1	*[entry_point.icon_path]*	Führt Powershell-Befehle aus, mit denen Citrix-Symbolinformationen aus dem Citrix-Repository abgerufen werden
powershell	Verschiedene Optionen	Führt PowerShell-Befehle aus

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Citrix Presentation Server (unter Windows)

Befehl	Parameter	Beschreibung
cscript	*//NoLogo*	Führt VB-Skripts ohne Popup-Fenster aus
GetAppsInFolder.wsf	*[entry_point.icon_path]*	Führt vbscript-Befehle aus, mit denen Citrix-Symbolinformationen aus dem Citrix-Repository abgerufen werden

Citrix NetScaler (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
Anzeigen	*cs policy, cs action,cs Policy, lb vserver*	Dieser Befehl wird nur zum Erkennen von ausgehenden Verbindungen verwendet. Zeigt die angeforderten Informationen an
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Citrix NetScaler Global Server Load Balancer (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
Anzeigen	*ns.conf*	Dieser Befehl wird nur zum Erkennen von ausgehenden Verbindungen verwendet, wenn keine SNMP- oder SSH-Anmeldeinformationen bereitgestellt wurden. Zeigt den Inhalt der Datei ns.conf an

Connect-IT Service (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

EMC Documentum Docbase (unter Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

FormEngine (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Allgemeine Anwendung (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
`tasklist`	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
`netsh`	`http show servicestate`	Zeigt einen Snapshot des HTTP-Service an

Allgemeine Anwendung (unter Linux)

Befehl	Parameter	Beschreibung
`systemctl list-units --type service`	Verschiedene Optionen	Zeigt den Servicestatus an
`/bin/systemctl status "+service_name +".service`	Verschiedene Optionen	Zeigt den Servicestatus an
`service --status-all`	Verschiedene Optionen	Zeigt den Servicestatus an
`read /etc/services`	Verschiedene Optionen	Erteilt Zugriff auf die Datei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy(Am UNIX Oder Windows)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
tail	Verschiedene Optionen	(Nur unter Unix) Zeigt das Ende der Ausgabe an

HP Service Manager-Anwendungsserver

Befehl	Parameter	Beschreibung
tnsping	Verschiedene Optionen	Ruft Informationen über Oracle-Verbindungen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

HP Service Manager-Index (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf

HP Service Manager Knowledge Base (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf

IBM WebSphere Message Broker (unter Windows)

Befehl	Parameter	Beschreibung
dmqdocbroker	*-s -c getdocbasemap* und *-t [computer_system.primaryHostname] -s -c getdocbasemap* und *-s -c getservermap [docbas]* *-t [computer_system.primaryHostname] -s -c getdocbasemap* [docbase]	Ruft die Docbase-Informationen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
`del`	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
`BTSTask`	`ExportBindings / Destination:%TEMP %\MyBindings.xml / Database:[MgmtDbName] / server:[serverName]`	Dieser Befehl wird nur verwendet, wenn keine MSSQL-Anmeldeinformationen vorhanden sind. Extrahiert die Bindungsinformationen und fügt sie in die XML-Datei ein

IBM CTRL-M Server (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf
`type`	-	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Zeigt den Dateiinhalt in der Ausgabe an

IBM DB2 (unter Linux)

Befehl	Parameter	Beschreibung
`Quelle`	`[installed_dir]db2profile`	Legt die DB2-Variablen fest
`db2`	list database directory	Zeigt die DB2-Installationsparameter an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM DB2 (unter Linux) (Fortsetzung)

Befehl	Parameter	Beschreibung
`grep`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`Kopf`	`-1`	Zeigt nur die erste Zeile der Ausgabe an
`db2level`	`-`	Zeigt die DB2-Version an
`cat`	`-`	Zeigt den Dateiinhalt in der Ausgabe an
`xargs`	`-I {} echo list tablespace containers for {} ';'`	Dieser Befehl wird zum Erstellen von Speicherverbindungen verwendet. Führt den Befehl an allen Listen der Ausgabe aus

IBM DB2 (unter Windows)

Befehl	Parameter	Beschreibung
`db2cmd`	`/c /w /i`	Listet die DB2-Verzeichnisse auf
`db2`	list database directory	Zeigt die DB2-Installationsparameter an
`find`	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien, Ordnern oder einer Standardausgabe
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`db2level`	`-`	Zeigt die DB2-Version an
`echo`	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Gibt Zeichenfolgen in der Ausgabe aus
`findstr`	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
`Für`	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Führt Schleifen aus

IBM DB2 (unter IBM z/OS)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Ruft den DB2-Namen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM J2EE EAR (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

IBM WebSphere Application Server (unter UNIX)

Befehl	Parameter	Beschreibung
versionInfo.sh	-	Ruft die Version von Websphere Application Server ab

IBM Websphere Application Server (unter IBM z/OS)

Befehl	Parameter	Beschreibung
"oeconsol 'D OMVS,A=ALL' | grep "+ $taskname	-	Ruft die Aufgabe von Websphere Application Server ab
netstat	*-a | grep "+$port+" | awk '{print $1}'*	Ruft den Aufgabennamen vom Listenerport ab
ps -ef -o user,pid,ppid,comm | awk '{print $1,$2,$3, $4}'		Ruft Attribute für Prozesse ab
$install_dir+"/bin/ versionInfo.sh | grep Version | tail -1"		Ruft die Version aus dem Skript ab
$install_dir +"/properties/version/ BASE.product"		Ruft die Version aus der Versionsdatei ab (Failover)
"ls "+$conf_dir +"/*/*/applications/ */deployments/*/META-INF/application.xml \| xargs grep \"<context-root>/"+$uri_search +"\""+" 1>/tmp/app.txt 2>/dev/null; cat /tmp/ app.txt"		Ruft die Liste der URI-Dateien ab
$ear_directory_name +"//*/*/wsdl/*.wsdl"*		Liest die WSDL-Dateien unter der erkannten Inklusion im Ear-Verzeichnis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Portal (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

IBM WebSphere Portal (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

IBM WebSphere Message Broker-Flow (unter UNIX)

Befehl	Parameter	Beschreibung
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
mqsiprofile	*-*	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
echo	*$ODBCINI*	(Nur unter Unix) Dieser Befehl wird nur zum Erstellen von Verbindungen mit IBM DB2 verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker-Flow (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Gibt Zeichenfolgen in der Ausgabe aus

IBM WebSphere Message Broker-Flow (unter Windows)

Befehl	Parameter	Beschreibung
mqsiprofile	*-*	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
ps	*-ef*	Ruft die Prozessinformationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
db2		Zeigt DB2-Installationsparameter an: Datenbankverzeichnis und Knotenverzeichnis

IBM WebSphere Message Broker (unter UNIX)

Befehl	Parameter	Beschreibung
mqsiprofile	*-*	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
echo	*$ODBCINI*	Dieser Befehl wird nur zum Erstellen von Verbindungen mit IBM DB2 verwendet. Gibt Zeichenfolgen in der Ausgabe aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker (unter Windows)

Befehl	Parameter	Beschreibung
mqsiprofile	-	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
ps	*-ef*	Ruft die Prozessinformationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an

IBM MQ (ein UNIX) – Früher IBM WebSphere MQ

Befehl	Parameter	Beschreibung
dspmq	-	Ruft den Status des Warteschlangenmanagers ab
dspmqver	-	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

IBM MQ (ein Windows)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dspmq	-	Ruft den Status des Warteschlangenmanagers ab
dspmqver	-	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

IBM MQ (unter z/OS)

Befehl	Parameter	Beschreibung
netstat	*-a | grep "+$port*	Ruft ab IBM MQ-Name.
df	*-k | grep MQ"*	Ruft das Dateisystem ab
"echo "+ $netstat_info[1].mq_name +" | cut -c1-4"	-	Ruft den Namen des Warteschlangenmanagers ab
"oeconsol '-"+ $queue_manager+" display qmgr ALL' "	-	Ruft die Informationen zum logischen MQ-Namen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM MQ (unter z/OS) (Fortsetzung)

Befehl	Parameter	Beschreibung
`"oeconsol '-"+ $queue_manager+" display queue ("+ $entry_point.queue_name +") ALL' | tr \"(\" \"# \" | tr \")\" \"\""`	-	Ruft die Informationen der MQ-Warteschlange zusammen mit den Informationen zu ihren Verbindungen ab
`"oeconsol '-"+ $queue_manager+" display queue ("+$name +")'"`	-	Ruft die MQ-Warteschlangeninformationen ab
`"oeconsol '-"+ $queue_manager +" display channel(*) CONNAME where(QMNAME EQ "+ $remote_queue_mngr_name +")'"`	-	Ruft die Kanalinformationen ab
`"oeconsol '-"+ $queue_manager+" display qlocal(*) '"`		Ruft die lokalen Warteschlangeninformationen ab

IBM MQ-Warteschlange (am UNIX) – Früher IBM WebSphere MQ-Warteschlange

Befehl	Parameter	Beschreibung
`dspmq`	-	Ruft den Status des Warteschlangenmanagers ab
`dspmqver`	-	Ruft die Version des Warteschlangenmanagers ab
`runmqsc`	`[queue manager]`	Ruft die Warteschlangeninformationen ab

IBM MQ-Warteschlange (am Windows)

Befehl	Parameter	Beschreibung
`dspmq`	-	Ruft den Status des Warteschlangenmanagers ab
`dspmqver`	-	Ruft die Version des Warteschlangenmanagers ab
`runmqsc`	`[queue manager]`	Ruft die Warteschlangeninformationen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JBoss-Modul (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur unter Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf

JBoss (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner
xargs	*grep <string>*	Sucht Zeichenfolgen in allen Dateien, die in der Ausgabedatei gefunden wurden
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf

JRun (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

JRun WAR Inc (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner
xargs	*grep <string>*	Sucht Zeichenfolgen in den Dateien, die in der Ausgabedatei gefunden wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JRun WAR Inc (unter UNIX und Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

Microsoft Exchange CAS (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	-	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
powershell	*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer -status -Identity [hostname]| export-clixml $env:TEMP \exchange_pwrshell_output.xml* und *Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status -Identity [hostname]| export-clixml $env:TEMP \exchange_pwrshell_output.xml* und	Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden. Ruft CAS-Status, Serverrollen und Exchange-Einrichtungsstruktur ab **Wichtig:** Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für Exchange CAS, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Exchange CAS (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung

	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer| format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer`
	und
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer`
	und
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-MailboxServer | format-list`	

`find`	Verschiedene Optionen	Dieser Befehl wird nur verwendet, wenn PowerShell nicht funktioniert. Sucht nach bestimmten Zeichenfolgen in den Dateien und Ordnern
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Microsoft Dynamic CRM (unter Windows)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft BizTalk-Orchestrierung (unter Windows)

Befehl	Parameter	Beschreibung
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus

Microsoft BizTalk Server (unter Windows)

Befehl	Parameter	Beschreibung
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
BTSTask	*ExportBindings / Destination:%TEMP %\MyBindings.xml / Database:[MgmtDbName] / server:[serverName]*	Dieser Befehl wird nur verwendet, wenn keine MSSQL-Anmeldeinformationen vorhanden sind. Extrahiert die Bindungsinformationen und platziert sie in der XML-Datei

Microsoft Exchange-Back-End-Server (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	-	Ruft den Hostnamen ab
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf

Microsoft Exchange-Front-End-Server (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	-	Ruft den Hostnamen ab
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf

Microsoft FAST Search Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Exchange-Hub-Transport-Server (unter Windows)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf
`hostname`	-	Ruft den Hostnamen ab
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`tasklist`	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
`echo`	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
`del`	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen

`powershell`	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP \exchange_pwrshell_output.xml`
	
	und
	`"Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status -Identity [entry_point.host_name] | export-clixml $env:TEMP \exchange_pwrshell_output.xml`
		Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden.
		
		Liefert den CAS-Status, die Serverrollen und die Exchange-Einrichtungsstruktur
		
		Wichtig: Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für Exchange Hub Transport-Server, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.

`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`find`	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Microsoft Internet Information Services (IIS) (unter Windows)

Befehl	Parameter	Beschreibung
`appcmd.exe`	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 7 und höher verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuelles Verzeichnis für Microsoft Internet Information Services (IIS) (unter Windows)

Befehl	Parameter	Beschreibung
appcmd.exe	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 7 und höher verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab
iisapp.vbs	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 6 verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf

Microsoft .NET-Befehle (unter Windows)

Befehl	Parameter	Beschreibung
ildasm.exe	Text, der den exe-Prozesspfad enthält	Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei für den ILDisassembler-Alias auszuführen. Diese Datei zerlegt Zeichenfolgen aus der .exe-Befehlsdatei.
.findstr	Verschiedene Optionen	Ruft die Zeichenfolgen aus der Ausgabe ab
dir	Verschiedene Optionen	Listet alle Dateien im angegebenen Ordner auf
connection_strings_browser.exe	*[encrypted_configs[*].Name]*	Dieser Befehl wird nur zum Erstellen von verschlüsselten Datenbankverbindungen verwendet. Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei für den ConnectionStringsBrowser-Alias auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft .NET-Befehle (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Entschlüsselt die Datenbankverbindungen

Microsoft Exchange-Postfach (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	-	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
powershell	*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP \exchange_pwrshell_output.xml* und *Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status | export-clixml $env:TEMP \exchange_pwrshell_output* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP \exchange_pwrshell_output.xml* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ClusteredMailBoxServerStatus*	Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden. Ruft den Status, die Serverrollen und die Einrichtungsstruktur des Exchange-Postfachs ab **Wichtig:** Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für das Exchange-Postfach, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung

	`| format-table -Property OperationalMachines`
	
	und
	
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer`
	
	und
	
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer`
	
	und
	
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-StorageGroup -server [hostname] | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv`
	
	und
	
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-StorageGroup | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv`
	
	und
	
	`Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-MailboxDatabase | select LogFolderPath | format-table -autosize -hideTableHeaders; Get-MailboxDatabase | select EdbFilePath| format-table -autosize -hideTableHeaders;Get-MailboxDatabase`	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	`| select TemporaryDataFolderPath| format-table -autosize -hideTableHeaders`	
`find`	Verschiedene Optionen	Dieser Befehl wird nur verwendet, wenn PowerShell nicht funktioniert. Sucht nach bestimmten Zeichenfolgen in den Dateien und Ordnern
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Microsoft SharePoint (unter Windows)

Befehl	Parameter	Beschreibung
`hostname`	`-`	Ruft den Hostnamen ab

Microsoft SQL-Datenbank (unter Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`hostname`	`-`	Ruft den Hostnamen ab
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

`sqlcmd`	`-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Q select nvcname###inboundtransporturl FROM adm_ReceiveLocation rl, bts_receiveport rp where rl.receiveportid=rp.nid`
	
	und
	
	`-Stcp: [computer_system.primaryManagementIP], [port] -d`
		Dieser Befehl wird nur zum Erkennen von Microsoft BizTalk verwendet.
		
		Ruft die BizTalk-Informationen aus der Datenbank ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft SQL-Datenbank (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	[entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nvcName,nApplicationID from bts_receiveport und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nvcName,nApplicationID from bts_sendport* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nOrcPortID,nReceivePortID,nSendPortid from bts_orchestration_port_binding* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nOrchestrationID from bts_orchestration_port* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y*	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft SQL-Datenbank (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	0 -h-1 -Qselect nID,nvcFullName from bts_orchestration und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect ah.Name###bo.nvcNamespace.bo.nvcName###ase.Name from bts_orchestration bo, adm_Host ah,adm_server ase,adm_Server2HostMapping ash where bo.nAdminHostID = ah.ID and ase.ID = ash.ServerID and ah.ID = ash.HostID* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nSendPortID,nvcAddress from bts_sendport_transport*	

Microsoft Message Queuing (MSMQ) (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf

Microsoft SQL-Datenbank (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft SQL-Datenbank (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
sqlservr.exe		Ruft die Version der Datenbank aus der ausführbaren Datei ab

MongoDB-Datenbank (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
mongo	--eval db.printShardingStatus()	Ruft den Status von MondoDB ab, der für den Lastenausgleich verwendet wird
mongo	--db.Name()	Ruft den Namen der mit dem MongoDB-Server verbundenen Datenbank ab

MySQL-Server (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a”*	Ruft den Parameterwert „userid“ ab
mysqld-nt/mysqld/ mysqld.exe	*-V*	Ruft die Version ab
mysql	*--user=[username] --password=[password] --port=[jdbc_port] --skip-column-names --silent --execute="SHOW ENGINE NDB STATUS;;”* und *--user=[username] --password=[password] --port=[jdbc_port] --skip-column-names --silent --execute="SHOW SLAVE STATUS;;”* und *--user=[username] --password=[password]*	Dieser Befehl wird nur zum Erstellen von Clusterknoten-Verbindungen sowie primären und sekundären Replikationen verwendet. Ruft die Bereitstellungsstruktur des MySQL-Servers ab

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Server (unter Windows oder UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
	`--port=[jdbc_port] --skip-column-names --silent --execute="select host from information_schema.processlist where command like '%%binlog%%';;”`	
`Welche`	`mysql`	Dieser Befehl wird nur zum Erstellen von Clusterknoten-Verbindungen sowie primären und sekundären Replikationen verwendet. Ruft den vollständigen Pfad der MySQL-Clusterknoten ab

MySQL-Cluster-MGM-Knoten (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

`ndb_mgmd`	`-V`
	und
	`-e show`
		Ruft die Version und den Status des MySQL Cluster MGM-Knotens ab

Nginx (unter UNIX)

Befehl	Parameter	Beschreibung
`nginx`	`-v`	Ruft die Version ab
`egrep`	`-v -e ^# -e "\t#"`	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Ignoriert Sonderzeichen

Oracle E-Business Suite (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`findstr`	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle E-Business Suite (unter Windows oder UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
export	-	(Nur für Unix) Legt Variablen fest
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung zur Oracle-Instanz
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
netstat	Verschiedene Optionen	(Nur für Windows) Listet offene Ports auf

Oracle Advanced Queue-Warteschlange (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
export	-	(Nur unter Unix) Legt eine Variable fest
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung zur Oracle-Instanz
Festlegen	-	(Nur unter Windows) Legt eine Variable fest
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf

Oracle Concurrent Server (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	(Nur für Windows) Listet die offenen Ports auf
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Discoverer Engine (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Discoverer-Benutzeroberfläche (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Form-Benutzeroberfläche (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Fulfillment Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle HTTP Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Metric-Client (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle OACORE-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle OAFM-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter UNIX)

Befehl	Parameter	Beschreibung
export	-	Legt die Variable fest
sqlplus	*-s [username]/ [password]@[entry_point.instance]*	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Oracle-Version und Informationen zur erweiterten Warteschlange ab
echo	*-e set head off feed off pages 0 line 3000\ \n\"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und *set head off feed off pages 0 line 3000\ \n\"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und *select member as NEEBULA from v\ $logfile;* und *select value as NEEBULA from v\$parameter where name='log_archive_dest'* und *select file_name as NEEBULA from dba_data_files;*	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Informationen zur erweiterten Warteschlange, den Speichergeräten und Datenbanklinks ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
	und `select DB_LINK,HOST from DBA_DB_LINKS`	

`lsnrctl`	`version`
	Und
	`services`
		Dieser Befehl wird nur zur Erkennung der RAC-Version (Real Application Cluster) verwendet.
		Ruft die RAC-Version ab

Oracle Database (unter Windows)

Befehl	Parameter	Beschreibung
`Festlegen`	`-`	Legt die Variable fest
`sqlplus`	`-s [username]/ [password]@[entry_point.instance]`	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Oracle-Version und Informationen zur erweiterten Warteschlange ab

`echo`	`-e set head off feed off pages 0 line 3000\ \n\"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);`
	und
	`set head off feed off pages 0 line 3000\ \n\"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);`
	und
		Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet.
		Ruft die Informationen zur erweiterten Warteschlange, den Speichergeräten und Datenbanklinks ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung

	`select member as NEEBULA from v\$logfile;`
	und
	`select value as NEEBULA from v\$parameter where name='log_archive_dest'`
	und
	`select file_name as NEEBULA from dba_data_files;`
	und
	`select DB_LINK,HOST from DBA_DB_LINKS`	

`lsnrctl`	`version`
	Und
	`services`
		Dieser Befehl wird nur zur Erkennung der RAC-Version (Real Application Cluster) verwendet.
		Ruft die RAC-Version ab

`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

Oracle iAS-Webmodul (unter Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`find`	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Webservices-Verbindungen verwendet. Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Net Listener (unter UNIX)

Befehl	Parameter	Beschreibung
`lsnrctl`	`version` und `status`	Ruft die Version und den Status des Oracle Net Listener ab
`export`	-	Legt die Variable fest
`crsctl`	`status res -t` und `config service -d`	Ruft den Servicestatus und die Konfiguration ab

Oracle PeopleSoft (unter UNIX)

Befehl	Parameter	Beschreibung
`psadmin`	Verschiedene Optionen	Ruft Informationen aus dem PeopleSoft-Repository oder -Server ab
`tnsping`	Verschiedene Optionen	Ruft Informationen zur Datenbankinstanz ab, die dem Befehl tnsping übergeben wurden
`sqlplus`	Verschiedene Optionen	Stellt eine Verbindung mit der Datenbankinstanz her und führt die SQL-Abfrage aus

Oracle-Prozessmanager (unter Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
`find`	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle Report Server (unter Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`dir`	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Report Server (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle Tnslsnr-Engine (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle WebLogic-Modul (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle WebLogic Server (Version 10.3) (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle WebLogic-On-Demand-Router-Lastenausgleichsmodul (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle WebLogic-On-Demand-Router-Lastenausgleichsmodul (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
versionInfo.sh	-	Ruft die Version von Websphere Application Server ab

Oracle Tuxedo (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene	(Nur für Windows) Listet alle vorhandenen Dateien im angegebenen Ordner auf
find	Verschiedene	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
find	*-name*	Dieser Befehl wird nur zum Erstellen von Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
tmadmin	*-v*	Ruft die Tuxedo-Version ab
netstat	Verschiedene	Ruft offene Ports ab
ss	Verschiedene Optionen	Listet die offenen Ports auf

Oracle Tuxedo-Portal (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene	(Nur für Windows) Listet alle vorhandenen Dateien im angegebenen Ordner auf
find	Verschiedene	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Tuxedo-Portal (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
find	*-name*	Dieser Befehl wird nur zum Erstellen von Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

PostgreSQL-Datenbank (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
postgres	*-v*	Ruft die Version ab
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

Red Hat Cluster Suite (unter Linux)

Befehl	Parameter	Beschreibung
ps	*-ef*	Zeigt den derzeit ausgeführten Prozess an
grep	Verschiedene Optionen	Durchsucht Nur-Text-Datensätze nach Zeilen, die dem regulären Ausdruck entsprechen
grep	*-v <string>*	Durchsucht Nur-Text-Datensätze nach Zeilen, die nicht dem regulären Ausdruck entsprechen
ps	*-ef | grep corosync | grep -v grep'*	Überprüft, ob der Corosync-Prozess auf dem Server ausgeführt wird Wenn der Prozess ausgeführt wird, läuft das Red Hat-Cluster auf diesem Server.
ifconfig	*-*	Zeigt Informationen zur aktuellen Netzwerkkonfiguration an
ip a	*-*	Zeigt Informationen zur aktuellen Netzwerkkonfiguration an
awk	Verschiedene Optionen	Ändert die Ausgabe
hostname	*-s*	Zeigt den vollständig qualifizierten Domänennamen (FQDN) an
hostname	*-f*	Zeigt die Kurzform des Hostnamens an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP BO BOXI ScheduleRouter (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
type	*-*	
tnsping	*instance*	Dieser Befehl wird zum Erstellen von Verbindungen zu Oracle verwendet.

SAP Business Objects CMS-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tnsping	*instance*	Dieser Befehl wird zum Erstellen von Verbindungen zu Oracle verwendet. Ruft die Version ab

SAP-Zentralinstanz (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
disp + work	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

SAP NetWeaver-Dialoginstanz (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
disp + work	*-V*	Ruft die Version ab
ping	*-c 1*	(Nur für Unix) Überprüft, ob der Host antwortet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP NetWeaver-Dialoginstanz (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
`ping`	`-n 1`	(Nur für Windows) Überprüft, ob der Host antwortet
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

SAP Evaluated Receipt Settlement (ERS) (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`disp + work`	`-V`	Ruft die Version ab
`ping`	`-n 1`	(Nur für Windows) Überprüft, ob der Host antwortet
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Listet die offenen Ports auf	Listet die offenen Ports auf

SAP HANA-Datenbank (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`hdbsql`	`-v`	Ruft die Version ab

SAP HANA-Datenbankkatalog auf UNIX

Befehl	Parameter	Beschreibung
`hdbsql`	Verschiedene Optionen	• Ruft Schemainformationen ab • Ruft die Zeitzone ab • Ruft die Datenträgergröße ab

SAP-Java-Cluster (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`dir`	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
`jlaunch`	`-V`	Ruft die Version ab
`ping`	`-n 1`	(Nur für Windows) Überprüft, ob der Host antwortet
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP Central Services (SCS) (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
msg_server	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

SQL Server Analysis Services (SSAS) (unter Windows)

Befehl	Parameter	Beschreibung
MsMdSrv.exe	*-n*	Ruft den Instanznamen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf

SQL Server Integration Services-Auftrag (SSIS) (unter Windows)

Befehl	Parameter	Beschreibung
MsMdSrv.exe	*-n*	Ruft den Instanznamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern
sqlcmd	*-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect convert(varchar(max), convert(varbinary(max),packagedata))from msdb.dbo.sysssispackages where name = '[name]' -o [tmp_dir]/[name].xml* und *-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect convert(varchar(max), job_id)###[command]@@@*	Dieser Befehl wird nur zum Erkennen von Aufträgen verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server Integration Services-Auftrag (SSIS) (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	from msdb.dbo.sysjobsteps und *-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect [name]###convert(varchar(max), job_id) from msdb.dbo.sysjobs*	

SQL Server Integration Services (SSIS) (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern
sqlcmd	*-Stcp: [computer_system.primaryManagementIP], [port] -h-1 -E -QSELECT [name]###DB FROM msdb.dbo.sysssispackages* und *-Stcp: [computer_system.managementIP], [port] -h-1 -E -QSELECT [name]###DB FROM msdb.dbo.sysssispackages* und *-Stcp: [computer_system.primaryManagementIP], [port] -h-1 -E -QSELECT [name]###JOB FROM msdb.dbo.sysjobs* und *-Stcp: [computer_system.managementIP],*	Dieser Befehl wird nur verwendet, wenn Sie Auftrage erkennen müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server Integration Services (SSIS) (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	`[port] -h-1 -E -Q SELECT [name]###JOB FROM msdb.dbo.sysjobs`	

Sun Directory (unter Solaris)

Befehl	Parameter	Beschreibung
`slapd-dirserv`	`-D [instance] -v`	Ruft die Version ab
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

Sun JES (unter Solaris)

Befehl	Parameter	Beschreibung
`configutil`	`-`	Ruft die JES-Konfiguration ab

Sybase (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
`dataserverv`	`-v`	Ruft die Version ab
`dir`	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

Symantec Enterprise Vault (unter Windows)

Befehl	Parameter	Beschreibung
`findstr`	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf
`ping`	`-n 1[ip]`	Überprüft, ob der SQL-Server ausgeführt wird

TIBCO ActiveMatrix Adapter (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
`hostname`	`-`	Ruft den Hostnamen ab
`"IFS=$'\n';for i in `find " + $tra_home + " -type f | grep -v / tmp | egrep \".process $\|.substvar$\"`; do result=`grep \"" + $entry_point.queue +`	`-`	Scannt die Bezeichnungsdatei und stellt die tatsächlichen Werte bereit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix Adapter (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
"\" $i`; echo $i### $result@@@; done| grep -v \"###@@@\""		

TIBCO ActiveMatrix BusinessWorks (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
TibcoFilesParser.ksh	-	(Nur für Unix) Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei auszuführen. Dadurch werden alle Tags in Tibco-Konfigurationsdateien ersetzt und im Ordner /tmp abgelegt.
hostname	-	Ruft den Hostnamen ab
cd	-	(Nur unter Unix) Ändert das Verzeichnis
chmod	-	(Nur unter Unix) Ändert Dateiberechtigungen
Für	Verschiedene Optionen	(Nur unter Unix) Führt Schleifen aus
echo	Verschiedene Optionen	(Nur unter Unix) Druckt Zeichenfolgen in der Ausgabe
Wenn	Verschiedene Optionen	(Nur unter Unix) Startet eine Bedingung
wc	*-l*	(Nur unter Unix) Zählt die Ausgabezeilen
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
hostname	-	Ruft den Hostnamen ab
cd	-	(Nur unter Unix) Ändert das Verzeichnis
chmod	-	(Nur unter Unix) Ändert Dateiberechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
Für	Verschiedene Optionen	(Nur unter Unix) Führt Schleifen aus
echo	Verschiedene Optionen	(Nur unter Unix) Druckt Zeichenfolgen in der Ausgabe
Wenn	Verschiedene Optionen	(Nur unter Unix) Startet eine Bedingung
wc	*-l*	(Nur unter Unix) Zählt die Ausgabezeilen
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Listet die offenen Ports auf	Listet die offenen Ports auf
cut	Verschiedene Optionen	(Nur unter Unix) Teil die Ausgabezeile

TIBCO Enterprise Message Service(EMS)-Warteschlange (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
rm	*-f /tmp/ems.cmd*	Bereitet das EMS-Skript vor
tibemsadmin	*-server tcp://+[computer_system.primaryManagementIP]:[port] -user [username] -password [password] -script [script]*	Stellt eine Verbindung mit dem EMS-Administrator her und ruft die Liste der EMS-Warteschlangenverbraucher ab
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus

TIBCO Enterprise Message Service (EMS) (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
rm	*-f /tmp/ems.cmd*	Bereitet das EMS-Skript vor
tibemsadmin	*-server tcp://+[computer_system.primaryManagementIP]:[port] -user [username] -password [password] -script [script]*	Stellt eine Verbindung mit dem EMS-Administrator her und ruft die Liste der EMS-Warteschlangenverbraucher ab
echo	Verschiedene Optionen	(Nur unter Windows) Druckt Zeichenfolgen in der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern

SNMP-basierte Abfragen

Service-Mapping greift über SNMP v1/v2c/v3 (Simple Network Management Protocol) auf Geräte der Netzwerkinfrastruktur wie Lastenausgleichsmodule und Router zu. Konfigurieren Sie SNMP-Community-Anmeldeinformationen, um diesen Zugriffstyp zu aktivieren.

Konfigurieren Sie SNMP-Community, wenn Sie SNMP v1/v2 verwenden, bzw. SNMPv3-Anmeldeinformationen, wenn Sie SNMP v3 verwenden. Informationen zum Betrieb finden Sie unter SSH-Anmeldeinformationen .

SNMP-basierte Abfragen haben das Format von Zeichenfolgen mit ganzen Zahlen.

Allgemeine SNMP-basierte Abfragen

Stellen Sie sicher, dass der Benutzer über Anmeldeinformationen für SNMPv3 verfügt, es sei denn, es wird eine schreibgeschützte Community-Zeichenfolge verwendet.

- 1.3.6.1.2.1.47.1.1.1.1.13
- 1.3.6.1.2.1.1.6
- 1.3.6.1.2.1.47.1.1.1.1
- 1.3.6.1.4.1.9.9.774.1.1.1
- 1.3.6.1.4.1.9.6

SNMP-basierte Abfragen für Switches und Router

- 1.3.6.1.4.1.9.9.46.1.3.1.1
- 1.3.6.1.4.1.9.9.68.1.2.1.1
- 1.3.6.1.2.1.17.1.4.1
- 1.3.6.1.2.1.17.4.3.1
- 1.3.6.1.2.1.17.7.1.2.2.1
- 1.3.6.1.2.1.17.2.15.1
- 1.3.6.1.4.1.9.9.23.1.2.1.1
- 1.3.6.1.4.1.45.1.6.13.2.1.1
- 1.0.8802.1.1.2.1.4.2.1
- 1.0.8802.1.1.2.1.4.1.1

A10 Thunder-Serie

- 1.3.6.1.4.1.1872.2.5.1.1.1.11
- 1.3.6.1.4.1.1872.2.5.3.1.3.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.2.4.1
- 1.3.6.1.4.1.1872.2.5.1.3.1.10
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.6.3.1
- 1.3.6.1.4.1.22610.2.4.1.1.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.22610.2.4.1.6.2
- 1.3.6.1.4.1.22610.2.4.3.4.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.2.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.3.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.4.3.1.1
- 1.3.6.1.4.1.22610.2.4.3.3.3.1.1

BIG-IP Local Traffic Manager (LTM) F5 (unter F5 BIG-IP) und BIG-IP Global Traffic Manager (GTM) F5

- 1.3.6.1.4.1.3375.2.1.6.3
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.3.3.3
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.1.2.1.1.2.1
- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.3.12.1.2.1
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.1.4.2
- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.2.10.8.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.4.2
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.3.11.1.2.1
- 1.3.6.1.4.1.3375.2.3.12.3.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.3.12.3.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.3.12.5.2.1
- 1.3.6.1.4.1.3375.2.3.6.7.2.1
- 1.3.6.1.4.1.3375.2.3.11.4.2.1
- 1.3.6.1.4.1.3375.2.3.3.1.2.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.3375.2.3.3.3.2.1
- 1.3.6.1.4.1.3375.2.3.9.1.2.1
- 1.3.6.1.4.1.3375.2.3.9.3.2.1

Cisco Content Services Switch (CSS)

- 1.3.6.1.4.1.2467.1.16.4.1
- 1.3.6.1.4.1.2467.1.31.3
- 1.3.6.1.2.1.1.2
- 1.3.6.1.4.1.2467.4.1
- 1.3.6.1.4.1.2467.4.2
- 1.3.6.1.4.1.2467.4.3
- 1.3.6.1.4.1.2467.4.4
- 1.3.6.1.2.1.1.1
- 1.3.6.1.4.1.2467.1.15.2.1
- 1.3.6.1.4.1.2467.1.16.4.1
- 1.3.6.1.4.1.2467.1.18.2.1

Cisco Global Site Selector (GSS)

- 1.3.6.1.2.1.1.5 - zum Abrufen des Hostnamens
- 1.3.6.1.2.1.1.1 - zum Abrufen des Produktnamens

Citrix Netscaler

- 1.3.6.1.4.1.5951.4.1.3.6.1
- 1.3.6.1.4.1.5951.4.1.3.2.1
- 1.3.6.1.4.1.5951.4.1.3.1.1
- 1.3.6.1.4.1.5951.4.1.2.7.1
- 1.3.6.1.4.1.5951.4.1.2.2.1
- 1.3.6.1.4.1.5951.4.1.2.11.1
- 1.3.6.1.4.1.5951.4.1.2.1.1
- 1.3.6.1.4.1.5951.4.1.1.6
- 1.3.6.1.4.1.5951.4.1.1.26.1
- 1.3.6.1.4.1.5951.4.1.1.24.1
- 1.3.6.1.4.1.5951.4.1.1.14
- 1.3.6.1.2.1.55.1.8.1
- 1.3.6.1.2.1.47.1.1.1.1
- 1.3.6.1.2.1.4.20.1
- 1.3.6.1.2.1.2.2.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.2.1.2.2.1
- 1.3.6.1.2.1.1.5

Citrix NetScaler Global Server-Lastenausgleichsmodul

- 1.3.6.1.4.1.5951.4.1.1.51.3.1.1
- 1.3.6.1.4.1.5951.4.1.2.1.1

HPE BladeSystem-Gehäuse

- 1.3.6.1.4.1.232.22.2.3.1
- 1.3.6.1.4.1.11.5.7.1.2

IBM WebSphere DataPower

- Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.2.1.4.20.1
  - 1.3.6.1.2.1.2.2.1
  - 1.3.6.1.4.1.14685.3.1.196.1
  - 1.3.6.1.4.1.14685.3.1.11.1
  - 1.3.6.1.4.1.14685.3.1.112.1
- Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.4.1.14685.3.1.11.1

Juniper Junos

1.3.6.1.4.1.2636.3.1.3

Filer Storage-Array für Netzwerkgerät

- 1.3.6.1.4.1.789.1.1.2
- 1.3.6.1.4.1.789.1.1.9

Radware Alteon NG

- 1.3.6.1.4.1.1872.2.5.4.2.32.1
- 1.3.6.1.4.1.1872.2.5.1.1.1.11
- 1.3.6.1.4.1.1872.2.5.3.1.3.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.2.4.1
- 1.3.6.1.4.1.1872.2.5.1.3.1.10

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.6.3.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.2.1.1.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.5.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.3.3.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.2.2.1
- 1.3.6.1.2.1.4.24.4.1
- 1.3.6.1.4.1.89.35.1.13.1.2
- 1.3.6.1.4.1.89.2.12
- 1.3.6.1.4.1.89.2.4
- 1.3.6.1.4.1.89.35.1.40.52.1.1
- 1.3.6.1.4.1.89.35.1.13.1
- 1.3.6.1.4.1.89.35.1.30.1
- 1.3.6.1.2.1.68.1.3.1
- 1.3.6.1.4.1.89.35.1.13.1
- 1.3.6.1.4.1.89.35.1.11.1
- 1.3.6.1.4.1.89.35.1.40.52.1.1

Zugehörige Informationen

ITOM Content Service – Referenz

Erkennungsverhalten für Unix-basierte Lastenausgleichsmodule erstellen

Wenn Ihr Netzwerk Lastenausgleichsmodule verwendet, die auf Linux-Hosts ausgeführt werden, erstellen Sie ein Erkennungsverhalten, um sicherzustellen, dass Service-Mapping und Discovery diese korrekt erkennen.

Vorbereitungen

Stellen Sie sicher, dass Discovery aktiviert ist.

Erforderliche Rolle: Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Der Erkennungs- und Zuordnungsprozess beginnt mit der Identifizierung des Hosts durch Discovery. Nach Abschluss der Host-Erkennung startet Service-Mapping die Erkennung, um auf diesem Host ausgeführte Anwendungen zu erkennen und zuzuordnen.

Der Standarderkennungsprozess identifiziert ein Configuration Item (CI) als Linux-Server, wenn ein verwendeter SSH-Port gefunden wird. Dies kann zu einer falschen Erkennung von Lastenausgleichsmodulen führen, die unter Linux als Linux-Server ausgeführt werden. Erstellen Sie ein Erkennungsverhalten, um zuerst Netzwerkgeräte mit dem SNMP-Protokoll zu erkennen. Nach Discovery Hat Unix-basierte Lastenausgleichsmodule richtig erkannt und die entsprechenden CIs für sie erstellt. Sie können mit der Erkennung und Zuordnung von Anwendungsservices in fortfahren Service-Mapping.

Discovery führt die Erkennung über einen MID-Server durch, der sich im privaten Unternehmensnetzwerk befindet. Ein Verhalten bestimmt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Welchen MID Server Discovery verwendet
- Welche Probes und Muster des ausgewählten MID-Server s ausgeführt werden

Prozedur

1. Erstellen Sie ein neues Verhalten zum Erkennen von Unix-basierten Lastenausgleichsmodulen:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Verhalten**an.
   b. Klicken Sie auf **Neu**.
   c. Geben Sie den Namen für dieses Verhalten ein.
   d. Klicken Sie mit der rechten Maustaste auf den Header und wählen Sie **Speichern** aus.
   e. Klicken Sie auf der Registerkarte **Discovery-Funktionalität** auf **Neu**.
   f. Geben Sie 1 in das Feld **Phase** ein.
   g. Wählen Sie **Nur SNMP** aus der Liste der **Funktionalitätendefinition** aus.
   h. Wählen Sie im Bereich **MID Server** die relevanten MID Servers aus.
   i. Aktivieren Sie das Kontrollkästchen **Aktiv**.
   j. Klicken Sie auf **Absenden**.
2. Erstellen Sie einen Erkennungszeitplan für das neu definierte Verhalten:
   a. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
   b. Klicken Sie auf **Neu**.
   c. Füllen Sie die Felder wie folgt aus:

Erkennungszeitplan-Formular für Discovery

Feld	Beschreibung
Name	Geben Sie einen eindeutigen, beschreibenden Namen für den Zeitplan ein.
Erkannt	Wählen Sie **Konfigurationselemente** aus.
Methode für MID Server-Auswahl	Wählen Sie **Verhalten verwenden** aus.
Verhalten	Wählen Sie das Verhalten aus, das Sie in Schritt 1 erstellt haben.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diesen Zeitplan zu aktivieren. Wenn Sie das Kontrollkästchen deaktivieren, wird der Zeitplan deaktiviert. Sie können über dieses Formular jedoch weiterhin manuell eine Erkennung mit den konfigurierten Werten ausführen.
Max. Ausführungszeit	Legen Sie eine Zeitbegrenzung für die Ausführung dieses Zeitplans fest. Nach Ablauf der konfigurierten Zeit werden die verbleibenden Aufgaben für die Erkennung abgebrochen, auch wenn der Scan nicht abgeschlossen ist. Verwenden Sie dieses Feld, um die Systemlast auf ein gewünschtes Zeitfenster zu beschränken. Wenn in dieses Feld kein Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	eingegeben wird, wird dieser Zeitplan solange ausgeführt, bis er abgeschlossen ist.
Max. Leerlaufzeit	Legen Sie eine Zeitgrenze für Inaktivität während der Discovery fest, um verzögerte Prozesse automatisch abzubrechen und das Ereignis zu protokollieren. Eine Discovery wird nur als inaktiv betrachtet, wenn keine Eingabedatensätze verarbeitet werden und nichts im Verarbeitungsstatus verbleibt. Die Leerlaufzeit wird vom letzten Change zu einem ECC-Warteschlangendatensatz gemessen. Die konfigurierte Leerlaufzeit wird zu Beginn der Discovery festgelegt und spiegelt bis zur nächsten Ausführung keine Änderungen wider. Wenn in dieses Feld kein Wert eingegeben wird, wird dieser Zeitplan bis zum Abschluss oder Abbruch ausgeführt.
„Ausführen“ und zugehörige Felder	Bestimmt den Ausführungszeitplan der Erkennung. Konfigurieren Sie die Häufigkeit im Feld **Ausführen** und in den anderen Feldern, die angezeigt werden, um eine genaue Zeit anzugeben. **Hinweis:** Für die Ausführungszeit wird immer die Systemzeitzone verwendet. Wenn Sie das optionale Feld **Als tz ausführen** hinzufügen, hat dies keine Auswirkungen auf die tatsächliche Ausführungszeit.

3. Erstellen Sie einen IP-Adressbereich für den Erkennungszeitplan:

   Wichtig: Der IP-Bereich für den Zeitplan muss zum IP-Bereich von MID-Server passen, den Sie dem Verhalten zugewiesen haben. Auch der MID-Server muss über die entsprechende Anwendung oder die Anwendung **ALL** verfügen.

   a. Klicken Sie auf der Registerkarte mit den Erkennungs-IP-Bereichen auf **Neu**.

   b. Geben Sie den Namen für diesen IP-Bereich ein.

   c. Konfigurieren Sie den IP-Bereich, indem Sie IP-Adressen in die Felder **IP-Startadresse** und **IP-Endadresse** eingeben.

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

MID-Server

Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist

Stellen Sie vor dem Zuordnen von Anwendungsservices sicher, dass Sie die MID Servers für die Erkennung von Anwendungsservices konfiguriert und alle erforderlichen Host- und Anwendungsanmeldeinformationen angegeben haben.

Vorbereitungen

Um die Bereitschaft der Zuordnung basierend auf Predictive Intelligence zu überprüfen, installieren Sie Service Mapping Plus aus dem ServiceNow Store.

Erforderliche Rolle: Service_Mapping_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping führt einen automatischen Scan der folgenden Ressourcen und Konfigurationen durch, um Ihnen den Bereitschaftsstatus zu geben:

- (Obligatorisch) Es gibt MID Servers mit korrekt konfigurierten IP-Bereichen und Einstellungen für Anwendungen und Funktionen. Weitere Informationen finden Sie unter Konfiguration des MID Servers für Service-Mapping.

  Wenn bei dieser Überprüfung keine richtig konfigurierten MID Servers erkannt werden, können Sie die Massenerkennung nicht ausführen.

- (Optional) Es gibt Anmeldeinformationen für Betriebssysteme und Anwendungen wie in Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping beschrieben.
- (Optional) Während der horizontalen Erkennung wurden mindestens drei Lastenausgleichsmodule erkannt.
- (Optional) In den letzten 14 Tagen wurden durch die horizontale Erkennung mindestens 100 Hosts erkannt.
- (Optional) Die Datensammlung mithilfe von Netflow- oder VPC Flow-Protokollen ist konfiguriert. Diese Konfiguration ist erforderlich, um die datenverkehrsbasierte Erkennung in Service-Mapping zu verbessern. Weitere Informationen finden Sie unter Datenerfassung und -erkennung mit Netflow und Datenerfassung und -erkennung mit VPC-Flow-Protokollen.
- (Optional) Cloud-Discovery ist aktiviert und konfiguriert. Diese Einstellung ist erforderlich, um Anwendungsservices basierend auf IaaS zu erkennen.

Wenn eine optionale Ressource oder Konfiguration fehlt, können Sie Anwendungsservices zwar weiterhin zuordnen, dies kann jedoch dazu führen, dass einige CIs und Verbindungen nur teilweise erkannt werden.

Darüber hinaus führt Service-Mapping die Bereitschaftsprüfung für die Zuordnungsfunktionalität basierend auf Predictive Intelligence durch.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.
2. Überprüfen Sie, dass Service-Mapping eingerichtet und bereit für die Discovery ist.
   Wenn einige obligatorische Konfigurationen fehlen, wird der Fehler oben im Fenster angezeigt.

   a. Klicken Sie auf den Link im Fehler, oder klicken Sie auf das Symbol **Bereitschaftsprüfliste** ( ).

   b. Klicken Sie im Service-Mapping-Fenster „Bereitschaftsprüfliste“ auf den Link neben der Setup-Kategorie mit dem Fehlersymbol ( ).
   Sie können nur dann eine Discovery und Zuordnung durchführen, wenn das Fenster „Bereitschafts-Prüfliste“ keine Fehler enthält.

   c. Führen Sie die erforderliche Aktion aus, um das Setup abzuschließen.
   Konfigurieren Sie beispielsweise fehlende Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn mehr als eine Setup-Kategorie einen Fehler aufweist, kehren Sie zum Fenster „Bereitschafts-Checkliste” zurück, und beheben Sie alle anderen Fehler.
4. Überprüfen Sie, dass Service-Mapping basierend auf Predictive Intelligence bereit für die Erkennung ist.

   a. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**, Und wählen Sie dann aus **Bereitschaft Des Anwendungsservice** Symbol .

   b. Stellen Sie sicher, dass sich alle Elemente in der Liste **Prerequisites status** (Status der Voraussetzungen) im Status **Bereit** befinden.
   Wenn eine der Voraussetzungen nicht erfüllt ist, führen Sie das erforderliche Verfahren aus und wählen Sie dann **Check readiness** (Bereitschaft prüfen) aus.

Nächste Maßnahme

Geschäftsservices im Stapel zuordnen

Zugehörige Informationen

Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Schnellstarttests für Service-Mapping

Führen Sie nach der Aktualisierung und Bereitstellung neuer Anwendungen oder Integrationen Schnellstarttests durch, um sicherzustellen, dass Service-Mapping weiterhin funktioniert. Wenn Sie angepasst haben Service-Mapping, Kopieren Sie die Schnellstarttests, und konfigurieren Sie sie für Ihre Anpassungen.

Service-Mapping-Schnellstarttests erfordern die Aktivierung des Plugins „Service-Mapping“ (com.snc.service-mapping) und das Laden der Demodaten.

Service-Mapping-Schnellstarttests

Test	Beschreibung	Release-Version
SM OOTB: Testet die Sichtbarkeit der SM-Anwendung nach Rollen	Validiert die Sichtbarkeit von Service-Mapping-Anwendungen und -Modulen für verschiedene Rollen. Der Test überprüft zum Beispiel, ob ein Anwender, der mit der Rolle service_mapping_user eingeloggt ist, auf das Administrations-Modul unter Service-Mapping zugreifen kann.	Madrid
SM OOTB: Verifizierung der Servicezuordnung	Testvorlage zur Erstellung anwenderdefinierter Tests, die verifizieren, dass die Topologie der wichtigsten Services nicht geändert wurde. Konfiguriert Werte unter „Datensätze der Testausführung“, um den Namen des zu testenden Service und die in diesem	Orlando, aktualisiert in Paris

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Schnellstarttests (Fortsetzung)

Test	Beschreibung	Release-Version
	Service erwarteten Knoten zu identifizieren. Geben Sie für die Knotennamenwerte das Knotenattribut genau so ein, wie es in der Zuordnung angezeigt wird, z. B. „Apache-Server“. Wenn der Attributname für einen Knoten abgeschnitten ist oder anzeigt, dass ein Knoten ein CI-Cluster ist, konfigurieren Sie diesen Knotennamenswert so, dass er die Darstellung in der Zuordnung widerspiegelt, beispielsweise „11x ExchangeF“ für eine Gruppe von 11 Exchange-Frontend-Servern. **Hinweis:** Sie können diesen Test nicht verwenden, um den Serviceinhalt über die oberste, nicht erweiterte Ebene hinaus zu überprüfen.	
SM OOTB: UI-Barrierefreiheit nach einem Upgrade überprüfen	Führen Sie diesen Test aus, um zu prüfen, ob die Service-Mapping-Anwenderoberfläche nach einem Upgrade vollständig funktionsfähig ist.	Orlando

Zugehörige Informationen

Einen automatisierten Test ausführen

Erweiterte Konfiguration von Service Mapping

Optimieren Sie die Zusammenarbeit von Service-Mapping mit anderen Komponenten und Modulen, und passen Sie die Datenanzeige in Serviceinstanz zuordnungen an.

Zusätzlich zu dem unter Service-Mapping konfigurieren beschriebenen Basissetup können Sie optionale Konfigurationen entsprechend den Anforderungen Ihres Unternehmens vornehmen.

- Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren
- Tag-basierte Discovery-Konfiguration
- Konfigurationsdateien nachverfolgen
- Nachverfolgung von Changes für die Change-Historie feintunen
- Datenerfassung und -erkennung mit Netflow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datenerfassung und -erkennung mit VPC-Flow-Protokollen
- Suchassistenten für Windows konfigurieren
- Anzeige für CI-Attribute ändern
- Unterstützung für Windows-Server mit nicht-englischen Betriebssystemen konfigurieren
- Datei rctrlx.exe auf MID Servers hochladen
- Feinabstimmung Service-Mapping Mit MID-Affinität und IP-Wiederverwendung

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Service-Mapping kann CIs erkennen und zuordnen, indem der ein- und ausgehende Datenverkehr erkannt wird, den die CIs generieren. Erstellen Sie eine datenverkehrsbasierte Erkennungsregel, um zu bestimmen, welche Konfigurationselemente für die datenverkehrsbasierte Zuordnung verfügbar sind.

Vorbereitungen

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Erforderliche Rolle: Service_Mapping_admin

- Stellen Sie sicher, dass die Traffic-basierte Discovery auf aktiviert ist Service-Mapping Produktebene: Navigieren Sie zu **Service-Mapping** > **Administration** > **Eigenschaften** Und verifizieren Sie, dass **Traffic-basierte Discovery** Das Kontrollkästchen ist aktiviert.
- Aktivieren Sie die datenverkehrsbasierte Erkennung für einen bestimmten Serviceinstanz (siehe Beschreibung in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping).

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zur musterbasierten Zuordnung können Sie die datenverkehrsbasierte Erkennung verwenden.

Sie können Regeln erstellen, um Service-Mapping für die Verwendung der datenverkehrsbasierten Erkennung für bestimmte CIs zu konfigurieren. Sie können datenverkehrsbasierte Erkennungsregeln konfigurieren, um bestimmte CIs oder CI-Typen zu überwachen.

Sie aktivieren beispielsweise die Traffic-basierte Discovery für eine bestimmte Serviceinstanz, die eine enthält Tomcat Server, eine MySQL-Datenbank und eine Webanwendung. Sie erstellen eine CI-Typregel, die alle ausschließt Tomcat Server aus Traffic-basierter Discovery. Sie erstellen jedoch auch eine Discovery-Regel, die die Traffic-basierte Discovery für einen bestimmten aktiviert Tomcat Server. Service-Mapping Verwendet die Traffic-basierte Discovery, um die MySQL-Datenbank, die Webanwendung und diese spezifische zu erkennen Tomcat Trotz der CI-Typregel, die alle ausschließt Tomcat Server.

Je nach Konfiguration ist das Systemverhalten bei der datenverkehrsbasierten Erkennung anders. Wenn Predictive Intelligence Ist aktiviert, Service-Mapping Fügt automatisch Verbindungen zu Serviceinstanzen basierend auf Verbindungsregeln hinzu. Diese Vorschläge werden mithilfe von verkehrsbezogenen Daten aus dem generiert Configuration Management Database (CMDB) Und die Analyse von Anwendungsfingerabdrücken, CIs und Prozessen von Predictive Intelligence.

Wenn Discovery auf basiert Predictive Intelligence Ist nicht aktiviert, Service-Mapping Fügt automatisch Traffic-basierte Verbindungen mithilfe von Daten aus dem hinzu CMDB Zu den Serviceinstanzen. Um Ihre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serviceinstanzen jedoch gut organisiert zu halten, müssen Sie möglicherweise Verbindungen zu irrelevanten CIs manuell entfernen. Weitere Informationen zur datenverkehrsbasierten Methode finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wenn in Ihrer Instanz Domänentrennung verwendet wird, können Sie datenverkehrsbasierte Regeln für bestimmte Domänen erstellen. Regeln im Basissystem werden der globalen Domäne zugewiesen und gelten für alle Domänen aller Ebenen.

Wenn Sie eine Regel für eine bestimmte Domäne erstellen, wird die neue Regel nur für diese Domäne verwendet und ist in keiner anderen Domäne vorhanden. Wenn Sie eine vorhandene Regel in der globalen Domäne anpassen und einer bestimmten Domäne zuweisen, erstellen Sie eine Kopie der globalen Regel, die weiterhin in allen anderen Domänen verwendet wird, mit Ausnahme der Domäne mit der angepassten Version dieser Regel. Wenn Sie eine Regel in der globalen Domäne anpassen, wirkt sich die Änderung auf alle Domänen aus, mit Ausnahme derjenigen, in der eine angepasste Kopie dieser Regel verwendet wird.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verkehrsbasierte Discovery**an.
2. Klicken Sie auf **Neu**.
3. Definieren Sie die Regelparameter wie folgt:

Feld	Beschreibung
Aktion	Wählen Sie **Aktivieren** aus, um dem spezifischen CI oder CI-Typ datenverkehrsbasierte Verbindungen hinzuzufügen.
Regelumfang	Wählen Sie **Spezifischer CI**, aus um Datenverkehr für ein Konfigurationselement zu erkennen, bzw. **CI-Typ**, um Datenverkehr für alle Konfigurationselemente in einer der CI-basierten Tabellen zu erkennen.
CI/CI-Typ	Wählen Sie ein bestimmtes CI aus, oder wählen Sie die Tabelle mit den CIs aus, für die Sie Datenverkehr erkennen möchten.
Domäne	Wählen Sie die Domäne aus, zu der die Regel gehört.

4. Klicken Sie auf **Absenden**.
5. Definieren Sie zur Feinabstimmung der datenverkehrsbasierten Erkennung wie folgt erweiterte Parameter:

Parameter	Beschreibung
sa.traffic_based_discovery.conn_aging_time	Zeitraum in Stunden, für den eine datenverkehrsbasierte Verbindung seit der letzten Erkennung aktiv bleibt ○ **Typ**: Ganzzahl ○ **Standardwert**: 72 ○ **Andere mögliche Werte**: beliebige Zahl über 24 ○ **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
sa.traffic_based_discovery.ignored_ports	Bei einer datenverkehrsbasierten Erkennung gefundene Ports, die ignoriert werden können. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Ändern Sie diese Eigenschaft, um Ports zu definieren, die Service-Mapping bei der datenverkehrsbasierten Erkennung ignoriert. Dadurch wird die Erkennung effizienter, da keine Ressourcen für die Erkennung irrelevanter Verbindungen verschwendet werden. ○ **Typ**: Zeichenfolge ○ **Standardwert**: 445, 139, 111, 2049, 860, 3260, 135, 53 ○ **Andere mögliche Werte**: alle relevanten Portnummern ○ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.traffic_based_discovery.max_connections	Maximale Anzahl datenverkehrsbasierter Verbindungen von einem einzelnen CI. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Diese Eigenschaft trägt dazu bei, die Größe der Zuordnung angemessen zu halten, indem die Anzahl der möglichen CI-Verbindungen begrenzt wird. ○ **Typ**: Ganzzahl ○ **Standardwert**: 30 ○ **Andere mögliche Werte**: beliebige Zahl über 1 ○ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Tag-basierte Discovery-Konfiguration

Sie können die Standardkonfiguration verfeinern, um zu steuern, welche CIs verwendet werden Service-Mapping Schließt während des Tag-basierten Discovery-Prozesses in Anwendungsservices ein.

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping Stellt vorkonfigurierte CI-Beziehungen bereit, die an der Tag-basierten Discovery teilnehmen können. Sie haben die Möglichkeit, diese CI-Beziehungen anzupassen und die Standardkonfiguration mit einer der folgenden Methoden zu verfeinern:

- CIs basierend auf Klassen in die Tag-basierte Discovery einbeziehen;
- CIs basierend auf ihrem Installationsstatus ausschließen;
- Vorkonfigurierte CI-Beziehungen ausschließen;
- Fügen Sie CI-Beziehungen hinzu, oder bearbeiten Sie sie.

Dient zum Anzeigen vorkonfigurierter CI-Beziehungen, welche Service-Mapping Schließt während der Tag-basierten Discovery in Anwendungsservices ein, siehe Vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery .

Zum Anzeigen von mit installierten Eigenschaften Service-Mapping Die sich auf die Tag-basierte Discovery beziehen, finden Sie unter Eigenschaften im Zusammenhang mit der Tag-basierten Discovery .

Schließen Sie CIs basierend auf Klassen in die Tag-basierte Discovery ein

Verwenden Sie CI-Klassen, um zu identifizieren, welche CIs Service-Mapping Schließt während der Tag-basierten Discovery in Anwendungsservices ein. Standardmäßig wird diese Liste leer angezeigt und enthält alle CIs, die zu allen CI-Klassen gehören. Definieren Sie CI-Klassen, und erlauben Sie nur CIs, die zu diesen Klassen oder ihren Erweiterungen gehören, an der Tag-basierten Discovery teilzunehmen.

Vorbereitungen

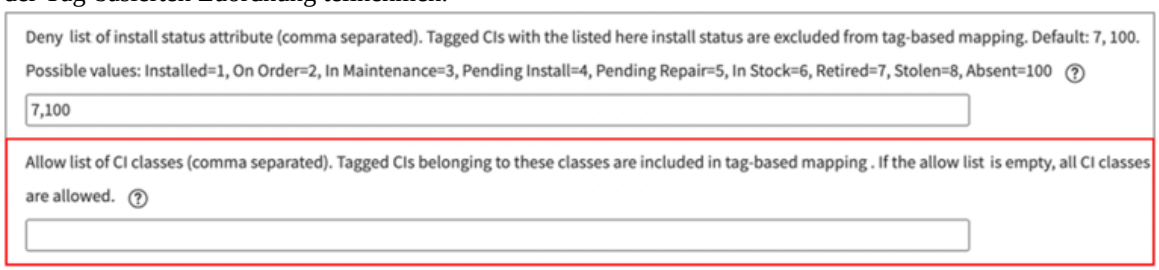
Erfahren Sie mehr über die Standardfunktionskonfiguration in Tag-basierte Discovery in Service-Mapping .

> **Hinweis:** Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**an.
2. Geben Sie durch Kommas getrennte CI-Klassen in der Allow-Liste ein, die steuert, welche getaggten CIs an der Tag-basierten Zuordnung teilnehmen.



3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie weitere Informationen unter Berechnen Sie zuvor erstellte Anwendungsservices neu Für die nächsten Schritte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließen Sie CIs basierend auf ihrem Installationsstatus in der Tag-basierten Discovery aus

Verwenden Sie den CI-Installationsstatus, um CI-Klassen zu erstellen und CIs während der Tag-basierten Discovery aus Anwendungsservices auszuschließen. Standardmäßig schließen Anwendungsservices basierend auf Tags CIs mit dem Status „stillgelegt“ oder „Abwesend“ aus. Sie können diese Liste der ausgeschlossenen CIs erweitern, um zusätzliche Installationsstatus wie „Installation ausstehend“ oder „gestohlen“ einzubeziehen.

Vorbereitungen

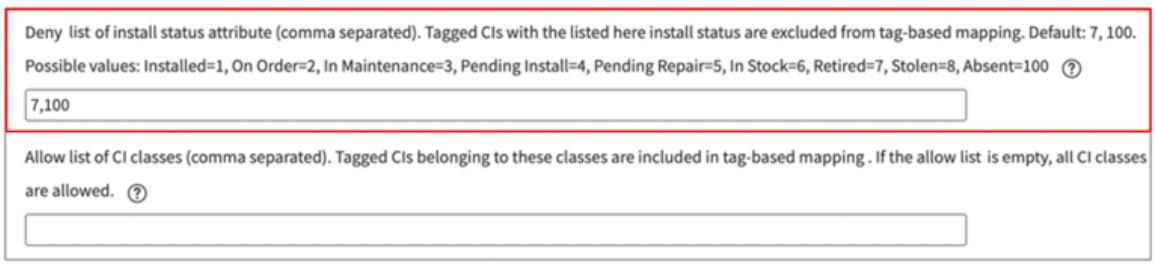
Erfahren Sie mehr über die Standardfunktionskonfiguration in Tag-basierte Discovery in Service-Mapping .

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**an.
2. Geben Sie Werte für Installationsstatus in die Deny-Liste ein, die steuert, welche CIs basierend auf dem Installationsstatus von der Tag-basierten Zuordnung ausgeschlossen werden sollen.
   Trennen Sie die Werte durch Kommas.



3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie weitere Informationen unter Berechnen Sie zuvor erstellte Anwendungsservices neu Für die nächsten Schritte.

Schließen Sie vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery aus

Schließen Sie vorkonfigurierte CI-Beziehungen aus dem Tag-basierten Discovery-Prozess aus, um die erstellten Anwendungsservices zu verfeinern. Service-Mapping Besteht aus vorkonfigurierten CI-Beziehungen und schließt CIs in diese Beziehungen ein, auch wenn ihnen keine Tags zugewiesen sind. Wählen Sie aus, welche vorkonfigurierten CI-Beziehungen ausgeschlossen werden sollen und welche verbleibenden CI-Beziehungen an der Tag-basierten Discovery teilnehmen.

Vorbereitungen

Erfahren Sie mehr über die Standardfunktionskonfiguration in Tag-basierte Discovery in Service-Mapping .

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Service_Mapping_admin

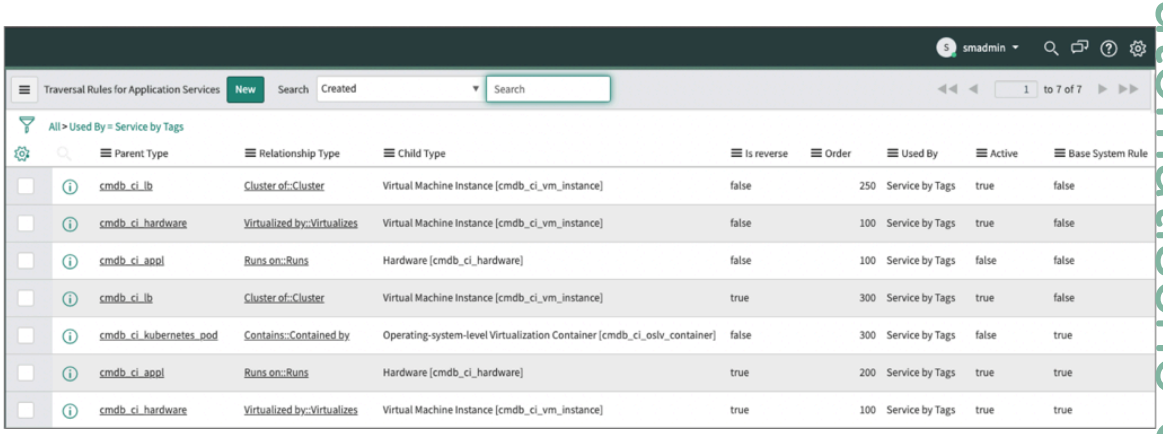
Warum und wann dieser Vorgang ausgeführt wird

In der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_Traversal_rules] werden die CI-Beziehungen gespeichert, die an der Tag-basierten Discovery teilnehmen. Standardmäßig haben vorkonfigurierte CI-Beziehungen, die in der Tag-basierten Discovery verwendet werden, die **Wahr** Wert in **Basissystemregel** Spalte. Verwenden Sie diese Informationen, um vorkonfigurierte CI-Beziehungen von der Tag-basierten Discovery auszuschließen.

Wichtig: Sie können vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, nicht aus der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_Traversal_rules] löschen oder ändern.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Service-Traversal-Regeln**an.



Parent Type	Relationship Type	Child Type	Is reverse	Order	Used By	Active	Base System Rule
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	false	250	Service by Tags	true	false
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	false	100	Service by Tags	true	false
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	false	100	Service by Tags	false	false
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	true	300	Service by Tags	true	false
cmdb_ci_kubernetes_pod	Contains::Contained by	Operating-system-level Virtualization Container [cmdb_ci_oslv_container]	false	300	Service by Tags	false	true
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	true	200	Service by Tags	true	true
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	true	100	Service by Tags	true	true

2. Klicken Sie auf die vorkonfigurierte CI-Beziehung, die Sie von der Tag-basierten Discovery ausschließen möchten.

   Informationen zum Anzeigen dieser CI-Beziehungen finden Sie unter Vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery

3. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
4. Klicken Sie Auf **Übermitteln** In **Durchlaufregeln für Anwendungsservices** Formular.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie weitere Informationen unter Berechnen Sie zuvor erstellte Anwendungsservices neu Für die nächsten Schritte.

Fügen Sie CI-Beziehungen in der Tag-basierten Discovery hinzu, oder bearbeiten Sie sie

Aktivieren Sie vorkonfigurierte CI-Beziehungen, die Service-Mapping Schließt standardmäßig keine zusätzlichen Beziehungen zur Verwendung in den Tag-basierten Discovery-Prozess ein oder fügt sie hinzu. Sie können beispielsweise eine CI-Beziehung zwischen Linux-Servern und Speichergeräten hinzufügen, um Server zu erkennen, die Speichergeräte basierend auf Tags hosten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erfahren Sie mehr über die Standardfunktionskonfiguration in Tag-basierte Discovery in Service-Mapping .

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

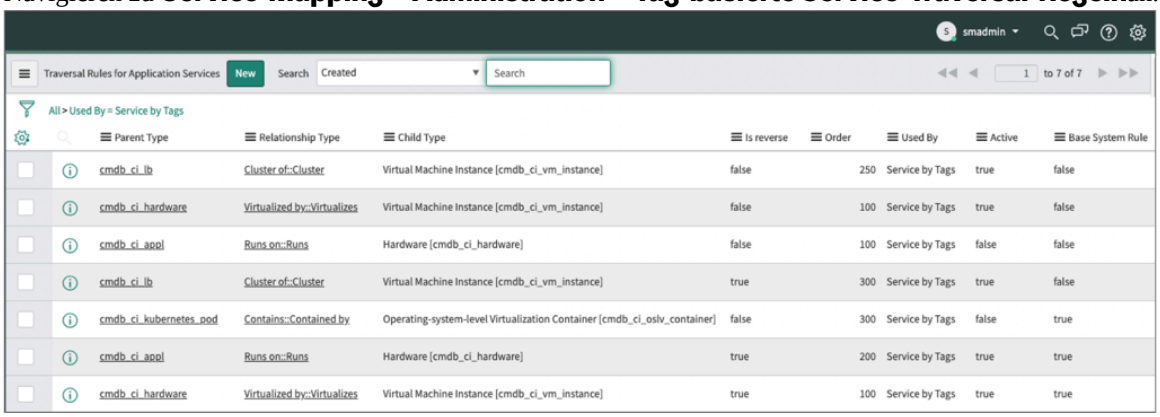
Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „Anwendungsservices“ [svc_traversal_rules] wird gefiltert, um nur CI-Beziehungen anzuzeigen, die für die Tag-basierte Erkennung verwendet werden. Standardmäßig haben vorkonfigurierte CI-Beziehungen, die in der Tag-basierten Discovery verwendet werden, die **Wahr** Wert in **Basissystemregel** Spalte. Verwenden Sie diese Informationen, um neue CI-Beziehungen zu erstellen oder vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery zu bearbeiten.

Wichtig: Sie können vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, nicht aus der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_Traversal_rules] löschen oder ändern.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Service-Traversal-Regeln**an.



2. Klicken Sie auf die vorhandene CI-Beziehung, die Sie ändern möchten, oder klicken Sie auf **Neu** Dient zur Verwendung einer zusätzlichen CI-Beziehung im Tag-basierten Discovery-Prozess.

   Informationen zum Anzeigen von Standard-CI-Beziehungen finden Sie unter Vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery .

3. Schließen Sie ab **Durchlaufregeln für Anwendungsservices** Formular.
   Informationen zum Ausfüllen dieses Formulars finden Sie unter Durchlaufregeln für Formularabschluss für Anwendungsservices .

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie weitere Informationen unter Berechnen Sie zuvor erstellte Anwendungsservices neu Für die nächsten Schritte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechnen Sie zuvor erstellte Anwendungsservices neu

Berechnen Sie Anwendungsservices neu, nachdem Sie die Standardkonfiguration verfeinert haben, um zu steuern, welche CIs in den Tag-basierten Discovery-Prozess einbezogen werden sollen.

Vorbereitungen

Führen Sie die Schritte aus, um die Standardkonfiguration für den Tag-basierten Discovery-Prozess zu verfeinern. Weitere Informationen finden Sie unter Tag-basierte Discovery-Konfiguration .

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**an.
2. Klicken Sie auf den entsprechenden Anwendungsservice.
3. Klicken Sie unter **Zugehörige Links** auf **Service neu berechnen**.
4. Wiederholen Sie diese Schritte für alle relevanten Tag-basierten Services.

Nachverfolgung von Changes für die Change-Historie feintunen

Definieren Sie CI-Felder, deren Changes in der Change-Historie für Anwendungsservices berücksichtigt werden. In der Ansicht der Change-Historie werden Changes angezeigt, die an CIs vorgenommen wurden, aus denen Anwendungsservices bestehen, sowie Changes, die an den eigentlichen Anwendungsservices vorgenommen wurden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Details zu Änderungen an einer Serviceinstanz und ihren CIs werden in der CMDB gespeichert. Normalerweise spiegeln diese Änderungen das Hinzufügen oder Entfernen von CIs aus einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien wider. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Ausschlussliste**an.
   In der daraufhin geöffneten Liste „Ausschlusslisten“ werden Datensätze angezeigt, die vom System dazu verwendet werden, Changes aus der Ansicht der Change-Historie auszuschließen.
2. Um Changes an einem weiteren Feld zu ignorieren, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Neu**.

b. Geben Sie den CI-Klassennamen in das Feld **Tabellenname** ein.
Geben Sie beispielsweise `cmdb_ci` für die Klasse „Konfigurationselement“ [cmdb_ci] ein.

> **Hinweis:** Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

c. Geben Sie in das Feld **Feldname** den Namen des Felds ein, das Sie ausschließen möchten.
Geben Sie beispielsweise `work_notes` ein, um Changes, die an den Arbeitsnotizen für Elemente vorgenommen werden, aus der Ansicht der Change-Historie auszuschließen.

d. Wählen Sie **Absenden** aus.

3. Um zuvor ignorierte Changes wieder in die Change-Historie aufzunehmen, gehen Sie wie folgt vor:

a. Aktivieren Sie die Kontrollkästchen neben den relevanten Datensätzen.

b. Wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option **Löschen** aus.

Zugehörige Informationen

Change-Historie von Anwendungsservices in veraltet Mitarbeiterbereich anzeigen

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

Datenerfassung und -erkennung mit Netflow

Service-Mapping kann eine Erkennung basierend auf Daten durchführen, die mit dem Protokoll Netflow erfasst wurden. Netflow ist ein Protokoll das Service-Mapping zum Erfassen von Daten über CIs und ihren Verbindungen mit Netstat- und Isof-Befehlen nutzen kann.

Die Verwendung des Netflow-Protokolls zum Erfassen von Daten ist eine der Methoden der datenverkehrsbasierten Erkennung. Andere von Service-Mapping bereitgestellte Methoden verwenden die Befehle netstat und lsof und die VPC-Flow-Protokolle. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden *`netstat`*, *`ss`*, Und *`lsof`*Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren.

Die Komponente, die Daten im Netflow-Format empfängt, ist der Netflow Collector. Sein Speicherort hängt davon ab, ob Sie die Datenerfassung für Testzwecke oder für den Standardbetrieb konfigurieren:

Zu Testzwecken

Dieses Setup führt zu einem halbautomatisierten Datenerfassungs-Flow, wobei Service-Mapping Daten nur importiert, wenn Sie sie manuell aus dem Netflow Collector kopieren. Sie platzieren den Netflow Collector auf einem Server innerhalb Ihres Unternehmensnetzwerks. Dies muss ein anderer Server sein als der Server, auf dem der MID-Server gehostet wird . Sie konfigurieren und testen dieses Setup wie in Einmaligen Datenimport mit Netflow zu Testzwecken konfigurieren beschrieben.

Für den Standardbetrieb

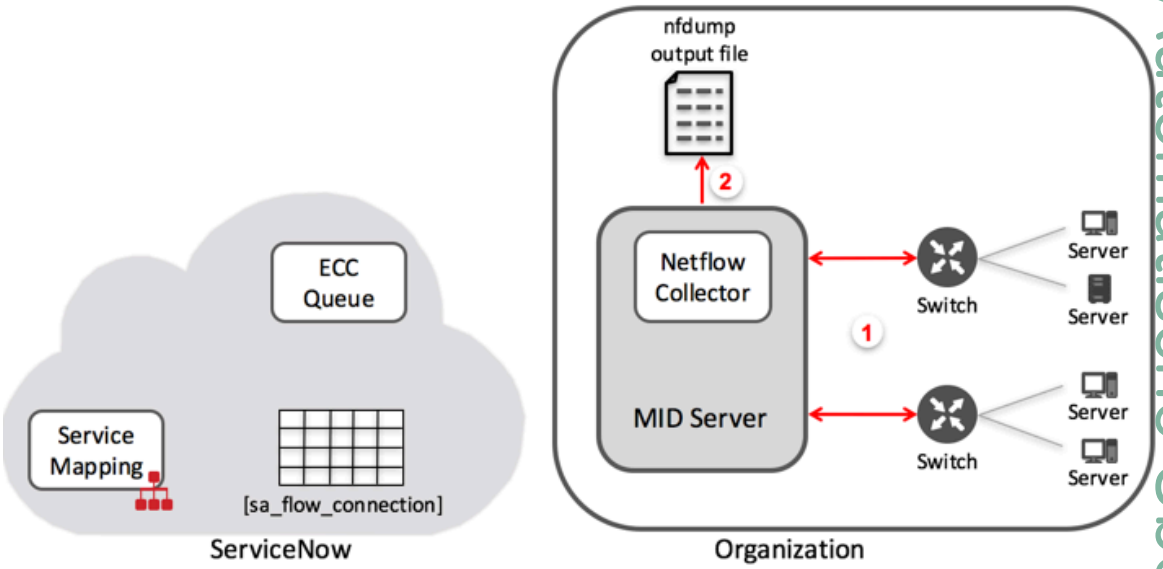
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Setup führt zu einem vollständig automatisierten Datenerfassungs-Flow, bei dem alle beteiligten Komponenten Daten automatisch senden, sammeln und analysieren. Sie platzieren den Netflow Collector auf demselben Server wie den MID-Server innerhalb Ihres Unternehmensnetzwerks. Anweisungen dazu finden Sie unter Datenerfassung mit Netflow konfigurieren.

Die Netflow-basierte Erkennung folgt dem folgenden Flow:

1. Der Netflow-Daemon wird ausgeführt und empfängt Daten von Switches, die mit Servern in der Organisation kommunizieren. Der Netflow Collector schreibt die vom Netflow-Daemon empfangenen Daten.
2. Der Server, der den Netflow Collector hostet, verwendet das Netflow-Dienstprogramm nfdump, um die Daten in die nfdump-Ausgabedatei zu schreiben. Diese Datei fasst die Rohdaten aller für die Serverkommunikation verwendeten Switches zusammen.

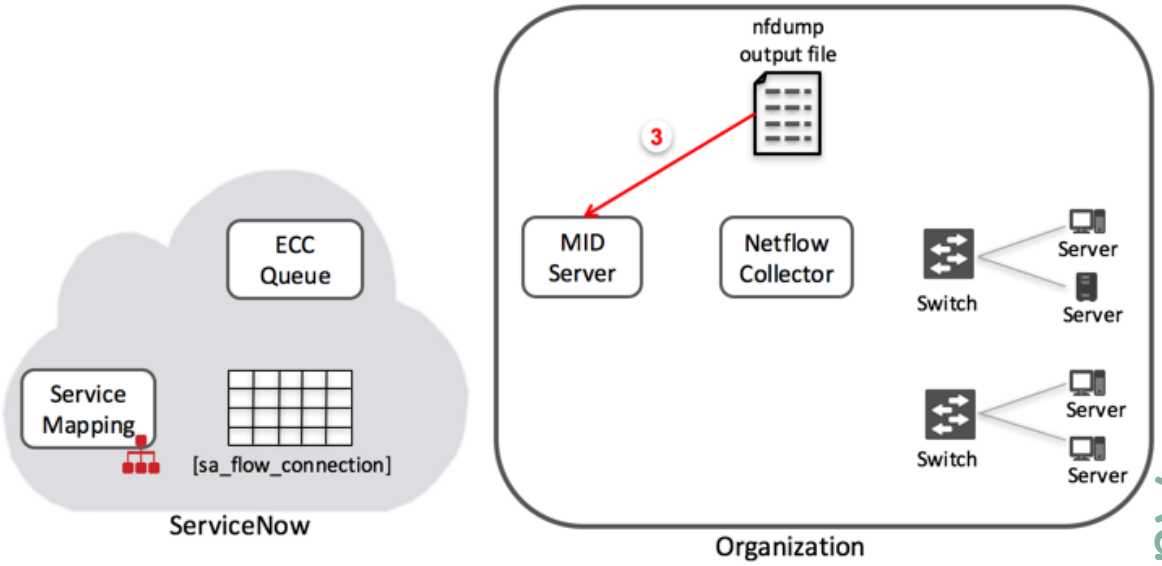
Daten erfassen und in die nfdump-Ausgabedatei schreiben



3. In Test-Setups, in denen sich der Netflow Collector nicht auf demselben Server wie der MID-Server befindet, müssen Sie nfdump möglicherweise in das gzip-Format konvertieren. Anschließend müssen Sie die Rohdaten aus der nfdump-Ausgabedatei manuell auf den MID-Server kopieren.

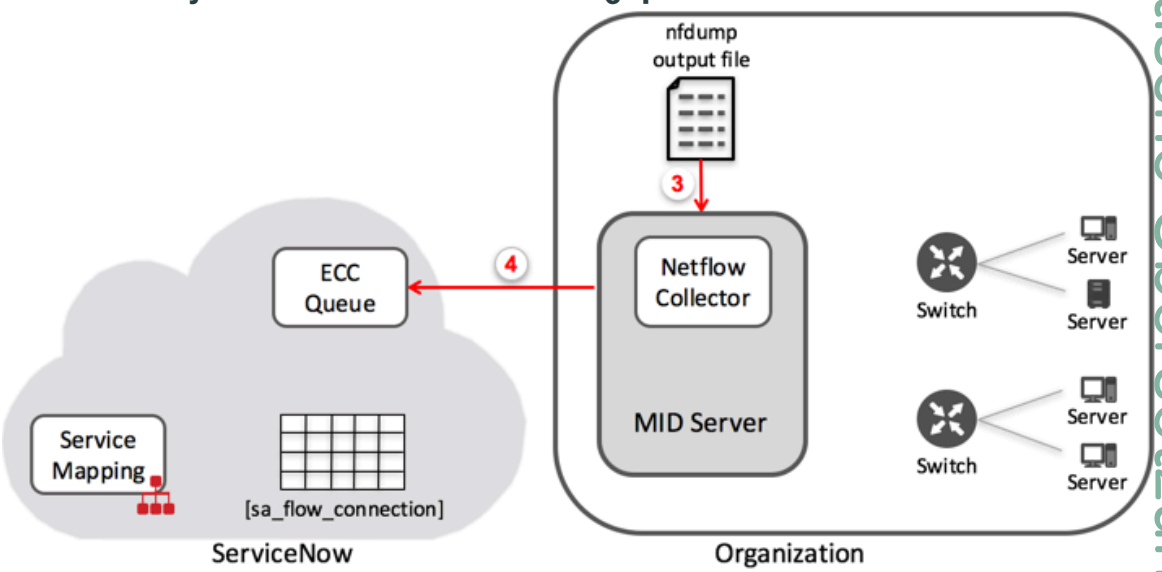
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nfdump-Ausgabedatei auf MID-Server kopieren



4. Der MID-Server verarbeitet die Rohdaten in der nfdump-Ausgabedatei und platziert die verarbeiteten Informationen in der ECC-Warteschlange.

Rohdaten analysieren und in ECC-Warteschlange platzieren



5. Ein Sensor ruft die Prozessdaten aus der ECC-Warteschlange ab und schreibt sie in die Flow-Verbindungstabelle [sa_flow_connection].

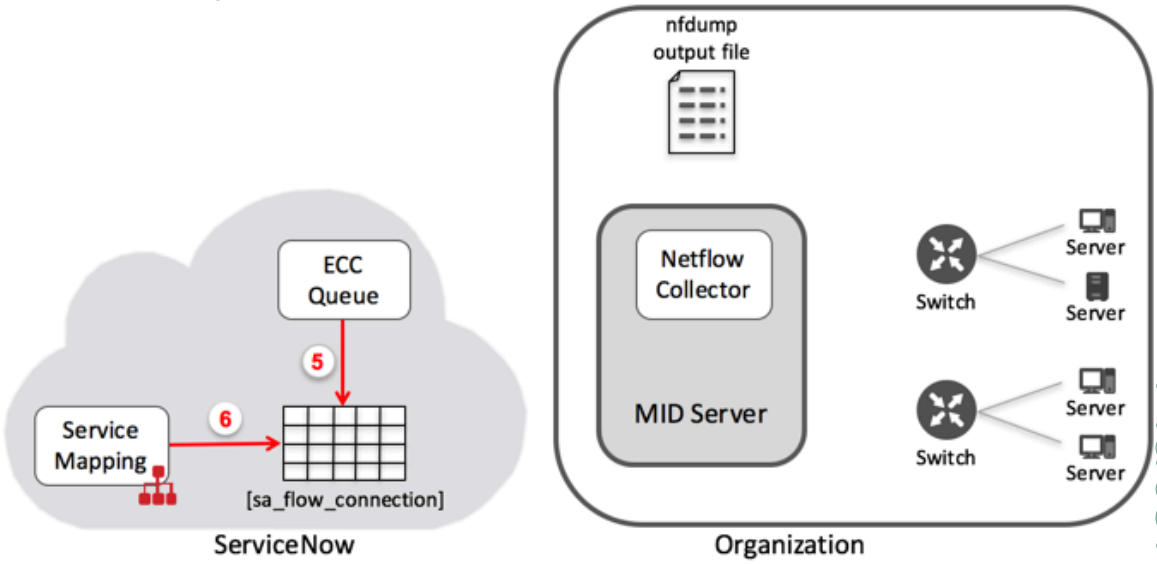
6. Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

Service-Mapping ruft Daten aus der Tabelle sa_flow_connection ab



Zugehörige Informationen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0597467

Einmaligen Datenimport mit Netflow zu Testzwecken konfigurieren

Konfigurieren und testen Sie den Erkennungsprozess in Service-Mapping basierend auf Daten, die mit dem Protokoll Netflow erfasst wurden.

Vorbereitungen

Informieren Sie sich über die Datenverkehrsbasierte Erkennung in Service-Mapping.

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden `netstat`, `ss`, Und `lsof`Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren. Weitere Informationen darüber, wie Sie in Service-Mapping Netflow-Daten erfassen, finden Sie unter Datenerfassung und -erkennung mit Netflow.

Installieren Sie den Netflow Collector (nfdump) zu Testzwecken auf einem Unix-Server in Ihrer Organisation. In diesem Fall darf es sich nicht um denselben Server handeln, auf dem der MID-Server gehostet wird.

Konfigurieren Sie den ServiceNow-Connector so, dass er MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie den Netflow Collector (nfdump) auf einen Unix-Server in Ihrer Organisation herunter, und installieren Sie ihn.
   - Laden Sie das nfdump-Paket für einen Linux-Server herunter, kompilieren Sie es und installieren Sie es. Sie können das nfdump-Paket von https://sourceforge.net/projects/nfdump/ herunterladen.
   - Installieren Sie für einen Ubuntu-Server das nfdump-Paket, ohne es vorher herunterzuladen oder zu kompilieren. Öffnen Sie das Befehlszeilenfenster und führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install nfdump
     ```

   - Wenn bei einem Ubuntu-Server der *apt-get*-Befehl fehlschlägt, laden Sie das nfdump-Paket herunter, speichern Sie es lokal, und installieren Sie es. Öffnen Sie das Befehlszeilenfenster und führen Sie die folgenden Befehle aus:

     ```
     sudo dpkg -i nfdump_1.6.15-3_i386.deb -
     ```

     ```
     sudo apt-get -f install
     ```

     Hinweis: Der Dateiname für das Paket nfdump hat das folgende Format: nfdump_<version number> .deb. In diesem Beispiel ist dies nfdump_1.6.15-3_i386.deb.

2. Konfigurieren Sie den Netflow-Collector, um Daten für einen Tag zu speichern.
   a. Öffnen Sie das Befehlszeilenfenster auf dem Server, auf dem sich der Netflow-Collector befindet.
   b. Erstellen Sie einen Cron-Job.
   `crontab -e`
   c. Geben Sie den folgenden Befehl mit den richtigen Pfaden ein.
   `*/10 * * * * /usr/local/bin/nfexpire -e /data/nfdump -t 1d`
3. Erstellen Sie eine Datei mit den nfdump-Daten.
   Verwenden Sie beispielsweise den folgenden Befehl:

   ```
   nfdump -q -m -R /data/nfdump/ -o extended -t 2016/07/06.07:00:00-2016/07/06.07:10:00 'inet and proto tcp' >> /tmp/my_file
   ```

4. Wenn die Datei sehr groß ist, können Sie sie im gzip-Format komprimieren, indem Sie den folgenden Befehl verwenden:
   `gzip /tmp/my_file`
5. Kopieren Sie die nfdump-Datendatei auf den MID-Server.
6. Konfigurieren Sie Service-Mapping zum Empfangen von vom Netflow Collector erfassten Daten:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**an.
   b. Klicken Sie auf **Neu**.
   c. Klicken Sie auf die **ndfdump-Datei**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Konfigurieren Sie die Parameter auf der Seite für die ndfdump-Datei wie folgt:

Feld	Beschreibung
Name	Beschreibender Name für den Connector
nfdump-Datenpfad	Pfad zu einem Speicherort auf dem MID-Server, in dem Sie die nfdump-Datendatei in 5 gespeichert haben
MID Server	MID-Server, auf den Sie die nfdump-Datei kopiert haben
Gzip-Datei	Wenn Sie die nfdump-Datei in das gzip-Format konvertiert haben, bevor Sie sie auf dem MID-Server gespeichert haben, setzen Sie diesen Parameter auf „true“, um die Datei zu dekomprimieren.

e. Klicken Sie auf **Absenden**.

7. Stellen Sie sicher, dass Service-Mapping Daten mit Netflow erfasst:

a. Wählen Sie im Formular für die **nfdump-Datei** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.

b. Navigieren zu **Systemdefinitionen** > **Tabellen**an.

c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]

d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.

e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Nächste Maßnahme

Wenn Sie mit den Testergebnissen zufrieden sind, konfigurieren Sie die Netflow-basierte Datenerfassung (siehe Beschreibung in Datenerfassung mit Netflow konfigurieren).

Datenerfassung mit Netflow konfigurieren

Richten Sie in Service-Mapping die Erkennung basierend auf Daten ein, die mit dem Protokoll Netflow erfasst wurden. Dieses Setup führt zu einem vollständig automatisierten Datenerfassungs-Flow, bei dem alle beteiligten Komponenten Daten automatisch senden, sammeln und analysieren.

Vorbereitungen

Informieren Sie sich über die Datenverkehrsbasierte Erkennung in Service-Mapping.

Aktivieren Sie den folgenden regelmäßigen Auftrag: Flow Discovery-Planer [sysauto_script_74c676f0dbb0220060ff742eaf9619f2]+

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden `netstat`, `ss`, Und `lsof`Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren. Weitere Informationen über die Nutzung von Netflow durch Service-Mapping finden Sie unter Datenerfassung und -erkennung mit Netflow.

Konfigurieren Sie den ServiceNow Netflow-Connector so, dass er den MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.

Prozedur

1. Installieren Sie das nfdump-Paket auf einem Server, der in Ihrer Organisation den MID-Server hostet:
   - Laden Sie das nfdump-Paket für einen Linux-Server herunter, kompilieren Sie es und installieren Sie es. Sie können das nfdump-Paket von https://sourceforge.net/projects/nfdump/ herunterladen.
   - Installieren Sie für einen Ubuntu-Server das nfdump-Paket, ohne es vorher herunterzuladen oder zu kompilieren. Öffnen Sie das Befehlszeilenfenster und führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install nfdump
     ```

   - Wenn bei einem Ubuntu-Server der *apt-get*-Befehl fehlschlägt, laden Sie das nfdump-Paket herunter, speichern Sie es lokal, und installieren Sie es. Öffnen Sie das Befehlszeilenfenster und führen Sie die folgenden Befehle aus:

     ```
     sudo dpkg -i nfdump_1.6.15-3_i386.deb -

     sudo apt-get -f install
     ```

     Hinweis: Der Dateiname für das Paket nfdump hat das folgende Format: nfdump_<version number> .deb. In diesem Beispiel ist dies nfdump_1.6.15-3_i386.deb.

2. Konfigurieren Sie den Netflow-Collector so, dass die nfdump-Datei im erforderlichen Verzeichnis gespeichert wird.

   a. Öffnen Sie die Datei `/etc/init.d/nfdump`.

   b. Ändern Sie den Parameter, der für das Speichern dieser Datei am erforderlichen Speicherort verantwortlich ist.
   Geben Sie beispielsweise auf einem Ubuntu-Server den Speicherort mit dem Parameter *DEAMON_ARGS* an:

   ```
   DATA_BASE_DIR="/var/cache/nfdump"

   DAEMON_ARGS="-D -l $DATA_BASE_DIR -P $PIDFILE"
   ```

   Betriebsinformationen finden Sie unter https://sourceforge.net/projects/nfdump/ .

3. Konfigurieren Sie die Switches so, dass ihre nfdump-Dateien an MID-Server weitergeleitet werden. Der Standardwert für MID-Server ist Port 9995.
4. Konfigurieren Sie den Netflow-Collector, um Daten für einen Tag zu speichern.

   a. Öffnen Sie das Befehlszeilenfenster auf dem Server, auf dem sich der Netflow-Collector befindet.

   b. Erstellen Sie einen Cron-Job.
   `crontab -e`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

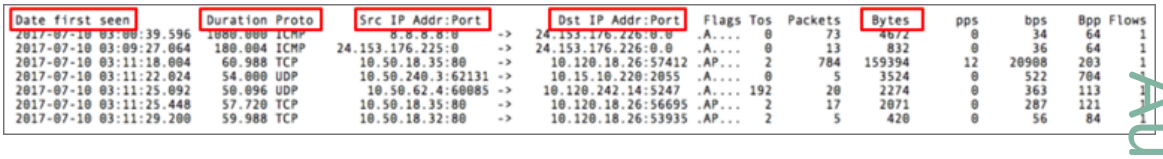
c. Geben Sie den folgenden Befehl mit den richtigen Pfaden ein.
`*/10 * * * * /usr/local/bin/nfexpire -e /data/nfdump -t 1d`

5. Stellen Sie sicher, dass der Netflow Collector ordnungsgemäß konfiguriert ist und von den Netzwerkressourcen die richtigen Daten erhält.

a. Führen Sie den folgenden Befehl aus:

```
nfdump -q -O tstart -R /data/nfdump/ -o extended
```

b. Überprüfen Sie in der Befehlsausgabe, ob die markierten Felder reale Daten enthalten:



Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2017-07-10 03:00:39.596	1080.000	ICMP	8.8.8.8:0	->	24.153.176.226:0.0	.A....	0	73	4672	0	34	64	1
2017-07-10 03:09:27.064	180.004	ICMP	24.153.176.225:0	->	24.153.176.226:0.0	.A....	0	13	832	0	36	64	1
2017-07-10 03:11:18.004	60.988	TCP	10.50.18.35:80	->	10.120.18.26:57412	.AP...	2	784	159394	12	20908	203	1
2017-07-10 03:11:22.024	54.000	UDP	10.50.240.3:62131	->	10.15.10.220:2055	.A....	0	5	3524	0	522	704	1
2017-07-10 03:11:25.092	50.096	UDP	10.50.62.4:60085	->	10.120.242.14:5247	.A....	192	20	2274	0	363	113	1
2017-07-10 03:11:25.448	57.720	TCP	10.50.18.35:80	->	10.120.18.26:56695	.AP...	2	17	2071	0	287	121	1
2017-07-10 03:11:29.200	59.988	TCP	10.50.18.32:80	->	10.120.18.26:53935	.AP...	2	5	420	0	56	84	1

6. Konfigurieren Sie Service-Mapping zum Empfangen von vom Netflow Collector erfassten Daten:

a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**an.

b. Klicken Sie auf **Neu**.

c. Klicken Sie auf **nfdump-Installation**

d. Konfigurieren Sie die Parameter auf der Seite „ndfdump-Installation“ wie folgt:

Feld	Beschreibung
Name	Beschreibender Name für den Connector
MID Server	MID-Server, auf dem der Netflow Collector installiert ist
nfdump-Datenverzeichnis	Datenverzeichnis, in dem in Ihrer Konfiguration der Netflow Collector die nfdump-Datei speichern soll

e. Klicken Sie auf **Absenden**.

7. Stellen Sie sicher, dass Service-Mapping Daten mit Netflow erfasst:

a. Wählen Sie im Formular **nfdump-Installation** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.

b. Navigieren zu **Systemdefinitionen** > **Tabellen**an.

c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]

d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.

e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerfassung und -erkennung mit VPC-Flow-Protokollen

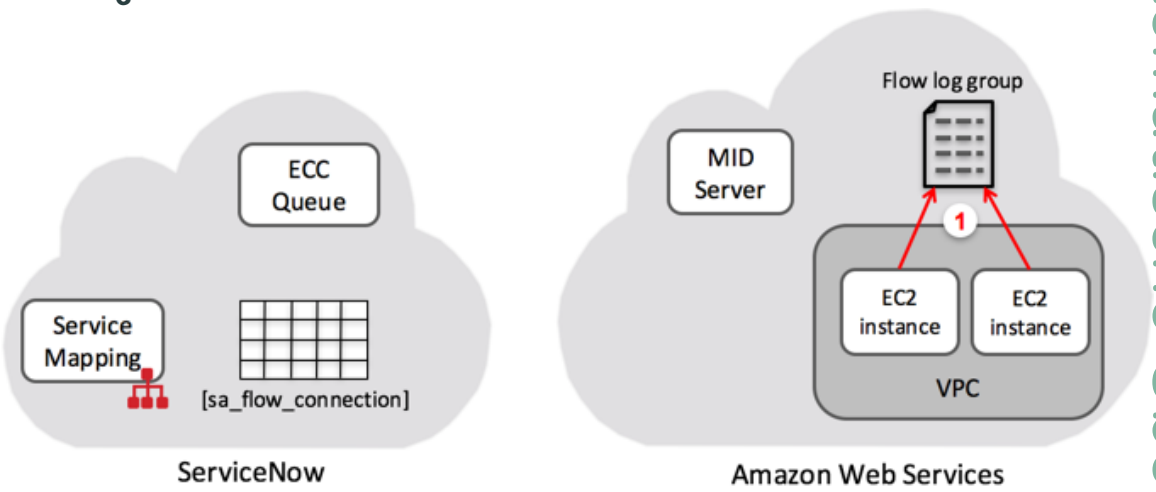
Service-Mapping kann eine Erkennung basierend auf Daten durchführen, die mit VPC-Flow-Protokollen erfasst wurden. Amazon VPC hostet Amazon EC2-Instanzen (Elastic Compute Cloud), die Amazon Web Services bereitstellen. VPC-Flow-Protokolle erfassen Daten über den IP-Datenverkehr, der von und zu Netzwerkschnittstellen in der VPC geleitet wird.

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden `netstat`, `ss`, Und `lsof`Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung von VPC-Flow-Protokollen konfigurieren.

Die Service-Mapping-Erkennung auf Basis von VPC-Flow-Protokollen folgt dem folgenden Flow:

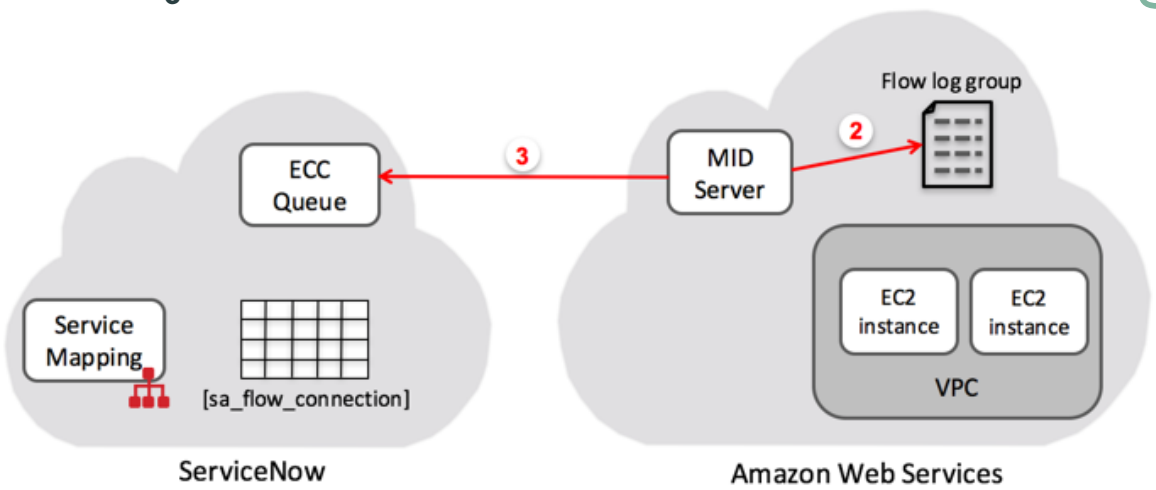
1. Amazon EC2-Instanzen erfassen ihre einzelnen Protokolle in Protokoll-Streams und leiten sie an die zentrale Flow-Protokollgruppe weiter.

Erfassung individueller Protokolle durch Amazon EC2-Instanzen



2. Der ServiceNow-Connector veranlasst den MID-Server, veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.
3. Der MID-Server stellt die verarbeiteten Informationen in die ECC-Warteschlange.

MID-Server erfasst Daten aus dem Flow-Protokoll und platziert sie in die ECC-Warteschlange

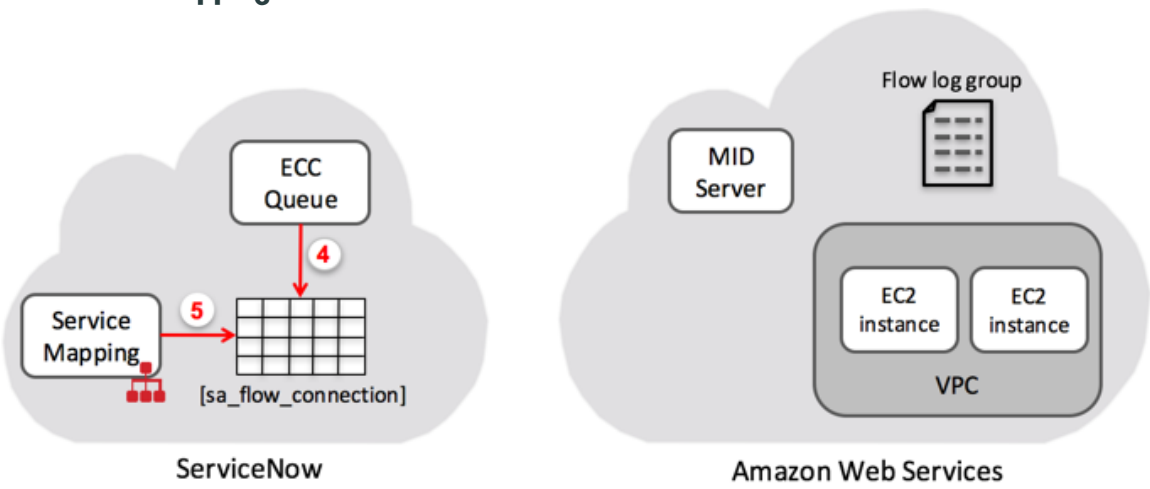


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Ein Sensor ruft die Prozessdaten aus der ECC-Warteschlange ab und schreibt sie in die Flow-Verbindungstabelle [sa_flow_connection].

5. Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von den Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

Gesammelte Daten werden in die Tabelle sa_flow_connection geschrieben, aus der Service-Mapping die Daten erfasst



Konfigurieren Sie in Bereitstellungen mit mehreren Flow-Protokollgruppen einen dedizierten Connector, der mit einem MID-Server pro Flow-Protokollgruppe arbeitet. Mehrere Flow-Protokollgruppen können dieselben AWS-Anmeldeinformationen verwenden.

Zugehörige Informationen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0597467

Datenverkehrsbasierte Erkennung in Service-Mapping

Datenerfassung mit VPC-Flow-Protokollen konfigurieren

Aktivieren Sie Service-Mapping, um eine Erkennung basierend auf Daten durchzuführen, die mithilfe von VPC-Protokollen (Virtual Private Cloud) erfasst wurden. Diese Methode ist für Organisationen relevant, die Amazon Web Services (AWS) verwenden.

Vorbereitungen

Überprüfen Sie, ob Anmeldeinformationen für den AWS-Account im Anmeldeinformationsmodul der Plattform konfiguriert sind, indem Sie zu navigieren **Service-Mapping** > **Anmeldeinformationen** > **AWS-Anmeldeinformationen**an. Weitere Informationen zu AWS-Anmeldeinformationen finden Sie unter Cloud-Anmeldeinformationen .

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen, bei denen es sich um die Standard- oder Standardkonfigurationen handelt, basiert die Traffic-basierte Discovery ausschließlich auf TCP-bezogenen Daten, die mit erfasst werden `netstat`, `ss`, Und `lsof`Befehle. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung von VPC-Flow-Protokollen konfigurieren. Weitere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erkennungs-Flow in Service-Mapping auf Basis von VPC-Flow-Protokollen finden Sie unter Datenerfassung und -erkennung mit VPC-Flow-Protokollen.

Amazon VPC hostet Amazon EC2-Instanzen (Elastic Compute Cloud), die Amazon Web Services bereitstellen. VPC-Flow-Protokolle erfassen Daten über den IP-Datenverkehr, der von und zu Netzwerkschnittstellen in der VPC geleitet wird.

Konfigurieren Sie den ServiceNow-Connector so, dass er MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten. Konfigurieren Sie in Bereitstellungen mit mehreren Flow-Protokollgruppen einen dedizierten Connector, der mit einem MID-Server pro Flow-Protokollgruppe arbeitet. Mehrere Flow-Protokollgruppen können dieselben AWS-Anmeldeinformationen verwenden.

Prozedur

1. Konfigurieren Sie VPC-Flow-Protokolle in der Amazon EC2-Konsole gemäß der Beschreibung in der offiziellen AWS-Dokumentation.
2. Konfigurieren Sie Service-Mapping für die Verwendung mit VPC-Flow-Protokollen:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**an.
   b. Klicken Sie auf **Neu**.
   c. Klicken Sie auf **AWS VPC-Flow-Protokolle**.
   d. Konfigurieren Sie auf der Seite „AWS VPC-Flow-Protokolle“ die Connector-Parameter wie folgt:

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Gruppenname	Name der zentralen Flow-Protokollgruppe, an die Amazon EC2-Instanzen ihre Protokoll-Streams weiterleiten
MID Server	MID-Server, den Service-Mapping zum Erfassen der Daten aus der Flow-Protokollgruppe in AWS verwendet
AWS-Anmeldeinformationen	Wählen Sie die AWS-Anmeldeinformationen für das Konto aus, für das Sie Flow-Protokolle erfassen möchten.

   e. Klicken Sie auf **Absenden**.
3. Vergewissern Sie sich, dass Service-Mapping Daten mit VPC-Flow-Protokollen erfasst:
   a. Wählen Sie im Formular **AWS VPC-Flow-Protokolle** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.
   b. Navigieren zu **Systemdefinitionen** > **Tabellen**an.
   c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.

e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Suchassistenten für Windows konfigurieren

Mit dem Suchassistenten im Musterdesigner können Sie in Dateien oder Registrierungen suchen. Laden Sie grep-Dateien in Ihre Instanz hoch, um diese Funktion für die Suche auf Windows-Servern zu aktivieren.

Vorbereitungen

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

grep ist ein Dienstprogramm, mit dem der Suchassistent Dateien nach Übereinstimmungen durchsucht. grep ist für Unix-basierte Systeme nativ, daher müssen Sie es nur für Windows-basierte Konfigurationselemente (CI) hochladen. Sobald Sie grep-Dateien in die Instanz hochladen, werden sie auf alle MID-Server übertragen, die anschließend die Dateien an alle Windows-basierten CIs in Ihrer Organisation verteilen.

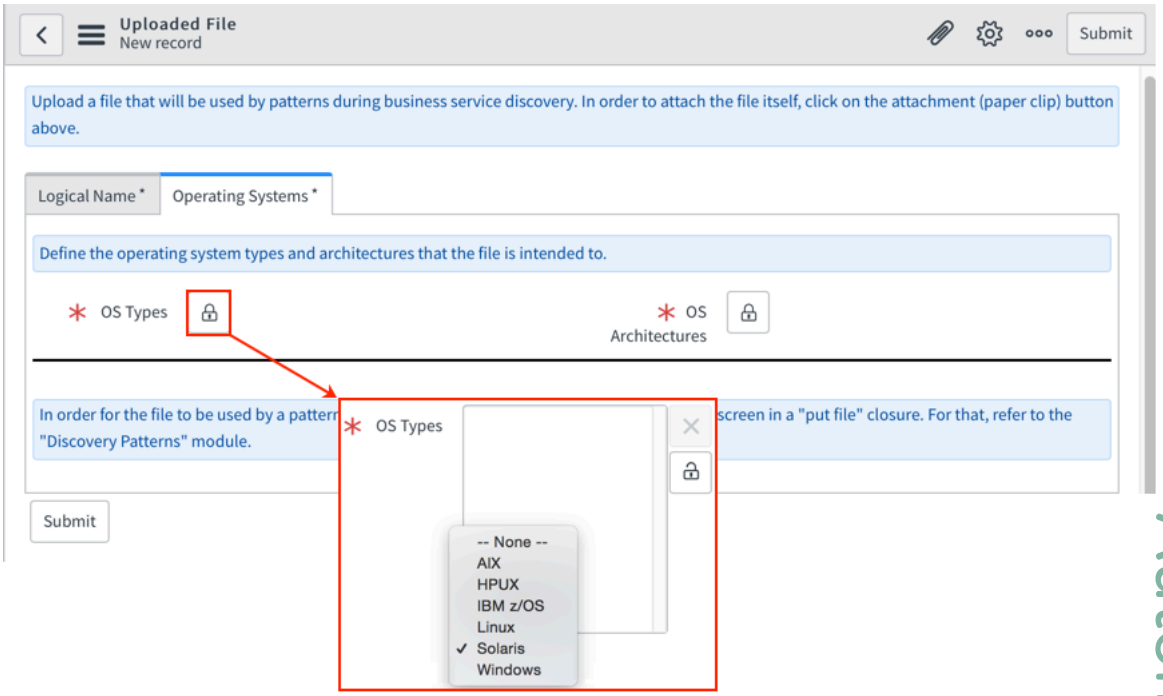
Prozedur

1. Laden Sie die folgenden Dateien aus dem Internet auf den Computer herunter.
   - egrep.exe
   - libiconv2.dll
   - libintl3.dll
   - pcre3.dll
   - regex2.dll

   Beispielsweise können Sie die ZIP-Dateien für die Ordner **Dependencies** und **Binaries** vom folgenden Speicherort herunterladen: http://gnuwin32.sourceforge.net/packages/grep.htm
2. Extrahieren Sie die Dateien.

   Nach dem Extrahieren der heruntergeladenen Ordner befinden sich die Dateien an folgenden Speicherorten:
   - grep-2.5.4-bin/bin/egrep.exe
   - grep-2.5.4-dep/bin/libiconv2.dll
   - grep-2.5.4-dep/bin/libintl3.dll
   - grep-2.5.4-dep/bin/pcre3.dll
   - grep-2.5.4-dep/bin/regex2.dll
3. Navigieren zu **Musterdesigner** > **Hochgeladene Dateien**an.
4. Klicken Sie auf **Neu**.
5. Geben Sie den ursprünglichen Dateinamen in das Feld **Name** auf der Registerkarte **Logischer Name** ein, z. B. egrep.exe.
6. Klicken Sie auf **BS-Typen** und wählen Sie **Windows** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **BS-Architekturen**, und wählen Sie sowohl die 32-Bit- als auch die 64-Bit-Option aus.
8. Klicken Sie auf das Symbol **Anhänge verwalten**.
9. Klicken Sie auf **Dateien wählen**.
10. Navigieren Sie im Ordner **Downloads** auf Ihrem Computer zu der Datei, deren Namen Sie zuvor eingegeben haben, z. B. egrep.exe.
11. Klicken Sie auf **Auswählen**.
12. Schließen Sie das Fenster „Anhänge“.
13. Wiederholen Sie Schritt 3 bis Schritt 11, um die restlichen Dateien hochzuladen:
    - libiconv2.dll
    - libintl3.dll
    - pcre3.dll
    - regex2.dll
14. Stellen Sie eine Verbindung zu jedem Windows-MID-Server her, und aktualisieren Sie die Umgebungsvariable PATH mit dem Speicherort des bin-Verzeichnisses, in dem egrep.exe installiert ist.

Anzeige für CI-Attribute ändern

Sie können steuern, welche Attribute der Configuration Items (CI) das System im Eigenschaftenbereich der Serviceinstanz -Karten anzeigt.

Vorbereitungen
Machen Sie sich mit dem Konzept der Ansichten vertraut. Weitere Informationen zu Ansichten finden Sie unter Ansichtsverwaltung .

Entscheiden Sie, für welche CI-Klassen Sie die Anzeige ändern möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheiden Sie, ob Sie die Anzeige für übergeordnete CI-Klassen ändern möchten, damit die Ansichtsänderungen in allen untergeordneten CI-Klassen wirksam werden. Führen Sie die folgenden Schritte aus, um die übergeordnete CI-Klasse einer CI-Klasse zu überprüfen:

Hinweis: Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

1. Navigieren zu **Systemdefinition** > **Tabellen**an.
2. Legen Sie das Suchfeld auf **Name** fest, und geben Sie die relevante CI-Klasse ein.

   Eine Liste mit allen CI-Klassen, die dem Namen entsprechen, wird angezeigt.
3. Überprüfen Sie die Spalte **Erweitert Tabelle**, um die übergeordnete CI-Klasse anzuzeigen.

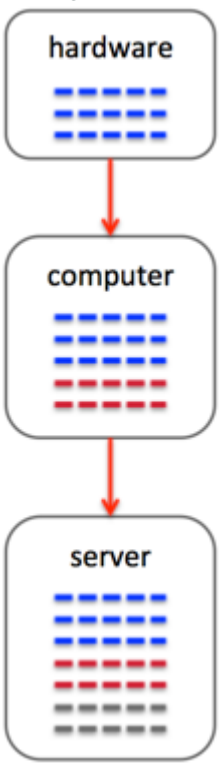
Erforderliche Rolle: Service_Mapping_admin oder App_Service_admin

Warum und wann dieser Vorgang ausgeführt wird
Bei der Arbeit mit Serviceinstanz -Karten werden im Eigenschaftenbereich Attribute für CIs und Verbindungen angezeigt, die Sie in einer Karte auswählen. Da eine große Anzahl von anzuzeigenden Attributen vorhanden ist, sollten Sie auswählen, welche Attribute in welcher Reihenfolge angezeigt werden.

Die Attribute und ihre Anzeigereihenfolge werden durch eine Kombination aus der CI-Typdefinition und der Ansicht für diesen CI-Typ bestimmt.

CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet.

Untergeordnete CI-Klassen leiten Attribute von ihren übergeordneten Klassen ab

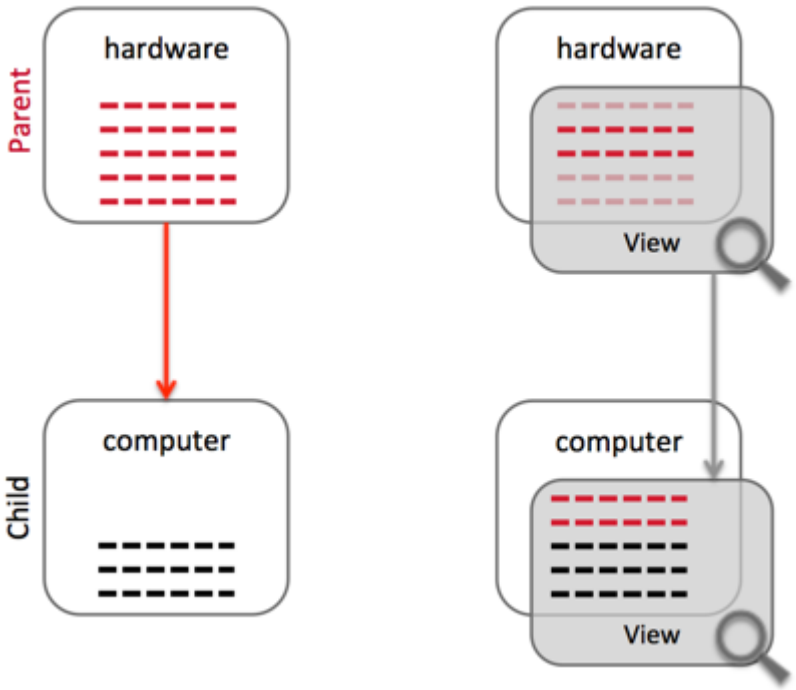


Die Ansicht, die die Attributanzeige in Serviceinstanz -Karten steuert, wird *sa_map_properties* genannt. Sie können diese Ansicht neuen CI-Klassen zuweisen oder

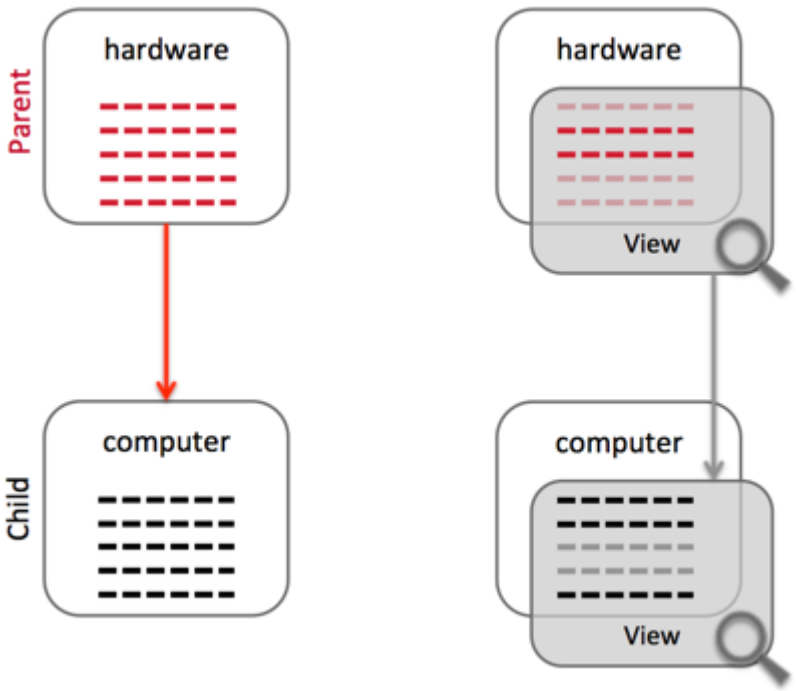
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Ansicht für CI-Klassen ändern, die sie bereits verwenden. Verwenden Sie die CI-Typhierarchie zum Konfigurieren der *sa_map_properties view*:

- Die übergeordnete CI-Klasse ganz oben in der Hierarchie lautet *cmdb*.
- Wenn Sie die Ansicht für eine untergeordnete CI-Klasse nicht definieren, zeigt das System vom übergeordneten Element abgeleitete Attribute und zusätzlich alle Attribute dieser untergeordneten CI-Klasse an.

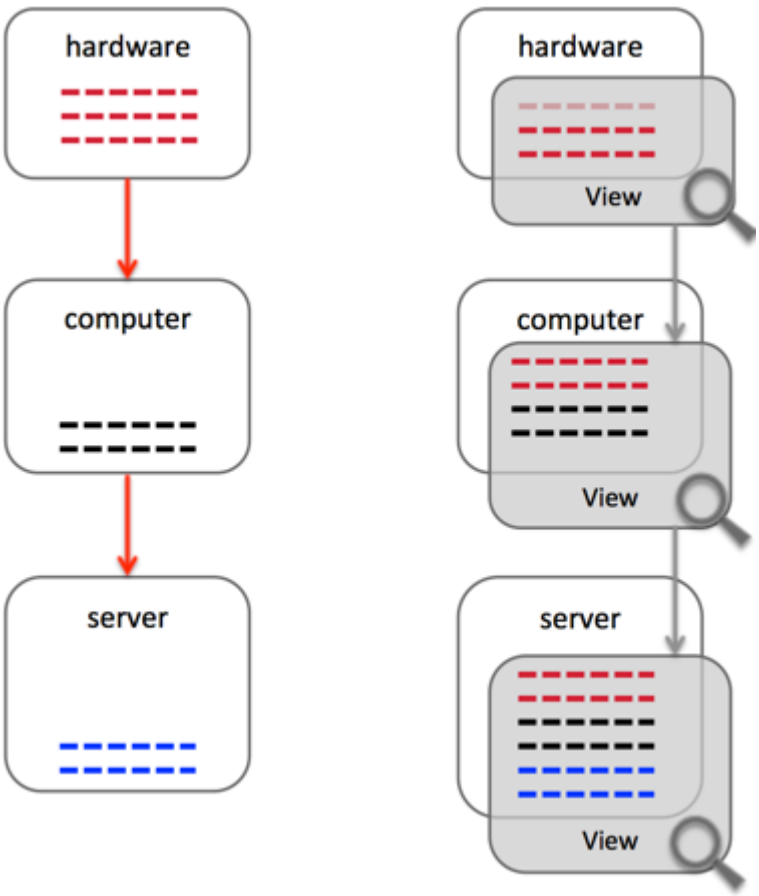


- Wenn Sie eine Ansicht für eine untergeordnete CI-Klasse definieren, enthält diese nur die Attribute, die Sie der untergeordneten CI-Klasse ausdrücklich hinzugefügt haben. Das System zeigt keines seiner übergeordneten Attribute automatisch an.



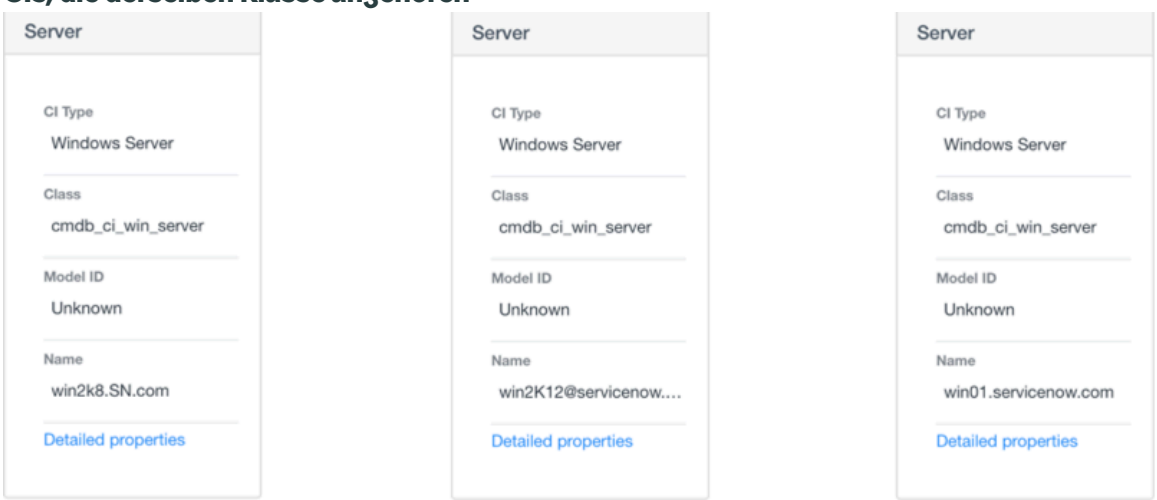
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie der Ansicht keine übergeordnete CI-Klasse oder deren untergeordnete CI-Klasse hinzufügen, verwendet das System die aufsteigende CI-Klasse, die der Ansicht hinzugefügt wurde, zusätzlich zu allen Attributen aller übergeordneten CI-Klassen in der Hierarchie zwischen diesen untergeordneten CI-Klassen sowie die übergeordnete CI-Klasse, die der Ansicht hinzugefügt wird.



Wenn Sie beispielsweise die Ansicht *sa_map_properties* für die CI-Klasse für Windows-Server definieren, werden im Eigenschaftenbereich für alle Windows-Server dieselben Attribute angezeigt: CI-Typ (Klasse), Klasse, Modell-ID und Name.

CIs, die derselben Klasse angehören



Sie können die Ansicht jederzeit ändern.

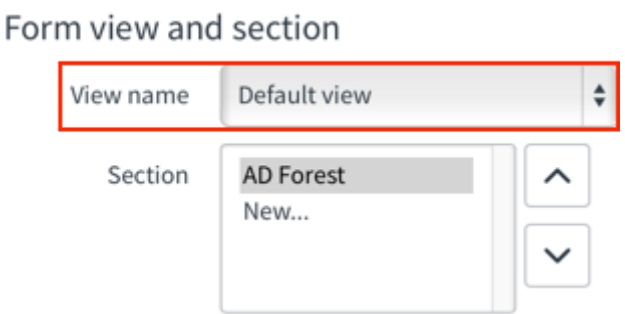
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Wählen Sie in der Serviceinstanz -Karte das CI aus, dessen Attribute Sie ändern möchten.
3. Klicken Sie im Bereich **Eigenschaften** auf **Detaillierte Eigenschaften**.

4. Klicken Sie auf der Seite „Detaillierte CI-Eigenschaften“ auf das Symbol **Zusätzliche Aktionen**, und wählen Sie **Konfigurieren > Formularlayout** aus.
5. Legen Sie in der Liste **Name der Ansicht** unter **Formularansicht und -abschnitt** fest, welche Ansicht Sie ändern möchten:



   - Wählen Sie **sa_map_properties** aus, wenn es in der Liste angezeigt wird, oder
   - Wenn **sa_map_properties** nicht in der Liste angezeigt wird:
     a. Wählen Sie **Neu**.
     b. Geben Sie im Feld **Name der Ansicht** `sa_map_properties` ein.
     c. Klicken Sie auf **OK**.
6. Verwenden Sie den Slushbucket, um Attribute zu der Ansicht hinzuzufügen oder daraus zu entfernen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Speichern**.
8. Kehren Sie zur Serviceinstanz -Karte zurück, und wählen Sie das CI, für das Sie die Ansicht geändert haben, erneut aus.
   Im Bereich **Eigenschaften** werden die Attribute angezeigt, die Sie für die Ansicht konfiguriert haben.
9. Wiederholen Sie bei Bedarf das Verfahren für weitere CI-Klassen.

Zugehörige Informationen

CI-Attribute in der Anwendungsservicezuordnung anzeigen –

Unterstützung für Windows-Server mit nicht-englischen Betriebssystemen konfigurieren

Sie können Ihre ServiceNow AI Platform so konfigurieren, dass sie Windows-Server unterstützt, die nicht das englische Windows-Betriebssystem (OS) verwenden.

Vorbereitungen

Sie können dieses Verfahren nur auf MID Servers n verwenden, die Standorte bedienen, die kein englisches Betriebssystem verwenden. Alternativ können Sie diese Konfiguration für alle MID Servers auf einmal durchführen, auch für MID Servers, die für Standorte mit englischen Betriebssystemen verwendet werden.

Erforderliche Rolle: mid_server

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Service-Mapping nicht bereitstellt, ist diese Konfiguration nicht erforderlich.

Manchmal entscheiden sich Unternehmen für die Verwendung von Betriebssystemen in lokalen Sprachen. Ein lokalisiertes Betriebssystem (BS) ist zwar benutzerfreundlich, stellt jedoch ein Problem dar, wenn es um die automatische Erkennung von Windows-Servern geht, auf denen das lokalisierte Betriebssystem ausgeführt wird. Während des Erkennungs- und Zuordnungsprozesses sendet Service-Mapping über einen MID-Server Erkennungsbefehle an die Windows-Server in Ihrer Infrastruktur. Wenn ein Windows-Server eine Nachricht in einer anderen Sprache als Englisch zurückgibt, erkennt Service-Mapping sie nicht als gültige Antwort, und die Interaktion schlägt fehl.

Wenn Ihre Organisation für einige der Windows-Server ein nicht englisches Betriebssystem verwendet, müssen Sie dieses Verfahren ausführen, um sicherzustellen, dass Service-Mapping auf alle Windows-Server zugreifen kann, nicht nur auf die mit dem englischen Betriebssystem. Diese Konfiguration ermöglicht es dem MID-Server, der sich zwischen Service-Mapping und Windows-Servern befindet, eine nicht englische Antwort von einem Windows-Server zu erkennen und die Sprache des CI-Betriebssystems in Englisch zu ändern.

Diese Konfiguration betrifft nur den Benutzer, für den Sie dieses Verfahren durchführen.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** In **Module** Bereich.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Feld **Name** `mid.servicewatch.wmi.mui` ein.
4. Im Feld **Wert** geben Sie `wahr` ein.
5. Wählen Sie im Feld **MID Server** den Server aus, auf den Sie diese Änderung anwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Änderung auf alle MID Server in Ihrer Organisation anwenden	Lassen Sie das Feld MID-Server leer.
Änderung auf einen bestimmten MID-Server anwenden	Wählen Sie den erforderlichen MID-Server aus der Liste aus.

6. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbezogene Zuordnungsfehler beheben

MID-Server

Datei rctrlx.exe auf MID Servers hochladen

Laden Sie die Datei rctrlx.exe auf MID Servers hoch, um die Ausführung von Erkennungsbefehlen unter Microsoft Exchange 2007 und 2010 sowie Citrix XenApp zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Während des Erkennungsprozesses führt der MID-Server Service-Mapping und Discovery-Muster auf Anwendungen und Geräten innerhalb des Organisationsnetzwerks aus. Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Um Befehle korrekt über PowerShell auszuführen, führt der MID-Server Muster als Services mit der Datei rctrlx.exe aus. Die Datei rctrlx.exe ist Teil des Open Source-Dienstprogramms ManagePC und kann im Internet heruntergeladen werden.

Laden Sie für jeden MID-Server in Ihrer Bereitstellung eine rctrlx.exe-Datei hoch.

Prozedur

1. Laden Sie die Datei rctrix.exe aus dem Internet auf Ihren Computer herunter.

   Beispielsweise finden Sie unter https://github.com/leonsodhi/rctrlx/releases die neuesten Versionen der Datei rctrlx.exe:

2. Speichern Sie die Datei rctrlx.exe im Ordner für Windows 32-Bit-Server:

   <MID Server-Installationsverzeichnis>\agent\bin\sw_wmi\bin\32

   Zum Beispiel: C:\SN_MID\SN_MID_Dev\agent\bin\sw_wmi\bin\32.

3. Speichern Sie die Datei rctrlx.exe im Ordner für Windows 64-Bit-Server:

   <MID Server-Installationsverzeichnis>\agent\bin\sw_wmi\bin\64

   Zum Beispiel: C:\SN_MID\SN_MID_Dev\agent\bin\sw_wmi\bin\64.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

MID-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feinabstimmung Service-Mapping Mit MID-Affinität und IP-Wiederverwendung

Die MID-Server Für die Zuordnung eines Anwendungsservice ist in Subnetzwerken mit sich überschneidenden IP-Bereichen und wiederverwendeten IP-Adressen möglicherweise falsch identifiziert. So aktivieren Sie die erfolgreiche Discovery von Ressourcen, die einem Subnetzwerk zugeordnet sind: Service-Mapping Stellt mehrere Eigenschaften für bereit MID-Server Identifizierung.

Die Netzwerke großer Organisationen sind oft in zahlreiche Subnetzwerke unterteilt, die jeweils als eigenes Netzwerk fungieren. Service-Mapping Wählt aus MID-Server Basierend auf dem IP-Bereich. Subnetzwerke mit überlappenden IP-Bereichen und der Wiederverwendung von IP-Adressen bergen das Risiko, dass der MID-Server, der zum Zuordnen eines Anwendungsservice erforderlich ist, falsch identifiziert wird. Discovery kann daher fehlschlagen, was zu unvollständigen oder ungenauen Servicezuordnungen führt.

Zwei Eigenschaften in enthalten Service-Mapping Bieten Sie Systemadministratoren eine Lösung an.

Hinweis: Um die volle Funktionalität zu gewährleisten, erfordert diese Funktion die Installation von CMDB CI-Klassenmodelle Version 1.50.0 oder höher.

- MID-Affinität: Wenn die horizontale Discovery konfiguriert wurde, können Sie aktivieren *sm.topdown.reuse_mid_from_hd_schedule*Systemeigenschaft. Identifiziert das Subnetzwerk MID-Server Das zuvor während der horizontalen Discovery konfiguriert wurde und für die Top Down-Discovery in wiederverwendet Service-Mapping. Konfigurieren von MID-Server Die Verwendung dieser Methode erfordert weniger Zeit und führt zu weniger Fehlidentifizierungen.
- Netzwerkstandort: Nachdem Standorte den horizontalen Discovery-Zeitplänen zugewiesen wurden, können Sie aktivieren *sm.network_location.detect_host_by_location*Systemeigenschaft, die einen hinzufügt **Netzwerkstandort** Feld zum Einstiegspunkt-Formular. Der Discovery-Prozess von oben nach unten beginnt mit dem in diesem Formular definierten Einstiegspunkt und kann dann beide identifizieren MID-Server Und den Host, der den im horizontalen Discovery-Zeitplan angegebenen Speicherort verwendet.

Weitere Informationen zum Aktivieren der einzelnen Eigenschaften finden Sie unter Mit Service-Mapping installierte Komponenten

Zugehörige Informationen

Horizontale Erkennung planen

Konfiguration des MID Servers für Service-Mapping

Konfigurieren Service-Mapping Zum Arbeiten mit Configuration Management Database (CMDB)

Konfigurieren Service-Mapping Um die vorhandenen Daten in zu verwenden CMDB Zum Ausführen der Top Down-Discovery und Zuordnen von Anwendungsservices.

Vorbereitungen

Überprüfen Sie, ob die erforderlichen Tabellen gemäß dem in erläuterten Prozess mit Daten gefüllt sind CMDB-basierte Zuordnung.

- Tabelle „TCP-Verbindung (Transmission Control Protocol)“ [cmdb_tcp]
- Tabelle „laufender Prozess“ [cmdb_running_Process]
- Tabelle „Hardware“ [cmdb_ci_Hardware]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestätigen Sie, dass Sie installiert haben Service-Mapping Plus August 2024-Version von ServiceNow® Store.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Eingeben von sys_properties.list im Navigationsfilter.
2. Suchen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] nach *sa.topdown.enable_cmdb_based_mapping*Eigenschaft.
3. Legen Sie fest *sa.topdown.enable_cmdb_based_mapping*Zu konfigurierende Systemeigenschaft Service-Mapping Um die Daten in zu verwenden CMDB.
   a. Bestätigen Sie, dass **Typ** Der Feldwert ist auf „wahr“|falsch“ festgelegt.
   b. Legen Sie fest **Wert** Feld bis Wahr .

Konfigurieren Agent Client Collector Zur Verwendung mit Service-Mapping

Konfigurieren Agent Client Collector Dient zum Erkennen und Zuordnen von Anwendungsservices, ohne Anmeldeinformationen für konfigurieren zu müssen MID-Server.

Vorbereitungen

Bestätigen Sie, dass Sie beide installiert haben Agent Client Collector Visibility – Inhalt Version 3.5.0 und Kubernetes Visibility Agent (KVA) Von ServiceNow® Store.

Stellen Sie sicher Agent Client Collector Wurde konfiguriert. Weitere Informationen finden Sie unter Anwendungsmuster für Agent Client Collector.

Überprüfen Sie, ob Service Desk-Mitarbeiter über die erforderlichen Berechtigungen verfügen, um die erforderlichen Anwendungsmusterbefehle für den erfolgreichen Abschluss der Top Down-Discovery auszuführen. Weitere Informationen finden Sie unter SSH-Befehle, die während der probenbasierten Discovery einen privilegierten Anwender erfordern und SSH-Befehle, die während der probenbasierten Discovery keinen privilegierten Anwender erfordern.

Wichtig: Diese Konfiguration erfordert einen MID-Server Die ausgeführt wird, um ordnungsgemäß zu funktionieren. Service-Mapping Wählt aus MID-Server Mit der der Ziel-Agent eine Verbindung herstellt, um Befehle über den Agent auszuführen.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector Aktiviert die Erkennung und Zuordnung von Anwendungsservices, ohne dass Sie Anmeldeinformationen für einrichten müssen MID-Server. Sie können sowohl Top Down als auch maschinelles Lernen bereitstellen Service-Mapping Und profitieren Sie von einem vereinfachten Ansatz für die Zuordnung von Anwendungsservices.

Prozedur

1. Eingeben von sys_properties.list im Navigationsfilter.
2. Suchen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] nach *sa.topdown.mapping_with_acc_mode*Eigenschaft.
3. Legen Sie die zu konfigurierende Eigenschaft fest Agent Client Collector Für Service-Mapping Und definieren Sie MID-Server Auswahlmodus für Discovery von oben nach unten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Bestätigen Sie, dass **Typ** Feldwert ist auf Ganzzahl festgelegt.

b. Legen Sie fest, wie die Top Down-Discovery ausgeführt werden soll, indem Sie festlegen **Wert** Feldwert. Mögliche Werte:

- `0` (Standard) – die Top Down-Discovery wird mit ausgeführt MID-Server Ausschließlich.
- `1` – Die Top Down-Discovery versucht anfänglich, mit auszuführen Agent Client Collector. Wenn kein Service Desk-Mitarbeiter verfügbar ist, wird standardmäßig verwendet MID-Server.
- `2` – Die Top Down-Discovery wird mit ausgeführt Agent Client Collector Ausschließlich. Wenn nicht erfolgreich, wird der Prozess beendet.

Service-Mapping Wird Verwendet

Als Service-Mapping Administrator, Sie unterstützen Unternehmen bei ihren Bemühungen, kritische Anwendungsservices zuzuordnen und zu verwalten, damit sie serviceorientiert bleiben.

Greifen Sie auf zu Einheitliche Übersicht Funktion aus dem Service-Mapping Arbeitsbereich

Zeigen Sie eine hierarchische Zuordnung von CIs und den Beziehungen zwischen ihnen an, indem Sie Zugriff auf hinzufügen Einheitliche Übersicht-Funktion für Service-Mapping Arbeitsbereich.

Vorbereitungen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- Vancouver Release oder höher
- Service-Mapping Plus, Release November 2023
- CMDB-Arbeitsbereich, Version 4.0.1 oder höher.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Einheitliche Übersicht Um mehr über zu erfahren Einheitliche Übersicht Funktion.

Hinweis: Die Einheitliche Übersicht Funktionsangebote eingeschränkt Service-Mapping Funktionalität.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Geben Sie Ein *`sn_sm_scoped_app.sa.unified_map.enabled`*Im Feld Suche.
3. Bestätigen Sie, dass der Wert der Eigenschaft auf „wahr“ festgelegt ist.
4. Navigieren zu **Arbeitsbereiche** > *`Service-Mapping`*an.

   Hinweis: Zugriff auf Einheitliche Übersicht Ist nur über verfügbar Service-Mapping Arbeitsbereich.

5. Wählen Sie das Widget zugeordnete Anwendungsservices aus.
6. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Anwendungsservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie aus **Zeigen Sie die Karte an** Schaltfläche.
   Eine neue Registerkarte mit wird geöffnet Einheitliche Übersicht Für den Anwendungsservice in CMDB Arbeitsbereich.

Zugehörige Informationen

Zeigen Sie die Attribute eines CI oder einer Beziehung an

Zeigen Sie Serviceinstanzen für ein CI an

Zeigen Sie historische Changes für ein CI an

Ordnen Sie Anwendungsservices basierend auf zu Empfehlungen für automatisierte Services

Ordnen Sie einen neuen Anwendungsservice basierend auf automatisch generierten Vorschlägen zu. Verwenden Sie Empfehlungen für automatisierte Services Oder Service-Fingerabdrücke Funktionen zum Erstellen eines neuen Anwendungsservice oder zum Hinzufügen zu einem vorhandenen Service mit wenigen Klicks.

Vorbereitungen

- Service-Mapping Plus muss installiert sein. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.
- Bestätigen Sie, dass die Anwendung bereit ist, Anwendungsservices zu erkennen und zuzuordnen. Weitere Informationen finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zu automatisch generierten Vorschlägen können Sie mit auch einen Anwendungsservice identifizieren und auswählen Service-Fingerabdrücke Vorschläge, die Informationen zu den Komponenten in den Anwendungsservice-Candidates enthalten. Weitere Informationen finden Sie unter Empfehlungen für automatisierte Services.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**
2. Wählen Sie Aus **ML-gestützte Kandidaten** .

   Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, der Filterprozess wurde aktualisiert, um nur die relevantesten Kandidaten einzubeziehen, ausgenommen ignorierte oder irrelevante Kandidaten. Diese Erweiterung erfordert die Installation von ITOM Content Service.

3. Wählen Sie einen Anwendungsservice entweder basierend auf Kandidatenvorschlägen aus, oder identifizieren Sie Services mit der gewünschten Komponente.

Suchmethode	Aktionen
Wählen Sie basierend auf einer gewünschten Komponente aus Kandidaten aus	**a.** Wählen Sie die Registerkarte Service-Fingerabdrücke aus. **b.** Überprüfen Sie die Liste von Service-Fingerabdrücke Vorschläge, die Komponenten enthalten. **c.** Wählen Sie Ihren bevorzugten Anwendungsservice-Kandidaten aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchmethode	Aktionen
Wählen Sie den Kandidaten anhand der grundlegenden Details aus	**a.** Wählen Sie die Registerkarte Anwendungsservicevorschläge aus. **b.** Überprüfen Sie die Liste der vorgeschlagenen Anwendungsservices. **c.** Wählen Sie Ihren bevorzugten Kandidaten aus.

4. **Wahlweise:** Zeigen Sie eine Vorschau der Karte an.

   a. Wählen Sie Aus **Vorschau der Karte anzeigen** .

   b. Überprüfen Sie die Komponenten der vorgeschlagenen Anwendungsservicezuordnung.

   > **Hinweis:** Diese Vorschauzuordnung kann sich von dem Kandidaten unterscheiden, da sie keine fehlenden Verbindungen anzeigt. Weitere Informationen finden Sie unter Automatisierte Problembehandlung für Servicevorschläge [KB1205971] artikel in ServiceNow Support Knowledge Base.

   c. Wählen Sie Aus **Listennavigation** Um zur Kandidatenliste zurückzukehren.

5. Wählen Sie Aus **Anwendungsservice zuordnen** .
6. Erstellen Sie entweder einen neuen Anwendungsservice mit dem vorgeschlagenen Kandidaten, oder fügen Sie den vorgeschlagenen Kandidaten einem vorhandenen Anwendungsservice hinzu.

Aktion	Sc te
Erstellen Sie einen neuen Anwendungsservice	**a.** Wählen Sie Aus **Erstellen Sie einen neuen Service** . **b.** Füllen Sie im Formular die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
Fel– der aus. **For mu lar „An wen dungs ser vice zu ord nen“** Name Vorab ausgefüllter eindeutiger Name für den neuen Anwendungs Verwenden Sie diesen Namen. Geben Sie einen eindeutigen Namen ein, oder wählen Sie aus **Andere Namensvorsc** Für zusätzliche Optionen. Weitere Informationen finden Sie unter Namensvorschl für	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
	Anwendungsser Kandidaten.
	Nr. Anzahl ausgefüllte eindeutige ID für den Anwendungsser
	Beschreibung des neuen Anwendungsser
	Der Servicebesitzer Anwender, der Änderungen am zugeordneten Anwendungsser genehmigt oder ablehnt.
	Eine Gruppe bestimmte Anwendungsser der Sie diesen Service hinzufügen möchten. Die Standardeinstell „alle“ bedeutet, dass der Anwendungsser für alle Gruppen verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
Fügen Sie einem vorhandenen Service einen Kandidaten hinzu	**a.** Wählen Sie Aus **Zu vorhandenem Service hinzufügen**. **b.** Beginnen Sie mit der Eingabe des Namens des vorhandenen Service, und wählen Sie den gewünschten Service aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie Aus **Kartenservice** .
8. **Wahlweise:** Wählen Sie Aus **Zeigen Sie die Karte an** Zum Anzeigen des neuen oder geänderten Anwendungsservice.

Zugehörige Informationen

Empfehlungen für automatisierte Services

Erstellen Sie einen Anwendungsservice für nicht zugeordnete Server

Maximieren Sie die Nutzung der Ressourcen Ihrer Organisation, indem Sie Anwendungsservicekandidaten zuordnen, die nicht zugeordnete Server enthalten. Verwenden Sie Service-Mapping Widget „nicht zugeordnete Server“ des Arbeitsbereichs, um einen Anwendungsservice zu erstellen und sicherzustellen, dass Ihre Server effizient genutzt werden.

Vorbereitungen

- Stellen Sie sicher Predictive Intelligence Ist aktiviert.
- Überprüfen Sie die Bereitschaft für maschinelles Lernen.
- Bestätigen Sie, dass die Daten trainiert wurden.

Weitere Informationen finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich.

Wichtig:

Service-Mapping Plus v.1.10.0 oder höher:

Informationen zum Aktualisieren Ihrer Daten und zum Anzeigen von Anwendungskandidaten für nicht zugeordnete Server finden Sie unter Schritte zur Fehlerbehebung für die Zuordnung nicht zugeordneter Server zu Anwendungsservicekandidaten [KB1585065] In Now Support Knowledge Base.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**an.
2. Wählen Sie den nicht zugeordneten Server aus, den Sie zum Erstellen eines Anwendungsservice verwenden möchten.

Version von Service-Mapping Plus	Aktionen
Versionen, die vor Version 1.16.3 veröffentlicht wurden	**a.** In **Nicht zugeordnete Server** Kachel wählen Sie aus **Nicht zugeordnete Server mit Kandidaten-ID** Diagramm. **b.** Überprüfen Sie die Liste der vorgeschlagenen Kandidaten. **c.** Organisieren Sie die Kandidatenliste, um Ihre Arbeit zu priorisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

<table>
<tr><th>Version von Service-Mapping Plus</th><th>Aktionen</th></tr>
<tr><td></td><td>
<table>
<tr><th>Organisationsmethod</th><th>Aktion</th></tr>
<tr><td>Reihenfolge</td><td>Wählen Sie einen Spaltennamen aus, um die Ergebnisse in aufsteigender oder absteigender Reihenfolge zu sortieren.</td></tr>
<tr><td>Gruppe</td><td>Wählen Sie das Menü (⋮) Symbol zum Gruppieren der Ergebnisse nach der ausgewählten Spalte.</td></tr>
</table>
d. Wählen Sie den bevorzugten Kandidaten aus.
e. Wählen Sie Aus Anwendungsservice zu ordnen .
</td></tr>
<tr><td>Ab Version 1.16.3</td><td>
a. In Nicht zugeordnete Server Kachel wählen Sie aus Nicht zugeordnete Server mit relevantem Kandidaten Diagramm.
Hinweis: Alle Anwendungsservice-Kandidaten wurden gefiltert, um irrelevante Tools auszuschließen, sodass nur die relevantesten Kandidaten angezeigt werden.
b. Überprüfen Sie die Liste der Server mit den zugehörigen Kandidaten.
c. Organisieren Sie die Kandidatenliste, um Ihre Arbeit zu priorisieren.
<table>
<tr><th>Organisationsmethod</th><th>Aktion</th></tr>
<tr><td>Reihenfolge</td><td>Wählen Sie einen Spaltennamen aus, um die Ergebnisse in aufsteigender oder absteigender Reihenfolge zu sortieren.</td></tr>
<tr><td>Gruppe</td><td>Wählen Sie das Menü (⋮) Symbol zum Gruppieren der</td></tr>
</table>
</td></tr>
</table>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version von Service-Mapping Plus	Aktionen
	Organisationsmethod: Aktion: Ergebnisse nach der ausgewählten Spalte. **d.** Wählen Sie den bevorzugten Server oder Kandidaten aus. **e.** Wählen Sie Aus **Anwendungsservice zu ordnen** .

Ergebnis

Der ausgewählte Anwendungsservice-Candidate wird in einen Anwendungsservice konvertiert, und die ausgewählten nicht zugeordneten Server werden zugeordnet.

Ordnen Sie Ihre Anwendungsservices mithilfe von Tags in zu Service-Mapping Arbeitsbereich

Kategorisieren und organisieren Sie die Konfigurationselemente der Organisation, und ordnen Sie sie mithilfe des Tag-basierten Dashboards in Anwendungsservices zu Service-Mapping Arbeitsbereich.

Vorbereitungen

- Überprüfen Sie, ob Sie installiert haben Service-Mapping Plus Version 1.16.3, die für den Zugriff auf die Tag-basierte Zuordnung in erforderlich ist Service-Mapping Arbeitsbereich. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.
- Überprüfen und analysieren Sie die Tag-Nutzung Ihrer Organisation, und erstellen Sie eine Liste aller Tags und ihrer Zwecke. Verwenden Sie die Tabelle „Schlüsselwert“ [cmdb_key_value], um die Tags in anzuzeigen Configuration Management Database (CMDB).
- Verwenden Tag-Governance Um die Tag-Anwendung in Ihrer Organisation zu optimieren. Siehe Tag-Governance Weitere Informationen finden Sie unter .
- Weisen Sie Konfigurationselementen (CIs) Tags zu, die Sie in Anwendungsservices einschließen möchten.
- Führen Sie Discovery aus, um CIs horizontal zu erkennen. Discovery befüllt die CMDB mit den CI-Daten einschließlich Tags. Weitere Informationen zur Discovery-Tag-basierten Discovery für finden Sie Service-Mapping Arbeitsbereich, siehe Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**, Und wählen Sie dann das Symbol Tag-basiertes Service-Mapping Aus dem Navigationsbereich.
2. Wählen Sie Aus **Erstellen Sie Servicezuordnungen** .
3. Wählen Sie entweder eine vorhandene Tag-Kategorie aus, oder erstellen Sie eine neue Tag-Kategorie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Kategorieoption	Aktion
Wählen Sie eine vorhandene Tag-Kategorie aus	**a.** Beginnen Sie mit der Eingabe des Kategorienamens in das Suchfeld. **b.** Wählen Sie die Tag-Kategorie aus der Liste aus. **c.** Wählen Sie Aus **Definieren Sie die Tag-Werte** Und geben Sie Werte für die ausgewählte Kategorie ein.
Eine neue Tag-Kategorie erstellen	**a.** Erstellen Sie eine neue Tag-Kategorie, indem Sie auswählen **Erstellen Sie eine neue Tag-Kategorie** . **b.** Geben Sie den Tag-Kategorienamen ein. **c.** Geben Sie Werte für die Tag-Schlüssel in ein **Tags** Feld.

4. Speichern Sie die Tag-Kategorie und -Werte, indem Sie auswählen **Speichern** .

   Hinweis: Um die Tag-Kategorien in einer Servicefamilie zu speichern, damit Sie später zurückkehren können, um den Zuordnungsprozess abzuschließen, wählen Sie aus **Speichern und beenden** Jederzeit.

5. Suchen Sie nach potenziellen Services, die den Tag-Kategorien entsprechen, indem Sie auswählen **Kandidaten suchen** .
6. Überprüfen Sie die Liste der Tag-basierten Servicekandidaten, indem Sie auswählen **Ordnen Sie ausgewählte Kandidaten zu** Wenn Sie Ihre bevorzugten Kandidaten ausgewählt haben.
7. Geben Sie bei Aufforderung einen eindeutigen Namen für die Tag-basierte Servicefamilie ein.
8. Wählen Sie Aus **Speichern und zuordnen** .

Ergebnis

Ein Tag-basierter Anwendungsservice und eine Tag-basierte Servicefamilie wurden erstellt.

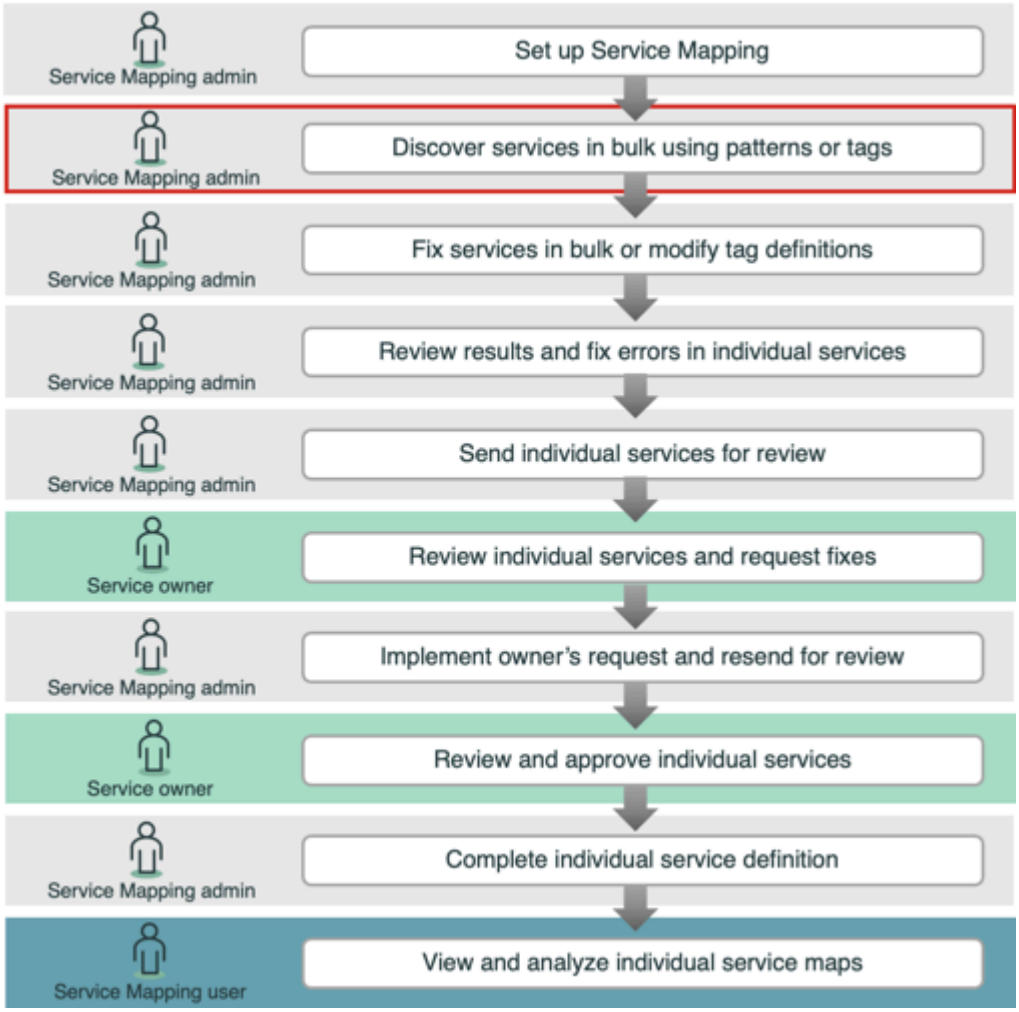
Anwendungsservice-Zuordnung mit klassisch Service-Mapping

Sie können die erste Zuordnung mehrerer oder einzelner Anwendungsservices in Ihrer Organisation mit einer Methode durchführen, die für Sie am besten geeignet ist.

Sie können Anwendungsservices zuordnen, nachdem Sie das Setup von Service-Mapping abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Workflow



Eine typische Organisation hat Hunderte von Anwendungsservices. Ihre individuelle Zuordnung kann zeit- und arbeitsaufwendig sein. Mit Service-Mapping können Sie die meisten IT-Services im Stapel zuordnen. Die gleichzeitige Zuordnung mehrerer Anwendungsservices ist sehr effektiv, aber nicht präzise. Möglicherweise müssen Sie Anwendungsservices, die bei der Stapelzuordnung ausgelassen wurden, individuell zuordnen.

Die Erkennungsmethode hängt davon ab, wie Sie Ihre Anwendungsservices vor der Zuordnung verwaltet haben und welche Informationen Sie über sie gesammelt haben:

- Ordnen Sie mehrere von vorgeschlagene Anwendungsservices zu klassisch Service-Mapping

  Service-Mapping verwendet Lastenausgleichsmodule in Ihrem Netzwerk, um mögliche Anwendungsservices (Kandidaten) zu identifizieren. Sie können alle oder ausgewählte Kandidaten im Stapel zuordnen und dabei mehrere Anwendungsservices in einem einzigen Vorgang erstellen. Diese Methode ist für Ihr Unternehmen geeignet, wenn es nicht allzu viele Informationen zu den Anwendungsservices gibt.

- Ordnen Sie Anwendungsservices mithilfe von Tags mit zu klassisch Service-Mapping

  Wenn Ihre Organisation Tags für das Asset-Management verwendet, können Sie diese Tags verwenden, um Serviceinstanzen zuzuordnen. Im Gegensatz zu anderen Zuordnungsmethoden ist es bei der tagbasierten Zuordnung nicht notwendig, Anmeldeinformationen zu konfigurieren oder Benutzern erweiterte Rechte zu gewähren. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

- Ordnen Sie mehrere Anwendungsservices aus einer CSV-Datei zu Verwenden klassisch Service-Mapping

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Methode ist für Sie geeignet, wenn Ihre Organisation organisationsübergreifende Zuordnungen und Analysen durchgeführt und einige Informationen zu geplanten Serviceinstanzen gesammelt hat. In diesem Fall können Sie die gesammelten Informationen in einer bestimmten Reihenfolge organisieren und als CSV-Datei speichern. Service-Mapping Extrahiert Informationen aus dieser Datei und erstellt potenzielle Serviceinstanzen, die als Servicekandidaten bezeichnet werden.

- Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

  Sie können individuelle, einzelne Anwendungsservices nacheinander zuordnen, indem Sie für jeden Serviceinstanz Attribute definieren. Verwenden Sie diese Zuordnungsmethode für alle Anwendungsservices, die Service-Mapping während der Stapelzuordnung nicht erkennt. Sie müssen wissen oder planen, welche Attribute von Anwendungsservices für die Zuordnung erforderlich sind.

Ordnen Sie mehrere von vorgeschlagene Anwendungsservices zu klassisch Service-Mapping

Sie können mehrere von Service Mapping identifizierte und vorgeschlagene Anwendungsservices in einem einzigen Vorgang zuordnen. Diese Methode ist für Ihr Unternehmen geeignet, wenn es nicht allzu viele Informationen zu den Anwendungsservices gibt.

Vorbereitungen
Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen haben Service-Mapping Aktiviert zum Zuordnen oder Überprüfen von Serviceinstanzen.

Unmittelbar nachdem Sie die das Service-Mapping-Setup abgeschlossen haben, erstellt Service-Mapping automatisch potenzielle Anwendungsservices, die als Kandidaten bezeichnet werden:

1. Service-Mapping extrahiert Einträge direkt von Lastenausgleichsmodulen in Ihrem Netzwerk.

2. Von Service-Mapping werden Einträge des Lastenausgleichsmoduls in potenzielle Einstiegspunkte konvertiert und in der Tabelle der Einstiegspunktkandidaten [sa_cand_entry_point] gespeichert.

   Service-Mapping erstellt auch Kandidateneinstiegspunkte basierend auf Netflow und TCP und speichert sie in der gleichen Tabelle.

   Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre Instanz des E-Mail-Services zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

3. Um Duplikate zu vermeiden, überprüft Service-Mapping, ob potenzielle Einstiegspunkte, die aus Netflow- und VPC-Protokollen erstellt werden, eindeutig sind und nicht von vorhandenen Anwendungsservices verwendet werden.

4. Service-Mapping Erstellt einen Serviceinstanzkandidaten für jeden Einstiegspunkt.

   Nicht alle Kandidaten-Serviceinstanzen korrelieren mit tatsächlichen Serviceinstanzen. Service-Mapping Filtert unwahrscheinliche Kandidaten heraus, indem ein Algorithmus angewendet wird, der Parameter wie leere IP-Adressen, Portnummern und die Anzahl der VIP-Treffer des Lastenausgleichsmoduls kleiner als 1000 berücksichtigt. Service-Mapping speichert die Kandidaten in der Tabelle „Kandidateneinstiegspunkt” [sa_cand_entry_point] in der CMDB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Discovery- und Zuordnungsprozesses Service-MappingErstellt eine Serviceinstanz aus jedem Kandidaten und weist ihm den vom Kandidaten abgerufenen Einstiegspunkt zu. Während die Mapping in Massenzuordnung eine effektive und schnelle Möglichkeit zum Erstellen zahlreicher Serviceinstanzen ist, ist das Ergebnis der Massenzuordnung nicht genau. Möglicherweise werden falsche oder doppelte Serviceinstanzen versehentlich erstellt, da die Daten aus dem Lastenausgleichsmodul Rohdaten sind. Während des Überprüfungs- und Genehmigungsprozesses überprüfen Sie alle zugeordneten Serviceinstanzen und entfernen diejenigen, die falsch erstellt wurden.

Sie können die Liste der Kandidaten weiter filtern, indem Sie bestimmte Kandidaten auswählen, die in die Erkennung aufgenommen oder von ihr ausgeschlossen werden sollen. Die Zuordnung nur ausgewählter Kandidaten bietet die folgenden Vorteile:

- Verkürzt die Erkennungszeit
- Minimiert die Anzahl der potenziell irrelevanten Anwendungsservices

Sie können unerwünschte Kandidaten mit diesen Methoden aus der Liste entfernen, indem Sie sie entweder herausfiltern oder aus der Tabelle „Kandidateneinstiegspunkt" [sa_cand_entry_point] löschen. In beiden Fällen können Sie ausgeblendete oder gelöschte Kandidaten wieder in die Liste aufnehmen.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.
2. Überprüfen Sie, dass Service-Mapping eingerichtet und bereit für die Discovery ist.
   Wenn einige obligatorische Konfigurationen fehlen, wird der Fehler oben im Fenster angezeigt.

   a. Klicken Sie auf den Link im Fehler, oder klicken Sie auf das Symbol **Bereitschaftsprüfliste** ( ).

   b. Klicken Sie im Service-Mapping-Fenster „Bereitschaftsprüfliste" auf den Link neben der Setup-Kategorie mit dem Fehlersymbol ( ).
   Sie können nur dann eine Discovery und Zuordnung durchführen, wenn das Fenster „Bereitschafts-Prüfliste" keine Fehler enthält.

   c. Führen Sie die erforderliche Aktion aus, um das Setup abzuschließen.
   Konfigurieren Sie beispielsweise fehlende Anmeldeinformationen.

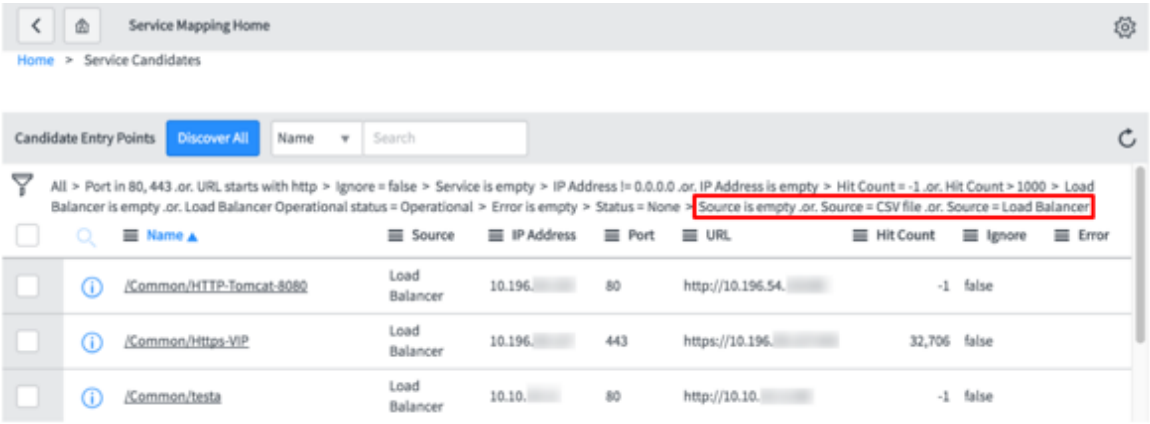
3. Um alle von Service-Mapping vorgeschlagenen Anwendungsservices zuzuordnen, klicken Sie auf **Alle erkennen** oder wählen Sie sie einzeln unter der Schaltfläche „Aktionen für ausgewählte Zeilen" aus und klicken Sie anschließend auf **Auswahl erkennen**.
4. So ordnen Sie von Service-Mapping vorgeschlagene ausgewählte Anwendungsservices zu:

   a. Klicken Sie unter der Kachel **Zuordnen** auf **Zusätzliche Optionen**.

   b. Wählen Sie **Kandidatenliste anzeigen** aus.

   c. **Wahlweise:** Zeigen Sie Kandidaten basierend auf datenverkehrsbasierten Verbindungen an, entfernen Sie die Bedingung, mit der Kandidaten herausgefiltert werden, die aus Lastenausgleichsmodulen abgerufen oder aus einer CSV-Datei importiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Kandidatenliste enthält Kandidaten mit dem Quellattribut *netstat*.

d. Überprüfen Sie die Liste der Kandidaten, um zu entscheiden, welche Sie als Anwendungsservices erkennen möchten.

e. Erstellen Sie Anwendungsservices aus den relevanten Kandidaten:

Wenn Sie Anwendungsservices aus den meisten Kandidaten erstellen möchten	**i.** Filtern Sie irrelevante Kandidaten heraus, indem Sie sie auswählen und auf **Aktionen für ausgewählte Zeilen** und dann auf **Ausgewählte ignorieren** klicken. Die irrelevanten Kandidaten werden in der Liste ausgeblendet. **Hinweis:** Zum Anzeigen von Kandidaten, die Sie zuvor herausgefiltert haben, setzen Sie die Filterbedingung **Ignorieren** auf **true**. **ii.** Alternativ filtern Sie irrelevante Kandidaten heraus, indem Sie sie auswählen, auf **Aktionen für ausgewählte Zeilen** klicken und dann **Löschen** wählen. Die irrelevanten Kandidaten werden aus der Tabelle „Kandidateneinstiegspunkt” [sa_cand_entry_point], die die Kandidaten enthält, entfernt. **Hinweis:** Service-Mapping erstellt gelöschte Kandidaten jedes Mal neu, wenn Discovery eine horizontale Erkennung derselben Lastenausgleichsmodule durchführt oder Sie Kandidaten aus derselben CSV-Datei erneut importieren. **iii.** Klicken Sie auf **Alle erkennen**.
Wenn Sie Anwendungsservices nur aus einigen Kandidaten erstellen möchten	**i.** Aktivieren Sie die Kontrollkästchen neben den relevanten Kandidaten. **ii.** Klicken Sie am unteren Bildschirmrand auf **Aktionen für ausgewählte Zeilen**. **iii.** Klicken Sie auf **Auswahl erkennen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping startet die Erkennung aller Kandidaten und erstellt Anwendungsservices aus ihnen. Wenn Sie viele Kandidaten haben, kann die Erkennung einige Zeit dauern.

Sobald der Erkennungsprozess abgeschlossen ist, erscheinen unter **Genehmigen** die Anwendungsservices, die Service-Mapping ohne Fehler und mit mindestens einem erkannten CI erkannt hat. Anwendungsservices, die mit Fehlern erkannt wurden, erscheinen auf der Kachel **Beheben**.

Nächste Maßnahme

- Wenn die Funktion für Verbindungsvorschläge aktiviert ist, fügt Service-Mapping datenverkehrsbasierte Verbindungen zu Anwendungsservices nicht automatisch hinzu, sondern macht entsprechende Vorschläge. CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen.
- Reparieren Sie die Anwendungsservices, die mit Fehlern erkannt wurden. Weitere Informationen finden Sie unter Fehler bei Anwendungsservices als Massenvorgang beheben.
- Überprüfen Sie die Liste der erstellten Anwendungsservices. Wenn Service-Mapping Anwendungsservices bei der Stapelzuordnung nicht wie erwartet erstellt hat, müssen Sie sie, wie in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping beschrieben, manuell erstellen.
- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.
- Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:
  - Service-Mapping Bietet nicht an, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
  - Es gibt keine Discovery-Nachricht, die darauf hinweist, dass die Serviceinstanz zu groß ist: *`The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.`*

  Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:

  - Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen.
  - Teilen Sie den Service in kleinere Services auf.

CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Wenn die Erkennung auf Basis von Predictive Intelligence aktiviert ist, enthalten die neu zugeordneten Anwendungsservices nur CIs und CI-Verbindungen, die anhand von Erkennungsmustern hinzugefügt wurden. Verwenden Sie Verbindungsvorschläge, um zu entscheiden, welche Konfigurationselemente (CIs) global ein- oder ausgeschlossen werden sollen. Anschließend aktualisiert Service-Mapping alle relevanten erkannten Anwendungsservices auf Grundlage Ihrer Entscheidungen.

Vorbereitungen

Bestätigen Sie, dass die auf Fingerabdrücken basierende Discovery aktiviert bleibt, da sie standardmäßig aktiviert ist. Navigieren Sie zum Überprüfen zu **Alle** > **System Eigenschaft S** > **Alle Eigenschaften**an. Überprüfen Sie, ob *`sys_property process.clustering.appfingerprint.enabled`*Eigenschaft wird nicht in der Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestätigen Sie diese Discovery basierend auf Predictive Intelligence Ist aktiviert.
Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob `sa_ml.connection_suggestions.active`Eigenschaft ist auf festgelegt **Wahr** .

Mithilfe von Verbindungsvorschlägen können Sie CIs nur in Bezug auf von Service-Mapping erkannte Anwendungsservices hinzufügen oder entfernen.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Predictive Intelligence Ist aktiviert, Service-Mapping Fügt automatisch Verbindungen zu Serviceinstanzen basierend auf Verbindungsregeln hinzu. Diese Vorschläge werden mithilfe von verkehrsbezogenen Daten aus dem generiert Configuration Management Database (CMDB) Und die Analyse von Anwendungsfingerabdrücken, CIs und Prozessen von Predictive Intelligence. Predictive Intelligence Wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und ordnet ihre Relevanz ein. Service-Mapping Verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Es werden auch Verbindungsvorschläge generiert Für Server und Lastenausgleichsmodule Damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wenn Sie nicht sicher sind, welche datenverkehrsbasierten Verbindungen relevant sind, identifizieren Sie eine Gruppe von Anwendungsservices, die Ihr Unternehmen für diesen Zweck verwendet. Sie können in dieser Gruppe CI-Verbindungen für einen einzelnen Anwendungsservice hinzufügen oder entfernen. Verwenden Sie dann die Verbindungen, die Sie für diesen Service erstellt haben, als Beispiel für datenverkehrsbasierte Verbindungen für mehrere Anwendungsservices.

Prozedur

1. **Wahlweise:** Folgen Sie den Schritten unter Anwendungen basierend auf Fingerabdrücken erkennen, um Informationen zu allen Anwendungs-CIs in Verbindungsvorschlägen anzuzeigen.

   Wichtig: Wenn Sie keine fingerabdruckbasierte Erkennung verwenden, kann dies dazu führen, dass manche Anwendungs-CIs als allgemeine Anwendungen zugeordnet werden.

2. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsvorschläge**an.
   Das Fenster für Verbindungsvorschläge wird geöffnet.
3. Erweitern Sie die relevante Gruppe, um die Verbindungsvorschläge anzuzeigen.
   Erweitern Sie beispielsweise die Gruppe **python - python**.
4. Überprüfen Sie die Vorschlagsdetails unter Berücksichtigung der Parameter, die in der Liste „Verbindungsvorschläge“ abgedeckt sind.
   Weitere Informationen finden Sie unter Liste „Verbindungsvorschlagen“.
5. Aktivieren Sie die Kontrollkästchen neben den relevanten Vorschlägen, und klicken Sie auf die Aktionsschaltfläche am unteren Rand des Fensters:

Aktion	Ergebnis
Hinzufügen	Service-Mapping Enthält sowohl die Verbindungen als auch die CIs, zu denen diese Verbindungen führen, wodurch sie Teil der Serviceinstanz werden. Der `Decision`-Wert für hinzugefügte Verbindungen ändert sich in **Manuell hinzugefügt**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Ergebnis
Ausschließen	Service-Mapping Schließt Verbindungen und die CIs aus, zu denen sie führen, aus der Serviceinstanz aus. Der `Decision`-Wert für entfernte Verbindungen ändert sich in **Manuell ausgeschlossen**.
Zurücksetzen	Service-Mapping Kehrt frühere Entscheidungen zurück, unabhängig davon, ob sie manuell oder per Regel getroffen wurden. Der Wert `Decision` für zurückgesetzte Verbindungen ändern sich in **Unentschieden**. Diese Aktion ist nur relevant, wenn Sie bereits Verbindungsvorschläge zum Abschließen dieser Serviceinstanz verwendet haben.

6. Aktualisieren Sie die Verbindungsvorschläge, um die von Ihnen vorgenommenen Changes anzuzeigen:
   a. Klicken Sie auf das Listensteuerelemente-Symbol .
   b. Wählen Sie **Liste neu laden** aus.

Ergebnis

Service-Mapping wendet die Changes an datenverkehrsbasierten Verbindungen im Hintergrund auf alle relevanten Anwendungsservices an.

CIs für mehrere Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

Erstellen Sie Regeln für das automatische Hinzufügen von verkehrsbasierten Verbindungen und CIs, zu denen sie in erkannten Serviceinstanzen führen. Erstellen Sie Regeln, die mehreren Anwendungsservices CIs hinzufügen.

Vorbereitungen

- Analysieren Sie die Infrastruktur, die Sie zuordnen, um die häufigsten Verbindungen zu identifizieren. Diese gängigen Verbindungen sind gute Kandidaten für Verbindungsregeln.
- Anwendungen basierend auf Fingerabdrücken erkennen.
- Bestätigen Sie diese Discovery basierend auf Predictive Intelligence Ist aktiviert. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob `sa_ml.connection_suggestions.active`Eigenschaft ist auf festgelegt **Wahr** .

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen über die Bewertung und Anwendung von Verbindungsregeln mit Service-Mapping finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Neben Verbindungsregeln, die mehreren Services CIs hinzufügen, können Sie Regeln zum Hinzufügen von CIs zu bestimmten Anwendungsservices erstellen.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsregeln**an.
   Alternativ wählen Sie in einer Serviceanwendungszuordnung die Option aus **Vorschläge** > **Globale Regeln**an.
2. Erstellen Sie eine neue Verbindungsregel, indem Sie auf **Neu** klicken.
   Alternativ können Sie eine vorhandene Regel anpassen, indem Sie in der Liste auf den Namen der Regeln klicken.

   Das Formular „Verbindungsregel“ wird geöffnet.
3. Wählen Sie **Aktiv** aus, um mit der Verwendung dieser Verbindungsregel zu beginnen.
   Service-Mapping wertet nur aktive Verbindungsregeln aus.
4. Geben Sie im Feld **Name** einen eindeutigen und aussagekräftigen Namen ein.
5. Geben Sie in das Feld **Reihenfolge** den Wert ein, den Service-Mapping für die Sequenz verwendet.
6. Konfigurieren Sie die Filterbedingung im Bereich **Bedingung**.

   a. Wählen Sie das Feld, den Operator und den Wert aus.

   Example
   Um beispielsweise ausgehende Verbindungen für einen Tomcat-Server hinzuzufügen, konfigurieren Sie die folgende Filterbedingung.

   b. Um eine zusätzliche Filterbedingung zu erstellen, klicken Sie auf **Filterbedingung hinzufügen**.

   c. Um eine zusätzliche Filterbedingung mit dem Operator ODER zu erstellen, klicken Sie auf **„ODER“-Klausel hinzufügen**.
7. Wählen Sie Global aus der Liste **Bereich** aus.
8. **Wahlweise:** Geben Sie Services an, für die diese Verbindungsregel nicht gilt.

   a. Klicken Sie im Bereich **Ausgeschlossene Services** auf **Neu**.
   Das Formular „Ausgeschlossener Service“ wird geöffnet.

   b. Wählen Sie den entsprechenden Service in der Liste **Erkannter Anwendungsservice** aus.

   c. Klicken Sie auf **Absenden**.
9. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Gehen Sie wie folgt vor, um zu prüfen, ob Service-Mapping wie erwartet CIs hinzugefügt hat:

1. Nachdem die Anwendungsservices durch die geplanten Aufgaben neu erkannt wurden, öffnen Sie die Zuordnungen der Anwendungsservices, bei denen damit zu rechnen war, dass Service-Mapping CIs hinzufügt.
2. Überprüfen Sie, ob die CIs basierend auf den Verbindungsregeln korrekt hinzugefügt wurden.

Zugehörige Informationen

Erkennung auf Basis von Predictive Intelligence

Ordnen Sie Anwendungsservices mithilfe von Tags mit zu klassisch Service-Mapping

Verwenden Sie Tags, mit denen Sie Konfigurationselemente (CIs) in Ihrer Organisation kategorisieren und organisieren können, um Anwendungsservices zuzuordnen. Für die Tag-basierte Zuordnung ist es nicht erforderlich, Anmeldeinformationen zu konfigurieren oder Benutzern erhöhte Rechte zu gewähren.

Vorbereitungen

Analysieren, überprüfen und definieren Sie Tags, wie in Zuordnung von Anwendungsservices basierend auf Tags vorbereiten beschrieben.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

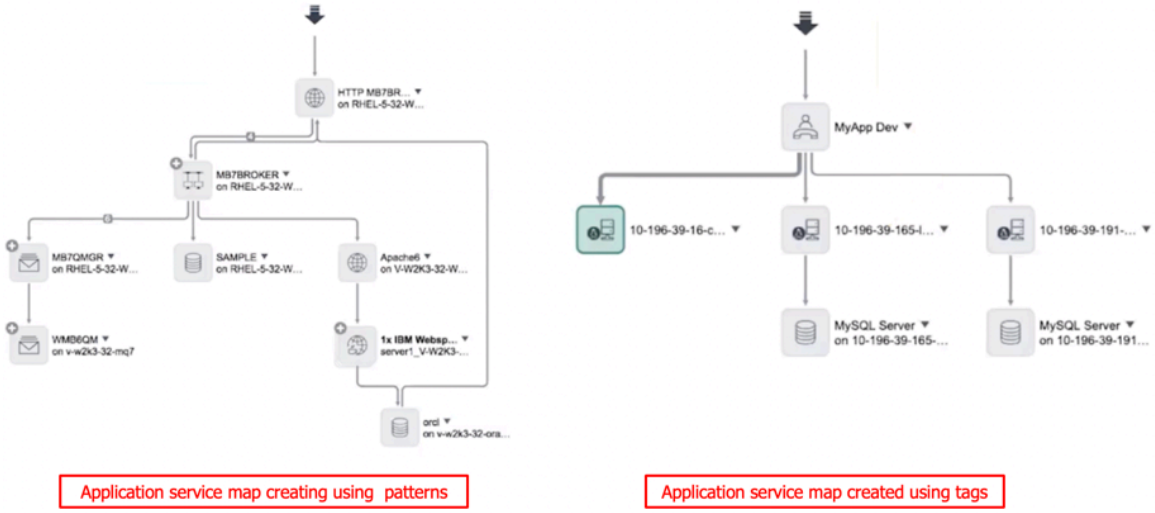
Ein Tag ist eine Bezeichnung, die aus einem Schlüssel-Wert-Paar besteht. Ihre Organisation verwendet möglicherweise Tags, um Assets zu kategorisieren und um die Abfrage- und Berichtsfunktionen zu verbessern. Discovery und Cloud Provisioning and Governance können die von allen wichtigen Cloud-Anbietern und Container-Ökosystemen verwendeten Tags erkennen. Sobald die Tags erkannt wurden, Service-Mapping Kann Serviceinstanzen basierend auf diesen Tags erstellen. Beispielsweise können Sie Tags verwenden, um alle Anwendungsservices zuzuordnen, die Ihr Unternehmen in der Produktionsumgebung in der EMEA-Region verwendet. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Das Ergebnis der tagbasierten Zuordnung ist eine hierarchische Servicezuordnung, die möglicherweise weniger genau ist als der mit Mustern erstellte Anwendungsservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich von musterbasierten und Tag-basierten Zuordnungsergebnissen



Service-Mapping erstellt Namen für Tag-basierte Services anhand von Tag-Werten, die für die Tag-Definitionen erkannt wurden, denen diese Tag-basierten Services angehören. Beispielsweise lautet der Standardservicename für die Tag-Kategorien „Environment“ und „Application“ mit „Production“ und „HR“ als Tag-Werte „production :: hr“. Tag-basierte Servicenamen verwenden Kleinbuchstaben.

Wichtig: Wenn Sie nach der Zuordnung von Services Tag-Kategorien hinzufügen oder entfernen, implementiert Service-Mapping diese Änderungen nicht für zuvor zugeordnete Services, die zu dieser Servicefamilie gehören. Weitere Informationen finden Sie unter Tag-Definitionen für die Tag-basierte Zuordnung ändern oder aktualisieren.

In nach Domänen getrennten Bereitstellungen Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.

Zum Zuordnen eines einzelnen Anwendungsservices mithilfe von Tags ohne vorläufige Konfiguration verwenden Sie den Flow basierend auf Gemeinsames Servicedatenmodell. Weitere Informationen finden Sie unter Füllen Sie Anwendungsservices mithilfe von Tags aus .

Hinweis: Ab Version 1.15.2 gibt es ein Limit von 200 Anwendungsservice-Kandidaten pro Familie.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**an.
2. Klicken Sie auf **Neu**.
3. Definieren Sie den Namen der Servicefamilienname.
4. **Wahlweise:** Wählen Sie Aus **Aktualisieren Sie Servicekandidaten regelmäßig** Für Service-Mapping Dient zum erneuten Generieren von Vorschlägen für Serviceinstanzen, die den Tag-Kategorien entsprechen, die Sie für die Servicefamilie definieren.
5. Definieren Sie die Tag-Kategorien und Tag-Werte, die für die Zuordnung von Serviceinstanzen verwendet werden sollen, die zu dieser Servicefamilie gehören.

   a. Wählen Sie unter **Selected tag categories** (Ausgewählte Tag-Kategorien) die entsprechende Tag-Kategorie aus der Liste der Tag-Kategorien aus, die Sie zuvor definiert haben.

   b. **Wahlweise:** Fügen Sie den Tag-Wert hinzu, um den Zuordnungsprozess zu präzisieren, z. B. „Produktion“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie für mehrere Tag-Werte Kommas als Trennzeichen: Staging, Produktion

c. Wahlweise: Zum Ändern der standardmäßigen Service-Namenskonvention legen Sie die Reihenfolge fest, in der von Service-Mapping die Tag-Werte im Kandidatennamen verwendet werden.
Beispiel: Die erste Kategorie der Servicefamilie ist „Umgebung“, und die zweite Kategorie ist „Anwendung“. Der Standardservicename, der dem Servicekandidaten von Service-Mapping zugewiesen wird, ist „Produktion::Finanzen“. Damit der Wert der Anwendungskategorie von Service-Mapping am Anfang des Namens verwendet wird, legen Sie den Wert für die Reihenfolge der Anwendungskategorie auf 1 fest.

d. Wahlweise: Wählen Sie andere Tag-Kategorien nach Bedarf für diese Servicefamilie aus.
Die maximal zulässige Anzahl von Kategorien pro Servicefamilie beträgt drei.

6. Klicken Sie auf **View service candidates** (Servicekandidaten anzeigen).
7. Überprüfen Sie im Servicekandidatenfenster die vorgeschlagenen Servicekandidaten, und wählen Sie diejenigen aus, die Sie zuordnen möchten.
Wenn es keine Servicekandidaten gibt, stellen Sie sicher, dass in der Tabelle „Schlüsselwert“ [cmdb_key_value] für die von Ihnen für die Zuordnung verwendeten Tag-Schlüssel entsprechende Tag-Werte vorhanden sind.
8. Klicken Sie auf **Ausgewählte zuordnen**.

Service-Mapping Erstellt Serviceinstanzen basierend auf den von Ihnen ausgewählten Kandidaten.

Wenn ein Fehler bezüglich des im System vorhandenen Servicenamens vorliegt, korrigieren Sie den Namen des Kandidaten, indem Sie die folgenden Schritte ausführen:

a. Klicken Sie auf **View service candidates** (Servicekandidaten anzeigen).

b. Klicken Sie auf den vorhandenen Namen, und ändern Sie ihn.

c. Klicken Sie **OK**, um die Änderung zu speichern.

d. Zeigen Sie die Servicekandidaten an, und ordnen Sie die relevanten zu.

Neue Kandidaten enthalten nur die Serviceinstanz-CIs als Einstiegspunkte. Von dem geplanten Auftrag „Berechnete Services ausfüllen“ werden einmal täglich neue Tag-basierte Services zugeordnet.

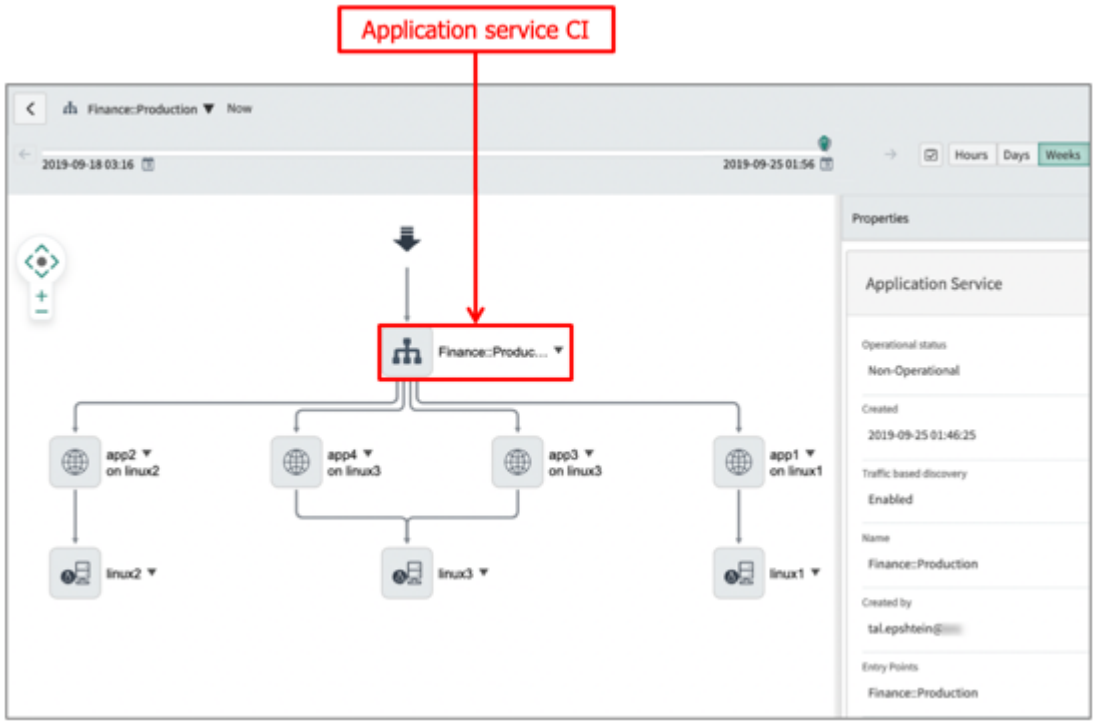
9. **Wahlweise:** So ordnen Sie einen neuen Serviceinstanz sofort zu, ohne auf das Ausfüllen des geplanten Auftrags zu warten:
   a. Wählen Sie den entsprechenden Serviceinstanz aus.
   b. Klicken Sie im Serviceinstanz -Formular links auf **Zusätzliche Informationen**.
   c. Klicken Sie unter **Zugehörige Links**auf **Service neu berechnen**.
   d. Klicken Sie oben im Formular auf **Karte anzeigen**, und überprüfen Sie das Zuordnungsergebnis.
10. Nachdem die geplante Aufgabe alle neuen Tag-basierten Services zugeordnet hat, navigieren Sie zur entsprechenden Tag-basierten Servicefamilie, und überprüfen Sie die neu zugeordneten Services, die unter **Zugeordnete Services** aufgeführt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Alle Tag-basierten Serviceinstanzen haben ihre jeweiligen Serviceinstanz-CIs als Einstiegspunkte.

Die Zuordnung für die Instanz „Finance::Production“ basierend auf Tags



Nächste Maßnahme

1. Nachdem die geplante Aufgabe alle neuen Tag-basierten Services zugeordnet hat, navigieren Sie zur entsprechenden Tag-basierten Servicefamilie, und überprüfen Sie die neu zugeordneten Services, die unter **Zugeordnete Services** aufgeführt sind.
2. Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind: Die folgende Discovery-Nachricht wird in einer Tag-basierten Serviceinstanz angezeigt: *`This tag-based service instance reached the maximum number of CIs. For more information, refer to the product documentation.`*

   Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:

   - Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen Um sicherzustellen Service-Mapping Schließt nur relevante CIs in der Serviceinstanz ein.
   - Falls erforderlich, Tag-basierte Discovery-Konfiguration Um zu ändern, welche CIs Service-Mapping Enthält in Tag-basierten Serviceinstanzen.
3. Um die tagbasierten Services feinzutunen oder zu korrigieren, ändern Sie die Tag-Kategorien, die Sie für die Servicefamilie verwendet haben.

> **Wichtig:** Im Kartenfenster werden Zuordnungen für Tag-basierte und dynamische Services nur im Ansichtsmodus angezeigt. Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Zugehörige Informationen

Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen

Tag-basierte Discovery-Konfiguration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnung von Anwendungsservices basierend auf Tags vorbereiten

Analysieren, überprüfen und definieren Sie Tags in Ihrer Organisation für eine erfolgreiche Zuordnung.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie zur Vorbereitung auf die Tag-basierte Zuordnung Tag-Kategorien, die Tags mit ähnlicher Verwendung enthalten.

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

Definieren Sie eine Tag-basierte Servicefamilie und Tags, die Sie für die Service-Mapping-Zuordnung verwenden möchten. Basierend auf den Tag-Definitionen für die Tag-basierte Servicefamilie, Service-Mapping Erstellt Servicekandidaten: Vorgeschlagene Serviceinstanzen. Sie überprüfen die Kandidaten und entscheiden, welche Sie zum Erstellen der tatsächlichen Tag-basierten Serviceinstanzen verwenden möchten. Details zum Tag-basierten Prozess finden Sie unter Tag-basierte Discovery in Service-Mapping.

CIs, die Tag-Werte für die von Ihnen ausgewählten Tag-Kategorien erkannt haben, werden Teil der Anwendungsservices. Service-Mapping erstellt einen separaten Servicekandidaten für jede Tag-Wert-Kombination. Wenn Sie die Kriterien einschränken, indem Sie zusätzlich zu Tag-Kategorien Tag-Werte definieren, ordnet Service-Mapping nur CIs zu, die die entsprechenden Werte aufweisen. CIs, denen mehr als ein Tag zugewiesen sind, können Teil mehrerer Services sein. Sie können eine Tag-Kategorie für Tags erstellen, die sich auf verschiedene Arten von Umgebungen beziehen, wenn Ihre Organisation die Tag-Werte „production“ und „staging“ verwendet. Bei der Tag-basierten Zuordnung wird nicht zwischen Groß- und Kleinschreibung unterschieden. Gleiche Schlüsselnamen und Schlüsselwerte mit Groß- und Kleinschreibung werden als identisch identifiziert.

Hinweis: Service-Mapping enthält CIs, die Teil von CI-Beziehungen sind, auch wenn diesen CIs keine Tags zugewiesen sind. Weitere Informationen finden Sie unter Tag-basierte Discovery in Service-Mapping.

Prozedur

1. Analysieren Sie die Tag-Nutzung in Ihrer Organisation, und erstellen Sie eine Liste aller Tags und ihrer Zwecke. Verwenden Sie die Schlüsselwerttabelle [cmdb_key_value], um die Tags in der CMDB anzuzeigen.

   Verwenden Tag-Governance Dient zum Analysieren und Optimieren der Tag-Anwendung in Ihrer Organisation. Weitere Informationen finden Sie unter Tag-Governance.

2. Falls erforderlich, weisen Sie CIs Tags zu, die Sie in Anwendungsservices aufnehmen möchten.

   Vermeiden Sie es, sehr große Anwendungsservices zu erstellen, die mehr als 5000 CI-Beziehungen enthalten. Derart große Anwendungsservices können zu Leistungsproblemen führen.

3. Erstellen und definieren Sie Tag-Kategorien, die Sie möchten Service-Mapping Zur Verwendung für die Zuordnung von Serviceinstanzen.

   Um beispielsweise alle Serviceinstanzen zuzuordnen, die Ihre Organisation in der Produktionsumgebung in der EMEA-Region verwendet, erstellen Sie die folgenden Tag-Kategorien: Anwendungen, EMEA-Region und Produktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Service-Mapping** > **Administration** > **CI-Tag-Kategorien**an.

b. Wählen Sie eine zu ändernde **CI-Tag-Kategorie** aus, oder wählen Sie **Neu**.

c. Definieren Sie den Tag-Kategorienamen, z. B. *Environment*.

d. Doppelklicken Sie unter **CI tag keys** (CI-Tag-Schlüssel) auf die Zeile, und geben Sie den Tag-Schlüssel ein, z. B. *Env*.

Da bei der tagbasierten Zuordnung Groß-/Kleinschreibung nicht berücksichtigt wird, werden Tag-Schlüssel-Varianten mit anderer Kapitalisierung, wie *Env*, *env* oder *ENV*, ebenfalls dieser Tag-Kategorie zugewiesen.

Wiederholen Sie diesen Schritt, bis Sie alle Tag-Schlüssel-Varianten hinzugefügt haben, die Ihre Organisation für denselben Zweck verwendet, z. B. *Env* und *Environment*.

Hinweis: Detaillierte Beispiele für die Definition von Tag-basierten Zuordnungskriterien für Servicefamilien finden Sie unter Beispieldefinitionen für Servicefamilien in Tag-basierter Zuordnung.

4. Führen Sie Discovery aus, um CIs horizontal zu erkennen. Discovery befüllt die CMDB mit den CI-Daten einschließlich Tags.

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Ordnen Sie mehrere Anwendungsservices aus einer CSV-Datei zu Verwenden klassisch Service-Mapping

Diese Methode ist für Sie geeignet, wenn Ihre Organisation organisationsübergreifende Zuordnungen und Analysen durchgeführt und einige Informationen zu geplanten Serviceinstanzen gesammelt hat. In diesem Fall können Sie die gesammelten Informationen in einer bestimmten Reihenfolge organisieren und als CSV-Datei speichern. Service-Mapping Extrahiert Informationen aus dieser Datei und erstellt potenzielle Serviceinstanzen, die als Servicekandidaten bezeichnet werden.

Vorbereitungen

Führen Sie das unter Eine CSV-Datei für die Zuordnung der Kandidaten vorbereiten beschriebene Verfahren aus.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen haben Service-Mapping Aktiviert zum Zuordnen oder Überprüfen von Serviceinstanzen.

Bei Bedarf können Sie Servicekandidaten aus mehreren CSV-Dateien importieren.

Beim erneuten Importieren von Serviceinstanz -Kandidaten importiert Service-Mapping keine Kandidaten, die Sie zuvor ignoriert haben.

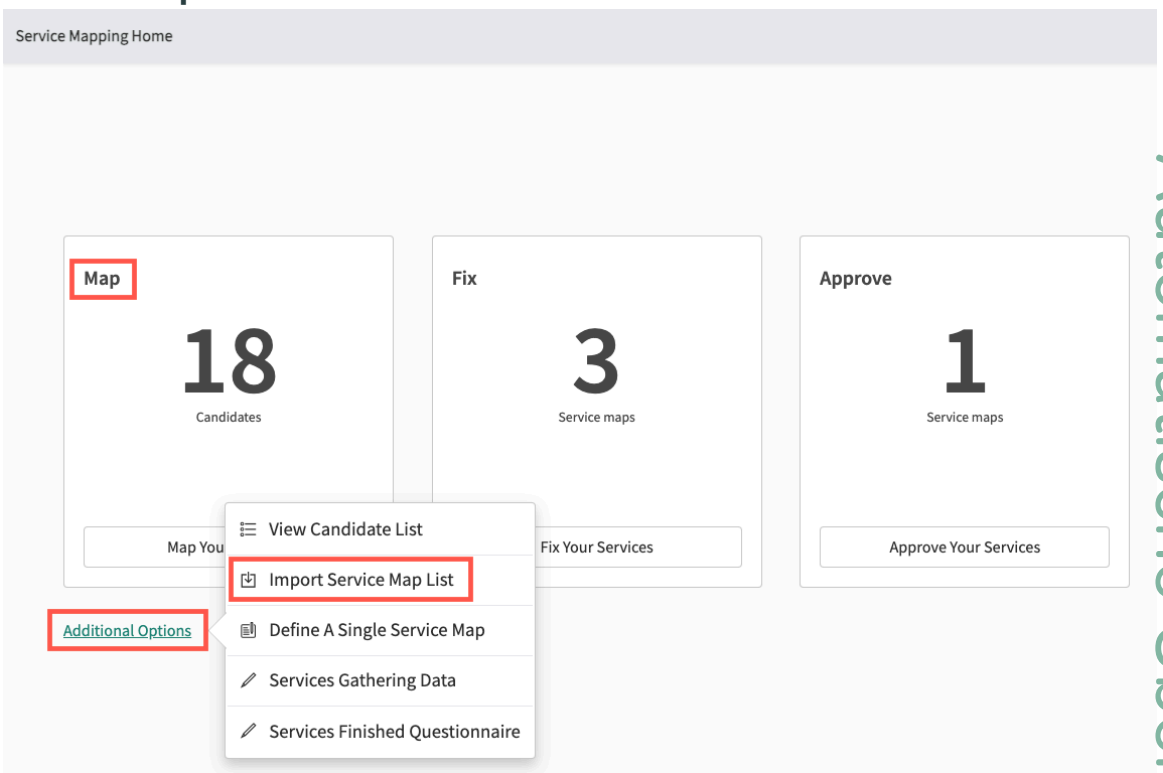
Nach Service-Mapping Erkennt zum ersten Mal Konfigurationselemente (Configuration Items, CIs), die zu Ihrer Serviceinstanz gehören, und erkennt dann CIs erneut, um Änderungen und Updates zu finden. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.
2. Unter **Zuordnung** Kachel auswählen **Zusätzliche Optionen** .
3. Wählen Sie Aus **Importieren Sie Die Servicezuordnungsliste** .

Zusätzliche Optionen für Kartenkachel



4. Wählen Sie im Fenster CSV-Datei importieren die Option aus **Wählen Sie die Datei aus** .
5. Navigieren Sie zur CSV-Datei, die für den Import verwendet werden soll, und wählen Sie aus **Öffnen** .
6. Wählen Sie **Importieren**.
   Die importierten Serviceinstanz -Kandidaten werden der Kandidatenliste hinzugefügt.
7. Überprüfen Sie, ob sich die Gesamtzahl der Service-Kandidaten auf der Kachel **Karte** um die erwartete Anzahl erhöht hat.
8. Auf der **Zuordnung** Kachel auswählen **Ordnen Sie Ihre Services Zu** Dient zum Erstellen von Anwendungsservices aus den Kandidaten, die Sie aus der CSV-Datei importiert haben.

Nächste Maßnahme

- Überprüfen Sie die Liste der erstellten Anwendungsservices. Wenn Service-Mapping Anwendungsservices bei der Stapelzuordnung nicht wie erwartet erstellt hat, müssen Sie sie, wie in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping beschrieben, manuell erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Reparieren Sie die Anwendungsservices, die mit Fehlern erkannt wurden. Weitere Informationen finden Sie unter Fehler bei Anwendungsservices als Massenvorgang beheben.
- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.

Eine CSV-Datei für die Zuordnung der Kandidaten vorbereiten

Organisieren Sie Informationen zu potenziellen Anwendungsservices (Kandidaten) in Ihrer Organisation und speichern Sie sie in einer CSV-Datei.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Erstellen Sie eine XLSX-Datei.
2. Definieren Sie Einstiegspunktattribute für die Servicekandidaten in der XLSX-Datei.
   Kunden verwenden diese Einstiegspunkte für den Zugriff auf Services. Beispielsweise verwenden sie http://www.google.com:8080, um auf die Google-Seite zuzugreifen.

Warnung: Die Spaltenreihenfolge in der XLSX-Datei muss beibehalten werden. Die Eingabe von Attributen in falschen Spalten verursacht Zuordnungsfehler.

Spalte	Beschreibung
A	Geben Sie einen eindeutigen Namen für den geplanten Serviceinstanz ein. Zum Beispiel„ NY Public Library” oder „Google”. **Warnung:** Service-Mapping importiert nur Anwendungsservices mit eindeutigen Namen. Wenn in den von Ihnen verwendeten CSV-Dateien mehrere Einträge mit demselben Namen vorhanden sind, überschreibt der zuletzt importierte Datensatz die vorherigen.
B	(Optional) Wenn Sie die URL kennen, die als Einstiegspunkt zu Ihrem Serviceinstanz dient, geben Sie sie in diese Spalte ein. Geben Sie beispielsweise„ https://www.nypl.org/” oder „www.google.com:8080” ein. **Warnung:** Wenn Sie die URL definieren, müssen Sie die IP-Adresse, den Port, den FQDN und das Protokoll nicht definieren. Service-Mapping analysiert die URL, um die IP-Adresse, den Port und den FQDN zu extrahieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Wenn keine URL vorhanden ist, die als Einstiegspunkt dient, definieren Sie andere Parameter in den Spalten C und E.
C	(Optional) Die IP-Adresse des Einstiegspunkts im IPv4-Format. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben.
D	(Optional) Der Port des Einstiegspunkts. Beispiel: „8080“ für die Google-Seite. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben. Wenn Sie weder URL noch Port angegeben haben, verwendet Service-Mapping Port 80 für das HTTP-Protokoll und Port 443 für das HTTPS-Protokoll.
E	(Optional) Der FQDN des Serviceeinstiegspunkts, z. B. „www.google.com“ für Google. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben.

3. Speichern Sie die Datei auf einem Laufwerk, auf das Sie während des Imports zugreifen können, mit der Erweiterung `.csv`.

Nächste Maßnahme

Ordnen Sie mehrere Anwendungsservices aus einer CSV-Datei zu Verwenden klassisch Service-Mapping

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

Neben der Stapelzuordnung von Anwendungsservices können Sie individuelle, einzelne Anwendungsservices zuordnen, indem Sie Attribute für jeden Anwendungsservice definieren. Verwenden Sie diese Zuordnungsmethode, wenn Sie bereits Details zum Anwendungsservice kennen oder planen. Service-Mapping muss zum Zuordnen oder Überprüfen von Anwendungsservices aktiviert sein.

Vorbereitungen

- Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist.
- Wenn der Serviceinstanz auf PaaS aufbaut, das von Microsoft Azure oder Amazon Web Services unterstützt wird, wählen Sie im Servicekonto der Cloud zuerst Rechenzentren erkennen und erstellen Sie dann horizontale Erkennungszeitpläne.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zur Stapelzuordnung, die für die Zuordnung mehrerer Anwendungsservices sehr effektiv, aber nicht besonders präzise ist, können Sie auch einzelne Anwendungsservices zuordnen. Möglicherweise müssen Sie Anwendungsservices, die bei der Stapelzuordnung ausgelassen wurden, individuell zuordnen.

Das wichtigste Attribut, das Sie zur Erkennung eines Anwendungsservice kennen und konfigurieren müssen, ist ein Einstiegspunkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Normalerweise ist dies entweder eine URL oder eine Kombination aus IP-Adresse und Port. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre Instanz des E-Mail-Services zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

Einstiegspunkte variieren je nach Art von Serviceinstanz . Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken.

Zusätzlich zu Einstiegspunkten, die Service-Mapping erkennen kann, können Sie Einstiegspunkte hinzufügen, die Service-Mapping nicht erkennen kann. Sie können einen solchen Einstiegspunkt als Hinweis darauf hinzufügen, dass Ihr Serviceinstanz ein Gerät oder eine Anwendung enthält.

Außerdem müssen Sie einen Eigentümer für den Serviceinstanz definieren. Der Besitzer der Serviceinstanz ist ein Anwender, der mit der Infrastruktur und den Anwendungen des Service vertraut ist. Dieser Anwender ist der Serviceinstanz-SME, der Informationen bereitstellt, die für eine erfolgreiche Erstellung einer Serviceinstanz erforderlich sind. Wenn ein Service zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor.

Nach Service-Mapping Erkennt zum ersten Mal Konfigurationselemente (Configuration Items, CIs), die zu Ihrer Serviceinstanz gehören, und erkennt dann CIs erneut, um Änderungen und Updates zu finden. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden.

Alle Serviceinstanzen, sowohl manuell erstellt als auch erkannt von Service-Mapping, Werden in der Tabelle „zugeordnete Serviceinstanz“ [cmdb_ci_Service_detected] gespeichert.

Sie können einen einzelnen Anwendungsservice auch manuell erstellen, indem Sie den Flow basierend auf Gemeinsames Servicedatenmodell verwenden. Mit Gemeinsames Servicedatenmodell (CSDM) können Sie Servicetypen und Serviceangebote optimieren. Sie können Beziehungen zwischen Anwendungsservices und anderen servicebezogenen Objekten in CSDM hinzufügen: Geschäftsanwendung, technische Serviceangebote oder Business Service-Angebote. Weitere Informationen finden Sie unter Erstellen Sie Anwendungsservices .

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.
2. Klicken Sie unter der Kachel **Zuordnen** auf **Zusätzliche Optionen**.
3. Klicken Sie auf **Einzelne Servicezuordnung definieren**.
4. Definieren Sie die grundlegenden Serviceinstanz -Attribute:

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Anwendungsservicenamen ein, der nicht von einem anderen Anwendungsservice verwendet wird. Verwenden Sie selbsterklärende Namen wie Mailservice Oder Druckservice .
Besitzer	Wählen Sie einen Besitzer aus, der für diese Serviceinstanz in der Organisation verantwortlich ist. Wenn der Besitzername nicht in der Liste angezeigt wird, erstellen Sie einen Benutzer für diese Person, und weisen Sie diesem Benutzer die Rolle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sm_app_owner zu. Alternativ können Sie einen Anwender mit der Rolle „Service_Mapping_admin“ auswählen.

5. Wenn Sie die Einstiegspunkte nicht kennen, fordern Sie sie wie unter Informationen zu Einstiegspunkten für Anwendungsservices anfordern beschrieben vom Eigentümer des Serviceinstanz an:
6. Führen Sie die folgenden Schritte aus, um einen Einstiegspunkt hinzuzufügen, den Service-Mapping erkennen kann.
   a. Klicken Sie auf **Erkennbar nach Servicezuordnung**.
   Die Seite bietet Kacheln für Anwendungen, die am häufigsten für Einstiegspunkte verwendet werden.
   b. Klicken Sie auf die Kachel, die der Anwendung entspricht, zu der der Einstiegspunkt gehört.
   Beispiel: **Webanwendung**, wenn Sie einen Serviceinstanz mit einer Webschnittstelle erstellen. Wenn die Kacheln die erforderliche Anwendung nicht enthalten, klicken Sie auf **Weitere Typen anzeigen**, um eine Auswahl aus der Liste aller vorkonfigurierten Einstiegspunkttypen zu treffen.

   > **Wichtig:** Verwenden Sie keine zentralen IT-Komponenten wie Microsoft MQ oder Microsoft Active Directory als Einstiegspunkte. Durch die Verwendung solcher Einstiegspunkte werden große Services erstellt, die Leistungsprobleme bei der Zuordnung und Überwachung verursachen.

   c. **Wahlweise:** Wenn der erforderliche Einstiegspunkttyp nicht in der Liste angezeigt wird, müssen Sie ihn möglicherweise wie in Einstiegspunkttypen für Service-Mapping erstellen beschrieben erstellen.
   d. Konfigurieren Sie Attribute für den Einstiegspunkt, wie in Einstiegspunktattribute beschrieben. Einstiegspunktattribute hängen vom ausgewählten Typ ab.
   e. Klicken Sie auf **Hinzufügen**.
   Der Einstiegspunkt wird unter **Einstiegspunkte** hinzugefügt.
   f. Zum Hinzufügen weiterer Einstiegspunkte klicken Sie auf **Einstiegspunkt hinzufügen** und wiederholen Schritt 6.
7. **Wahlweise:** Führen Sie die folgenden Schritte aus, um einen statischen Einstiegspunkt hinzuzufügen, den Service-Mapping nicht erkennen kann.
   a. Klicken Sie auf **Manuell erstellt**.
   b. Definieren Sie das CI, das als Einstiegspunkt dienen soll.

Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. `cmdb_ci_appl` für Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.

c. Klicken Sie auf **Absenden**.

8. Klicken Sie auf **Speichern** oder **Aktualisieren**, um alle von Ihnen bis zu diesem Zeitpunkt definierte Attribute zu speichern und weiter Attribute für diesen Serviceinstanz zu konfigurieren.
Service-Mapping speichert den neuen Serviceinstanz in der Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered]. Außerdem wird im Hintergrund der Erkennungsprozess gestartet.

9. Um Definitionen zu speichern, führen Sie eine Erkennung dieses Serviceinstanz durch, navigieren Sie zur Zuordnung für diesen Serviceinstanz , und klicken Sie auf **Karte anzeigen**.
Service-Mapping startet den Erkennungsprozess. Die Seite mit der Zuordnung für diesen Serviceinstanz wird geöffnet und zeigt die gerade stattfindende Zuordnung an. Der Serviceinstanz -Status wird auf „In Bearbeitung“ geändert.

Nächste Maßnahme

- Wenn Service-Mapping den Serviceinstanz mit Fehlern erkennt, beheben Sie Fehler in einzelnen Anwendungsservices mithilfe von Erkennungsmeldungen.
- Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:
  - Service-Mapping Bietet nicht an, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
  - Es gibt keine Discovery-Nachricht, die darauf hinweist, dass die Serviceinstanz zu groß ist: *`The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.`*

  Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:
  - Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen.
  - Teilen Sie den Service in kleinere Services auf.
- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.

Informationen zu Einstiegspunkten für Anwendungsservices anfordern

Das wichtigste Attribut, das Sie zur Erkennung eines Serviceinstanz kennen und konfigurieren müssen, ist ein Einstiegspunkt. Wenn Sie die Einstiegspunkte für den Serviceinstanz nicht kennen, fordern Sie sie vom Eigentümer des Serviceinstanz an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Das Anfordern von Informationen zu Einstiegspunkten ist ein optionaler Teil der Zuordnung eines einzelnen Anwendungsservice.

Erforderliche Rollen: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Normalerweise ist dies entweder eine URL oder eine Kombination aus IP-Adresse und Port. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre Instanz des E-Mail-Services zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

Einstiegspunkte variieren je nach Art von Serviceinstanz . Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken.

Prozedur

1. Klicken Sie auf den Link **Daten anfordern**.
   Das Fenster „Anforderung von Daten“ wird geöffnet.
2. Wenn die Liste **Zugewiesen an** leer ist, wählen Sie den Namen des Verantwortlichen für den Serviceinstanz aus.
3. Geben Sie Ihre Fragen zu Serviceinstanz in das Feld **Beschreibung** ein.
   Beispielsweise können Sie nach den Einstiegspunkten fragen.
4. Klicken Sie auf **Absenden**.
   Das System öffnet die Aufgabe ServiceNow für den Eigentümer und sendet automatisch eine E-Mail-Benachrichtigung.
5. Überprüfen Sie die Informationen, die der Eigentümer auf den Registerkarten **Andere Eingabepunkte** und **Komponenten** hinzugefügt hat.
   Sobald der Besitzer fehlende Informationen bereitstellt, erhalten Sie eine E-Mail-Benachrichtigung.
6. Klicken Sie auf den Link in der E-Mail, um den Fragebogen für den entsprechenden Serviceinstanz zu öffnen.
7. Setzen Sie die Zuordnung eines einzelnen Anwendungsservice fort.

Geben Sie Einstiegspunkte für die Zuordnung eines Anwendungsservice an

Als Anwendungsservice-Eigentümer erhalten Sie in einer E-Mail-Benachrichtigung möglicherweise eine Anforderung, Informationen zu den Einstiegspunkten bereitzustellen. Stellen Sie Informationen zu Einstiegspunkten bereit, damit Administratoren die Erkennung eines Anwendungsservice starten können.

Vorbereitungen

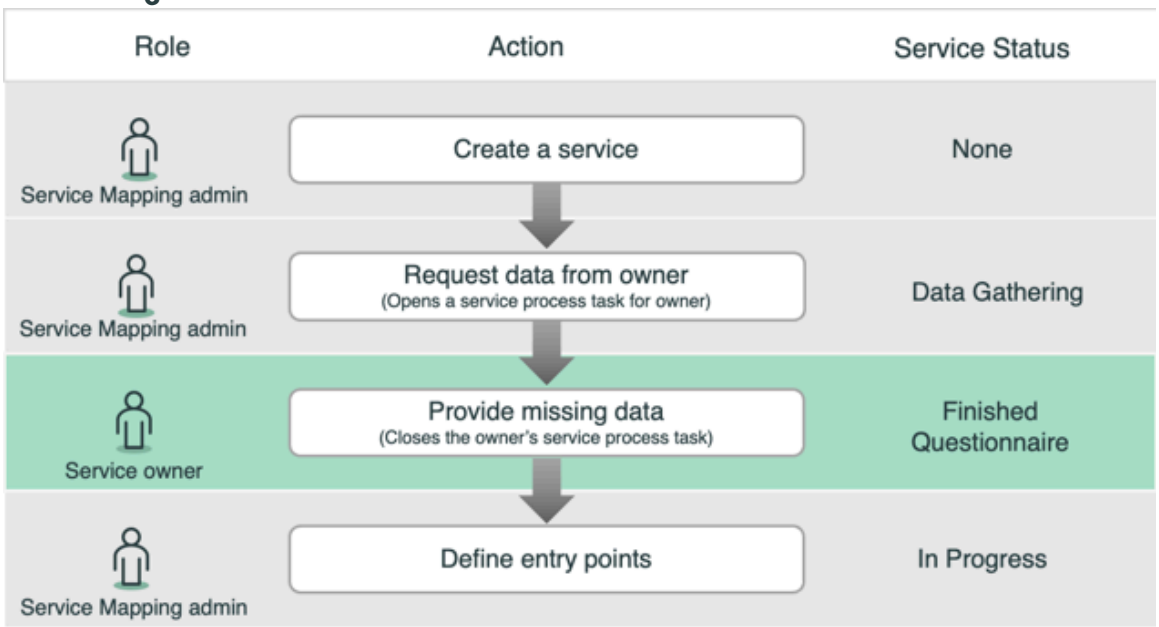
Erforderliche Rolle: sm_App_owner oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Informationen zu den Serviceinstanz -Einstiegspunkten fehlen, kann ein Administrator die Zuordnung des Serviceinstanz s nicht starten. In diesem Fall sendet der Administrator eine Anforderung für fehlende Daten aus dem Serviceinstanz -Formular, wodurch eine Serviceprozessaufgabe erstellt und Ihnen zugewiesen wird. Sie erhalten eine E-Mail-Benachrichtigung mit dem Link zur Fragebogenseite, auf der Sie die fehlenden Daten eingeben müssen. Die wichtigsten Informationen beziehen sich auf die Einstiegspunkte, jedoch sind zusätzliche Daten über Anwendungsservicekomponenten, deren Verbindungen oder Verwendung für den Administrator hilfreich. Wenn Sie die Dateneingabe abgeschlossen und den Fragebogen übermittelt haben, schließt das System die Serviceprozessaufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservice-Flows zuordnen



Prozedur

1. Klicken Sie auf den Link in der Benachrichtigungs-E-Mail, um auf die Seite **Fragebogen** zuzugreifen.
2. Sie können die Seite **Fragebogen** auch in der Liste der Ihnen zugewiesenen Aufgaben öffnen.
   a. Navigieren zu **Service-Mapping** > **Administration** > **Meine Aufgaben**an.
   b. **Wahlweise:** Sortieren Sie die Liste der Serviceprozessaufgaben nach Bedarf.
   c. Klicken Sie auf die erforderliche Aufgabe.
   d. Klicken Sie auf den Formularlink des Serviceinstanz .
   e. Klicken Sie im linken Bereich auf **Fragebogen**.
3. Geben Sie auf der Registerkarte **Geplante benutzerdefinierte Einstiegspunkte** Informationen zu den Serviceinstanz -Einstiegspunkten ein.

Hinweis:

Wenn Sie die genauen Attribute der Einstiegspunkte, wie z. B. die URL oder die IP-Adresse, nicht angeben können, fügen Sie allgemeine Informationen hinzu, die den Administrator leiten können. Beispielsweise den Typ der Anwendung wie Tomcat-Server.

4. Um Informationen zu anderen Komponenten hinzuzufügen, die diesen Serviceinstanz enthalten, klicken Sie auf die Registerkarte **Komponenten** und geben die entsprechenden Daten ein.
5. Wenn Sie mit der Eingabe der Informationen fertig sind, klicken Sie auf **Aktionen** und anschließend auf **Fragebogen senden**.
   Die Ihnen zugewiesene Datenanforderungsaufgabe wird geschlossen. Der Serviceinstanz -Status wird auf „In Bearbeitung“ geändert.
6. Wenn es weitere hilfreiche Informationen zu diesem Serviceinstanz gibt, geben Sie diese im Feld **Hinweise** unter **Arbeitsnotizen** ein, und drücken die Eingabetaste, um Ihren Kommentar zu veröffentlichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Wenn Discovery auf basiert Predictive Intelligence Ist aktiviert, enthalten neu zugeordnete Anwendungsservices nur Konfigurationselemente (Configuration Items, CIs) und CI-Verbindungen, die mithilfe von Discovery-Mustern hinzugefügt wurden. Verwenden Sie die von generierten Vorschläge für CI-Verbindungen Service-Mapping, Um den Anwendungsservice abzuschließen.

Vorbereitungen

- Bestätigen Sie, dass die auf Fingerabdrücken basierende Discovery aktiviert bleibt, da sie standardmäßig aktiviert ist. Navigieren Sie zum Überprüfen zu **Alle** > **System Eigenschaft S** > **Alle Eigenschaften**an. Überprüfen Sie, ob `sys_property process.clustering.appfingerprint.enabled`Eigenschaft wird nicht in der Liste angezeigt.
- Bestätigen Sie diese Discovery basierend auf Predictive Intelligence Ist aktiviert. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob `sa_ml.connection_suggestions.active`Eigenschaft ist auf festgelegt **Wahr** .

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Discovery auf basiert Predictive Intelligence Ist aktiviert, Service-Mapping Fügt automatisch Verbindungen zu Serviceinstanzen basierend auf Verbindungsregeln hinzu. Diese Vorschläge werden aus verkehrsbezogenen Daten in generiert Configuration Management Database (CMDB) Und eine Analyse von Fingerabdrücken, CIs und Prozessen der Anwendung. Predictive Intelligence Wertet die Relevanz dieser Verbindungen aus, und Service-Mapping Verwendet dann diese Informationen, um Verbindungen zu erstellen und Vorschläge für bereitzustellen Server und Lastenausgleichsmodule . Dann können Sie entscheiden, welche Verbindungen hinzugefügt oder aus Serviceinstanzen entfernt werden sollen. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wichtig: Mithilfe von Verbindungsvorschlägen können Sie CIs nur in Bezug auf von Service-Mapping erkannte Anwendungsservices hinzufügen oder entfernen.

Prozedur

1. **Wahlweise:** Zeigen Sie Informationen zu allen Anwendungs-CIs in Verbindungsvorschlägen an. Weitere Informationen finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.

   Wichtig: Wenn Sie keine auf Fingerabdrücken basierende Discovery verwenden, werden einige Anwendungs-CIs möglicherweise als generische Anwendungen zugeordnet, ohne spezifische Identifizierungen oder detaillierte Informationen.

2. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
3. Auswahlvorgang **Vorschläge** > **Verbindungsvorschläge** Oben in der Karte, um Vorschläge für den gesamten Anwendungsservice anzuzeigen.
   Klicken Sie alternativ mit der rechten Maustaste auf ein CI, für das Sie Verbindungsvorschläge anzeigen möchten, und wählen Sie **Verbindungsvorschläge anzeigen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Überprüfen Sie die Vorschlagsdetails unter Berücksichtigung der Parameter, die in der Liste „Verbindungsvorschläge“ abgedeckt sind.
   Weitere Informationen finden Sie unter Liste „Verbindungsvorschlagen“.
5. **Wahlweise:** Wenn keine Anwendungs-CIs erkannt wurden, ermitteln Sie ein eigenständiges CI der Anwendungsklasse basierend auf Fingerabdrücken:

   a. Wählen Sie aus **Vorschau** Symbol Neben dem relevanten Vorschlag basierend auf den Fingerabdrücken der Anwendung (AFP).
   In der daraufhin geöffneten Liste „Verbindungsvorschlag“ werden Details zum betreffenden Vorschlag angezeigt.

   b. Wählen Sie aus **Vorschau dieses Datensatzes anzeigen** Symbol neben **Ziel-AFP** , Und wählen Sie dann aus **Öffnen Sie Den Datensatz** .

   c. Wählen Sie Aus **Anwendung Erkennen** .

   d. Wählen Sie Aus **Aktualisieren** Im Fenster vorgeschlagene Verbindungen überprüfen, um sicherzustellen, dass die angezeigten Informationen die erkannten CI-Klassen widerspiegeln.

6. Aktivieren Sie die Kontrollkästchen neben den relevanten Vorschlägen, und klicken Sie auf die Aktionsschaltfläche am unteren Rand des Fensters:

Aktion	Ergebnis
Hinzufügen	Service-Mapping Enthält sowohl die Verbindungen als auch die CIs, zu denen diese Verbindungen führen, wodurch sie Teil der Serviceinstanz werden. Der `Decision`-Wert für hinzugefügte Verbindungen ändert sich in **Manuell hinzugefügt**.
Ausschließen	Service-Mapping Schließt Verbindungen und die CIs aus, zu denen sie führen, aus der Serviceinstanz aus. Der `Decision`-Wert für entfernte Verbindungen ändert sich in **Manuell ausgeschlossen**.
Zurücksetzen	Service-Mapping Kehrt frühere Entscheidungen zurück, unabhängig davon, ob sie manuell oder per Regel getroffen wurden. Der Wert `Decision` für zurückgesetzte Verbindungen ändern sich in **Unentschieden**. Diese Aktion ist nur relevant, wenn Sie bereits Verbindungsvorschläge zum Abschließen dieser Serviceinstanz verwendet haben.

7. Wählen Sie Aus **Schließen** Um das Fenster „vorgeschlagene Verbindungen überprüfen“ zu verlassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Die Anwendungsservicezuordnung spiegelt die von Ihnen vorgenommenen Änderungen wider. Die von Ihnen hinzugefügten Verbindungen werden zusammen mit den CIs, zu denen sie führen, auf der Karte angezeigt.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung in Service-Mapping

CIs für einzelne Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

Erstellen Sie Regeln für das automatische Hinzufügen von verkehrsbasierten Verbindungen und CIs, zu denen sie in erkannten Serviceinstanzen führen. Fügen Sie mithilfe von Verbindungsregeln CIs für bestimmte Anwendungsservices hinzu.

Vorbereitungen

- Analysieren Sie die Infrastruktur, die Sie zuordnen, um die häufigsten Verbindungen zu identifizieren. Diese gängigen Verbindungen sind gute Kandidaten für Verbindungsregeln.
- Bestätigen Sie diese Discovery basierend auf Predictive Intelligence Ist aktiviert.
  Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob `sa_ml.connection_suggestions.active`Eigenschaft ist auf festgelegt **Wahr** .
- Anwendungen basierend auf Fingerabdrücken erkennen.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

Sie können Verbindungsregeln erstellen, die für bestimmte Anwendungsservices oder für alle Anwendungsservices gelten. Wenn die Regel für einen bestimmten Service gilt, die Regelbedingung jedoch auf ein CI verweist, das Teil mehrerer Services ist, fügt Service-Mapping dieses CI allen relevanten Services hinzu.

Weitere Informationen über die Bewertung und Anwendung von Verbindungsregeln mit Service-Mapping finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Neben Verbindungsregeln, die bestimmten Services CIs hinzufügen, können Sie Regeln zum Hinzufügen von CIs zu mehreren Anwendungsservices erstellen.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsregeln**an.
   Alternativ wählen Sie in einer Serviceanwendungszuordnung die Option aus **Vorschläge** > **Lokale Regeln**an.
2. Erstellen Sie eine neue Verbindungsregel, indem Sie auf **Neu** klicken.
   Alternativ können Sie eine vorhandene Regel anpassen, indem Sie in der Liste auf den Namen der Regeln klicken.
3. Wählen Sie **Aktiv** aus, um mit der Verwendung dieser Verbindungsregel zu beginnen.
   Service-Mapping wertet nur aktive Verbindungsregeln aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Feld **Name** einen eindeutigen und aussagekräftigen Namen ein.
5. Geben Sie in das Feld **Reihenfolge** den Wert ein, den Service-Mapping für die Sequenz verwendet.
6. Konfigurieren Sie die Filterbedingung im Bereich **Bedingung**.

   a. Wählen Sie das Feld, den Operator und den Wert aus.

   Example
   Um beispielsweise ausgehende Verbindungen für einen Tomcat-Server hinzuzufügen, konfigurieren Sie die folgende Filterbedingung.

   b. Um eine zusätzliche Filterbedingung zu erstellen, klicken Sie auf **Filterbedingung hinzufügen**.

   c. Um eine zusätzliche Filterbedingung mit dem Operator ODER zu erstellen, klicken Sie auf **„ODER"-Klausel hinzufügen**.

7. Wählen Sie Lokal aus der Liste **Bereich** aus.
8. Wählen Sie in der Liste **Erkannter Anwendungsservice** einen vorhandenen Service aus, für den diese Regel gilt.
9. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme
Gehen Sie wie folgt vor, um zu prüfen, ob Service-Mapping wie erwartet CIs hinzugefügt hat:

1. Öffnen Sie die Zuordnung für den Anwendungsservice, den Sie für diese Verbindungsregel ausgewählt haben.
2. Klicken Sie oben im Kartenfenster auf **Erkennen**.
3. Nachdem der Anwendungsservice erneut erkannt wurde, überprüfen Sie, ob CIs basierend auf der Verbindungsregel korrekt hinzugefügt wurden.

Aktivieren Sie die Traffic-basierte Discovery für einen Anwendungsservice

Sorgen Sie dafür, dass Service-Mapping datenverkehrsbasierte Verbindungen verwendet, um die CIs zu erkennen, aus denen ein Anwendungsservice besteht.

Vorbereitungen
Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als Traffic-basierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Weitere Informationen dazu, wie Service-Mapping eine datenverkehrsbasierte Erkennung durchführt, finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Führen Sie in der klassischen Umgebung die folgenden Schritte aus:

   a. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.

   b. Klicken Sie auf der Kachel **Abgeschlossen** auf **Ihre Services anzeigen**.

   c. Wählen Sie den entsprechenden Anwendungsservice.

   d. Klicken Sie auf **Zusätzliche Informationen**.

   e. Aktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.

   f. Klicken Sie auf **Aktualisieren**.

2. Alternativ führen Sie die folgenden Schritte in der Mitarbeiterbereich-Benutzeroberfläche aus:

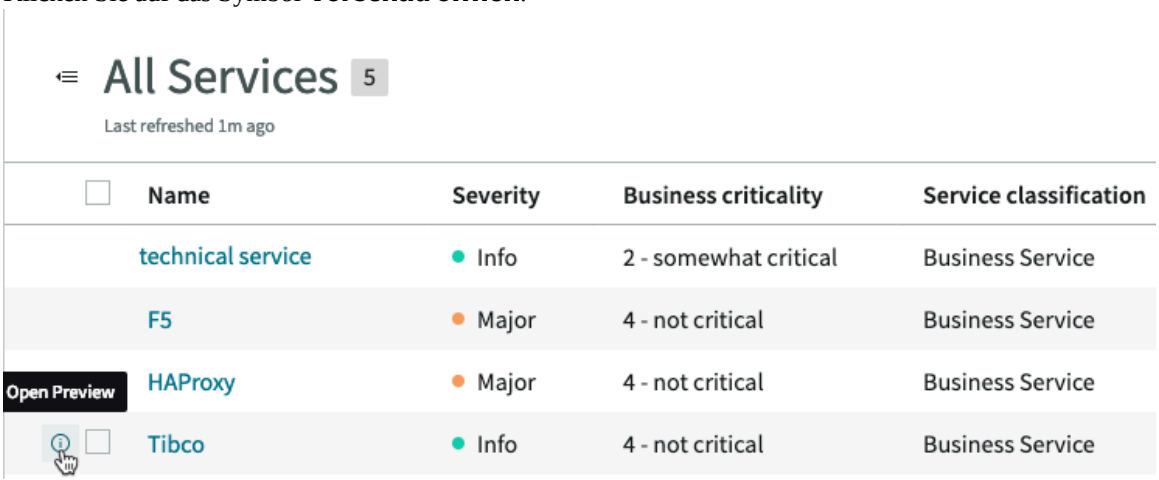
   a. Navigieren zu **Mitarbeiterbereich** > **Mitarbeiterbereich-Startseite**an.

   b. Klicken Sie im linken Bereich auf **Listen**.

   c. Navigieren zu **Services** > **Alle Services**an.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.

   d. Wählen Sie den entsprechenden Anwendungsservice.

   e. Klicken Sie auf das Symbol **Vorschau öffnen**.



   Der Detailbereich wird auf der rechten Seite geöffnet.

   f. Aktivieren Sie im Bereich „Details” das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.

   g. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservices zuordnen, die Citrix XenApp und Presentation Server enthalten

Service-Mapping kann Anwendungsservices erkennen, die Citrix XenApp, Presentation Server und Citrix Usage Collector enthalten.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Citrix XenApp-Server	Windows	6.x> 6.5, 7.x <7.6	WMI WinRM	Horizontal und von oben nach unten	Citrix XenApp- oder Präsentationsserver
Citrix Presentation Server	Windows	4.x, 5.x, 6.x <6,5	WMI WinRM	Horizontal und von oben nach unten	Citrix XenApp- oder Präsentationsserver
Citrix-Nutzungssammler	Windows	7.x> 7,5, 8.x	WMI WinRM	Von oben nach unten	Citrix Collector
Allgemeine Anwendung basierend auf dem Symbolpfad	Windows	-	WMI WinRM	Von oben nach unten	Symbolpfad der Citrix-Anwendung

Anwendungsservices zuordnen, die Citrix XenApp und Presentation Server enthalten

Ordnen Sie einen Anwendungsservice mit Citrix XenApps, Presentation Servern und Citrix Usage Collectors zu und vergewissern Sie sich, dass Service-Mapping alle Citrix-Komponenten richtig erkannt hat.

Vorbereitungen

- Erteilen Sie einem Benutzer die Berechtigung zum Lesen und Abfragen des Citrix-Repository:
  - Bei Versionen 4.5 und höher ein PowerShell-Skript vom XenApp-Server.
  - Für Versionen vor 4.5 ein Microsoft Visual Basic Script (VBScript) vom Citrix-Präsentationsserver
- Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.

  Hinweis: Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_collector fest.

- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren Sie einen Benutzer mit Berechtigungen zum Ausführen von PowerShell-Befehlen auf dem Citrix-Server.
- (Nur für die Erkennung von Citrix Presentation Server) Ermitteln Sie den Symbolpfad für den Einstiegspunkt:
  1. Navigieren Sie in der Citrix Access Management Console zu **Präsentationsserver** > **Anwendungen**an.
  2. Suchen Sie den Ordner „Icon Path“ in der Navigationsstruktur.
  3. Klicken Sie mit der rechten Maustaste auf den Ordner „Icon Path“, und klicken Sie auf **Pfad kopieren**.
- (Nur für die Erkennung von Citrix XenApp Server) Ermitteln Sie den Symbolpfad für den Einstiegspunkt, indem Sie das Attribut „Distinguished Name“ für den Symbolpfad überprüfen.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.
   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Serviceinstanz :
   a. Wählen Sie die Kachel **Citrix XenApp** aus.
   b. Definieren Sie die Einstiegspunktattribute.

Attribut	Beschreibung
Host	Die URL der Citrix XenApp bzw. des Presentation Server. Die URL muss eine VIP-IP oder einen physischen Host enthalten.
Port	Der Port, den die Citrix XenApp oder der Presentation Server auf dem Host verwendet
Pfad für Symbol	Der Pfad zum logischen Anwendungsspeicherort, wie er in der Citrix Access Management-Konsole angezeigt wird. Der Pfad muss mit dem Application-Ordner beginnen. Beispiel: /Application/Jane/Windows Media Player.
URL	Die URL muss eine VIP-IP oder einen physischen Host enthalten. Beispiel: http://<host>/Citrix/StoreWeb.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

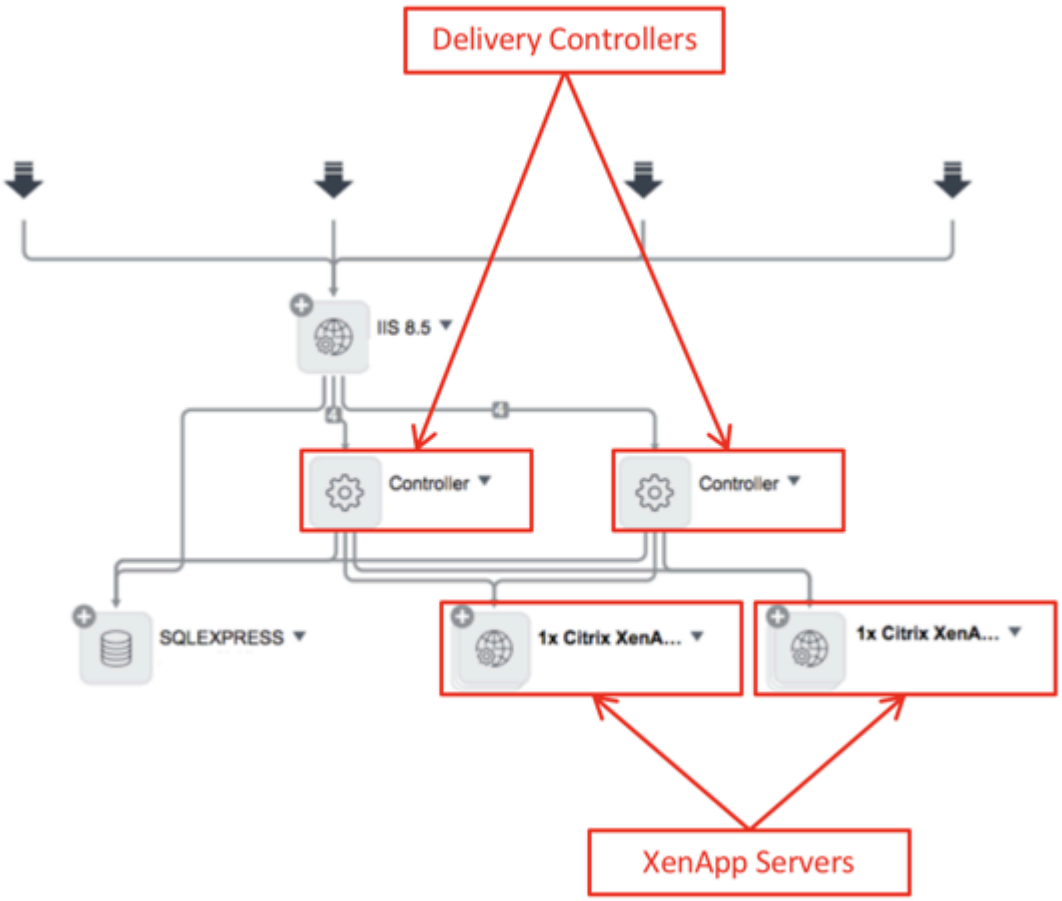
c. Klicken Sie auf **Hinzufügen**.

d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

b. Überprüfen Sie die Anwendungsservicezuordnung, und stellen Sie sicher, dass sie dem folgenden Beispiel ähnelt.



Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Nachricht an, die mit dem folgenden Text beginnt: Sie haben keine ausreichenden Berechtigungen.	Die Anzeigeabschnitte des Musters schlagen fehl, da der Benutzer keine Berechtigungen zum Ausführen von PowerShell-Befehlen hat.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern mit Citrix XenApp, Presentation Server oder Citrix Usage Collector bereitgestellt haben.
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die den folgenden Text enthält: CategoryInfo : NotSpecified: (:) [], PSSecurityException + FullyQualifiedErrorId : RuntimeException	Der MID-Server kann PowerShell-Befehle nicht remote ausführen, da die Ausführungsrichtlinie auf den Zielservern auf RemoteSigned festgelegt ist.	Verwenden Sie den Befehl `set-executionpolicy remotesigned` auf den Zielservern, damit MID-Server PowerShell-Befehle erfolgreich auszuführen kann.
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die den folgenden Text enthält: Import-XAFarm: Das PowerShell-Snapin für allgemeine Citrix-Befehle ist nicht installiert.	Der Zielhost verfügt nicht über diese PowerShell-Bibliothek: PowerShell-Snapin für allgemeine Citrix-Befehle.	Laden Sie das PowerShell-SDK für Citrix XenApp herunter, und installieren Sie es auf allen Servern, auf denen Citrix XenApp, Presentation Server oder Citrix Usage Collector gehostet wird.
Die Anwendungsservicezuordnung enthält den Citrix Delivery Controller, jedoch nicht Citrix XenApp, Citrix Presentation Server oder Citrix Usage Collector.	Der von Ihnen definierte Symbolpfad ist falsch.	Überprüfen Sie den Symbolpfad und geben Sie ihn in den Einstiegspunktattributen für den Anwendungsservice erneut ein.

Zuordnung von Anwendungsservices, die Microsoft Exchange Server enthalten

Service-Mapping Kann erkennen Service Instanz S Enthält einen Microsoft Exchange Server und die Exchange Server-Komponenten.

Erkannte Komponenten

Wenn E-Mail-Services in Ihrer Organisation Microsoft Exchange Server bereitstellen, umfasst der erkannte Anwendungsservice die folgenden Komponenten:

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Microsoft Azure Active Directory Domain Services	Windows	13, 30, 31, 44, 47, 52, 56, 69	WMI WinRM	Von oben nach unten	Active Directory Servicemuster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Microsoft Server (als Microsoft Exchange Komponente)	Windows	2003, 2007, 2010, 2013, 2016	WMI WinRM	Horizontal und von oben nach unten	ExchangeFrontEndServer auf Windows; PatternExchangeBackEndServer auf Windows-Muster
HUB-Transport-Server (als Microsoft Exchange Komponente)	Windows	2003, 2007, 2010, 2013, 2016	WMI WinRM	Horizontal und von oben nach unten	Hub-Transport-Server auf Windows-Muster
Clientzugriffsserver (CAS) (als eine Microsoft Exchange-Komponente)	Windows	2003, 2007, 2010, 2013, 2016	WMI WinRM	Horizontal und von oben nach unten	CAS auf Windows-Muster

Normalerweise möchten Sie keine mit dem Exchange Server verbundenen Outlook-Clients erkennen, um Störungen zu vermeiden. Ist dies der Fall, deaktivieren Sie die datenverkehrsbasierte Erkennung für diesen Anwendungsservice.

Informationen zum Erkennung-Flow finden Sie unter „Musterbasierte Erkennung“ in Service-Mapping. Wenn Benutzer nicht mit den erforderlichen Berechtigungen versehen werden, führt Service-Mapping möglicherweise eine datenverkehrsbasierte Erkennung durch.

Einschränkungen

Discovery und Service-Mapping können Exchange Server nicht erkennen, wenn seine Konfiguration keine öffentlichen Ordner, Edge-Transporte und öffentliches Messaging unterstützt. Erstellen Sie ein Muster, oder passen Sie das vorhandene Muster an, um Exchange Server mit einer solchen Konfiguration zu erkennen.

Anwendungsservices zuordnen, die Microsoft Exchange-Server enthalten

Ordnen Sie einen Anwendungsservice zu, der einen Microsoft Exchange-Server enthält, und vergewissern Sie sich, dass Service-Mapping alle Serverkomponenten von Microsoft Exchange richtig erkannt hat.

Vorbereitungen

- Konfigurieren Sie auf der ServiceNow AI Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. Verwenden Sie als Windows-Anmeldeinformationen Anwendername und Passwort des Microsoft Exchange Server-Administrators. Zum Beispiel Anwendername: local\administrator und Passwort: Are1300.

  Hinweis: Wenn Sie Windows-Anmeldeinformationen für einen anderen Benutzer als den Microsoft Exchange Server-Administrator konfigurieren, verwendet Service-Mapping die Traffic-basierte Discovery, die zur Zuordnung aller Microsoft Exchange-Clients führt.

- (Für Exchange CAS 2010 und 2013, 2016) Konfigurieren Sie auf der ServiceNow AI Platform Applicative-Anmeldeinformationen , indem Sie den CI-Typ auf „Exchange-Postfach“ einstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Warnung:** Verwechseln Sie den CI-Typ der Exchange Mailbox nicht mit dem CI-Typ des Exchange Mailbox-Servers.

Service-Mapping Verwendet diese anwendbaren Anmeldeinformationen für den Zugriff auf den Ordner of/Servers/Servers.slab im Key Exchange Admin Center (EAC). Service-Mapping Verwendet auch die anwendbaren Anmeldeinformationen, um die folgenden PowerShell-Befehle für auszuführen MID Servers:

- Get-ExchangeServer
- Get-ExchangeServer
- Get-Mailboxserver
- Get-ClusteredMailBoxServerStatus
- Get-ExchangeServer
- Get-StorageGroup
- Get-MailboxDatabase

- (Für Microsoft Exchange CAS 2010 und 2016) Installieren Sie das Microsoft.Exchange.Management.PowerShell.E2010-Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet.
- (Für Microsoft Exchange CAS 2007) Installieren Sie das Microsoft.Exchange.Management.PowerShell.Admin-Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet.
- (Für Microsoft Exchange CAS 2007, 2010) Laden Sie das rctrlx-Tool zum Ausführen von PowerShell-Befehlen auf ServiceNow AI Platform hoch, wie in Datei rctrlx.exe auf MID Servers hochladen beschrieben.
- (Für Microsoft Exchange CAS 2007 und 2010) Statten Sie einen Exchange Mailbox-Betriebssystem-Benutzer mit den Rechten zum Ausführen von Exchange-Services unter Windows und der Berechtigung zum Abfragen des Exchange-Repositorys aus:

  Konfigurieren Sie auf der ServiceNow AI Platform die Windows-Anmeldeinformationen , indem Sie das Attribut `Credential alias` auf [cmdb_ci_exchange_mailbox] einstellen. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.

- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
- Vergewissern Sie sich, dass Sie den Einstiegspunkt kennen, der zum Erkennen des Microsoft Exchange-Servers erforderlich ist. Verwenden Sie die URL für den Outlook-Webzugriff im folgenden Format:

  http(s)://<hostname>:<port>/owa

  Zum Beispiel http(s)://myhost:<443>/owa

Erforderliche Rolle: Service_Mapping_admin

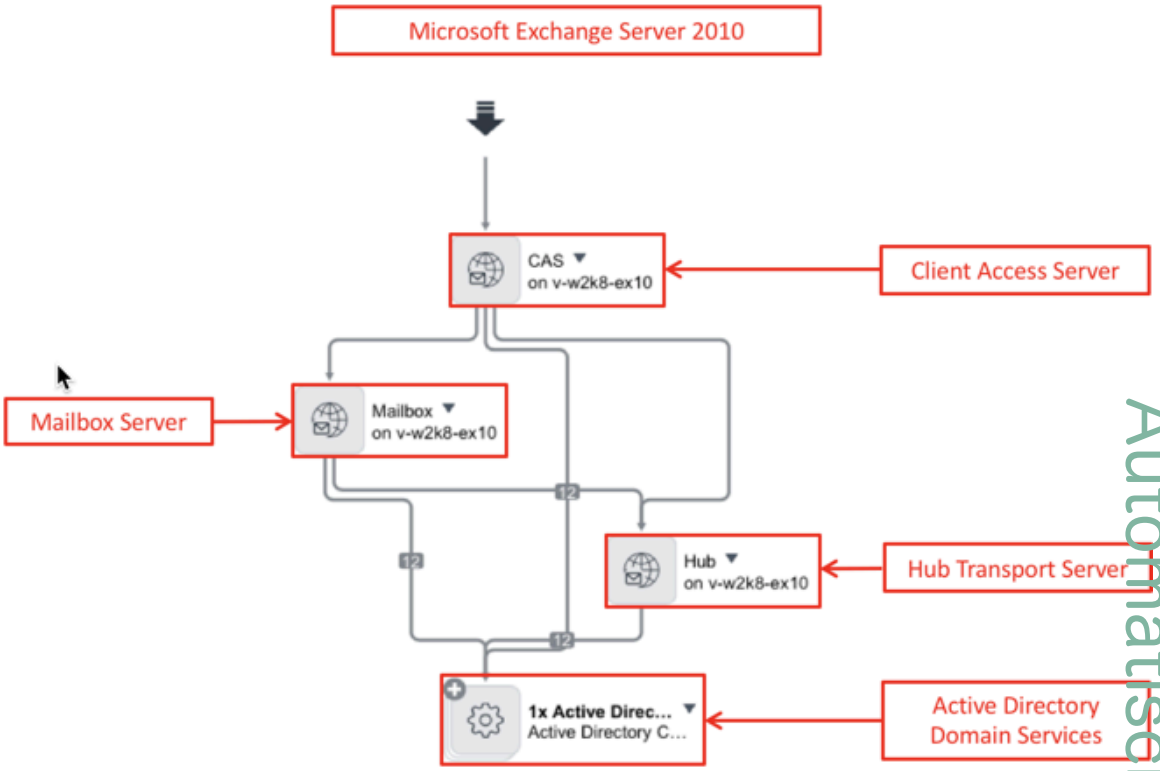
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.
   b. Klicken Sie auf **Neu**.
      Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Serviceinstanz :
   a. Wählen Sie die Kachel **Webanwendung** aus.
      Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.
   b. Geben Sie im Feld **URL** die URL des Outlook-Webzugriffs ein.
      Beispiel: http(s)://myhost:<443>/owa.
   c. Klicken Sie auf **Hinzufügen**.
   d. Klicken Sie auf **Speichern**.
3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:
   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist.
      Es kann einige Minuten dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die Anwendungsservice-Zuordnung, und stellen Sie sicher, dass das Servicelayout wie in den Beispielen unten aussieht.



Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Nachricht an, die mit dem folgenden Text beginnt: Sie müssen das PowerShell-Snapin für allgemeine Exchange-Befehle installiert haben, um dieses Skript zu verwenden.	Die Anzeigeabschnitte des Musters schlagen fehl, da der Benutzer keine Berechtigungen zum Ausführen von PowerShell-Befehlen hat.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern bereitgestellt haben, die Serverkomponenten von Microsoft Exchange wie CAS hosten.
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die mit dem folgenden Text beginnt: [servername.destination.com] Die Verbindung zum Remote-Server ist mit der folgenden Fehlermeldung fehlgeschlagen: Der WinRM-Client kann die	Die Anzeigeabschnitte des Musters schlagen fehl, da der MID-Server auf der zu erkennenden	Fügen Sie den MID Server der Liste der vertrauenswürdigen Hosts auf allen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
Anforderung nicht verarbeiten. Der vom Client angeforderte Authentifizierungsmechanismus wird vom Server nicht unterstützt, oder der unverschlüsselte Datenverkehr ist in der Servicekonfiguration deaktiviert. Überprüfen Sie die Einstellung für unverschlüsselten Datenverkehr in der Servicekonfiguration, oder geben Sie einen der vom Server unterstützten Authentifizierungsmechanismen an.	Komponente nicht als vertrauenswürdiger Host konfiguriert ist.	Hosts hinzu, die Sie erkennen möchten.
Die Anwendungsservice-Zuordnung ist sehr groß, da sie Verbindungen zu allen Outlook-Clients enthält.	(In Bereitstellungen mit Microsoft Exchange Server 2007, 2010 oder 2013) Service-Mapping hat Verbindungen mithilfe einer datenverkehrsbasierten Erkennung erstellt, die alle offenen Verbindungen verfolgt, anstatt PowerShell-Befehle zu verwenden.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern bereitgestellt haben, die Serverkomponenten von Microsoft Exchange wie CAS hosten.

Tibco BusinessWorks- und EMS-Erkennung

Discovery kann Tibco ActiveMatrix BusinessWorks und Enterprise Message Service (EMS) erkennen. Service-Mapping kann Anwendungsservices erkennen, die Tibco BusinessWorks, Enterprise Message Service (EMS) und die zugehörigen Komponenten enthalten.

Von Discovery für Tibco ActiveMatrix BusinessWorks gesammelte Daten

Die folgenden Daten werden in der ActiveMatrix Business Works-Tabelle [cmdb_ci_appl_tibco_matrix] gesammelt.

Tabelle und Feld	Beschreibung
ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]	
Name [name]	Die Attribute des ActiveMatrix BusinessWorks-Konfigurationselements
Version [version]	
TCP-Port(s) [tcp_port]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
IP-Adresse [ip_address]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Installationsverzeichnis [install_directory]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Projekt [project]	

Von Discovery für Tibco Enterprise Message Service gesammelte Daten

In der Standardeinstellung verwendet Discovery das Muster *`Enterprise Message Service`*, um Tibco Enterprise Message Service zu erkennen.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Tabelle und Feld	Feldname
Tibco Enterprise Message Services [cmdb_ci_appl_tibco_message]	
Name [name]	Attribute des Konfigurationselements Tibco Enterprise Message Services.
Version [version]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
IP-Adresse [ip_address]	
Installationsverzeichnis [install_directory]	
TCP-Port(s) [tcp_port]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Installationsverzeichnis [install_directory]	

Durch Service-Mapping erfasste Daten

Service-Mapping kann Anwendungsservice erkennen, die Tibco ActiveMatrix BusinessWorks (einschließlich BusinessWorks Process), Tibco Enterprise Message Service (EMS) und die Tibco Enterprise Message Service- (EMS-)Warteschlange enthalten.

Anwendungsservices zuordnen, die Tibco BusinessWorks und EMS enthalten

Ordnen Sie einen Anwendungsservice zu, der Tibco BusinessWorks und Enterprise Message Service (EMS) enthält, und vergewissern Sie sich, dass von Service-Mapping alle Tibco-Komponenten korrekt erkannt wurden.

Vorbereitungen

- (Beim Hosting auf Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Tibco EMS.
- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform Windows-Anmeldeinformationen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der ServiceNow AI Platform SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

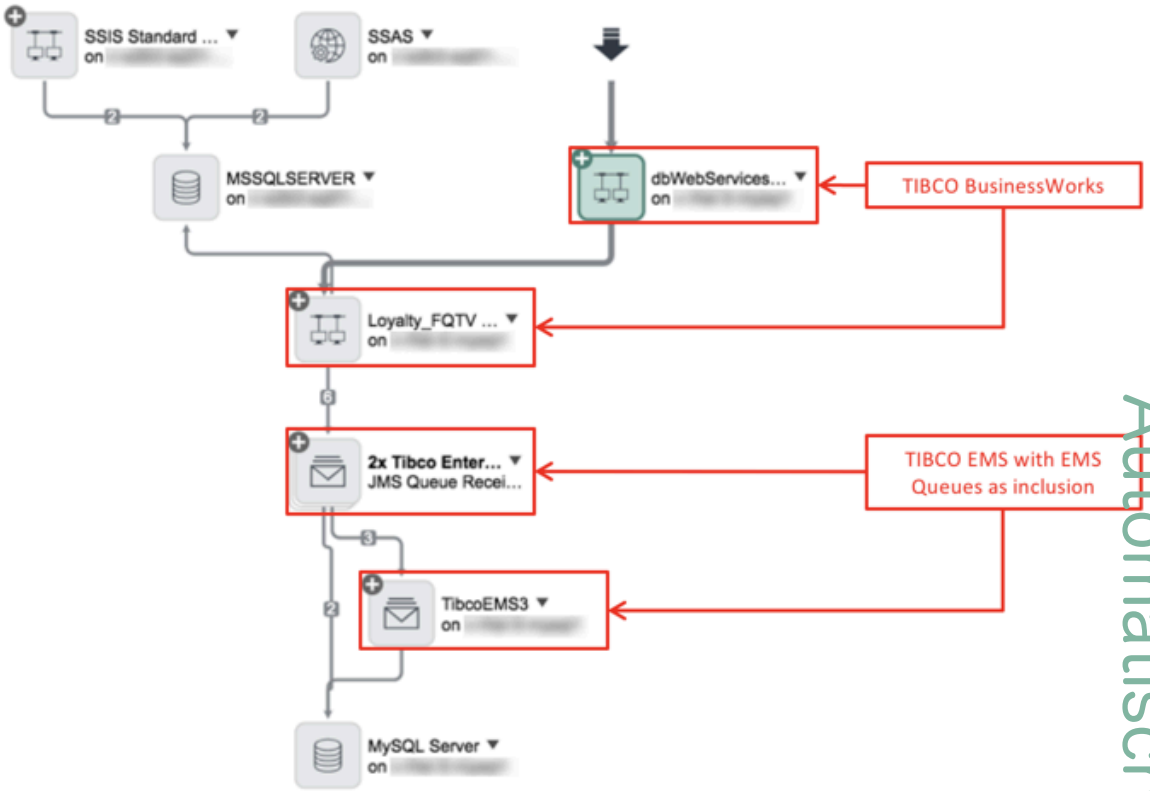
Erforderliche Rolle: Service_Mapping_admin

Prozedur

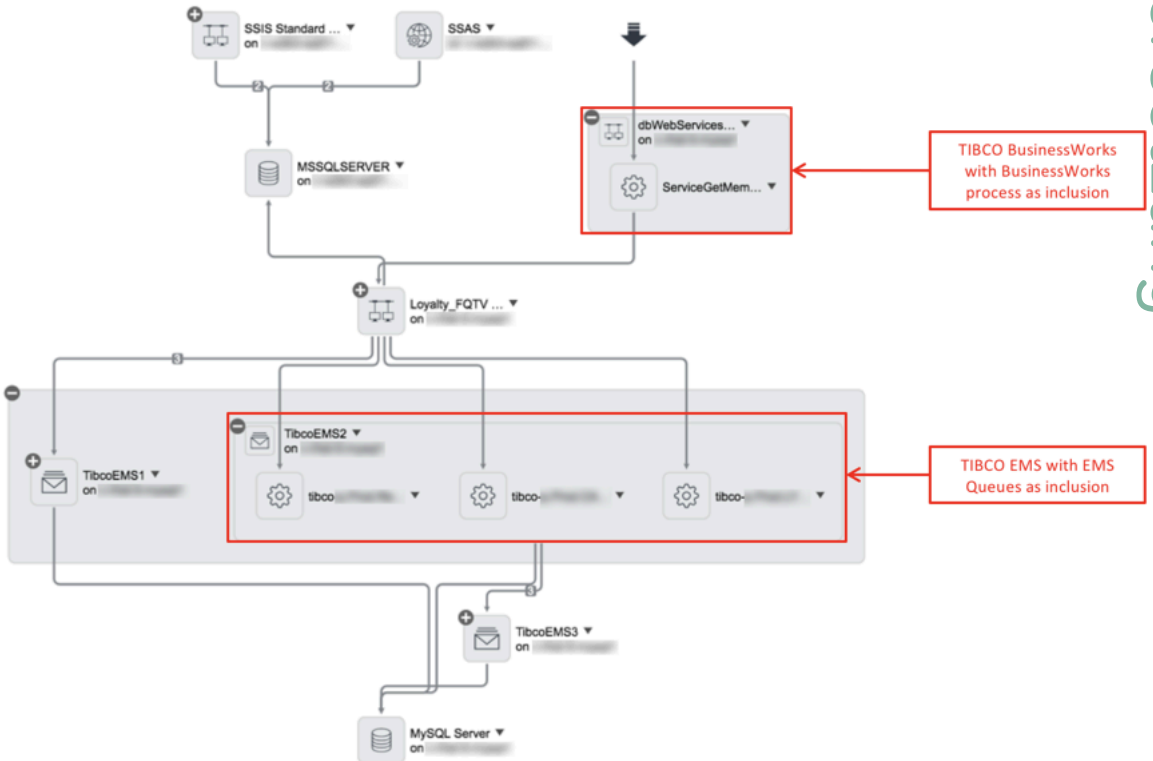
1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.
   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:
   a. Wählen Sie die Kachel **Sonstige Anwendung**.
   Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.
   b. Wählen Sie in der Liste „Eingangspunkttyp auswählen“ den Eintrag `HTTP(s)-Endpunkt, TCP-Endpunkt, Tibco BW-Endpunkt` aus.
   c. Definieren Sie den Einstiegspunkt wie folgt:
      - Die URL des Prozesses, der dem Tibco BusinessWorks-Projekt entspricht, z. B. `http://10.xx.xx.xx:6710/GetMemberActivitiy/Processes/ServiceGetMemberActivitiy.service` .
      - (Optional) Der Hostname, auf dem das BusinessWorks-Projekt als Service ausgeführt wird.
   d. Klicken Sie auf **Hinzufügen**.
   e. Klicken Sie auf **Speichern**.
3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:
   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist.
   Es kann einige Minuten dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die Zuordnung des Anwendungsservice, und stellen Sie sicher, dass das Servicelayout wie in den folgenden Beispielen aussieht.



Stellen Sie außerdem sicher, dass die BusinessWorks-CIs mit eingeschlossen sind und jedes der Elemente jeweils einen BusinesWorks-Prozess enthält. Stellen Sie außerdem sicher, dass die EMS-CIs eingeschlossen sind und EMS-Warteschlangen enthalten.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
(Nur für Bereitstellungen, bei denen BusinessWorks auf einem Unix-Server gehostet wird) Die Serviceinstanz -Zuordnung zeigt das BusinessWorks-CI ohne Einbeziehung des BusinessWorks-Prozesses. Das Erkennungsprotokoll zeigt die Fehlermeldung an, dass der Benutzer nicht über ausreichende Anmeldeinformationen verfügt.	Service-Mapping konnte den Befehl `TibcoFilesParser.ksh` nicht ausführen.	Stellen Sie sicher, dass Sie einem Benutzer erhöhte Rechte gewährt haben, wie in Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschrieben.
Service-Mapping konnte die ausgehenden Verbindungen von EMS zum EMS-Prozess nicht erkennen.	Service-Mapping konnte den Befehl `tibemsadmin` nicht ausführen.	Stellen Sie sicher, dass Sie einem Benutzer erhöhte Rechte gewährt haben, wie in Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschrieben.

Anwendungsservices zuordnen, die Oracle GlassFish-Server enthalten

Service-Mapping kann Anwendungsservices erkennen, die Oracle GlassFish-Server enthalten.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle GlassFish Server	Windows UNIX	3.1, 4.0, 4.1	WMI WinRM SSH	Horizontal und von oben nach unten	GlassFish Server
Oracle GlassFish WAR-Datei	Windows UNIX	3.1, 4.0, 4.1	WMI WinRM SSH	Horizontal und von oben nach unten	GlassFish WAR

Anwendungsservices zuordnen, die Oracle GlassFish-Server enthalten

Ordnen Sie einen Serviceinstanz , der Oracle GlassFish-Server enthält, korrekt zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der ServiceNow AI Platform Windows-Anmeldeinformationen .
- (Beim Hosting auf einem Linux- oder UNIX-Server) (Optional) Konfigurieren Sie in der ServiceNow AI Platform SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.
   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:
   a. Wählen Sie die Kachel **Sonstige Anwendung**.
   Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.
   b. Definieren Sie den Einstiegspunkt, indem Sie die Felder ausfüllen.

Feld	Beschreibung
Typ des Einstiegspunkts auswählen	Einstiegspunkttyp: ▪ HTTP(S)-Endpunkt ▪ TCP-Endpunkt ▪ TIBCO BW-Endpunkt
URL	Die URL des Prozesses, die mit dem GlassFish-Server korreliert, z. B. http://10.196.xx.xx:28080/hello/. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** ausgewählt ist.
Host	Der Server, der den GlassFish-Server hostet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.
Host-Name	Der Hostname des Servers, der den GlassFish-Server hostet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** ausgewählt ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Port	Der Port, den der mit dem GlassFish-Server korrelierende Prozess verwendet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.
Prozessname	Der Name des Prozesses, der mit dem GlassFish-Server korreliert. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** ausgewählt ist.
Kommentare	Freitextkommentar, um Informationen zum Endpunkt bereitzustellen. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.

c. Klicken Sie auf **Hinzufügen**.

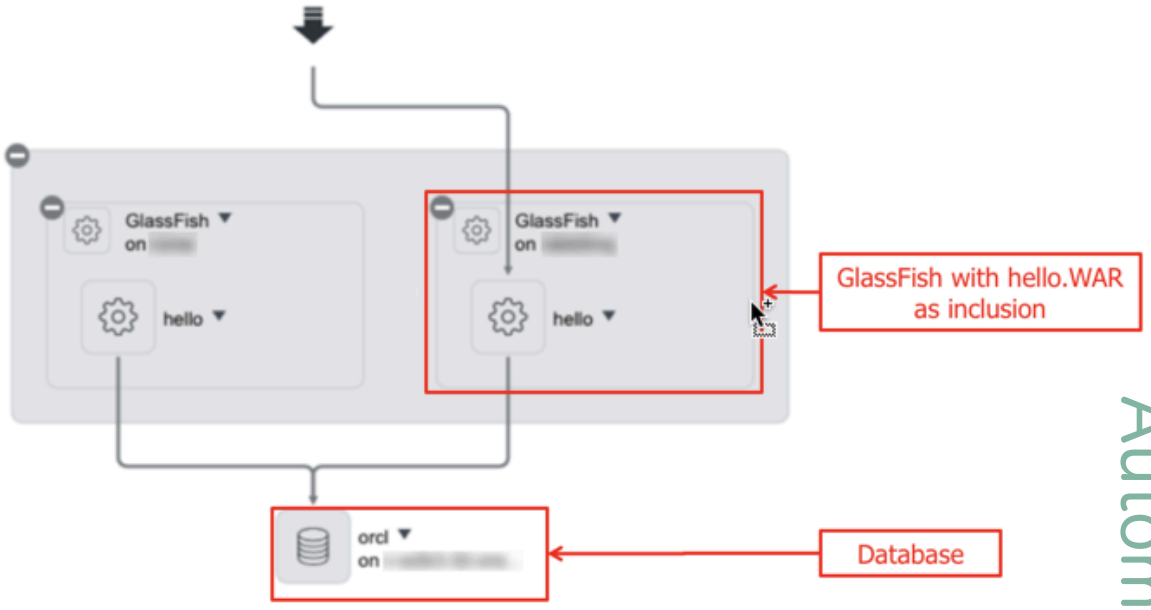
d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die Zuordnung des Anwendungsservices, und stellen Sie sicher, dass das Servicelayout wie im folgenden Beispiel aussieht.



Stellen Sie außerdem sicher, dass die GlassFish-Server-CIs eingeschlossen sind und jedes von ihnen eine WAR-Datei enthält.

Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Service-Mapping kann das GlassFish-Server-CI nicht erkennen. Das Erkennungsprotokoll zeigt die folgende Meldung an: Der Prozess wird nicht ausgeführt, oder der Port ist nicht korrekt. Das CI wurde nicht erkannt, da auf dem Host 10.196.xx.xx keine Anwendung auf Port 28080 ausgeführt wird. Stellen Sie sicher, dass die Anwendung ausgeführt wird, und führen Sie eine schnelle Erkennung auf dem Host aus.	Auf dem Port, der Teil des Einstiegspunkts ist, wird kein Prozess ausgeführt.	1. Stellen Sie sicher, dass der Einstiegspunkt korrekt ist. 2. Wenn der Einstiegspunkt korrekt ist, überprüfen Sie, ob hier ein Prozess für den Port ausgeführt wird, indem Sie eine schnelle Erkennung auf dem Host ausführen.

Anwendungsservices zuordnen, die Oracle Tuxedo-Plattform enthalten

Service-Mapping kann Anwendungsservices erkennen, die die Oracle Tuxedo-Plattform und die zugehörigen Komponenten enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle Tuxedo	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tuxedo
Oracle Tuxedo-Portal	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tuxedo Portal - Muster

Anwendungsservices zuordnen, die Oracle Tuxedo-Plattform enthalten

Ordnen Sie einen Anwendungsservice zu, der eine Oracle Tuxedo-Plattform enthält, und vergewissern Sie sich, dass Service-Mapping alle Tuxedo-Komponenten richtig erkannt hat.

Vorbereitungen

- Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
- (Wenn auf Unix gehostet wird) Geben Sie einem Benutzer die erweiterten Rechte zum Ausführen von Befehlen, die in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern beschrieben werden.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.
   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:
   a. Wählen Sie die Kachel **Sonstige Anwendung**.
   b. Wählen Sie `TCP-Endpunkt` aus der Liste aus.
   c. Definieren Sie den Einstiegspunkt wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Host des Servers, der den Tuxedo-Prozess hostet.
- Ein Port auf diesem Server, der vom Tuxedo-Prozess geöffnet wird.

d. Klicken Sie auf **Hinzufügen**.

e. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

b. Überprüfen Sie die Zuordnung des Anwendungsservices.

Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Service-Mapping kann das Tuxedo-CI nicht erkennen. Das Erkennungsprotokoll zeigt die Meldung an, dass die Anmeldeinformationen für die Ausführung des Befehls nicht ausreichen, einschließlich „permissions.tmadadmin -v“.	Der angegebene Benutzer hat keine erhöhten Berechtigungen zum Ausführen dieses Befehls.	Stellen Sie sicher, dass Sie einem Benutzer die Berechtigungen zum Ausführen von Befehlen mit erhöhten Rechten gewährt haben.
Service-Mapping kann das Tuxedo-CI nicht erkennen. Das Erkennungsprotokoll zeigt die Meldung an, dass der Benutzer das Skript „tux.env“ nicht ausführen kann.	Der angegebene Benutzer ist nicht berechtigt, das Skript „tux.env“ auszuführen.	Stellen Sie sicher, dass Sie einem Benutzer die Berechtigungen zum Ausführen des Skripts „tux.env“ gewährt haben.

Tag-Definitionen für die Tag-basierte Zuordnung ändern oder aktualisieren

Sie können Tag-Definitionen ändern, die Service-Mapping für die Tag-basierte Zuordnung verwendet. Service-Mapping verwendet aktualisierte Tag-Definitionen, um neue Tag-basierte Services zu erstellen, ohne Tag-bezogene Änderungen auf zuvor zugeordnete Services anzuwenden.

Vorbereitungen

Wenn Sie eine neue Tag-Kategorie erstellen oder eine vorhandene Tag-Kategorie ändern müssen, beachten Sie die Voraussetzungen unter Ordnen Sie Anwendungsservices mithilfe von Tags mit zu klassisch Service-Mapping.

Lesen Sie die Empfehlungen in Zuordnung von Anwendungsservices basierend auf Tags vorbereiten.

Erforderliche Rolle: Service_Mapping_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

In den folgenden Fällen können Sie Tag-Kategorien einer Tag-basierten Servicefamilie hinzufügen oder daraus entfernen:

- Wenn Sie mit den Ergebnissen der tagbasierten Zuordnung nicht zufrieden sind, z. B. wenn der Service zu groß ist, da er irrelevante CIs enthält
- Wenn sich die Verwendung von Tags in Ihrer Organisation ändert, z. B. durch neue Tags.

Wenn Sie für eine tagbasierte Servicefamilie definierte Tag-Kategorien ändern oder eine tagbasierte Servicefamilie insgesamt löschen, werden alle zugeordneten Services von dieser tagbasierten Servicefamilie getrennt. Diese Services sind weiterhin vorhanden und werden von Service-Mapping weiterhin mit der ursprünglichen Tag-Definition aktualisiert. Um zu vermeiden, dass Tag-basierte Services auf veralteten Tag-Definitionen basieren, löschen Sie alle vorhandenen Tag-basierten Services.

Service-Mapping generiert neue Tag-basierte Servicekandidaten, die Sie zum Zuordnen von Services auf Grundlage der geänderten Tag-Definition verwenden.

Wichtig: Neue Services, die auf geänderten Tag-Definitionen basieren, überschreiben zuvor zugeordnete Services nicht.

Prozedur

1. Löschen Sie vorhandene tagbasierte Services:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**an.
   b. Wählen Sie die Tag-basierte Servicefamilie aus, für die Sie die Tag-Definition ändern möchten.
   c. Klicken Sie unter **Zugeordnete Services** auf **Zugeordnete Services löschen**, um alle Services zu löschen.
   d. Oder klicken Sie auf das Symbol **Zum Löschen markieren** neben dem entsprechenden Service in der Liste, und klicken Sie dann auf **Löschen**.
2. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**an.
3. Wählen Sie den Tag-basierten Service aus, für den Sie die Tag-Definition ändern möchten.
4. Führen Sie unter **Ausgewählte Tag-Kategorien** eine der folgenden Aktionen aus:
   - Fügen Sie eine neue Tag-Kategorie hinzu, indem Sie auf die leere Zeile doppelklicken und die entsprechende Tag-Kategorie aus der Liste der zuvor definierten Tag-Kategorien auswählen.
   - Entfernen Sie eine Tag-Kategorie, indem Sie neben der Kategorie auf das Symbol **Zum Löschen markieren** klicken.
   - Ändern Sie die Verwendung einer Tag-Kategorie, die bereits der Servicefamilie zugeordnet ist, indem Sie die Tag-Werte oder die Reihenfolge der Servicenamen ändern.

     Verwenden Sie für mehrere Tag-Werte Kommas als Trennzeichen. Die Servicebenennungs-Reihenfolge definiert, wie Service-Mapping den Tag-Kategorienamen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in den Namen der Anwendungsservices verwendet, die für die Servicefamilie generiert werden.

- Ändern Sie die Tag-Kategorie selbst, indem Sie auf den Tag-Kategorienamen klicken und dann die CI-Tag-Schlüssel definieren.

5. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Tag-basierte Anwendungsservices neu zuordnen, um Tag-Änderungen widerzuspiegeln

Tag-basierte Anwendungsservices neu zuordnen, um Tag-Änderungen widerzuspiegeln

Erstellen Sie Tag-basierte Services neu, wenn sich die Art und Weise, wie Tags in Ihrer Organisation verwendet werden, geändert hat oder nachdem Tag-Definitionen für Tag-basierte Servicefamilien geändert wurden.

Vorbereitungen

Ändern Sie bei Bedarf Tag-Definitionen für die relevante tagbasierte Servicefamilie.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ordnen Sie vorhandene Tag-basierte Services neu zu, nachdem Sie Tag-Definitionen manuell geändert haben. Wenn Ihre Organisation neue Tag-Schlüssel oder Tag-Werte verwendet, sollten Sie eventuell auch die vorhandenen Services neu zuordnen. In beiden Fällen aktualisiert Service-Mapping die vorhandenen Services nicht automatisch mit den Tag-Änderungen.

Prozedur

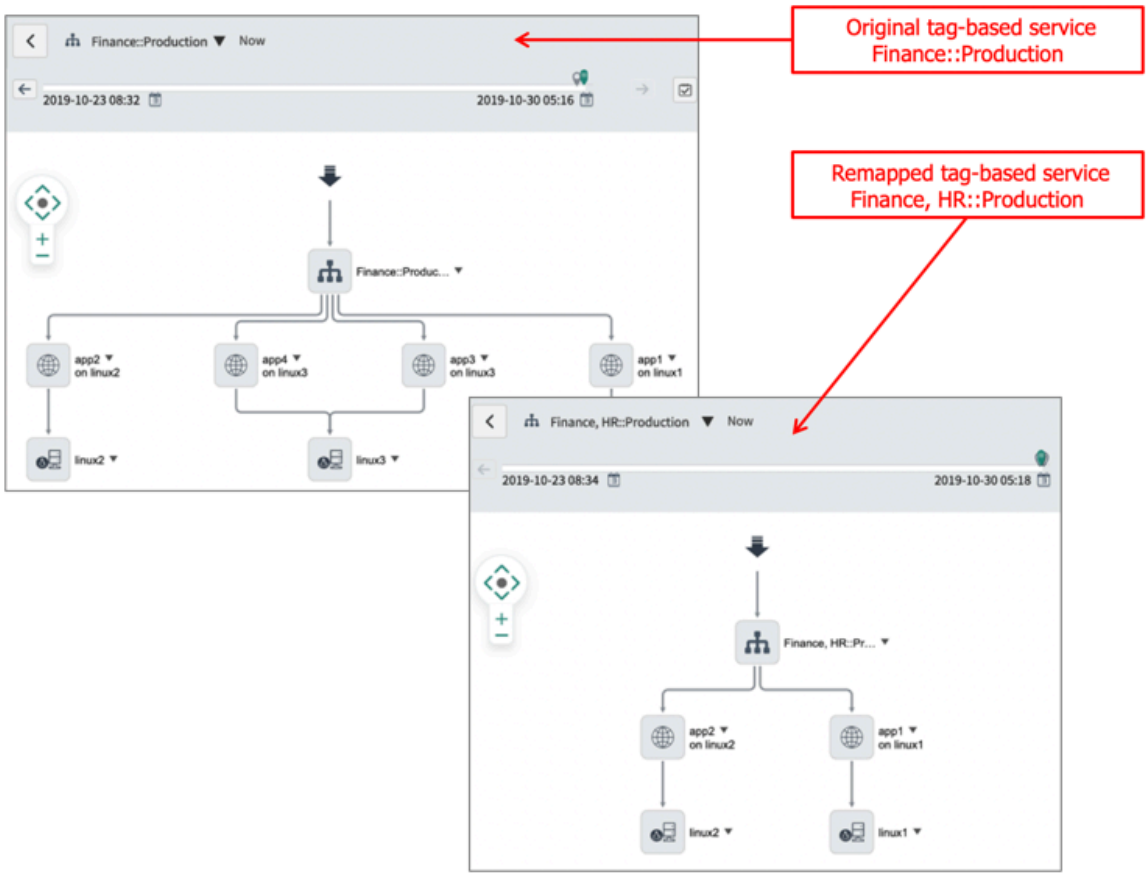
1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**an.
2. Wählen Sie die Tag-basierte Servicefamilie aus, deren Tag-Definitionen sich geändert hat.
3. Klicken Sie unter **Zugehörige Links** auf **Kandidaten manuell aktualisieren**, um neue Servicekandidaten mit den geänderten Tag-Definitionen zu generieren.
4. Überprüfen Sie im Fenster „Servicekandidat“ die vorgeschlagenen Servicekandidaten, und wählen Sie diejenigen aus, die Sie zuordnen möchten.
   Wenn keine Servicekandidaten vorhanden sind, stellen Sie sicher, dass Sie die Tag-Werte ausgewählt haben, die in der Tabelle Schlüsselwert [cmdb_key_value] vorhanden sind.
5. Klicken Sie auf **Ausgewählte zuordnen**.
   Service-Mapping erstellt Anwendungsservices anhand der von Ihnen ausgewählten Kandidaten.
6. Überprüfen Sie die neu erstellten Services unter **Zugeordnete Services**, um sicherzustellen, dass das Ergebnis Ihren Erwartungen entspricht.
   Wenn Service-Mapping anbietet, anstatt einer Zuordnung für einen Anwendungsservice die CI-Liste anzuzeigen, ist der Service zu groß. Nehmen Sie ein Feintuning vor, wie unter Tag-Definitionen für die tagbasierte Zuordnung ändern oder aktualisieren beschrieben.

Ergebnis

Sie haben den Anwendungsservice basierend auf den neuesten Tag-Definitionen zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neu zugeordneter Tag-basierter Anwendungsservice



Nächste Maßnahme

Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:

- Service-Mapping Bietet nicht an, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
- Es gibt keine Discovery-Nachricht, die darauf hinweist, dass die Serviceinstanz zu groß ist: *`The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.`*

Wenn der Service zu groß ist, führen Sie die folgenden Aktionen aus:

- Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen Um sicherzustellen Service-Mapping Schließt nur relevante CIs in der Serviceinstanz ein.
- Falls erforderlich, Tag-basierte Discovery-Konfiguration Um zu ändern, welche CIs Service-Mapping Enthält in Tag-basierten Serviceinstanzen.

Fehler bei Anwendungsservices als Massenvorgang beheben

Von Service-Mapping werden Fehler nach ihrer Ursache klassifiziert, z. B. fehlende Anmeldeinformationen oder Zeitüberschreitung bei einer Aufgabe. Für einen schnellen und effizienten Prozess beheben Sie jeweils die Fehler im Stapelverfahren, die zu derselben Kategorie gehören.

Vorbereitungen

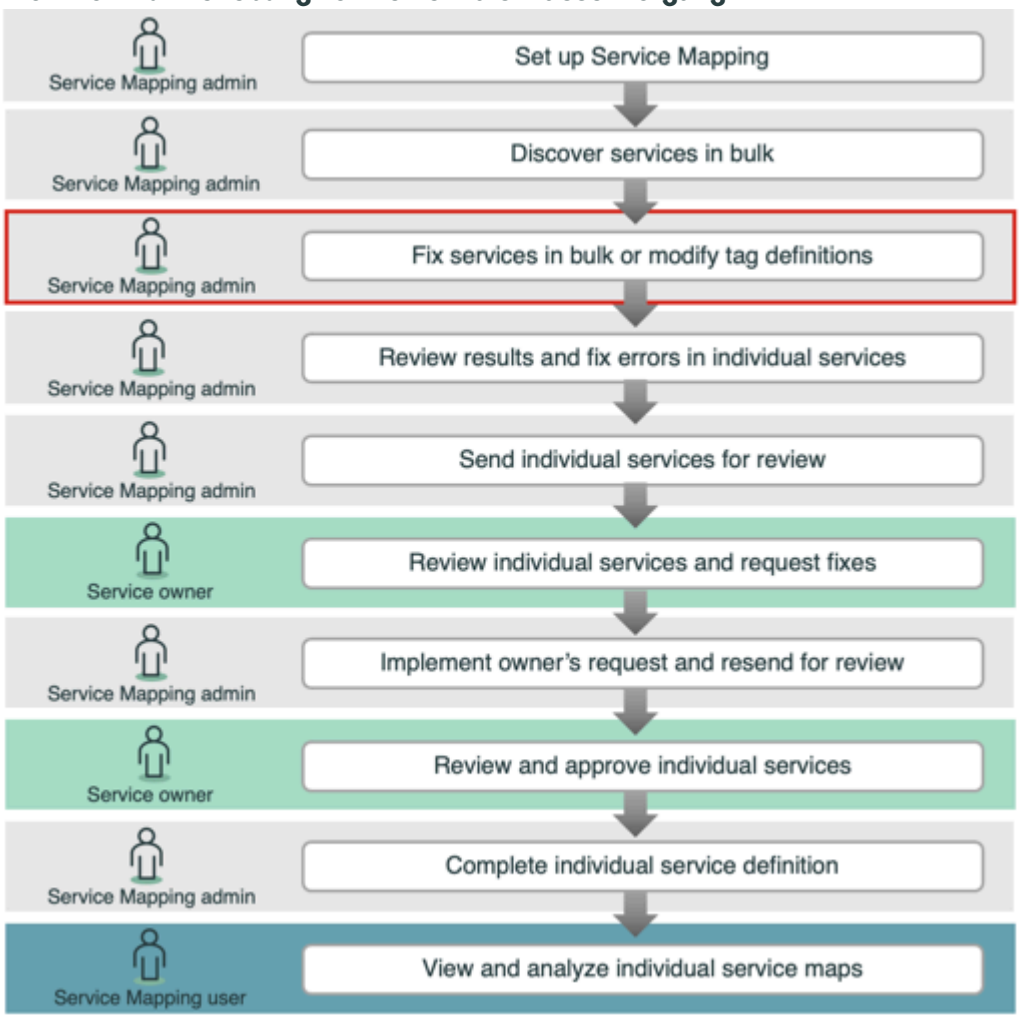
Erforderliche Rolle: Service_Mapping_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Sie können Fehler nach Kategorie anzeigen, z. B. **Konfiguration**, **Netzwerk** und **Anmeldeinformationen**. Jede Kategoriespalte enthält auch einen Fehlerzähler.

Als Teil des Service-Mapping-Workflows können Sie, nachdem Sie Anwendungsservices als Massenvorgang zugeordnet haben, mehrere Fehler im Zusammenhang mit Anwendungsservices gleichzeitig (als Gruppe) beheben.

Workflow zur Behebung von Fehlern als Massenvorgang



Nach der ersten Zuordnung erkennt Service-Mapping Konfigurationselemente (CIs) regelmäßig neu und aktualisiert die Liste der Fehler ständig. Erkennungszeitpläne definieren, wie oft Service-Mapping den Erkennungsprozess für CIs ausführt. Service-Mapping erkennt nur CIs von Anwendungsservices mit dem Status „Betriebsbereit“.

Manche Erkennungsfehler sind eventuell keiner Kategorie zugewiesen:

- Nachdem Service-Mapping von der Version Jakarta oder älter aktualisiert wurde.
- Wenn Konfigurationselemente (CIs) vorhanden sind, denen Fehler zugeordnet sind und die zuerst aus Anwendungsservices entfernt und dann den Anwendungsservices erneut hinzugefügt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite** Und klicken Sie dann auf **Korrigieren Sie Ihre Services** In **Beheben** Feld.
   Die Zahl im Feld **Korrigieren** gibt die Anzahl der betroffenen Servicezuordnungen an. Klicken Sie auf **Aktualisieren** ( ), um die Anzeige zu aktualisieren.

   Hinweis: Um die Fehler für einen bestimmten Service zu beheben, klicken Sie auf **Fehler nach Service verwalten**.

2. Wenn nicht kategorisierte Fehler vorhanden sind, können Sie sie nach Serviceinstanz kategorisieren:

   a. Klicken Sie auf **Nicht kategorisierte Fehler nach Service anzeigen**.

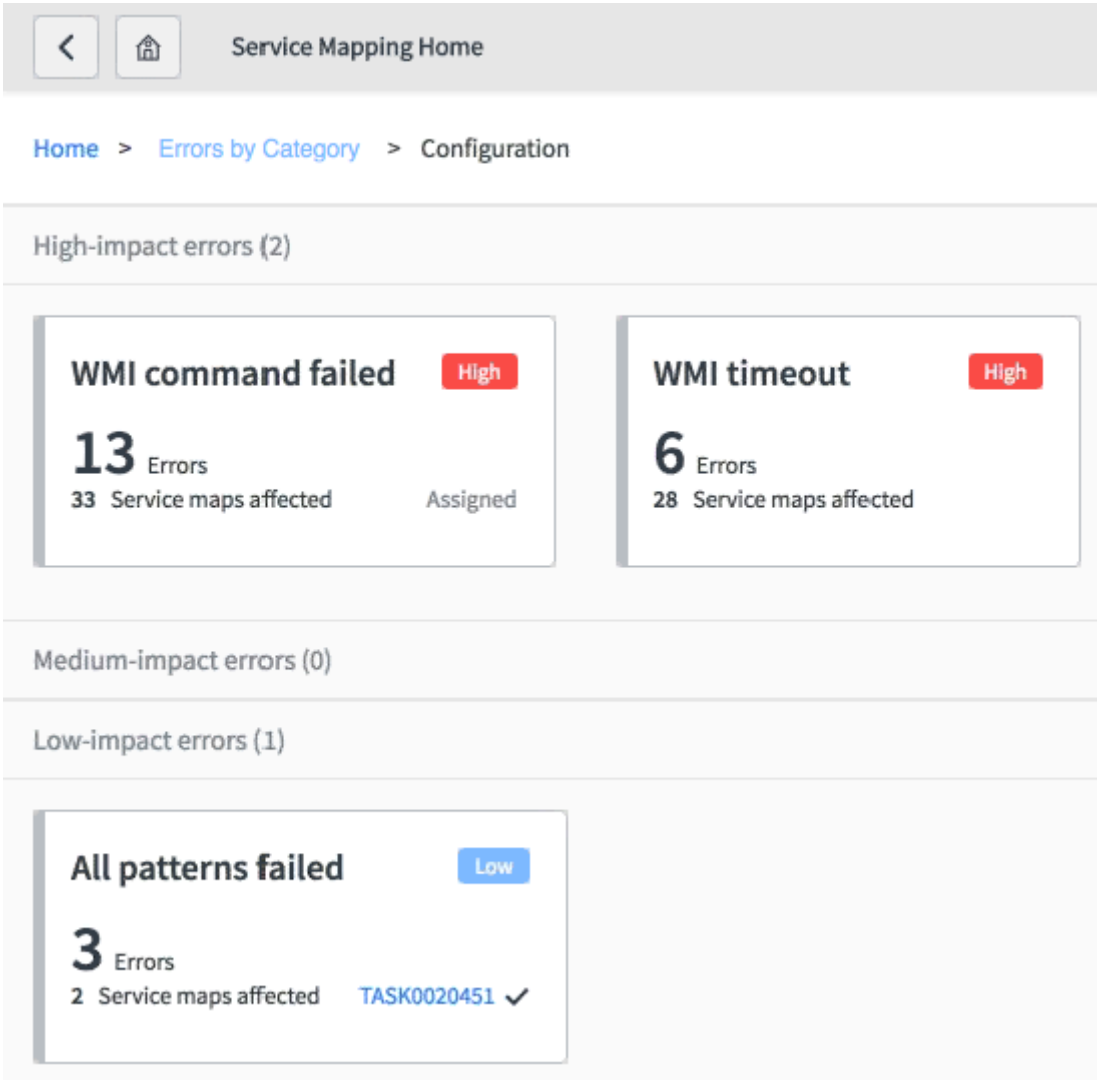
   b. Klicken Sie auf den entsprechenden Servicenamen.

   c. Klicken Sie in der Serviceinstanz -Zuordnung auf **Erkennung ausführen**.
   Service-Mapping erkennt alle CIs, die mit Fehlern erkannt wurden und zu diesem Serviceinstanz gehören.

3. Wenn nicht kategorisierte Fehler vorhanden sind, kategorisieren Sie sie durch Klicken auf **Relevante CIs erneut erkennen** und per Klick auf **Weiter** in der Bestätigungsnachricht.
   Service-Mapping erkennt alle CIs, die mit Fehlern erkannt wurden und zu Anwendungsservices mit dem Status „Betriebsbereit“ gehören.

4. Klicken Sie in das Feld einer Fehlerkategorie.
   Im Beispiel unten sind Konfigurationsfehler ausgewählt.
   - Auf der Seite „Fehler nach Kategorie“ werden Fehler nach hohen, mittleren und geringen Auswirkungen auf die Services sortiert.
   - Für jede Auswirkungskategorie werden Fehler nach Fehlercode (möglicherweise die Ursache) in Felder gruppiert.
   - Wenn Fehleraufgaben zugewiesen wurden, werden die Aufgabennummern im Feld angezeigt. Klicken Sie auf eine Aufgabe, um Details anzuzeigen. Zeigen Sie auf eine Aufgabe, um Kommentare anzuzeigen, die die zuweisende Person möglicherweise hinzugefügt hat. Ein Häkchen zeigt an, dass eine Aufgabe abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

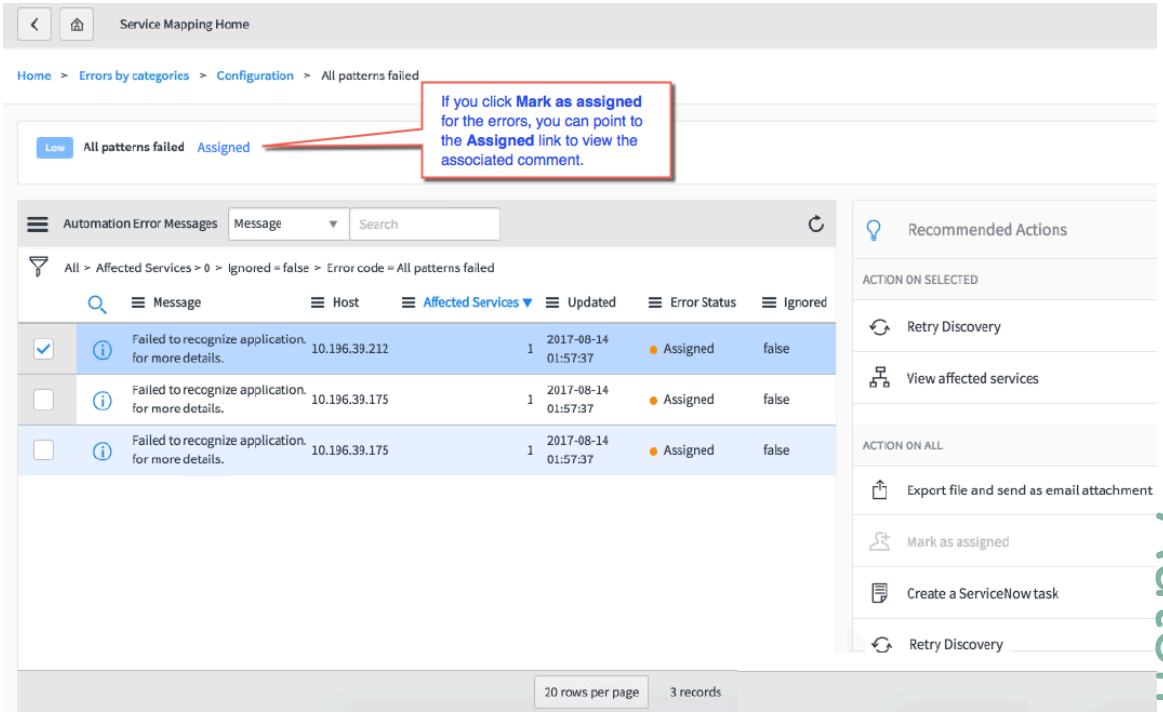


5. Klicken Sie auf das Feld, um eine Liste der Fehler anzuzeigen, die denselben Fehlercode aufweisen. Sie können eine der **Empfohlenen Aktionen** auf ausgewählte Elemente bzw. alle Elemente in der Liste anwenden.

   Im Beispiel ist **Alle Muster fehlgeschlagen** ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf eine Aktion im Abschnitt **Aktion auf alle**, oder wählen Sie Fehler aus, und klicken Sie auf eine Aktion im Abschnitt **Aktion auf Ausgewählte**.

Discovery erneut starten

Führt den kompletten Discovery-Prozess aus. Normalerweise führen Sie Discovery aus, nachdem Sie die Korrekturanweisungen befolgt haben, die angezeigt werden, wenn Sie auf **Anweisungen anzeigen** klicken.

Betroffene Services anzeigen

Zeigt eine Popup-Liste aller Services an, die vom ausgewählten Fehler betroffen sind. Klicken Sie in der Liste auf einen Service, um Servicedetails anzuzeigen.

Als zugewiesen markieren

Wenden Sie die Aktion **Als zugewiesen markieren** an, wenn Sie eine Out-of-Band-Aktion ausführen möchten, um eine Person zu benachrichtigen, die den Fehler beheben soll (normalerweise eine Person, die die ServiceNow-Instanz nicht verwendet). Sie können im Popup-Fenster **Als zugewiesen markieren** einen **Kommentar** eingeben. Klicken Sie auf **Aktualisieren**, um das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen** zu setzen und den **Kommentar** mit dem Fehler zu verknüpfen. Zeigen Sie zum Anzeigen des Kommentars auf den Link **Zugewiesen**.

Hinweis: Die Aktion **ServiceNow-Aufgabe erstellen** setzt auch das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**.

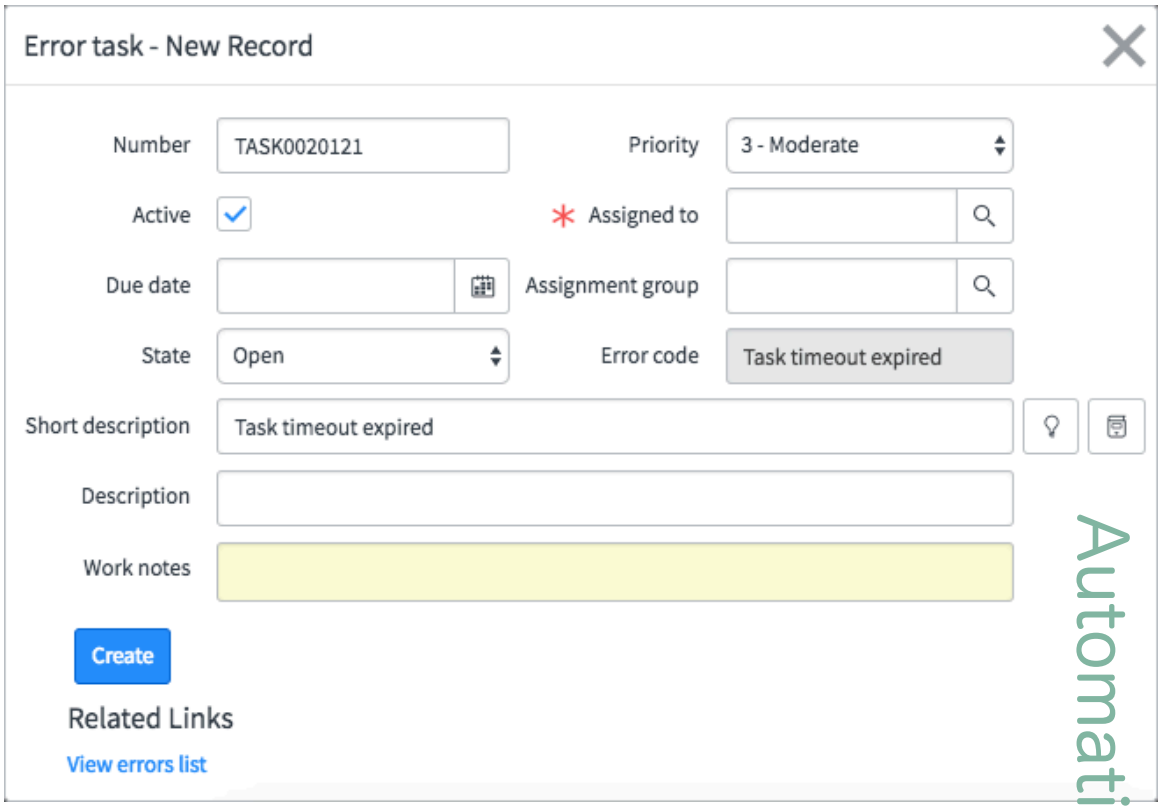
ServiceNow-Aufgabe erstellen

Öffnet das ServiceNow-Fehleraufgabenformular in einem Popup-Fenster, in dem Sie eine Aufgabe für die ausgewählten Fehler erstellen und zuweisen können. Setzt das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**. Informationen zum Erstellen von Fehleraufgaben finden Sie unter Eine Tabelle erstellen Und Erstellen Sie eine Aufgabe aus einem Incident, einem Problem oder einer Change-Anforderung .

Hinweis: Die Aktion **Als zugewiesen markieren** setzt auch das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Discovery erneut starten

Führt den kompletten Discovery-Prozess aus. Normalerweise führen Sie Discovery aus, nachdem Sie die Korrekturanweisungen befolgt haben, die angezeigt werden, wenn Sie auf **Anweisungen anzeigen** klicken.

Anweisungen anzeigen

Zeigt ein Problembehebungsverfahren in einem Popup-Fenster an. Führen Sie die Schritte aus, um den Fehler zu beheben.

Fehler ignorieren

Klicken Sie mit der rechten Maustaste auf einen Fehler, und wählen Sie dann **Fehler ignorieren** aus, um den Wert **Ignoriert** auf **true** zu setzen.

Das System führt die Aktion für die Elemente aus, zeigt zuerst **In Bearbeitung** und anschließend das Ergebnis (Erfolg oder Fehlschlag) der Aktion an. Wenn der Fehler behoben ist, wird das **Fehlerstatus**-Feld im Fehlerprotokoll auf **Gelöst** gesetzt.

Hinweis: Wenn eine Aktion (z. B. Discovery) im Gange ist, aber zu lange dauert, können Sie auf **Stopp** klicken, um sie anzuhalten.

7. Klicken Sie auf **Fertig**, um die Statusmeldung zu schließen.
8. Wenn Sie eine Aktion für eine Auswahl ausgeführt haben und der Fehler behoben wurde, können Sie auf **Alle korrigieren** klicken, um die gleiche Aktion auf alle Elemente in der Liste anzuwenden.

Fehler in individuellen Anwendungsservicezuordnungen beheben

Sie können Erkennungsprobleme in jeder Anwendungsservicezuordnung einzeln behandeln.

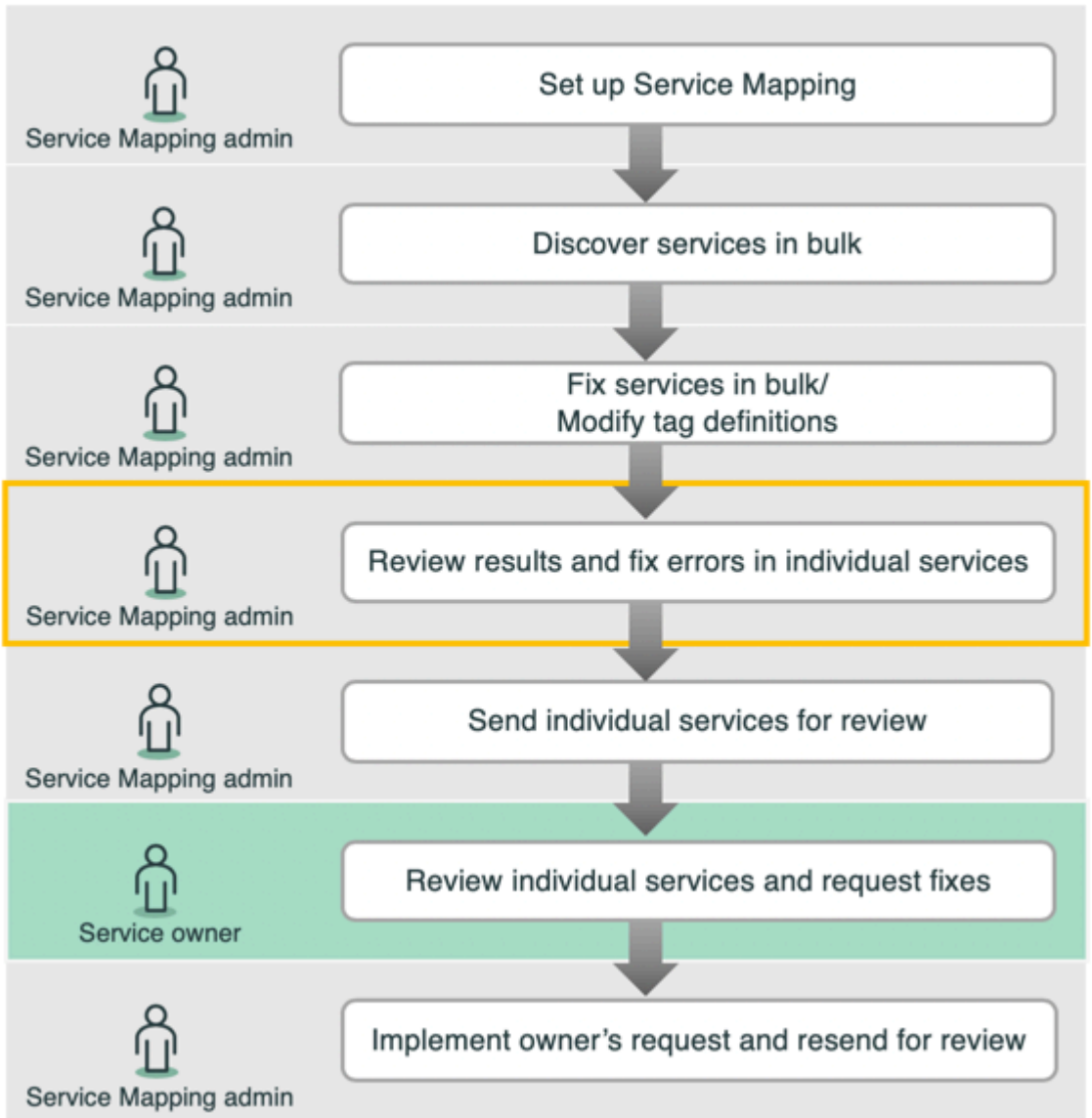
Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Sie können Fehler in einzelnen Anwendungsservices jederzeit beheben. Nach der ersten Zuordnung von Anwendungsservices in Ihrer Organisation beheben Sie normalerweise Fehler in einzelnen Anwendungsservices, nachdem Sie Fehler in mehreren Services als Massenvorgang behoben haben. Möglicherweise müssen Sie aber auch noch später Fehler in einem genehmigten und abgeschlossenen Anwendungsservice beheben.

Service-Mapping-Workflow

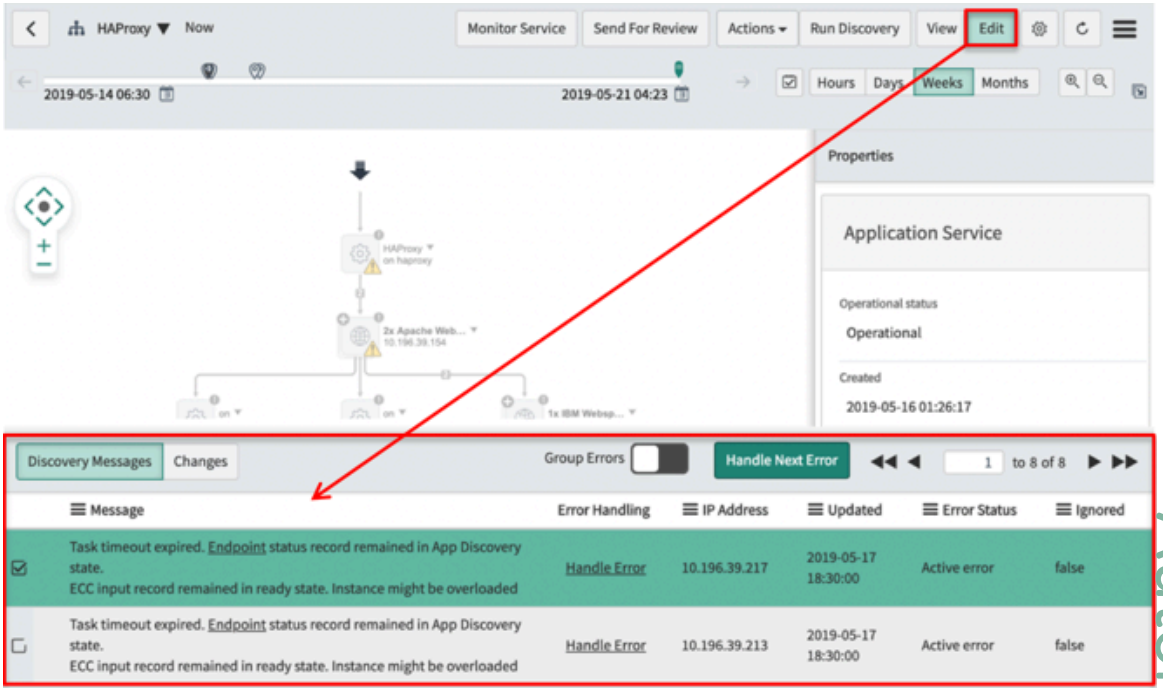


Automatische Übersetzung

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Fehlerhafte CIs werden mit dem Warnsymbol (⚠) auf der Karte angezeigt. Discovery-Nachrichten auf der Registerkarte **Discovery-Nachrichten** bieten kurze Fehlerbeschreibungen.

3. **Wahlweise:** Gruppieren Sie Fehler nach Typen, indem Sie auf **Fehler gruppieren** klicken.
   Die Erkennungsfehlermeldungen auf der Registerkarte **Discovery-Nachrichten** sind nach vordefinierten Typen (Fehlercodes) sortiert.
4. Um einen Fehler aus der Liste zu prüfen und zu beheben, klicken Sie auf **Fehler behandeln** neben der Fehlerbeschreibung.
   Oder
5. Um den ersten Fehler in der größten Fehlergruppe zu prüfen, klicken Sie in der Zuordnung oben links auf **Nächsten Fehler behandeln**.
6. Um zu erfahren, wie der Fehler behoben werden kann, klicken Sie im rechten Fensterbereich unter **Aktion für Auswahl** auf **Anweisungen öffnen**.

   Hinweis: Anweisungen sind nur für die am häufigsten vorkommenden Fehler verfügbar.

7. Klicken Sie auf die entsprechende halbautomatisierte Lösungsoption, um den Fehler im rechten Fensterbereich unter **Aktion für Auswahl** zu beheben.
   Die Fehlerlösungsoptionen variieren, da sie vom spezifischen Erkennungsfehler abhängen, der dem ausgewählten CI zugeordnet ist.

Verwenden Sie diese Option	Zu diesem Zweck
Management-IP hinzufügen	Geben Sie die Management-IP ein, um eine Erkennung für die Hostressourcen und -verbindungen auszulösen. Normalerweise benötigen Sie diese Lösung für Anwendungsservices, die nicht erkannte Geräte wie Lastenausgleichsmodule als Einstiegspunkte haben. Die Management-IP-Adresse eines Netzwerkgeräts ist die Adresse, die Sie verwenden, um das Gerät

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie diese Option	Zu diesem Zweck
	über SNMP oder ein anderes Verwaltungsprotokoll zu erreichen. **Hinweis:** Das System speichert die von Ihnen konfigurierte Management-IP nicht.
Neue WMI-Anmeldeinformationen erstellen	Öffnen Sie das Windows-Anmeldeinformationsformular, und konfigurieren Sie fehlende Windows-Anmeldeinformationen für das ausgewählte CI. Siehe Windows-Anmeldeinformationen .
Neue SSH-Anmeldeinformationen erstellen	Öffnen Sie das SSH-Anmeldeinformationsformular, und konfigurieren Sie fehlende SSH-Anmeldeinformationen für das ausgewählte CI. Siehe SSH-Anmeldeinformationen .
Neuen privaten SSH-Schlüssel erstellen	Öffnen Sie das Formular für private SSH-Schlüssel, und konfigurieren Sie die fehlenden Anmeldeinformationen für das ausgewählte CI. Siehe Anmeldeinformationstyp des privaten SSH-Schlüssels .
Neue SNMP-Anmeldeinformationen erstellen	Öffnen Sie das SNMP-Anmeldeinformationsformular, und konfigurieren Sie fehlende SNMP-Anmeldeinformationen für das ausgewählte CI. Siehe SNMP-Anmeldeinformationen .
Discovery-Protokoll anzeigen	Im Protokoll erfahren Sie, in welcher Phase ein Fehler aufgetreten ist und was ihn verursacht hat.
Überspringen und fortsetzen	Fügen Sie das CI, dessen Erkennung fehlgeschlagen ist, manuell hinzu, und konfigurieren Sie Attribute des Einstiegspunkts, ab dem Service-Mapping die Erkennung fortsetzen soll. Weitere Informationen finden Sie unter Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren.
Erkennung wiederholen	Führen Sie den Erkennungsprozess für das ausgewählte CI aus, nachdem Sie versucht haben, einen zugehörigen Erkennungsfehler zu beheben.
Betroffene Services anzeigen	Zeigen Sie eine Liste aller Services an, die vom ausgewählten Fehler betroffen sind. Klicken Sie in der Liste auf einen Service, um Servicedetails anzuzeigen.

8. Wenn keine Anweisungen oder halbautomatisierte Lösungsoptionen verfügbar sind, beheben Sie die Fehler auf Basis der Symptome und Erkennungsmeldungen.
9. Zum Ignorieren eines irrelevanten Fehlers klicken Sie mit der rechten Maustaste auf die entsprechende Fehlermeldung auf der Registerkarte **Discovery-Nachrichten** und wählen Toggle Ignore State (Ignorieren-Status umschalten).
   Der ignorierte Fehler verschwindet aus der Zuordnung und aus der Liste der Erkennungsfehlermeldungen.

   Hinweis: Bei Bedarf können Sie ignorierte Fehler trotzdem anzeigen, indem Sie die Option **Ignorierte Fehler einschließen** im Menü **Weitere Optionen** aktivieren. Weitere Informationen finden Sie unter Ansicht für Anwendungsservicezuordnung ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Um den nächsten Fehler in der größten Fehlergruppe zu prüfen, klicken Sie auf **Nächsten Fehler behandeln**.
11. Wenn Sie mit dem Überprüfen und Behandeln von Fehlern fertig sind, klicken Sie auf eine beliebige Stelle in der Zuordnung, um den Bereich **Fehler beheben** zu schließen.

Nächste Maßnahme

Wenn Sie die meisten Fehler gelöst haben, Senden Sie Serviceinstanz Zur Überprüfungan.

Zugehörige Informationen

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Fehler in einzelnen Anwendungsservices mithilfe von Discovery-Nachrichten beheben

Service-Mapping bietet keine halbautomatisierten Lösungsoptionen für Fehler, die eine erweiterte Lösung erfordern. Beheben Sie solche Fehler mithilfe von Symptomen und Erkennungsmeldungen.

Vorbereitungen

Versuchen Sie, Fehler mit halbautomatisierten Lösungsoptionen zu beheben, wie in Fehler in individuellen Anwendungsservicezuordnungen beheben beschrieben.

Erforderliche Rolle: Service_Mapping_admin

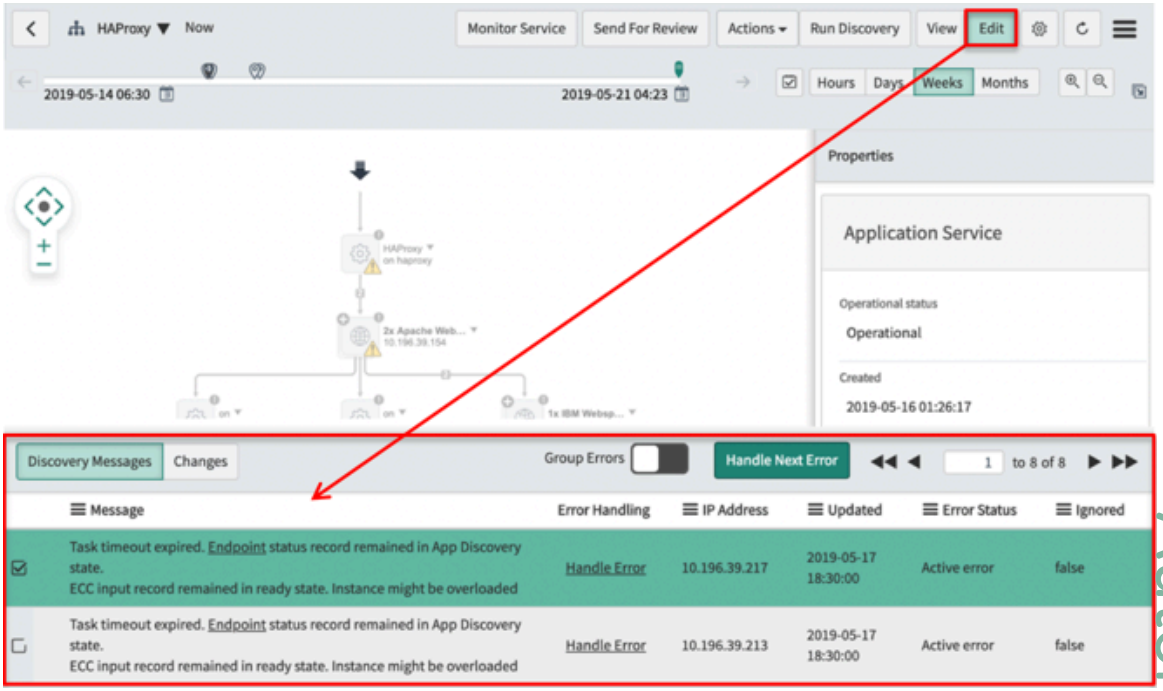
Warum und wann dieser Vorgang ausgeführt wird

Sie können Fehler in einzelnen Anwendungsservices jederzeit beheben.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie Auf **Karte Anzeigen** Neben der relevanten Serviceinstanz.
3. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Fehlerhafte CIs werden mit dem Warnsymbol (⚠) auf der Karte angezeigt. Discovery-Nachrichten auf der Registerkarte **Discovery-Nachrichten** bieten kurze Fehlerbeschreibungen.

4. Beheben Sie Fehler basierend auf den Symptomen und Erkennungsmeldungen.

Symptom	Lösung
Die folgende Erkennungsmeldung wird angezeigt: Die Zuordnung zeigt nicht den gesamten Service an, da er zu groß ist. Die Anzahl der CI-Verbindungen hat das zulässige Maximum überschritten.	Reduzienen Sie die Größe des Anwendungsservice. ○ Führen Sie für einen Anwendungsservice, der mit musterbasierter und datenverkehrsbasierter Erkennung zugeordnet ist, die folgenden Aktionen aus: ▪ Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen. ▪ Teilen Sie den Service in kleinere Services auf. ○ Führen Sie für einen Anwendungsservice, der aus einem Anwendungsservice umgewandelt wurde, die folgenden Aktionen aus: ▪ Überprüfen Sie die konvertierte Serviceinstanz, um CI-Beziehungen zu identifizieren, die für diesen Service irrelevant oder redundant sind. Entfernen Sie solche CI-Beziehungen in der CMDB.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
	▪ Entscheiden Sie, wie viele Ebenen zugehöriger CIs Sie in diese Serviceinstanz aufnehmen müssen. Ändern Sie bei Bedarf die Anzahl der bei der Konvertierung verwendeten Ebenen, um die Servicegröße zu reduzieren.
Die folgende Discovery-Nachricht wird in einer Tag-basierten Serviceinstanz angezeigt: *This tag-based service instance reached the maximum number of CIs. For more information, refer to the product documentation.*	Führen Sie die folgenden Aktionen aus: ○ Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen Um sicherzustellen Service-Mapping Schließt nur relevante CIs in der Serviceinstanz ein. ○ Falls erforderlich, Tag-basierte Discovery-Konfiguration Um zu ändern, welche CIs Service-Mapping Enthält in Tag-basierten Serviceinstanzen.
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ○ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: Fehler beim Ausführen des Befehls mit sudo auf dem Host <IP-Adresse des Hosts>.	KB0621669: Resolving failure to execute commands using sudo during Discovery in Service Mapping (Fehler beim Ausführen von Befehlen mit sudo während der Erkennung in Service Mapping beheben)
Die folgende Fehlermeldung wird für das Konfigurationselement angezeigt: Zugriff verweigert.	KB0564283: Resolving an issue of denied access to a Windows Server (Problem mit verweigertem Zugriff auf einen Windows-Server beheben)
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Windows-Servers an. ○ Die folgende Erkennungsmeldung für den Windows-Server angezeigt: RPC-Server nicht verfügbar.	KB0564282: Resolving issue of RPC Server unavailable during Windows Server discovery in Service Mapping (Problem eines nicht verfügbaren RPC-Servers während der Windows Server-Ermittlung in Service Mapping beheben)
○ In der Serviceinstanz -Zuordnung wird anstatt des Lastenausgleichsmodul-CI das Warnsymbol ⚠ angezeigt. ○ Die folgende Erkennungsmeldung wird angezeigt: Service Mapping hat eine horizontale Erkennung ausgelöst, um den Host x.x.x.x zu finden, da dieser Host nicht in der CMDB war. Die horizontale Erkennung ist fehlgeschlagen. Weitere Informationen finden Sie unter Erkennungsstatus.	KB0610414: Resolving failure to discover operating system for a load balancer (Fehler beim Erkennen des Betriebssystems für ein Lastenausgleichsmodul beheben)
Anstelle der Zuordnung wird die folgende Erkennungsmeldung angezeigt: Die Zuordnung	KB0596671: Lösung eines großen Topologieproblems in Serviceinstanz Zuordnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
kann nicht angezeigt werden. Topologie zu groß.	
Eine virtuelle IP (VIP) für das Service-CI eines Lastenausgleichsmoduls wird manchmal mit den IP-Adressen eines anderen Lastenausgleichsmoduls aktualisiert.	KB0610412: Resolving load balancers merging into one CI in Service Mapping (Zusammenführung von Lastenausgleichsmodulen in ein einzelnes CI in Service Mapping beheben)
Die Zuordnung zeigt für Lastenausgleichsmodule falsche virtuelle IP-Namen an.	KB0610413: Resolving incorrect virtual IP names of load balancers in Service Mapping (Falsche virtuelle IP-Namen von Lastenausgleichsmodulen in Service Mapping beheben)
Die Serviceinstanz -Zuordnung besteht jedes Mal aus verschiedenen CIs, wenn Sie den Zuordnungsprozess für dieselben Einstiegspunkte ausführen, um denselben Serviceinstanz zu erkennen.	KB0595227: Troubleshooting inconsistent mapping results (Problembehandlung bei inkonsistenten Zuordnungsergebnissen)
In der Serviceinstanz -Zuordnung ist kein Lastenausgleichsmodul-CI vorhanden. Es gibt Verbindungen, die direkt vom Einstiegspunkt des Serviceinstanz zu den CIs der nächsten Ebene wechseln. Die übrigen CIs verschwinden ebenfalls aus der Zuordnung.	KB0621529: Resolving the issue of a load balancer disappearing from the application service map (Problem, dass ein Lastenausgleichsmodul nicht mehr in der Anwendungsservicezuordnung angezeigt wird, lösen)
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ○ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: Timeout des SSH-Befehls auf dem Host.	KB0621670: Resolving the issue of SSH command time-out during discovery in Service Mapping (Problem einer Zeitüberschreitung des SSH-Befehls während der Erkennung in Service Mapping lösen)
Ein Cluster-CI wird getrennt von allen CIs in den darüber oder darunter liegenden Zuordnungsebenen angezeigt.	KB0621531: Auflösen getrennter Cluster-CIs auf dem Serviceinstanz Zuordnen
○ In der Zuordnung wird entweder das Konfigurationselement (CI) des Lastenausgleichsmoduls mit einem Warnsymbol oder nur das Warnsymbol ⚠ angezeigt. ○ Die folgende Erkennungsmeldung wird für das CI angezeigt, das als Lastenausgleichsmodul im Serviceinstanz fungieren soll: Anwendung wurde nicht erkannt. Weitere Details finden Sie im Erkennungsprotokoll.	KB0621576: Resolving failure to discover VIP for a load balancer (Fehler beim Erkennen des VIP für ein Lastenausgleichsmodul beheben)
Die Serviceinstanz -Zuordnung zeigt ein anderes Lastenausgleichsmodul als das, das Sie in diesem Anwendungsservice erwartet haben.	KB0621616: Business service map displays a wrong load balancer in Service Mapping (Business Service-Übersicht in Service Mapping zeigt ein falsches Lastenausgleichsmodul an)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ○ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: Timeout des SSH-Befehls auf dem Host.	KB0621670: Resolving the issue of SSH command time out during discovery in Service Mapping (Problem einer Zeitüberschreitung des SSH-Befehls während der Erkennung in Service Mapping lösen)
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ○ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: Kein aktiver MID Server für IP X.X.X.X gefunden	KB0622808: Resolving a failure to find a MID Server for an IP address (Fehler bei der Suche nach einem MID Server für eine IP-Adresse beheben)
○ Die Serviceinstanz -Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ○ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: „64\rctrlx“ wird nicht als interner oder externer Befehl, ausführbares Programm oder Batch-Datei erkannt.	Führen Sie das unter Datei rctrlx.exe auf MID Servers hochladen beschriebene Verfahren aus.
Ein CI oder ein Segment der Zuordnung ist ausgegraut, nachdem Service-Mapping die Erkennung von oben nach unten für einen zuvor zugeordneten Serviceinstanz ausgeführt hat. In diesem Anwendungsservice konnte das CI bzw. konnten die Verbindungen, die zu diesem CI führten, von Service-Mapping nicht erneut erkannt werden.	Führen Sie die nachfolgenden Schritte durch: **a.** (Optional für ausgegraute Segmente) Identifizieren Sie das fehlerhafte CI, das zum Ausgrauen des Segments führt. **b.** Verwenden Sie die Erkennungsmeldung, die diesem fehlerhaften CI zugeordnet ist, um das Problem zu lösen.

5. Klicken Sie auf **Discovery ausführen**.

Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren

Wenn Sie wissen, aus welchen Konfigurationselementen (Configuration Items, CIs) und Verbindungen Ihre Serviceinstanz besteht, können Sie aktivieren Service-Mapping Um die Discovery der Serviceinstanz fortzusetzen, auch wenn Fehler auftreten. Sie können Fehler überspringen, um die Fehlerbehebung später zu beheben, sodass Sie die Zuordnung des größten Teils der Serviceinstanz abschließen können, auch wenn einige CIs fehlen.

Vorbereitungen

Machen Sie sich mit der Struktur des Anwendungsservice vertraut, um zu erfahren, welche CIs die nächste Ebene nach dem problematischen CI bilden. Wenden Sie sich bei Bedarf an den Anwendungsservice-Eigentümer, um die erforderlichen Informationen zu erhalten.

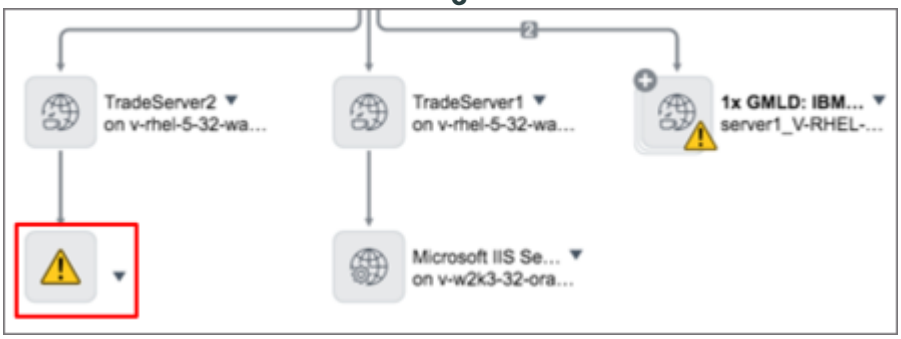
Erforderliche Rolle: Service_Mapping_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Normalerweise wird die Erkennung eines Anwendungsservices beendet, wenn Service-Mapping ein CI nicht identifizieren kann. In diesem Fall wird in der Zuordnung anstelle des nicht erkannten CI ein Warnungssymbol angezeigt. Das nicht erkannte CI enthält keine CIs oder ausgehenden Verbindungen.

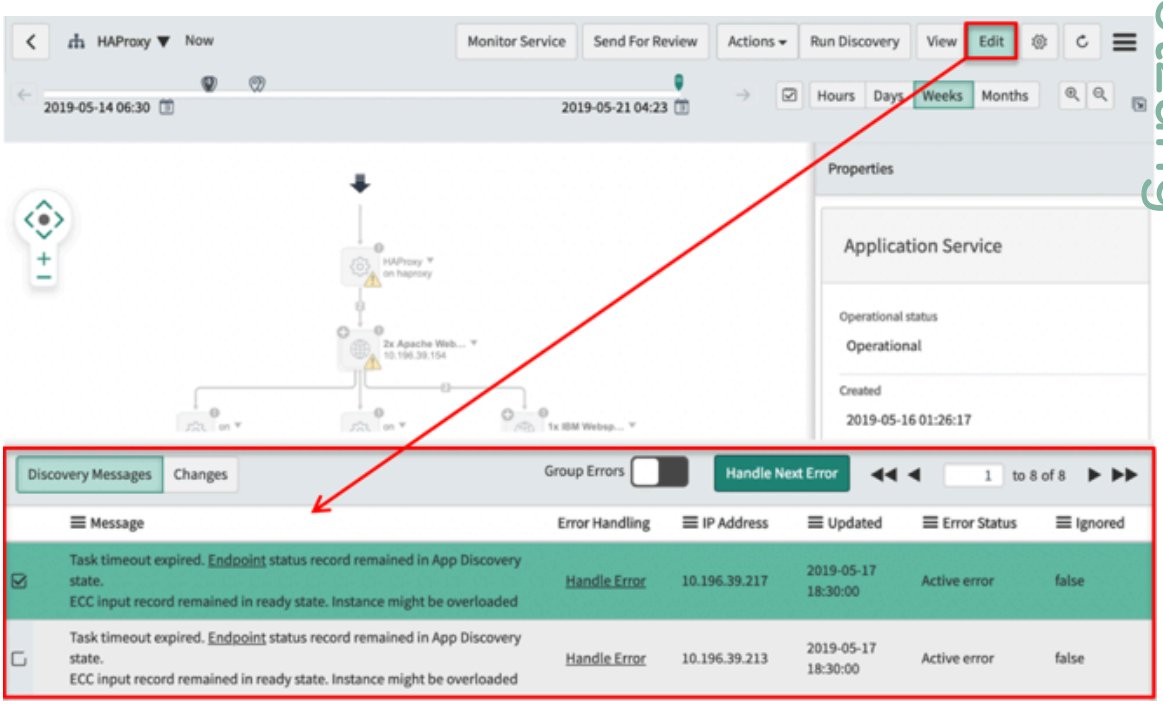
Nicht erkanntes CI in der Zuordnung



Sie können das Problem des nicht erkannten CI überwinden und die Erkennung von den CIs aus neu starten, die zur nächsten Ebene hinter dem problematischen CI gehören. Fügen Sie dazu manuell ein CI hinzu, wenn Sie wissen, welches das nicht erkannte CI ist und was die eingehende Verbindung des CI der nächsten Ebene ist. Service-Mapping verwendet während der Erkennung eingehende Verbindungen für den Zugriff auf ein CI. Diese Verbindungen werden als Endpunkte bezeichnet.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Stellen Sie sicher, dass sich die Zuordnung nicht in der Host-Ansicht befindet.
4. Klicken Sie auf den Pfeil neben dem nicht erkannten CI, und wählen Sie **Überspringen und fortsetzen**.
5. Definieren Sie Attribute des CI, das Sie anstelle des nicht erkannten CI manuell platzieren möchten.

Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. `cmdb_ci_appl` für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

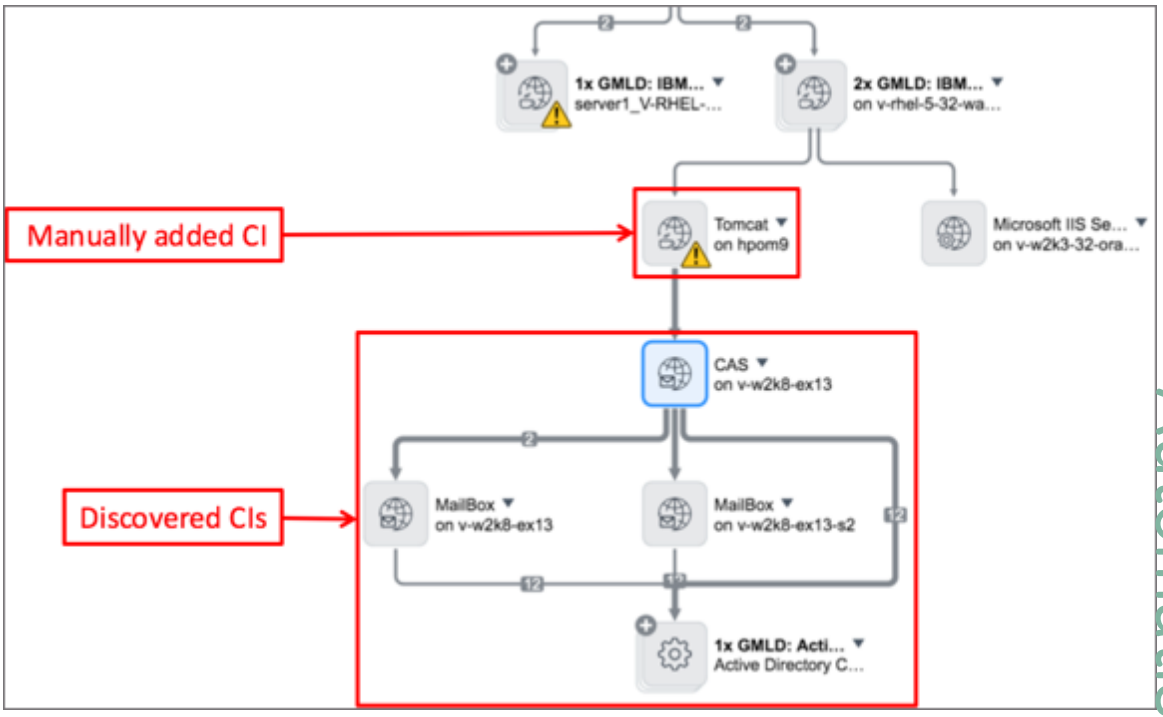
Hinweis:

Wenn der CI-Typ nicht in der Liste angezeigt wird, lässt Service-Mapping das manuelle Hinzufügen von CIs dieses Typs nicht zu. Sie können beispielsweise keinen Anwendungscluster oder Endpunkt manuell hinzufügen.

6. Konfigurieren Sie Attribute des Einstiegspunkts, ab dem Service-Mapping fortgesetzt wird, indem Sie den Einstiegspunkttyp auswählen und relevante Felder eingeben.
   Wenn der erforderliche Einstiegspunkttyp nicht in der Liste „Einstiegspunkttyp auswählen“ angezeigt wird, müssen Sie ihn wie in Einstiegspunkttypen für Service-Mapping erstellen beschrieben erstellen.
7. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Zuordnung zeigt das manuell hinzugefügte CI anstelle des nicht erkannten CI. Service-Mapping startet die Erkennung für CIs der nächsten Stufen. Nach Abschluss des Erkennungsprozesses zeigt die Zuordnung unter dem manuell hinzugefügten CI alle erkannten CIs an.



Nächste Maßnahme

So erkennen Sie das problematische CI automatisch:

1. Führen Sie die erforderliche Fehlerbehebung durch, damit Service-Mapping das problematische CI erkennen kann. Beispielsweise müssen Sie eventuell das relevante Muster anpassen, fehlende Anmeldeinformationen bereitstellen oder die datenverkehrsbasierte Erkennung optimieren.
2. Navigieren Sie zur betreffenden Serviceinstanz -Zuordnung.
3. Klicken Sie auf **Discovery ausführen**.
4. Überprüfen Sie nach Abschluss des Erkennungsprozesses, ob Service-Mapping das CI erkannt hat. Wenn Service-Mapping das CI erkannt hat, zeigt die Zuordnung das tatsächliche CI ohne das Warnsymbol (⚠) an.

Zugehörige Informationen

Von ITOM-Transparenz verwendete Erkennungsmuster

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Musterbezogene Zuordnungsfehler beheben

Sie können Zuordnungsfehler beheben, die durch Muster verursacht werden.

Service Mapping Teil 2 | Problembehandlung

Dieses Video bietet eine alternative Möglichkeit zur Behebung musterbezogener Fehler.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Überprüfen Sie in der Erkennungsmeldung, ob der Zuordnungsfehler tatsächlich auf ein falsches Muster zurückzuführen ist. Wenn die Meldung „Anwendung konnte nicht erkannt werden“ lautet, ist der Fehler musterbezogen.

Sie müssen mit dem Musterdesignermodul von Service-Mapping vertraut sein.

Erforderliche Rolle: admin und Service_Mapping_admin

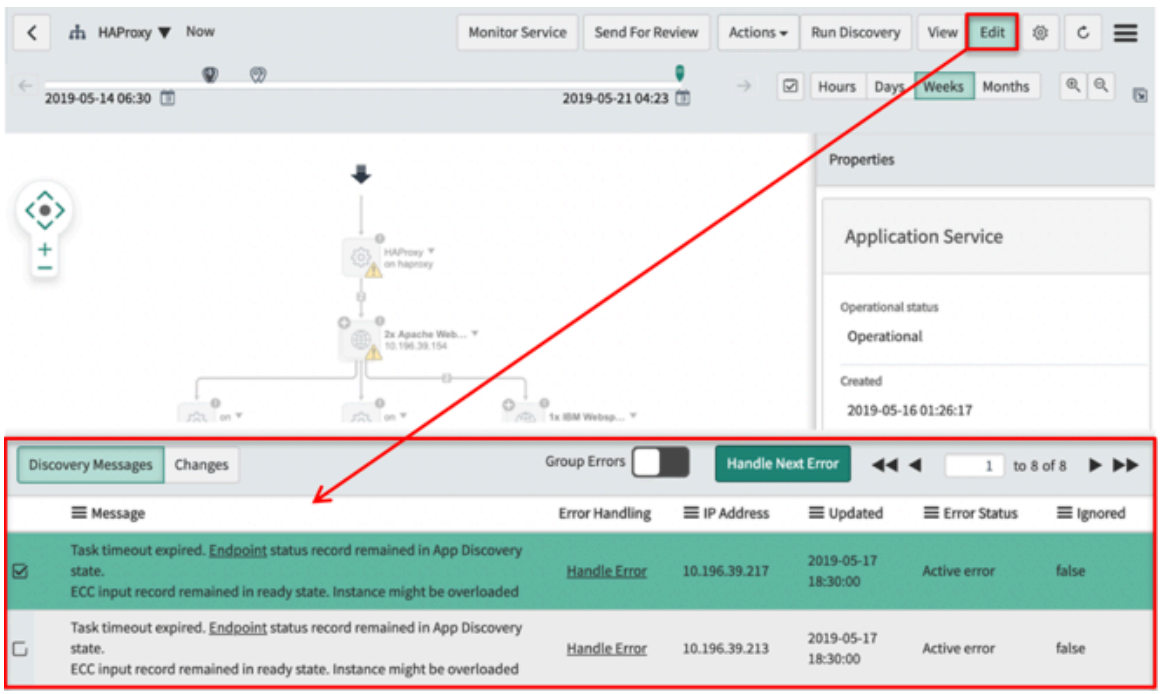
Warum und wann dieser Vorgang ausgeführt wird

Wenn Konfigurationselemente (CIs) vorhanden sind, die Service-Mapping nicht ordnungsgemäß zuordnen konnte, werden sie auf der Serviceinstanz -Zuordnung mit Warnsymbolen ⚠ angezeigt. In der Regel treten Zuordnungsfehler auf, wenn Service-Mapping keine Verbindung zu einem CI herstellen oder dieses aufgrund eines ungenauen Musters nicht erkennen kann.

Sie können problematische Schritte in Ihrem Muster identifizieren und beheben, ohne alle Schritte und Vorgänge im Muster zu überprüfen. So können Sie musterbezogene Fehler schnell und effektiv beheben.

Prozedur

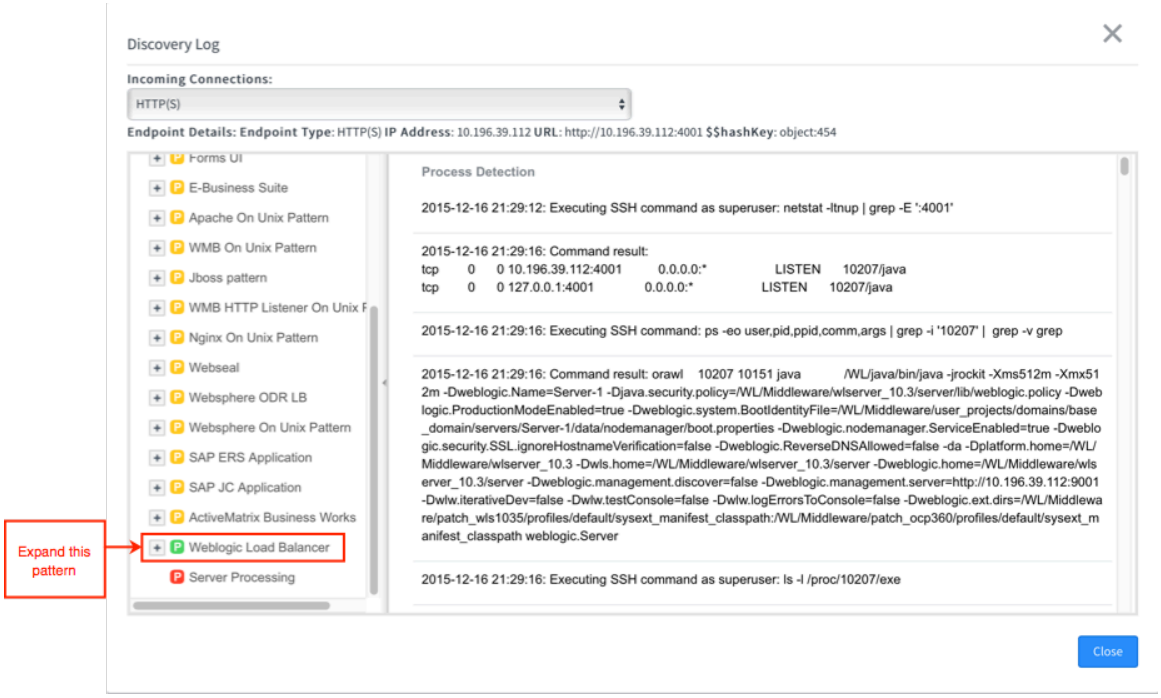
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird und Erkennungsmeldungen und Fehler anzeigt.



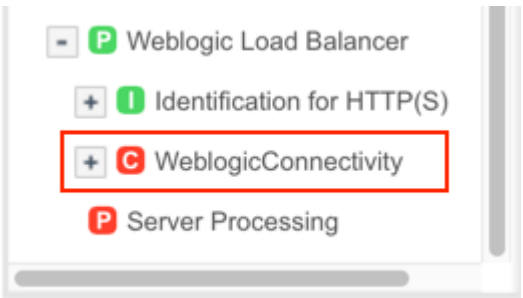
3. Klicken Sie mit der rechten Maustaste auf das CI mit dem Warnsymbol (⚠), und wählen Sie **Discovery-Protokoll anzeigen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erweitern Sie das fehlgeschlagene Muster, das über dem rot markierten Ergebnis angezeigt wird.



5. Erweitern Sie den fehlgeschlagenen Abschnitt, und klicken Sie auf den fehlgeschlagenen Schritt.

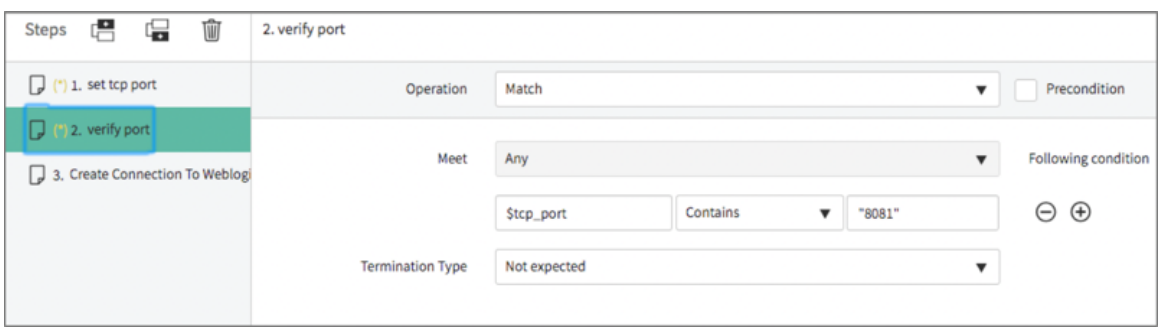


6. Klicken Sie auf **Debuggen**.

7. Klicken Sie auf den ersten Schritt, und warten Sie, bis der Musterdesigner ihn ausgeführt hat.

   Wiederholen Sie diese Aktion für weitere Schritte in der angegebenen Reihenfolge, bis Sie den fehlerhaften Schritt erreicht haben, der den Fehler verursacht.

   Im folgenden Beispiel lautet die Portnummer 8081 anstatt 8080, was das Problem verursacht.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **OK**.
9. Korrigieren Sie das Musterattribut, das das Problem verursacht.
10. Klicken Sie auf **Testen**.
11. Stellen Sie sicher, dass der Musterdesigner eine Erfolgsmeldung zurückgibt.
12. Klicken Sie auf **Speichern**.
13. Klicken Sie auf **Aktivieren**.
14. Kehren Sie zur Serviceinstanz -Zuordnung zurück, die den Zuordnungsfehler enthielt.
15. Klicken Sie mit der rechten Maustaste auf das CI, für das das Muster repariert wurde, und wählen Sie **Discovery fortsetzen**.
16. Stellen Sie sicher, dass das CI erkannt und richtig zugeordnet wird.

Anwendungsservicezuordnungen prüfen und genehmigen

Nachdem der Administrator Service-Mapping IT-Services zugeordnet und Fehler darin behoben hat, arbeiten der Administrator und der Eigentümer zusammen, um die Servicezuordnungen zu überprüfen und zu genehmigen. Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

Sie müssen haben Service-Mapping Aktiviert zum Zuordnen oder Überprüfen von Serviceinstanzen.

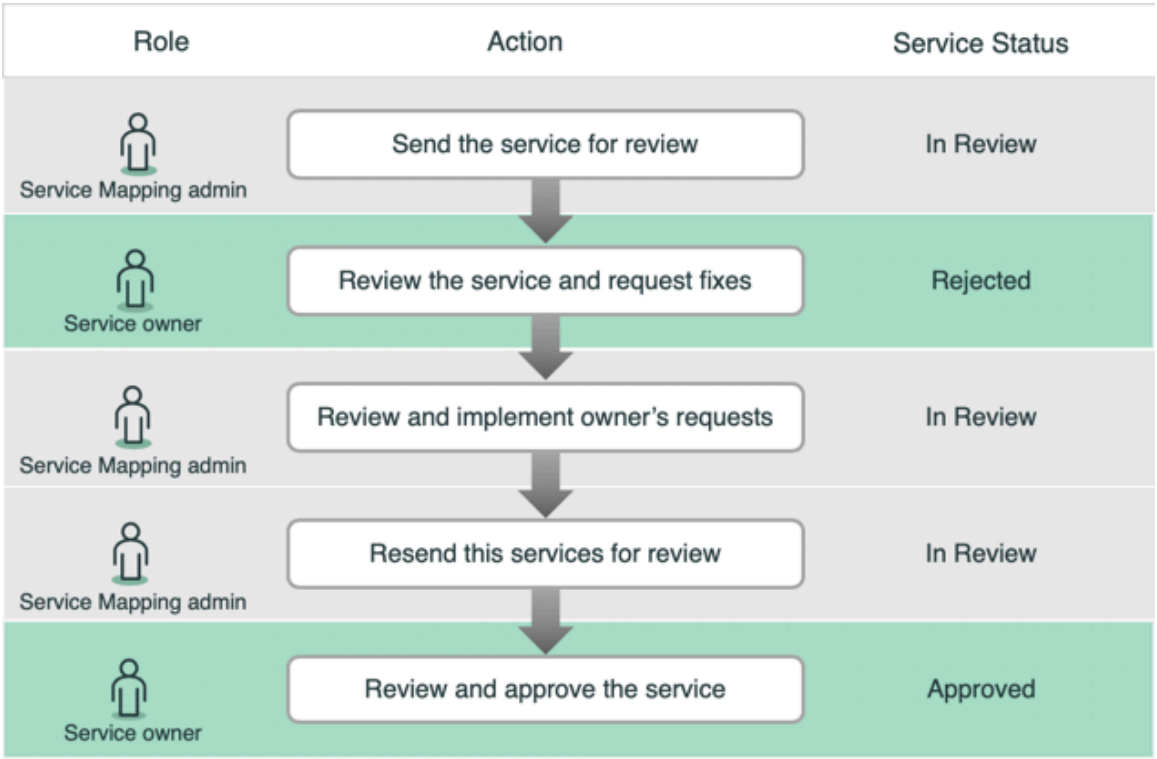
Benutzer, die die Überprüfung und Genehmigung durchführen, haben die Rollen eines Service-Mapping-Administrators. Ein Service-Mapping-Administrator ist für die Zuordnung, Korrektur und Wartung von Anwendungsservices verantwortlich. Der Besitzer der Serviceinstanz überprüft, ob die Zuordnungen der Serviceinstanz vollständig sind und alle Hauptkomponenten, aus denen sie besteht, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer Kommentare, die als Ablehnungsnachrichten bezeichnet werden, in Serviceinstanzzuordnungen für die Service-Mapping Zu implementierender Administrator.

Der Überprüfungs- und Genehmigungsprozess wird in den folgenden Phasen durchgeführt:

1. Nach der ersten Zuordnung von Serviceinstanzen behebt der Administrator Fehler und sendet einzelne Serviceinstanzen zur Überprüfung. Das System erstellt eine Serviceprozessaufgabe, die dem Serviceinstanzbesitzer zugewiesen ist, und sendet eine E-Mail-Benachrichtigung darüber.
2. Der Besitzer der Serviceinstanz überprüft, ob die Zuordnungen der Serviceinstanz vollständig sind und alle Hauptkomponenten, aus denen sie besteht, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer Kommentare, die als Ablehnungsnachrichten bezeichnet werden, in Serviceinstanzzuordnungen für die Service-Mapping Zu implementierender Administrator. Die dem Inhaber zugewiesene Serviceprozess-Aufgabe wird geschlossen. Das System sendet eine E-Mail-Benachrichtigung an den Administrator, dass der Inhaber Kommentare geschrieben hat.
3. Der Administrator erhält die E-Mail-Benachrichtigung, zeigt die Anforderungen des Besitzers an und implementiert sie.
4. Der Administrator sendet die Serviceinstanzzuordnungen erneut zur Überprüfung. Das System erstellt erneut eine Serviceprozessaufgabe, die dem Serviceinstanzbesitzer zugewiesen ist, und sendet eine E-Mail-Benachrichtigung darüber.
5. Wenn die überarbeiteten Serviceinstanzzuordnungen zufriedenstellend sind, genehmigt der Serviceinstanzbesitzer sie. Wenn nicht, fordert der Verantwortliche weitere Fehlerkorrekturen an, die der Administrator umsetzen muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie zum Anzeigen der Dokumentation für eine Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Senden Sie Serviceinstanz Zur Überprüfung
2. Business Service prüfen und Korrekturen anfordern
3. Anforderungen des Eigentümers prüfen und implementieren
4. Anwendungsservices erneut zur Überprüfung senden
5. Überprüfen und genehmigen Sie die Anwendungsservices

Die Prüfung des Anwendungsservice kann einige Zeit in Anspruch nehmen, da Änderungen erforderlich sind und der Zuordnungsprozess für den Anwendungsservice wiederholt ausgeführt werden muss. Normalerweise sind mehrere Iterationen erforderlich, um das gewünschte Ergebnis zu erzielen.

Sobald der Eigentümer einen Anwendungsservice genehmigt hat, ändert sich der Status des Anwendungsservice in „Genehmigt“ und er erscheint in der Liste der abgeschlossenen Anwendungsservices auf der **Startseite**.

Anwendungsservicezuordnungen zur Überprüfung senden

Nachdem Sie einen Anwendungsservice zugeordnet haben, senden Sie ihn zur Überprüfung an den Besitzer des Anwendungsservice, um sicherzustellen, dass die Zuordnung korrekt ist.

Vorbereitungen

Führen Sie eine erste Fehlerbehebung wie in Fehler bei Anwendungsservices als Massenvorgang beheben und Fehler in individuellen Anwendungsservicezuordnungen beheben beschrieben durch.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können zwar Fehler im Stapelverfahren beheben, müssen jedoch Anwendungsservices immer einzeln nacheinander zur Prüfung senden.

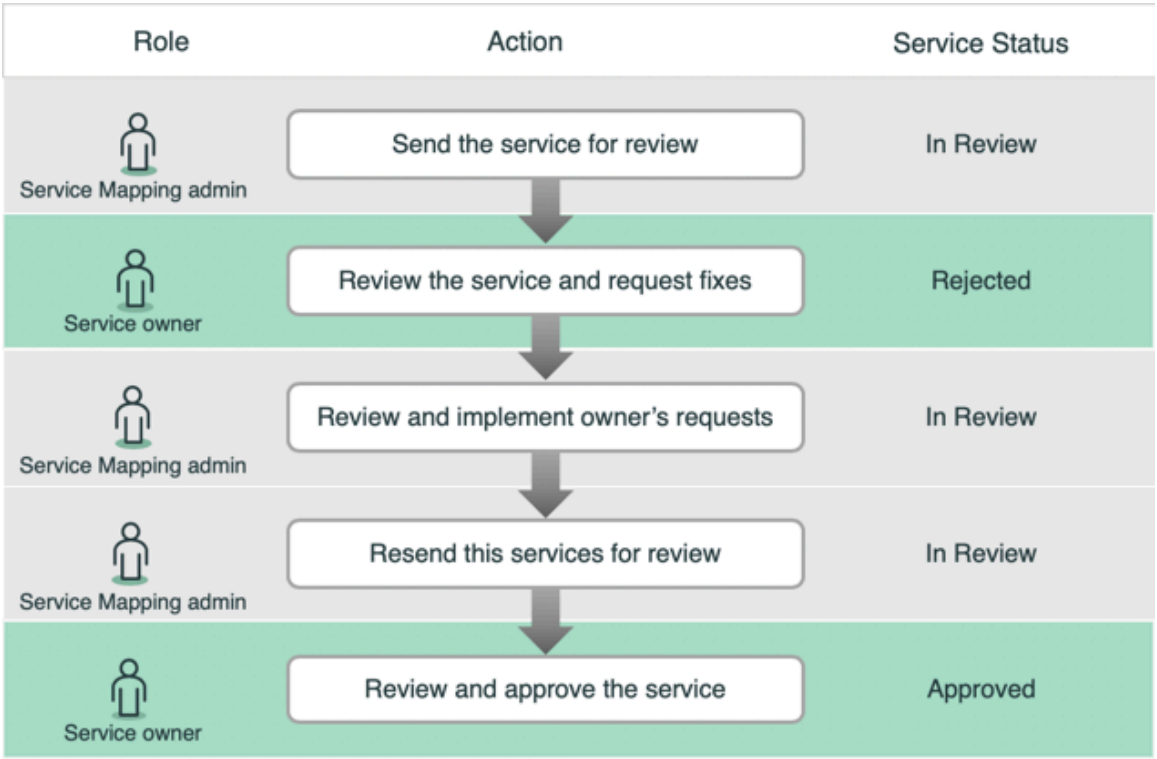
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Senden von Anwendungsservicezuordnungen zur Überprüfung ist Teil des Überprüfungs- und Genehmigungsprozesses. Normalerweise senden Sie jede Anwendungsservicezuordnung zweimal zur Überprüfung: Das erste Mal für die erste Prüfung durch den Eigentümer und das zweite Mal, nachdem Sie das Eigentümerfeedback implementiert haben.

Nach der erstmaligen Zuordnung der Anwendungsservices beheben Sie Fehler und senden einzelne Anwendungsservices zur Überprüfung. Das System erstellt eine Serviceprozessaufgabe, die dem Serviceinstanzbesitzer zugewiesen ist, und sendet eine E-Mail-Benachrichtigung darüber.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Überprüfung des folgenden Elements: Serviceinstanz Und Korrekturen anfordern
2. Anforderungen des Eigentümers prüfen und implementieren
3. Senden Sie erneut Serviceinstanz Zur Überprüfung
4. Überprüfen und genehmigen Sie Serviceinstanz

Prozedur

1. So senden Sie einen Serviceinstanz zur Überprüfung über das Serviceinstanz -Formular:
   a. Öffnen Sie die Serviceinstanzzuordnung.
   b. Sortieren Sie die Liste der geplanten Anwendungsservices nach Status und scrollen Sie, um die Services mit dem Status **in Bearbeitung** anzuzeigen, oder verwenden Sie den Filter, um die Liste einzugrenzen.
   c. Klicken Sie auf den erforderlichen Serviceinstanz .
   d. Klicken **Aktionen** > **Zur Überprüfung Senden**an.
2. Sie können einen Serviceinstanz auch über dessen Zuordnung zur Überprüfung senden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Service-Mapping** > **Startseite**an.
Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.

b. Klicken Sie auf die Kachel **Genehmigen**.

c. Klicken Sie auf **Zur Überprüfung senden**.

d. Klicken Sie auf den erforderlichen Serviceinstanz .
Die Zuordnung für diesen Serviceinstanz wird geöffnet.

e. Klicken Sie Auf **Zur Überprüfung Senden** In der oberen Ecke des Fensters.

Nächste Maßnahme

Wenn Sie eine E-Mail-Benachrichtigung erhalten, dass der Eigentümer Kommentare zu diesem Serviceinstanz gesendet hat, überprüfen und implementieren Sie die Anforderungen des Eigentümers.

Anwendungsservicezuordnungen prüfen

Als Eigentümer des Anwendungsservice für die Anwendungsservicezuordnung erhalten Sie eine E-Mail-Benachrichtigung, dass Ihnen die Anwendungsservicezuordnung zur Überprüfung zugewiesen ist. Überprüfen Sie die Zuordnungsergebnisse auf Richtigkeit, und geben Sie entweder Ihr Feedback ab, oder genehmigen Sie die Anwendungsservicezuordnung. Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

Vorbereitungen

Erforderliche Rolle: sm_app_owner

Warum und wann dieser Vorgang ausgeführt wird

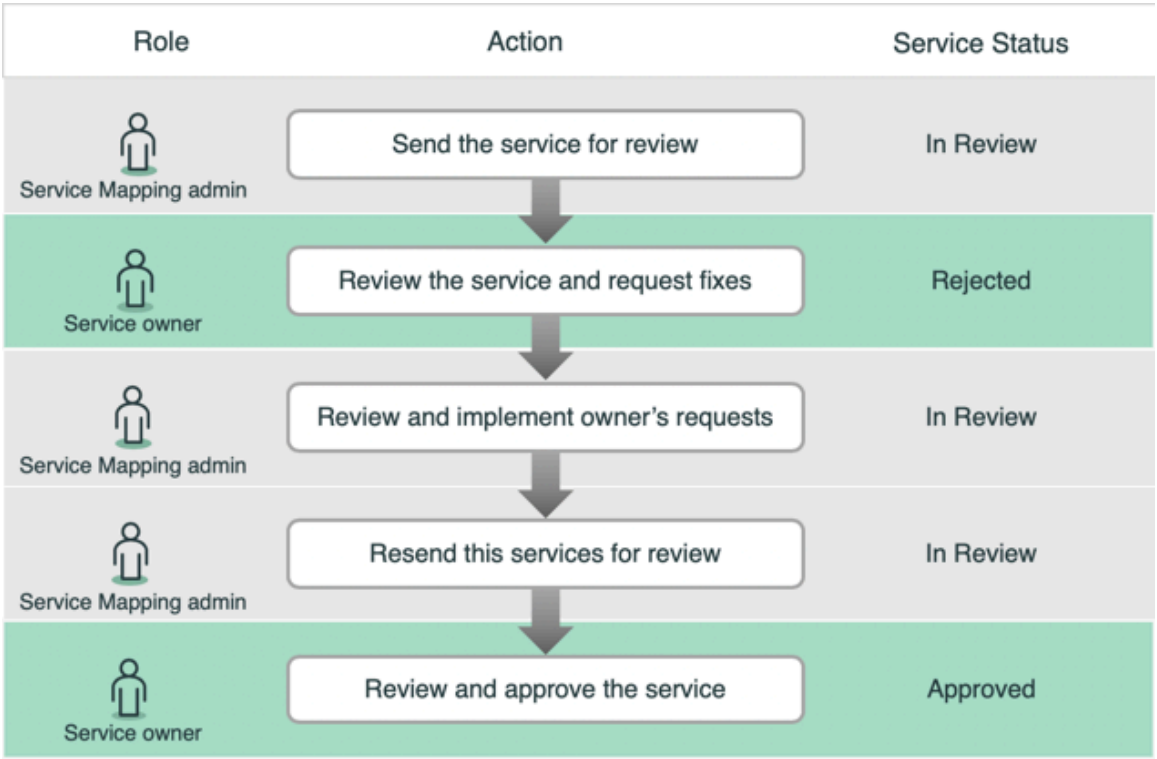
Idealerweise überprüft nur der Anwendungsserviceverantwortliche den geplanten Anwendungsservice. Benutzer mit der Rolle „sm_App_owner“ oder „Service_Mapping_admin“ können diese Aufgabe jedoch auch ausführen.

Das Überprüfen von Anwendungsservicezuordnungen ist Teil des Überprüfungs- und Genehmigungsprozesses. Die Prüfung des Anwendungsservice kann einige Zeit in Anspruch nehmen, da Änderungen erforderlich sind und der Zuordnungsprozess für den Anwendungsservice wiederholt ausgeführt werden muss. Normalerweise sind mehrere Iterationen erforderlich, um das gewünschte Ergebnis zu erzielen. Sobald Sie mit dem Ergebnis der Erkennung zufrieden sind, genehmigen Sie den Anwendungsservice.

Nachdem Sie Korrekturen angefordert oder den Anwendungsservice genehmigt haben, wird die Ihnen zugewiesene Serviceprozessaufgabe geschlossen.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



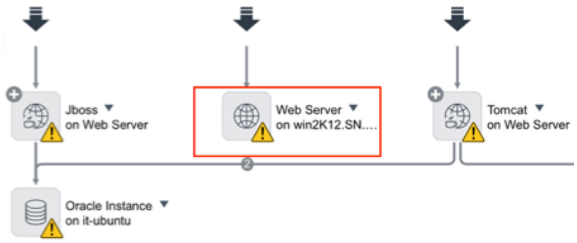
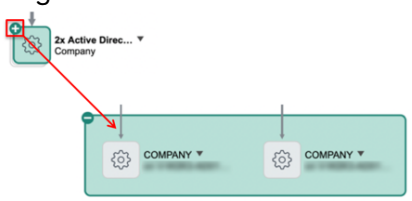
1. Anwendungsservice zur Überprüfung senden
2. Anforderungen des Eigentümers prüfen und implementieren
3. Anwendungsservices erneut zur Überprüfung senden

Prozedur

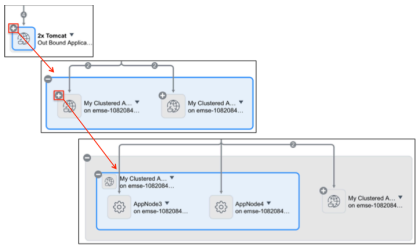
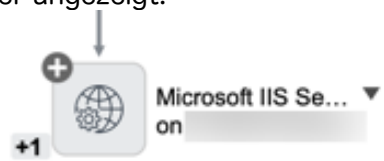
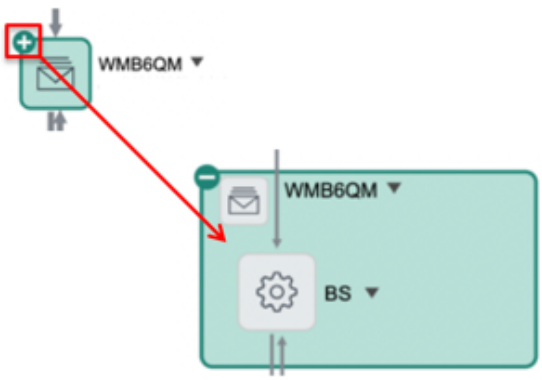
1. Klicken Sie auf den Link zur Anwendungsservicezuordnung in der E-Mail-Benachrichtigung.
   Die Zuordnung des Anwendungsservice wird in der ServiceNow-Instanz geöffnet.
2. Sie können den Anwendungsservice zur Prüfung auch aus der Liste der Ihnen zugewiesenen Aufgaben öffnen.
   a. Navigieren zu **Service-Mapping** > **Administration** > **Meine Aufgaben**an.
   b. **Wahlweise:** Sortieren Sie die Liste der Serviceprozessaufgaben nach Bedarf.
   c. Klicken Sie auf die erforderliche Aufgabe.
   d. Klicken Sie auf den Link des Anwendungsservice-Formulars.
   e. Klicken Sie auf **Karte anzeigen**.
3. Überprüfen Sie in der Anwendungsservicezuordnung, ob alle wichtigen CIs aus dem Anwendungsservice erkannt und korrekt zugeordnet wurden.

Zweck	Aktion
Stellen Sie sicher, dass keine CI-Verbindungen fehlen.	Achten Sie auf CIs ohne Connectors zu anderen CIs. Beispielsweise fehlen in der folgenden Abbildung beim CI win2K12 Verbindungen zum Webserver.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zweck	Aktion
	 Wenn Verbindungen und CIs, zu denen sie führen, fehlen, spiegelt die Zuordnung nicht den tatsächlichen Status desService-instanz und seinem Betrieb wider. Es kön–nen auch falsche Daten an Ereignismanage-ment übertragen werden, was zu einem un–genauen Monitoring führt.
Vergewissern Sie sich, dass nur CIs vorhanden sind, die zum Service gehören.	Überprüfen Sie alle CIs, die die Anwendungsser-vicezuordnung enthält, um CIs zu identifizieren, die nicht zu diesem Anwendungsservice gehören. In der Regel handelt es sich um Anwendungen, die inter-ne Services unterstützen. Beispielsweise ist die Ver-bindung zwischen Microsoft Internet Information Services (IIS) und Active Directory möglicherweise nicht Teil des Anwendungsservice.
Überprüfen Sie, ob die Verbindungen zwischen CIs korrekt sind.	Zeigen Sie CI-Verbindungsattribute in einer Anwen-dungsservicezuordnung an klassisch Service-Map-ping.
Überprüfen Sie, ob Cluster richtig dargestellt werden.	Klicken Sie auf das Pluszeichen (+) neben einem CI. Es gibt zwei Clustertypen: **Anwendungscluster** In einem Anwendungscluster sind zwei oder mehr Anwendungen oder Geräte so konfiguriert, dass sie zu-sammenarbeiten und denselben Zweck erfüllen. Normalerweise bieten Cluster Hochverfügbarkeit oder Las-tenausgleich. Ein Beispiel sind Web-server, die hinter einem Lastenaus-gleichsmodul arbeiten. Dieser Clustertyp wird als Sta–pel von CIs mit einer Bezeich–nung angezeigt, die die An–zahl der CIs in diesem Cluster mit dem Multiplikationszeichen zeigt. 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zweck	Aktion
	Anwendungscluster können ein Cluster innerhalb eines Clusters haben, jedoch nie mehr als zwei Ebenen:  **BS-Cluster** In einem BS-Cluster hostet ein Server zwei identische Betriebssysteme. Normalerweise bietet der Cluster ein Failover. Dieser Clustertyp wird als CI mit einem Pluszeichen und der Anzahl der CIs in diesem Cluster angezeigt. 
Überprüfen Sie, ob Inklusionen richtig dargestellt werden.	Klicken Sie auf das Pluszeichen (+) neben einem CI. Bei einer Inklusion hostet ein Server Anwendungen, die als unabhängige Objekte behandelt werden. Beispielsweise kann das virtuelle IIS-Verzeichnis auf einem Windows-Dienst als Host ausgeführt werden. 

4. Führen Sie die folgenden Schritte aus, um den Servicezuordnungsadministrator über eine erforderliche Änderung oder Korrektur zu benachrichtigen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie über der Zuordnung auf **Aktionen**.

b. Wählen Sie **Servicezuordnung ablehnen**.

c. Geben Sie im Fenster „Ablehnungsnachricht hinzufügen“ Ihren Kommentar ein, und klicken Sie auf **Hinzufügen**.
Der neue Kommentar wird auf der Registerkarte **Discovery-Nachrichten** unter der Zuordnung angezeigt. Der Status des Anwendungsservice wird in „Abgelehnt“ geändert.

d. Fügen Sie bei Bedarf weitere Kommentare hinzu.

5. Wenn Sie mit den Ergebnissen zufrieden sind, genehmigen Sie diesen Anwendungsservice, indem Sie auf **Aktionen** klicken und dann den **Service genehmigen**.
Der Status des Anwendungsservice ändert sich in „Genehmigt“ und er erscheint in der Liste der abgeschlossenen Anwendungsservices auf der **Startseite**. Der operative Status ändert sich in „Funktionsfähig“. Ab diesem Zeitpunkt können andere Anwendungen Daten verwenden, die von Service-Mapping gesammelt und organisiert wurden.

Zugehörige Informationen

Fehler in individuellen Anwendungsservicezuordnungen beheben

Anwendungsservices feinabstimmen, um Eigentümeranforderungen zu implementieren

Als Administrator bearbeiten und optimieren Sie Zuordnungen basierend auf Kommentaren des Eigentümers des Anwendungsservice.

Vorbereitungen
Erforderliche Rolle: Service_Mapping_admin

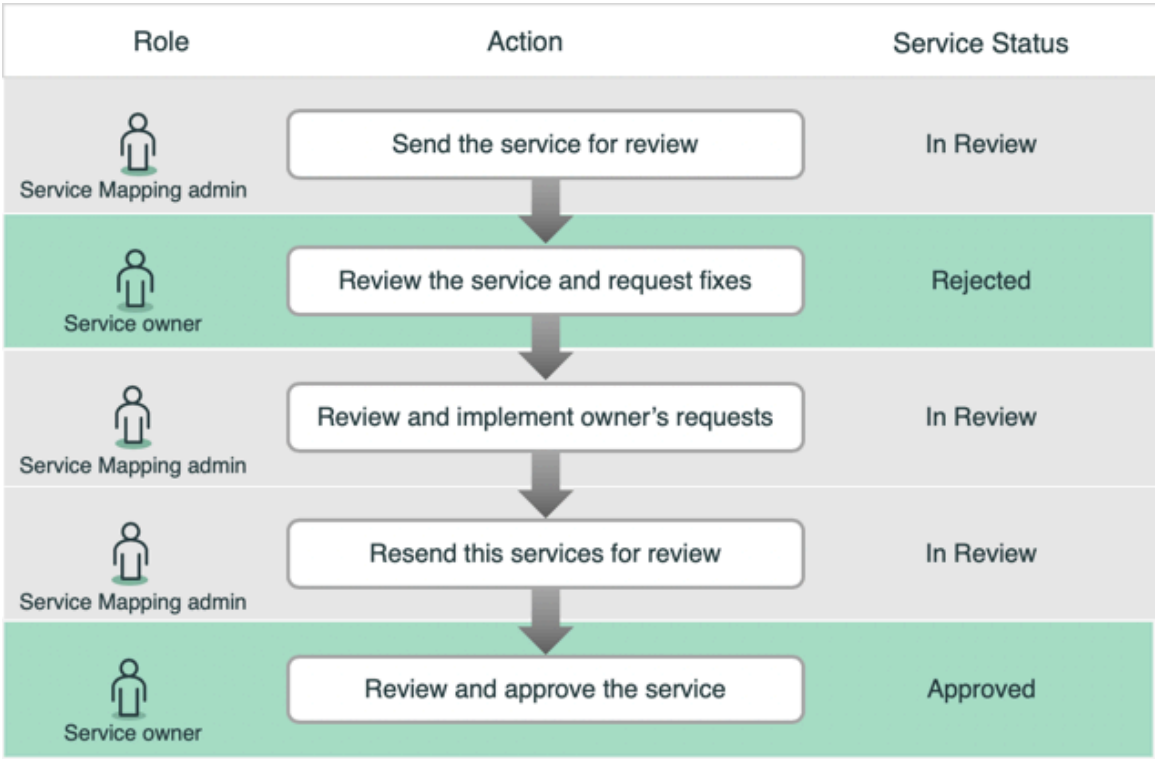
Warum und wann dieser Vorgang ausgeführt wird
Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Die Überprüfung von Eigentümeranforderungen ist Teil des Überprüfungs- und Genehmigungsprozesses.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



1. Senden Sie Serviceinstanz Zur Überprüfung
2. Überprüfung des folgenden Elements: Serviceinstanz Und Korrekturen anfordern
3. Anwendungsservices erneut zur Überprüfung senden
4. Überprüfen und genehmigen Sie Serviceinstanz

Prozedur

1. Navigieren Sie zu dem entsprechenden Anwendungsservice.

   a. Klicken Sie auf der **Startseite** auf **Genehmigen**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.

   b. Klicken Sie auf **Reparatur abgelehnt**.

   c. Klicken Sie mit der rechten Maustaste auf den erforderlichen Anwendungsservice und wählen Sie **Serviceformular öffnen**.
   Das Formular für diesen Anwendungsservice wird geöffnet.

2. Klicken Sie links auf **Nachrichten ablehnen**.
   Die Eigentümerkommentare werden auf der Registerkarte **Service-Discovery-Nachrichten** angezeigt.
3. Überprüfen Sie die Ablehnungsnachrichten, um Kommentare anzuzeigen, die der Eigentümer des Anwendungsservice hinterlassen hat.
4. Klicken Sie auf **Karte anzeigen**.
5. Implementieren Sie die vom Eigentümer des Anwendungsservice angeforderten Änderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf die Discovery-Nachricht, die den von Ihnen behobenen Servicefehler beschreibt, und klicken Sie rechts unter **Aktion für Auswahl** auf **Als gelöst markieren**.
7. Senden Sie den Anwendungsservice gegebenenfalls erneut zur Überprüfung.

CIs einem Anwendungsservice manuell hinzufügen

Fügen Sie Konfigurationselemente zu manuell erstellten Anwendungsservices oder zu von erkannten Services hinzu Service-Mapping.

Vorbereitungen

- Überprüfen Sie, ob der CI-Typ für das Konfigurationselement (CI) vorhanden ist, das Sie hinzufügen möchten. Erstellen Sie bei Bedarf den CI-Typ wie in beschrieben Erstellen Sie CI-Typen für Service-Mapping und Discovery .
- Fügen Sie bei Bedarf für das Gerät oder die Anwendung, die Sie hinzufügen möchten, der CMDB CIs hinzu. Siehe Füllen Sie die CMDB aus Weitere Informationen finden Sie unter .

Erforderliche Rolle: App_Service_admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Um einem Anwendungsservice ein CI hinzufügen zu können, muss eine Beziehung zwischen dem neuen CI und einem CI in dem Anwendungsservice erstellt werden. Sie können einem manuell erstellten Anwendungsservice auf eine der folgenden Arten CIs hinzufügen:

- Methode zum Füllen des Anwendungsservice hinzufügen

  Navigieren zu **CSDM** > **Technologiemanagement-Services verwalten** > **Anwendungsservice**an. Wählen Sie einen Anwendungsservice aus, und wählen Sie dann auf der Registerkarte **Anwendungsservice auffüllen** eine Methode zum Füllen des Anwendungsservice aus. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsservice .

- Mit der Anwendungsservicezuordnung wie im Folgenden beschrieben

  Der Standardbeziehungstyp der hinzugefügten Verbindung lautet in diesem Fall `Depends on::Used by`. Sie können diesen Standard-Beziehungstyp ändern, indem Sie den Wert von ändern `sa.it_service.manual_ci_rel_type`Eigenschaft. Siehe Mit Anwendungsservices installierte Komponenten Weitere Informationen finden Sie unter .

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Manuelles Hinzufügen eines neuen CI zu einem vorhandenen CI in einem Serviceinstanz Fordert auf CMDB Zum Aktualisieren der Informationen zu beiden CIs, einschließlich ihres Beziehungstyps. Wenn andere Anwendungsservices denselben anwendbaren Flow verwenden, wird CMDB Erkennt das neue CI und fügt es automatisch auch diesen Services hinzu.

Beispielsweise fügen Sie einem IBM WebSphere HTTP-Listener im Bank-Kundenportal manuell einen IBM WebSphere Message Broker hinzu. Vom System wird dieser IBM WebSphere Message Broker auch demselben HTTP-Listener im internen Portalservice der Bank hinzugefügt, da dieser HTTP-Listener von ihm verwendet wird. Wenn Sie ein manuell hinzugefügtes CI entfernen, entfernt das System es aus allen Anwendungsservices, in denen Sie es entweder manuell hinzugefügt haben oder es automatisch durch Analogie hinzugefügt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ein CI nur manuell mit tatsächlichen CIs verbinden, die in der CMDB vorhanden sind, nicht mit einer Visualisierung anderer Elemente in der Karte wie Cluster oder Grenzen. Außerdem ist es nicht zulässig, einem Anwendungsservice CIs dieser CI-Typen hinzuzufügen:

- NAT [cmdb_ci_Translation_rule]
- Endpunkt [cmdb_ci_Endpoint]
- Qualifizierer [cmdb_ci_Qualifier]
- Anwendungscluster [cmdb_ci_Application_Cluster]

In der Tabelle „Manuelle CI-Ausschlüsse/-Einschlüsse“ [svc_Manual_ci_Exclusions_inclusions] sind Systemdatensätze vorhanden. Siehe Mit Anwendungsservices installierte Komponenten Weitere Informationen finden Sie unter .

In Umgebungen mit Domain Separation werden nur CIs, die zu derselben Domäne gehören, wie der Serviceinstanz , dem Serviceinstanz hinzugefügt. Wenn es eine Domänenhierarchie gibt, müssen CIs zur gleichen untergeordneten Domäne gehören wie der Serviceinstanz .

Wenn Sie mit einem von Service-Mapping erkannten Serviceinstanz arbeiten, fügen Sie manuell ein CI hinzu:

- Um anzugeben, dass ein Serviceinstanz ein Gerät oder eine Anwendung enthält, die Service-Mapping nicht erkennen kann. Fügen Sie beispielsweise dem Produktionsflächenservice eine Klimaanlage hinzu.
- Um einen temporären Platzhalter für ein CI hinzufügen, das Service-Mapping nicht ermittelt hat. In diesem Fall planen Sie die erforderliche Fehlerbehebung, um sicherzustellen, dass Service-Mapping dieses CI in der Zukunft ermittelt. Fügen Sie beispielsweise einen IBM WebSphere Message Broker zum Kundenportalservice der Bank hinzu.
- Um einen Serviceinstanz zu erstellen, der Einstiegspunkte und CIs, die automatisch von Service-Mapping ermittelt wurden, mit Einstiegspunkten und CIs aus der CMDB kombiniert. Nachdem Sie manuell einen Einstiegspunkt hinzugefügt haben, können Sie den Serviceinstanz mit CIs aus der CMDB basierend auf den dort definierten Beziehungen aktualisieren.

Für zusätzliche Informationen im Zusammenhang mit Service-Mapping, Siehe Musteranpassung Und Aktivieren Sie die Traffic-basierte Discovery für CI-Typen oder bestimmte CIs .

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Um ein CI mit einem anderen CI in der Karte zu verbinden, klicken Sie mit der rechten Maustaste auf das CI, mit dem Sie das neue CI verbinden möchten, und wählen Sie dann **Ein CI hinzufügen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Dialogfeld „Ein CI hinzufügen“ das hinzuzufügende CI an:

Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. `cmdb_ci_appl` für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.

5. Klicken Sie auf **Absenden**.
Das manuell hinzugefügte CI wird in der Karte angezeigt.

Hinweis: Wenn Sie ein CI, das eine Anwendung ist, manuell als untergeordnetes Element zu einem Service hinzufügen, der bereits das übergeordnete Anwendungs-CI enthält, wird das neu hinzugefügte untergeordnete Anwendungs-CI in der Inklusion ausgeblendet. Klicken Sie auf das Pluszeichen (+) neben dem übergeordneten Anwendungs-CI, um das untergeordnete Anwendungs-CI anzuzeigen.

6. **Wahlweise:** Wenn Service-Mapping aktiviert ist, fügen Sie eine erkennbare ausgehende Verbindung für das manuell hinzugefügte CI hinzu:

   a. Klicken Sie mit der rechten Maustaste auf das manuell hinzugefügte CI.

   b. Wählen Sie **Manuell eine Verbindung hinzufügen**.

   Hinweis: Wenn Sie die Option **Manuell eine Verbindung hinzufügen** im Rechtsklick-Menü nicht sehen, stellen Sie sicher, dass Sie mit dem Benutzer angemeldet sind, der zu derselben Domäne gehört wie der Anwendungsservice.

   c. Konfigurieren Sie Attribute für den Einstiegspunkt wie in beschrieben Einstiegspunkte-Attribute .

   d. Klicken Sie auf **Absenden**.
   Discovery und Service-Mapping versuchen, dieses CI zu erkennen. Bei Erfolg wird das CI auf der Karte angezeigt. Andernfalls erscheint ein Warnsymbol (⚠).

7. **Wahlweise:** Wenn Service-Mapping aktiviert ist und Sie möchten, dass von Service-Mapping ein CI, das Sie zuvor manuell hinzugefügt haben, automatisch erkannt wird:

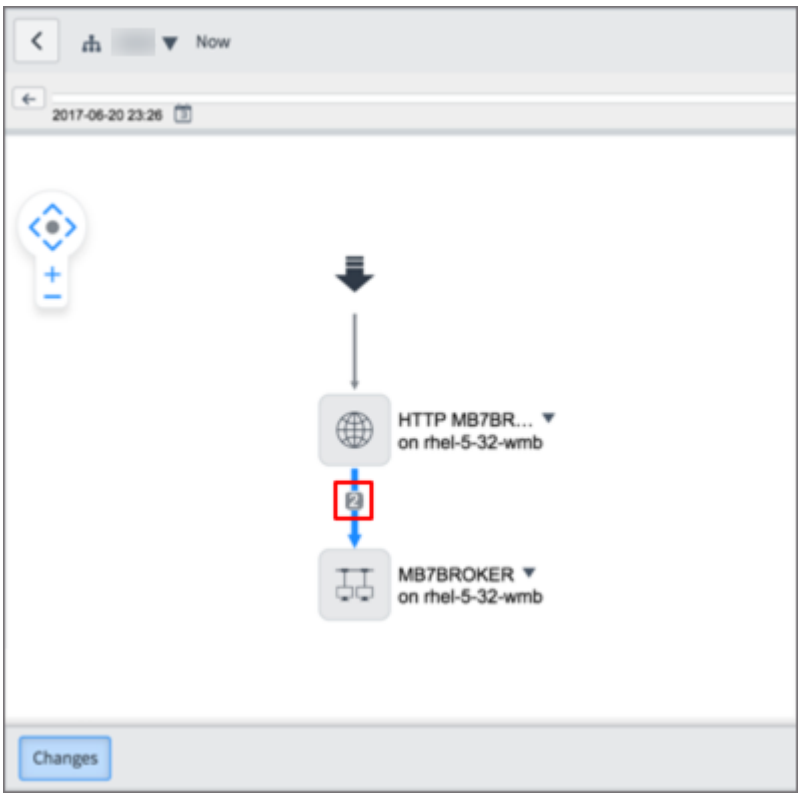
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Passen Sie das relevante Muster an, oder optimieren Sie die verkehrsabhängige Erkennung, um Service-Mapping für die Erkennung des CI freizuschalten.

b. Navigieren Sie zur betreffenden Serviceinstanz zuordnung.

c. Klicken Sie auf **Discovery ausführen**.

d. Überprüfen Sie nach Abschluss des Erkennung-Prozesses, ob Service-Mapping das CI erkannt hat durch Überprüfen des Connectors, der zum CI führt.
Wenn Service-Mapping das CI erkannt hat, erscheinen zwei Connectors, ein manueller und ein automatisch erkannter, für das CI.



e. Klicken Sie mit der rechten Maustaste auf das CI, das Sie manuell hinzugefügt haben.
In dem Beispiel ist es IBM WebSphere Message Broker.

f. Wählen Sie **Manuell hinzugefügtes CI entfernen**.
Die Karte zeigt das CI mit nur einem Connector, der zu ihm führt. Wenn für dieses CI manuell hinzugefügte Verbindungen vorhanden sind, werden diese zusammen mit dem manuell hinzugefügten CI entfernt.

Zugehörige Informationen

Anwendungsservices verknüpfen

addCI()

Nicht zu Anwendungsservices gehörende CIs entfernen

Entfernen Sie CIs, die fälschlicherweise als Teil eines Anwendungsservice von zugeordnet sind Service-Mapping. Unnötige CIs, die in der Zuordnung enthalten sind, können in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

irrelevante Warnungen generieren Ereignismanagement. Wenn Sie beispielsweise einen Anwendungsservice für ein Webportal erstellen, Service-Mapping Erkennt möglicherweise automatisch eine Verbindung zu nicht verbundenen externen Services wie PayPal.

Vorbereitungen

Sie entfernen CIs nur aus Anwendungsservices, die von Service-Mapping erkannt wurden.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch Entfernung von CIs aus der Zuordnung werden auch alle zugehörigen Verbindungen entfernt. Wenn Sie beispielsweise ein CI der zweiten Ebene aus der Zuordnung entfernen, werden auch alle CIs der dritten Ebene entfernt, die über ausgehende Verbindungen mit ihm verbunden sind.

Je nachdem, warum Service-Mapping ein unerwünschtes CI zugeordnet hat, können Sie es mit den folgenden Methoden entfernen:

- Fügen Sie Zuordnungsgrenzen hinzu, um die unnötigen CIs zu entfernen. Eine Grenze bewirkt, dass Service-Mapping die Erkennung ab diesem Punkt anhält und ausgehenden Verbindungen nicht folgt. Nutzen Sie diese Methode, um CIs zu entfernen, die Service-Mapping anhand von Mustern oder einer datenverkehrsbasierten Erkennung erkannt hat.
- Optimieren Sie die Traffic-basierte Discovery. Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als Traffic-basierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Service-Mapping Generiert Verbindungsvorschläge basierend auf Traffic-basierten Verbindungen und auf Predictive Intelligence Analyse der Fingerabdrücke der Anwendung. Wenn die Verbindungsvorschlagsfunktion aktiviert ist, Service-Mapping Fügt Anwendungsservices nicht automatisch Traffic-basierte Verbindungen hinzu und gibt Vorschläge. Überprüfen Sie die Vorschläge, und wählen Sie aus, welche CIs hinzugefügt oder entfernt werden sollen.

  Wenn die Funktion für Verbindungsvorschläge deaktiviert ist, fügt Service-Mapping Anwendungsservices datenverkehrsbasierte Verbindungen und CIs automatisch hinzu. Entfernen Sie Verbindungen, die zu irrelevanten CIs führen, um Anwendungsservices zu deklarieren.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Entfernen Sie CIs, die nicht zu diesem Serviceinstanz gehören, indem Sie die folgenden Aktionen ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Schritte
Zuordnungsgrenzen hinzufügen	**a.** Klicken Sie mit der rechten Maustaste auf den Connector, der zu dem CI führt, das Sie entfernen möchten. **b.** Wählen Sie **Grenze markieren** aus. Das CI wird in der Zuordnung als Grenze markiert ( ). **Hinweis:** Stellen Sie sicher, dass Sie sich die Karte in der Bearbeitungsansicht ansehen.
(Wenn die Funktion für Verbindungsvorschläge deaktiviert ist) Mithilfe datenverkehrsbasierter Verbindungen erkannte CIs entfernen	**a.** Klicken Sie mit der rechten Maustaste auf das CI in der Zuordnung. **Hinweis:** Sie können datenverkehrsbasierte Verbindungen für ein CI anzeigen, auch wenn Sie die datenverkehrsbasierte Erkennung für einen Serviceinstanz deaktiviert haben, zu dem das CI gehört. **b.** Wählen Sie **Traffic-basierte Verbindungen anzeigen**. Die Liste der datenverkehrsbasierten Verbindungen wird geöffnet. Weitere Informationen finden Sie unter Traffic-basierte Verbindungsliste. **c.** Suchen Sie in der **Liste der Traffic-basierten Verbindungen** nach der Verbindung, die zur Erkennung des unerwünschten CI verwendet wird. **d.** Wählen Sie für diese Verbindung im Feld **Benutzerentscheidung** die Option `Entfernen` aus. **e.** Klicken Sie auf **Schließen**.
(Wenn die Funktion für Verbindungsvorschläge aktiviert ist) Mithilfe datenverkehrsbasierter Verbindungen erkannte CIs entfernen	Führen Sie das unter CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen beschriebene Verfahren aus.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Zuordnungssegmente auf andere Anwendungsservices übertragen

Sie können eine Verzweigung eines Service entfernen und auf einen anderen (neuen oder vorhandenen) Anwendungsservice platzieren. Übertragen Sie Zuordnungssegmente, um große Services zu teilen oder Services anders als das ursprüngliche Zuordnungsergebnis zu organisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

> **Wichtig:** Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein Zuordnungssegment auf einen anderen Anwendungsservice übertragen, erstellen Sie eine Verknüpfung zwischen dem ursprünglichen Anwendungsservice und dem Anwendungsservice, in den Sie das Zuordnungssegment platziert haben. Die Verbindung mit dem obersten CI im Segment wird zum Einstiegspunkt, wenn Sie es auf einen anderen (vorhandenen oder neuen) Anwendungsservice übertragen.

Die ursprüngliche Servicezuordnung zeigt den Link zum anderen Anwendungsservice anstelle des Zuordnungssegments. Der Service, der den Verweis enthält, wird zu einem abhängigen Service. Der Service, der als Referenz angezeigt wird, ist ein enthaltener Service.

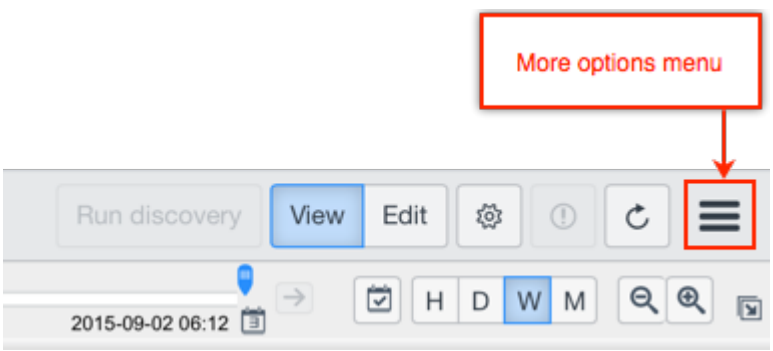
Wenn Sie ein Zuordnungssegment auf einen anderen Anwendungsservice übertragen, werden die Informationen zur Verbindung mit dem obersten CI im übertragenen Segment in der CMDB aktualisiert. Wenn andere Anwendungsservices dieselbe eingehende Verbindung (Endpunkt) verwenden, erkennt die CMDB dies und ersetzt Zuordnungssegmente, die aus derselben Verbindung stammen, per Analogie mit den verbundenen Service-CIs.

Sie können Links nicht zu mehreren Anwendungsservices aus derselben Verbindung einfügen.

Wenn Sie Ereignismanagement für die Serviceüberwachung in Ihrer Organisation verwenden, enthalten abhängige Anwendungsservices Warnungen, die für die enthaltenen Services generiert wurden.

Prozedur

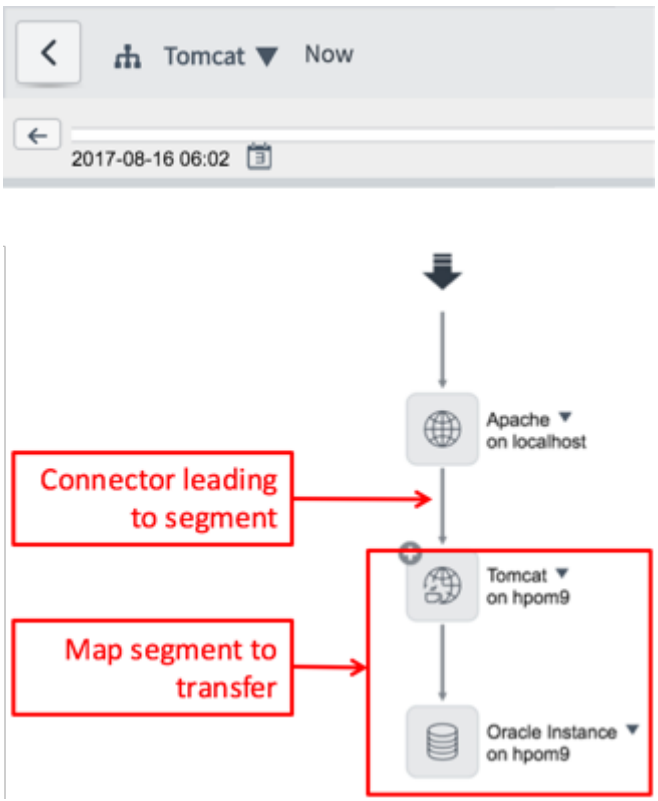
1. Öffnen Sie die Anwendungsservicezuordnung, die das Segment enthält, das Sie übertragen möchten:
   a. Navigieren zu **Service-Mapping** > **Anwendungsservices**an.
   b. Klicken Sie auf **Karte anzeigen** neben dem relevanten Serviceinstanz .
   c. **Wahlweise:** Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.
   d. Wenn die Hostansicht aktiviert ist, schalten Sie sie aus, indem Sie zuerst auf **Weitere Optionen** klicken und dann den Schalter für **In Host-Ansicht anzeigen** umschalten.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Identifizieren Sie das Segment der Zuordnung, das Sie übertragen möchten.
3. Klicken Sie im oberen Bereich dieses Segments mit der rechten Maustaste auf die Verbindung, die zum CI führt.



4. So übertragen Sie das Segment in eine vorhandene Anwendungsservicezuordnung und stellen eine Verbindung her:

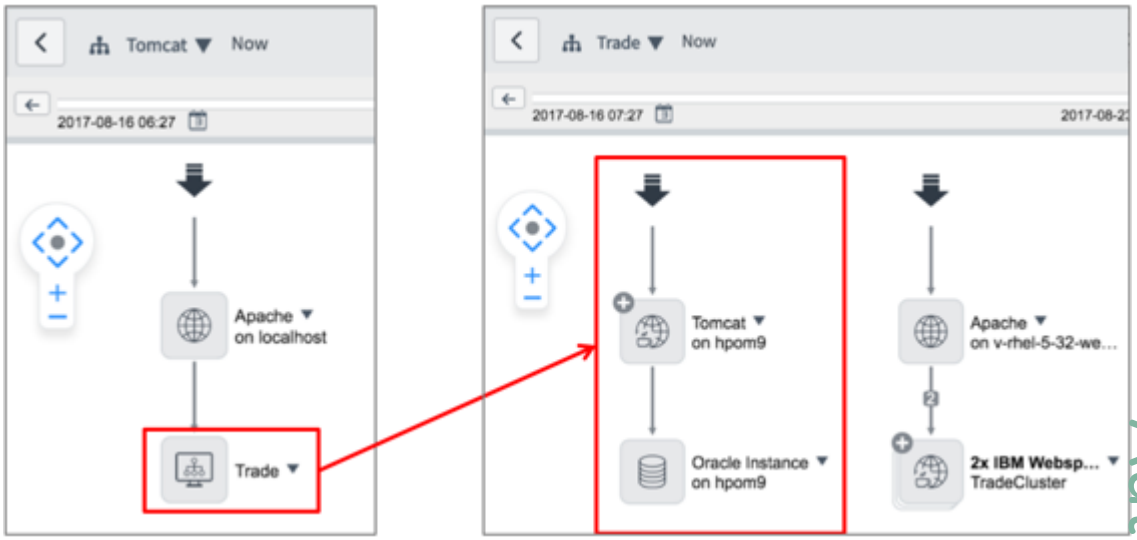
   a. Wählen Sie **Mit vorhandenem Service verbinden** aus.

   b. Wählen Sie im Fenster „Zu vorhandenem Discovery-Service hinzufügen“ den Anwendungsservice aus, an den Sie das Segment übertragen möchten.

   c. Klicken Sie auf **Auswählen**.
   Die Zuordnung zeigt das Symbol des enthaltenen Anwendungsservice anstelle des übertragenen Segments an. Die Anwendungsservicezuordnung, an die Sie das Segment übertragen haben, zeigt es unter dem neu hinzugefügten Einstiegspunkt an. Beispielsweise beinhaltet die Anwendungsservicezuordnung „Tomcat“ den Anwendungsservice „Trade“ als enthaltenen Service. Der Anwendungsservice „Tomcat“ wird zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einem vom Service „Trade“ abhängigen Service. Die Anwendungsservicezuordnung „Trade“ zeigt das Segment, das vom Anwendungsservice „Tomcat“ übertragen wurde.



5. So übertragen Sie das Segment in eine neue Zuordnung des Serviceinstanz und stellen eine Verbindung her:

a. Wählen Sie **Neuen Service von hier erstellen** aus.

b. Definieren Sie im Fenster „Neuen Discovery-Service erstellen“ Attribute für den Serviceinstanz , den Sie für dieses Segment erstellen möchten:

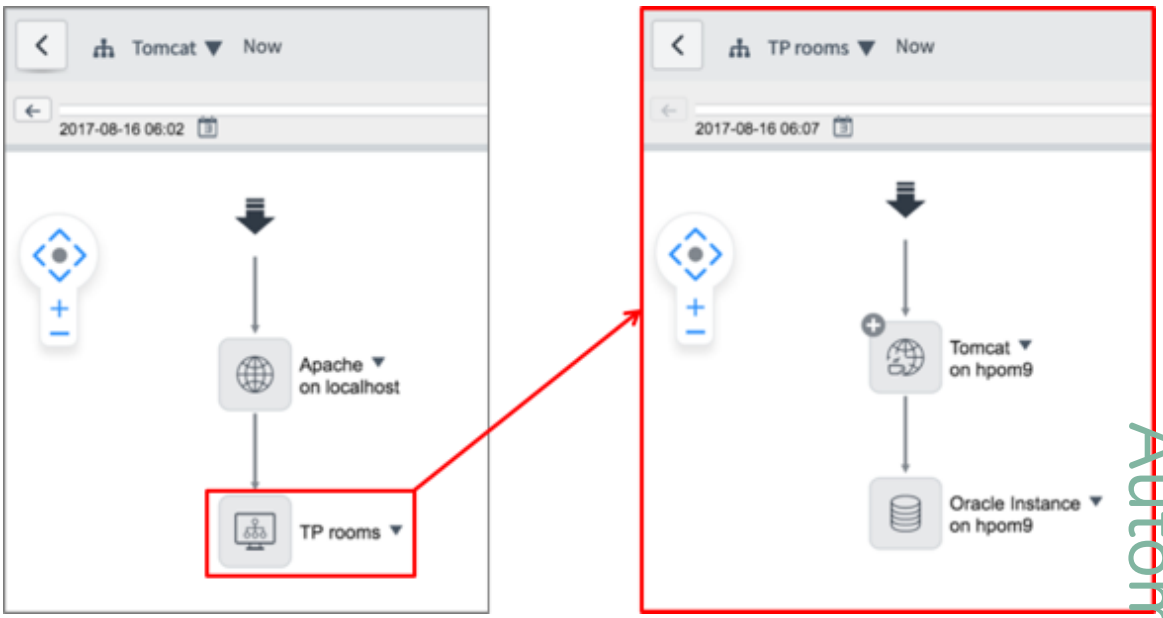
Feld	Beschreibung
Name	Geben Sie den Namen des Serviceinstanz ein. Dieser Name muss eindeutig sein. Verwenden Sie selbsterklärende Namen wie Mailing-Service oder Druckservice.
Gruppe	(Optional) Schränken Sie den Zugriff auf einen Serviceinstanz ein, indem Sie ihn zu einer Gruppe von Serviceinstanz s hinzufügen. Benutzer müssen dann über die Servicegruppenrolle verfügen, um auf den Serviceinstanz zugreifen zu können.
Relevanz	(Optional) Wählen Sie die Option aus, die widerspiegelt, wie wichtig dieser Serviceinstanz für den Betrieb Ihrer Organisation ist. Weitere Informationen zur Relevanz von Serviceinstanz s finden Sie unter Wichtigkeit für Anwendungsservices definieren.

c. Klicken Sie auf **Erstellen**.
Die Zuordnung zeigt das Symbol des enthaltenen Anwendungsservice anstelle des übertragenen Segments an. Der neue Anwendungsservice wird in der Liste der Anwendungsservices angezeigt und enthält das übertragene Segment der Zuordnung. Beispielsweise enthält der Anwendungsservice „Tomcat“ den Service „TP Rooms“ als enthaltenen Service. Der Anwendungsservice „Tomcat“ wird zu einem vom

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

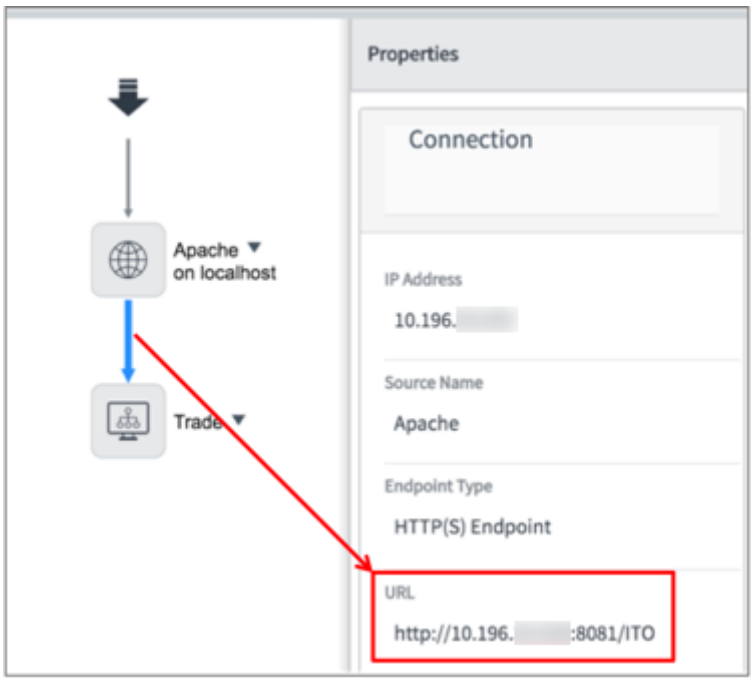
Service „TP Rooms“ abhängigen Service. Die Anwendungsservicezuordnung „TP Rooms“ enthält das Segment, das vom Anwendungsservice „Tomcat“ übertragen wurde.



Nächste Maßnahme

So machen Sie diesen Vorgang rückgängig:

1. Klicken Sie in der Zuordnung des Serviceinstanz , die das verbundene Service-CI enthält, auf die Verbindung, die zum CI führt.
2. Beachten Sie im Eigenschaftsbereich das URL-Attribut der Verbindung.



3. Doppelklicken Sie auf das verbundene Service-CI.

   Die Zuordnung des Serviceinstanz für das CI mit dem übertragenen Segment wird geöffnet.

4. Klicken Sie auf **Formular „Servicezuordnung“**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Suchen Sie unter „Einstiegspunkte“ auf der linken Seite nach dem Einstiegspunkt mit der gleichen URL, die Sie sich notiert haben.
6. Klicken Sie auf der Registerkarte „Einstiegspunkt“ auf **Löschen** und anschließend zur Bestätigung auf **Entfernen**.

   Dieser Einstiegspunkt wird aus dem Formular des Serviceinstanz entfernt.

   Das übertragene Segment wird aus der Zuordnung dieses Serviceinstanz entfernt.
7. Navigieren Sie zur Zuordnung, die das verbundene Service-CI enthielt.

   Anstelle des CI für einen verbundenen Service zeigt diese Zuordnung eine Grenze ( ) an.
8. Klicken Sie auf das Grenz-CI und anschließend auf **Markierung für Grenze aufheben**.

   Die Zuordnung wird aktualisiert und zeigt das Segment des Serviceinstanz an.

Zugehörige Informationen

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Benutzerzugriff auf Anwendungsservices steuern

Anwendungsservices verknüpfen

Sie können zwei Anwendungsservices manuell verknüpfen, indem Sie einen Verweis auf einen Anwendungsservice in einen anderen Anwendungsservice einfügen. Der Service, der den Verweis enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service. Sie können Anwendungsservices untereinander verknüpfen, um Abhängigkeiten für die Überwachung der Auswirkungen in Ereignismanagement zu erstellen.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Vergewissern Sie sich, dass Sie Name und Servicetyp des Anwendungsservice kennen, dem Sie einen Verweis hinzufügen möchten.

Erforderliche Rolle: App_Service_admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Um eine Verbindung herzustellen, fügen Sie einen Verweis auf den Anwendungsservice als ausgehende Verbindung des relevanten CI in dem anderen Anwendungsservice hinzu. Sie können beispielsweise den Anwendungsservice „UK Portal“ als Link zum Anwendungsservice „Online Store“ hinzufügen. In diesem Fall wird der Service „Online Store“ zu einem vom Service „UK Portal“ abhängigen Service bzw. dieser zu einem enthaltenen Service. Der Service „Online Store“ spiegelt Erkennungsfehler für den enthaltenen Service im Zuordnungsmodus „Bearbeiten“ sowie Warnungen in Ereignismanagement wider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für verknüpfte Anwendungsservices

Wenn Sie einen Anwendungsservice mit einem anderen Anwendungsservice verbinden, werden die Informationen über das CI, mit dem Sie den Service verknüpft haben, in der CMDB aktualisiert. Die CMDB erkennt andere Anwendungsservices, die denselben Anwendungs-Flow verwenden, und fügt den enthaltenen Anwendungsservice analog zu diesen Anwendungsservices hinzu. Die gleiche Logik gilt, wenn Sie einen enthaltenen Anwendungsservice entfernen: Das System entfernt ihn aus allen Anwendungsservices, in denen entweder Sie diesen Service manuell verknüpft haben oder das System diesen Service analog dazu verknüpft hat.

Wenn Sie Service-Mapping verwenden, möchten Sie möglicherweise Anwendungsservices verknüpfen, um Folgendes zu erstellen:

- Eine Abhängigkeit zwischen zwei Anwendungsservices.
- Einen Platzhalter für einen Kartenteil, den Service-Mapping nicht erkennen konnte. Wenn Sie ein Muster erstellen oder ändern, um das CI zu erkennen, das als Einstiegspunkt für das enthaltene Serviceinstanz dient, kann Service-Mapping diesen enthaltenen Service erkennen.
- Einen Hinweis darauf, dass ein Serviceinstanz eine Verzweigung enthält, die Service-Mapping nicht erkennen kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können einen Serviceinstanz bei Bedarf beliebig vielen Serviceinstanz s als enthaltenen Service hinzufügen.

Prozedur

1. Navigieren zu **Service-Mapping** > **Anwendungsservices**an.
2. Klicken Sie neben dem zugehörigen Anwendungsservice auf **Karte anzeigen**.
3. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.
4. Klicken Sie mit der rechten Maustaste auf das CI, mit dem Sie einen Anwendungsservice als Referenz verknüpfen möchten.
5. Wählen Sie **CI hinzufügen**.
6. Wählen Sie im Dialogfeld „CI hinzufügen“ den Anwendungsservice aus, den Sie als enthaltenen Service hinzufügen möchten:

Feld	Beschreibung
CI-Typ	Wählen Sie den entsprechenden Servicetyp aus dieser Liste aus: ○ Tag-basierter Anwendungsservice ○ Zugeordneter Anwendungsservice für erkannte oder manuell erstellte Anwendungsservices ○ Berechneter Anwendungsservice für dynamische Services ○ Dynamic CI-Gruppe
CI-Name	Wählen Sie den Namen des Anwendungsservice, den Sie als enthaltenen Service verknüpfen möchten.

7. Klicken Sie auf **Absenden**.
   Das Symbol für den enthaltenen Service wird in der Zuordnung angezeigt.

Zugehörige Informationen

Anwendungsservices

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Als generische Anwendungen identifizierte CIs erkennen

Service-Mapping identifiziert Anwendungskonfigurationselemente (CIs), die nicht ordnungsgemäß als generische Anwendungen erkannt wurden. Identifizieren Sie generische Anwendungen korrekt, indem Sie ein vereinfachtes Erkennungsmuster aus einer Anwendungsservicezuordnung erstellen, anstatt mithilfe des Musterdesigners ein vollständig funktionsfähiges Muster von Grund auf neu zu erstellen.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Es ist wichtig, dass Sie die Discovery-Prozessklassifizierung verstehen.

Wenden Sie sich an den Eigentümer des Anwendungsservice, um ihn um Informationen über das als generische Anwendung erkannte CI zu bitten.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

Erstellen Sie im Rahmen der Erstellung eines vereinfachten Musters für die vollständige und ordnungsgemäße Erkennung von Anwendungs-CIs die folgenden erforderlichen Elemente:

CI-Typ

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden. Ein CI-Typ (oder eine Klasse) enthält mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten. Vorkonfigurierte CI-Typen bilden eine Hierarchie, in der untergeordnete CI-Typen Attribute von ihren übergeordneten Elementen ableiten.

Definieren Sie den Namen und die Bezeichnung des CI-Typs für Service-Mapping, um einen untergeordneten CI-Typ für den CI-Typ der Anwendung [cmdb_ci_appl] zu erstellen. Weitere Informationen zu CI-Typen finden Sie unter CI-Typen für Service-Mapping und Discovery erstellen.

Prozessklassifizierung

Service-Mapping Basiert auf Prozessinformationen, die von erfasst und klassifiziert werden Discovery Zum Ausführen relevanter Muster zum Erkennen eines Anwendungs-CI. Während der horizontalen Erkennung überprüft Discovery, ob die Attribute der von der Anwendung ausgeführten Prozesse den von Ihnen definierten Klassifizierungskriterien entsprechen. Wenn eine Übereinstimmung gefunden wird, verwendet Discovery den vorhandenen Bezeichner der Anwendungsregel, um zu überprüfen, ob das Anwendungs-CI neu ist oder bereits in der CMDB vorhanden ist. Anschließend aktualisiert Discovery entweder einen vorhandenen Datensatz oder erstellt einen neuen Datensatz für dieses Anwendungs-CI in der CMDB.

Bevor Sie die Top Down-Discovery eines Anwendungs-CI starten, Service-MappingÜberprüft seine Prozessklassifizierung in CMDB. Anschließend werden nur die Muster ausgeführt, die für dieses Anwendungs-CI relevant sind.

Erstellen Sie eine Prozessklassifizierung, indem Sie die Klassifizierungskriterien basierend auf vorkonfigurierten Prozessattributen definieren. Die neue Prozessklassifizierung wird der Tabelle „Prozessklassifizierung“ [discovery_classy_proc] hinzugefügt. Informationen zur Prozessklassifizierung finden Sie unter Discovery-Klassifizierer.

Muster

Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Wenn Sie ein vereinfachtes Muster für eine generische Anwendung erstellen, weist Service-Mapping das neue vereinfachte Muster dem CI-Typ zu, den Sie als Teil dieses Prozesses definieren. Der Standardname für das Muster beginnt mit „ga_“.

Verknüpfung eines Symbols mit diesem CI-Typ

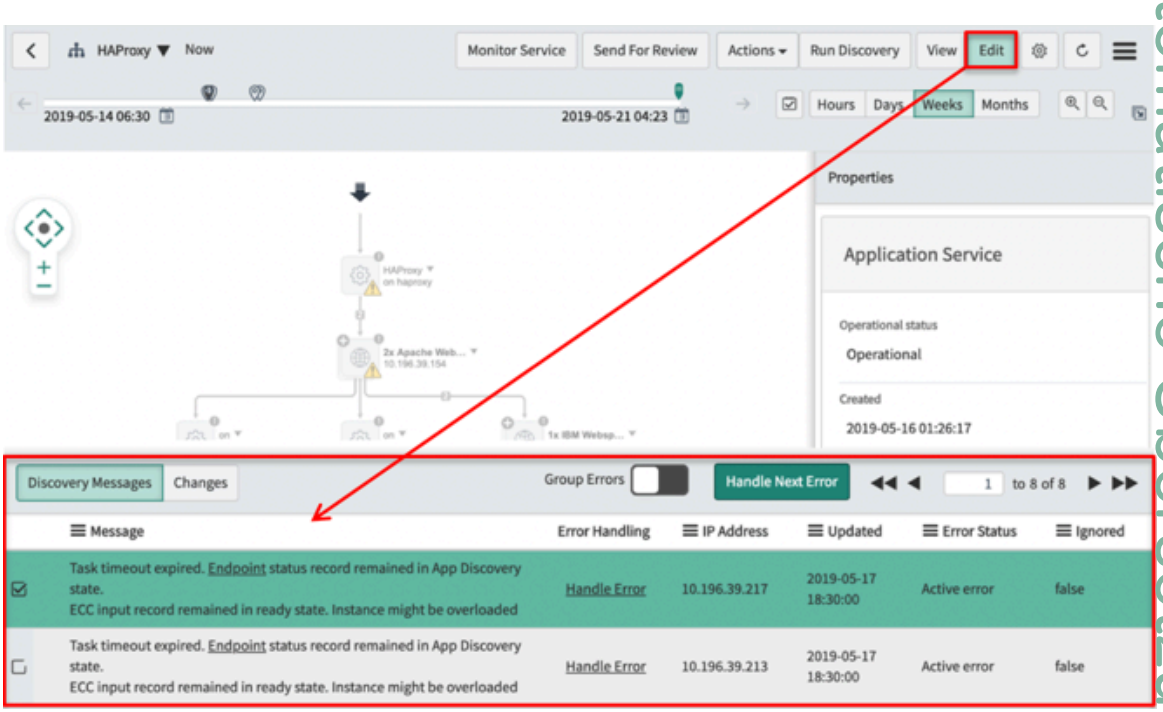
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder CI-Typ ist einem Symbol zugeordnet. Wenn ein CI erkannt und als zu einem CI-Typ gehörend klassifiziert wird, zeigt die Zuordnung das zugehörige Symbol zur Darstellung dieses CI an.

Sie können keine vereinfachten Muster aus generischen Anwendungen erstellen, die auf mehreren Prozessen basieren. In diesem Fall müssen Sie entweder ein voll funktionsfähiges Muster mit dem Musterdesigner erstellen oder einen neuen CI-Typ erstellen.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. **Wahlweise:** Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.



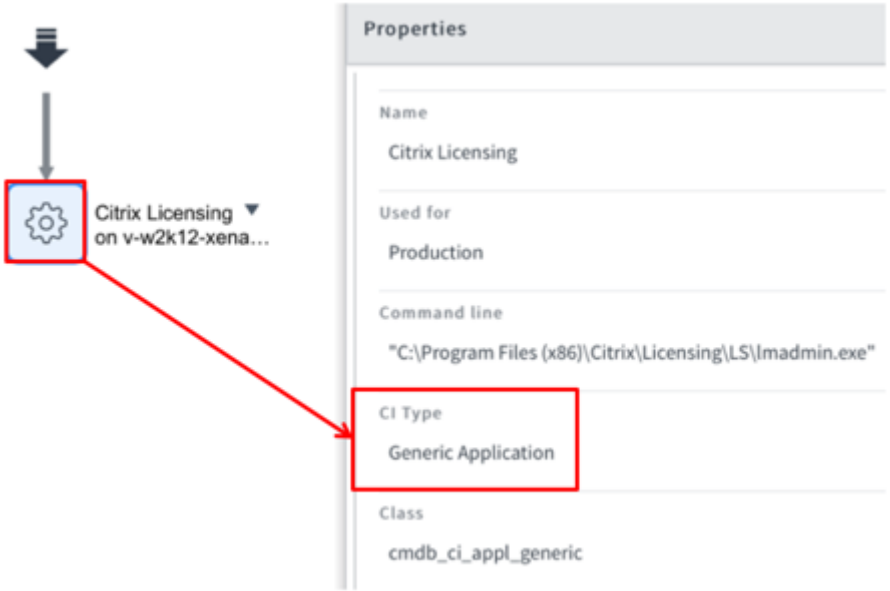
3. Klicken Sie in der Zuordnung mit der rechten Maustaste auf das relevante CI einer generischen Anwendung.

   Das Attribut *CI Type* im Bereich **Anwendung** lautet „Allgemeine Applikation“.

   Im Basissystem zeigt die Zuordnung CIs generischer Anwendungen mit dem Zahnradsymbol an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Muster für diese allgemeine Applikation erstellen** aus.
5. Definieren Sie den CI-Typ für die Anwendung.

Feld	Beschreibung
Bezeichnung	Name des CI-Typs. Beispiel: „Citrix-Lizenzierungsserver“
Name	Der Tabellenname, der Daten für diesen CI-Typ enthält. Beispiel: cmdb_ci_app_license_server. Verwenden Sie einen Namen, der mit vorhandenen CI-Typnamen übereinstimmt. Normalerweise beginnen CI-Typnamen mit „cmdb_ci_app“.
Symbol	Wählen Sie den Namen des vorhandenen Symbols aus, mit dem diese Anwendung in Zuordnungen dargestellt werden soll.

6. Erstellen Sie die Prozessklassifizierung für dieses CI, indem Sie Klassifizierungskriterien zur Identifizierung des Prozesses definieren, der von der generischen Anwendung ausgeführt wird.
   Im Basissystem gibt es zwei Bedingungen, die auf dem Namen und dem Befehl des laufenden Prozesses basieren. Die Werte werden von der letzten Prozesserkennung eingetragen.

   a. Wählen Sie das CI-Attribut aus der Liste aus.
      Die Attribute in der Liste stammen aus der Tabelle „Laufender Prozess“ [cmdb_running_process].

   b. Wählen Sie einen Operator aus der Liste aus.
      Wenn Sie Ist Leer auswählen, wird das zweite Feld irrelevant und wird ausgeblendet.

   c. Geben Sie den Wert für die Übereinstimmung an.
      Das Wertfeld zeigt einen dynamisch generierten Vorschlag aus der letzten Prozesserkennung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Zum Hinzufügen einer abhängigen Bedingung klicken Sie auf **ODER** oder **UND**.

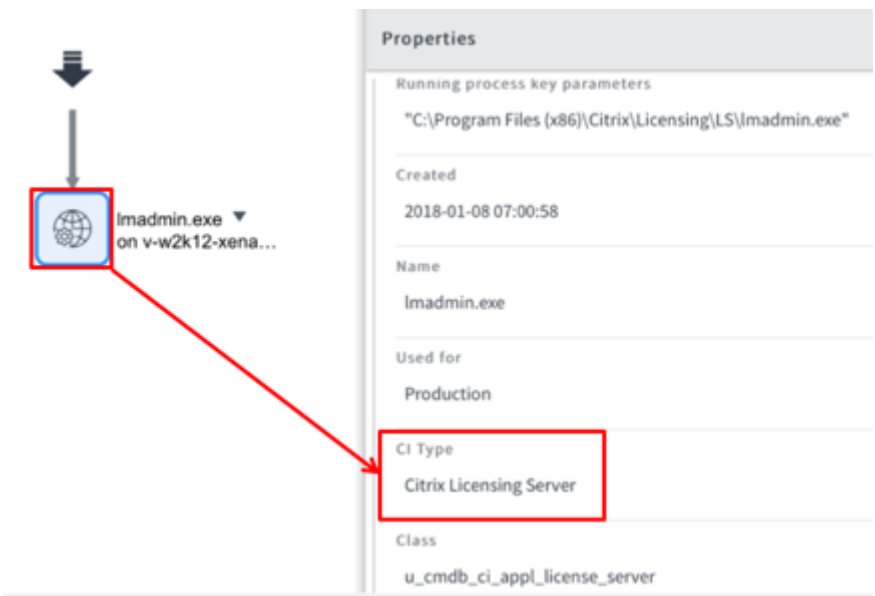
Hinweis: Wenn der Wert in der ersten Bedingung nicht eindeutig ist (Beispiel: „Java.exe“), verwenden Sie zusätzliche Bedingungen, um die Ergebnisse einzugrenzen.

Um beispielsweise einen Citrix-Lizenzierungsserver zu erkennen, verwenden Sie die folgenden Klassifizierungskriterien: den Prozessnamen lmadmin.exe mit dem Befehl C:\Programmdateien (x86)\Citrix\Licensing\LS\lmadmin.exe.

e. Um eine Bedingung auf oberster Ebene hinzuzufügen, klicken Sie auf **Neue Kriterien**.

7. Klicken Sie auf **Erstellen**.
Sobald Service-Mapping die Erstellung von CI-Typ, Muster und Prozessklassifizierung abgeschlossen hat, wird die Erkennung des CI fortgesetzt, das ursprünglich als generische Anwendung identifiziert wurde.

8. Vergewissern Sie sich, dass Service-Mapping das CI erwartungsgemäß erkannt hat.



Beachten Sie, dass Service-Mapping den Namen des Prozesses für die CI-Bezeichnung in der Zuordnung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Wenn Service-Mapping das CI immer noch nicht wie erwartet erkannt hat, müssen Sie die Übereinstimmungs- und Klassifizierungskriterien für den Prozessklassifizierer feinabstimmen und erweiterte Klassifizierungsparameter konfigurieren.

Wenn Sie mit dem Ändern von Mustern im Musterdesigner vertraut sind, können Sie das vereinfachte Muster auch erweitern, indem Sie Vorgänge definieren, die weitere Attribute für das CI erkennen.

Sie können Discovery so konfigurieren, dass ein anderer Bezeichner verwendet wird. Weitere Informationen finden Sie unter Discovery-Bezeichner.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

Fertigstellung des Anwendungsservice

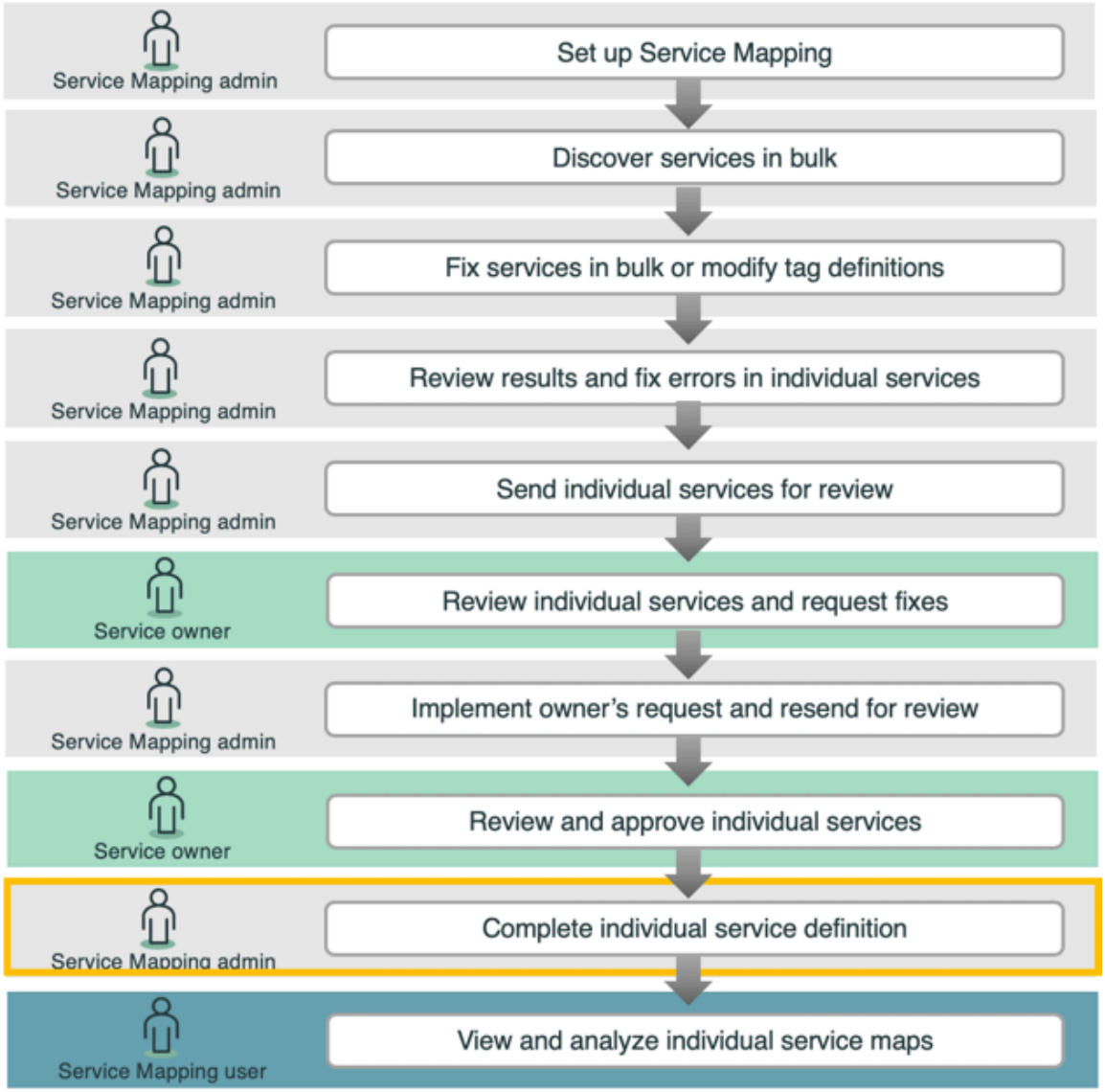
Nachdem ein Anwendungsservice geprüft und genehmigt wurde, können Sie Attribute definieren, die seine Erkennung verbessern, seine Bedeutung widerspiegeln und den Zugriff auf ihn steuern.

Es gibt mehrere Konfigurationen, die Sie ausführen müssen, um die Definition eines Anwendungsservice abzuschließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Workflow



Automatische Übersetzung

Wichtigkeit für Anwendungsservices definieren

Wählen Sie für jede Serviceinstanz eine Relevanzstufe aus, die widerspiegelt, wie wichtig sie für den Betrieb Ihrer Organisation ist.

Vorbereitungen

Bestimmen Sie, wie wichtig der Anwendungsservice für Ihr Unternehmen ist.

Erforderliche Rolle: Service_Mapping_admin

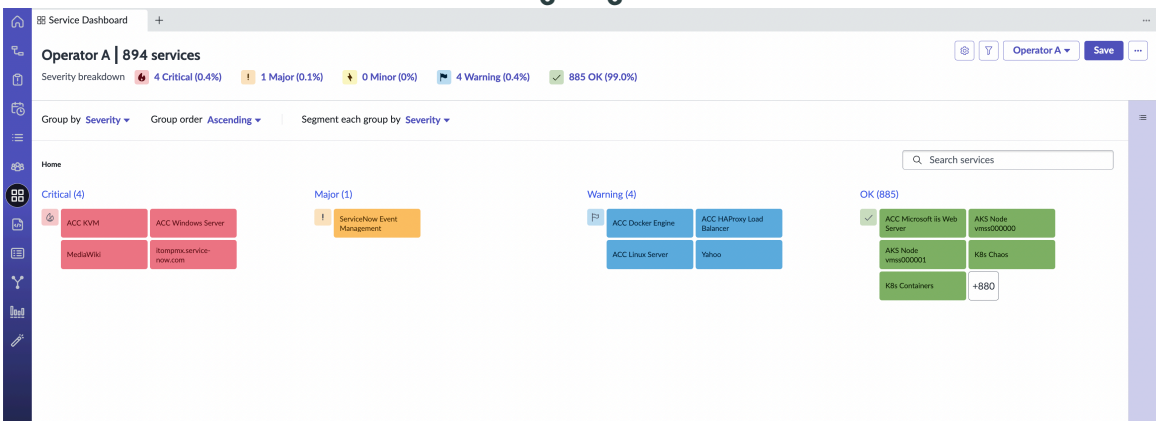
Warum und wann dieser Vorgang ausgeführt wird

In der Regel weisen Sie Serviceinstanzen eine hohe Relevanz zu, die sich auf Ihren Kundenstamm oder Ihren Umsatz auswirkt, während Sie internen Serviceinstanzen eine geringe Relevanz verleihen, die den Mitarbeitern der Organisation geringfügige Unannehmlichkeiten verursachen. Sie können beispielsweise eine hohe Relevanz für eine Serviceinstanz festlegen, die die Vertriebsfunktionalität mithilfe der Website der Organisation unterstützt. Eine Serviceinstanz, die internen Druck für die Mitarbeiter der Organisation bereitstellt, kann eine geringe Relevanz erhalten.

Sie können auch einen Kritikalitätswert verwenden, um Wiederherstellungsstrategien zu definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Betreiber-Arbeitsbereich-Seite angezeigte Relevanzstufen



Prozedur

1. Führen Sie in der klassischen Umgebung die folgenden Schritte aus:

a. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**an.
Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die Service-Mapping Kann erkennen oder wurde bereits erkannt. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mithilfe der API erstellt werden.

b. Klicken Sie auf der Kachel **Abgeschlossen** auf **Ihre Services anzeigen**.

c. Wählen Sie den entsprechenden Anwendungsservice.

d. Klicken Sie auf **Zusätzliche Informationen**.

e. Wählen Sie die entsprechende Option aus der Liste **Geschäftsrelevanz** aus.

f. Klicken Sie auf **Aktualisieren**.

2. Alternativ führen Sie die folgenden Schritte in der Mitarbeiterbereich-Benutzeroberfläche aus:

a. Navigieren zu **Mitarbeiterbereich** > **Mitarbeiterbereich-Startseite**an.

b. Klicken Sie im linken Bereich auf **Listen**.

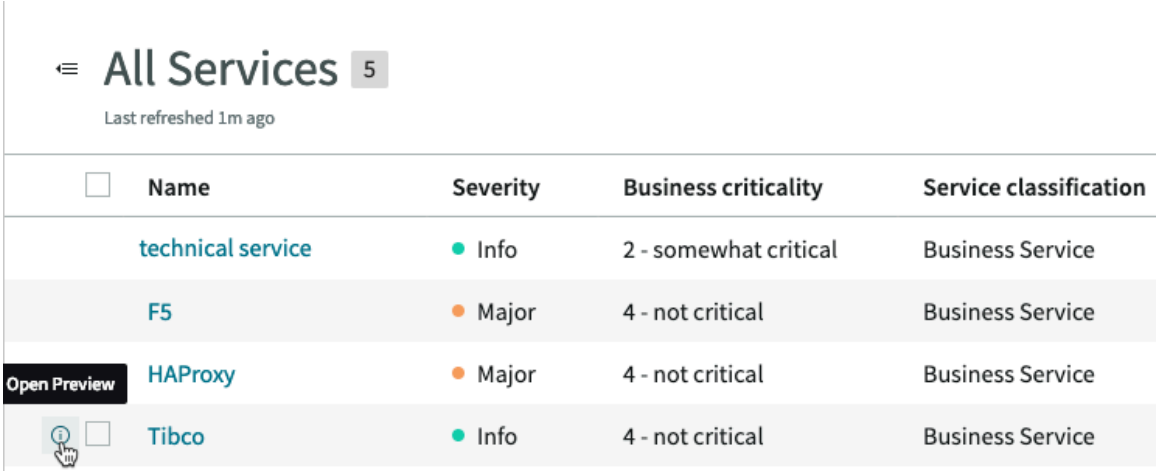
c. Navigieren zu **Services** > **Alle Services**an.
Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.

d. Wählen Sie den entsprechenden Anwendungsservice.

e. Klicken Sie auf das Symbol **Vorschau öffnen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Detailbereich wird auf der rechten Seite geöffnet.

f. Wählen Sie die entsprechende Option aus der Liste **Geschäftsrelevanz** aus.

g. Klicken Sie auf **Aktualisieren**.

Gruppen-Anwendungsservices

Organisieren Sie Anwendungsservices nach Gruppen, um Aktionen für mehrere Services gleichzeitig auszuführen und den Benutzerzugriff auf Services zu steuern. Sie können Ereignismanagement verwenden, um die Serviceintegrität nach Servicegruppen nachzuverfolgen.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin oder App_Service_admin

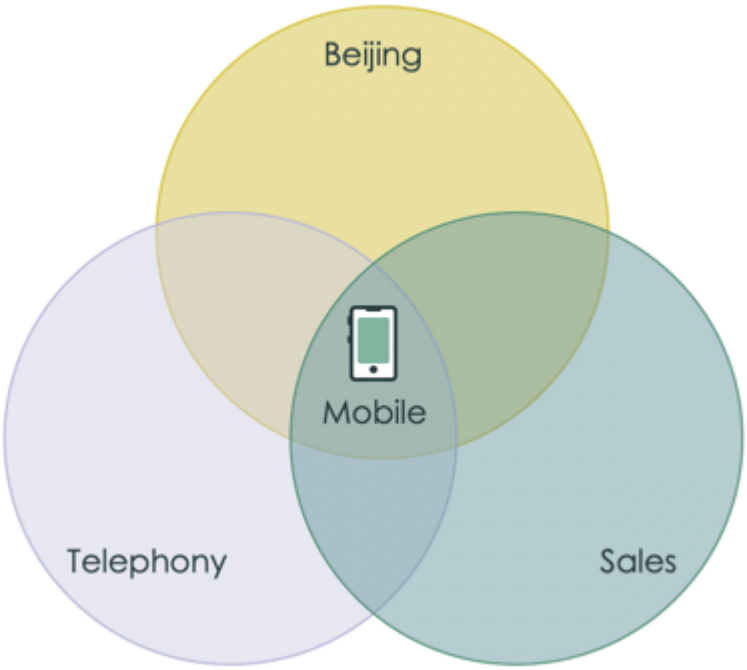
Warum und wann dieser Vorgang ausgeführt wird

In der Regel verfügen Unternehmen über Hunderte von Services, sodass es nicht praktikabel ist, sie einzeln zu verwalten. Servicegruppen können Servicelisten wesentlich kürzer machen und einfacher verwalten, insbesondere in großen Organisationen oder Diensteanbietern.

Wie Sie Serviceinstanzen gruppieren, hängt vom Anwender und von den Servicebereitstellungsrichtlinien in Ihrem Unternehmen ab. Die Beziehung zwischen Serviceinstanzen in Gruppen ist rein logisch, und dieselbe Serviceinstanz kann mehreren Gruppen angehören. Zum Beispiel kann der Mobile-Service zu den folgenden Servicegruppen gehören: Vertrieb, Peking und Telefonie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Serviceinstanz, die zu verschiedenen Gruppen gehört



Sie können eine Servicegruppe in eine andere Servicegruppe einbetten, um eine Hierarchie von Servicegruppen zu erstellen. Wenn Benutzer Zugriff auf eine übergeordnete Servicegruppe haben, haben sie automatisch Zugriff auf alle untergeordneten Gruppen. Standardmäßig werden alle neuen Services dem zugewiesen **Alle** Servicegruppe, mit der alle Anwender Serviceinstanzen anzeigen und verwalten können. Wenn Sie einer Servicegruppe eine Rolle zuweisen, können die Anwender mit dieser Rolle auf Serviceinstanzen in dieser Servicegruppe und in zugreifen **Alle** Servicegruppe. Um Benutzern mit dieser Rolle den Zugriff auf andere Services zu ermöglichen, weisen Sie diese Rolle der jeweiligen Servicegruppe zu. Weisen Sie der Servicegruppe **Alle** keine Anwenderrollen direkt zu.

Wenn Service-Mapping aktiviert ist, können Servicegruppen eine Mischung von manuell erstellten Anwendungsservices und den von Service-Mapping erkannten Anwendungsservices enthalten.

Sie können ServiceNow AI Platform Benachrichtigungen verwenden, um Benutzer zu warnen, wenn der Servicegruppenschweregrad zu „kritisch“ geändert wird. Der Gesamtschweregrad der Gruppe wird durch den höchsten Warnungsschweregrad innerhalb der Gruppe bestimmt.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Applikationsservices** > **Servicegruppen**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie den Namen der neuen Serviceinstanz -Gruppe im Feld **Name** ein.
4. Um diese Gruppe in eine andere Gruppe einzubetten, geben Sie den Namen der anderen Gruppe in dem Feld **Übergeordnete Gruppe** ein.
5. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.
6. Fügen Sie der neu erstellten Servicegruppe eine Serviceinstanz hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie im Abschnitt Servicegruppenmitglieder auf **Neu**.

b. In **Name** Geben Sie den Namen der Serviceinstanz ein.
Wenn Sie Ereignismanagement verwenden, können Sie auch einen Benachrichtigungs-Gruppennamen eingeben.

c. Klicken Sie auf **Absenden**.

7. Alternativ können Sie einer Gruppe eine Serviceinstanz über das Serviceinstanzformular hinzufügen.
   a. Navigieren zu **Alle** > **Konfiguration** > **Serviceinstanzen** > **Serviceinstanzen**an.
   b. Wählen Sie die Serviceinstanz aus, die Sie einer Servicegruppe hinzufügen möchten.
   c. Im Abschnitt **Servicegruppenmitglieder** doppelklicken Sie **Neue Zeile einfügen**.
   d. Geben Sie den Namen der Servicegruppe ein, der Sie die ausgewählte Serviceinstanz hinzufügen möchten.
   e. Klicken Sie auf das Symbol **OK** ( ).
   f. Klicken Sie auf **Aktualisieren**.

Benutzerzugriff auf Anwendungsservices steuern

Weisen Sie Servicegruppen Benutzerrollen zu, um Benutzern Zugriff auf Anwendungsservices in Ihrer Organisation zu gewähren. Ihre Organisation kann aus Sicherheits- oder Geheimhaltungsgründen den Zugriff auf bestimmte Services einschränken.

Vorbereitungen

Stellen Sie sicher, dass Sie die Benutzerbereitstellungsaufgaben für die Benutzer ausgeführt haben, denen Sie Zugriff gewähren möchten:

1. Fügen Sie Anwendern zu Anwendergruppen hinzu .
2. Erstellen Sie neue Rollen .
3. Weisen Sie Anwendern oder Anwendergruppen Rollen zu .

Stellen Sie außerdem sicher, dass Sie Servicegruppen erstellt haben, wie in Gruppen-Anwendungsservices beschrieben.

Erforderliche Rolle: App_Service_admin oder Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem bieten die folgenden Rollen Zugriff auf Anwendungsservices:

app_service_admin

Erstellt und ändert Serviceinstanzen, erstellt Servicegruppen, zeigt Serviceinstanzzuordnungen an und bearbeitet sie.

app_service_user

Zeigt Zuordnungen für operative Serviceinstanzen an und ruft Serviceinhalte mithilfe der getContent – GET REST API ab. Die ITIL-Rolle, die als die grundlegende Help Desk-Technikerrolle dient, enthält die Rolle „app_service_user“.

Service-Mapping bietet diese vorkonfigurierten Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

service_mapping_admin

Richtet die Service-Mapping-Anwendung ein. Ordnet Serviceinstanzen zu, korrigiert und verwaltet sie. Führt auch eine erweiterte Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.

service_mapping_user

Zeigt Zuordnungen für operative Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität und Verfügbarkeit von Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.

sm_app_owner

Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_App_owner Anwendern zu, die Serviceinstanzen besitzen und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.

Hinweis: Nur Benutzer mit der Rolle itil können alle Serviceinstanzen anzeigen.

Ereignismanagement bietet diese vorkonfigurierten Rollen:

evt_mgmt_admin

Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.

evt_mgmt_operator

Neben den evt_mgmt_user-Berechtigungen können auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktiviert werden.

evt_mgmt_user

Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat Schreibzugriff auf Alarme, um die Alarmlebensdauer zu verwalten. Hat die Rolle, um Vorfälle verwalten zu können, die aus Alerts erstellt werden.

evt_mgmt_integration

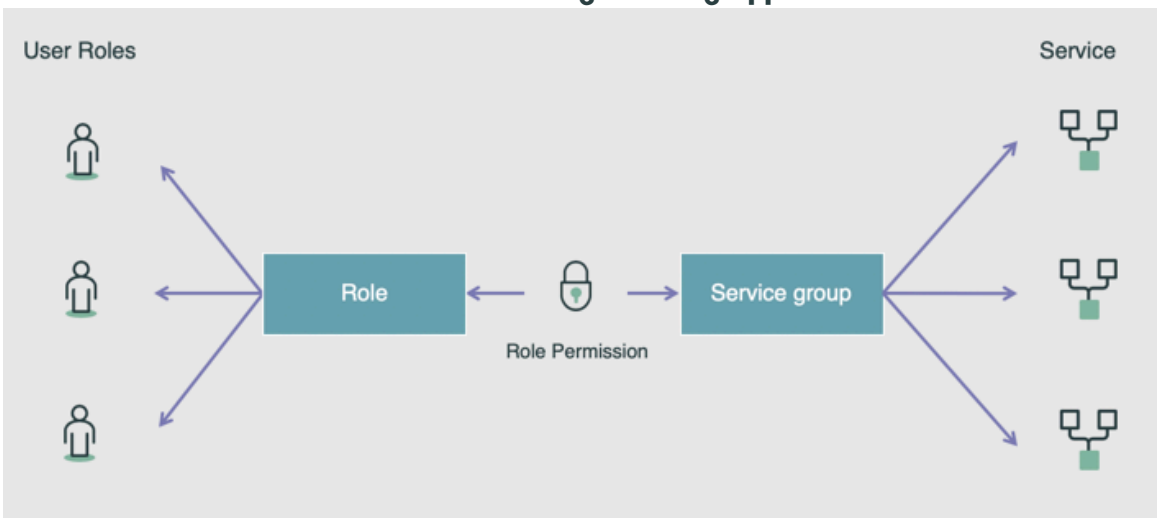
Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie mit externen Ereignisquellen zu integrieren.

In der Regel verfügen Unternehmen über Hunderte von Services, sodass es nicht praktikabel ist, sie einzeln zu verwalten. Servicegruppen können Servicelisten wesentlich kürzer machen und einfacher verwalten, insbesondere in großen Organisationen oder Diensteanbietern. In einer Hierarchie von Servicegruppen gewährt der Zugriff auf eine übergeordnete Servicegruppe automatisch Zugriff auf alle untergeordneten Servicegruppen.

Benutzer erben Berechtigungen von Rollen, die ihnen zugewiesen sind. Sie können einige Rollen direkt Servicegruppen zuweisen, damit alle Benutzer mit dieser Rolle auf alle Anwendungsservices zugreifen können, die zu dieser Gruppe gehören. Die meisten Unternehmen entscheiden sich jedoch dafür, ihre Rollen als Hierarchie zu organisieren. Es ist hilfreich, Rollen über mehrere ServiceNow Anwendungen zu verwalten. Zum Beispiel die Service-Mapping Der Administrator [Service_Mapping_admin] kann Teil einer breiteren Administratorrolle wie Administrator [admin] sein. Sie können Benutzer zu Benutzergruppen hinzufügen und dann den Benutzergruppen Rollen zuweisen, um allen Gruppenbenutzern gleichzeitig Berechtigungen dieser Rolle zu erteilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisen einer Rolle zu einer Anwendungsservicegruppe



Standardmäßig werden alle neuen Services dem zugewiesen **Alle** Servicegruppe, mit der alle Anwender Serviceinstanzen anzeigen und verwalten können. Wenn Sie einer Servicegruppe eine Rolle zuweisen, können die Anwender mit dieser Rolle auf Serviceinstanzen in dieser Servicegruppe und in zugreifen **Alle** Servicegruppe. Um Benutzern mit dieser Rolle den Zugriff auf andere Services zu ermöglichen, weisen Sie diese Rolle der jeweiligen Servicegruppe zu. Weisen Sie der Servicegruppe **Alle** keine Anwenderrollen direkt zu.

Prozedur

1. Navigieren Sie zu einem der folgenden Elemente:
   - **Konfiguration** > **Applikationsservices** > **Zuständigkeiten der Servicegruppe**an.
   - Wenn Service-Mapping Ist aktiviert: **Service-Mapping** > **Services** > **Zuständigkeiten der Servicegruppe**an.
   - Wenn Ereignismanagement Ist aktiviert: **Ereignismanagement** > **Services** > **Zuständigkeiten der Servicegruppe**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular „Zuständigkeiten der Anwendungsservicegruppe“ aus.

Feld	Beschreibung
Anwendungsservice-Gruppe	Servicegruppe, der Sie eine Rolle zuweisen möchten.
Rolle	Rolle, die Sie der ausgewählten Servicegruppe zuweisen möchten. Zum Beispiel financial_services_admin.

3. Klicken Sie auf **Absenden**.

Example:
So verwalten Sie den Zugriff auf Services, die vertrauliche Finanzinformationen in Ihrer Organisation enthalten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Organisieren Sie die Services in der Gruppe „Finanzservices“.
2. Erstellen Sie eine neue Benutzerrolle, die Rolle des Finanzservice-Administrators [financial_services_admin], die die Rolle [app_service_admin] enthält.
3. Weisen Sie die Administratorrolle „Finanzservices“ der Gruppe „Finanzservices“ zu.

Damit können nur Benutzer mit der Administratorrolle „Finanzservices“ auf Anwendungsservices zugreifen, die zu der Gruppe „Finanzservices“ gehören.

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Nach Service-Mapping Erkennt zum ersten Mal Konfigurationselemente (Configuration Items, CIs), die zu Ihrer Serviceinstanz gehören, und erkennt dann CIs erneut, um Änderungen und Updates zu finden. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden. Sie können beispielsweise anwenderdefinierte Discovery-Zeitpläne erstellen, um redundante Belastungen für die Infrastruktur zu vermeiden.

Vorbereitungen
Definieren Sie Anwendungsservices, bevor Sie Erkennungszeitpläne für die Erkennung von CIs definieren, die Teil dieser Services sind.

Stellen Sie beim Erstellen eines Zeitplans für CI-Typen oder für bestimmte CIs sicher, dass sich mindestens ein Anwendungsservice, der das entsprechende CI enthält, im Status `operational` befindet.

Erfahren Sie mehr über verschiedene Arten von Discovery-Zeitpläne von oben nach unten .

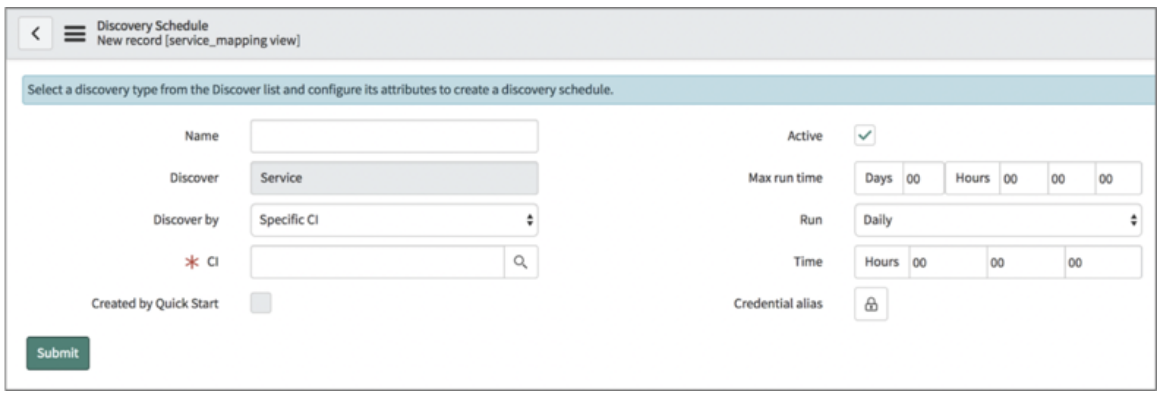
Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Discovery-Zeitpläne**an.
2. Um einen neuen Erkennungszeitplan zu erstellen, klicken Sie auf **Neu**.
   Oder

   Klicken Sie zum Anpassen des generischen Zeitplans für alle Anwendungs-CIs auf **Alle Applikationen** oder **Load Balancer-Service**.



3. Füllen Sie in neu installierten oder zurückgesetzten Instanzen die Felder im Formular „Discovery-Zeitplan“ wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie für einen neuen spezifischen Zeitplan einen eindeutigen und beschreibenden Namen ein.
Erkennen	Standardmäßig ist der Wert für dieses Feld Service, wodurch angegeben wird, dass Sie den Zeitplan für eine Erkennung von oben nach unten erstellen. Sie können diesen Wert nicht ändern.
Erkennen bis	Die Zeitplantypen für bestimmte Top Down-Discovery: ○ CI-Typ ○ Spezifischer CI ○ Serviceattribute ○ Servicegruppenattribute
CI-Typ	Dieses Feld ist verfügbar, wenn unter „Select Discovery (Erkennung auswählen)“ die Option „CI-Typ“ ausgewählt ist. Wählen Sie für einen neuen CI-Typ-basierten Zeitplan den entsprechenden Anwendungs-CI-Typ aus der Liste aus.
CI	Dieses Feld ist verfügbar, wenn Bestimmtes CI Ist aus ausgewählt **Erkennen bis** . Wählen Sie für einen neuen Zeitplan für ein bestimmtes CI das entsprechende CI aus der Liste aus.
Zu erkennende Services filtern	Dieser Bereich enthält den Bedingungsgenerator und ist verfügbar, wenn Serviceattribute Ist aus ausgewählt **Erkennen bis** . Verwenden Sie den Filter, um die Filterkriterien für Services zu erstellen. Service-Mapping erkennt nur Services, die die definierten Kriterien erfüllen.
Zu erkennende Gruppen filtern	Dieses Feld enthält den Bedingungsgenerator und ist verfügbar, wenn Servicegruppenattribute Ist aus ausgewählt **Erkennen bis** . Verwenden Sie den Filter, um die Filterkriterien für Servicegruppen zu erstellen. Service-Mapping erkennt nur Services, die zu den Gruppen gehören, die die definierten Kriterien erfüllen.

4. **Wahlweise:** Klicken Sie für einen Discovery-Zeitplan basierend auf Serviceattributen auf **Zeigen Sie Ausgewählte Services An** Um eine Vorschau der Liste der Services anzuzeigen, die die von Ihnen eingegebenen Filterkriterien erfüllen, und wählen Sie dann aus **Schließen** .
5. **Wahlweise:** Klicken Sie für einen Discovery-Zeitplan basierend auf Servicegruppenattributen auf **Zeigen Sie Ausgewählte Gruppen An** Um eine Vorschau der Liste der Gruppen anzuzeigen, die die von Ihnen eingegebenen Filterkriterien erfüllen, und wählen Sie dann aus **Schließen** .
6. Definieren Sie die Häufigkeit der erneuten Erkennung, indem Sie die entsprechende Option aus der auswählen **Ausführen** Liste.
   Weitere Informationen finden Sie unter Optionen für Discovery-Zeitpläne ausführen.
7. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

Discovery-Zeitpläne von oben nach unten

Erfahren Sie mehr über Zeitpläne, die die Top Down-Discovery von Anwendungsservices auslösen.

Wenn Sie einen neuen Anwendungsservice definieren, führt Service-Mapping die Erkennung aller CIs durch, die an diesem Anwendungsservice beteiligt sind, und erstellt die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnung. Nachdem die erste Zuordnung abgeschlossen ist, Service-Mapping Generiert Anwendungsservice-Zuordnungen regelmäßig neu, indem die CIs eines Anwendungsservice erneut erkannt werden.

Standardmäßig ist Service-Mapping mit diesen generischen Zeitplänen vorkonfiguriert:

Alle Anwendungen

Dieser Zeitplan löst die Erkennung von oben nach unten aller CIs vom Anwendungstyp [cmdb_ci_appl] aus.

Load Balancer-Service

Dieser Zeitplan startet die Erkennung von oben nach unten aller CIs des Servicetyps Lastenausgleichsmodul [cmdb_ci_lb_service].

Die generischen Zeitpläne lösen einmal täglich die Erkennung aller Anwendungen und Lastenausgleichsservices in Ihrer Organisation aus. Normalerweise reichen diese vorkonfigurierten Zeitpläne aus, um die Informationen für Anwendungsservices zu aktualisieren. Wenn jedoch bestimmte CIs oder Services häufiger erkannt werden müssen, können Sie die folgenden anwenderdefinierten Discovery-Zeitpläne erstellen:

Typen der Erkennung von oben nach unten planen

Zeitplantyp	Beschreibung	Beispiel
Services	Service-Mapping erkennt alle CIs, die zu bestimmten Services gehören und Filterkriterien erfüllen.	In Ihrem Unternehmen sind einige Anwendungsservices kritischer als andere und es ist wichtig, dass Sie die Erkennung solcher Services mit hoher Relevanz häufiger wiederholen. Erstellen Sie einen benutzerdefinierten Erkennungszeitplan, um alle Services zu erkennen, deren Wert für geschäftliche Relevanz auf `most critical` gesetzt ist. Alternativ werden bestimmte Services in Ihrer Organisation häufiger als einmal pro Tag geändert. Sie können benutzerdefinierte Zeitpläne erstellen, damit solche Services häufiger neu erkannt werden. Sie können auch einen Zeitplan dieses Typs erstellen, um Anwendungsservices in einer Test- und Entwicklungsumgebung zu erkennen, in der sich Services noch nicht im Status `operational` befinden.
Services, die zu einer Gruppe gehören	Service-Mapping erkennt alle CIs, die zu Services gehören, die Gruppen zugewiesen sind, welche Filterkriterien erfüllen. Service-Mapping erkennt nur Services, die sich direkt in der Gruppe befinden und definierte Filterkriterien erfüllen. Service-	In einer verteilten Organisation mit Büros an mehreren geografischen Standorten möchten Sie möglicherweise einen benutzerdefinierten Erkennungszeitplan erstellen, um die Erkennung von Services an einem dieser Standorte zu wiederholen. Beispielsweise kann ein Zeitplan die erneute Erkennung aller Services, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typen der Erkennung von oben nach unten planen (Fortsetzung)

Zeitplantyp	Beschreibung	Beispiel
	Mapping erkennt keine Services in eingebetteten Gruppen. Beachten Sie, dass Sie Zeitpläne basierend auf Servicegruppen definieren können, auch wenn Ihre Rolle keinen Zugriff auf diese Servicegruppen hat.	für den EMEA-Standort relevant sind, um 7 Uhr GMT auslösen, während ein anderer Zeitplan die erneute Erkennung von Services für den US-Hauptsitz um 7 Uhr PT starten kann.
Für CI-Typen	Service-Mapping erkennt alle Anwendungs-CIs, die zu diesem Anwendungstyp gehören. Einige Anwendungs-CI-Typen werden tendenziell häufiger geändert und aktualisiert als andere, daher können Sie die Last verwalten, indem Sie den Erkennungszeitplan an die Art der einzelnen CI-Typen anpassen. Wenn Sie Erkennungszeitpläne auf Grundlage von Anwendungs-CI-Typen definieren, gelten für dasselbe CI möglicherweise mehrere Zeitpläne. Um zu vermeiden, dass dieselben CIs mehr als ein Mal erkannt werden, wird dem spezifischsten Zeitplan immer Vorrang eingeräumt. Wenn Sie beispielsweise separate Erkennungszeitpläne für einen übergeordneten CI-Typ und seinen untergeordneten CI-Typ erstellen, werden CIs, die zum untergeordneten CI-Typ gehören, anhand des spezifischen Zeitplans erkannt. Wenn kein Zeitplan für einen untergeordneten CI-Typ vorhanden ist, wird für die Erkennung der untergeordneten CIs der Zeitplan des übergeordneten CI-Typs verwendet. Dieser Zeitplan erkennt nur CIs, die zu Anwendungsservices mit dem Status `operational` gehören.	Wenn Sie eine bestimmte Anwendung häufiger ändern als andere, möchten Sie die Erkennung möglicherweise häufiger durchführen als bei anderen CIs. Erstellen Sie in diesem Fall einen benutzerdefinierten Erkennungszeitplan für einen solchen Anwendungs-CI-Typ.
Bestimmte CIs	Service-Mapping erkennt nur ein einziges CI, das Sie für diesen Zeitplan angegeben haben. Wenn Sie einen Erkennungszeitplan für ein bestimmtes CI sowie einen Zeitplan	Für seltene Fälle, in denen ein bestimmtes CI neu erneut erkannt wird und häufig Erkennungsfehler verursacht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typen der Erkennung von oben nach unten planen (Fortsetzung)

Zeitplantyp	Beschreibung	Beispiel
	für den CI-Typ definieren, zu dem dieses CI gehört, verwendet Service-Mapping den Zeitplan für dieses spezifische CI und nicht den generischen Zeitplan für seinen CI-Typ. Dieser Zeitplan erkennt nur CIs, die zu Anwendungsservices mit dem Status `operational` gehören.	

Ein Teil der Erkennung eines Anwendungs-CI besteht in der Identifizierung seines Hosts. Service-Mapping prüft, ob das Gerät, das dieses Anwendungs-CI hostet, in der CMDB vorhanden ist. Für einen Lastenausgleichsservice überprüft Service-Mapping, ob das Lastenausgleichsgerät, das diesen Lastenausgleichsservice hostet, in der CMDB vorhanden ist. Wenn nicht, veranlasst Service-Mapping Discovery, eine horizontale Erkennung durchzuführen. Daher führt Discovery eine Hosterkennung durch und aktualisiert die Informationen zu den Hosts in der CMDB. Bei Bedarf können Sie die Zeitpläne, die die horizontale Erkennung auslösen, wie folgt verwalten:

- Horizontale Erkennung planen — für eine standardmäßige horizontale Erkennung
- Zeitplan für standardmäßige serverlose Erkennung erstellen – zum Erkennen von CIs mithilfe eines Protokolls wie REST, ohne die IP-Adresse von Geräten oder Hosts zu verwenden
- Zeitplan für hostbasierte serverlose Erkennung erstellen – zum Erkennen von CIs, die sich auf einem bereits erkannten Host befinden und diesen Host als Proxy-Server verwenden

Zugehörige Informationen

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Servicedefinition von einer Instanz zur anderen übertragen

Sparen Sie Zeit und Aufwand, indem Sie Definitionen von Serviceinstanzen aus der Quellinstanz exportieren und diese Definitionen in die Zielinstanz importieren. Sie können diese Methode verwenden, um Definitionen von Serviceinstanzen nur des erkannten Typs zu kopieren.

Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: eine für die Produktion und eine für die Entwicklung. Führen Sie die erste Zuordnung von Anwendungsservices in Ihrer Organisation in der Entwicklungsinstanz durch, die Sie zum Testen verwenden. Die Ergebnisse der anfänglichen Zuordnung erfordern häufig eine grundlegende Fehlerbehebung oder Feinabstimmung. Sobald Sie die Zuordnung der Anwendungsservices in Ihrer Quellinstanz abgeschlossen haben, übertragen Sie die Servicedefinitionen auf die Ziel- bzw. Produktionsinstanz.

Beachten Sie, dass Sie nicht die tatsächlichen Anwendungsservices exportieren können, sondern nur die Servicedefinitionen. Die Zuordnung ist ein dynamischer Prozess, und das Zuordnungsergebnis spiegelt die tatsächliche Infrastruktur und deren Konfiguration wider. Daher sehen die Services, die Sie aus einer Instanz exportiert und in eine andere importiert haben, möglicherweise unterschiedlich aus.

Standardmäßig exportieren Sie die folgenden Servicedefinitionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Servicename
- Nutzung der datenverkehrsbasierten Erkennung
- Eingabepunkt
- Business-Relevanz
- Gruppe, zu der der Service gehört

  Wenn diese Servicegruppe Teil einer Servicegruppenhierarchie ist, werden auch alle übergeordneten Servicegruppen in dieser Hierarchie exportiert.

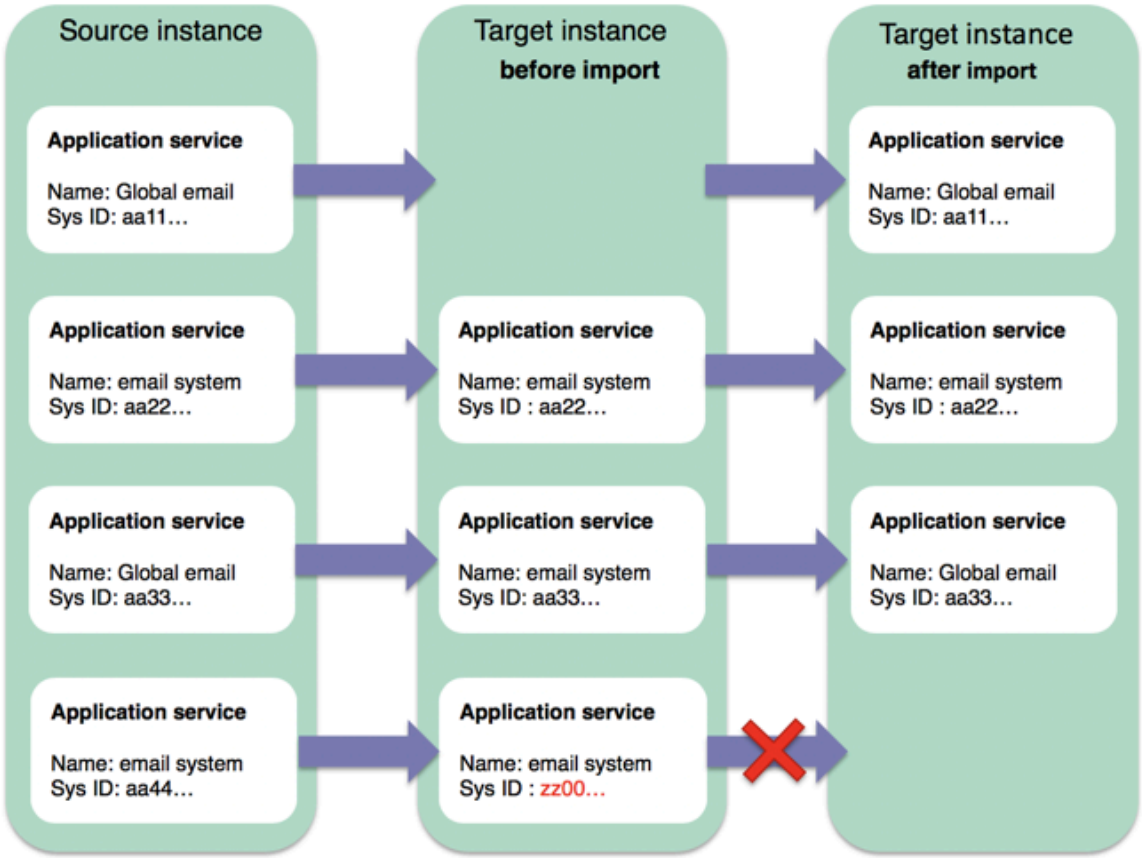
- Kommentare

Das System verwendet das Sys-ID-Attribut [sys_id], um Services in den Quell- und Zielinstanzen zu identifizieren, und implementiert den Import von Servicedefinitionen gemäß den folgenden Regeln:

- Wenn in der Zielinstanz keine Service-Sys-ID vorhanden ist, erstellt das System in der Zielinstanz einen neuen Service.
- Wenn in der Zielinstanz bereits eine Sys-ID und ein Name für einen Service vorhanden sind, aktualisiert das System diesen Service, indem die vorhandenen Servicedefinitionen mit den importierten Definitionen überschrieben werden.
- Wenn in der Zielinstanz eine Service-Sys-ID vorhanden ist, die jedoch einem anderen Servicenamen zugeordnet ist, aktualisiert das System den Service mit dieser Sys-ID. Das System überschreibt Servicedefinitionen, einschließlich des Servicenamens.
- Wenn derselbe Name in der Quell- und Zielinstanz für verschiedene Services verwendet wird, importiert das System keine Servicedefinitionen.
- Manuelle Services können nicht exportiert werden. Ebenso können Sie manuell hinzugefügte Einstiegspunkte nicht exportieren. Beim Importieren von Definitionen eines Service mit manuellen Einstiegspunkten nimmt das System keine Änderungen an den Einstiegspunkten vor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow für Servicedefinitionen exportieren



Beim Übertragen von Servicedefinitionen zwischen Instanzen werden importierte Serviceinstanzen und Servicegruppen der Domäne des Anwenders zugewiesen.

Standardmäßig weist das System Anwendungsservices, deren Definitionen Sie importiert haben, den Status `Non-operational` zu.

Bei der Übertragung von Servicedefinitionen wird die Standardfunktion für Import Sets bereitgestellt, die auf der ServiceNow AI Platform verfügbar ist. Wenn Sie Servicedefinitionen aus der Quellinstanz exportieren, erstellt das System eine JSON-Datei mit den exportierten Daten. Wenn Sie Servicedefinitionen in die Zielinstanz kopieren, importieren Sie die Daten aus dieser JSON-Datei, die zu einem Import Set wird.

Servicedefinitionen exportieren

Erstellen Sie ein Import Set, das Servicedefinitionen enthält. Dieses Import Set verwenden Sie, um Servicedefinitionen in eine andere Instanz zu importieren.

Vorbereitungen

- Entscheiden Sie, welche Servicedefinitionen Sie exportieren möchten.

  Wichtig: Sie können diese Methode verwenden, um Definitionen von Anwendungsservices nur des erkannten Typs zu kopieren.

- Stellen Sie sicher, dass sich die Quell- und Zielinstanzen im selben ServiceNow-Release befinden.

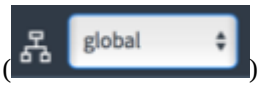
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Öffnen Sie die Quellinstanz, aus der Sie Servicedefinitionen kopieren möchten.
- Optimieren Sie bei Bedarf die Erstellung des Importsatzes, indem Sie relevante Eigenschaften unter ändern **Service-Mapping** > **Administration** > **Eigenschaften**an. Weitere Informationen finden Sie unter Mit Service-Mapping installierte Komponenten.

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Wenn Ihre Instanz Domänentrennung nutzt und Sie Zugriff auf die globale Domäne haben, wählen Sie die Domäne, zu der der Serviceinstanz gehört, über die Domänenauswahl (

) aus.
Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.
2. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**an.
3. Wählen Sie die Anwendungsservices aus, die Sie exportieren möchten.
4. Klicken Sie am unteren Seitenrand auf **Aktionen für ausgewählte Zeilen**, und wählen Sie **Export Services (Services exportieren)** aus.
Das Import Set wird im Ordner Downloads angezeigt. Der Dateiname folgt der folgenden Konvention: export_service_<DatumUhrzeit>.json.
5. Kopieren Sie bei Bedarf das Import Set an einen anderen Speicherort auf dem Computer.

Servicedefinition aus einer Instanz in eine andere importieren

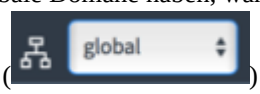
Importieren Sie Definitionen der Anwendungsservices aus der Quellinstanz.

Vorbereitungen

- Stellen Sie sicher, dass sich die Quell- und Zielinstanzen im selben ServiceNow-Release befinden.
- Öffnen Sie die Zielinstanz, in die Sie Servicedefinitionen kopieren möchten.

Erforderliche Rolle: import_admin

Prozedur

1. Wenn Ihre Instanz Domänentrennung nutzt und Sie Zugriff auf die globale Domäne haben, wählen Sie die Domäne, zu der der Serviceinstanz gehört, über die Domänenauswahl (

) aus.
Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.
2. Navigieren zu **Service-Mapping** > **Services** > **Servicedefinitionen importieren**an.
3. Klicken Sie im Fenster „Servicedefinitionen importieren“ auf **Datei auswählen**, navigieren Sie zur JSON-Datei, die Servicedefinitionen enthält, und klicken Sie auf **OK**.
4. **Wahlweise:** Klicken Sie auf **Vorschau anzeigen**, und überprüfen Sie die Definitionen in der ausgewählten JSON-Datei.
5. Klicken Sie auf **Importieren**.
6. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie zum Importieren von Servicedefinitionen bereit sind.

> **Wichtig:** Während des Imports überschreibt das System die aktuellen Servicedefinitionen unwiderruflich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fortschrittsfenster zeigt die Erfolgsnachricht an.

Service-Mapping startet automatisch die Erkennung von Services, die importierte Einstiegspunkte enthalten.

7. Überprüfen Sie importierte oder aktualisierte Services, nachdem Service-Mapping den Zuordnungsprozess abgeschlossen hat.
   Wenn das Übertragungsergebnis nicht Ihren Erwartungen entspricht, gehen Sie wie in der folgenden Tabelle beschrieben vor, um eine grundlegende Fehlerbehebung durchzuführen.

Trouble?

Symptom	Ursache	Lösung
Kürzlich an einem Serviceinstanz vorgenommene Änderungen werden nicht angezeigt.	Definitionen von vorhandenen Anwendungsservices werden während der Übertragung immer überschrieben.	1. Nehmen Sie die erforderlichen Änderungen an den Definitionen dieses Serviceinstanz erneut vor. 2. Führen Sie die Erkennung von oben nach unten dieses Serviceinstanz aus, indem Sie in der Servicezuordnung auf **Discovery ausführen** klicken.
Eine importierte Servicegruppe wird nicht angezeigt.	Der Import eines dieser Gruppe zugewiesenen Anwendungsservice ist fehlgeschlagen und die Gruppe wurde vom System nicht erstellt, da sie leer zu sein scheint.	1. Beheben Sie das Problem, das verhindert hat, dass das System den Serviceinstanz importiert, der zu dieser Gruppe gehört. 2. Importieren Sie das Import Set erneut. 3. Überprüfen Sie, ob die Servicegruppe angezeigt wird.
Einer importierten Servicegruppe wurden anscheinend falsche Anwendungsservices zugewiesen.	Dies ist eine andere Servicegruppe mit demselben Namen, nicht die von Ihnen importierte Servicegruppe. Das System konnte die Servicegruppe nicht importieren, da die Quellinstanz bereits eine Servicegruppe mit demselben Namen bzw. mit demselben Namen und derselben Sys-ID hat.	1. Überprüfen Sie das Importprotokoll. 2. Wenn ein Fehler besagt, dass eine Datensatzerstellung während der Ausführung der Geschäftsregel „Check Name Uniqueness (Eindeutigkeit des Namens prüfen)“ fehlgeschlagen ist, gehen Sie wie folgt vor: a. Benennen Sie die Servicegruppe in der Quellinstanz um. b. Exportieren Sie die dieser Gruppe zugewiesenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
		Anwendungsservices erneut. **c.** Importieren Sie das letzte Import Set in die Zielinstanz. **3.** Wenn ein Fehler besagt, dass eine Datensatzerstellung fehlgeschlagen ist, weil die Sys-ID bereits vorhanden ist, gehen Sie wie folgt vor: **a.** Erstellen Sie die Servicegruppe in der Quellinstanz neu, und achten Sie darauf, dass Sie einen anderen Gruppennamen und eine andere Sys-ID angeben. **b.** Exportieren Sie die dieser Gruppe zugewiesenen Anwendungsservices erneut. **c.** Importieren Sie das letzte Import Set in die Zielinstanz. **4.** Stellen Sie sicher, dass die Servicegruppe in der Quellinstanz korrekt angezeigt wird.

Analyse und Wartung von Anwendungsservices mithilfe von klassisch Service-Mapping

Service-Mapping erstellt Zuordnungen, mit deren Hilfe Sie die Architektur und Organisation von Anwendungsservices anzeigen können. Diese Zuordnungen sind nützlich bei der Planung von Änderungen oder Migrationen sowie zur Analyse der Kontinuität und Verfügbarkeit von Services.

Zuordnungen sind in folgenden Fällen nützlich:

Migration eines kompletten Serviceinstanz oder seiner Segmente planen

Verwenden Sie die Zuordnung, um anzuzeigen, welche Konfigurationselemente (CIs) verschoben werden müssen oder welche CIs redundant werden.

Upgrade oder Ersetzung eines CI planen

Überprüfen Sie die Zuordnung, um zu sehen, welche anderen CIs betroffen sind, wenn das CI während der Wartung nicht betriebsbereit ist. Sie können die Ausfallzeit bewerten und planen oder Vorkehrungen treffen, um Ausfallzeiten zu vermeiden.

Da dasselbe CI für mehrere Anwendungsservices verwendet werden kann, überprüfen Sie das CI mit der Anwendung Dependency Views. Mit dieser Anwendung können Sie alle Anwendungsservices anzeigen, zu denen ein CI gehört.

Serviceinstanz auf hohe Verfügbarkeit und Kontinuität analysieren

Verwenden Sie die Zuordnung, um CIs zu identifizieren, die für die Serviceleistung wichtig sind. Entscheiden Sie, ob Sie diese CIs durch die Erstellung von Clustern stärken möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehebung bei Anwendungsservices

Verwenden Sie die Zuordnung, um die Auswirkungen eines Problems zu verstehen und zu bestimmen, welches CI das Problem verursacht.

Anwendungsservicezuordnungen in klassisch Service-Mapping

Zuordnungen bieten Ihnen eine Visualisierung von Daten zu Konfigurationselementen (CIs), die Anwendungsservices umfassen, sowie Beziehungen und Verbindungen zwischen diesen CIs.

Eine neue Zuordnung wird jedes Mal erstellt, wenn Sie einen Anwendungsservice manuell erstellen oder einen Anwendungsservice mithilfe von Service-Mapping zuordnen. Das System aktualisiert die Zuordnung jedes Mal, wenn Sie dem Anwendungsservice CIs hinzufügen oder wenn Service-Mapping eine Erkennung für CIs ausführt, die zu diesem Anwendungsservice gehören.

Hinweis:

Die für eine Zuordnung verfügbaren Informationen und Aktionen hängen von Ihrer Rolle ab:

- Als Serviceanwender [App_Service_user] oder Service-Mapping Anwender [Service_Mapping_user], können Sie die Karte im Ansichtsmodus anzeigen.
- Als Serviceadministrator [App_Service_admin] oder Service-Mapping Administrator [Service_Mapping_admin], Sie können Anwendungsservices im Ansichtsmodus anzeigen und erkannte und manuell erstellte Services im Bearbeitungsmodus ändern.

  Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

- Als Service-Mapping Administrator [Service_Mapping_admin], Sie können von generierte Discovery-Nachrichten und Fehler anzeigen Service-Mapping Und ändern Sie Services im Bearbeitungsmodus. Außerdem können Sie die Zuordnung neu laden, um sicherzustellen, dass sie die neuesten Informationen enthält.
- Als Serviceverantwortlicher [sm_app_owner] können Sie Services, die mithilfe von Service-Mapping erkannt wurden, im Ansichtsmodus anzeigen, Feedback hinterlassen und genehmigen.

  Hinweis: Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

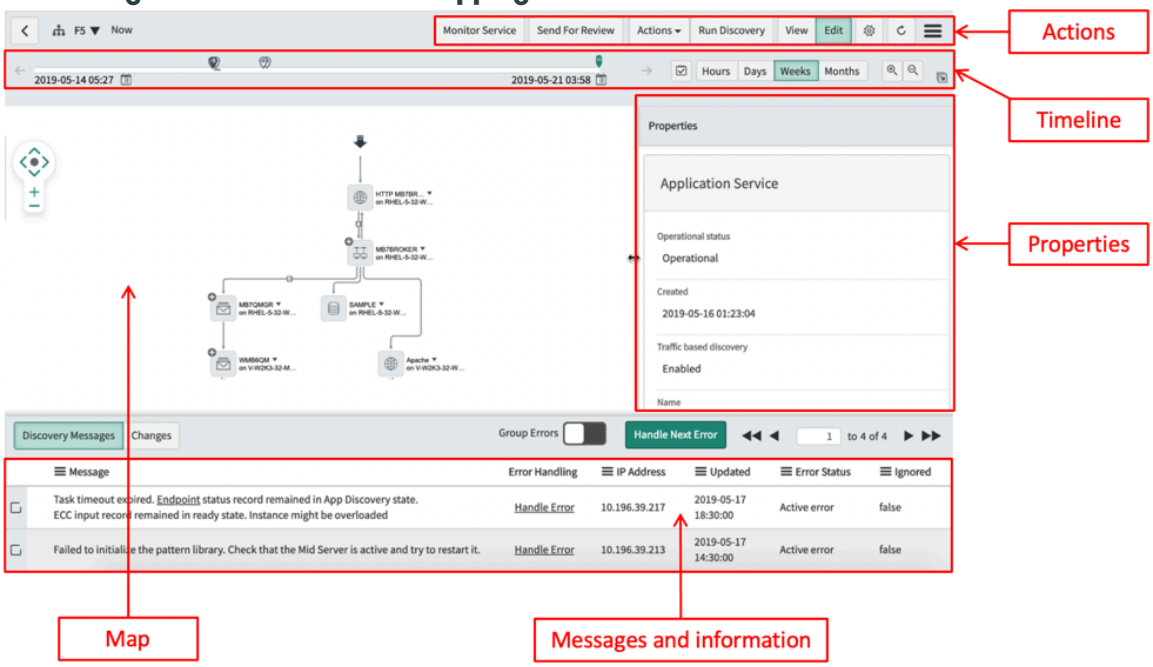
Aktionen und Informationen sind im Zusammenhang mit der automatischen Erkennung mit Service-Mapping sind nicht verfügbar bei CIs, die Service-Mapping nicht erkennen kann. Beispiel: Für manuell erstellte Serviceinstanz , die Service-Mapping nicht erkennt, wird die Registerkarte „Discovery-Nachrichten“ nicht angezeigt.

Zuordnungsfenster

Neben der Zuordnung selbst werden im Zuordnungsfenster auch der Bereich „Eigenschaften“ und Registerkarten mit zusätzlichen Informationen angezeigt.

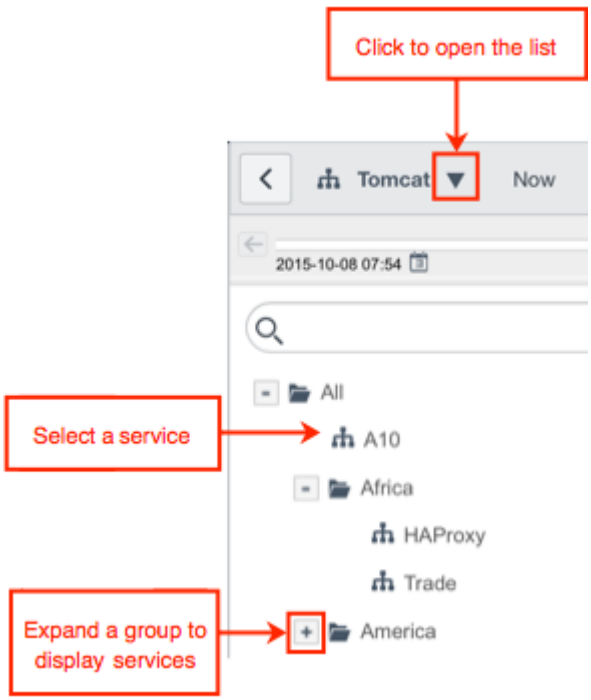
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsfenster von Service-Mapping



Von diesem Fenster aus können Sie direkt zu einer anderen Anwendungsservicezuordnung navigieren, indem Sie diesen in der Liste auswählen.

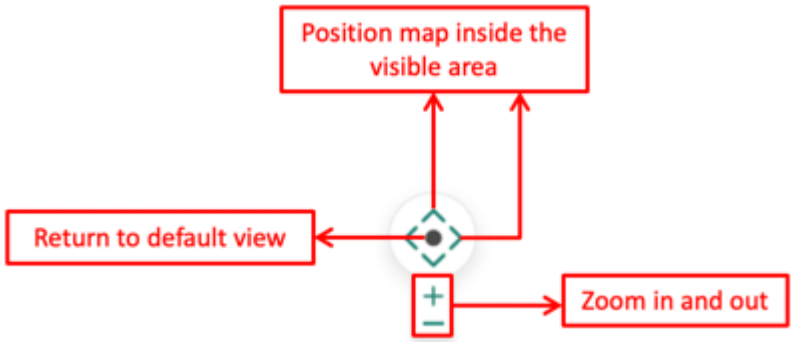
Serviceliste



Standardmäßig wird die gesamte Zuordnung in der Mitte des sichtbaren Fensterbereichs der Zuordnung angezeigt. Mit den folgenden Steuerungen können Sie die Zuordnung vergrößern und verkleinern sowie positionieren, je nachdem, welches Segment der Zuordnung Sie sehen möchten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsnavigation



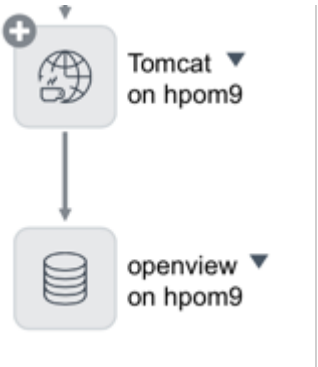
Sie können auch auf eine beliebige Stelle im Zuordnungsbereich klicken und das gewünschte Segment der Zuordnung in den sichtbaren Bereich ziehen.

Sie können Änderungen an einem Serviceinstanz als Ganzes sowie an einzelnen CIs anzeigen, die zu einem Service gehören, indem Sie einen Zeitraum auswählen. Weitere Informationen finden Sie unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen.

Elemente und ihr Erscheinungsbild zuordnen

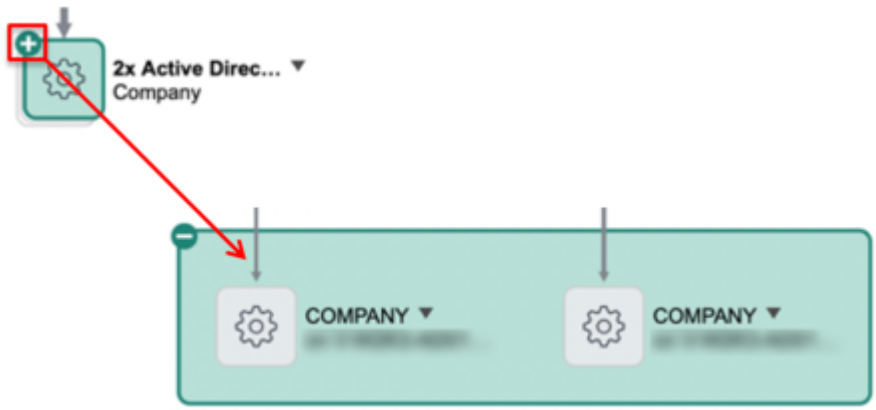
Jede Zuordnung besteht aus Symbolen, die CIs darstellen, und Pfeilen, die die Verbindungen zwischen diesen darstellen.

Verbundene CIs



Einige Zuordnungselemente (wie Anwendungscluster) können weitere Elemente enthalten. In der Zuordnung werden Anwendungscluster als Stapel von CIs mit Pluszeichen (+) daneben angezeigt. Die Clusterbezeichnung enthält die Anzahl der CIs im Cluster mit dem Multiplikationszeichen.

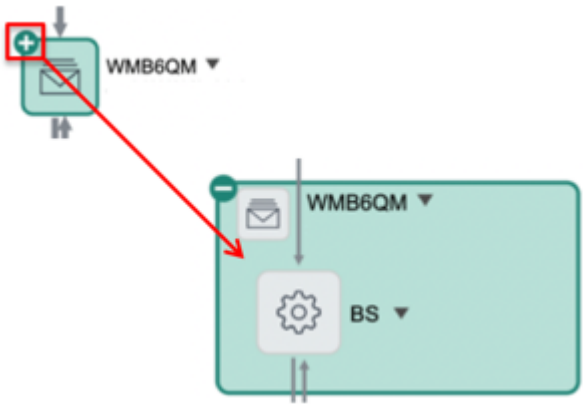
CI-Cluster



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das CI Inklusionen aufweist, wird neben dem CI-Symbol das Pluszeichen (+) angezeigt, und die enthaltene Anwendung wird angezeigt, wenn Sie es erweitern.

Inklusion



Ein BS-Cluster wird als CI mit einem Pluszeichen und der Anzahl der CIs im Cluster angezeigt.

BS-Cluster-CI

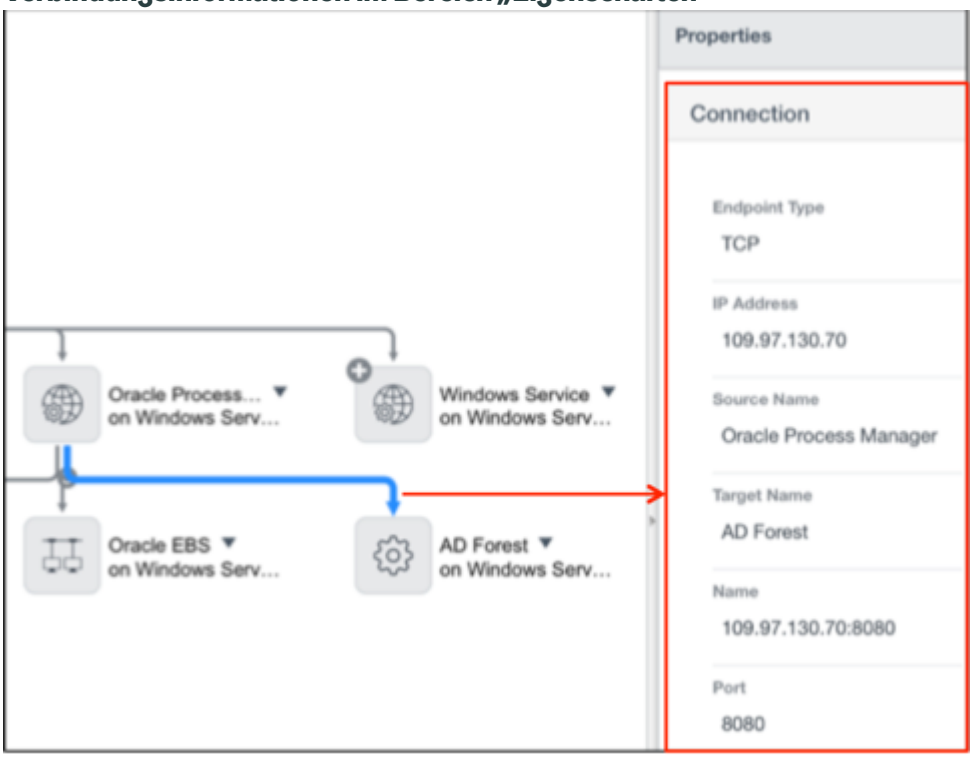
CI-Attribute und CI-bezogene Nachrichten

Wenn eine Zuordnung geladen ist und keine Elemente ausgewählt sind, werden im Eigenschaftenbereich die Details dieses Serviceinstanz angezeigt.

Ausgewählte Geräte, Anwendungen oder Connectors werden blau angezeigt und sind hervorgehoben. Informationen zum ausgewählten Zuordnungselement werden im Eigenschaftenbereich rechts von der Zuordnung angezeigt. Der Bereich „Eigenschaften“ enthält die Links zur Seite „Detaillierte Eigenschaften“.

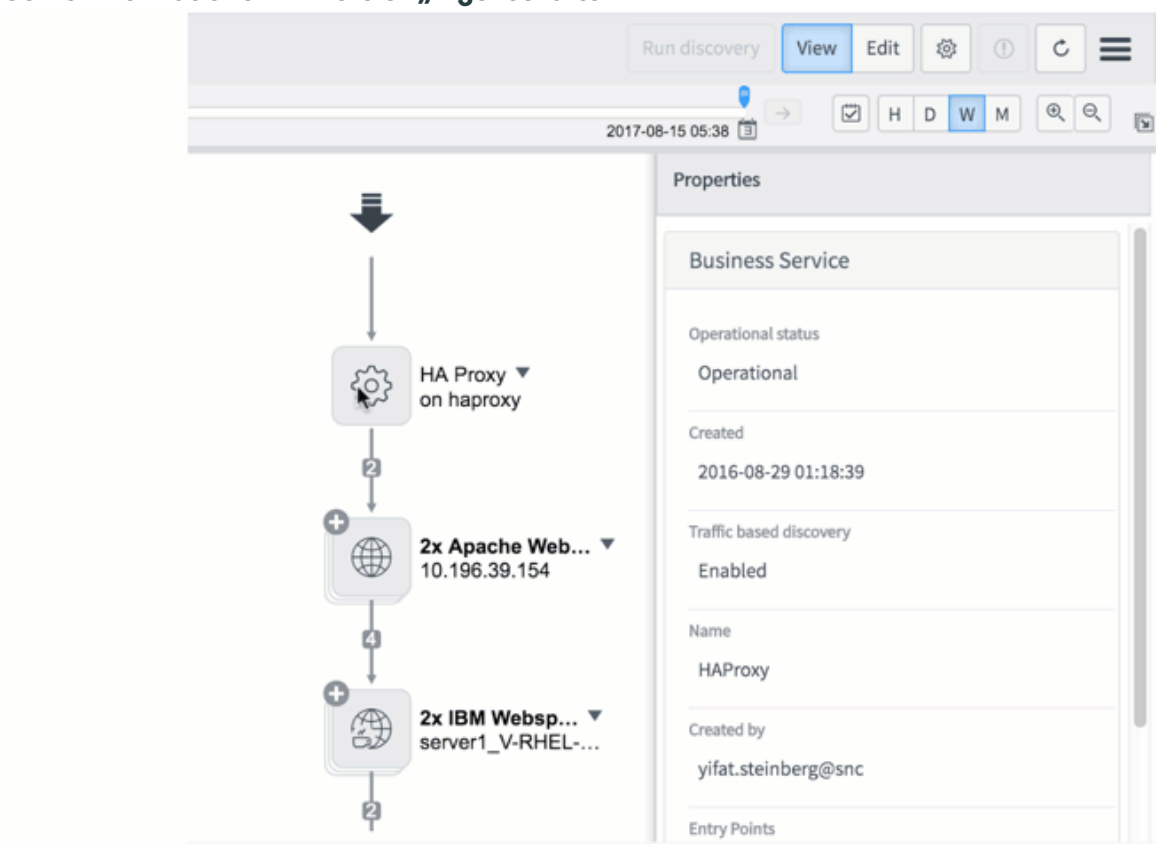
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungsinformationen im Bereich „Eigenschaften“



Die Attribute für den Server, auf dem die Anwendungen gehostet werden, und die Anwendungen selbst werden im Bereich „Eigenschaften“ getrennt angezeigt.

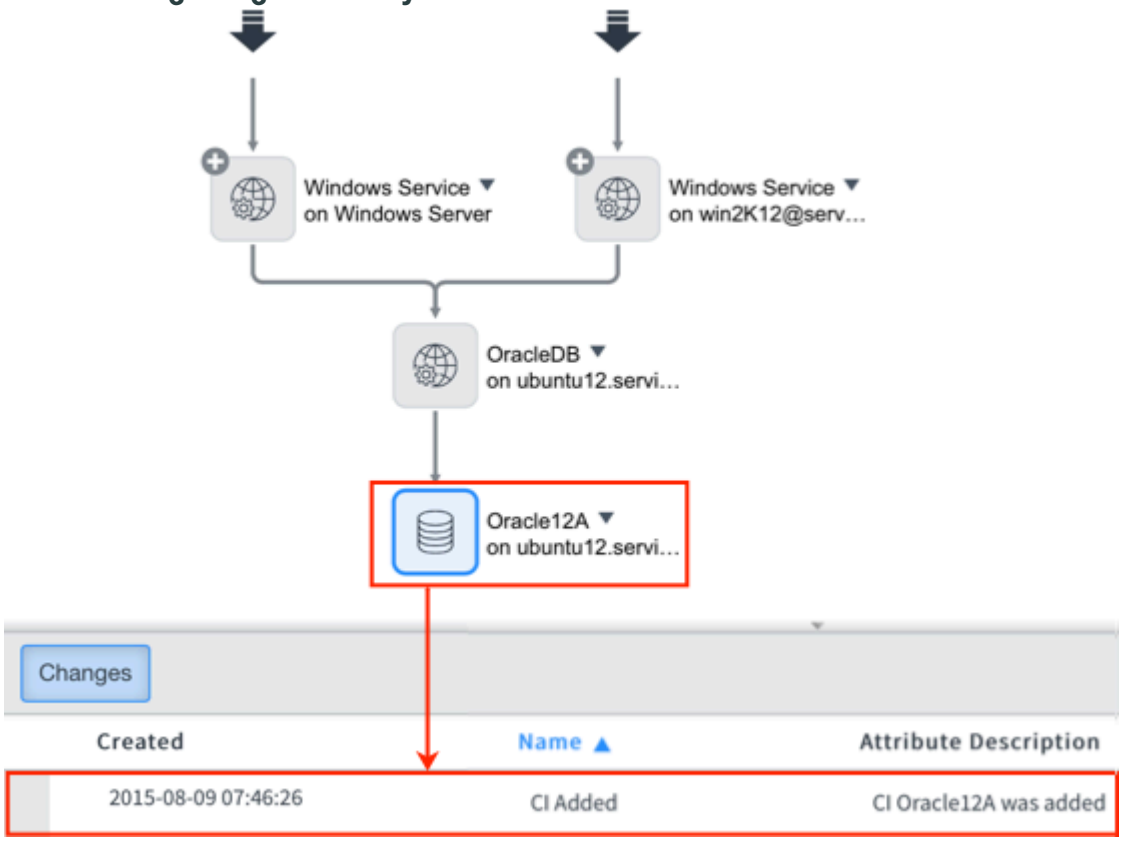
Serverinformationen im Bereich „Eigenschaften“



Wenn Informationen zum ausgewählten CI oder zur ausgewählten Verbindung vorhanden sind, werden diese auf der Registerkarte unten im Fenster hervorgehoben.

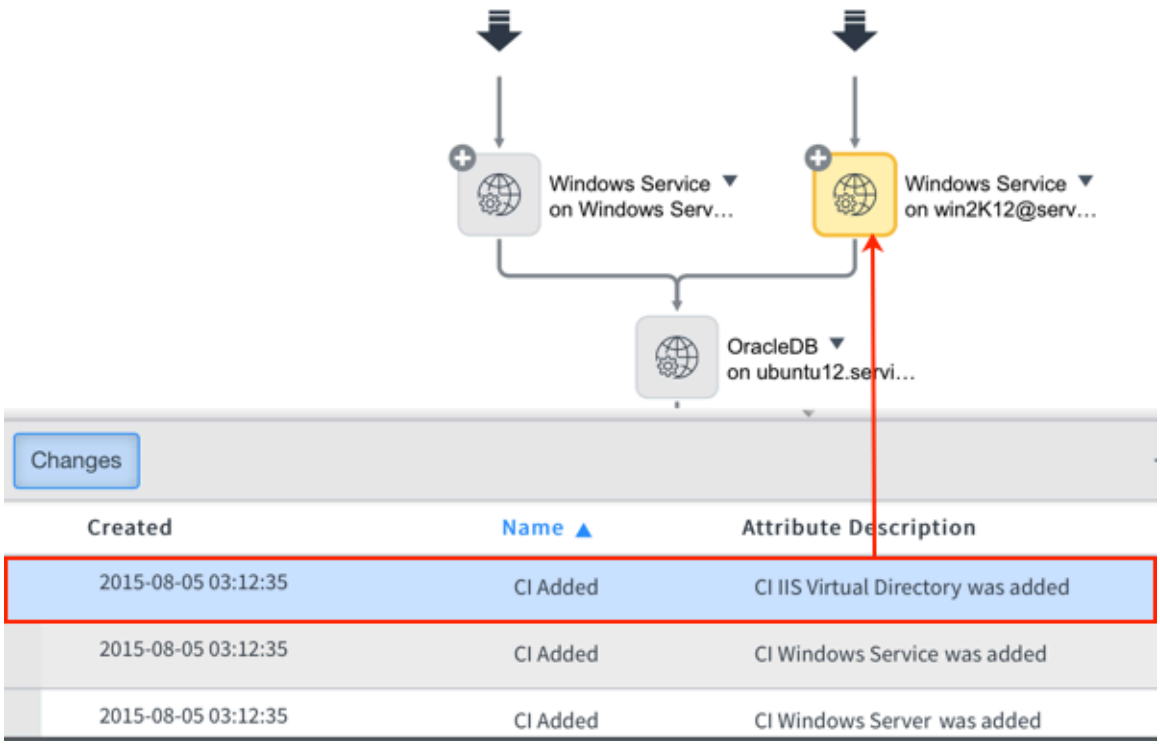
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI und die zugehörige Discovery-Nachricht



Wenn Sie Informationen auf einer Registerkarte im Zuordnungsfenster unten auswählen, wird das zugehörige CI in Gelb angezeigt.

Die Meldung und das CI, für das sie generiert wird

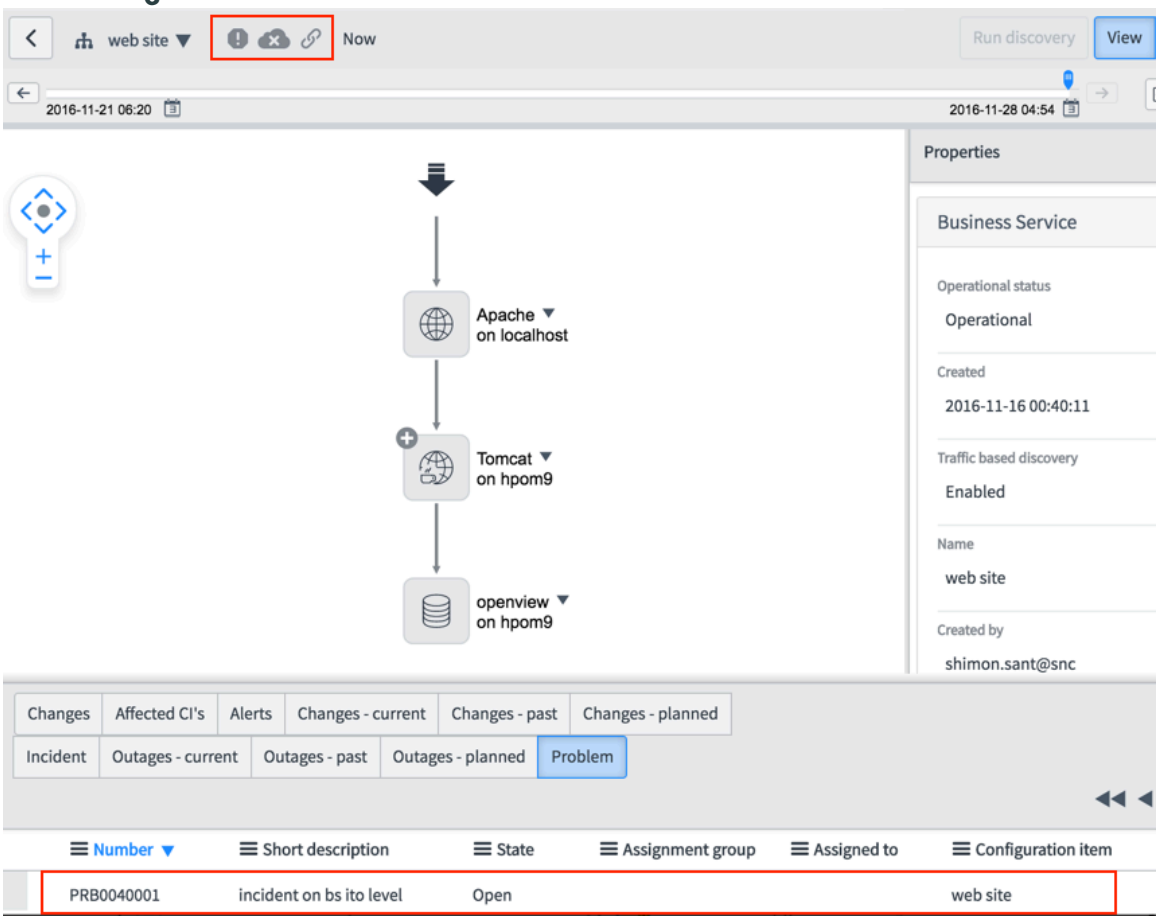


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsindikatoren

Sie können zusätzliche Informationen für ein CI oder den Serviceinstanz selbst anzeigen, indem Sie zugehörige Datensätze anzeigen, zum Beispiel Warnungen, Ausfälle, Incidents und Probleme. Wenn Sie diese Funktion aktivieren, werden neben relevanten CIs und dem Namen des Serviceinstanz Datensatzindikatoren angezeigt. Die Datensätze selbst werden auf den Registerkarten unten im Zuordnungsfenster angezeigt.

Anwendungsservice mit Indikatoren

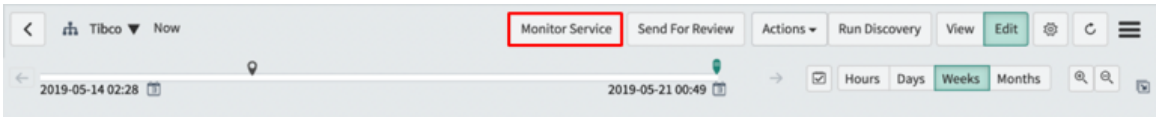


Zuordnungsansichten

Passen Sie eine Zuordnungsansicht an, um irrelevante Informationen auszuschließen und die Übersichtlichkeit zu erhöhen (siehe Beschreibung in Ansicht für Anwendungsservicezuordnung ändern).

Um diesen Serviceinstanz im Ereignismanagement zu öffnen und Warnungen zu CIs anzuzeigen, die Teil des Serviceinstanz sind, klicken Sie oben im Fenster auf **Service überwachen**.

Schaltfläche „Service überwachen“



Zugehörige Informationen

Zeigen Sie CI-Attribute in einer Anwendungsservice-Zuordnung in an klassisch Service-Mapping

Anzeige für CI-Attribute ändern

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht für Anwendungsservicezuordnung ändern

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Zeigen Sie CI-Attribute in einer Anwendungsservice-Zuordnung in an klassisch Service-Mapping

Die Anwendungsservicezuordnung zeigt Attribute für jedes Configuration Item (CI), das Teil des Anwendungsservice ist, sowie für den Anwendungsservice selbst an. Die Attribute stammen aus dem CMDB.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können für jedes CI die folgenden Informationen anzeigen:

Namensschild

Der CI-Name. Dieses Attribut wird entweder im CI vorkonfiguriert oder während der CI-Installation konfiguriert.

Grundlegende Attribute

Eine Zusammenfassung der wichtigsten CI-Attribute.

Detaillierte Attribute

Eine vollständige Liste aller für das CI erfassten Attribute.

Jeder CI-Typ (CI-Klasse) hat unterschiedliche Attribute. Beispielsweise hat der Linux-Server-Typ andere Attribute als der SQL-Instanz-Typ.

Wenn Service-Mapping Wird bereitgestellt, hängt die Art und Weise, wie CIs auf der Karte angezeigt werden, von ab Ansicht, die Sie für die Karte auswählen . Die zur Ansicht verfügbaren Attribute hängen auch von dem Service-Mapping Setup ab. Weitere Informationen finden Sie unter Beschreibung von Mit Service-Mapping installierte Komponenten .

Prozedur

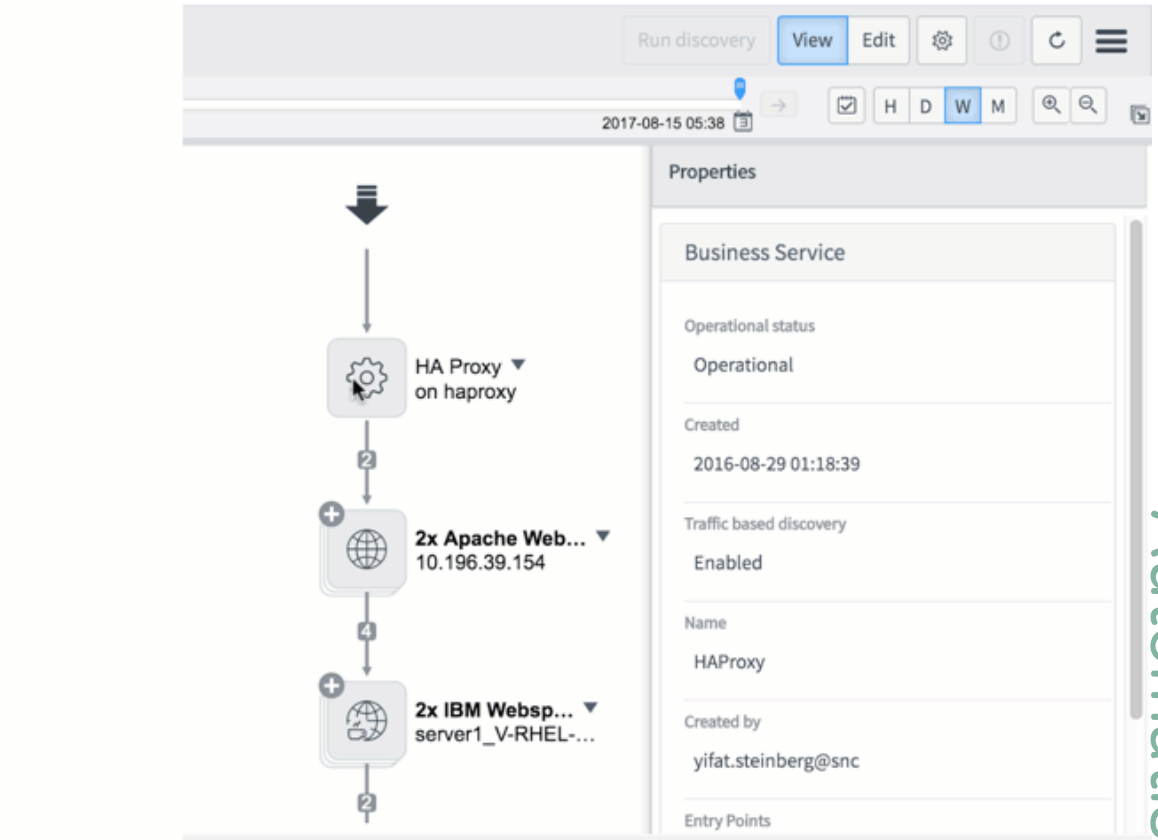
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Um den vollständigen Namen eines CI anzuzeigen, dessen Name auf der Karte gekürzt wurde, zeigen Sie auf das CI.

   Ein Tooltip zeigt den vollständigen CI-Namen an.
4. Klicken Sie auf ein CI, um seine Details im Bereich **Eigenschaften** anzuzeigen.

   Die Attribute von Anwendungen und die Server, auf denen sie gehostet werden, werden separat angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Um detailliertere Attribute für das CI anzuzeigen, klicken Sie auf **Detaillierte Eigenschaften** am unteren Rand des Bereichs „Eigenschaften“.
6. **Wahlweise:** Gehen Sie folgendermaßen vor, um Konfigurationsdateien anzuzeigen, die einem CI in Umgebungen zugeordnet sind, in denen Service-Mapping oder Discovery sowie die Nachverfolgung von Änderungen an Konfigurationsdateien für ein CI aktiviert sind:
   - Überprüfen Sie die Liste der Dateien unter **Verfolgte Dateien** im Bereich **Eigenschaften**. Klicken Sie auf den Dateinamen, um die tatsächliche Datei zu öffnen.
   - Klicken Sie auf die Registerkarte **Betroffene CIs**, und zeigen Sie die Liste der Konfigurationsdateien an. Klicken Sie auf den Dateinamen, um die tatsächliche Datei zu öffnen.

Zeigen Sie CI-Verbindungsattribute in einer Anwendungsservicezuordnung an klassisch Service-Mapping

Sie können Attribute von Verbindungen zwischen Konfigurationselementen (CIs) anzeigen.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

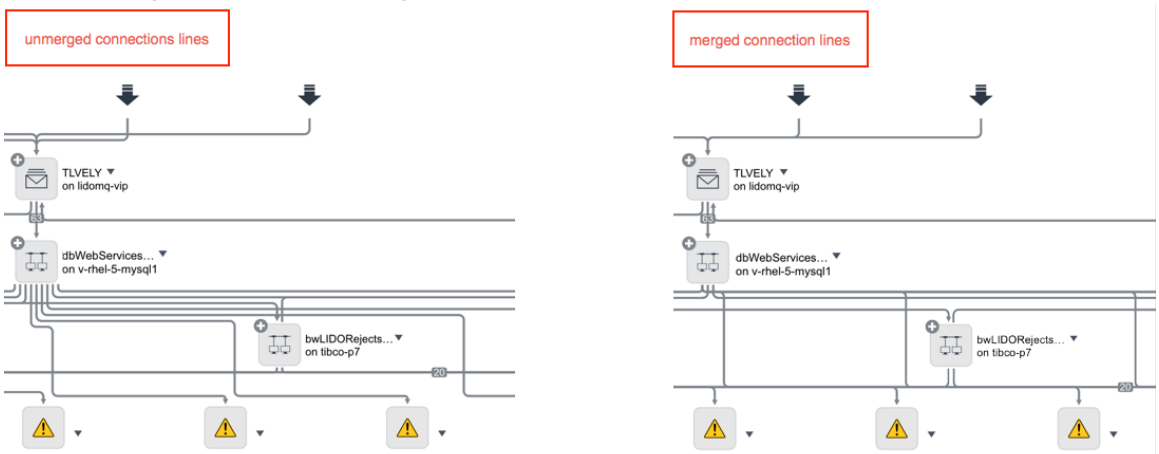
Für jede Verbindung können Sie die folgenden Informationen anzeigen:

- Quell- und Ziel-CIs einer Verbindung im Kontextmenü (Rechtsklick-Menü)
- Vollständige Liste aller über die Verbindung erfassten Attribute im Bereich „Eigenschaften“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig führt Service-Mapping Verbindungslinien für dasselbe CI zusammen, damit die Anwendungsservicezuordnung übersichtlich bleibt. Dadurch lässt sich die Zuordnung leichter interpretieren.

Zusammengeführte Verbindungslinien



Jeder Verbindungstyp besitzt andere Attribute. Für eine zusammengeführte Verbindungslinie werden alle zugrunde liegenden Verbindungen aufgelistet.

Wie in der Zuordnung eines Serviceinstanz Verbindungsattribute angezeigt werden, hängt von folgenden Faktoren ab:

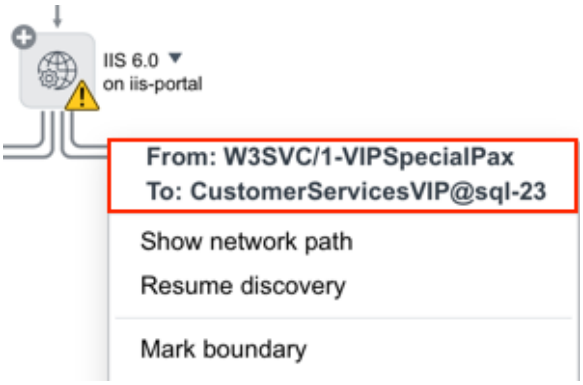
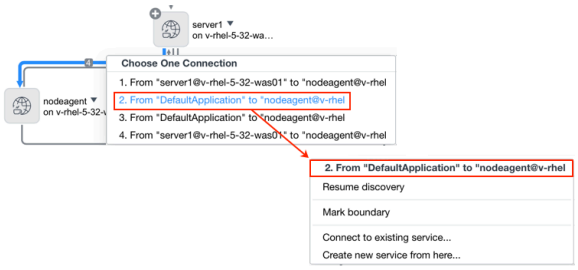
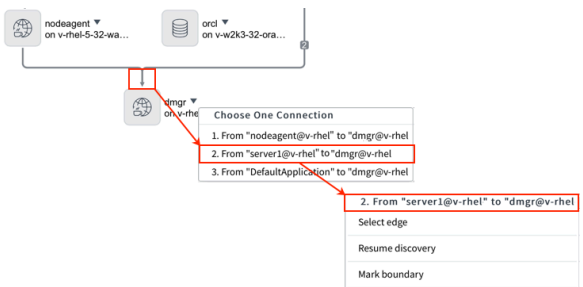
- Ansichten, die Sie für CIs konfigurieren Definieren Sie, welche Verbindungsattribute im Eigenschaftenbereich der Karte angezeigt werden.
- Verbindungslinien in der Zuordnung sind abhängig von der Ansicht, die Sie für die Zuordnung auswählen.
- Zum Anzeigen verfügbare Attribute hängen ebenfalls vom Setup von Service-Mapping ab. Weitere Informationen finden Sie in der Beschreibung der mit Service Mapping installierten Komponenten.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Zeigen Sie Verbindungsattribute wie folgt an:

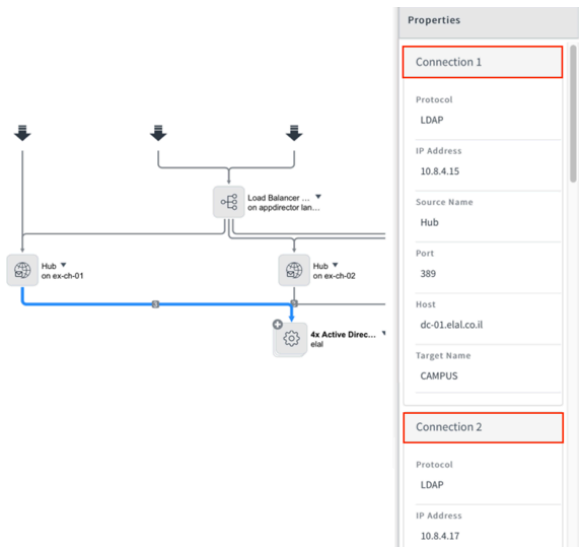
Anzuzeigende Elemente	Aktion
Quell- und Ziel-CI einer regulären Verbindung	Klicken Sie mit der rechten Maustaste auf die Verbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

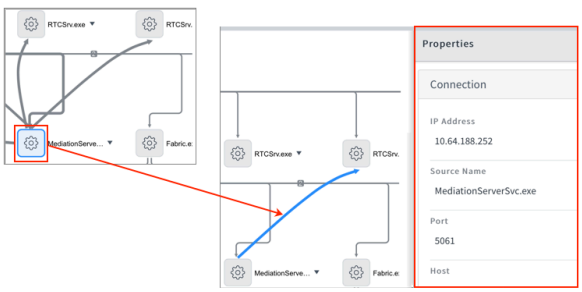
Anzuzeigende Elemente	Aktion
	
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Quell- und Ziel-CI einer zusammengeführten Verbindung	○ Klicken Sie mit der rechten Maustaste auf die zusammengeführte Verbindungslinie mit einer Zahl, und wählen Sie die entsprechende Verbindung aus.  Oder ○ Wenn ein Segment einer Verbindungslinie von mehreren zusammengeführten Verbindungen gemeinsam verwendet wird, gibt es keinen Hinweis darauf, dass es sich um eine zusammengeführte Linie handelt. Klicken Sie mit der rechten Maustaste auf die Verbindungslinie, die aus einem CI heraus- oder in ein CI hineinführt, und wählen Sie die entsprechende Verbindung aus. 
Quell- und Ziel-CI einer Verbindung, wenn die Bereichsstrukturansicht aktiviert ist Die Spanning Tree-Ansicht vereinfacht eine Serviceinstanz	**a.** Klicken Sie auf das CI, dessen Verbindungen Sie anzeigen möchten. In der Zuordnung werden alle verborgenen Verbindungen für dieses CI angezeigt.

Automatische Übersetzung

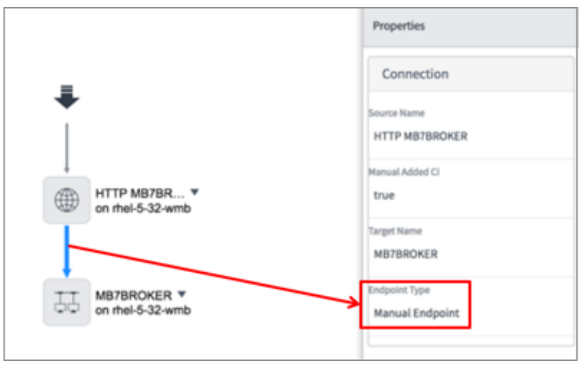
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
zuordnung, bei der die meisten Verbindungslinien verborgen sind.	**b.** Klicken Sie mit der rechten Maustaste auf die entsprechende Verbindungslinie.
Detailattribute einer regulären Verbindung im Bereich **Eigenschaften**	Klicken Sie auf die Verbindungslinie.
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Detailattribute einer zusammengeführten Verbindung im Bereich **Eigenschaften**.	Klicken Sie auf die zusammengeführte Verbindungslinie, die mit einer Zahl gekennzeichnet ist. Alle zugrunde liegenden Verbindungen werden im Bereich **Eigenschaften** separat angezeigt. 
Detailattribute eines Verbindungssegments, das von mehr als einer zusammengeführten Verbindung genutzt wird, im Bereich **Eigenschaften**	Klicken Sie mit der rechten Maustaste auf die Verbindungslinie, die aus einem CI heraus- oder in ein CI hineinführt, und wählen Sie die entsprechende Verbindung sowie anschließend **Edge auswählen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
	Die Detailattribute werden im Bereich **Eigenschaften** angezeigt. **Hinweis:** Bei gemeinsam genutzten Segmenten gibt es keinen Hinweis darauf, dass es sich um eine zusammengeführte Linie handelt.
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Detaileigenschaften einer Verbindung im Bereich **Eigenschaften**, wenn die Bereichsstrukturansicht aktiviert ist. Die Spanning Tree-Ansicht vereinfacht eine Serviceinstanz zuordnung, bei der die meisten Verbindungslinien verborgen sind.	**a.** Klicken Sie auf das CI, dessen Verbindungen Sie anzeigen möchten. In der Zuordnung werden alle verborgenen Verbindungen für dieses CI angezeigt. **b.** Klicken Sie auf die erforderlich Verbindungslinie. 
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Datenverkehrsbasierte Verbindungen für ein CI.	**a.** Klicken Sie mit der rechten Maustaste auf das CI, dessen datenverkehrsbasierte Verbindungen Sie prüfen möchten. **b.** Wählen Sie **Traffic-basierte Verbindungen anzeigen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
Hinweis: Sie können datenverkehrsbasierte Verbindungen für ein CI anzeigen, auch wenn Sie die datenverkehrsbasierte Erkennung für einen Serviceinstanz deaktiviert haben, zu dem das CI gehört.	Die Liste der datenverkehrsbasierten Verbindungen wird geöffnet und zeigt Informationen aus der Tabelle „Liste der Traffic-basierten Verbindungen“ an. **c.** Wenn Sie die Anzeige dieser Liste beenden möchten, klicken Sie auf **Schließen**.
Manuell hinzugefügte Verbindung. Manuell können Sie eine Verbindung oder ein CI hinzufügen. In beiden Fällen ist die Verbindung, die Sie manuell hinzufügen, ein Einstiegspunkt zur nächsten Ebene des Anwendungs-Flow.	Klicken Sie auf die manuell hinzugefügte Verbindung. Im Bereich **Eigenschaften** wird unter **Endpunkttyp** die Option „Manueller Endpunkt“ angezeigt. 

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	○ **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. ○ **Nein** – Wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie Entfernen.

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

Sie können die Änderungen anzeigen, die an einem Anwendungsservice als Ganzes oder an den einzelnen Konfigurationselementen (CIs), aus denen der Service besteht, vorgenommen wurden. Die Change-Historie ist nützlich für Wartungs-, Planungs- oder Fehlerbehebungsverfahren.

Vorbereitungen

Erforderliche Rolle: admin, Service_Mapping_admin, Service_Mapping_user, App_Service_admin oder App_Service_user

Warum und wann dieser Vorgang ausgeführt wird

Details zu Änderungen an einer Serviceinstanz und ihren CIs werden in der CMDB gespeichert. Normalerweise spiegeln diese Änderungen das Hinzufügen oder Entfernen von CIs aus einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien wider. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

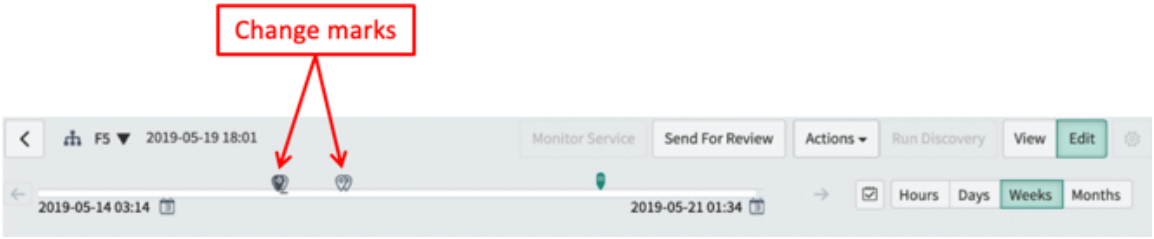
Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Während Sie Change-Datensätze für ein bestimmtes CI im Kontext von Anwendungsservices anzeigen können, können Sie auch den detaillierten Verlauf eines bestimmten CI separat von anzeigen Serviceinstanz Wie in beschrieben Verlaufszeitleiste .

Wenn die ServiceNow AI Platform für die Validierung von Changes konfiguriert ist, werden alle Changes bewertet und als gültig oder nicht angezeigt. Wenn ein Change gültig ist, wird sein Change-Datensatz in der Serviceinstanzzuordnung als genehmigt markiert. Weitere Informationen zum Konfigurieren der Plattform für die Validierung von Changes finden Sie unter Vorgeschlagene Changes verwalten .

Changes an dem Serviceinstanz erscheinen in der Verlaufszeitleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Art der Änderungsmarke hängt von der Art der Changes ab, die sie darstellt:

Hellgrauer Ballon (**)**

Nicht genehmigter Change, der das Verhalten der Serviceinstanz nicht beeinflusst. Zum Beispiel eine Change in einem Netzwerkpfad oder das Hinzufügen eines Knotens zu einem Cluster.

Dunkelgrauer Ballon (**)**

Nicht genehmigter Change, der das Verhalten der Serviceinstanz ändert.

Grüner Ballon (**)**

Eine genehmigte Change in Bereitstellungen, bei denen die ServiceNow AI Platform für die Validierung der Changes konfiguriert ist.

Doppelter Ballon (**)**

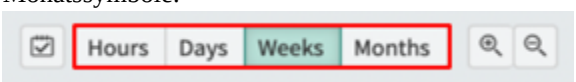
Mehrere getrennte Changes, die kurz hintereinander stattfanden.

Sie können Zeiten auf der Verlaufsskala markieren, indem Sie Baselines erstellen, um schnell zur markierten Ansicht zurückzukehren.

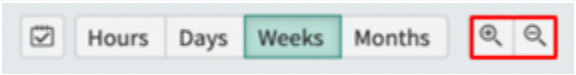
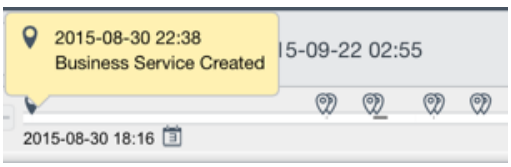
Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Zeigen Sie auf der Registerkarte **Changes** unten auf der Seite die Change-Datensätze an, die für diesen Serviceinstanz erstellt wurden.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Legen Sie auf der Verlaufszeitleiste den Zeitbereich der Änderungen fest, die Sie anzeigen möchten.

Option	Aktion
Zeitbereich der Verlaufszeitleiste festlegen	Klicken Sie auf die Stunden-, Tages-, Wochen- oder Monatssymbole. 
Den Zeitbereich vergrößern oder verkleinern	Klicken Sie auf die Symbole zum Vergrößern und Verkleinern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

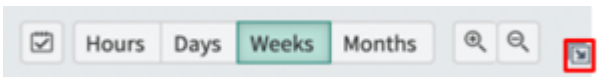
Option	Aktion
	
Um die obere Grenze Ihres Verlaufsbereichs zu ändern,	klicken Sie auf die Verlaufsskala. Die Zeit, die als Obergrenze dient, wird über der Verlaufszeitleiste angezeigt. **Hinweis:** Sie können den unteren Grenzwert für Ihren Verlaufsbereich nicht auf einen Zeitpunkt festlegen, bevor diese Serviceinstanz erstellt wurde. Diese Zeit ist mit dem Event **IT-Service erstellt** auf der Verlaufszeitleiste markiert. 

Die Karte zeigt die Verlaufsansicht der Serviceinstanz für die ausgewählte Zeit.

Hinweis: Die Registerkarte **Änderung** zeigt alle Änderungssätze - auch die, die aus der Verlaufsansicht herausgefiltert werden.

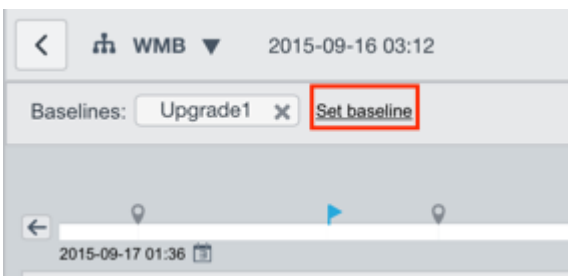
4. Um eine Zeit auf der Zeitskala zu markieren, legen Sie eine Baseline fest:

   a. Klicken Sie auf das Symbol **Vergleichen**.



   b. Navigieren Sie zu der Zeit, zu der Sie eine Baseline auf der Verlaufsskala markieren möchten.

   c. Klicken Sie auf **Baseline festlegen**.

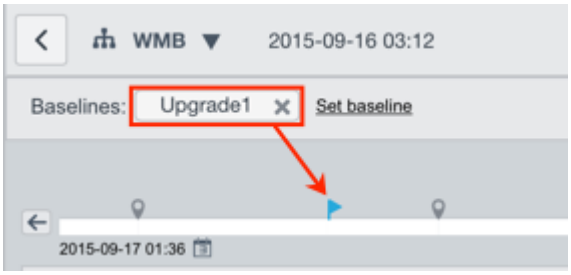


   d. Geben Sie den Namen der Baseline ein, und klicken Sie auf **OK**.

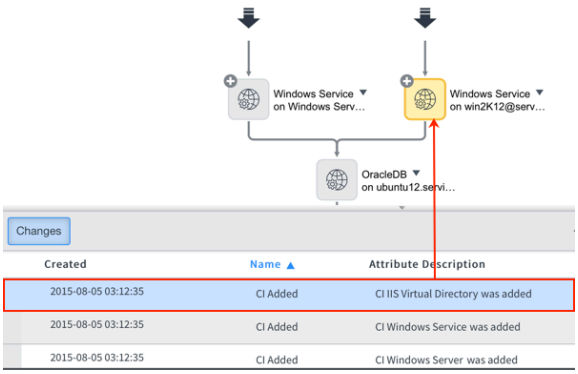
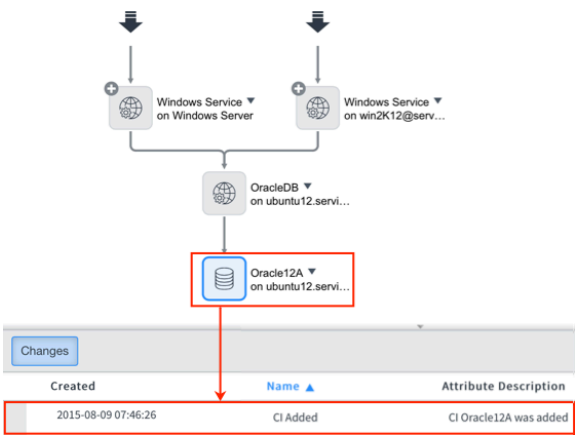
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die neue Baseline wird als Schaltfläche oberhalb der Verlaufsskala und als blaue Flagge auf der Verlaufsskala angezeigt.



5. Zeigen Sie die Change-Historie an.

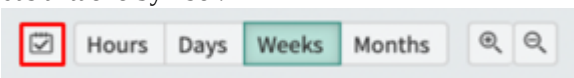
Option	Aktion
Für Änderungsdatensätze verantwortliche CIs anzeigen	Wählen Sie einen Änderungsdatensatz über die Registerkarte **Änderungen**. Das zugehörige CI ist in der Karte gelb markiert. 
Nur Change-Datensätze anzeigen, die sich auf ein CI beziehen	Wählen Sie das erforderliche CI oder die Verbindung auf der Karte. Auf der Registerkarte **Änderungen** werden nur Änderungsdatensätze angezeigt, die sich auf das ausgewählte CI oder die ausgewählte Verbindung beziehen. 

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Konfigurationsdateien zu ausgewählten Zeitpunkten in der Vergangenheit anzeigen	**a.** Stellen Sie die Zeit auf der Verlaufsskala ein. **b.** Scrollen Sie in dem Fenster **Eigenschaften** zu **Verfolgte Konfigurationsdateien**, und klicken Sie auf den Dateinamen. Die neue Registerkarte wird mit dem Inhalt der verfolgten Konfigurationsdatei zu dem ausgewählten Zeitpunkt angezeigt.
Das Netzwerk zum ausgewählten Zeitpunkt in der Vergangenheit anzeigen	**a.** Stellen Sie die Zeit auf der Verlaufsskala ein. **b.** Klicken Sie mit der rechten Maustaste auf die Verbindung, und wählen Sie **Netzwerkpfad anzeigen**. Die neue Registerkarte wird mit der Netzwerk- oder Speicherpfadkarte für den von Ihnen ausgewählten Zeitpunkt angezeigt. **Hinweis:** Sie können den Netzwerkpfad für Verbindungen, die als Grenzen für dieses Serviceinstanz markiert sind, nicht anzeigen.

6. Um die Verlaufsansicht zu verlassen und den aktuellen Status des Serviceinstanz anzuzeigen, klicken Sie auf das aktuelle Symbol.



Zugehörige Informationen

Anwendungsservicezuordnung im Basissystem anzeigen

Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen

Nachverfolgung von Changes in Konfigurationsdateien ändern

Nachverfolgung von Changes für die Change-Historie feintunen

Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen

Sie können eine Zusammenfassung der Änderungen des Anwendungsservice auf einen Blick anzeigen, indem Sie zwei Versionen eines Anwendungsservice vergleichen. Diese Funktion ist hilfreich zur Überprüfung des Status des Anwendungsservice vor und nach einer bestimmten Änderung oder einem bestimmten Problem.

Vorbereitungen

Erforderliche Rolle: admin, App_Service_admin, App_Service_user, Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Geben Sie zwei Zeitpunkte an, für die Sie die beiden Versionen eines Anwendungsservice vergleichen möchten. Sie können die Änderungsindikatoren in der Zeitleiste verwenden, um einen Zeitpunkt vor und einen anderen nach einer Änderung anzugeben, für die Details

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

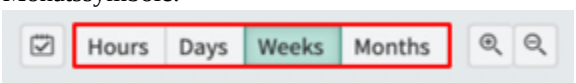
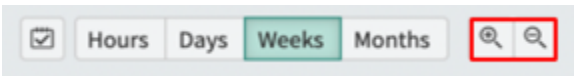
angezeigt werden sollen. Zum Beispiel können Sie, wenn Sie wissen, dass das Fehlschlagen eines Anwendungsservice zu einem bestimmten Zeitpunkt begonnen hat, zwei Versionen des Anwendungsservice (eine vor und eine nach Einsetzen des Problems) vergleichen. Dieser Vergleich zeigt Ihnen die Zusammenfassung der Changes, die möglicherweise zu den Problemen geführt haben.

Wenn Service-Mapping bereitgestellt ist, werden alle Änderungen an einem CI, einschließlich der dem CI zugeordneten Konfigurationsdateien, nachverfolgt und angezeigt. Wenn Sie zwei Versionen eines Anwendungsservice vergleichen, können Sie Änderungen an Konfigurationsdateien als Änderungen an CIs sehen. Sie können auch zwei Versionen einer Konfigurationsdatei vergleichen, um die tatsächlichen Changes in den Dateien innerhalb des für den Vergleich angegebenen Zeitraums anzuzeigen.

Prozedur

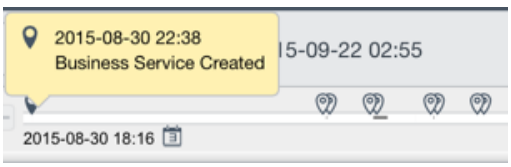
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Legen Sie auf der Verlaufszeitleiste den Zeitbereich der Änderungen fest, die Sie anzeigen möchten.

Option	Aktion
Zeitbereich der Verlaufszeitleiste festlegen	Klicken Sie auf die Stunden-, Tages-, Wochen- oder Monatssymbole. 
Den Zeitbereich vergrößern oder verkleinern	Klicken Sie auf die Symbole zum Vergrößern und Verkleinern. 
Um die obere Grenze Ihres Verlaufsbereichs zu ändern,	klicken Sie auf die Verlaufsskala. Die Zeit, die als Obergrenze dient, wird über der Verlaufszeitleiste angezeigt.

Automatische Übersetzung

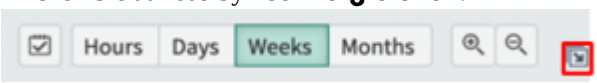
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Hinweis: Sie können den unteren Grenzwert für Ihren Verlaufsbereich nicht auf einen Zeitpunkt festlegen, bevor diese Ser–viceinstanz erstellt wurde. Diese Zeit ist mit dem Event **IT-Service erstellt** auf der Verlaufszeitleiste markiert. 

Die Karte zeigt die Verlaufsansicht der Serviceinstanz für die ausgewählte Zeit.

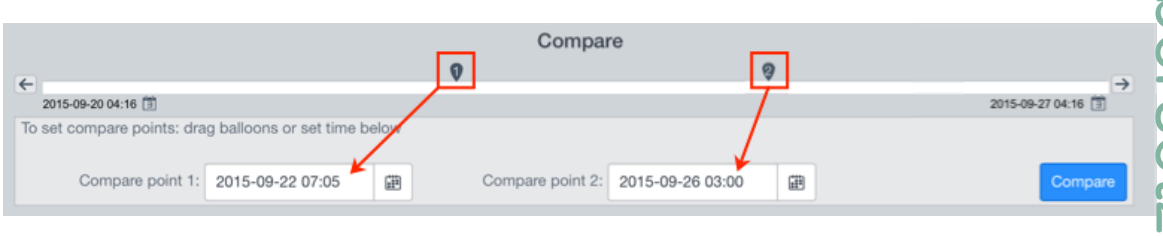
Hinweis: Die Registerkarte **Änderung** zeigt alle Änderungssätze - auch die, die aus der Verlaufsansicht herausgefiltert werden.

4. Klicken Sie auf das Symbol **Vergleichen**.

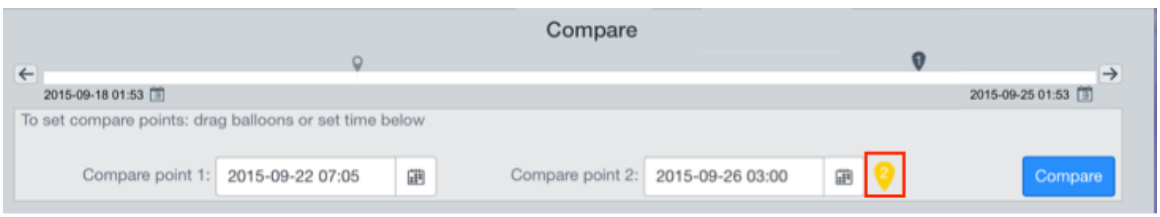


5. Stellen Sie **Vergleichspunkt 1** und **Vergleichspunkt 2** als die beiden Zeitpunkte für den Vergleich ein.

Sie können die Zeiger auf der Verlaufsskala ziehen, um entsprechende Zeitpunkte festzulegen.



Configuration Management DatabaseWenn die Verlaufsskala den für den Vergleich festgelegten Zeitpunkt nicht enthält, wird der entsprechende Zeiger neben dem Vergleichspunkt in gelb angezeigt:



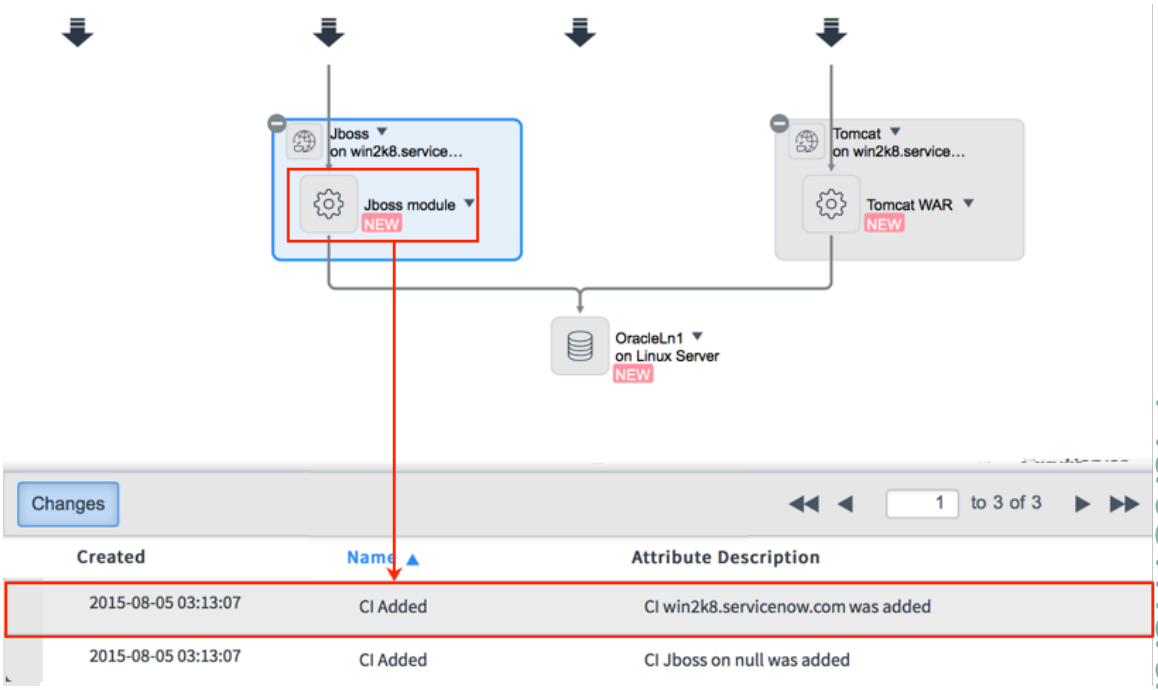
Hinweis: Wenn während des von **Vergleichspunkt 1** und **Vergleichspunkt 2** angegebenen Zeitintervalls keine Änderungen an dem Service vorgenommen werden, werden keine Änderungsdetails angezeigt.

6. Klicken Sie auf **Vergleichen**.
Die Vergleichsansicht wird in einer separaten Registerkarte geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie ein markiertes CI aus, um den entsprechenden Änderungsdatensatz über die Registerkarte **Änderungen** anzuzeigen.



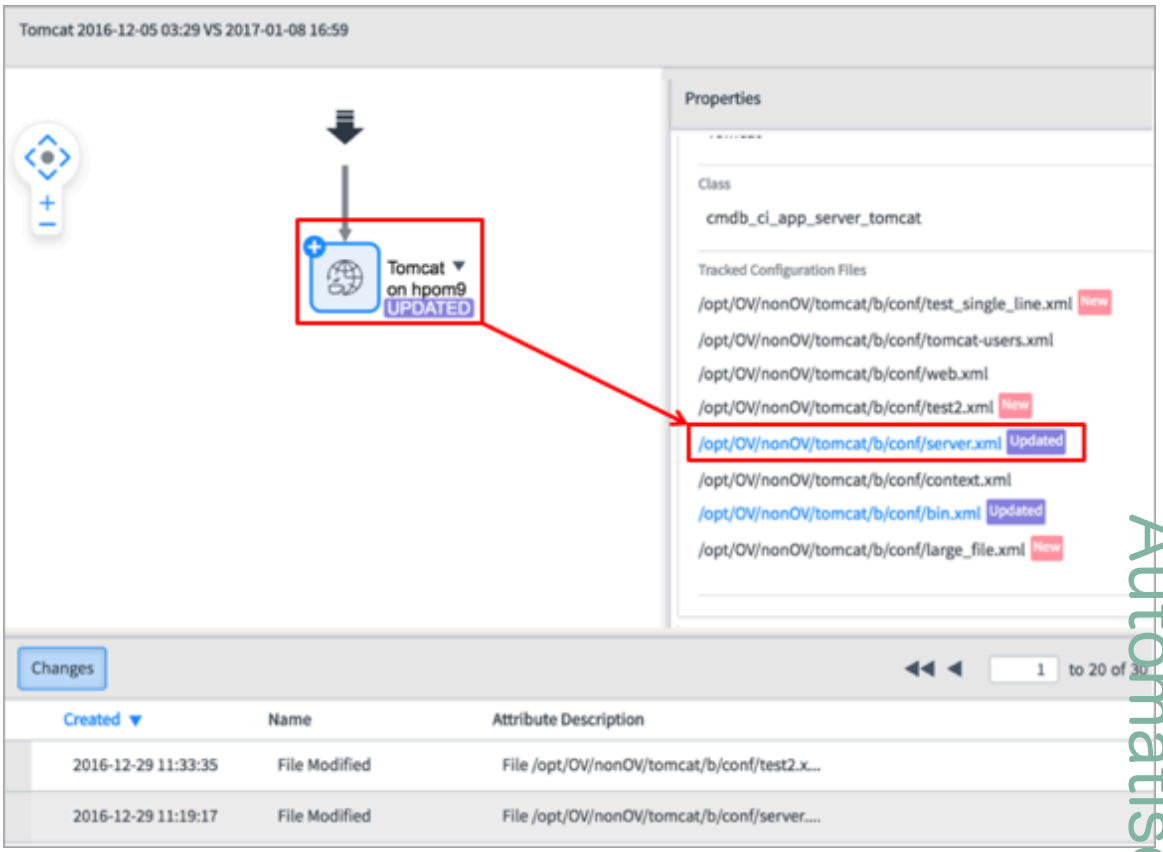
8. **Wahlweise:** Wenn Service-Mapping bereitgestellt wird, können Sie zwei Versionen einer Konfigurationsdatei vergleichen, die auf der Karte als „Aktualisiert“ angezeigt wird:

   a. Wählen Sie das CI aus, das der aktualisierten Konfigurationsdatei zugeordnet ist.

   b. Klicken Sie im Bereich **Eigenschaften** auf den Link zur aktualisierten Datei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Registerkarte **Versionen von verfolgten Konfigurationsdateien vergleichen** wird geöffnet und zeigt zwei Versionen der Konfigurationsdatei nebeneinander an.

c. Überprüfen Sie die tatsächlichen Änderungen.

(Optional) Hervorhebungsfarben geben die Art der Änderung an:

- Lila - Aktualisierte Linie
- Pink - Neue Linie
- Grau - Zeile gelöscht

d. Navigieren Sie mit den Pfeilen in der oberen rechten Ecke zwischen den Änderungen.

e. Schließen Sie die Registerkarte **Versionen von verfolgten Konfigurationsdateien vergleichen**, wenn Sie fertig sind.

9. Schließen Sie die Vergleichsansicht, wenn Sie fertig sind.

Zugehörige Informationen

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

Versionen von CI-Konfigurationsdateien vergleichen

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Überprüfen Sie, welche Anwendungsservices von einem Anwendungsservice abhängig sind, und öffnen Sie Zuordnungen für abhängige Anwendungsservices.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rollen: Service_Mapping_user

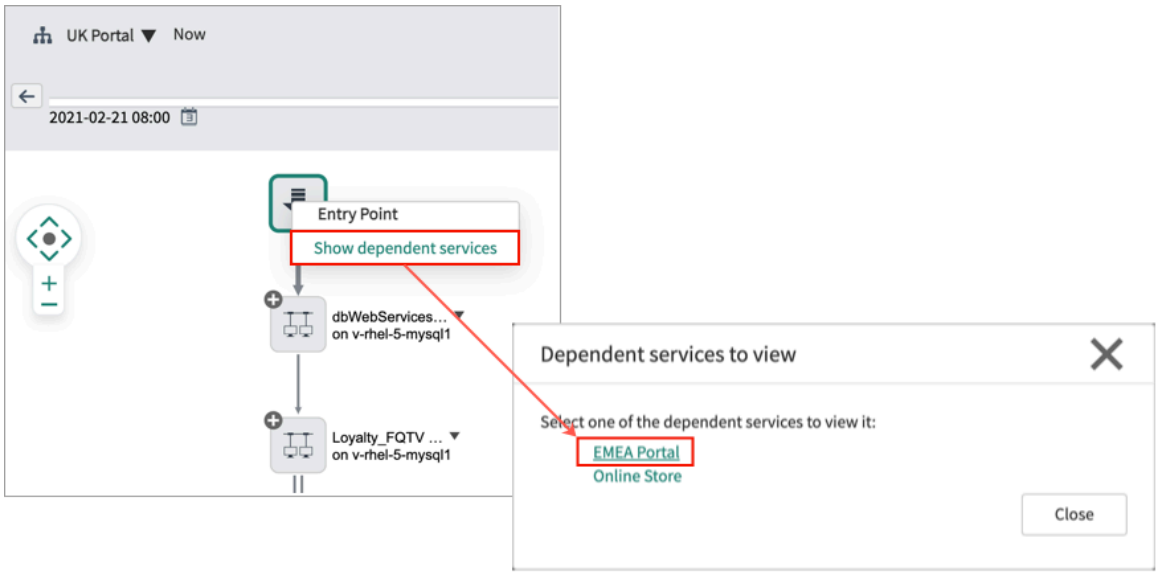
Warum und wann dieser Vorgang ausgeführt wird
Der Service, der einen Verweis auf eine andere Serviceinstanz enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service.

Abhängige Servicezuordnung mit Verweis auf enthaltenen Anwendungsservice

Prozedur
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie mit der rechten Maustaste auf den Einstiegspunkt, und wählen Sie **Abhängige Services anzeigen** aus.
   Im Popup-Fenster werden die Links zu allen abhängigen Services für diesen Anwendungsservice angezeigt.
3. Klicken Sie auf den Link für den abhängigen Service, dessen Zuordnung Sie anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Zuordnungsfenster wird die Zuordnung für den ausgewählten abhängigen Service angezeigt.

Zugehörige Informationen

Anwendungsservices verknüpfen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Ein enthaltener Anwendungsservice ist eine Referenz, die in einem anderen, abhängigen Anwendungsservice enthalten ist. Sie können die Zuordnung des enthaltenen Service direkt aus der Zuordnung des abhängigen Service öffnen.

Vorbereitungen

Erforderliche Rollen: Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Der Service, der einen Verweis auf eine andere Serviceinstanz enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängige Servicezuordnung mit Verweis auf enthaltenen Anwendungsservice

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie mit der rechten Maustaste auf das CI, das den enthaltenen Service darstellt, und wählen Sie **Enthaltenen Service anzeigen** aus.
   Die Zuordnung zeigt eine automatische Weiterleitung an die Webadresse für den enthaltenen Service. Es müssen keine zusätzlichen Registerkarten geöffnet werden.

CI-Abhängigkeiten überprüfen

Sie können prüfen, ob ein bestimmtes Konfigurationselement (CI) Teil eines anderes Anwendungsservice ist und ob es von anderen CIs abhängig ist.

Vorbereitungen

Erforderliche Rolle: admin, app_service_admin, app_service_user

Automatische Übersetzung

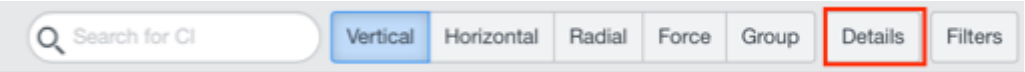
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping zeigt die Position eines CI in einem bestimmten Anwendungsservice. Ihre Organisation kann dasselbe CI jedoch auch in anderen Anwendungsservices verwenden. Wenn Sie Änderungen an diesem CI vornehmen möchten, müssen Sie sicherstellen, dass die Änderungen keine Auswirkungen auf andere Anwendungsservices haben.

Prozedur

1. Klicken Sie in der Zuordnung mit der rechten Maustaste auf das relevante CI, und wählen Sie **Ansicht der Abhängigkeiten öffnen** aus.
   Die Seite „Abhängigkeitsansichten“ wird in einer neuen Registerkarte geöffnet und zeigt das ausgewählte CI in der Mitte.
2. Klicken Sie auf **Details**.



3. Klicken Sie auf die Registerkarte **Zugehörige Services**.
   Die Liste der Links zu allen Anwendungsservices, die dieses CI enthalten, wird auf der Registerkarte **Zugehörige Services** angezeigt.
4. Klicken Sie auf den entsprechenden Link, um die Zuordnung eines anderen Anwendungsservice anzuzeigen, der dieses CI enthält.

Zugehörige Informationen

Anwendungsservicezuordnungen in klassisch Service-Mapping

Abhängigkeitsansichten

Netzwerk- oder Speicherpfad in klassisch Service-Mapping anzeigen

Um Probleme mit der Serviceleistung zu beheben oder um Ihr Netzwerk zu warten, können Sie einen Drilldown ausführen, um die Objekte hinter einer Verbindung in einer Zuordnung anzuzeigen. Für manuell erstellte Services oder Services in Instanzen mit Edge Encryption ist diese Funktion nicht verfügbar.

Vorbereitungen

Erforderliche Rolle: admin, Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Durch die Anzeige eines Netzwerk- oder Speicherpfads können Sie Router, Switches und Hostports anzeigen, die Teil der Verbindung sind. Die folgenden Verbindungstypen sind vorhanden:

Netzwerkpfad

Die Infrastrukturroute zwischen zwei CIs vom Typ Host.

Speicherpfad

Die Infrastrukturroute zwischen einem CI vom Typ Host und einem CI vom Typ Speicher.

Service-Mapping erkennt keine Netzwerkgeräte im WAN oder in der öffentlichen Cloud, sondern nur solche, die sich im lokalen Netzwerk Ihrer Organisation befinden, und zeigt sie an. Wenn Service-Mapping auf eine Verbindung zwischen zwei Anwendungen stößt, wird mithilfe von traceroute der Pfad vom Quellhost zum Zielhost ermittelt. Dann verwendet Service-Mapping die SNMP-Anmeldeinformationen, um die im Pfad gefundenen Geräte zu erkennen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping kann Geräte für Speicherpfade mit den folgenden Protokollen anzeigen:

- Fiber Channel: Storage Area Network (SAN)
- IP-Ethernet: Internet Small Computer Systems Interface (iSCSI) oder Network Attached Storage (NAS)

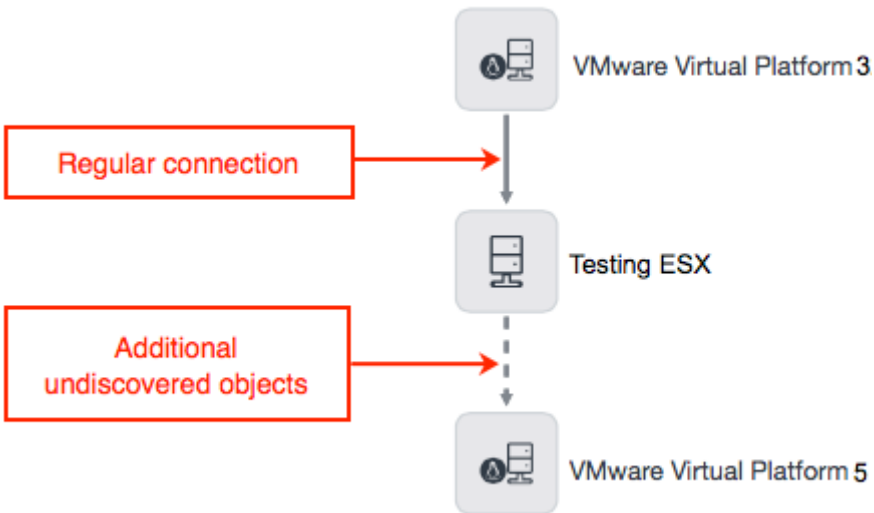
> **Hinweis:** Für Speicherpfade, die Fibre Channel verwenden, zeigt Service-Mapping keine Fibre Channel Switches an.

Zwischen einem Host-CI und einem Speicher-CI können zwei separate Speicherpfade mit unterschiedlichen Protokollen vorhanden sein: Fibre Channel und IP-Ethernet. Wenn das der Fall ist, zeigt die Zuordnung des Serviceinstanz eine Verbindungslinie für beide Protokolle an.

Sie können die Change-Historie für Netzwerk- und Speicherpfade für Anwendungsservices anzeigen. Eine Überprüfung der Pfadhistorie für manuelle oder technische Services wird nicht unterstützt.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie in der Zuordnung mit der rechten Maustaste auf die Verbindung für den Netzwerk- oder Speicherpfad, den Sie sehen möchten.
3. Wählen Sie **Netzwerkpfad anzeigen** oder **Speicherpfad anzeigen** aus.
4. Wählen Sie bei Bedarf den Protokolltyp aus, und klicken Sie im Dialogfeld „Protokolltyp auswählen“ auf **Auswählen**.
   Die Ansicht mit dem Netzwerk- oder Speicherpfad wird auf einer neuen Registerkarte geöffnet.



Wenn Service-Mapping nicht alle Objekte in einer Verbindung erkennen kann, wird die Connector-Linie im Netzwerk- oder Speicherpfad wie oben dargestellt gepunktet angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Verwenden Sie für Speicherpfade die Registerkarte „Speicherzuordnung“ am unteren Bildschirmrand, um die Korrelation zwischen Dateisystemen auf dem Host und dem Speichervolume oder dem freigegebenen Ordner auf dem Speichergerät anzuzeigen.
6. Führen Sie die Schritte unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen aus , um die Change-Historie für Netzwerkpfade anzuzeigen.
7. Wenn Sie von Ereignismanagement aus auf die Netzwerk- oder Speicherpfadzuordnung zugreifen, wird die Liste der zu diesem Pfad gehörenden Warnungen unten im Bildschirm angezeigt.

Zugehörige Informationen

Anwendungsservicezuordnungen in klassisch Service-Mapping

SNMP-basierte Abfragen

Liste der einem Anwendungsservice zugehörigen CIs anzeigen

Zeigen Sie eine vollständige Liste von CIs an, aus denen ein Anwendungsservice besteht, einschließlich der CIs, die nicht in der Anwendungsservicezuordnung angezeigt werden: nachverfolgte Konfigurationsdateien, Endpunkte, Prozesse und Netzwerkgeräte.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

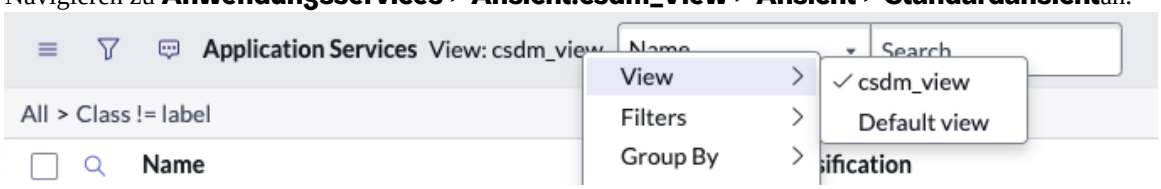
Standardmäßig werden in Anwendungsservicezuordnungen Anwendungs-CIs und Verbindungen zwischen diesen angezeigt. Die übrigen CIs hinter Anwendungen und die Verbindungen zwischen ihnen sind ausgeblendet. In der CI-Liste werden die folgenden zusätzlichen CIs angezeigt:

- Server, die Anwendungen hosten
- Netzwerkgeräte wie Router oder Switches
- Prozesse, die auf Hosting-Servern ausgeführt werden. Prozesse werden zur Identifizierung und Klassifizierung von Anwendungen verwendet.
- Nachverfolgte Konfigurationsdateien für Anwendungen, die Teil des Service sind
- Endpunkte, die zu den Anwendungen gehören. Endpunkte enthalten Informationen, die für die Verbindung mit Anwendungen erforderlich sind, zum Beispiel Hosts und Ports.
- Das Anwendungsservice-CI für diesen Anwendungsservice

Die CI-Listen für leere Anwendungsservices, die keine CIs enthalten, enthalten nur ein einziges CI: für den Anwendungsservice selbst.

Prozedur

1. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
2. Navigieren zu **Anwendungsservices** > **Ansicht:csdm_View** > **Ansicht** > **Standardansicht**an.

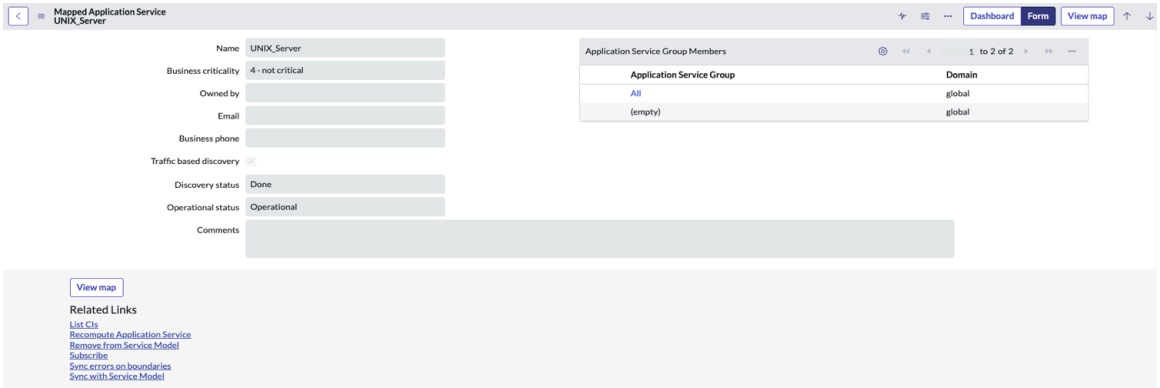


3. Klicken Sie auf den Namen des Anwendungsservice, für den Sie die Liste der CIs anzeigen möchten. Der Erkennungsstatus des ausgewählten Service muss **Fertig** lauten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Listen Sie CIs auf** Unter zugehörige Links.



5. Zeigen Sie die vollständige Liste der CIs an, die Teil des ausgewählten Anwendungsservice sind.
6. Klicken Sie in Ihrem Browser auf die Schaltfläche „zurück“, um zur Seite „zugeordneter Anwendungsservice“ zurückzukehren, wenn Sie die Überprüfung der Liste der CIs abgeschlossen haben.
7. Wählen Sie Aus **Zeigen Sie die Karte an** Um zur Anwendungsservice-Zuordnung zu navigieren.

Anwendungsservicezuordnungen in PDFs konvertieren

Sie können eine PDF-Datei für eine Zuordnung erstellen, um Informationen über den Serviceinhalt mit anderen Personen zu teilen. PDF-Dateien sind besonders nützlich während des Überprüfungs- und Genehmigungsprozesses für von Service-Mapping erkannte Anwendungsservices.

Vorbereitungen

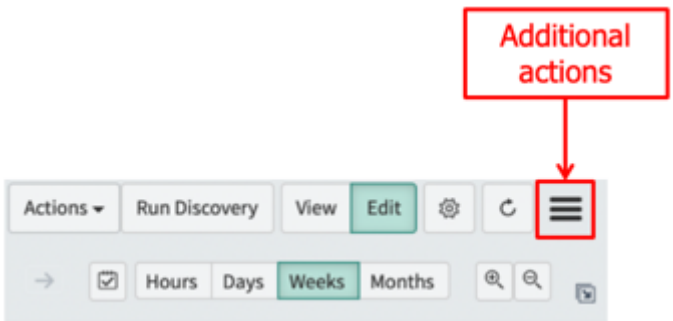
Erforderliche Rolle: app_service_admin, app_service_user

Warum und wann dieser Vorgang ausgeführt wird

Die PDF-Datei der Anwendungsservicezuordnung zeigt den Namen des Anwendungsservice und den genauen Zeitpunkt der Erstellung der PDF-Datei.

Prozedur

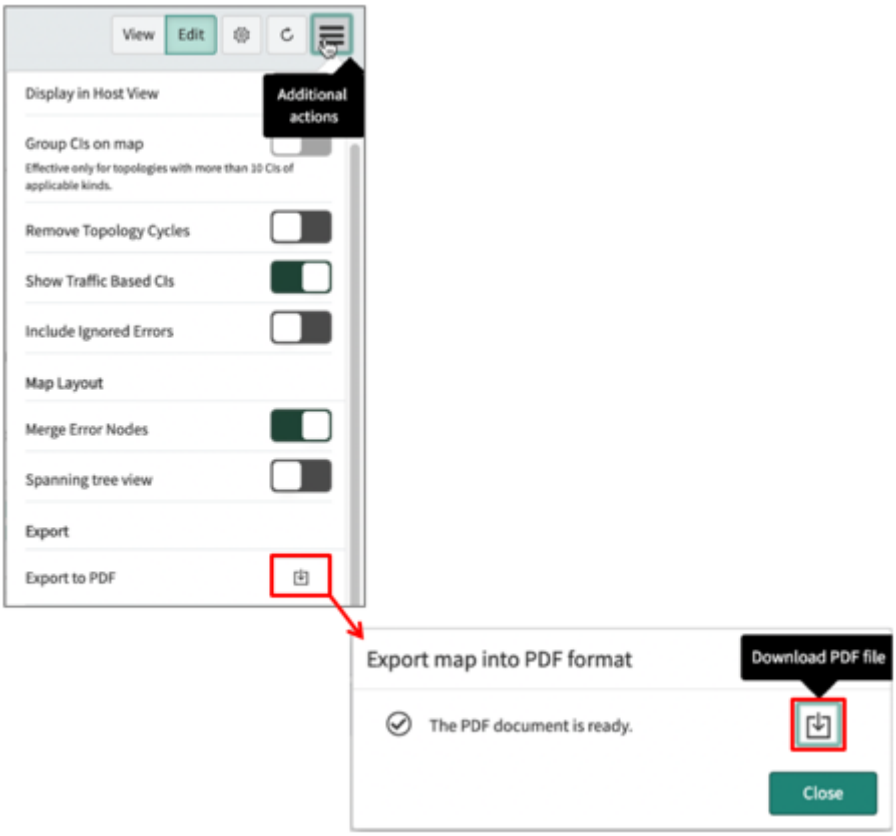
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie auf das Menü **Zusätzliche Aktionen**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die Schaltfläche neben der Option **PDF-Export**.



4. Wenn die PDF-Datei fertig ist, klicken Sie im Dialogfeld „Zuordnung im PDF-Format exportieren“ auf die Schaltfläche **PDF herunterladen**.
   Das PDF-Dokument wird in den Ordner „Downloads“ auf Ihrem Computer geladen.

Ansicht für Anwendungsservicezuordnung ändern

Passen Sie eine Zuordnungsansicht an, um relevante Informationen anzuzeigen und die Übersichtlichkeit zu erhöhen.

Vorbereitungen

Erforderliche Rolle: App_Service_admin, App_Service_user, Service_Mapping_admin oder Service_Mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig sind Servicezuordnungen präzise und enthalten alle Details zu allen CIs, die Sie manuell hinzugefügt haben oder die von Service-Mapping zugeordnet wurden. Obwohl sie ein umfassendes Bild vermittelt, könnte die Verwendung einer solchen Zuordnung schwierig sein. Durch das Anpassen der Zuordnungen können Sie:

- die Navigation in der Zuordnung erleichtern
- irrelevante Informationen ausblenden
- wichtige Informationen anzeigen

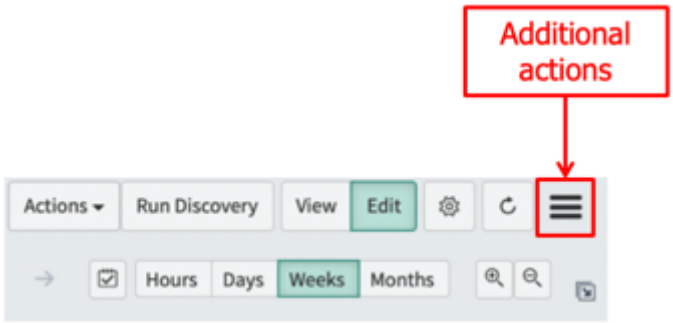
Attribute, die Sie beim Anpassen von Zuordnungen anzeigen oder ausblenden, werden nicht dauerhaft entfernt und können nach Bedarf wieder angezeigt oder ausgeblendet werden. Das System speichert die Änderungen in der Kartenansicht und zeigt die letzte Kartenansicht an, wenn Sie eine Serviceinstanz erneut öffnen.

Automatische Übersetzung

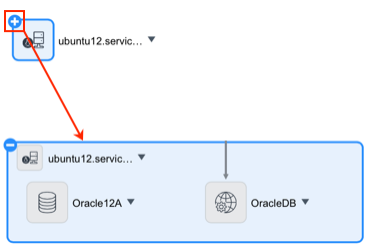
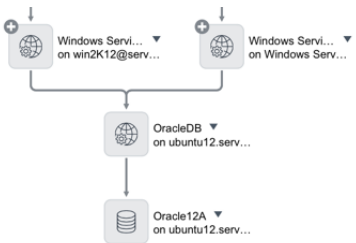
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

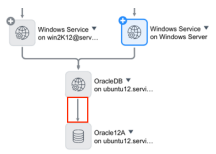
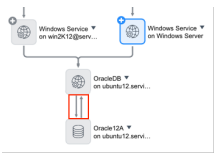
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**an.
   b. Wählen Sie die erforderliche Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz die Option aus **Karte Anzeigen** .
2. Klicken Sie auf das Menü **Zusätzliche Aktionen**.



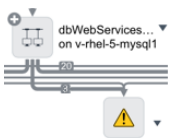
3. Wählen Sie die relevante Option aus:

Option	Wenn aktiviert	Wenn deaktiviert
In Host-Ansicht anzeigen Diese Option ist nur verfügbar, wenn das Service-Mapping-Plugin aktiviert ist. Wechseln Sie zwischen der CI-Ansicht, in der Hosts ausgeblendet werden, und der Host-Ansicht, in der CIs ausgeblendet werden. Die Host-Ansicht kann dabei helfen zu bestimmen, dass von Service-Mapping alle Hosts richtig erkannt und zugeordnet wurden, und hilft, Verbindungen zu jedem Host zu finden. Die Host-Ansicht vereinfacht auch die Zuordnung, insbesondere wenn viele Anwendungen auf wenigen Hosts ausgeführt werden. Die Host-Ansicht ist nur für Serviceinstanzen nützlich, die mit erkannt wurden Service-Mapping. Diese Ansicht enthält keine zusätzlichen Informationen	Von der Servicezuordnung werden Host-CIs dargestellt. Klicken Sie auf die Plus-Symbole, um Anwendungs-CIs anzuzeigen, die auf den Hosts ausgeführt werden.  Im Bereich **Eigenschaften** werden nur Informationen zu Servern angezeigt, die als Hosts fungieren.	In der Servicezuordnung werden Anwendungs-CIs dargestellt.  Im Bereich **Eigenschaften** werden nur Informationen zu Servern angezeigt, die als Hosts fungieren, sowie zu Anwendungen, die auf diesen Hosts ausgeführt werden.

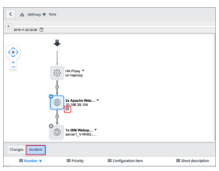
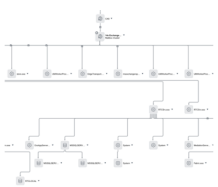
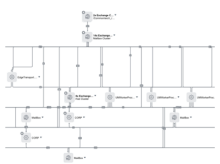
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
für manuell erstellte Serviceinstanzen.		
CIs in Zuordnung gruppieren Vereinfachen Sie Zuordnungen, indem Sie CIs gruppieren, die zu demselben Typ gehören und auf Servern gehostet werden, die sich Präfix und Domänennamen teilen. Die Zuordnung gibt den Anwendungs-Flow weiterhin korrekt wieder, da gruppierte CIs zur selben Ebene gehören. Diese Option ist für Serviceinstanzen relevant, die aus mehr als 10 CIs bestehen.	Die Serviceinstanzzuordnung zeigt Gruppen von CIs an. Die Zuordnung ist kompakter.	In der Serviceinstanzzuordnung werden alle CIs separat angezeigt. Die Zuordnung ist größer.
Topology Cycles entfernen Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Blenden Sie Verbindungen aus, die zu demselben Configuration Item (CI) zurückkehren, von dem sie stammen, um die Übersichtlichkeit der Zuordnung zu verbessern. Normalerweise sind diese zurückgegebenen Verbindungen für die Analyse oder Fehlerbehebung von Serviceinstanzen nicht wichtig.	In der Serviceinstanzzuordnung werden Topologiezyklen ausgeblendet. 	Die Serviceinstanzzuordnung zeigt Topologiezyklen an. 
Datenverkehrsbasierte CIs anzeigen	Die Serviceinstanzzuordnung zeigt CIs und Hosts an, die	Die Serviceinstanzzuordnung zeigt nur CIs und Hosts,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie mithilfe von datenverkehrsbasierter Zuordnung gefundene Configuration Items (CIs) an.	Service-Mapping Sowohl mit Mustern als auch mit der Traffic-basierten Discovery erkannt. Die Erkennung von eingehendem und ausgehendem CIs erstellt zwar eine inklusive Zuordnung, kann aber auch dazu führen, dass viele redundante CIs zugeordnet werden, die den Serviceinstanzvorgang nicht beeinflussen.	die mithilfe von Mustern erkannt wurden.
Fehlerknoten zusammenführen Diese Option ist nur für Anwender mit der Rolle eines Service-Mapping-Administrators [service_mapping_admin] verfügbar. Führen Sie CIs mit Fehlern zusammen, die durch dasselbe Quell-CI verursacht werden, um die Zuordnung eines Serviceinstanz übersichtlicher zu gestalten. Ein Erkennungs- oder Betriebsfehler in einem CI wirkt sich häufig auf alle darunter liegenden Verbindungen in der Hierarchie aus, wodurch Ihre Ansicht überfrachtet wird. Sie können durch dasselbe CI verursachte, identische Fehler entfernen, indem Sie sie in der Zuordnung zu einem einzelnen Objekt zusammenführen. Wenn beispielsweise ein CI einen Fehler in sechs damit verbundenen CIs verursacht, können Sie in der Zuordnung nur ein einziges CI mit diesem Fehler anzeigen. Die	Alle CIs mit identischen Fehlern sind in der Zuordnung des Serviceinstanz in einem einzelnen CI zusammengeführt. Die Zahl in der Connector-Zeile gibt die Anzahl der CIs mit diesem Fehler an. 	In der Zuordnung des Serviceinstanz werden alle CIs mit identischen Fehlern separat angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
Connector-Zeile gibt die Anzahl der tatsächlichen Verbindungen wieder.		
Zuordnungsindikatoren Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Serviceanwender [app_service_user] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie zusätzliche Informationen für ein CI oder eine Serviceinstanz selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen. Das Basissystem bietet Kartenindikatoren für die folgenden Datensatztypen: ○ Betroffene CIs ○ Offene Warnungen ○ Aktuelle, geplante oder kürzlich erfolgte Change-Anforderungen ○ Offene Incidents ○ Aktuelle, geplante oder kürzlich erfolgte Ausfälle ○ Offene Probleme Weitere Informationen finden Sie unter Ereignismanagement-Kartenindikatoren (Video) .	Für jeden Datensatztyp, der für die Anzeige festgelegt ist, werden der entsprechende Indikator und die Registerkarte angezeigt. Beispielsweise wird die Registerkarte **Incidents** unter der Zuordnung angezeigt. Der Indikator **Incidents** wird neben CIs angezeigt, denen Incidents zugeordnet sind. 	Die Serviceinstanzzuordnung zeigt CIs ohne zugehörige Indikatoren.
	Wenn ein Datensatz dem Serviceinstanz selbst zugeordnet ist, wird der Indikator neben dem Namen des Serviceinstanz angezeigt. 	Neben dem Namen des Serviceinstanz sind keine Zuordnungsindikatoren zu sehen.
Strukturansicht wird segmentiert Vereinfachen Sie die Zuordnung, indem Sie CIs in einer Baumstruktur anordnen und manche der Verbindungslinien verbergen. Diese Option ist besonders für sehr große Karten nützlich.	In der Zuordnung wird eine Serviceinstanz als Struktur angezeigt.  Um tatsächliche Verbindungen anzuzeigen, zeigen Sie auf ein CI.	Die Zuordnung spiegelt die tatsächliche Struktur einer Serviceinstanz wider. 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
	Weitere Informationen zum Anzeigen von Verbindungen finden Sie unter Zeigen Sie CI-Verbindungsattribute in einer Anwendungsservicezuordnung an klassisch Service-Mapping.	
Ignorierte Fehler einschließen Diese Option ist nur für Anwender mit der Rolle eines Service-Mapping-Administrators [service_mapping_admin] verfügbar. Sie können Fehler anzeigen, die zuvor in der Zuordnung ausgeblendet wurden.	In der Zuordnung werden alle (aktiven und ignorierten) Fehler angezeigt.	Ignorierte Fehler werden in der Zuordnung nicht angezeigt.

Analyse und Wartung von Anwendungsservices mithilfe von veraltet Mitarbeiterbereich

Service-Mapping erstellt Zuordnungen, mit deren Hilfe Sie die Architektur und Organisation von Anwendungsservices anzeigen können. Diese Zuordnungen sind nützlich bei der Planung von Änderungen oder Migrationen sowie zur Analyse der Kontinuität und Verfügbarkeit von Services.

Anwendungsservicezuordnungen in veraltet Mitarbeiterbereich

Zuordnungen bieten Ihnen eine Visualisierung von Daten zu Konfigurationselementen (CIs), die Anwendungsservices umfassen, sowie Beziehungen und Verbindungen zwischen diesen CIs.

Eine neue Zuordnung wird jedes Mal erstellt, wenn Sie einen Serviceinstanz manuell erstellen oder einen Serviceinstanz mithilfe von Service-Mapping zuordnen. Das System aktualisiert die Zuordnung jedes Mal, wenn Sie CIs zu Serviceinstanz hinzufügen oder wenn Service-Mapping eine Erkennung für CIs ausführt, die zu Serviceinstanz gehören.

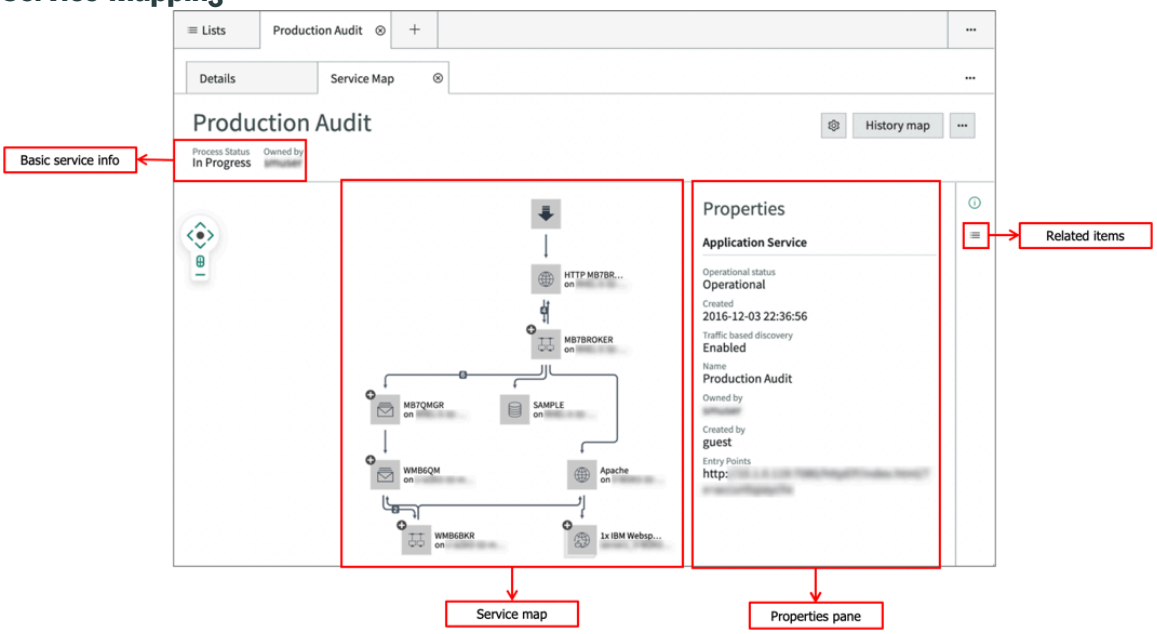
Zuordnungsfenster

Neben der Zuordnung selbst können in der Servicezuordnung auch grundlegende Serviceinformationen wie Schweregrad, Status und Anwendungsbesitzer des Service angezeigt werden. Auch im Eigenschaftenbereich für den Service können Sie zusätzliche Serviceinformationen anzeigen. Klicken Sie auf das Symbol „Zugehörige Elemente“, um alle Warnungen oder Änderungen anzuzeigen, die mit CIs in diesem Anwendungsservice verknüpft sind oder den Anwendungsservice selbst betreffen.

Die Serviceinstanzzuordnung in Ereignismanagement Die Ansicht spiegelt den Schweregradstatus von CIs wider, die zur Serviceinstanz gehören.

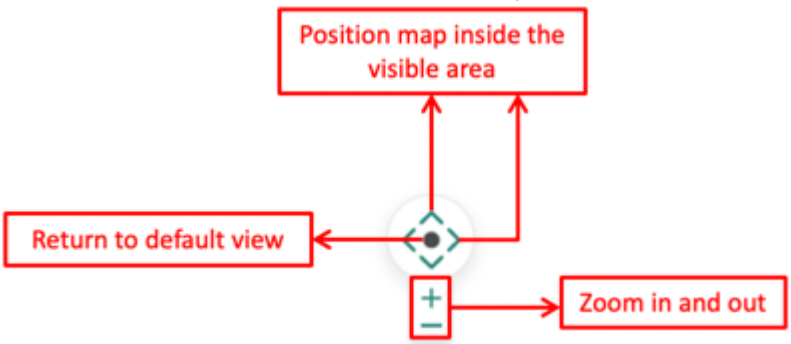
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping



Standardmäßig wird die gesamte Zuordnung in der Mitte des sichtbaren Fensterbereichs der Zuordnung angezeigt. Positionieren Sie die Zuordnung und vergrößern oder verkleinern Sie sie mit den folgenden Steuerungen.

Zoomen und Positionieren der Zuordnung steuern



Sie können auch auf eine beliebige Stelle im Zuordnungsbereich klicken und das gewünschte Segment der Zuordnung in den sichtbaren Bereich ziehen.

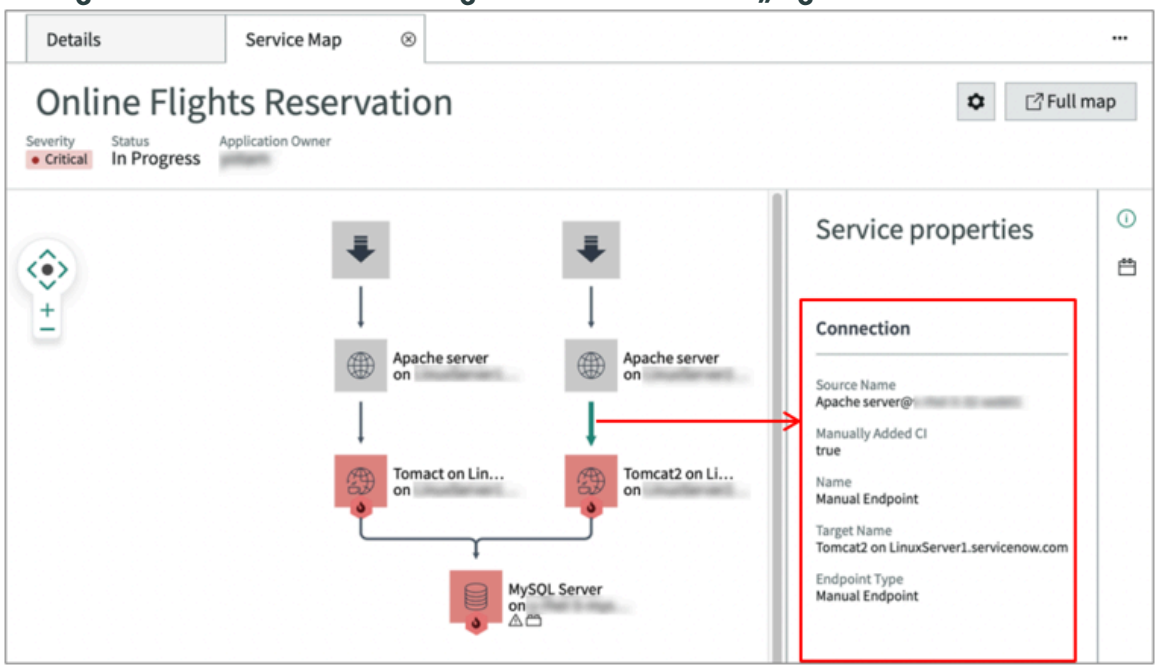
CI-Attribute und CI-bezogene Nachrichten

Wenn eine Zuordnung geladen ist und keine Elemente ausgewählt sind, werden im Bereich „Serviceeigenschaften“ die Details dieses Serviceinstanz angezeigt.

Ausgewählte Geräte, Anwendungen oder Connectors werden grün angezeigt und sind hervorgehoben. Informationen zum ausgewählten Zuordnungselement werden im Eigenschaftenbereich rechts von der Zuordnung angezeigt.

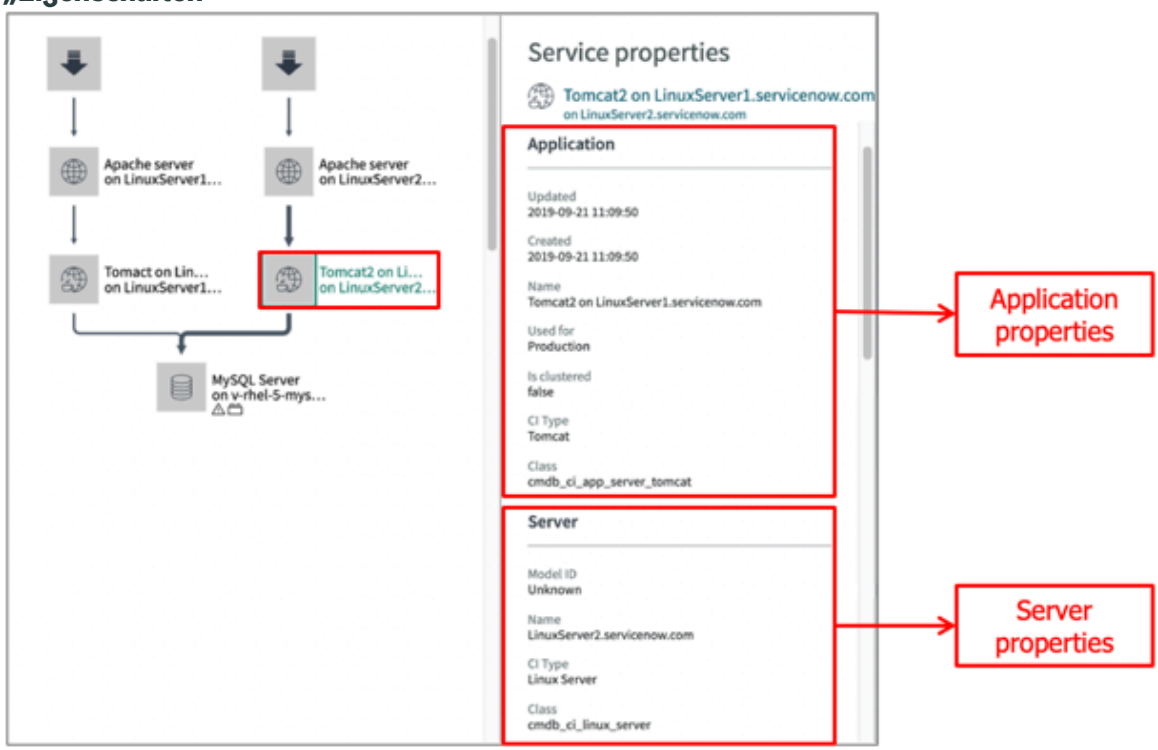
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeige der Attribute für Verbindungen und CIs im Bereich „Eigenschaften“



Die Attribute für den Server, auf dem die Anwendungen gehostet werden, und die Anwendungen selbst werden im Bereich „Eigenschaften“ getrennt angezeigt.

Separate Anzeige der Attribute für Hosts und Anwendungen im Bereich „Eigenschaften“



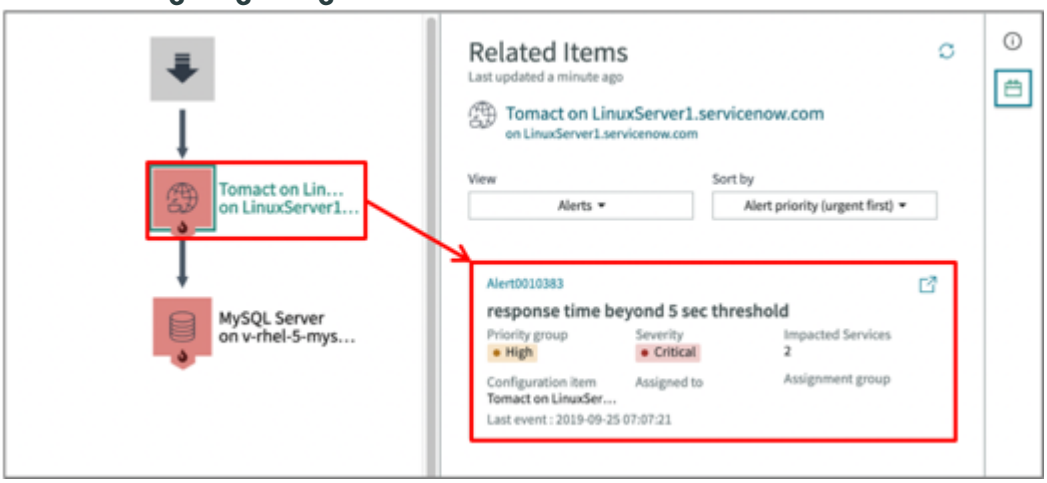
Zu Next-Gen BSM zugehörige Elemente

Klicken Sie auf das Symbol **Zugehörige Elemente**, um alle Warnungen oder Änderungen anzuzeigen, die mit diesem Anwendungsservice oder seinen CIs verknüpft sind.

Wenn Informationen zum ausgewählten CI oder zur ausgewählten Verbindung vorhanden sind, werden diese im Bereich „Zugehörige Elemente“ rechts im Fenster hervorgehoben.

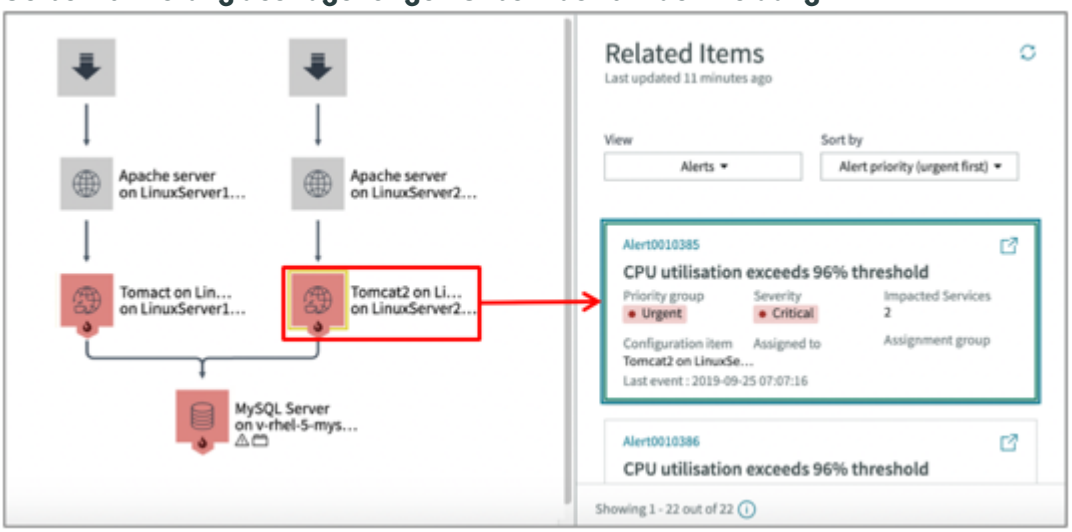
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs zur Anzeige zugehöriger Informationen auswählen



Wenn Sie Informationen im Bereich „Zugehörige Elemente“ im Zuordnungsfenster rechts auswählen, wird das zugehörige CI in Gelb angezeigt.

Gelbe Markierung des zugehörigen CI bei Auswahl der Meldung



Sie können andere zugehörige Elemente wie geplante Änderungen oder Fälle anzeigen, die dem Anwendungsservice zugeordnet sind. Weitere Informationen finden Sie unter Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich.

Zugehörige Informationen

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Zeigen Sie Zuordnungen für Anwendungsservices in an veraltet Mitarbeiterbereich

Verwenden Sie Zuordnungen, um Details von Anwendungsservices anzuzeigen. Zuordnungen zeigen Konfigurationselemente (CIs), aus denen Anwendungsservices bestehen, Verbindungen zwischen diesen CIs und andere servicebezogene Details.

Vorbereitungen

Erforderliche Rolle: sm_App_owner, Service_Mapping_user, evt_mgmt_admin, evt_mgmt_Operator oder evt_mgmt_user

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

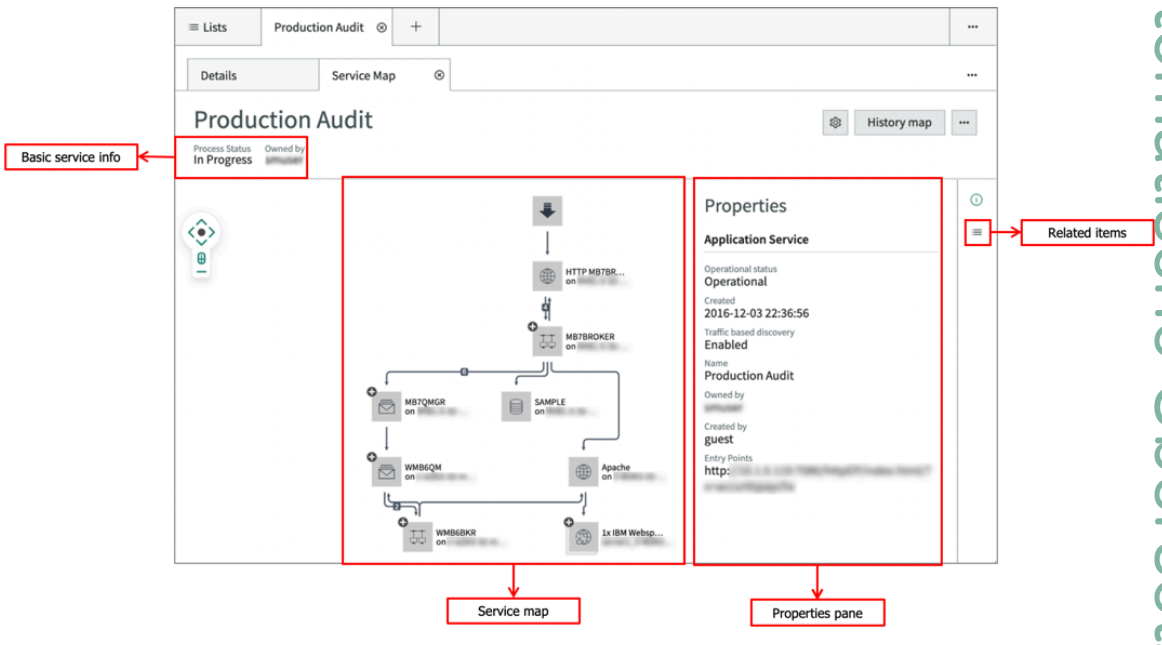
Warum und wann dieser Vorgang ausgeführt wird

Die Serviceinstanzzuordnung in Ereignismanagement Die Ansicht spiegelt den Schweregradstatus von CIs wider, die zur Serviceinstanz gehören. Weitere Informationen zum Anzeigen von Servicedetails in Zuordnungen finden Sie unter Anwendungsservicezuordnungen in veraltet Mitarbeiterbereich.

Prozedur

1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Alle** > **Services** > **Alle Services**an.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen der relevanten Serviceinstanz.
   Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.
4. Klicken Sie auf **Servicezuordnung**.

   Die Registerkarte „Servicezuordnung“ wird geöffnet und zeigt die Zuordnungsübersicht dieses Anwendungsservice an.



5. Klicken Sie auf CIs oder deren Verbindungen, um die Details im Bereich „Serviceeigenschaften“ auf der rechten Seite anzuzeigen.
6. Zeigen Sie zusätzliche Informationen für ein CI oder den Anwendungsservice selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen.
   Weitere Informationen finden Sie unter Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich.
7. Um auf die Servicezuordnung in der Standard-UI von Ereignismanagement zuzugreifen, die den vollständigen Funktionsumfang für Zuordnungen bietet, klicken Sie auf **Vollständige Karte**.

Zugehörige Informationen

Service-Mapping

Change-Historie von Anwendungsservices in veraltet Mitarbeiterbereich anzeigen

Zeigen Sie Änderungen an, die an einer Serviceinstanz und an den einzelnen Konfigurationselementen (Configuration Items, CIs) vorgenommen wurden, die den Service in enthalten Mitarbeiterbereich. Sie können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auch den Servicestatus vor und nach einem bestimmten Change oder Problem vergleichen. Die Change-Historie ist nützlich für Wartungs-, Planungs- oder Problembehebungsverfahren.

Vorbereitungen

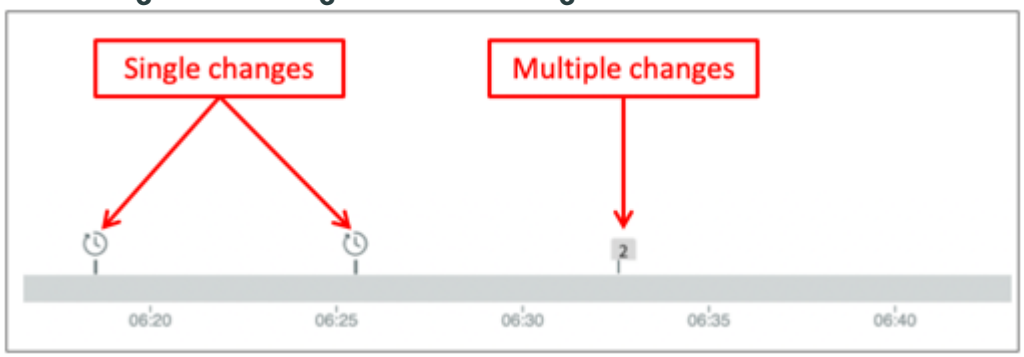
Erforderliche Rolle: admin, Service_Mapping_admin, Service_Mapping_user, App_Service_admin oder App_Service_user

Warum und wann dieser Vorgang ausgeführt wird

Details zu Änderungen an einer Serviceinstanz und ihren CIs werden in der CMDB gespeichert. Normalerweise spiegeln diese Änderungen das Hinzufügen oder Entfernen von CIs aus einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien wider. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

Änderungen an einem Anwendungsservice werden an der Verlaufszeitleiste angezeigt.

Darstellung der Änderungen am Anwendungsservice



Geben Sie zwei Zeitpunkte an, für die Sie die beiden Versionen eines Anwendungsservice vergleichen möchten. Mithilfe von Change-Markierungen auf der Zeitleiste können Sie Zeitpunkte angeben, die vor und nach der Änderung liegen, dessen Details Sie sehen möchten. Zum Beispiel können Sie, wenn Sie wissen, dass das Fehlschlagen eines Anwendungsservice zu einem bestimmten Zeitpunkt begonnen hat, zwei Versionen des Anwendungsservice (eine vor und eine nach Einsetzen des Problems) vergleichen. Dieser Vergleich zeigt Ihnen die Zusammenfassung der Changes, die möglicherweise zu den Problemen geführt haben.

Der Standardbereich der Zeitleiste ist die letzte Woche. Die Obergrenze für den Zeitbereich ist der Moment, in dem Sie die Zuordnung in der Ansicht „Change-Historie“ geöffnet haben. Wenn der Anwendungsservice vor weniger als einer Woche erstellt wurde, beginnt der Zeitbereich ab dem Zeitpunkt der Serviceerstellung.

Der Zeitbereich darf nicht mehr als 1000 Änderungen enthalten. Wenn sich innerhalb des ausgewählten Bereichs mehr Änderungen befinden, wird die Verlaufsskala automatisch so angepasst, dass 1000 Änderungen angezeigt werden.

Den Validierungsstatus von Änderungen sowie Änderungen an zugehörigen Elementen, zum Beispiel nachverfolgte Konfigurationsdateien, können Sie in der klassischen UI von Service-Mapping anzeigen. Weitere Informationen finden Sie unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen und Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

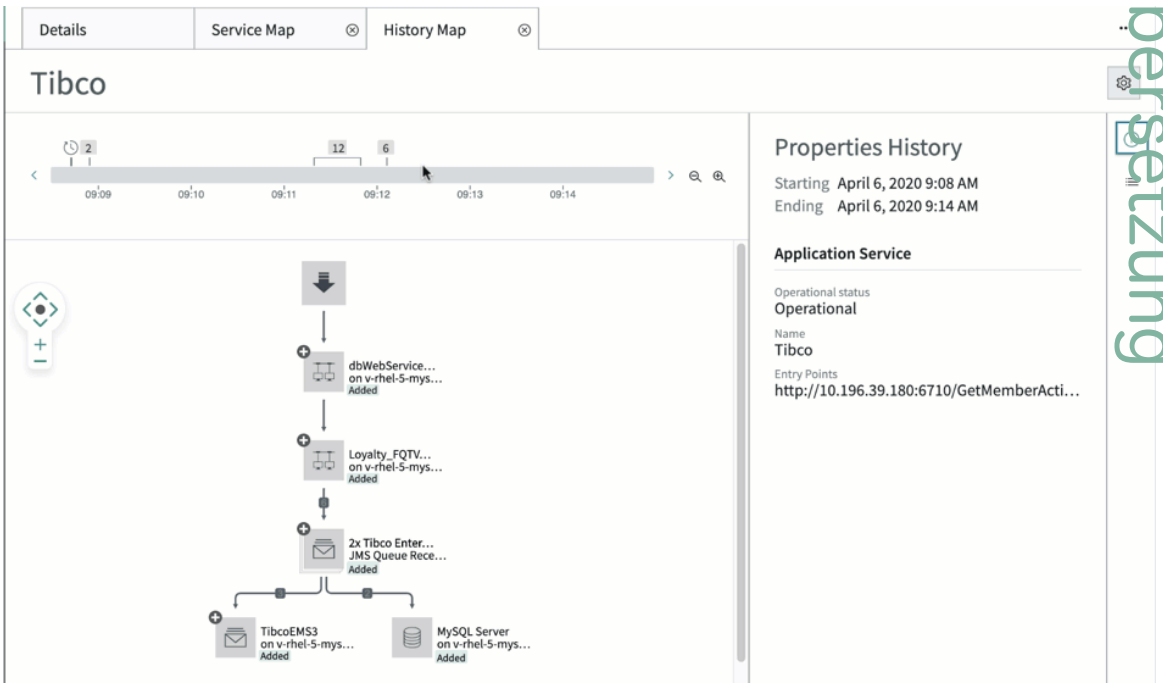
1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Alle** > **Services** > **Alle Services**an.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen der relevanten Serviceinstanz.
   Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.
4. Klicken Sie auf **Servicezuordnung**.

   Die Registerkarte „Servicezuordnung“ wird geöffnet und zeigt die Zuordnungsübersicht dieses Anwendungsservice an.
5. Klicken Sie auf **Change History Map (Change-Historienzuordnung)**.
   Die Registerkarte „Verlaufszuordnung“ zeigt die Zuordnung in der Verlaufsansicht an. Standardmäßig ist der Zeitraum eine Woche.
6. Um den Anwendungsservice vor und nach einer Änderung zu vergleichen, gehen Sie wie folgt vor:

   a. Ändern Sie den Zeitbereich auf der Zeitleiste, indem Sie neben der Zeitleiste auf die Schaltflächen **Vergrößern** oder **Verkleinern** klicken.
   Alternativ zeigen Sie auf die Zeitleiste und scrollen.

   Die Zuordnung zeigt Änderungen an CIs. CIs werden als hinzugefügt, aktualisiert oder gelöscht markiert.

   Im Bereich **Eigenschaftenverlauf** wird eine Vergleichsübersicht der Änderungen an diesem Anwendungsservice angezeigt. Klicken Sie auf **Change-Historie** , um Change-Datensatzkarten für diesen Anwendungsservice anzuzeigen.

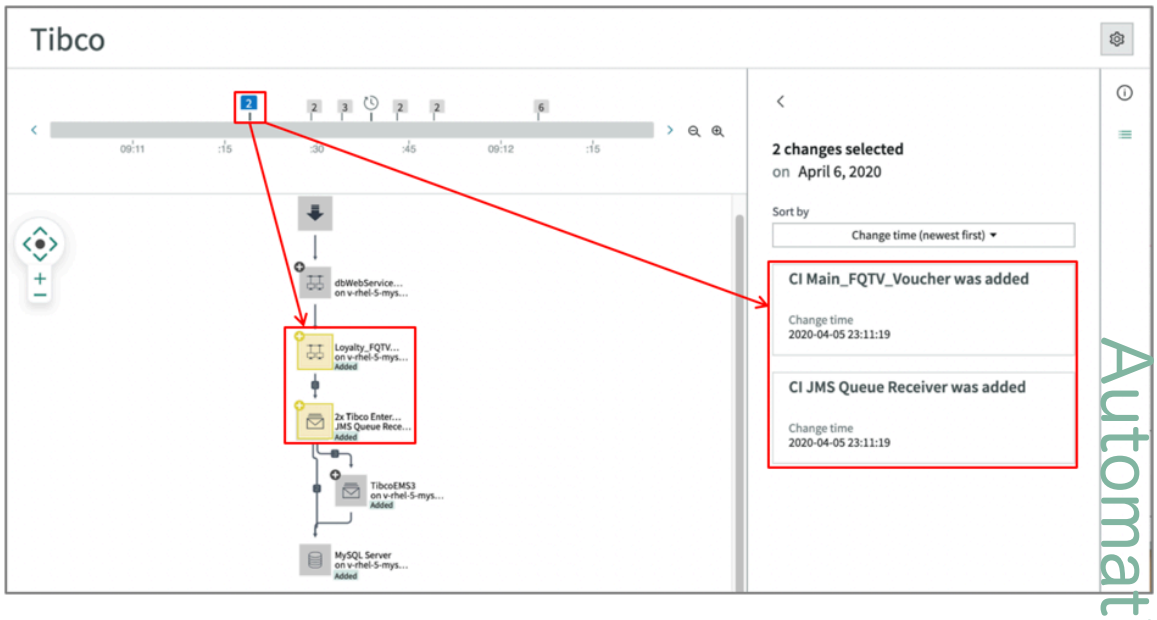


   b. Mit einer der folgenden Methoden können Sie Änderungen in der Zuordnung fokussieren:

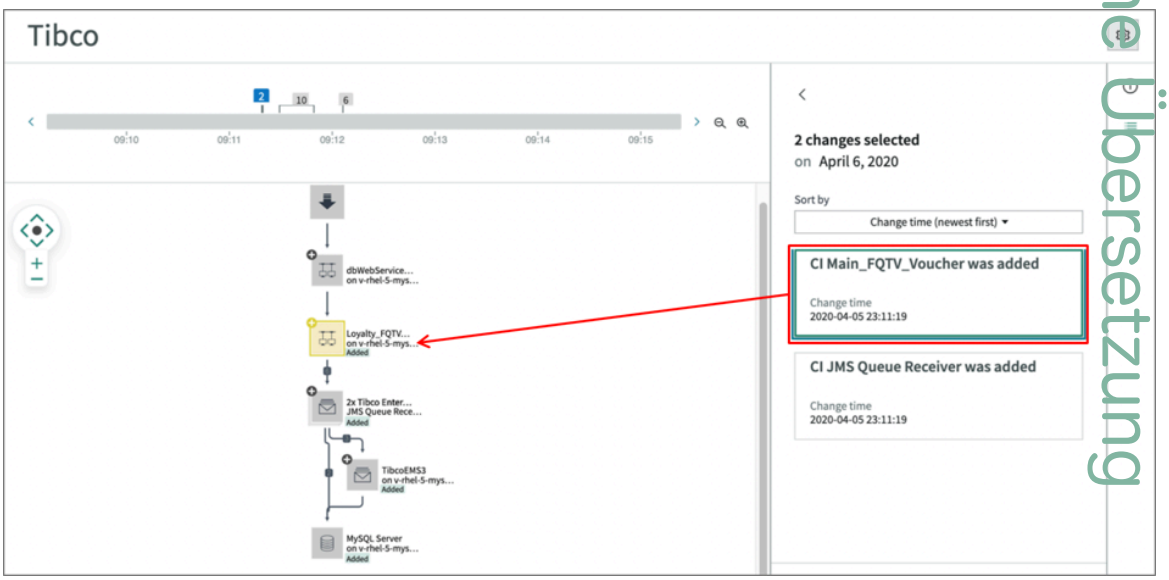
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um das für den Change-Datensatz verantwortliche CI zu markieren und die Change-Datensatzkarte anzuzeigen, klicken Sie auf die Change-Markierung auf der Zeitleiste. Sie können mehrere CIs markieren, indem Sie auf die Markierung für mehrere Changes klicken.



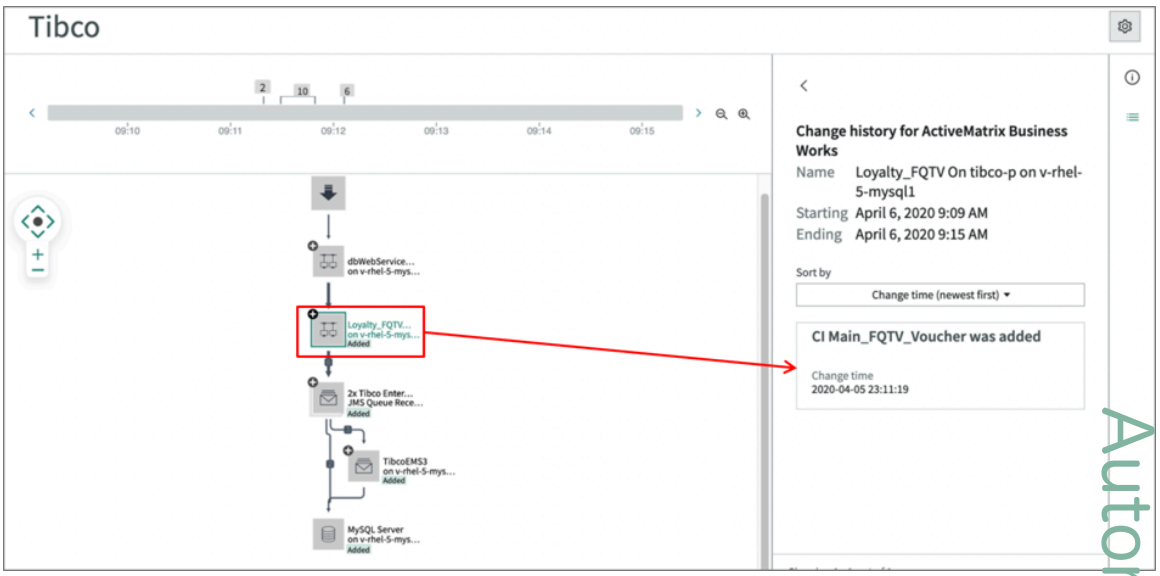
- Um das für den Change verantwortliche CI in der Zuordnung zu markieren, klicken Sie auf die Change-Datensatzkarte im Bereich „Change-Historie“.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie zum Anzeigen der zugehörigen Change-Datensatzkarte im Bereich „Change-Historie“ auf das CI in der Zuordnung.



Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich

Passen Sie eine Zuordnungsansicht an, um relevante Informationen anzuzeigen und die Übersichtlichkeit zu erhöhen.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_user, sm_App_owner, evt_mgmt_admin, evt_mgmt_Operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig sind Servicezuordnungen präzise und enthalten alle Details zu allen CIs, die Sie manuell hinzugefügt haben oder die von Service-Mapping zugeordnet wurden. Obwohl sie ein umfassendes Bild vermittelt, könnte die Verwendung einer solchen Zuordnung schwierig sein. Durch das Anpassen der Zuordnungen können Sie:

- die Navigation in der Zuordnung erleichtern
- irrelevante Informationen ausblenden
- wichtige Informationen anzeigen

Attribute, die Sie beim Anpassen von Zuordnungen anzeigen oder ausblenden, werden nicht dauerhaft entfernt und können nach Bedarf wieder angezeigt oder ausgeblendet werden. Das System speichert die Änderungen in der Kartenansicht und zeigt die letzte Kartenansicht an, wenn Sie eine Serviceinstanz erneut öffnen.

Die Serviceinstanzzuordnung in Ereignismanagement Die Ansicht spiegelt den Schweregradstatus von CIs wider, die zur Serviceinstanz gehören.

Prozedur

1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Services** > **Alle Services**an.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen des betreffenden Serviceinstanz .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

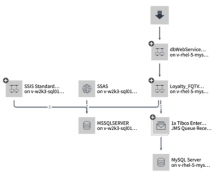
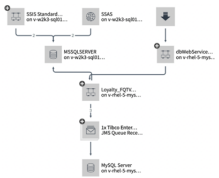
Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.

4. Klicken Sie auf **Servicezuordnung**.
5. Klicken Sie auf die Schaltfläche **Kartenanzeigeeinstellungen öffnen**.

6. Wählen Sie die relevante Option aus:

Option	Wenn aktiviert	Wenn deaktiviert
In Host-Ansicht anzeigen Die Host-Ansicht vereinfacht auch die Zuordnung, insbesondere wenn viele Anwendungen auf wenigen Hosts ausgeführt werden. Die Host-Ansicht ist nur für Serviceinstanzen nützlich, die mit erkannt wurden Service-Mapping. Diese Ansicht enthält keine zusätzlichen Informationen für manuell erstellte Serviceinstanzen.	Von der Servicezuordnung werden Host-CIs dargestellt.	In der Servicezuordnung werden Anwendungs-CIs dargestellt.
CIs in Zuordnung gruppieren Vereinfachen Sie Zuordnungen, indem Sie CIs gruppieren, die zu demselben Typ gehören und auf Servern gehostet werden, die sich Präfix und Domänennamen teilen. Die Zuordnung gibt den Anwendungs-Flow weiterhin korrekt wieder, da gruppierte CIs zur selben Ebene gehören. Diese Option ist für Serviceinstanzen relevant, die aus mehr als 10 CIs bestehen.	Die Serviceinstanzzuordnung zeigt Gruppen von CIs an. Die Zuordnung ist kompakter.	In der Serviceinstanzzuordnung werden alle CIs separat angezeigt. Die Zuordnung ist größer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
Topology Cycles entfernen Blenden Sie Verbindungen aus, die zu demselben Configuration Item (CI) zurückkehren, von dem sie stammen, um die Übersichtlichkeit der Zuordnung zu verbessern. Normalerweise sind diese zurückgegebenen Verbindungen für die Analyse oder Fehlerbehebung von Serviceinstanzen nicht wichtig.	In der Serviceinstanzzuordnung werden Topologiezyklen ausgeblendet.	Die Serviceinstanzzuordnung zeigt Topologiezyklen an.
Strukturansicht wird segmentiert Vereinfachen Sie die Zuordnung, indem Sie CIs in einer Baumstruktur anordnen und manche der Verbindungslinien verbergen. Diese Option ist besonders für sehr große Karten nützlich.	In der Zuordnung wird eine Serviceinstanz als Struktur angezeigt. 	Die Zuordnung spiegelt die tatsächliche Struktur einer Serviceinstanz wider. 
Datenverkehrsbasierte CIs anzeigen Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie mithilfe von datenverkehrsbasierter Zuordnung gefundene Configuration Items (CIs) an.	Die Serviceinstanzzuordnung zeigt CIs und Hosts an, die Service-Mapping Sowohl mit Mustern als auch mit der Traffic-basierten Discovery erkannt. Die Erkennung von eingehendem und ausgehendem CIs erstellt zwar eine inklusive Zuordnung, kann aber auch dazu führen, dass viele redundante CIs zugeordnet werden, die den Serviceinstanzvorgang nicht beeinflussen.	Die Serviceinstanzzuordnung zeigt nur CIs und Hosts, die mithilfe von Mustern erkannt wurden.
Zuordnungsindikatoren Zeigen Sie zusätzliche Informationen für ein CI	Für jeden Datensatztyp, der für die Anzeige festgelegt ist, werden der	Die Serviceinstanzzuordnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
oder eine Serviceinstanz selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen. Das Basissystem stellt Zuordnungsindikatoren für die folgenden Datensatztypen bereit: ○ Betroffene CIs ○ Änderungen: Aktuell, in der Vergangenheit oder geplant ○ Ausfälle: Aktuell, in der Vergangenheit oder geplant ○ Problem Weitere Informationen erhalten Sie im Video Event Management Map Indicators (Zuordnungsindikatoren in Event Management) .	entsprechende Indikator und die Registerkarte angezeigt. Beispielsweise wird die Registerkarte **Incidents** unter der Zuordnung angezeigt. Der Indikator **Incidents** wird neben CIs angezeigt, denen Incidents zugeordnet sind.	zeigt CIs ohne zugehörige Indikatoren.
	Wenn dem Anwendungsservice selbst ein Datensatz zugeordnet ist, wird der Indikator neben dem Namen des Anwendungsservice angezeigt.	Neben dem Anwendungsservicenamen sind keine Zuordnungsindikatoren zu sehen.

Service-Mapping-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Service-Mapping-Listen und -Formularen.

Service-Mapping Arbeitsbereich

Die Service-Mapping Der Arbeitsbereich bietet einen zentralen Ort, um den Prozess der Zuordnung Ihrer Anwendungsservices zu optimieren. Verwenden Sie die Visualisierungen und Berichte, um Ihre Ressourcen zu analysieren, zu überwachen und zu aktualisieren, Anwendungsservices zu erstellen und Ihre Servicezuordnungsaufgaben effizient zu verwalten.

Zugriff

Navigieren zu **Arbeitsbereiche** > **Service-Mapping**an.

Wichtige Funktionen und Fähigkeiten

- **Bereitschaft für maschinelles Lernen (ML)** – Bestätigen Sie, dass Ihre Umgebung für maschinelles Lernen vorbereitet ist, bevor Sie mit der Zuordnung von Anwendungsservices beginnen.
- **Detaillierte Servicezuordnungen** – Drilldown für detaillierte Informationen zu Servicezuordnungen für verschiedene Kategorien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *Empfehlungen für automatisierte Services*– Nutzen Empfehlungen für automatisierte Services Um vorgeschlagene Anwendungsservice-Kandidaten zu bewerten und sie zum Erstellen von Anwendungsservices oder zur Verbesserung vorhandener Services zu verwenden.
- **Verbesserte Ressourcennutzung** – Verwenden Sie nicht zugeordnete Server, die mit einem Anwendungsservice-Candidate verknüpft sind, um Anwendungsservices zu erstellen.
- **Tag-basierte Servicezuordnung** – Verwenden Sie das tagbasierte Zuordnungs-Dashboard, um die Konfigurationselemente (CIs) Ihrer Organisation Anwendungsservices zuzuordnen.

Wichtig:

Zugriff auf Tag-basierte Servicezuordnung in Service-Mapping Arbeitsbereich erfordert die Installation von Service-Mapping Plus Version 1.16.3. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Schlüsselmetriken

Zugeordnete Anwendungsservices

Die Anzahl der zuvor zugeordneten Anwendungsservices. Wählen Sie diese Option aus, um bestimmte Informationen zu diesen Services anzuzeigen, z. B. Betriebsstatus und Geschäftsrelevanz.

ML-gestützte Kandidaten

Die Anzahl der mit identifizierten Anwendungsservice-Candidates Empfehlungen für automatisierte Services Funktion.

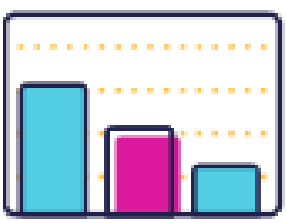
Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, der Filterprozess wurde aktualisiert, um nur die relevantesten Kandidaten einzubeziehen, ausgenommen ignorierte oder irrelevante Kandidaten. Diese Erweiterung erfordert die Installation von ITOM Content Service.

Zugeordnete Server

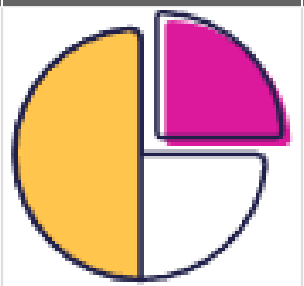
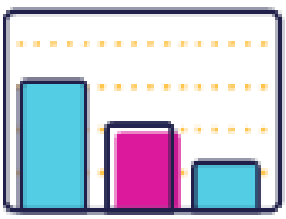
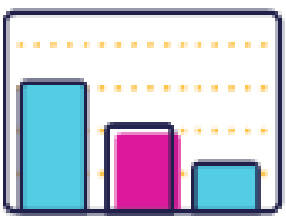
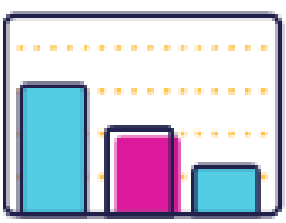
Die Anzahl der Server, die derzeit mit einem Anwendungsservice verknüpft sind. Wählen Sie diese Option aus, um Informationen wie Betriebsstatus und Besitzer anzuzeigen.

Berichte

Wählen Sie den entsprechenden Abschnitt jedes Berichts aus, um detailliertere Informationen anzuzeigen.

Titel	Typ	Quelltabelle	Beschreibung
Servicezuordnungen nach Betriebsart	Balkenbericht 	Zugeordneter Anwendungsservice [cmdb_ci_Service_detected]	Ein Balkenbericht, der die zugeordneten Anwendungsservices gruppiert nach Vorgangstyp darstellt.
Servicezuordnungen nach Erstellungsmethode	Kreisbericht	Zugeordneter Anwendungsservice [cmdb_ci_Service_detected]	Ein Kreisbericht, der die zugeordneten Anwendungsservices

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			gruppiert nach Erstellungsmethode darstellt.
Servicezuordnungen nach Relevanz	Balkenbericht 	Zugeordneter Anwendungsservice [cmdb_ci_Service_detected]	Ein Balkenbericht, der die zugeordneten Anwendungsservices gruppiert nach Relevanzgrad darstellt.
Nicht zugeordnete Server **Hinweis:** Diese Ansicht gilt für Anwender mit Service-Mapping Plus Versionen vor 1.16.3.	Balkenbericht 	Server [cmdb_ci_server] Zuordnung des Service-Konfigurationselements [svc_ci_assoc] Anwendungsservice-Kandidat [sa_ml_Application_Service_Candidate]	Ein Balkenbericht, der nicht zugeordnete Server enthält, die mit einem Anwendungsservice-Candidate abgeglichen wurden, sowie Server ohne Candidate. Wählen Sie Aus **Nicht zugeordnete Server mit Kandidat** Zum Anzeigen von Servern können Sie einen Anwendungsservice erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsservice für nicht zugeordnete Server.
Nicht zugeordnete Server **Hinweis:** Diese Ansicht ist ab verfügbar Service-Mapping Plus Version 1.16.3.	Balkenbericht 	Server [cmdb_ci_server] Zuordnung des Service-Konfigurationselements [svc_ci_assoc] Anwendungsservice-Kandidat [sa_ml_Application_Service_Candidate]	Ein Balkenbericht, der die Anzahl der nicht zugeordneten Server darstellt, unterteilt in zwei Kategorien: • **Nicht zugeordnete Server ohne Kandidat** – Server, die mit einem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Anwendungsservice-Candidate abgeglichen wurden. • **Nicht zugeordnete Server mit relevantem Kandidaten** – Server, die keinen Kandidaten haben. **Hinweis:** Beginnend mit Service-Mapping Plus Version 1.16.3, der Filterprozess wurde aktualisiert, um nur die relevantesten Kandidaten einzubeziehen, ausgenommen ignorierte oder irrelevante Kandidaten. Diese Erweiterung erfordert die Installation von ITOM Content Service.

Zusätzliche Komponenten

Mit Daten befüllen

Sie können diese Schaltfläche auswählen, um die Seite zu aktualisieren und die angezeigten Informationen so zu aktualisieren, dass sie die neuesten Daten widerspiegeln.

Suchen Sie nach Server

Sie können in diesem Feld einen bestimmten Server suchen, indem Sie den Servernamen eingeben, um eine Liste der Optionen anzuzeigen. Wählen Sie den gewünschten Server aus der Liste aus, und dann **Suchen** , Führt Sie zu **Zugeordneter Server** Seite. Wählen Sie den Servernamen aus, um detailliertere Informationen zu erhalten.

Tag-basiertes Service-Mapping

Wählen Sie das Symbol Tag-basierte Servicezuordnung aus Dient zum Zugriff auf das tagbasierte Servicezuordnungs-Dashboard. Hier können Sie die lokalen und Cloud-Ressourcen Ihres Unternehmens kategorisieren und Anwendungsservices zuordnen. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Anwendungsservice-Bereitschaft“

Wählen Sie das Symbol Anwendungsservice-Bereitschaft Um auf das Dashboard „Anwendungsservice-Bereitschaft“ zuzugreifen.

Verwenden Sie dieses Dashboard, um sicherzustellen, dass Sie aktiviert haben Predictive Intelligence, Überprüfen Sie die Bereitschaft für maschinelles Lernen, und bestätigen Sie, dass Ihre Daten trainiert wurden.

Weitere Informationen zur Anwendungsbereitschaft finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich.

Zugehörige Informationen

Empfehlungen für automatisierte Services

Ordnen Sie Anwendungsservices basierend auf zu Empfehlungen für automatisierte Services

Namensvorschläge für Anwendungsservice-Kandidaten

Namensvorschläge für Anwendungsservice-Kandidaten

Empfehlungen für automatisierte Services Bietet aussagekräftige Namensvorschläge für die Service-Identifizierung, auf die Sie im zugreifen können **Anwendungsservicevorschläge** Registerkarte in Service-Mapping Arbeitsbereich.

Namensvorschläge für Anwendungsservice-Candidate

Namensvorschlag	Beschreibung
Kandidatennamenvorschlag	Der Namensvorschlag des primären Kandidaten priorisiert Service-Fingerabdrücke Name, wird dann nach Bedarf auf andere Namensvorschläge zurückgestellt.
Servicefingerabdruck	Namensvorschläge aus maximal drei Service-Fingerabdrücke Bezieht sich auf den Kandidaten.
Lastenausgleichsmodul	Namensvorschläge aus den Namen der drei wichtigsten Lastenausgleichsmodul-Services, die dem Kandidaten zugeordnet sind.
Prozess	Namensvorschläge aus den Befehlszeilen des Prozesseinstiegspunkts für den Kandidaten. Ein Algorithmus identifiziert die relevantesten Wörter und stellt die drei wichtigsten Namensvorschläge bereit.
Eingabepunkt	Namensvorschläge aus allen Einstiegspunkt-IP-Adressen, die dem Kandidaten zugeordnet sind. Vorschläge für Einstiegspunktnamen sind ab Version 1.12.3 veraltet. Diese Spalte wird weiterhin angezeigt, aber nicht mehr mit Daten gefüllt. Es wird schließlich entfernt.
AFP (Anwendungsfingerabdruck)	Namensvorschläge aus den drei wichtigsten Anwendungsfingerabdrücken, die dem Kandidaten zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Empfehlungen für automatisierte Services

Ordnen Sie Anwendungsservices basierend auf zu Empfehlungen für automatisierte Services

Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Überprüfen Sie die Informationen im Dashboard, um sicherzustellen, dass Sie bereit sind, Anwendungsservices basierend auf maschinellem Lernen (ML) zu erkennen und zuzuordnen. Service-Mapping Verwendet von verarbeitete Daten Predictive Intelligence Zum Generieren von Vorschlägen für verkehrsbasierte Verbindungen.

Das Dashboard „Anwendungsservice-Bereitschaft“ ist Teil von Service-Mapping Plus, Verfügbar auf ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Predictive Intelligence Wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und ordnet ihre Relevanz ein. Service-Mapping Verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Es werden auch Verbindungsvorschläge generiert Für Server und Lastenausgleichsmodule Damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen.

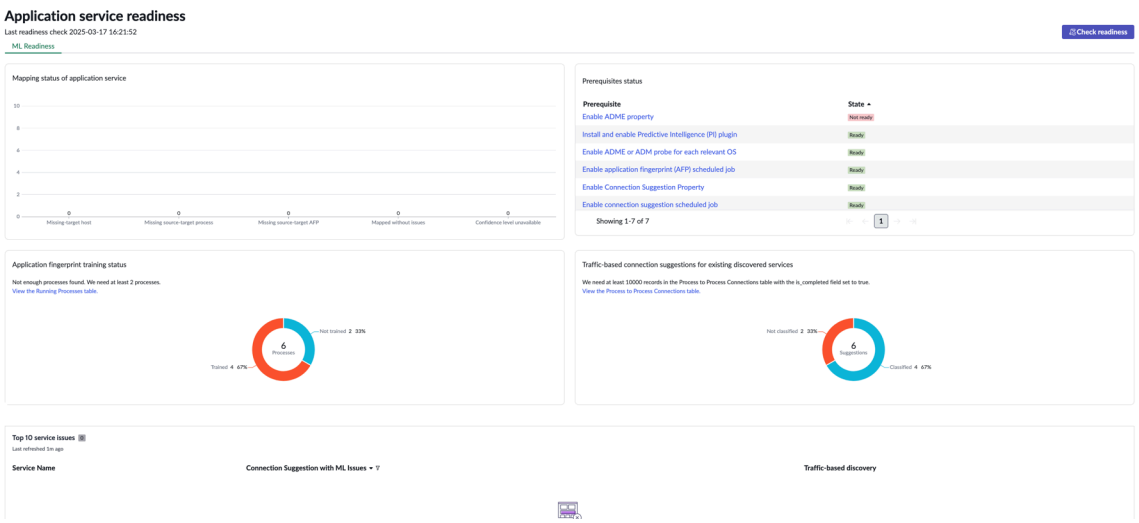
Widgets auf der ML-Dashboard-Seite zeigen die Informationen zu Voraussetzungen und Problemen im Zusammenhang mit der Service-Discovery basierend auf Predictive Intelligence an. Wählen Sie Links in den Widgets und Berichten aus, um zur zugehörigen Liste oder zum zugehörigen Formular zu navigieren.

Erforderliche ServiceNow AI Platform-Rollen

service_mapping_admin

Auf das Dashboard für Anwendungsservice-Bereitschaft zugreifen

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Service-Mapping**an. Wählen Sie dann das Symbol für Anwendungsservice-Bereitschaft .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte

Das Dashboard enthält die folgenden Berichte.

Titel	Typ	Quelltabelle	Beschreibung
Mapping status of application service (Zuordnungsstatus des Anwendungsservice)	Ein Balkenbericht	ML-Related Service Status [ml_related_service_status] (ML-bezogener Servicestatus)	Ein Balkenbericht, der die Zusammenfassung von ML-bezogenen Problemen in zugeordneten Anwendungsservices enthält. Ausführliche Informationen finden Sie unter Zuordnungsstatus der Anwendungsservices.
Application fingerprints training status (Trainingsstatus von Anwendungsfingerabdrücken)	Ein Ring-Bericht	AFP-Trainingsstatus [afp_training_status]	Ein Ringbericht, der den Trainingsstatus von Anwendungsfingerabdrücken zeigt. Predictive Intelligence trainiert Vorhersagemodelle und ML-Lösungen (maschinelles Lernen). Zeigen Sie mit Predictive Intelligence den Trainingsstatus für Anwendungs-Fingerabdrücke an, um zu verstehen, ob Ihre Bereitstellung für die Zuordnung bereit ist.
Datenverkehrsbasierte Verbindungsvorschläge für vorhandene erkannte Services	Ein Ring-Bericht	Verbindungsvorschläge [sa_ml_connection_Suggestion]	Ein Ringbericht, der das Verhältnis von klassifizierten Verbindungen zu gültigen Verbindungen in der Tabelle „Verbindungsvorschläge“ widerspiegelt. Diese Tabelle wird nur während der Top Down-Discovery ausgefüllt.

Zuordnungsstatus der Anwendungsservices

Überprüfen Sie die Zusammenfassung der ML-bezogenen Probleme in zugeordneten Anwendungsservices.

Kategorie	Beschreibung
Ohne Probleme zugeordnet	Die Anzahl der Serviceinstanzen, die ohne ML-bezogene Probleme erkannt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Beschreibung
Quell-Ziel-AFP fehlt	Die Anzahl der Serviceinstanzen, bei denen einige Anwendungsfingerabdrücke für einen Quell- oder Zielprozess fehlen. Um diese Probleme zu beheben, kalibrieren Sie die auf Fingerabdrücken basierte Discovery.
Quell-Ziel-Prozess fehlt	Die Anzahl der Serviceinstanzen, denen einige Quell-/Ziel-Prozessinformationen fehlen. Um diese Probleme zu beheben, lassen Sie die Zielhosts erneut erkennen und stellen Sie sicher, dass die relevanten Prozesse erkannt werden.
Konfidenzniveau nicht verfügbar	Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist. Wenn das Konfidenzniveau als **N/V** angezeigt wird, warten Sie, bis das Training der Anwendungsfingerabdrücke abgeschlossen ist.
Zielhost fehlt	Die Anzahl der Serviceinstanzen mit einigen CI-Verbindungen, die nicht vollständig erkannt wurden, da die horizontale Discovery Host-CIs nicht erkannt hat. Um diese Probleme zu beheben, lassen Sie die Zielhosts erneut erkennen und stellen Sie sicher, dass die relevanten Prozesse erkannt werden.

Status der Voraussetzungen

Die Serviceinstanzzuordnung erfordert die Integration mehrerer Module und Anwendungen: Anmeldeinformationen, Predictive Intelligence, Erweiterte Discovery von Application Dependency Mapping (ADME) und geplante Aufgaben. Überprüfen Sie die Liste der Voraussetzungen und stellen Sie sicher, dass der Status aller Voraussetzungen **Bereit** lautet.

Voraussetzung	Beschreibung
Installieren und aktivieren Sie das Plugin „Predictive Intelligence (PI)“.	Service-Mapping verwendet Predictive Intelligence, um Verbindungsvorschläge zu generieren. 1. Stellen Sie sicher, dass das Plugin „Predictive Intelligence“ als **Installiert** angezeigt wird. 2. Klicken Sie auf die Kachel Predictive Intelligence und überprüfen Sie, ob der **Status** als **Aktiv** angezeigt wird. Wenn der Status **Inaktiv** ist, wählen Sie unter **Zugehörige Links** den Link **Aktivieren/Reparieren** aus.
Aktivieren Sie die Eigenschaft ADME.	Service-Mapping verwendet ADME-Proben. Stellen Sie sicher, dass die Eigenschaft `glide.discovery.enable_adme` auf **true** festgelegt ist.
Aktivieren Sie ADME- oder ADM-Probe für jedes relevante Betriebssystem	Es gibt mehrere ADME-Proben für verschiedene Arten von Betriebssystemen. Aktivieren Sie alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzung	Beschreibung
	erforderlichen Proben, um Konfigurationselemente (CIs) in Ihrer Umgebung zu erkennen.
Erweiterung der IP-Adresse zulassen	Diese Einstellung hilft bei der Verwaltung der Erweiterung globaler Adressen (z. B. „0,0.0,0“ oder „*“) in einzelne IP-Adressen. Der Grenzwert für diese Erweiterung muss größer als 0 sein. So überprüfen und legen Sie diesen Grenzwert fest: 1. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_property]. 2. Suchen Sie nach *sn.adm.ip_expansion_limit*Eigenschaft. 3. Stellen Sie sicher, dass diese Eigenschaft auf eine positive Zahl festgelegt ist.
Aktivieren Sie die regelmäßige AFP-Aufgabe (Application Fingerprint).	Stellen Sie sicher, dass die geplante Aufgabe *Applications suggestion - ITOM Autodisco* für die auf Fingerabdrücken basierte Discovery auf **Aktiv** festgelegt ist.
Aktivieren Sie die Eigenschaft „Verbindungsvorschlag“.	Bestätigen Sie diese Discovery basierend auf Predictive Intelligence Ist aktiviert. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob *sa_ml.connection_suggestions.active*Eigenschaft ist auf festgelegt **Wahr** .
Aktivieren Sie die regelmäßige Aufgabe für Verbindungsvorschläge.	Stellen Sie sicher, dass der **Status** der regelmäßigen Aufgabe *Service Mapping - Traffic Process to Process* **Aktiv** ist. Diese regelmäßige Aufgabe löst die Generierung von Verbindungsvorschlägen aus.

Serviceprobleme

Überprüfen Sie die Liste der Serviceinstanzen, die am stärksten von ML-bezogenen Problemen betroffen sind. Die Liste der am stärksten betroffenen Services ist verfügbar, wenn die Funktion für Verbindungsvorschläge in Ihrer Bereitstellung aktiviert ist. Die Liste zeigt Servicenamen und die Anzahl der ML-bezogenen Probleme für jeden von ihnen. Sie gibt auch an, ob die datenverkehrsbasierte Funktion für die Services aktiviert ist.

Zugehörige Informationen

Weitere Informationen zu ADME-Probes

Erkennung mithilfe von ADME-Probes aktivieren und konfigurieren

Auf Fingerabdrücken basierte Erkennung kalibrieren

Sicherstellen, dass die auf Fingerabdrücken basierte Erkennung Vorschläge generiert

Troubleshooting guide for Service Mapping ML Connection Suggestions (Fehlerbehebungsleitfaden für ML-Verbindungsvorschläge von Service Mapping) [KB0963421]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Service-Mapping Plus installierte Komponenten

Bei der Aktivierung des Service-Mapping Plus-Plugins werden mehrere Arten von Komponenten installiert, z. B. Tabellen und regelmäßige Aufgaben.

Hinweis: Die Service-Mapping Plus Die Anwendung ist in verfügbar ServiceNow Store an.

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Update statistics for application service readiness dashboard (Statistiken für das Dashboard der Anwendungsservice-Bereitschaft aktualisieren)	Aktualisiert die im Dashboard „Application Service Readiness“ (Bereitschaft von Anwendungsservices) angezeigten Informationen. Wird stündlich ausgeführt. Wird darüber hinaus ausgeführt, wenn die Schaltfläche **Check readiness** (Bereitschaft prüfen) im **Dashboard „Application Service Readiness“** (Bereitschaft von Anwendungsservices) ausgewählt wird. Das System löst diesen regelmäßigen Auftrag nicht früher als fünf Minuten nach der letzten Ausführung aus.

Installierte Tabellen

Tabelle	Beschreibung
ML-Related Service Status [ml_related_service_status] (ML-bezogener Servicestatus)	Enthält die Informationen zu ML-bezogenen Problemen in zugeordneten Anwendungsservices.
Top ML Error Services [top_ml_err_services_list] (Services mit meisten ML-Fehlern)	Enthält die Liste von bis zu 10 Anwendungsservices mit der größten Anzahl von ML-bezogenen Problemen.
ML Dashboard Prerequisites [ml_dashboard_prerequisites] (ML-Dashboard-Voraussetzungen)	Enthält die Links zu Formularen und Tabellen, die die Einrichtung der Zuordnung basierend auf ML erfordern, sowie die Statusinformationen für diese Konfigurationen.
AFP-Trainingsstatus [afp_training_status]	Enthält den Status des Trainings der Anwendungsfingerabdrücke.
Connection Suggestions Training Status [connection_suggestion_training_status] (Verbindungsvorschläge-Trainingsstatus)	Enthält den Status der Verbindungsvorschläge.
ML P2P ETA-Berechnungskonstanten [sa_ml_p2p_eta_values_list]	Speichert die Informationen darüber, wie das System die verbleibende Zeit für das Training von Verbindungsvorschlägen berechnet.

Installierte Eigenschaften

Eigenschaft	Beschreibung
sa.asc.Logger_level	Fügt dem Systemprotokoll für den Anwendungsservice-Candidate Nachrichten hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ:** Zeichenfolge • **Standardwert:** Fehler • **Andere mögliche Werte:** Debuggen **Hinweis:** Wenn Sie die Eigenschaft auf Debuggen festlegen, werden sowohl Debug- als auch Fehlermeldungen angezeigt.
sa.Topdown.enable_cmdb_based_Mapping	Diese Eigenschaft aktiviert die CMDB-basierte Zuordnung mit CMDB Anstelle von MID-Server. • **Typ:** boolescher wert • **Standardwert:** false • **Andere mögliche Werte:** Wahr
sn_sm_Scoped_App_App.sa.Unified_Map.enabled	Aktiviert den Zugriff auf Einheitliche ÜbersichtÜber Service-Mapping Arbeitsbereich. • **Typ:** boolescher wert • **Standardwert:** false • **Andere mögliche Werte:** Wahr
sn_cmdb_WS_config_property.unifiedmap.Map_search.max_nodes	Um eine hohe Leistung sicherzustellen, begrenzt diese Eigenschaft die Anzahl der Knoten, die auf einer Karte angezeigt werden können. • **Typ:** Ganzzahl • **Standardwert:** 250 Höhere Werte können die Leistung beeinträchtigen, da Einheitliche Übersicht Lädt alle Elemente und zugehörigen Details, wenn sie geöffnet werden. **Hinweis:** Die `unifiedmap.map_search.max_nodes`Die Eigenschaft in der arbeitsbereichsspezifischen Tabelle [sn_cmdb_WS_config_property] ersetzt die veraltete `sn_cmdb_ws.node.map.max.edge.count`Eigenschaft.
sn_sm_scoped_App.svc_by_Tags.max_Candidates_per_family	Begrenzt die maximale Anzahl von Tag-basierten Servicekandidaten, die für eine einzelne Familie erstellt wurden. Wenn die Familiendefinition weitere Kandidaten enthält, haben die zuletzt aktualisierten CIs Vorrang. Dieser Wert gilt für alle Tag-basierten Servicefamilien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ:** Ganzzahl • **Standardwert:** 200
sn_sm_Scoped_App.max_valid_Discovery_period_in_days	Legt die maximale Anzahl von Tagen fest, die ein Host beim Generieren von Anwendungsservice-Kandidaten als gültig gilt. Durch Festlegen dieses Werts auf eine nicht positive Ganzzahl wird diese Funktion deaktiviert. ⚠ **Warnung:** Wenn dieser Wert niedriger als oder zu nahe am Discovery-Zyklus festgelegt wird, werden möglicherweise alle Hosts entfernt. Daher werden keine neuen Kandidaten erstellt, und vorhandene Kandidaten werden gelöscht. • **Typ:** Ganzzahl • **Standardwert:** 0

Mit Service-Mapping installierte Komponenten

Bei Aktivierung des Service-Mapping-Plugins werden mehrere Arten von Komponenten installiert, zum Beispiel Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
[app_service_admin]	Erstellt und ändert Serviceinstanzen, erstellt Servicegruppen, zeigt Serviceinstanzzuordnungen an und bearbeitet sie.	[itil]
[app_service_user]	Zeigt Zuordnungen für operative Serviceinstanzen an und ruft Serviceinhalte mithilfe der getContent – GET REST API ab. Die ITIL-Rolle, die als die grundlegende Help Desk-Technikerrolle dient, enthält die Rolle „app_service_user“.	[cmdb_read]
[itom_admin]	Konfigurieren Sie IT Operations Management-Anwendungen mit dem geführten Setup für ITOM.	[sn_bm_client.benchmark_data_viewer] [sm_itom_license.reader]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Das ITOM Guided Setup umfasst nicht Service-Mapping.	
[sam_core_admin]	Eine interne Rolle	[sam_core_user]
[sam_core_user]	Eine interne Rolle	[itil]
[Service_Mapping_admin]	Richtet die Service-Mapping-Anwendung ein. Ordnet Serviceinstanzen zu, korrigiert und verwaltet sie. Führt auch eine erweiterte Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.	• [app_service_admin] • [app_service_owner] • [discovery_admin] • [itil_admin] • [itom_admin] • [sam_core_admin] • [personalize_dictionary] • [pd_admin] • [pd_user] • [Service_Mapping_user]
[sm_app_owner]	Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_App_owner Anwendern zu, die Serviceinstanzen besitzen und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.	[Service_Mapping_user]
[sm_itom_license.reader]	Zeigen Sie Abonnementinformationen und Statistiken für IT Operations Management-Anwendungen an.	[cmdb_read]
[Service_Mapping_user]	Zeigt Zuordnungen für operative Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität	• [sam_core_user.service_mapping_user] • [itil.service_mapping_user]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	und Verfügbarkeit von Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.	
[sn_svc_err.admin]	Behebt Erkennungsfehler als Massenvorgang mithilfe der Fehler-Framework-Funktion in Service-Mapping und Discovery.	[itil]
[pd_admin]	Erzeugt neue und modifiziert vorhandene Muster, die Service-Mapping und Discovery für die Horizontal- und die Top Down-Discovery verwenden.	[pd_user]

Hinweis: Nur Benutzer mit der Rolle itil können alle Serviceinstanzen anzeigen.

Regelmäßige Aufgaben installiert

Regelmäßige Aufgabe	Beschreibung
Aufgeschobene Discovery-Bereinigung [sysauto_script_ba4bee737f0022008f1c3b19befa9108]	Wird jede Minute ausgeführt. Erkennt und beendet Erkennungszeitpläne für TCP-Verbindungen, die sich nicht mehr im aktiven Status befinden (5 Minuten ohne Aktivität).
Abfragebasierte Services aktualisieren [sysauto_script_08745913f31131002e6bae4716612bf1]	Wird alle 10 Minuten ausgeführt. Aktualisiert Ansichten für alle definierten technischen Services.
Anwendungsservicestatus aktualisieren [sysauto_script_5641702ac32102003e76741e81d3ae9e]	Wird jede Minute ausgeführt. Aktualisiert das Discovery-Statusattribut für Anwendungsservices. Der Discovery-Status wird als Gesamtstatus für alle Endpunkte berechnet, die ein sind Serviceinstanz Enthält.
Flow Discovery-Planer [sysauto_script_74c676f0dbb0220060ff742eaf9619f2]	Wird alle 10 Minuten ausgeführt. Löst die Netzwerk-Flow-Discovery aus und schreibt die Daten in die Tabelle [sa_flow_connector]. Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese regelmäßige Aufgabe, um CIs mithilfe von Netflow zu erkennen (siehe Beschreibung in Datenerfassung und -erkennung mit Netflow).
Einstiegspunktkandidaten aus Netflow- und netstat-Daten generieren [sysauto_script_b0b95067c3d0030039a3553a81d3aeb5]	Wird täglich ausgeführt. Scannt die TCP-Verbindungstabelle [cmdb_tcp] und verwendet diese Daten, um Einstiegspunkte zu generieren und in der Tabelle „Kandidateneinstiegspunkte“ [sa_cand_entry_point] zu speichern. Diese regelmäßige Aufgabe unterstützt das Generieren von Einstiegspunkten, die für die Zuordnung mehrerer Anwendungsservices (als Massenvorgang) erforderlich sind. Diese regelmäßige Aufgabe ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Thread-Sicherungen speichern [sysauto_script_a49cd030c302020039a3553a81d3aefb]	Standardmäßig nicht aktiv. Wenn die Aufgabe aktiviert wird, werden Thread-Sicherungen gesammelt, und die Daten werden in der Tabelle [sys_thread_dump] gespeichert.
Statistiken für langsame Schritte speichern [sysauto_script_dc0de690c302020039a3553a81d3aee0]	Wird jede Minute ausgeführt. Sammelt Daten zur langsamen Ausführung von Musterschritten und schreibt diese Daten in die Tabelle [sys_step_pattern].
Anzahl der Server berechnen [sys_trigger_db438f407f510200f128134f8dfa91c6]	Wird jeden Sonntag ausgeführt. Aktualisiert die Lizenzierungsmetrik mit der Gesamtanzahl der erkannten Server in der Instanz. Diese Informationen dienen zur Abrechnung. In Instanzen mit Domänentrennung wird die Anzahl für jede Domäne aktualisiert.
DNS-Suche für alle Einstiegspunkte und manuellen Verbindungsendpunkte ausführen [f178ab457fb213001952baf8befa91d3]	Führt für alle Einstiegspunkte und manuellen Verbindungsendpunkte die Probe zur DNS-Suche aus und aktualisiert Informationen über die entsprechenden IP-Adressen in der CMDB. Diese regelmäßige Aufgabe ist standardmäßig deaktiviert.
[SM-Deduplizierungs-Tracker für bestimmte Erkennungsquellen]	In einigen Fällen identifizieren Service-Mapping und Discovery- oder Überwachungstools von Drittanbietern dasselbe Konfigurationselement (CI) unterschiedlich. Das führt dazu, dass die Anwendungstabelle CMDB zwei Datensätze für dasselbe CI enthält. Diese regelmäßige Aufgabe scannt die CMDB-Anwendungstabellen mit den Informationen über CIs, die als generische Anwendungen identifiziert wurden. Wenn die regelmäßige Aufgabe aufgrund des CI-Typs und der Erkennungsquelle doppelte Datensätze identifiziert, wird eine Deduplizierungsaufgabe erstellt.
[sys_auto_flush_5211e7e1c320220039a3553a81d3aee6]	Bereinigt in der Tabelle [sa_flow_connection] Datensätze, die in den letzten sieben Tagen nicht aktualisiert wurden
[sys_auto_flush_956d498b938503006a7031f6357ffbec]	Bereinigt in der Tabelle [sa_performance_statistics] Datensätze, die Statistiken über die gesamte Ereignisverarbeitungszeit enthalten und vor mehr als 30 Tagen erstellt wurden
[sys_auto_flush_ce1a978193001200e0e931f6357ffb59]	Bereinigt in der Tabelle [sa_performance_statistics] Datensätze, die vor mehr als 2 Tagen erstellt wurden
[sys_auto_flush_b24d9c30c302020039a3553a81d3ae53]	Bereinigt in der Tabelle [sys_thread_dump] Datensätze, die vor mehr als 7 Tagen erstellt wurden
[sys_auto_flush_cf129ebe7f223200995cbaf8befa916f]	Bereinigt in der Tabelle [sa_ml_feature_data] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden und einen Sonderstatus aufweisen (leeres Bezeichnungsfeld)
[sys_auto_flush_d2516be1c320220039a3553a81d3ae21]	Bereinigt in der Tabelle [sa_flow_service] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
[sys_auto_flush_db416be1c320220039a3553a81d3ae1f]	Bereinigt in der Tabelle [sa_flow_server_comm] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden.
[sys_auto_flush_41d9b007b71310105984eb25de11a96e]	Löscht die Tabelle für Verbindungsvorschläge [sa_ml_connection_suggestion] aus den alten Datensätzen, die den folgenden Bedingungen entsprechen: • Sie wurden in den letzten 7 Tagen nicht aktualisiert. • Der Vorschlagsdatensatz enthält eine aktive erkannte TCP-Verbindung (TCP-Verbindungsdatensatz fehlt nicht). • Dem Datensatz ist keine Benutzerentscheidung vom Typ „Hinzufügen“ oder „Entfernen“ zugeordnet.

Installierte Tabellen

Tabelle	Beschreibung
Skripts für Aufgabe vor Service Mapping [sa_pre_task_script]	Enthält Skripts, die Service-Mapping in der Instanz ausführt, und sammelt Informationen, die bei der Identifizierung des relevanten Musters für ein CI helfen
Verkehrsbasierte Verbindungsqualifizierer [cmdb_ci_qualifier_traffic_based_connection]	Veralteter Inhalt. Wird in der aktuellen Version nicht verwendet.
Dynamic CI-Gruppe [cmdb_ci_query_based_service]	Enthält technische Services
Komponenten [sa_bs_components]	Enthält Informationen über Komponenten, die Teil des Serviceinstanz sind. Kunden geben diese Informationen manuell auf der Registerkarte „Fragebogen“ im Formular des Serviceinstanz ein.
Kandidateneinstiegspunkte [sa_cand_entry_point]	Enthält Informationen über potenzielle Einstiegspunkte, die Service-Mapping aus Lastenausgleichsmodulen oder datenverkehrsbasierten Verbindungen abgerufen hat
Dashboard-Ansicht [sa_dashboard_view]	Enthält eine Konfiguration, die definiert, welche Services in der Servicestruktur angezeigt werden
Service-Discovery-Nachrichten [sa_discovery_message]	Enthält Erkennungsmeldungen und -fehler, die Service-Mapping während des Erkennungsprozesses generiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
ITOM-Fehleraufgabe [sa_error_handler_task]	Enthält Informationen, die Service-Mapping und Discovery zur Fehlerbehandlung verwenden
Fehler-EP ALS manueller EP [sa_errors_as_manual_ep]	Enthält Daten zu Fehlern, die Kunden während des folgenden Verfahrens überspringen: Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren.
Manuelle Verbindungen [sa_manual_connections]	Enthält Informationen über Endpunkte, die Kunden beim Hinzufügen manueller Verbindungen verwenden
ML-Featuredaten [sa_ml_feature_data]	Interne Tabelle
ML-Modell [sa_ml_model]	Interne Tabelle
ML-Datenverkehrvalidierung [sa_ml_traffic_validation]	Interne Tabelle
Leistungsstatistiken [sa_performance_statistics]	Interne Tabelle zum Speichern von Leistungsdaten zur Auswirkungsberechnung in Ereignismanagement
Servicezuordnungen [sa_service_counters]	Speichert Daten über die Anzahl der CIs und Erkennungsfehler pro erkanntem Service
Eingabepunkte für Simulation [sa_simulation_entry_points]	Interne Tabelle
Serviceaufgabenprozess [service_process_task]	Speichert Datenanforderungen und Überprüfungsanforderungen für Anwendungsservices.
Langsame Schritte [sys_step_pattern]	Speichert Informationen über die langsame Ausführung von Musterschritten. Diese Daten werden zur Überwachung und Problembehandlung verwendet.
Thread-Sicherung [sys_thread_dump]	Interne Tabelle zum Speichern von Leistungsdaten für die Fehlerbehebung in Ereignismanagement
Automatisierungsfehler-Kategorie [automation_error_category]	Speichert alle unterstützten Kategorien für Fehler
Automatisierungsfehler-Kategorien-Statistik [automation_error_category_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlerkategorien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Automatisierungsfehlercode [automation_error_code]	Speichert alle unterstützten Fehlercodes für Erkennungsfehler
Automatisierungs-Fehlercode-Statistik [automation_error_code_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlercodes
Statistik zu Automatisierungsfehler-Discovery-Kategorien [automation_error_discovery_category_stats]	Veraltet.
Statistik zum Automatisierungsfehler-Discovery-Code [automation_error_discovery_code_stats]	Veraltet.
Automatisierungsfehler-Discovery-Nachricht [automation_error_discovery_msg]	Speichert die neuesten Fehlermeldungen
Automatisierungsfehlerkategorien – Statistiken [automation_error_instance_category_stats]	Speichert die neuesten Fehlerstatistiken für alle Kategorien pro Instanz (Discovery-Status)
Automatisierungsfehler-Kategorien-Statistik [automation_error_instance_code_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlercodes pro Instanz (Discovery-Status)
Automatisierungsfehler # Instanzmeldung [automation_error_instance_msg]	Speichert alle der Instanz zugeordneten neuesten Fehler (Discovery-Status)
Automatisierungsfehler # Instanzmeldung [automation_error_stats_update_time]	Speichert die letzte Aktualisierungszeit für jede Anwendung
Automatisierungsfehlervorschlag [automation_error_suggestion]	Enthält alle konfigurierten Vorschläge, die an der Benutzeroberfläche für verschiedene Fehlercodes angezeigt werden
Automatisierungsquellenapplikation [automation_source_application]	Enthält die Quellanwendungen, die das Fehler-Framework von Discovery und Service-Mapping verwenden
Zuordnung zwischen Vorschlag und Fehlercode [suggestion_error_code_m2m]	Enthält Informationen über die Zuordnung zwischen Fehlercode und Empfehlung
ITOM-Fehleraufgabe [sa_error_handler_task]	Enthält die für verschiedene Fehlergruppen konfigurierten Aufgaben
Applicative-Anmeldeinformationen [sa_applicative_credentials]	Enthält Anmeldeinformationen, die beim Ausführen von anwendungsspezifischen Befehlen auf Servern verwendet werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Service-Mapping CI-Attribute [sa_ci_attr]	Enthält CI-Attribute, die nur für den Erkennungsprozess relevant sind
Zugehörige CI-Typen [sa_ci_to_pattern]	Weist Mustern CI-Typen zu (nur relevant für die horizontale Erkennung durch Discovery)
Muster-Debugger-Sitzung [sa_debug_session]	Diese interne Tabelle wird für die Komponenten des Musterdesigners verwendet.
Status der Muster-Debugger-Sitzung für UI [sa_debug_session_status]	Diese interne Tabelle wird für die Komponenten des Musterdesigners verwendet.
Sa zurückgestellte Service-Discovery [sa_deferred_service_discovery]	Diese interne Tabelle wird für die Service-Mapping-Komponenten verwendet.
Service-Discovery-Protokoll [sa_discovery_log]	Enthält von Service-Mapping gesammelte Discovery-Protokolle
Service-Discovery-Nachrichten [sa_discovery_message]	Enthält Nachrichten, die von Service-Mapping während der Serviceerkennung erstellt wurden
Sa-Endpunkt-Status [sa_endpoint_status]	Enthält den Discovery-Status für Endpunkte in Service-Mapping
Hostskripts suchen [sa_find_host_scripts]	Enthält die Namen von Skripteinbindungen, die basierend auf den Endpunkt-Glide-Datensätzen nach Hosts suchen
nfdump-Datei [sa_flcon_file_nfdump]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
nfdump-Installation [sa_flcon_local_nfdump]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
AWS VPC-Flow-Protokolle [sa_flcon_vpc_flow_log]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
SA-Flow-Verbindung [sa_flow_connection]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Flow-Connector [sa_flow_connector]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Flow-Serverkommunikation	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_flow_server_comm]	
IP/Port und Statistiken für Fluss-Services [sa_flow_service]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Host-Klasse zu Fähigkeit [sa_host_class_to_capability]	Ordnet den Servertyp den für Service-Mapping erforderlichen Fähigkeiten zu
Infrapfad zu Elementen [sa_infra_path_assoc]	Enthält Daten zu Komponenten, die Teil eines Netzwerkpfads sind
Externe Discovery-Befehle zuordnen [sa_mapping_ext_commands]	Enthält Daten über benutzerdefinierte Befehle, die vom Benutzer erstellt wurden
Netzwerkpfade [sa_network_paths]	Enthält Daten zu Netzwerkpfaden, die von Service-Mapping erkannt wurden.
Horizontale erkannte ausgelagerte Payloads [sa_paged_payload]	Service-Mapping verwendet die Daten in dieser Tabelle, um die von MID-Server gesendete Nutzlast zu teilen, wenn die Erkennung zu einer sehr großen Nutzlast führt.
Discovery-Muster [sa_pattern]	Enthält vorkonfigurierte und benutzerdefinierte Muster, die Service-Mapping für die Erkennung verwendet
Service-Mapping-Entwurfsmuster [sa_pattern_draft]	Enthält nicht aktivierte Erkennungsmuster
Service-Mapping-Beziehungsattribute [sa_rel_attr]	Enthält während des Service-Erkennungsprozesses verwendete Beziehungsattribute
Bez. zu Infrapfad [sa_rel_to_infra_path]	Ordnet Beziehungen Netzwerk- oder Speicherpfaden zu
Servicezuordnung für Servernutzung [sa_server_usage]	Enthält die Anzahl der von Service-Mapping verwendeten Server
Dateisystem zu Speicherpfad [sa_storage_paths]	Enthält Daten zu von Service-Mapping erkannten Speicherpfaden
Speicherpfad-Verbindungszuordnung [sa_storage_path_connectivity_map]	Ordnet das Dateisystem dem Speichervolume zu
Verkehrsbasierte Discoveryregeln	Enthält Daten über die Konfiguration der datenverkehrsbasierten Erkennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_traffic_based_rules]	
Hochgeladene Date [sa_uploaded_file]	Enthält Daten zu Dateien, die auf den MID-Server hochgeladen und von Service-Mapping verwendet werden
Configuration Item [cmdb_ci]	Speichert Daten über alle Konfigurationselemente (CIs) in CMDB
Applikation [cmdb_ci_appl]	Speichert Daten über alle Konfigurationselemente (CIs) vom Typ Anwendung in CMDB
IP-Service [cmdb_ip_service]	Speichert Daten zur Unterstützung der Erkennung ohne Anmeldeinformationen für die ursprüngliche Tabelle
Applikationskategorie [discovery_category_appl]	Speichert Daten über Anwendungskategorien, die vom Musterdesigner zur Verwaltung von Musterbibliotheken verwendet werden
Geräteklassifizierungskategorie [discovery_category_device_class]	Speichert Informationen über die Beziehung zwischen einem Geräteklassifizierer und einem Protokoll, das bei einer horizontalen Erkennung durch Discovery verwendet wird
Geräteinfokategorie [discovery_category_device_info]	Speichert Informationen über die Gerätekategorie, die bei einer horizontalen Erkennung durch Discovery verwendet wird
Protokollkategorie [discovery_category_protocol]	Speichert Informationen über die Protokollkategorie, die bei einer horizontalen Erkennung durch Discovery verwendet wird
HTTP-Klassifizierung [discovery_classy_http]	Speichert die HTTP-Klassifizierungsdefinition
Übereinstimmung der HTTP-Klassifizierung [discovery_classy_http_match]	Speichert die HTTP-Klassifizierungsbedingungen und die Informationen über das Muster, das bei Übereinstimmung mit der Klassifizierungsbedingung gestartet werden soll
Startprogramm für Discovery-Muster [discovery_pattern_launcher]	Speichert Informationen über den Musterstartmechanismus
Cloud-Ausführungsmuster [discovery_ptrn_cld_lchr]	Speichert Informationen über den Musterstartmechanismus für die Erkennung von Cloud-Anwendungen
Ausführungsmuster ohne Server [discovery_ptrn_hostless_lchr]	Speichert Informationen über den Musterstartmechanismus für die serverlose Erkennung
Parameter für Discovery-Muster	Speichert die Parameter für die serverlose/Cloud-Anwendungsausführung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[discovery_ptrn_lnch_param]	
Eingabeparameter für Muster [discovery_ptrn_lnch_param_def]	Speichert die nach Mustern gesammelten Schlüsselparameter
Applicative-Anmeldeinformationen [sa_applicative_credentials]	Speichert die Applicative-Anmeldeinformationen
Zugehörige CI-Typen [sa_ci_to_pattern]	Speichert zugehörige CIs in Mustern
Benutzerdefinierter Vorgang [sa_custom_operation]	Speichert Informationen über von Benutzern definierte Erkennungsmustervorgänge
Benutzerdefinierte Vorgangsparameter [sa_custom_operation_param]	Speichert benutzerdefinierte Vorgangsparameter für Erkennungsmuster
Benutzerdefinierte Analysestrategie [sa_custom_parsing_strategy]	Speichert Informationen über von Benutzern definierte Musteranalysestrategien
Debug-Sitzung [sa_debug_session]	Speichert Informationen aus Debug-Sitzungen
Status der Muster-Debugger-Sitzung für UI [sa_debug_session_status]	Speichert Informationen zum Status der Debug-Sitzung für UI-Zwecke
Sa zurückgestellte Service-Discovery [sa_deferred_service_discovery]	Enthält Informationen zum Starten der Debug-Sitzung von oben nach unten, wenn der relevante Host noch nicht erkannt wurde
Discovery-Protokoll [sa_discovery_log]	Das Protokoll mehrerer Erkennungsvorgänge
Hostskripts suchen [sa_find_host_scripts]	Enthält Skripts zum Suchen von Hosts in der CMDB basierend auf den Einstiegspunktinformationen
Host-Klasse zu Fähigkeit [sa_host_class_to_capability]	Enthält Informationen, die den Hosttyp zu MID-Server-Fähigkeiten zuordnen. Beispielsweise wird das Linux-Betriebssystem der SSH-WMI-Fähigkeit zugeordnet.
Zuordnung von Discovery-Befehlen [sa_mapping_ext_commands]	Enthält anpassbare Vorgänge für den Musterdesigner
Horizontale erkannte ausgelagerte Payloads	Enthält die Nutzlast der IE-Ausgabe, wenn der Teilungsmechanismus bereitgestellt wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_paged_payload]	
Discovery-Muster [sa_pattern]	Speichert veröffentlichte Muster
Servicezuordnungsentwurfsmuster [sa_pattern_draft]	Speichert die geänderte Version von Mustern
Mustererweiterungen [sa_pattern_extension]	Speichert Mustererweiterungsabschnitte
Muster des Vor-/Post-Skripts [sa_pattern_prepost_script]	Speichert Vor-/Nach-/Vor-Ausführungskripts für Muster
Snapshot von erkannten horizontalen Nutzlasten [sa_payload_snapshot]	Speichert die Nutzlast der IE-Ausgabe zum Löschen pro Haupt-CI
Nachverfolgte Datei – Definition [sa_tracked_file_definition]	Speichert die Definitionen der Funktion zur Dateinachverfolgung
Hochgeladene Date [sa_uploaded_file]	Speichert von der Muster-Engine verwendete Skripts und Dateien

Installierte Eigenschaften

Hinweis: ***Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter*** `sys_properties.list` ***ein.***

Eigenschaft	Beschreibung
sa.max_relations_in_service	Die maximale Anzahl von CI-Beziehungen für einen Service. Wenn der Wert überschritten wird, wird automatisch verhindert, dass einige Services in der Kartenansicht angezeigt werden. Sehr große Anwendungsservices können zu Leistungsproblemen führen. Anstelle von Karten können Benutzer für große Anwendungsservices CI-Listen anzeigen. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Grenzwert** : 10000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
best_practice.check_connectivity.expand_listening_port	Diese Eigenschaft steuert, welche PIDs Service-Mapping während des Hop-Vorgangs bei der Konnektivitätsprüfung prüft. Wenn diese Eigenschaft true ist, überprüft Service-Mapping die Konnektivität nur für PIDs, deren Ports sich im Status `listening` befinden, nicht jedoch, wenn der Status `connected` lautet. • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
com.snc.sw.mapping.reaper.checkpoints_to_keep	Die maximale Anzahl von Change-Markierungen, die in der Verlaufszeitleiste des Service beibehalten werden. Wenn Sie den Wert auf Null oder eine negative Ganzzahl festlegen, wird die Standardeinstellung überschrieben und alle Change-Markierungen für maximal drei Monate beibehalten. Die Verwendung der Eigenschaft „com.snc.SW.Mapping.Reaper.ignore_Services_from_Optimization“ ermöglicht den Ausschluss bestimmter Services und kehrt basierend auf Intervallen zum Entfernen von Change-Markierungen zurück. • **Typ**: Ganzzahl • **Standardwert**: 1.000
Com.snc.SW.Mapping.Reaper.ignore_Services_from_Optimization	Diese Eigenschaft enthält die durch Kommas getrennten Service-IDs. Anstelle der von der Eigenschaft „com.snc.sw.mapping.reaper.checkpoints_to_keep' angegebenen Anzahl behalten diese Services alle Change-Markierungen für maximal drei Monate bei. **Typ**: Ganzzahl
Com.snc.SW.Mapping.Reaper.max_Reap_size	Die maximale Anzahl von Change-Markierungen, die jedes Mal gelöscht werden, wenn das System alte und nicht verwendete Datensätze aus dem Verlauf der Changes am Service entfernt. Wenn Sie den Wert auf Null oder eine negative Ganzzahl festlegen, wird der Grenzwert überschrieben und alle unnötigen Change-Markierungen entfernt. • **Typ**: Ganzzahl • **Standardwert**: 100000
glide.service_mapping.computation_depth	Diese Eigenschaft steuert die maximale Tiefe der Serviceinstanz -Zuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 25 • **Andere mögliche Werte**: beliebige Zahl über 1 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa_ml.connection_suggestions.active	Aktivieren Sie die Funktion zum Generieren von Verbindungsvorschlägen, die auf der datenverkehrsbasierten Erkennung basiert. Service-Mapping generiert Verbindungsvorschläge anhand der von Predictive Intelligence analysierten Daten. Wenn diese Funktion aktiviert ist, können Sie Verbindungsvorschläge zum Verwalten von CI-Verbindungen in Anwendungsservices verwenden. • **Typ**: Boolesch • **Standardwert**: true **Hinweis:** Wenn die datenverkehrsbasierte Erkennung in Ihrer Bereitstellung vor Release Quebec aktiviert war und Sie diese Funktion verwendet haben, um mindestens einen Anwendungsservice zu erkennen, ist der Wert standardmäßig auf `false` festgelegt. • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.debugger.max_timeout	Maximale Zeitüberschreitung (in Sekunden) seit der letzten Serveraktivität während einer Ausführung des Muster-Debuggers • **Typ**: Ganzzahl • **Standardwert**: 120 • **Andere mögliche Werte**: beliebige Zahl über 60 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an. Weitere Informationen finden Sie unter KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung .
sa.discovery_task_timeout_min	Maximale Zeit für eine Service-Mapping-Aufgabe in Minuten (einschließlich Warten auf Ausführung in internen Warteschlangen und ECC-Warteschlange)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Zeichenfolge • **Standardwert**: 120 • **Andere mögliche Werte**: beliebige Zahl über 30 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.enable_gray_out_on_resume_discovery	Hiermit wird die Unterstruktur ausgegraut, nachdem Service-Mapping die Erkennung am Edge wieder aufgenommen hat, oder die Erkennung wird für die gesamte Topologie erneut ausgeführt. • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.excluded_Discovery_sources	Fügen Sie diese Eigenschaft hinzu, um Discovery-Quellen während der Host-Erkennung auszuschließen. • **Standardwert** : Eventmanagement • **Andere mögliche Werte** : Zusätzliche Discovery-Quellen, die nach Eventmanagement hinzugefügt werden, durch Komma getrennt
sa.map.enable_loops_on_service_split	Ermöglicht es Ihnen, einen Serviceinstanz mit einem anderen, bereits vorhandenen Serviceinstanz zu verbinden, auch wenn die CI-Verbindung (Endpunkt), die Sie herstellen, Teil dieses anderen Serviceinstanz ist. Diese Eigenschaft trägt dazu bei, Schleifen oder Zyklen in Servicezuordnungen zu vermeiden. • **Typ**: Boolesch • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa_ml.connection_suggestions.lb.routing.enabled	Status, wenn ein Zielhost ein Mitglied des Lastenausgleichsmoduls ist oder nicht in der Liste „Verbindungsvorschlagen“ ist. • **Typ**: true/false • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties].
sa.network_path_calculation.arp_enableadded pro Dokument 1074513 in Vancouver	Steuert Abfragen für die ARP-Tabelle. Daten werden nur berechnet, wenn der Wert auf „wahr“ festgelegt ist. **Hinweis:** Weitere Informationen zum Abfragen der ARP-Tabelle finden Sie unter ARP-Eigenschaftsdokumentation für Service-Mapping [KB1311037] artikel in der Now Support Knowledge Base. • **Typ**: true/false • **Standardwert**: false • **Weitere mögliche Werte**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.network_path_calculation.active	Aktiviert die Netzwerkpfadberechnung • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa.rediscovery.batch_size	Anzahl der in einem einzigen Stapel ausgeführten Erkennungsaufgaben • **Typ**: Ganzzahl • **Standardwert**: 100 • **Andere mögliche Werte**: beliebige Zahl über 10 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa.service_history.max_allowed_bubbles	Anzahl der Änderungen, die auf der Verlaufsskala und der Registerkarte „Changes“ angezeigt werden • **Typ**: Ganzzahl • **Standardwert**: 3000 • **Andere mögliche Werte**: beliebige Zahl über 3000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Wichtig: Das Erhöhen des Werts für diese Eigenschaft kann zu Leistungsprobleme beim Laden von Zuordnungen des Serviceinstanz führen. • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa.service.max_ci_service_population	Die maximale Anzahl von CI-Verbindungen, die Anwendungsservices während der folgenden Vorgänge hinzugefügt werden: Manuelle Services, die in erstellt wurden, werden konvertiert Ereignismanagement In Anwendungsservices mit Änderungen von CMDB. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Grenzwert** : 2000 • **Standort** : Zu Systemeigenschaften hinzufügen [sys_properties] Tabelle. Das Erhöhen des Standardwerts kann zu Leistungsproblemen führen.
sa.storage_path_calculation.active	Aktiviert die Speicherpfadberechnung • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa.Topdown.Mapping_with_ACC_Mode	Diese Eigenschaft aktiviert die Top Down-Discovery und die Servicezuordnung mit Agent Client Collector Durch Definieren von MID-Server Auswahlmodus für Discovery von oben nach unten. • **Typ:** Ganzzahl • **Standardwert:** 0 • **Andere mögliche Werte:** 1,2 0: Discovery von oben nach unten wird mit ausgeführt MID-Server Ausschließlich. 1: Die Top Down-Discovery versucht anfänglich, mit auszuführen Agent Client Collector. Wenn kein Service Desk-Mitarbeiter verfügbar ist, wird standardmäßig verwendet MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	2: Discovery von oben nach unten wird mit ausgeführt Agent Client Collector Ausschließlich. Wenn nicht erfolgreich, wird der Prozess beendet.
sa.traffic_based_discovery.active	Datenverkehrsbasierte Erkennung • **Typ**: true/false • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an. **Hinweis:** Diese Eigenschaft gilt nur für veraltete Traffic-basierte Verbindungen. Wenn Verbindungsvorschläge für maschinelles Lernen (ML) aktiviert sind, stellen Sie sicher, dass der Eigenschaftswert auf festgelegt bleibt Falsch .
sa.traffic_based_discovery.conn_aging_time	Zeitraum in Stunden, für den eine datenverkehrsbasierte Verbindung seit der letzten Erkennung aktiv bleibt • **Typ**: Ganzzahl • **Standardwert**: 72 • **Andere mögliche Werte**: beliebige Zahl über 24 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sa.traffic_based_discovery.ignored_ports	Bei einer datenverkehrsbasierten Erkennung gefundene Ports, die ignoriert werden können. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Ändern Sie diese Eigenschaft, um Ports zu definieren, die Service-Mapping bei der datenverkehrsbasierten Erkennung ignoriert. Dadurch wird die Erkennung effizienter, da keine Ressourcen für die Erkennung irrelevanter Verbindungen verschwendet werden. • **Typ**: Zeichenfolge • **Standardwert**: 445, 139, 111, 2049, 860, 3260, 135, 53

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Andere mögliche Werte**: alle relevanten Portnummern • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.traffic_based_discovery.max_connections	Maximale Anzahl datenverkehrsbasierter Verbindungen von einem einzelnen CI. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Diese Eigenschaft trägt dazu bei, die Größe der Zuordnung angemessen zu halten, indem die Anzahl der möglichen CI-Verbindungen begrenzt wird. • **Typ**: Ganzzahl • **Standardwert**: 30 • **Andere mögliche Werte**: beliebige Zahl über 1 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.update_paths_in_service_model.active	Aktualisiert Netzwerk- und Speicherpfade im Servicemodell • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
service_watch.implied_match.endpoint.black_list	Eine Liste von Endpunkttypen, auf die Service-Mapping während der Musterausführung von oben nach unten keine Prozessabgleichlogik anwendet • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_endpoint_ssis_mssql, cmdb_ci_endpoint_ssas_mssql • **Andere mögliche Werte**: kommagetrennte Liste von Endpunkten • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.blacklist	Schließt die genannten Felder aus dem Datensatz in der Exportdatei der Servicedefinition aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.blacklist.cmdb_ci_endpoint	Schließt die genannten Felder aus dem Einstiegspunkt-Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.blacklist.cmdb_ci_service_discovered	Schließt die genannten Felder aus dem Anwendungsservice-Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Zeichenfolge • **Standardwert**: discovery_status,operational_status,process_status,work_ • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.blacklist.cmdb_ci_service_group	Schließt die genannten Felder aus dem Servicegruppen-Datensatz in der Exportdatei der Servicedefinition aus Trennen Sie die einzelnen Felder mit Kommas. • **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.max_services_limit	Definiert die maximal zulässige Anzahl von zu exportierenden Services

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 100 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.skip_empty_fields	Schließt Felder mit einem leeren Wert aus dem Datensatz in der Exportdatei der Servicedefinitionen aus. • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.skip_reference_fields	Schließt Referenzfelder aus dem Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.export.skip_sys_fields	Schließt Felder, die mit „sys_“ beginnen, aus dem Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sm.service.import.auto_start_discovery	Aktiviert die automatische Erkennung aller erfolgreich importierten Einstiegspunkte • **Typ**: Boolesch • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**an.
sn_cloud_migration.categories.inclusion_list	Kommagetrennte Allow-Liste von Kategorien für die Cloud-Migration. Am Migrationsprozess können nur Ressourcen teilnehmen, die hier aufgelisteten Kategorien zugewiesen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Zeichenfolge • **Standardwert**: Physisch, VMware, HyperV, IBM HMC, OpenStack, Solaris, Nutanix, Amazon AWS, Microsoft Azure, Google Cloud, IBM Cloud • **Standort**: **Cloud-Migration** > **Arbeitsbereich Für Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.server_status.inclusion_list	Kommagetrennte Allow-Liste des Serverstatus für die Cloud-Migration. Am Migrationsprozess können nur Server mit einem hier aufgeführten Installationsstatus teilnehmen. • **Typ**: ? • **Standardwert**: 1 • **Anderer möglicher Wert**: Installiert = 1, Bestellt = 2, In Wartung = 3, Ausstehende Installation = 4, Ausstehende Reparatur = 5, Auf Lager = 6, Stillgelegt = 7, Gestohlen = 8, Abwesend = 100 • **Standort**: **Cloud-Migration** > **Arbeitsbereich Für Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.os.exclusion_list	Kommagetrennte Deny-Liste von Betriebssystemen für die Cloud-Migration. Server, deren Betriebssystem hier aufgeführt ist, werden vom Migrationsprozess ausgeschlossen. • **Typ**: Zeichenfolge • **Standardwert**: ESX, Windows 2000, Windows XP. • **Standort**: **Cloud-Migration** > **Arbeitsbereich Für Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.vm_state.inclusion_list	Kommagetrennte Allow-Liste von VM-Instanzstatus für die Cloud-Migration. Am Migrationsprozess können nur VMs mit einem hier aufgeführten Status teilnehmen. • **Typ**: ?? • **Standardwert**: Ein • **Andere mögliche Werte**: Ein, Aus, Angehalten, Geplant, Wird gestartet, Wird gestoppt, Stillgelegt, Beendet, Fehler,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Abgebrochen, Wird angehalten, Wird beendet • **Standort**: **Cloud-Migration** > **Arbeitsbereich Für Cloud-Migration** > **Administration** > **Eigenschaften**
	Die Anzahl der CI-Beziehungen, nach deren Überschreiten Anwendungsservices nicht automatisch in der Zuordnungsansicht angezeigt werden. Sehr große Anwendungsservices können zu Leistungsproblemen führen. Anstelle von Karten können Benutzer für große Anwendungsservices CI-Listen anzeigen. Durch das Festlegen eines negativen Werts wird die Anzahl der hinzugefügten CI-Beziehungen nicht eingeschränkt. Wenn ein ungültiger Wert wie eine Zeichenfolge festgelegt wird, entspricht dies dem Standardwert 5000. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_Tags.classes.Whitelist	Diese Eigenschaft enthält die Liste der zulässigen CI-Klassen, die durch Kommas getrennt sind. Die Tag-basierte Zuordnung enthält die CIs, die zu diesen Klassen gehören. Ein leeres Feld „Wert“ gibt die Einbeziehung aller CI-Klassen an.
svc_by_tags.install_status.blacklist	Diese Eigenschaft enthält die Liste der Ausschlüsse basierend auf dem Installationsstatus, getrennt durch Kommas. Die Tag-basierte Zuordnung schließt alle getaggten CIs mit den folgenden Installationsstatus aus: **Standardwert** : 7.100 **Andere mögliche Werte**: Installiert=1, bestellt=2, in Wartung=3, ausstehende Installation=4, ausstehende Reparatur=5, auf Lager = 6, stillgelegt = 7, gestohlen = 8
svc_by_tags.max.categories.per.family	Legen Sie die maximale Anzahl von Kategorien fest, die pro Servicefamilie zulässig sind. • **Typ**: Ganzzahl • **Standardwert**: 3
svc_by_tags.max.traversal.rules.active	Legen Sie die maximal zulässige Anzahl von CI-Beziehungen fest, die sich im aktiven Status befinden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	können. Service-Mapping verwendet für die Tag-basierte Erkennung nur aktive CI-Beziehungen. • **Typ**: Ganzzahl • **Standardwert**: 5 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_tags.max_ci_limit	Legen Sie die maximal zulässige Anzahl von CIs fest, die ein auf Tags basierender Anwendungsservice enthalten kann. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Grenzwert** : 2000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sm.Topdown.Reuse_Mid_from_hd_schedule	Verwenden Sie MID-Server Während der horizontalen Discovery für die Top Down-Discovery konfiguriert. • **Typ:** boolescher wert • **Standardwert:** false • **Andere mögliche Werte:** Wahr • **Standort: Service-Mapping** > **Administration** > **Eigenschaften**
sm.network_location.detect_host_by_location	Wählen Sie den Subnetzwerkstandort aus, um die Identifizierung des entsprechenden Hosts und zu ermöglichen MID-Server. **Wichtig:** Um die besten Ergebnisse zu erzielen, müssen Sie diese Eigenschaft und sm.topdown.reuse_Mid_from_hd_schedule gleichzeitig aktivieren. • **Typ:** boolescher wert • **Standardwert:** false • **Andere mögliche Werte:** Wahr • **Standort: Service-Mapping** > **Administration** > **Eigenschaften**

Domain Separation und Service-Mapping

Die Domänentrennung wird in Service-Mapping unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Service-Mapping

Wechseln Sie in Umgebungen mit Domänentrennung zu relevanten Blattdomänen, um auf Aktionen im Zusammenhang mit der Zuordnung durch Service-Mapping zuzugreifen. Ein Endknoten ist eine untergeordnete Domäne der untersten Ebene, d. h. sie verfügt selbst nicht über untergeordnete Domänen.

Die Domänentrennung wird etwas anders gehandhabt als die einfache Konfiguration separater Domänen. Beachten Sie, dass Sie die entsprechende Blattdomäne auswählen oder angeben müssen, um in Umgebungen mit Domänentrennung die folgenden Zuordnungsaktionen durchzuführen:

- Beim Erstellen eines Serviceinstanz wird der Serviceinstanz der Domäne des Benutzers zugewiesen.
- Beim manuellen Hinzufügen eines CI zu einem Serviceinstanz können Sie nur CIs auswählen, die zu der Servicedomäne gehören.
- Beim manuellen Hinzufügen von Verbindungen zu CIs zu Serviceinstanz müssen Benutzer derselben Domäne angehören wie der Anwendungsservice.
- Beim Übertragen von Servicedefinitionen zwischen Instanzen werden importierte Serviceinstanzen und Servicegruppen der Domäne des Anwenders zugewiesen.

Domain Separation und Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services unterstützt Domänentrennung. Dies bedeutet:

- Der Quell- und Zielprozess müssen sich in derselben Domäne befinden, um eine Verbindung zu erstellen.
- Der Anwender kann nur die Daten in der aktuellen Domäne anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Nach der Installation Service-Mapping Plus Mit Unterstützung der Domänentrennung überprüfen Sie, ob sich der gesamte Inhalt in der entsprechenden Domäne befindet. Eine detaillierte Erklärung der erforderlichen Schritte finden Sie unter Servicezuordnung plus für domänengetrennte Instanz [KB1303398] artikel in der Now Support Knowledge Base.

Empfehlungen für automatisierte Services Unterstützt Domänentrennung ab Version 1,9.0. Für lokale Instanzen wird derzeit kein Support angeboten. Wenden Sie sich an das Produktmanagement, um weitere Informationen zu erhalten.

Weitere Informationen zu diesem Kontext finden Sie unter Von ITOM-Transparenz verwendete Erkennungsmuster Thema und Konfiguration des MID Servers für Service-Mapping. Die folgenden Themen enthalten operative Informationen zur Verwendung von Service-Mapping in Bereitstellungen mit Domänentrennung:

- Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren
- Ordnen Sie Anwendungsservices mithilfe von Tags mit zu klassisch Service-Mapping
- Muster erstellen oder anpassen
- Einstiegspunkttypen für Service-Mapping erstellen
- Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern

Zugehörige Informationen

Domänentrennung

Empfohlene Domain Separation-Verfahren für Service Provider

Neuberechnung Des Service-Mapping

Halten Sie Anwendungsservices auf dem neuesten Stand, und verfolgen Sie Änderungen an Services mithilfe der Neuberechnungsfunktion der Anwendungsservice-Funktion von Service-Mapping. Neuberechnungsaufträge berechnen zugeordnete Anwendungsservices neu, wenn Änderungen an einem zugeordneten Konfigurationselement (CI) in der Configuration Management Database (CMDB) auftreten.

Die häufigsten Änderungen, die eine Neuberechnung verursachen können, sind:

- Topologieänderungen: Die Beziehung des zugeordneten CI zu anderen CIs ändert sich. Diese Änderungen können das Hinzufügen einer neuen Beziehung oder das Entfernen einer vorherigen umfassen.
- CI-Changes: Ein Feldwert der CI-Changes.

Diese Änderungen können durch horizontale Discovery, Top Down-Discovery, Service Graph Connectors oder manuelle Vorgänge verursacht werden. Wenn sich der CI-Change nicht auf die Topologie oder Servicezuordnungen auswirkt, wird der Neuberechnungsprozess ohne Änderungen am Service beendet.

Im Systemplaner sind zwei Arten von Neuberechnungsaufträgen verfügbar: Service-Mapping Neuberechnung und Service-Mapping Schnelle Neuberechnung. Bei der schnellen Neuberechnung werden Services mit nur CI-Changes als Teil des neuesten Batches ausgewählt und Topologieänderungen nicht berücksichtigt.

Neuberechnungsaufträge sind so konfiguriert, dass sie alle fünf Sekunden ausgeführt werden. Nachdem die Aufträge initiiert wurden, beginnen sie mit dem Service, der am längsten gewartet hat. Wenn der Auftrag abgeschlossen ist, können sich die Auswirkungen von Topologieänderungen in der Topologie der Karte oder einer Änderung in den Servicezuordnungen widerspiegeln. Sie können CI-Änderungen anzeigen, indem Sie den Zuordnungsknoten des CI auswählen. Erfolgreiche Neuberechnungen werden als einzelner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfpunkt auf der Zeitleiste des Anwendungsservice angezeigt, unabhängig davon, ob es sich um eine Änderung oder einen Batch von Changes handelt.

Sie können den Neuberechnungstyp, die Häufigkeit und andere Faktoren nach Bedarf konfigurieren. Weitere Informationen zu finden Service-Mapping, Siehe Service-Mapping-Neuberechnungsaufträge: Konfiguration und Best Practices [KB1001151] artikel in der Now Support Knowledge Base.

Liste „Verbindungsvorschlagen“

Überprüfen Sie die Details der Verbindungsvorschläge, um zu entscheiden, welche Verbindungen für Anwendungsservices relevant sind.

Spalten der Liste „Verbindungsvorschlagen“

Spalte	Beschreibung
Von	Die CI-Klasse oder der Fingerabdruckprozess des CI, das die Verbindungsquelle ist. Dieses Feld wird nur angezeigt, wenn Sie durch Navigieren zu auf Verbindungsvorschläge zugreifen **Service-Mapping** > **Administration** > **Verbindungsvorschläge**an.
An	Die CI-Klasse oder der Fingerabdruckprozess des CI, das das Verbindungsziel ist
Zielhost	Der Host des CI, das das Verbindungsziel ist Wenn in der Spalte **VIP** der Wert **true** angezeigt wird, ist der Zielhost Mitglied eines Lastenausgleichsmoduls. Wenn Sie einen solchen Zielhost auswählen, fügt das System das Lastenausgleichsmodul und alle zugehörigen Mitglieder als CIs im Anwendungsservice hinzu.
IP	Die IP-Adresse des CI, das das Verbindungsziel ist
Port	Der Port des CI, das das Verbindungsziel ist
Vertrauen	Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist. • **Hoch** – Diese Verbindung bezieht sich wahrscheinlich auf eine interne Komponente, die nur von dieser bestimmten Komponente oder Anwendung verwendet wird. • **Mittel** – Diese Verbindung bezieht sich wahrscheinlich auf eine Middleware-Komponente, die von mehreren Services verwendet wird, z. B. IBM MQ oder Oracle WebLogic-Server. • **Niedrig** – Diese Verbindung wird wahrscheinlich mit einer Anwendung verbunden, die auf zahlreichen Servern in der Organisation bereitgestellt wird,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalten der Liste „Verbindungsvorschlagen“ (Fortsetzung)

Spalte	Beschreibung
	normalerweise zu Überwachungszwecken, z. B. Tivoli Enterprise Monitoring Agents oder MID-Server. • **Sehr niedrig** – Diese Verbindung bezieht sich wahrscheinlich auf eine zentrale Anwendung, die von der gesamten Organisation verwendet wird, z. B. Microsoft Active Directory Oder Okta. Wenn das Konfidenzniveau als **N/V** angezeigt wird, warten Sie, bis das Training der Anwendungsfingerabdrücke abgeschlossen ist. Siehe Statusbericht zum Training von Anwendungsfingerabdrücken . Das Konfidenzniveau ist nur verfügbar, wenn die auf Fingerabdrücken basierende Discovery aktiviert ist. Weitere Informationen finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.
Entscheidung	Dieser Wert gibt das Ergebnis der vorherigen Aktion an, die für diesen Verbindungsvorschlag ausgeführt wurde: • **Manuell hinzugefügt** – Sie haben eine Verbindung basierend auf diesem Vorschlag hinzugefügt. • **Manuell ausgeschlossen** – Sie haben eine Verbindung basierend auf diesem Vorschlag entfernt. • **Unentschieden** – Sie setzen die vorherige Entscheidung zurück, eine Verbindung basierend auf diesem Vorschlag hinzuzufügen oder zu entfernen. • **Durch Regel hinzugefügt** – Service-Mapping hat eine Verbindung auf Grundlage einer Verbindungsregel hinzugefügt.
Regel	Die Regel, die von Service-Mapping zum Hinzufügen einer Verbindung angewendet wurde.
VIP	Der Zielhost ist Mitglied eines Lastenausgleichsmoduls. Das System zeigt diese Informationen nur für Lastenausgleichsmodule an, die Sie zuvor mithilfe der horizontalen Erkennung erkannt haben. Dieses Feld wird nur angezeigt, wenn Sie durch Navigieren zu auf Verbindungsvorschläge zugreifen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalten der Liste „Verbindungsvorschlagen“ (Fortsetzung)

Spalte	Beschreibung
	Service-Mapping > **Administration** > **Verbindungsvorschläge**an.
Entscheidung geändert von	Der Benutzer, der die Entscheidung zuletzt geändert hat. Wenn die Entscheidung durch eine Regel geändert wurde, wird in diesem Feld angezeigt MID-Server Anwender. Weitere Informationen zum Einrichten von finden Sie MID-Server Anwenderrolle, siehe MID-Server-Benutzer erstellen und die Rolle erteilen . Dieses Feld wird nur angezeigt, wenn Sie durch Navigieren zu auf Verbindungsvorschläge zugreifen **Service-Mapping** > **Administration** > **Verbindungsvorschläge**an.
Aktualisiert	Der Zeitstempel der letzten Änderung dieser Verbindung

Zugehörige Informationen

Erkennung auf Basis von Predictive Intelligence

CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Einstiegspunktattribute

Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken. Überprüfen Sie die Attributdefinitionen, damit die Einstiegspunkte Ihren Anwendungsservices korrekt hinzugefügt werden.

Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Einstiegspunkte werden als Datensätze in den Tabellen „Endpunkt“ [cmdb_ci_Endpoint] gespeichert.

Es gibt einige allgemeine Attribute, die von fast allen Einstiegspunkttypen gemeinsam verwendet werden, wie in der folgenden Tabelle beschrieben:

Allgemeine Attribute

Attribut	Beschreibung
Host/Hostname/Host Name	Der Wert des Zielservers, auf dem der Dienst ausgeführt wird. Dieser Wert kann einen echten Hostnamen, einen Aliasnamen, eine IP-Adresse oder eine VIP-Adresse enthalten. **Wichtig:** Verwenden Sie für die Discovery und Zuordnung keine localhost- oder loopback-Adresse (127.0.0.1).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Attribute (Fortsetzung)

Attribut	Beschreibung
Port	Die Portnummer des Dienstes, den Sie ermitteln möchten.
Name	Der Name des Dienstes, den Sie entdecken möchten.
URL	Die URL des Service, den Sie erkennen möchten, im folgenden Format: http(s)://(Adresse):(Port). Wenn Sie den Port nicht angeben, verwendet das System den Standardport 443.
Netzwerkstandort	Standort des entsprechenden Subnetzwerks. **Hinweis:** Dieses Feld ist optional und nur sichtbar, wenn der Netzwerkstandort aktiviert ist.

Informationen zum Konfigurieren von Einstiegspunkten für Subnetze finden Sie unter Feinabstimmung Service-Mapping Mit MID-Affinität und IP-Wiederverwendung.

Es gibt einige Attribute, die Sie je nach Einstiegspunkt unterschiedlich konfigurieren, wie in der folgenden Tabelle beschrieben:

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind

Einstiegspunkttyp	Attribut	Beschreibung
Active Directory-Domäne zu Domänencontroller-Endpunkt	Domänenname	Der AD-Domänenname
	Forest-Name	Der Name des Active Directory Forest (AD Forest)
	Domänencontroller – Distinguished Name	Der Distinguished Name des AD-Domänencontrollers. Normalerweise handelt es sich um eine Kompilierung des Domänencontroller- und des Hostnamens.
	Domänencontroller-Name	Der Name des AD-Domänencontrollers
Active Directory-Gesamtstruktur – Endpunkt	Forest-Name	Der Name des Active Directory Forest (AD Forest)
AWS-Ressourcenamensendpunkt	ARN	Der Name der Amazon-Ressource
Anwendung zu Speicherendpunkt	Durch Applikation verwendete Datei	Der Pfad zu der von einer Anwendung verwendeten Datei Beispiel: mssql verwendet c:\applications\mssql\users.db. Service-Mapping füllt dieses Attribut anhand von Mustern auf.
	Dateisystemname	Das Dateisystem, das die von einer Anwendung verwendete Datei enthält. Wenn mssql beispielsweise c:\applications\mssql\users.db verwendet, ist der Wert „c:“.
	Angeschlossene Array-IDs	N/V

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
Erweiterte Warteschlange	Schema	Der Name der Oracle DB-Tabelle, in der die Warteschlange definiert ist
	Instanz	Der Name der Oracle-Instanz
	Warteschlange	Der Name der Warteschlange
BizTalk-Verbindung	Adapteradresse	Die Verbindungszeichenfolge für den Biztalk-Adapter. Dies kann ein Pfad, eine URL, ein Host oder ein Port sein.
	Transporttyp	Der Typ des Biztalk-Adapters. Beispielsweise eine URL, Datei-SOAP oder FTP.
CRM-Komponente	Rolle	Die Rolle des CRM. Lassen Sie das Feld leer, wenn diese unbekannt ist.
DB2 UDB	Instanz	Der Name der DB2-Instanz
DCTM-Verbindung zu Broker	Repository	Der Name des Dokumentations-Repository
DCTM-Index-Agent-Verbindung	Instanzname	Der Name der Instanz des Dokumentationsindex-Agent
	Repository	Der Name des Dokumentations-Repository
DCTM-Jobprozessor	Repository	Der Name des Dokumentations-Repository
Citrix Delivery Controller	Farm-Typ	Der Typ des Delivery-Controllers
	Controller-Name	Der Name des Citrix-Controllers
DocBase-Verbindung	Repository	Der Name des Dokumentations-Repository
EJB	JNDI-Name	Der jndi-Name der Ziel-EJB
EMS	Warteschlange	Name der Tibco EMS-Warteschlange
EMS JNDI	JNDI-Name	Der jndi-Name der Tibco EMS-Verbindung
F5-Spiegel	Ursprüngliche IP	Die IP-Adresse des zweiten F5-Gerätepaars
	Ursprünglicher Host	Der Hostname des zweiten F5-Gerätepaars
Schnellsuche	Repository	Der Name des Repository für die schnelle Suche
ITAM Asset Center	Ordner	Der Pfad zum Konfigurationsordner
JMS-Fluss	JMS-Projekt	Der Name des Tibco-Projekts
JMS-Fluss	Abfragename	Name der Tibco EMS-Warteschlange
JMS-Server	Abfragename	Der Name der auf dem JMS-Server definierten Warteschlange
HTTP-Listener für WMB-Abhängigkeit	Verzeichnis	Der Pfad zum WMB-Installationsverzeichnis
LDAP	Protokoll	Der Protokollname: `ldap`
	Typ	Der LDAP-Abfragetyp. Dieses Attribut wird nicht unterstützt. Leer lassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
MQ	Abfragename	Der Name der IBM MQ-Warteschlange.
MQ-Fluss	Quelle-IP	Die IP der Quell-IP, die eine Verbindung mit MQ herstellt
	Abfragename	Der Name der IBM MQ-Warteschlange.
MQ Cross-memory	Befehlszeile	Die Befehlszeile von MQ
	Abfragename	Der Name der IBM MQ-Warteschlange.
MSMQ Flow	Abfragename	Der Name der MS MQ-Warteschlange.
MS SQL-Server	Instanz	Der Name der MSSQL-Instanz
MySQL Cluster-Datenknoten	Knoten-ID	Die ID der MySQL-Instanz
	Knotengruppe	Die Gruppe der MySQL-Instanz
MySQL Cluster-MGM	Knoten-ID	Die ID der MySQL-Instanz
Sekundärer MySQL-Server	Konfig.-IP	Die IP des MySQL-Konfigurationsservers
	Konfig.-Port	Der Port des MySQL-Konfigurationsservers
Oracle-DB	Schema	Der Name der Tabelle auf der Oracle-Instanz
	Instanz	Der Name der Oracle-Instanz
Oracle ESB-Verbindung	Adapterdaten	Der Inhalt des Adapters
	Adaptertyp	Der Typ des Adapters
Oracle RAC-DB	Servicename	Der Name des Oracle RAC-Services
PostgreSQL-DB	Instanz	Der Name der PostgreSQL-Datenbank
Remote-TCP Cross-Speicher	Source_ IP	Die IP des Quellhostprozesses
	Quell-Port	Der Port des Quellprozesses
SAP APP-EP	SID	Der SID-Name der SAP-Instanz
	Instanz	Der Name der Instanz.
SAP BO-Server	Servername	Der Name des BO-Servers
Sharepoint-Verbindung	Ursprungs-URL	Die URL des IIS
SSAS	Projekt	Der Name des SSAS-Projekts (kann leer sein)
SSAS für MSSQL	Instanz	Der Name der MSSQL-Instanz
	Clienttyp	Der Typ des verbundenen Clients
SSIS	Auftrag	Der Name des SSIS-Auftrags kann leer sein.
SSIS-Datei	Paketdateiname	Der Name der Paketdatei
SSIS für MSSQL	Instanz	Der Name der MSSQL-Instanz
	Clienttyp	Der Typ des verbundenen Clients
StoreParameters-Komponenten	Front	Die Parameter der Citrix-Anwendung
	Farm	Der Farm-Host für die Citrix-Anwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
	Anwendungsname	Der Name der Citrix-Anwendung
XenApp- oder Präsentationsserver	Typ	Der Type der Citrix-Anwendung
	Farm	Der Farm-Host für die Citrix-Anwendung
	Symbol-Pfad	Der logische Pfad der Citrix-Anwendung
	Argument	Die Parameter der Citrix-Anwendung
	Pfad	Der logische Pfad der Citrix-Anwendung
	Ausführung	Der EXE-Name der Citrix-Anwendung
	IP-Adresse	Die IP des Hosts gehört zur Citrix-Farm.
Sybase	Instanz	Der Name der Sybase-Instanz
Tibco Konf.-Datei	Konfigurationsdatei	Der Pfad zum Tibco BW-Projekt
	Prozessname	Der Name des Tibco BW-Hauptprozesses
	Warteschlangenport	Der Port der vom Tibco-Prozess verwendeten Warteschlange
	Konfig.-IP	Die IP der Quelle der Warteschlange
Tibco BW	Prozessname	Der Name des Tibco BW-Hauptprozesses
TIBCO Datei-Listener	Datei	Der Pfad der Datei wird von Tibco BW für die Integration verwendet.
TIBCO Hawk	Konfigurationsverzeichnis	Der Pfad zum Tibco Hawk-Konfigurationsordner
WMB-Abhängigkeit	Befehlszeile	Die Befehlszeile von WMB
XenApp- oder Presentation Server-Komponenten	Farm	Der Farm-Host für die Citrix-Anwendung
	Symbol-Pfad	Der logische Pfad der Citrix-Anwendung

Zugehörige Informationen

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

Einstiegspunkttypen für Service-Mapping erstellen

MID-Server-Eigenschaften, die von Service-Mapping verwendet werden

Service-Mapping verwendet die MID-Server-Parameter während der Erkennung und Zuordnung. Ändern Sie keine Standardwerte für diese Parameter, es sei denn, Sie beheben Probleme im Erkennungsprozess.

Allgemeine Eigenschaften

Eigenschaft	Beschreibung
mid.file_tracking.file_path_forbidden_strings	Kommagetrennte Liste von Zeichenfolgen, nach denen in nachverfolgten Dateipfaden gesucht werden soll. Sobald eine Zeichenfolge in dieser Liste in einem nachverfolgten Dateipfad gefunden wurde, wird die Datei aus der weiteren Verarbeitung entfernt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Standardwert**: mit Status ERROR abgeschlossener Auftrag • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .

SSH-bezogene Eigenschaften

Eigenschaft	Beschreibung
mid.sa.ssh.path	Verzeichnis im Zielsystem, in dem MID-Server nach auszuführenden Befehlen sucht. • **Standardwert**: /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.truncate_last_line_regex	Regulärer Ausdruck einer Zeile, den MID-Server am Ende der SSH-Befehlsantwort entfernt. • **Standardwert**: Command.*performed by.* • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.remove_first_line_regex	Regulärer Ausdruck einer Zeile, den MID-Server am Anfang jeder SSH-Befehlsantwort entfernt. • **Standardwert** : [Leere Zeichenfolge] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.privileged_command_message	Eingabeaufforderung, die MID-Server mit Befehlen mit Rechten auf Sudo-Ebene sendet. Beispiel: Ein Befehl auf Sudo-Ebene wird mit „Password:“ gesendet. • **Standardwert** : [Leere Zeichenfolge] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.restricted_shell_regex	Regulärer Ausdruckstext, der beim Öffnen der Nachricht einer eingeschränkten Shell enthalten ist. Mit einer eingeschränkten Shell führt der SSH-Provider während der Sitzungsinitialisierung einige Befehle nicht aus. • **Standardwert**: eingeschränkte Shell • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.terminal_cols	Anzahl der Spalten in den Terminalfenstern, die mit der SSH-Sitzung geöffnet werden. • **Standardwert**: 300 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.terminal_rows	Anzahl der Zeilen in den Terminalfenstern, die mit der SSH-Sitzung geöffnet werden. • **Standardwert**: 800 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.time_between_change_shell_and_prompt	Wartezeit zwischen dem Ändern einer Shell während der Initialisierung und dem Zeitpunkt, zu dem die Shell-Eingabeaufforderung angezeigt wird (in Millisekunden). • **Standardwert**: 1.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.connect_timeout	Zeitüberschreitung für die anfängliche SSH-Verbindung (in Millisekunden). • **Standardwert**: 2.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.max_chars_single_response	Maximale Anzahl von Zeichen, die in einer einzelnen SSH-Befehlsantwort zulässig sind. • **Standardwert**: 1.0000.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.break_session_chars	ASCII-Wert des Zeichens, das zum Unterbrechen einer Sitzung verwendet wird. • **Standardwert**: 7 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.no_change_shell_regex	Regulärer Textausdruck in der Befehlsantwort nach dem Senden von „su“, um zum Superuser zu wechseln. Wenn der reguläre Ausdruck übereinstimmt, ändert MID-Server die Shell nicht. • **Standardwert**: pfsh • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.permission_denied_regex	Regulärer Ausdruck von Befehlsantworten, die der MID-Server als Zugriffsproblem erkennt und eine entsprechende Meldung generiert. • **Standardwert**: Berechtigung verweigert • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.more_line_command_regex	Wenn die SSH-Antwort die Terminalgröße überschreitet, sendet das System die Zeile „more“, die dem regulären Ausdruck entspricht. Wenn der MID Server die Zeile „more“ erkennt, sendet er das Leerzeichen. Dies ist relevant für proprietäre Systeme, die eine nicht standardmäßige Eingabeaufforderung „more“ senden. • **Standardwert**: [leer] • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.become_superuser_command	Ein SSH-Befehl zur Umwandlung in einen Superuser.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Standardwert**: su • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.prompt_changing_command_regex	SSH-Befehle, die die Shell-Eingabeaufforderung ändern. Wenn der vom MID Server gesendete Befehl mit dem regulären Ausdruck übereinstimmt, erwartet der MID Server eine Änderung der Eingabeaufforderung des Servers. • **Standardwert**: changeto\\s+[^\\s]+ • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.ignore_errors_on_commands_regex	Regulärer Ausdruck für den Befehl, für den der MID Server Berechtigungsfehler ignoriert. • **Standardwert**: stat.*|istat.*|perl.* • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.prompt_last_char_regex	Regulärer Ausdruck des letzten Zeichens in der Standardaufforderung des Servers. • **Standardwert**: [$#>\\]\\:] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.timeout	Zeitüberschreitung des SSH-Befehls (in Millisekunden). • **Standardwert**: 60.000 • **Typ**: Ganzzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.port	SSH-Portnummer. Um mehr als einen Port hinzuzufügen, trennen Sie Portnummern durch Kommata. Beispiel: 22,33,44. • **Standardwert**: 22 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.connect.retry	Anzahl der SSH-Verbindungswiederholungen. • **Standardwert**: 1 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.additional_setup	Befehl, den MID-Server sendet, nachdem die SSH-Sitzung erstellt wurde. • **Standardwert**: [leer] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.expect_after_su	Regulärer Ausdruck des letzten Zeichens in der Aufforderung nach dem Senden von „su“. • **Standardwert**: [:$#>\\]] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.privileged_command_last_char	Zeichen, das das letzte erwartete Zeichen in der Zeichenfolge eines Befehlsergebnisses angibt. Sobald dieses Zeichen im Ergebnis erkannt wird, wartet der MID Server nicht auf weitere Ausgaben. • **Standardwert**: [leer] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.prompt	Zeichenfolge, die die nicht standardmäßige SSH-Eingabeaufforderung darstellt. Der MID-Server verwendet diese Zeichenfolge beim Analysieren von Ergebnissen von SSH-CLI-Befehlen. • **Standardwert**: SERVNOW> • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.proprietary_system_trial_count	Anzahl der zusätzlichen Wartezeiten auf proprietären Nicht-UNIX/Linux-Systemen. Der MID-Server wartet nach der anfänglichen Wartezeit von 5 Sekunden auf eine Antwort. Nach den ersten 5 Sekunden wartet der MID Server so oft auf die Antwort, wie durch diesen Parameter definiert. Die zusätzliche Wartezeit beginnt mit 1 Sekunde und erhöht sich bei jeder Iteration um 1 Sekunde. • **Standardwert**: 10 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
mid.sa.ssh.restart_after_unstopped_threads	Anzahl der zulässigen nicht angehaltenen Threads, bevor MID-Server neu gestartet wird, wenn versucht wird, die SSH-Sitzung zu schließen. • **Standardwert**: 50 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.stty_command	stty-Befehl zum Konfigurieren der entsprechenden Einstellungen. Der MID-Server führt diesen Befehl aus, wenn das SSH-Terminal initialisiert wird. • **Standardwert**: [leer] • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.inocrrect_password_regex	Erwartete Zeichenfolge, die das SSH-Terminal zurückgibt, wenn der MID-Server während beim Anmeldeprozess ein falsches Passwort verwendet. • **Standardwert**: Sorry, try again|incorrect password attempt • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.max_unstopped_threads	Identisch mit Parameter mid.sa.ssh.restart_after_unstopped_threads. • **Standardwert**: 50 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.ssh.idle_after_sudo	Zeitraum (in Millisekunden), den der MID-Server nach dem Senden eines sudo-Befehls wartet, ohne Aktivität in der Zeile zu erwarten. • **Standardwert**: 3000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .

WMI-bezogene Eigenschaften

Wichtig: Ab New York Patch 10 und höher wird WMI Collector nicht mehr unterstützt. Weitere Informationen finden Sie unter KB0791835 WMI Collector deprecation details (Details zur Einstellung der Unterstützung von WMI Collector).

Eigenschaften	Beschreibung
mid.servicewatch.wmi.host	Host/IP des Servers, auf dem ServiceNow WMI Collector ausgeführt wird. • **Standardwert**: localhost • **Typ**: Zeichenfolge • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.servicewatch.wmi.port	Port, an dem der ServiceNow WMI Collector-Service auf Anforderungen des MID Servers lauscht. • **Standardwert**: 8585 • **Typ**: Ganzzahl • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.sa.wmi.timeout	Zeitüberschreitung bei Befehlsausführung in Millisekunden. Diese Eigenschaft steuert auch die PowerShell-Befehle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
	• **Standardwert**: 60.000 • **Typ**: Ganzzahl • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.sa.wmi.max_bytes_in_response	Maximale Anzahl von Zeichen, die in einer Antwort zulässig sind. • **Standardwert**: 20.971.520 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.servicewatch.wmi.get_file_on_shared_drive_from_collector	Der MID-Server versucht, auf die angeforderte Datei auf einem freigegebenen Laufwerk direkt vom MID-Server aus zuzugreifen. • **Standardwert**: true • **Typ**: true/false • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.sa.wmi.access_denied_regex	Regulärer Ausdruck von Fehlermeldungen, die vom Server zurückgegeben werden und die der MID Server als Zugriffsproblem betrachtet und es daher mit anderen Anmeldeinformationen versucht. • **Standardwert**: Access is denied|Access denied|service installation failed|User credentials cannot be used for local connections|System error 1312|generic failure|Insufficient privilege|user rights|HRESULT: 0x800706BA • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
mid.sa.wmi.send_retry_count	Anzahl der Kommunikationsversuche mit dem ServiceNow WMI Collector-Service für jede Anforderung. • **Standardwert**: 1 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.servicewatch.wmi.mui	Der MID-Server unterstützt die MUI-Konfiguration (Multilingual UI). • **Standardwert**: false • **Typ**: true/false • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.powershell_api.winrm.remote_port	Legen Sie den Port fest, den WinRM für die Verbindung zu Remotehosts verwendet. • **Standardwert**: 5985 • **Typ**: Ganzzahl • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.windows.management_protocol	Verwaltungsprotokoll, das der MID Server für die Verbindung mit Windows-Servern verwendet. Zulässige Werte sind WMI und WinRM. • **Standardwert**: WMI • **Typ**: Zeichenfolge • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.servicewatch.wmi.protocol	Kommunikationsprotokoll zwischen MID-Server und WMI Collector. Erlaubte Werte: http/https.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
	• **Standardwert**: http • **Typ**: Zeichenfolge • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.use_powershell	Ermöglicht die Verwendung von PowerShell zum Ausführen von Befehlen auf Windows-Servern. • **Standardwert**: false • **Typ**: true/false • **Standort:** Diese Eigenschaft ist unter „spezifisch“ verfügbar MID-Server Parameter wie in beschrieben Fügen Sie einen MID-Server-Parameter hinzu .
mid.sa.prefer_powershell	Macht PowerShell zur bevorzugten Methode zum Ausführen von Befehlen auf Windows-Servern. **Hinweis:** Wenn Sie diesen Parameter auf „true“ setzen, müssen Sie auch den Parameter mid.sa.use_powershell auf „true“ festlegen. • **Standardwert**: false • **Typ**: true/false • **Standort: MID-Server** > **Eigenschaften**
mid.win.baseboard.or.bios.insertion	Bewirkt, dass das Muster `Windows OS - Servers` anstelle der Baseboard-Seriennummer die BIOS-Seriennummer erkennt. • **Mögliche Werte**: false – zum Ausfüllen der BaseBoard-Nummer; true – zum Ausfüllen der BIOS-Seriennummer. • **Typ**: true/false • **Standardwert**: false • **Standort: MID-Server** > **Eigenschaften**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMP-bezogene Eigenschaften

Eigenschaft	Beschreibung
mid.snmp.request.timeout	Zeit (in Millisekunden), die der MID Server auf eine Antwort für jede OID-Anforderung wartet. • **Standardwert**: 1.500 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.port	SNMP-Port. • **Standardwert**: 161 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.retry	Anzahl der SNMP-Wiederholungen. • **Standardwert**: 1 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.table_size_limit	Maximale Tabellengröße, die in die SNMP-Tabellenanforderungen aufgenommen werden soll. • **Standardwert**: 20.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.table_walk_limit	Maximale Anzahl von Anforderungen in der SNMP-Walk-Sitzung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Standardwert**: 10.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.get_table_timeout_sec	Maximale Zeit (in Sekunden), die für das Laden einer gesamten SNMP-Tabelle zulässig ist. • **Standardwert**: 600 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.walk_timeout_sec	Maximale Zeit (in Sekunden), die für die SNMP-Walk-Sitzung zulässig ist. • **Standardwert**: 600 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.discover_engine	Autorisierende Discovery Engine-ID in SNMP V3-Sitzungen. • **Standardwert**: true • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.snmp_v2_disabled	Verwendung von SNMP Version 2 deaktivieren • **Standardwert**: false • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .
mid.sa.snmp.failed_status_oid	OID, die den Status „Fehlgeschlagen“ angibt. Wenn ein SNMP-Ergebnis mit dieser OID beginnt, betrachtet der MID-Server es als Fehler. • **Standardwert**: 1.3.6.1.6.3.15.1.1.3 • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie in beschrieben hinzufügen Erstellen Sie eine MID-Server-Eigenschaft .

Vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery

Standardmäßig nehmen mehrere vorkonfigurierte CI-Beziehungen an der Tag-basierten Discovery teil. In der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_Traversal_rules] werden diese Beziehungen gespeichert.

Wichtig: Sie können vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, nicht aus der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_Traversal_rules] löschen oder ändern.

Vorkonfigurierte CI-Beziehungen, die standardmäßig bei der Tag-basierten Erkennung berücksichtigt werden

CI	Beziehung	CI
VM-Instanz [cmdb_ci_vm_instance]	Virtualisiert::Virtualisiert von	Hardware [cmdb_ci_hardware]
Hardware [cmdb_ci_hardware]	Wird ausgeführt:Wird ausgeführt auf	Anwendung [cmdb_ci_appl]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthält::Enthalten in	Virtualisierungscontainer auf Betriebssystemebene [cmdb_ci_oslv_container]

Zusätzliche vorkonfigurierte CI-Beziehungen für die tagbasierte Erkennung

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Kubernetes-Service [cmdb_ci_kubernetes_service]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche vorkonfigurierte CI-Beziehungen für die tagbasierte Erkennung (Fortsetzung)

CI	Beziehung	CI
OpenShift-Projekt [cmdb_ci_openshift_project]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Cluster::Cluster von	Kubernetes-Service [cmdb_ci_kubernetes_service]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	Bereitgestellte OpenShift-Konfiguration [cmdb_ci_openshift_dep_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Buildkonfiguration [cmdb_ci_openshift_build_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Route [cmdb_ci_openshift_route]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Image-Stream [cmdb_ci_openshift_images_stream]

Eigenschaften im Zusammenhang mit der Tag-basierten Discovery

Das Service-Mapping-Plugin enthält mehrere Eigenschaften, die sich speziell auf die Tag-basierte Discovery beziehen.

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie ein `sys_properties.list` Im Navigationsfilter.

Eigenschaft	Beschreibung
sn_sm_scoped_App.svc_by_Tags.max_Candidates_per_family	Begrenzt die maximale Anzahl von Tag-basierten Servicekandidaten, die für eine einzelne Familie erstellt wurden. Wenn die Familiendefinition weitere Kandidaten enthält, haben die zuletzt aktualisierten CIs Vorrang. Dieser Wert gilt für alle Tag-basierten Servicefamilien. • **Typ:** Ganzzahl • **Standardwert:** 200
svc_by_Tags.classes.Whitelist	Diese Eigenschaft enthält die Liste der zulässigen CI-Klassen, die durch Kommas getrennt sind. Die Tag-basierte Zuordnung enthält die CIs, die zu diesen Klassen gehören. Ein leeres Feld „Wert“ gibt die Einbeziehung aller CI-Klassen an.
svc_by_tags.install_status.blacklist	Diese Eigenschaft enthält die Liste der Ausschlüsse basierend auf dem Installationsstatus, getrennt durch Kommas. Die Tag-basierte Zuordnung schließt alle getaggten CIs mit den folgenden Installationsstatus aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: In diesem Kontext werden CIs, die durch Durchlaufregeln bereitgestellt werden, nicht als getaggt betrachtet. Diese Eigenschaft gilt nur für ursprüngliche CIs mit Tags. **Standardwert** : 7.100 **Andere mögliche Werte**: Installiert=1, bestellt=2, in Wartung=3, ausstehende Installation=4, ausstehende Reparatur=5, auf Lager = 6, stillgelegt = 7, gestohlen = 8
svc_by_tags.max.categories.per.family	Legen Sie die maximale Anzahl von Kategorien fest, die pro Servicefamilie zulässig sind. • **Typ**: Ganzzahl • **Standardwert**: 3
svc_by_tags.max.traversal.rules.active	Legen Sie die maximal zulässige Anzahl von CI-Beziehungen fest, die sich im aktiven Status befinden können. Service-Mapping verwendet für die Tag-basierte Erkennung nur aktive CI-Beziehungen. • **Typ**: Ganzzahl • **Standardwert**: 5 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_tags.max_ci_limit	Legen Sie die maximal zulässige Anzahl von CIs fest, die ein auf Tags basierender Anwendungsservice enthalten kann. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Durchlaufregeln für Formularabschluss für Anwendungsservices

Um während des Tag-basierten Discovery-Prozesses eine vorhandene CI-Beziehung zu bearbeiten oder eine neue CI-Beziehung hinzuzufügen, füllen Sie das Formular „Durchlaufregeln für Anwendungsservices“ aus.

Feld	Beschreibung
Regeldefinition	Wählen Sie eine vorkonfigurierte CI-Beziehung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Erstellen Sie alternativ eine neue CI-Beziehung: 1. Klicken Sie auf **Neu**. 2. Wählen Sie die CI-Klasse aus der Liste **Übergeordneter Typ** aus. 3. Wählen Sie den Beziehungstyp aus der Liste **Beziehungstyp** aus. 4. Wählen Sie die CI-Klasse aus der Liste **Untergeordneter Typ** aus. 5. Klicken Sie auf **Absenden**. Die neue CI-Beziehung wird der Tabelle „Regeldefinitionen für CI-Beziehungstyp“ [cmdb_rel_type_rule_definitions_list] hinzugefügt. Um beispielsweise Linux-Server zu erkennen, die Speichergeräte hosten, wählen Sie die folgenden Werte aus: • Übergeordneter Typ: Linux-Server [cmdb_ci_linux_Server] • Beziehungstyp: Enthält::Enthalten in • Untergeordneter Typ: Speichergerät [cmdb_ci_storage_device]
Ist umgekehrt	Aktivieren Sie dieses Kontrollkästchen in den folgenden Fällen: • Wenn das getaggte CI in der Beziehung ein CI der untergeordneten CI-Klasse ist. • Wenn das CI, das bereits Teil des Service in der Beziehung ist, ein CI der untergeordneten CI-Klasse ist.
Verwendet von	Wählen Sie nur aus **Service nach Tags** . **Hinweis:** Nicht auswählen **Service-Neuberechnung** . Dadurch wird verhindert, dass vorhandene CI-Beziehungen bearbeitet oder neue hinzugefügt werden, und es wird eine Fehlermeldung ausgegeben.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese CI-Beziehung in der Tag-basierten Erkennung zu verwenden. Deaktivieren Sie dieses Kontrollkästchen alternativ, um diese CI-Beziehung von der Tag-basierten Erkennung auszuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Standardmäßig sind an der Tag-basierten Erkennung nur fünf CI-Beziehungen beteiligt. Um die maximale Anzahl aktiver CI-Beziehungen zu ändern, bearbeiten Sie den Wert für die Eigenschaft svc_by_tags.max.traversal.rules.active in der Tabelle „Systemeigenschaften“ [sys_properties].
Reihenfolge	Geben Sie eine Zahl für die Reihenfolge ein. Das System verwendet CI-Beziehungen zur Erkennung in aufsteigender Reihenfolge..

Tastaturkürzel zur Benutzung von Service-Mapping im Eingabehilfemodus

Im Eingabehilfemodus können Sie über eine Tastatur auf alle Serviceinstanz zuordnungen und Serviceformulare zugreifen.

Wenn die gesamte Zuordnung ausgewählt ist, enthält die Informationsnachricht oben im Fenster Anleitungen zur Navigation innerhalb der Zuordnung.

Aktion	Tastaturkürzel
Kontextmenüs aufrufen	Platz
Cluster erweitern	Geben Sie Folgendes ein:
Aus dem Bereich **Eigenschaften** in den Zuordnungsbereich wechseln	Escape-Taste
Im Menü „Weitere Optionen“ Optionen ein- und ausblenden	Platz
CIs und Verbindungen in der Zuordnung auswählen	Pfeiltaste
In der Zeitleiste können Sie die Zeit im aktuell ausgewählten Zeitraum bearbeiten.	Zahlen (1-9)
Im Fenster der Serviceinstanz zuordnung durch UI-Elemente navigieren	Registerkarte

Beispieldefinitionen für Servicefamilien in Tag-basierter Zuordnung

Erstellen Sie bei der Vorbereitung der Zuordnung von Anwendungsservices basierend auf Tags Tag-Kategorien, die Tags mit ähnlicher Verwendung enthalten. Definieren Sie eine Tag-basierte Servicefamilie und die Tags, die Sie für die Zuordnung verwenden möchten. Neben Tag-Kategorien können Sie auch Tag-Werte definieren, um die Kriterien für die von erstellten Servicekandidaten einzugrenzen Service-Mapping. Verwenden Sie diese Beispiele als Anleitung.

Detaillierte Informationen zum Definieren von Servicefamilien in der Tag-basierten Zuordnung finden Sie unter Zuordnung von Anwendungsservices basierend auf Tags vorbereiten.

Hinweis: Beginnend mit Service-Mapping Plus Version 1.16.3, nutzen Sie die Vorteile von Tag-basiert Service-Mapping Arbeitsbereich zur effizienten Zuordnung Ihrer Anwendungsservices. Weitere Informationen finden Sie unter Tag-basierte Zuordnung in Service-Mapping Arbeitsbereich Und Tag-basierte Discovery für Service-Mapping Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für die Definition von Tag-basierten Zuordnungskriterien für Servicefamilien

Definitionen der Servicefamilie	Kategorie	Schlüssel	Wert (optional)	Ergebnis
Beispiel 1: eine Tag-Kategorie, keine Werte	Umgebung	ENV	Nicht definiert	Service-Mapping erstellt für den ENV-Schlüssel einen Servicekandidaten für jeden Tag-Wert. Jeder Servicekandidat enthält nur CIs mit demselben Wert für den ENV-Schlüssel.
Beispiel 2: eine Tag-Kategorie, ein Wert	Umgebung	ENV	Produktion	Service-Mapping erstellt einen Servicekandidaten, der nur CIs enthält, die den ENV-Tag-Schlüssel mit dem Tag-Wert „production” enthalten.
Beispiel 3: eine Tag-Kategorie, zwei Werte	Umgebung	ENV	Staging, Production	Service-Mapping erstellt zwei Servicekandidaten: Einer enthält CIs mit dem Tag-Wert „production”; ein weiterer enthält CIs mit dem Tag-Wert „staging”.
Beispiel 4: zwei Tag-Kategorien, keine Werte	Umgebung Applikation	ENV App	Nicht definiert	Service-Mapping erstellt für alle definierten Tag-Schlüssel einen Servicekandidaten für jede Kombination von Tag-Werten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für die Definition von Tag-basierten Zuordnungskriterien für Servicefamilien (Fortsetzung)

Definitionen der Servicefamilie	Kategorie	Schlüssel	Wert (optional)	Ergebnis
Beispiel 5: zwei Tag-Kategorien, zwei Werte für jede Kategorie	Umgebung Applikation	ENV App	Production, Staging HR, Finance	Service-Mapping erstellt vier Servicekandidaten: production::hr, production::finance, staging::hr, staging::finance.

Traffic-basierte Verbindungsliste

In diesem Diagramm finden Sie Informationen zu verkehrsbasierten Verbindungen, wenn Sie CIs aus einem Anwendungsservice entfernen.

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	• **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. • **Nein** – Wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie Entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ITOM-Transparenz verwendete Erkennungsmuster

Von Service-Mapping und Discovery werden Muster in den jeweiligen Discovery-Prozessen verwendet, die die meisten branchenüblichen Netzwerkgeräte und Anwendungen abdecken. Sie können diese Muster anpassen und neue erstellen.

ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

Was sind Erkennungsmuster?

Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen. Service-Mapping und Discovery teilen sich einen Satz vorkonfigurierter Muster, die die meisten häufig verwendeten Geräte und Anwendungen abdecken. Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden. Beispiel: Discovery Führt die horizontale Discovery mit dem Apache-Webserver-Muster aus, um alle Apache-Webserver in Ihrer Organisation zu finden und aufzulisten. Service-Mapping Führt die Top Down-Discovery mit demselben Muster aus, um einen bestimmten Apache-Webserver zu erkennen und in einer Serviceinstanzzuordnung zu platzieren.

Hinweis: Mustervorgänge bieten derzeit keine Unterstützung mehrerer Sprachen. Wenn die Werte, die von Mustervorgängen zurückgegeben werden, nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Muster-Discovery schlägt fehl.

Musterverwendung von Service-Mapping und Discovery

Produkt	Mustertyp	Ergebnis
Discovery	Infrastrukturmuster	Bestandsliste der Geräte
	Anwendungsmuster	Bestandsliste der Anwendungen
Service-Mapping	Anwendungsmuster	Serviceinstanz map

Für die Erkennung von Geräten, die als Hosts für Anwendungen agieren, verlässt sich Service-Mapping auf Discovery. Als Teil des Erkennungsprozesses von oben nach unten weist Service-Mapping Discovery an, seine horizontale Erkennung im Hintergrund durchzuführen. Service-Mapping verwendet dann die Informationen zu den Hosts, die bei der horizontalen Erkennung ermittelt werden, zum Erstellen von Serviceinstanz -Karten.

Muster aller Typen werden in der Tabelle „Erkennungsmuster“ [sa_pattern] gespeichert.

Discovery verwendet eine Kombination aus Probes und Mustern. Weitere Informationen finden Sie unter Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren.

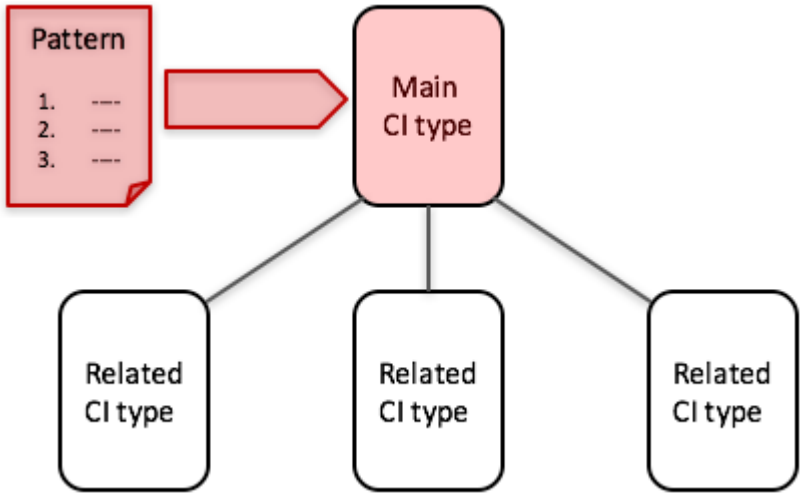
Korrelation zwischen Muster und CI-Typ

Muster werden den CI-Typen zugewiesen, die zur Erkennung dienen. Bei Bedarf können Sie pro Muster mehrere CI-Typen zuweisen. In diesem Fall definieren Sie einen Haupt-CI-Typ und mehrere zugehörige CI-Typen. Beispiel: Ein Muster zur Erkennung von BIG-IP Global Traffic Manager (GTM) F5 weist BIG-IP Global Traffic Manager (GTM) F5 als Haupt-CI-Typ und zugehörige CI-Typen für den DNS-Namen, den Netzwerkadapter und andere Komponenten auf.

Bei der Erkennung von oben nach unten durch Service-Mapping dient jedes Anwendungsmuster nur zur Erkennung des Haupt-CI-Typs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

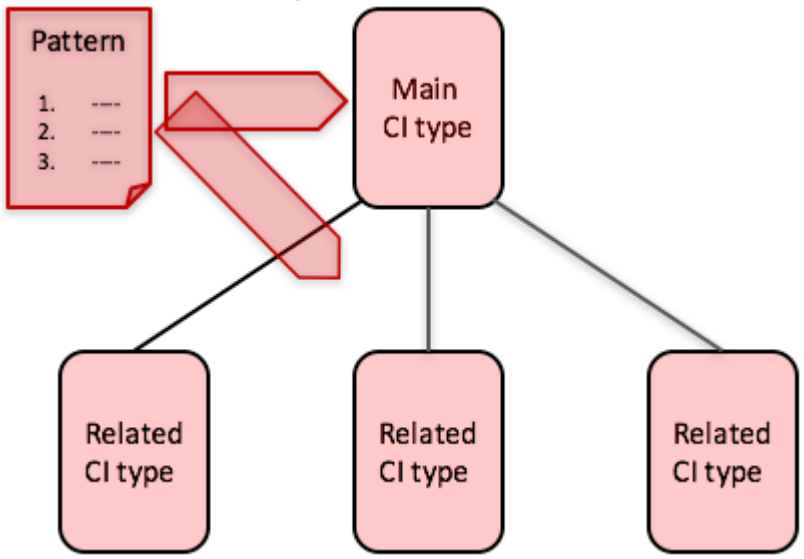
Erkennung des Haupt-CI-Typs während der Erkennung von oben nach unten



Gleichzeitig verwendet Service-Mapping in der Regel mehr als ein Muster, um denselben CI-Typ zu erkennen, da ein CI-Typ verschiedene Protokolle, Betriebssysteme, Einstiegspunkte usw. verwenden kann.

Im Gegensatz zur Erkennung von oben nach unten verwendet der Prozess der horizontalen Erkennung jedes Muster, um einen Haupt-CI-Typ mit allen zugehörigen CI-Typen zu erkennen.

Erkennung des Haupttyps und der zugehörigen CI-Typen während der horizontalen Erkennung



Warum Muster aus dem ServiceNow Store installieren

ServiceNow veröffentlicht monatlich neue Discovery-Muster im ServiceNow Store , um sicherzustellen, dass Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann. Hauptversionen von ServiceNow enthalten Muster, die zuvor im ServiceNow Store veröffentlicht wurden.

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

Visibility Content (sn_pattern_design)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Sie können die neuesten verfügbaren Versionen der Musteranwendungen aus dem ServiceNow Store installieren. Alternativ können Sie diese Anwendungen als Plugins auf Ihrer Instanz von ServiceNow installieren.

Warum Muster anpassen

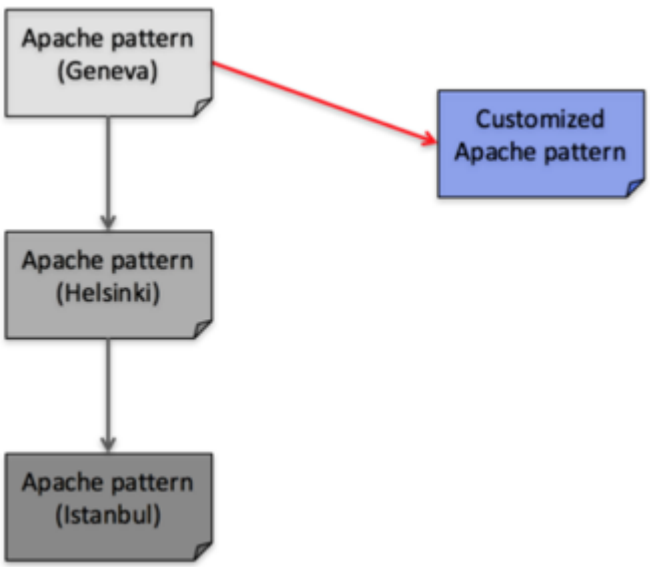
Sie können Muster in den folgenden Fällen anpassen:

- Wenn Ihr Unternehmen proprietäre Geräte und Anwendungen verwendet, erstellen Sie Muster für diese Elemente, damit Discovery und Service-Mapping sie erkennen können.
- Wenn Sie Schlüsselattribute von CI-Typen mit entsprechenden Mustern ändern, ändern Sie die relevanten Muster entsprechend der Änderung.

Musterversionen

Wenn Sie ein Muster anpassen, erstellen Sie tatsächlich eine Kopie des ursprünglichen vorkonfigurierten Musters. Während Service-Mapping oder Discovery die angepasste Version verwenden, wird die ursprüngliche Version nicht gelöscht. Wenn Sie ein Update des Musters aus dem ServiceNow Store herunterladen, wird das ursprüngliche Muster aktualisiert, nicht die angepasste Kopie.

Ausschluss eines benutzerdefinierten Musters von einem Upgrade



Wenn Sie das angepasste Muster verwerfen und das aktualisierte ursprüngliche Muster verwenden möchten, können Sie wie in Musterversion auswählen beschrieben zum ursprünglichen Muster zurückkehren.

Wer Muster anpassen kann

Anwender müssen über die Rolle pd_admin verfügen, um Muster anzupassen. Im Basissystem enthält die Rolle service_mapping_admin die pd_role. Das Anpassen von Mustern erfordert Grundkenntnisse in der Programmierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

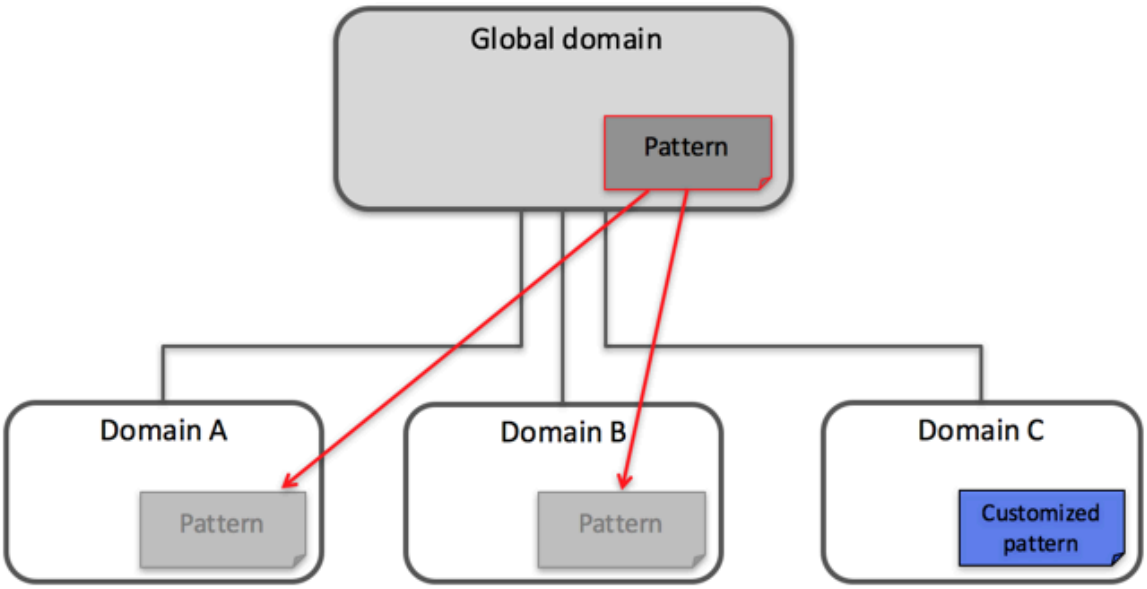
Muster für Instanzen mit Domänentrennung

In Instanzen, die Domänentrennung verwenden, können Muster domänenspezifisch sein und nur Domänen umfassen, für die Sie sie erstellt haben, oder global und auf alle Domänen angewendet werden.

Muster gehören zu Domänen. Standardmäßig werden alle vorkonfigurierten Muster der globalen Domäne zugewiesen und gelten für alle Domänen aller Ebenen.

Sie können Muster für bestimmte Domänen erstellen. In diesem Fall wird das neue Muster nur für diese Domäne verwendet und ist in keiner anderen Domäne vorhanden. Wenn Sie ein vorhandenes Muster in der globalen Domäne anpassen und einer bestimmten Domäne zuweisen, erstellen Sie eine Kopie des globalen Musters, das weiterhin in allen anderen Domänen verwendet wird, mit Ausnahme der Domäne mit der angepassten Version dieses Musters. Wenn Sie ein Muster in der globalen Domäne anpassen, wirkt sich die Änderung entsprechend auf alle Domänen aus, mit Ausnahme derjenigen, die eine angepasste Kopie dieses Musters verwendet.

Globale oder domänenspezifische Muster



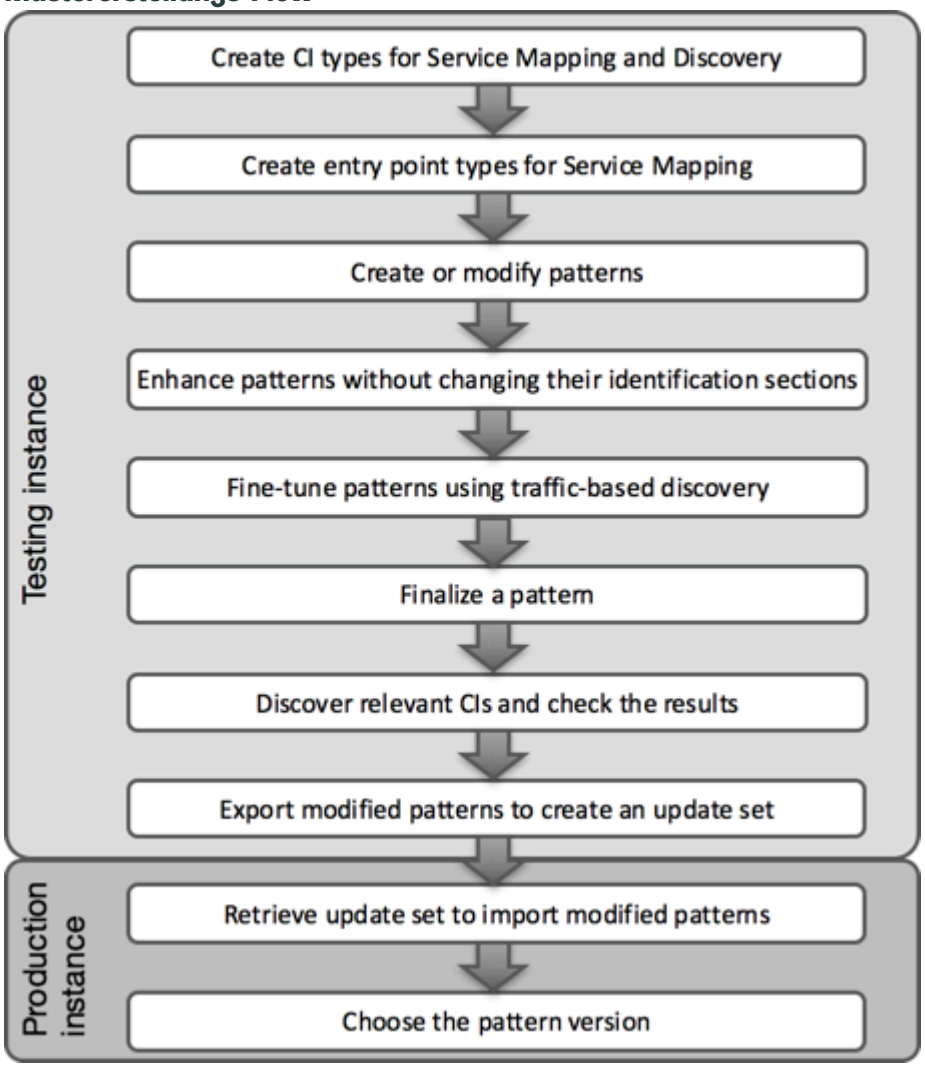
Erstellungs- oder Änderungs-Flow für Muster

Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: für die Produktion und für die Entwicklung. Erstellen oder ändern Sie Muster, testen Sie sie und überprüfen Sie die Ergebnisse in der Entwicklungsinstanz. Wenn Sie mit den Discovery-Ergebnissen zufrieden sind, exportieren Sie relevante Muster aus der Entwicklungsinstanz, um einen Update-Satz zu erstellen. Anschließend rufen Sie den Aktualisierungssatz in Ihrer Produktionsinstanz ab und legen Sie ihn fest.

Wenn Sie ein Muster für Anwendungen und Geräte erstellen, die in der Anwendung ITOM Visibility Global Content nicht unterstützt werden, erstellen Sie zuerst CI-Typen für sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mustererstellungs-Flow



Zugehörige Informationen

- Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte
- Klassendiagramme und Klassenattribute für wichtige CMDB-Klassen
- Beschreibung der wichtigsten CMDB-Tabellen im Basissystem
- CMDB CI Class Models: ServiceNow Store-App, die Klassenmodelle hinzufügt, die die CMDB-Klassenhierarchie erweitern
- Informationen zu den verschiedenen Optionen zum Füllen der CMDB
- ServiceNow Store-Apps, die vordefinierte Service Graph-Connectors zum Importieren und Integrieren gängiger Daten von Drittparteien in CMDB-Klassen bereitstellen
- KB0747679: Pre/Post Processing Scripts for patterns (Vor-/Nachverarbeitungsskripts für Muster)
- Anwendungsmuster für Agent Client Collector

Verfügbare lokale Discovery-Muster

ITOM-Transparenz wird mit einer umfangreichen Musterbibliothek geliefert.

ServiceNow veröffentlicht monatlich neue Discovery-Muster im ServiceNow Store , um sicherzustellen, dass Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann. Hauptversionen von ServiceNow enthalten Muster, die zuvor im ServiceNow Store veröffentlicht wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine vollständige Liste der Geräte und Anwendungen, die ITOM-Transparenz erkennen kann, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Apache Cassandra Datenbank-Discovery

ServiceNow Discovery Findet Apache Und DataStax Cassandra Datenbank auf UNIX Mit dem Muster „verteilte Cassandra-DB“. Um einige dieser Ressourcen zu erkennen, muss installiert werden Muster für Discovery und Service-Mapping Von ServiceNow® Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Geben Sie Anmeldeinformationen für die Erkennung des Hosts an

Identifizieren Sie die Server, auf denen ein gehostet wird Cassandra Datenbank und Anmeldeinformationen angeben, die für die horizontale Discovery dieser Server erforderlich sind. Weitere Informationen finden Sie unter Für die Hosterkennung erforderliche Anmeldeinformationen.

Überprüfen Sie, ob die Store-App „CMDB-CI-Klassenmodelle“ auf dem neuesten Stand ist

Stellen Sie sicher, dass Ihre Instanz unterstützt Cassandra CI-Klassenmodelle durch Bereitstellung der Version 1.14.0 der Store-App „CMDB CI-Klassenmodelle“ aus der ServiceNow Store.

Überprüfen Sie die Berechtigungen für Cassandra Befehle für UNIX

Für die Liste von Cassandra Befehle, siehe Cassandra (für UNIX) Abschnitt in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Überprüfen Sie den Lesezugriff auf cassandra.yaml

Mögliche Speicherorte der Datei „cassandra.yaml“:

- `$config_Directory + „/cassandra.yaml“`
- `$Process.EnvironmentVariables.CASSANDRA_CONF.value + „/cassandra.yaml“`
- `$install_Directory + „/conf/cassandra.yaml“`

Daten erfasst von Discovery Für Cassandra Datenbank

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „verteilte Cassandra-DB“.

Cassandra-Cluster [cmdb_ci_cassandra_cluster]

Feld	Beschreibung
Name [name]	Der Name des Clusters dient auch als Anzeigename.

Cassandra-Clusterknoten [cmdb_ci_cassandra_cluster_node]

Feld	Beschreibung
Cluster [cluster]	Referenz von Cassandra Cluster-CI, zu dem dieser Knoten gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra-Clusterknoten [cmdb_ci_cassandra_cluster_node] (Fortsetzung)

Feld	Beschreibung
Clustername [Cluster_Name]	Name des Clusters.
IP-Adresse [ip_address]	IP-Adresse des Clusterknotens (Hostcomputer)
Name [name]	Anzeigename im folgenden Format: cluster_name@hostname
Betriebsstatus [operational_status]	Betriebsstatus des Clusterknotens
Server [Server]	Referenz des Server-CI (Hostcomputer)

Cassandra-Instanz [cmdb_ci_cassandra_instance]

Feld	Beschreibung
Clustername [Cluster_Name]	Name des Clusters.
Konfigurationsverzeichnis [config_directory]	Verzeichnispfad, in dem Konfigurationsdateien verfügbar sind
Konfigurationsdatei [config_file]	Dateipfad der BaseInit-Konfigurationsdatei, in der andere konfigurationsbezogene Pfade konfiguriert werden können
Rechenzentrum [Data_Center]	Rechenzentrum, in dem der Clusterknoten Teil eines Clusters ist
Installationsverzeichnis [install_directory]	Der Installationspfad
IP-Adresse [ip_address]	IP-Adresse des Hostcomputers, auf dem der Prozess ausgeführt wird
Name [name]	Anzeigename, der mit der <uid> identisch ist
PID [pid]	Prozess-ID, die auf dem Hostcomputer ausgeführt wird
Rack [Rack]	Die Rack-Informationen, zu denen der Clusterknoten gehört
Beschreibung [short_description]	Eine Kurzbeschreibung der Instanz
TCP-Port(s) [tcp_port]	Liste der TCP-Ports, die wie in der Konfigurationsdatei „cassandra.yaml“ konfiguriert sind (Format: „:port1:port2:port3:“)
UID [UID]	Die eindeutige ID zum Identifizieren der Instanz (Format: <cluster_name> __ <data_center> __ <rack> @hostname)
Anbieter [vendor]	Lieferantenname für Referenz aus der Tabelle „Core_Company“, falls bereits verfügbar. Wenn er nicht verfügbar ist, wird logisch ein neuer Eintrag mit dem Namen „Apache“ oder „DataStax“ erstellt.
Arbeitsauslastung wird ausgeführt [Workload_running]	Der Name der Workload, die auf der Instanz ausgeführt wird

Cassandra-Keyspace [cmdb_ci_cassandra_keyspace]

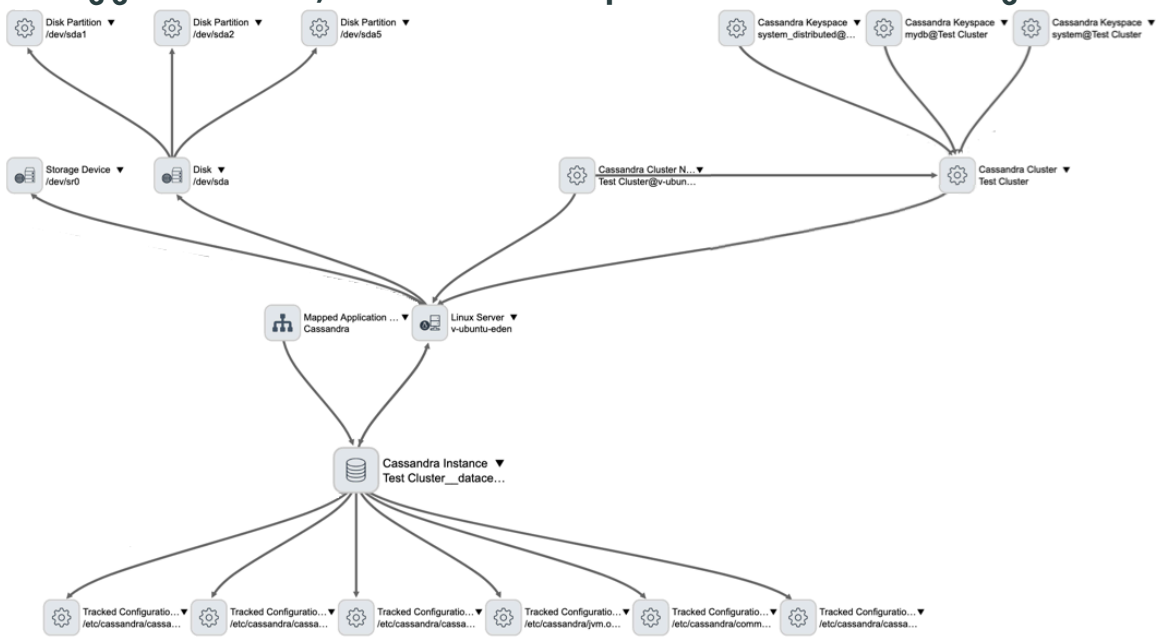
Feld	Beschreibung
Cluster [cluster]	Die Referenz von Cassandra Cluster-CI, zu dem der Keyspace gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra-Keyspace [cmdb_ci_cassandra_keyspace] (Fortsetzung)

Feld	Beschreibung
Clustername [Cluster_Name]	Name des Clusters, zu dem der Keyspace gehört
Keyspace-Name [keyspace_Name]	Name des Keyspace
Name [name]	Der Anzeigename im folgenden Format: <keyspace_name>@<cluster_name>.

Abhängigkeitsansichten, die erkannt werden Apache Cassandra Bereitstellung



CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Apache Cassandra Datenbank-Discovery.

CI	Beziehung	CI
Cassandra-Instanz [cmdb_ci_cassandra_instance]	Wird ausgeführt auf::Wird ausgeführt	Server [cmdb_ci_server]
Cassandra-Clusterknoten [cmdb_ci_cassandra_cluster_node]	Gehostet auf::Hostet	Server [cmdb_ci_server]
	Cluster von::Cluster	Cassandra-Cluster [cmdb_ci_cassandra_cluster]
Cassandra-Keyspace [cmdb_ci_cassandra_keyspace]	Gehostet auf::Hostet	Cassandra-Cluster [cmdb_ci_cassandra_cluster]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping führt die Top Down-Discovery von durch Cassandra, Die normalerweise als verteilte Datenbank auf einem Cluster von Serverknoten ausgeführt wird. Während der Top

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Down-Discovery Service-Mapping Erkennt Instanzen, die auf Knoten ausgeführt werden, und zeigt sie in der Anwendungsservice-Zuordnung an.

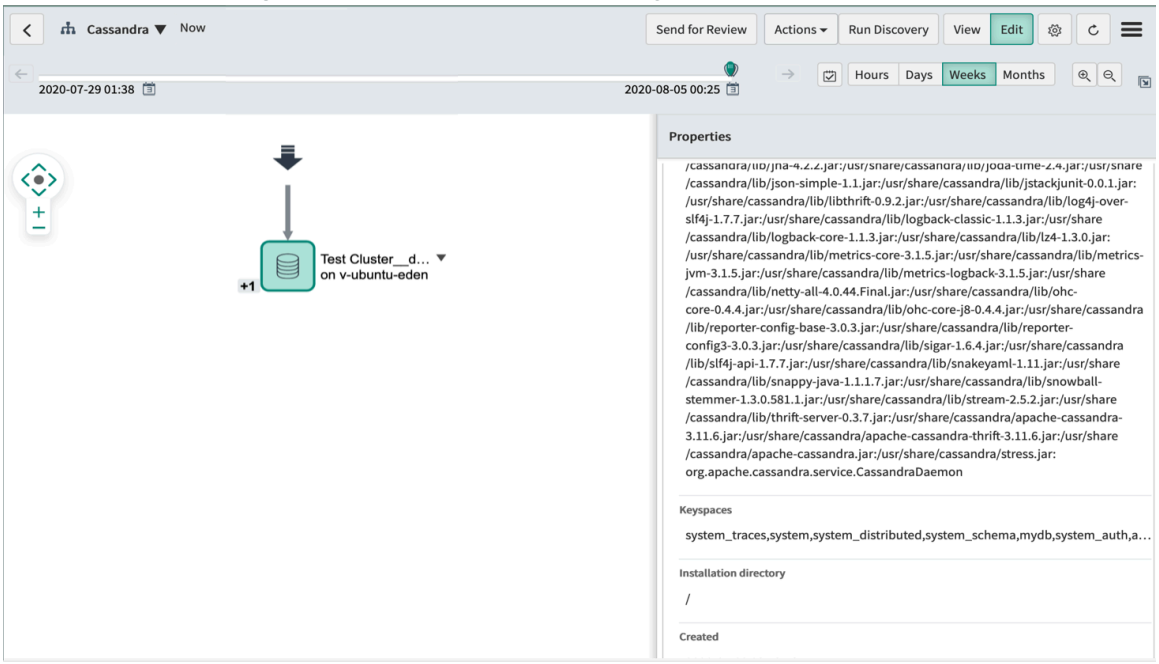
Zusätzlich zu den während der horizontalen Erkennung erkannten Tabellen und Feldern werden bei der Erkennung von oben nach unten auch die in der folgenden Tabelle aufgeführten Felder erkannt.

Cassandra-Instanz [cmdb_ci_cassandra_instance]

Feld	Beschreibung
Keyspaces [Keyspaces]	Keyspace(s), auf die die Instanz zugreifen kann (nur in Erkennung von oben nach unten ausgefüllt)

Bei eingehenden Verbindungen wird die Instanz erkannt, wie im folgenden Bild dargestellt.

Cassandra Discovery-Top-Down-Servicezuordnung



Zugehörige Informationen

Discovery des Berichts „Datenbankadministrator“ (DBA)

Erkennung von Apache Kafka und Apache Zookeeper

ServiceNow Discovery verwendet das Erkennungsmuster „Kafka and Zookeeper“, um Kafka-Daten zu finden, die für den Zookeeper-Synchronisierungsservice erstellt wurden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App „CMDB CI Class Models“

Stellen Sie sicher, dass die Store-App CMDB CI Class Models (Version 1.20.0) installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.72) installiert ist.

Zertifizierungsstellen-Prozess

Stellen Sie sicher, dass auf dem Hostcomputer der CA-Prozess ausgeführt wird.

Discovery-Anmeldeinformationen

Stellen Sie sicher, dass Sie über die Anmeldeinformationen für die Ausführung von Discovery auf dem Host-Computer verfügen, auf dem der CA-Prozess ausgeführt wird.

Die Kafka- und Zookeeper-Prozesse müssen auf dem Host ausgeführt werden.

Hinweis: Die Discovery des Kafka-Brokers muss zuerst ausgeführt werden, gefolgt von Zookeeper. In der Zookeeper-Konfigurationsdatei muss die Reihenfolge der Knoten, die das Cluster bilden, für alle Knoten im Cluster einheitlich sein.

Von Discovery während der horizontalen Erkennung erfasste Daten

In der Tabelle [cmdb_ci_appl_kafka_connect] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
node	Knoten, auf dem Zookeeper installiert ist
tier	Stufe von Zookeeper
install_directory	Pfad des Installationsverzeichnisses
config_file	Pfad der Konfigurationsdatei
config_directory	Pfad des Konfigurationsverzeichnisses

In der Tabelle [cmdb_ci_appl_kafka_topic] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
isr	Synchronisiertes Replikat
replicas	Anzahl der Replikate des Themas
partition_count	Anzahl der Partitionen des Themas
replication_factor	Replikationsfaktor des Themas

In der Tabelle [cmdb_ci_appl_zoo_keeper] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
node	Knoten, auf dem Zookeeper installiert ist
tier	Stufe von Zookeeper
config_file	Pfad der Konfigurationsdatei
install_directory	Pfad der Installation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Tabelle [cmdb_ci_kafka_cluster] erkannte Ressourcen

Felder	Beschreibung
Cluster_id	Eindeutige clusterspezifische ID

In der Tabelle [cmdb_ci_zoo_keeper_cluster] erkannte Ressourcen

Felder	Beschreibung
Cluster_id	Eindeutige clusterspezifische ID

In der Tabelle [cmdb_ci_kafka_cluster_node] erkannte Ressourcen

Felder	Beschreibung
Name	Name des Knotens
Clustername	Name des Clusters, zu dem der Knoten gehört

In der Tabelle [cmdb_ci_zoo_keeper_cluster_node] erkannte Ressourcen

Felder	Beschreibung
Name	Name des Knotens
clustername	Name des Clusters, zu dem der Knoten gehört

CI-Beziehungen

Das Muster „Kafka and Zookeeper“ erstellt keine CI-Beziehungen.

Erkennung von Apigee Edge Enterprise Edition

Die Anwendung ServiceNow Discovery verwendet das APIGee-Muster, um Apigee Edge Enterprise Edition-Versionen 4.xx zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das APIGee-Muster verwendet einen integrierten Cache-Mechanismus, der Daten von jedem API-Service in einer lokalen Cache-Datei sammelt. Service-Mapping führt eine Erkennung von oben nach unten für diese Cache-Dateien durch, um ausgehende Apigee Edge-Verbindungen zu finden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Linux-Benutzer

Gewähren Sie einem Benutzer des Linux-Betriebssystems erhöhte Rechte für die Ausführung der Befehle cat, ls, netstat und stat. Weitere Informationen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erteilen Sie diesem Linux-Benutzer außerdem die Berechtigung, die folgenden Befehle im Home-Ordner des Betriebssystembenutzers auszuführen:

Befehl	Beschreibung
"date +%s"	Ruft das aktuelle Datum ab
"ls -d $HOME/APIGee_Cache/cache_folder*"	Ruft den letzten Cache-Ordner ab
"mkdir-p $HOME/APIGee_Cache/ cache_folder_" + $today + ";ls -d$HOME/ APIGee_Cache/cache_folder_" + $today	Erstellt die Cache-Datei, wenn die Cache-Datei leer ist
"ls -d $HOME/APIGee_Cache/cache_folder*"	Überprüft, ob die Cache-Datei erstellt wurde
"echo `expr " + $today + " -" + $current_date + "`"	Berechnet die Lücke zwischen dem Zeitpunkt der Ordnererstellung und dem aktuellen Datum
"if [" + $diff + " -ge" + $week_seconds+ "]; then echo true; fi"	Prüft, ob der Ordner neu erstellt werden muss
"ls" + $cache_folder+ "/* | sort | xargsgrep -l " + $entry_point.source_url	Überprüft, ob vorhandene Cache-Dateien die Quell-URL enthalten, die Sie als Einstiegspunkt für den Service eingeben
"rm-rf" + $cache_folder+ ";mkdir-p $HOME/ APIGee_Cache/cache_folder_" + $today + ";ls -d $HOME/APIGee_Cache/cache_folder_" + $today	Entfernt alte Cache-Dateien
“curl -k -X GETurl-H '<ClientID>: <Token>’”	Ruft die API-Antwort für das angegebene Token ab
"ls" + $cache_folder+ "/* | sort | xargsgrep -l " + $entry_point.source_url	Ruft die URL-Definition aus der Cache-Datei ab

Applicative-Anmeldeinformationen

Konfigurieren Sie die Applicative-Anmeldeinformationen wie folgt:

Formular „Applicative-Anmeldeinformationen“

Feld	Beschreibung
Name	Der Name der Anmeldeinformationen, z. B. „Apigee-Token“
Aktiv	Kontrollkästchen zum Aktivieren dieser Anmeldeinformationen für die Erkennung
Benutzername	Der Name des Benutzers dieser Applicative-Anmeldeinformationen. Sie können einen beliebigen Benutzer für die Anmeldeinformationen für dieses Muster verwenden, da die Informationen aus einem lokalen Cache extrahiert werden.
Passwort	Das tatsächliche Benutzerpasswort für diese Applicative-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Applicative-Anmeldeinformationen“ (Fortsetzung)

Feld	Beschreibung
CI-Typ	Der CI-Typ, für den diese Anmeldeinformationen verwendet werden: APIGee-Service [cmdb_ci_appl_apigee_srv]. **Hinweis:** ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
Reihenfolge	Geben Sie die Reihenfolge (Reihenfolge) ein, in der die Plattform diese Berechtigungsnachweise versucht, während sie versucht, sich an Geräten anzumelden. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge.

Curl-Befehl

Stellen Sie sicher, dass der Befehl „curl“ auf dem Linux-Server installiert ist, der Apigee Edge hostet.

Systemeigenschaften konfigurieren

- Zum Erstellen von ausgehenden Apigee Edge-Verbindungen von oben nach unten konfigurieren Sie die Systemeigenschaft Apigee-URLs (apigee.urls) mit der folgenden Syntax:

  01#DVL#https://<url1>.com/dashboard/v1/targetServers/dvl### 02#QA#https://<url2>.com/dashboard/v2/targetServers/qa###

  Wobei

  01 die URL-Nummer ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DVL der Umgebungstyp ist, wie z. B. Entwicklung.

das Trennzeichen zwischen den Attributen ist. Platzieren Sie es genau an der Stelle wie im Beispiel oben.

das Trennzeichen zwischen URLs ist.

- Konfigurieren Sie die Systemeigenschaft Apigee API Client ID (apigee.api.Client.ID), indem Sie die Apigee API Client ID in das Feld Wert eingeben. Das Muster verwendet diese Eigenschaft als Header für den Curl-Befehl mit dem Token:

```
curl -k -X GET " + url + " -H ' apigee.api.client.id: " + token
```

Das Muster füllt diese beiden Systemeigenschaften mithilfe des *Apigee-URLs und Apigee API Client-ID hinzufügen* sa_pre_task_script aus.

Daten erfasst von Discovery Für die Apigee Edge Enterprise-Edition

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Apigee-Musters.

Apigee-Service [cmdb_ci_appl_apigee_srv]

Feld	Beschreibung
Name [name]	Der Name des Servers, der Apigee Edge hostet
Version [version]	Die Version von Apigee Edge
Installationsverzeichnis [install_directory]	Der Ordner mit allen Apigee Edge-Bibliotheken und ausführbaren Dateien
Konfigurationsverzeichnis [config_directory]	Der Ordner mit allen Apigee Edge-Konfigurationsdateien

CI-Beziehungen

Das APIGee-Muster erstellt keine CI-Beziehungen.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Das APIGee-Muster identifiziert Verbindungen von Apigee Edge zu anderen CIs basierend auf der URL, die Sie im Verbindungsabschnitt des Musters konfigurieren.

Avi Vantage-Lastenausgleicherkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden die Muster für die Avi-Lastenausgleicherkennung, um die Komponenten des Avi Vantage-Lastenausgleichsmoduls zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery verwendet das Muster „Avi Load Balancer Controller“ und sowie das Muster „Avi Load Balancer Controller - Session-based“, um die horizontale Erkennung auszuführen. Von beiden Mustern werden REST-APIs dazu verwendet, die Lastenausgleichsmodule zu finden. Sie unterscheiden sich nur in der Art der Authentifizierung, die beim Ausführen der API-Abfragen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die Erkennung von oben nach unten verwendet Service-Mapping das Muster „Avi Load Balancer VIP“.

Die Muster unterstützen Avi-Infrastrukturen unter AWS und VMware. Sie verknüpfen die erkannten CIs nur, wenn sie auf ausgeführt werden VMware . Die Muster unterstützen auch Global Server Load Balancing (GSLB).

Sie können diese Muster auf der ServiceNow AI Platform® mit Release Madrid Patch 5, New York oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihre Instanz die CI-Klassenmodelle des Avi-Lastenausgleichsmoduls unterstützt, indem Sie die neueste Version der Store-App CMDB CI Class Models bereitstellen. Installieren Sie die Anwendung aus dem ServiceNow Store.
- Für das Muster „Avi Load Balancer Controller“:
  - Stellen Sie im Avi-Controller sicher, dass Standardauthentifizierung zulässig ist.
  - Konfigurieren Sie die folgenden Anmeldeinformationen:
    1. Navigieren zu **Discovery** > **Anmeldeinformationen**
    2. Klicken Sie auf **Neu**.
    3. Klicken Sie auf **Basisanmeldedaten**, füllen Sie das Formular aus, und klicken Sie dann auf **Senden**.

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Wählen Sie **Alle MID Server**.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zufälliger Reihenfolge durch. Der Standardwert ist 100.
Benutzername	Name des Benutzers für die Ausführung der Avi-Lastenausgleicherkennung
Passwort	Passwort für diesen Benutzer

4. Schnell-Discovery ausführen auf der IP-Adresse des Avi Controller-Clusters.

- Für das Muster „Avi Load Balancer Controller - Session-based“:
  - Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung mit einem Alias:
    1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
    2. Klicken Sie auf **Neu**.
    3. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie **Anmeldeinformationen** als Alias-Typ aus.
    4. Klicken Sie auf **Absenden**.
    5. Öffnen Sie den neuen Alias.
    6. Klicken Sie auf der Registerkarte Anmeldeinformationen auf **Neu**.
    7. Wählen Sie **Basisanmeldedaten** für den Anmeldeinformationstyp aus, und füllen Sie das Formular aus.

       Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Benutzername	Name des Benutzers für die Ausführung der Avi-Lastenausgleicherkennung
Passwort	Passwort für diesen Benutzer

    8. Klicken Sie auf **Aktualisieren**.
  - Erstellen Sie einen Zeitplan für eine Erkennung ohne Server.

    Führen Sie dann folgende Schritte aus:
    1. Klicken Sie im Planer auf **Serverlose Ausführungsmuster** Registerkarte.
    2. Klicken Sie auf **Neu**.
    3. Füllen Sie das Formular aus, und klicken Sie dann auf **Senden**.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Muster	Wählen Sie das Muster „Avi Load Balancer Controller - Session-based“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie den in den vorherigen Schritten erstellten Datensatz, und konfigurieren Sie diese Parameter:

Parameter	Beschreibung
IP-Adresse	Die Avi-IP-Adresse
Anmeldeinformationsalias	Den Namen des oben erstellten Anmeldeinformationsalias

- Für das Muster „Avi Load Balancer Controller“ und das Muster „Avi Load Balancer Controller - Session-based“ erteilen Sie einem Benutzer Berechtigungen zum Senden der folgenden API-Abfragen.
  - /api/cluster
  - /api/serviceengine
  - /api/pool
  - /api/vimgrvmruntime?controller_vm=true
  - /api/cloud
  - /api/virtualservice
  - /api/serviceenginegroup
  - /api/gslbservice
  - /api/tenant
- Für das Muster „Avi Load Balancer VIP“:
  - Erstellen Sie einen Serviceinstanz an.
  - Vor der Verwendung des Musters „Avi Load Balancer VIP“ verwenden Sie eines der Muster für die horizontale Avi-Lastenausgleicherkennung, um die Avi-Infrastruktur zu finden.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Avi Controller [cmdb_ci_avi_controller]	
Name [name]	Name des Avi-Controllers
Vollständig qualifizierter Domänenname [fqdn]	Hostname des virtuellen Computers (VM)
IP-Adresse [ip_address]	IP-Adresse des FQDN
Avi-Service-Engine [cmdb_ci_avi_service_engine]	
Name [name]	Name der Avi-Service-Engine
IP-Adresse [ip_address]	IP-Adresse der Avi-Service-Engine
Version [version]	Version der Avi-Service-Engine
Objekt-ID [object_id]	Eindeutiger Bezeichner der Avi-Service-Engine

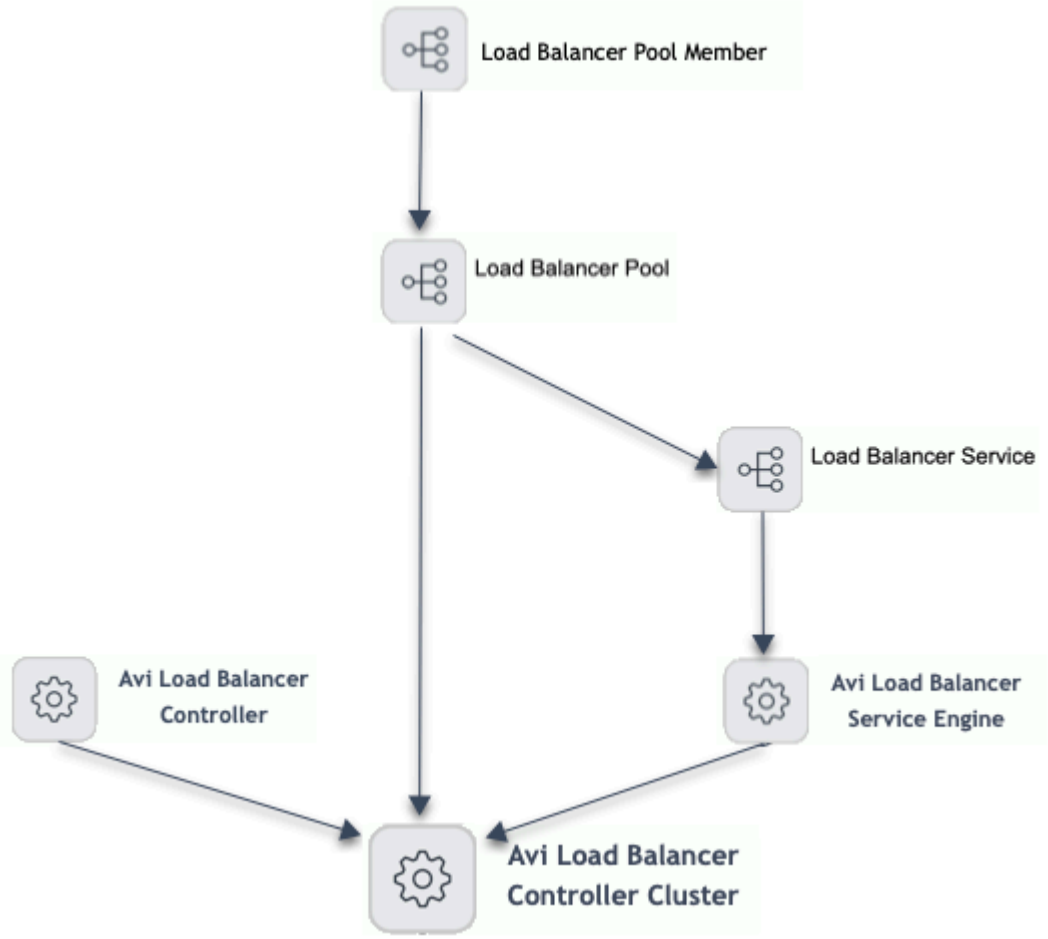
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Avi-Controller-Cluster [cmdb_ci_avi_controller]	
Cluster-ID [cluster_id]	Eindeutiger Bezeichner des Avi Controller-Clusters
Name [name]	Name des Avi-Controller-Clusters
IP-Adresse [ip_address]	IP-Adresse des Hosts des Avi-Controller-Clusters
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Name des Pools von Lastenausgleichsmodulen
Server-ID [server_id]	Eindeutiger Bezeichner des Pools von Lastenausgleichsmodulen
Lastenausgleichsmethode [load_balancing_method]	Methode, die Avi Vantage zur Entscheidung über den Lastenausgleich verwendet. Das Muster übersetzt die Algorithmen wie folgt: • „LB_ALGORITHM_LEAST_CONNECTIONS“: „wenigste Verbindungen“ • „LB_ALGORITHM_ROUND_ROBIN“: „Round-Robin“ • „LB_ALGORITHM_FASTEST_RESPONSE“: „schnellste Antwort“ • „LB_ALGORITHM_CONSISTENT_HASH“: „konsistenter Hash“ • „LB_ALGORITHM_LEAST_LOAD“: „geringste Last“ • „LB_ALGORITHM_FEWEST_SERVERS“: „wenigste Server“ • „LB_ALGORITHM_RANDOM“: „zufällig“ • „LB_ALGORITHM_FEWEST_TASKS“: „wenigste Aufgaben“ • „LB_ALGORITHM_NEAREST_SERVER“: „nächstgelegener Server“
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name des Poolmitglieds @ Name des Pools
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Load Balancer-Service [cmdb_ci_lb_service]	
Name [name]	Name der virtuellen IP (VIP)
IP-Adresse [ip_address]	IP-Adresse der VIP
Objekt-ID [object_id]	Eindeutiger Bezeichner der VIP
Port [port]	Port der Host-VM
Avi-Mandant [cmdb_ci_avi_tenant]	
name	Name des Mandanten
object_id	object_id des Mandanten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
tenant_url	URL zum Mandanten

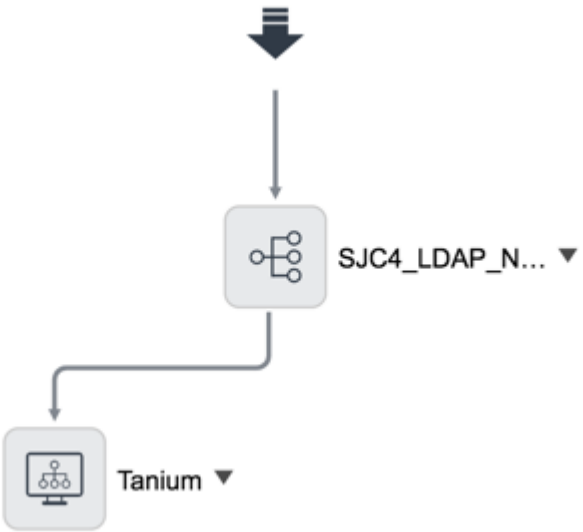
Die Dependency Views-Zuordnung zeigt die erkannten Lastenausgleichsmodul-CIs und deren Beziehung untereinander.



Die folgende Abbildung zeigt die Ergebnisse einer Erkennung von oben nach unten, die das Muster „Avi Load Balancer VIP“ verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von oben nach unten mithilfe des Musters „Avi Load Balancer VIP“



CI-Beziehungen

Die folgenden Beziehungen werden zur Unterstützung der Avi-Lastenausgleicherkennung erstellt:

CI	Beziehung	CI
Avi-Controller-Cluster [cmdb_ci_avi_controller]	Cluster von::Cluster	Avi Controller [cmdb_ci_avi_controller]
Avi-Mandant [cmdb_ci_avi_tenant]	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
	Enthält::Enthalten in	Load Balancer-Service [cmdb_ci_lb_service]
Load Balancer-Pool [cmdb_ci_lb_pool]	Verwendet von::Verwendet	Load Balancer-Service [cmdb_ci_lb_service]
	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Avi-Service-Engine [cmdb_ci_avi_service_engine]	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
Avi Controller [cmdb_ci_avi_controller]	Enthält::Enthalten in	Avi-Service-Engine [cmdb_ci_avi_service_engine]
Load Balancer-Service [cmdb_ci_lb_service]	Verwendet von::Verwendet	Avi-Service-Engine [cmdb_ci_avi_service_engine]
	Wird ausgeführt auf::Wird ausgeführt	Avi-Controller-Cluster [cmdb_ci_avi_controller]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Nur Referenz	Avi-Controller-Cluster [cmdb_ci_avi_controller]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung

Wenn die Erkennung von oben nach unten des Avi-Lastenausgleichsmoduls fehlschlägt, finden Sie eine Problemumgehung im KB-Artikel KB0824019 .

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Nächste Generation Cisco Firewall-Discovery

Die ServiceNow Discovery Die Anwendung verwendet das Cisco Firewall-Muster der nächsten Generation, um zu finden Cisco Firewalls. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Cisco-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der ServiceNow AI Platform® mit Madrid-Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .
- Fügen Sie der ServiceNow-Instanz den OID-Datensatz des SNMP-Systems für das Cisco-Gerät hinzu. Aktualisieren Sie Folgendes:
  - Klassifizierer: Cisco-Firewall
  - Klasse: Cisco-Firewall-Gerät
- Stellen Sie das Muster wie folgt bereit:
  1. Herunterladen und installieren Firewall-Erweiterungsklassen Von ServiceNow Store. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind.
  2. Laden Sie herunter, und installieren Sie Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store .
  3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Cisco-Firewall-Musters der nächsten Generation.

Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]

Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer des Geräts
Name [name]	Administrativ zugewiesener Name für diesen verwalteten Knoten. Gemäß Konvention ist dies der vollqualifizierte Domänenname des Knotens (FQDN).
IP-Adresse [ip_address]	IP-Adresse des Geräts.
Firmware-Version [Firmware-Version]	Firmware-Version
Vollständig qualifizierter Domänenname [fqdn]	FQDN des Geräts.
Hersteller [manufacturer]	Gerätehersteller
Modell-ID [model_id]	Gerätemodellname.
Hardware-Betriebssystem [Hardware_os]	Betriebssystem (OS), das auf der Hardware ausgeführt wird.
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Beschreibung [short_description]	Kurzbeschreibung von Cisco Gerät.
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco] (Fortsetzung)

Feld	Beschreibung
Hardwarestatus [hardware_status]	Detaillierte Beschreibung des aktuellen Status der Ressource.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Cisco Firewall.
Netzmaske [netmask]	Netzmaske von Cisco Firewall.
NIC [nic]	Verweist auf die Tabelle „Netzwerkadapter“ [cmdb_ci_Network_Adapter].

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „Cisco-Firewall-Gerät“ [cmdb_ci_Firewall_device_cisco].

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

Diese Abhängigkeitsansichten-Zuordnung auf dem Cisco Firewall-CI zeigt das Cisco Firewall-Gerät.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Cisco Firewall-Discovery.

CI	Beziehung	CI
Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]
Routerschnittstelle [dscy_router_interface]	Referenzen	Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]
Seriennummer [cmdb_serial_number]	Referenzen	Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]

Cisco Switch-Discovery für Wireless Access Point (WAP)

Die ServiceNow Discovery Die Anwendung verwendet die Cisco WAPs-Erweiterung, um Wireless Access Points (WAPs) zu finden, die von gesteuert werden CiscoNetzwerk-Switch. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Diese Erweiterung erweitert das Erkennungsmuster „Network Switch“. Weitere Informationen finden Sie unter Netzwerk-Switch- und Router-Discovery.

Discovery verwendet die Cisco WAP-Erweiterung zum Ausführen der horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Voraussetzungen im Zusammenhang mit der Erkennung von Netzwerk-Switches finden Sie unter Netzwerk-Switch- und Router-Discovery.

Darüber hinaus müssen diese Voraussetzungen für die Cisco WAP-Erweiterung erfüllt sein:

- Berechtigung zum Abfragen der OID: 1.3.6.1.4.1.14179.2.2.1.1.
- Der Client muss in der Lage sein, Erkennungsmuster auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

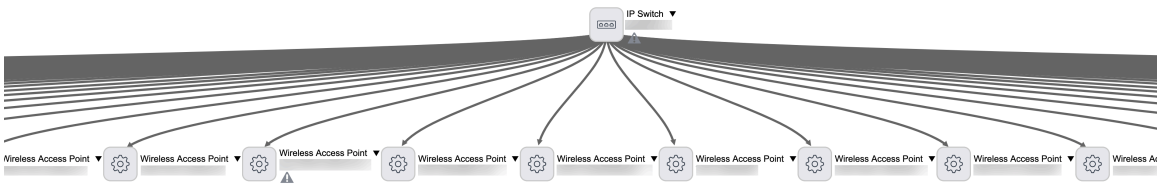
- Der Client muss einen verwenden CiscoNetzwerk-Switch.
- Der Client muss SNMP-Zugriff auf haben CiscoNetzwerk-Switch, der die WAP-Geräte steuert.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die von der Cisco WAP-Erweiterung erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabellen und Felder	Beschreibung
Haupt-CI-Klasse [cmdb_ci_wap_network]	
Name [name]	Name, der dem WAP zugewiesen wurde. Gesammelt von bsnAPName.
MAC-Adresse [mac_address]	Die MAC-Adresse des WAP. Gesammelt von bsnAPDot3MacAddress.
IP-Adresse [ip_address]	Die IP-Adresse des WAP. Gesammelt von bsnApIpAddress.
Firmware-Version [Firmware-Version]	IOS-Version des IOS CiscoWAP. Gesammelt von bsnAPIOSVersion.
Seriennummer [serial_number]	WAP-Seriennummer Gesammelt von bsnAPSerialNumber.
Modellnummer [model_number]	WAP-Modell. Gesammelt von bsnAPModel.
snmp_sys_location	Benutzerdefinierter Speicherort des WAP. Gesammelt von bsnAPLocation.
Hersteller [manufacturer]	Hersteller des WAP (Cisco).

Die Zuordnung der Abhängigkeitsansichten zeigt alle erkannten an CiscoWAP-CIs und die Beziehungen zwischen ihnen.



CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt CiscoWAPS-Discovery:

CI	Beziehung	CI
cmdb_ci_ip_switch	Controller für::Gesteuert von	cmdb_ci_wap_network

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Citrix NetScaler-SDX-Discovery

Die ServiceNow Discovery Anwendung kann erkennen Citrix NetScaler-SDX-Geräte, die das Citrix NetScaler-SDX-Muster verwenden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können dieses Muster für verwenden ServiceNow AI Platform® Beginnend mit Quebec Release.

Der in Quebec eingeführte neue Klassifizierungsmechanismus löst das Muster aus. Der Klassifizierungsmechanismus verhindert, dass die gesamte Probe ausfällt, wenn eine untergeordnete Probe in einer Mehrfachprobe ausfällt.

Der Klassifizierungsmechanismus enthält eine neue Tabelle „trigger_probe_m2m“, die definiert, welche Klassifizierungs-Probe in Bezug auf das relevante Protokoll ausgelöst werden soll. Für dieses Muster wird die interaktive Probe Shell über das Protokoll *ssh* ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen installiert sind

- CMDB CI-Klassenmodelle (Version 1,0.20)
- Muster für Discovery und Service-Mapping (Version 1,0.72)

SSH-Anmeldeinformationen erstellen

Erstellen Sie SSH-Anmeldeinformationen für Citrix NetScaler-SDX-Gerät. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Überprüfen Sie die Berechtigungen für die folgenden Befehle

Überprüfen Sie, ob Discovery Anwender wurde in hinzugefügt ServiceNow AI Platform Instanz kann die folgenden Befehle ausführen:

Befehl	Beschreibung
`Vmdevice anzeigen`	VM-Instanzen abrufen.
`Hardware anzeigen`	Bietet einen schnellen Überblick über alle konfigurierbaren Einstellungen für Citrix NetScaler-SDX-Geräte.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Citrix NetScaler SDX-Musters.

Citrix NetScaler SDX [cmdb_ci_citrix_netscaler_sdx]

Feld	Beschreibung
Name [name]	Der Name des Citrix NetScaler-SDX-Gerät.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

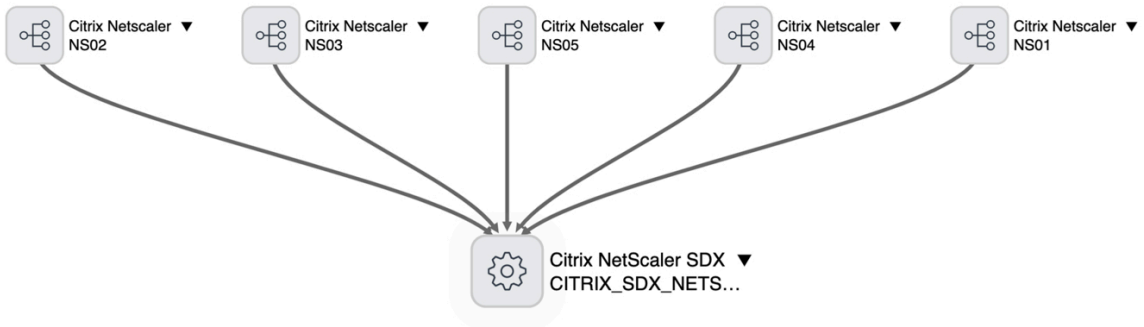
Citrix NetScaler SDX [cmdb_ci_citrix_netscaler_sdx] (Fortsetzung)

Feld	Beschreibung
Seriennummer [serial_number]	Die Seriennummer des Citrix NetScaler-SDX-Gerät.
IP-Adresse [ip_address]	Die IP-Adresse des Citrix NetScaler-SDX-Gerät.
Objekt-ID [object_id]	Der CI-Bezeichner des Citrix NetScaler-SDX-Gerät, das Serial_number und ip_address enthält.
Beschreibung [short_description]	Die Beschreibung von Citrix NetScaler-SDX-Gerät.
BS-Version [os_Version]	Die Version von Citrix NetScaler-SDX-Gerät.

Citrix Netscaler [cmdb_ci_lb_netscaler]

Feld	Beschreibung
Name [name]	Der Name des Citrix NetScaler-Lastenausgleichsmodul.
Seriennummer [serial_number]	Die Seriennummer des Citrix NetScaler-Lastenausgleichsmodul.
IP-Adresse [ip_address]	Die IP-Adresse des Citrix NetScaler-Lastenausgleichsmodul.

Auf der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten anzeigen Citrix NetScaler-SDX-Ressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen.



CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Citrix NetScaler-SDX-Discovery:

CI	Beziehung	CI
Citrix Netscaler [cmdb_ci_lb_netscaler]	Registriert auf::Hat sich registriert	Citrix NetScaler SDX [cmdb_ci_citrix_netscaler_sdx]

Citrix Xen-Hyper-V-Discovery

ServiceNow Discovery verwendet das Citrix Xen Hyper-V-Muster, um Instanzen zu suchen und zuzuordnen. Erkennen Sie diese Ressourcen, indem Sie die Musteranwendungen aus installieren ServiceNow Speichern und hinzufügen Citrix Xen Hyper-V zum Erweiterungsabschnitt des Linux-Servermusters.

Verwenden Sie die Befehle Xen (XE) und (XL), um zu erkennen Citrix Xen Hyper-V, seine Komponenten und die entsprechenden Attribute. Suchen Sie Informationen zu Hyper-V-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Server, zugeordneten Pools, VMs, Netzwerk und Speicher und deren Beziehungen zu neuen und vorhandenen CIs.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die RBAC-Rolle des Pooladministrators

Diese Rolle ist für den SSH-Zugriff auf den Linux-Server erforderlich, der den Hypervisor hostet, und zum Ausführen aller erforderlichen Befehle zum Extrahieren von Informationen aus der Hypervisor-Umgebung. Weitere Informationen zu RBAC-Rollenberechtigungen oder zum Hinzufügen von Citrix-Anwendern zu einer Domäne und zum Zuweisen von Rollen finden Sie unter Citrix-Dokumentation .

Verifizieren MID-Server Erreichbarkeit

Verifizieren MID-Server Ist für das Zielgerät zugänglich.

Erstellen Sie SSH-Anmeldeinformationen mit Zugriff auf das Ziel Linux Host

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen

Erstellen Sie einen Erweiterungsabschnitt nach dem Linux Server-Muster

Erstellen Sie einen Erweiterungsabschnitt nach dem Linux Server-Muster, und ordnen Sie zu **Citrix Xen HyperV** Muster, das nach der Ausführung des Linux Server-Discovery-Musters ausgelöst werden soll. Weitere Informationen zum Erstellen von Erweiterungsabschnitten finden Sie unter Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Citrix Xen HyperV-Musters.

Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]

Feld	Beschreibung
object_id	UUID des Hyper-V-Ressourcenpools
name	Name des Hyper-V-Ressourcenpools
Default_sr	Das Standard-Speicher-Repository ist, in dem die VDIs standardmäßig gespeichert werden

Hyper-V-Server [cmdb_ci_hyper_v_server]

Feld	Beschreibung
object_id	UUID des Hyper-V-Servers

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-Server [cmdb_ci_hyper_v_server] (Fortsetzung)

Feld	Beschreibung
name	Name des Hyper-V-Servers im Format NAME@Hyper-V-Server
serial_number	Seriennummer des Linux-Servers, auf dem der Citrix Xen Hyper-V-Server ausgeführt wird, im Format SERIAL-NUMBER_Hyper_V_Server, um sich vom Linux-Server zu unterscheiden
manufacturer	Lieferant des Hyper-V-Servers
model_id	Modell-ID des Hyper-V-Servers
short_description	Beschreibung des Hyper-V-Servers
os	Betriebssystem des Hyper-V-Servers
os_version	Version des Betriebssystems des Hyper-V-Servers
host_name	Hostname des Hyper-V-Servers
ip_address	IP-Adresse des Hyper-V-Servers
virtual	Legen Sie diese Option auf „falsch“ fest, da dieser Wert von Rechnern verwendet wird, um die Kennzeichnung „IsVirtual“ im Dashboard (SAM) auszufüllen.
free_memory	Verfügbarer Arbeitsspeicher des Hyper-V-Servers
total_memory	Gesamtspeicher des Hyper-V-Servers
Edition	Edition des Hyper-V-Servers
cpu_core_count	Die Anzahl der Kerne pro physische CPU
cpu_count	Anzahl der CPUs insgesamt
ram	RAM-Arbeitsspeicher insgesamt in MB
cpu_speed	CPU-Geschwindigkeit in MHz
cpu_manufacturer	Hersteller der CPU
cpu_type	Typ der CPU
cpu_core_thread	Die Anzahl der Threads pro CPU-Kern

Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]

Feld	Beschreibung
object_id	UUID des Hyper-V-Servers
name	Name des Hyper-V-Servers
Status	Status der Hyper-V-Instanz
ip_address	IP-Adresse der Hyper-V-Instanz
host_id	Die UUID des Hosts, auf dem sich die Instanz befindet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance] (Fortsetzung)

Feld	Beschreibung
baseboard_serial	UUID der Hyper-V-Instanz
chassis_serial	UUID der Hyper-V-Instanz
bios_serial	UUID der Hyper-V-Instanz

Virtuelles Hyper-V-Netzwerk [cmdb_ci_Hyper_V_Network]

Feld	Beschreibung
object_id	UUID des virtuellen Hyper-V-Netzwerks
pif_UUID	UUID der physischen NIC
name	Name des virtuellen Hyper-V-Netzwerks
Brücke	Typ des Netzwerk-Setups: Entweder überbrückt oder nicht

Virtuelle Hyper-V-Netzwerkkomponente [cmdb_ci_Hyper_V_Network_comp]

Feld	Beschreibung
object_id	UUID der Hyper-V-Netzwerkkomponente
mac_address	MAC-Adresse der Hyper-V-Netzwerkkomponente
VM	UUID der Hyper-V-Instanz, der die Netzwerkkomponente zugeordnet ist
name	Name der Hyper-V-Netzwerkkomponente

Hyper-V-Speicher [cmdb_ci_hyper_v_storage]

Feld	Beschreibung
object_id	LUN des Hyper-V-Speichers
name	Name des Hyper-V-Speichers
Beschreibung	Beschreibung des Hyper-V-Speichers
type	Typ des Speichers (SR)
vm_object_ID	UUID der Hyper-V-Instanz, der der Speicher zugeordnet ist
vm_ID	UUID der Hyper-V-Instanz, der der Speicher zugeordnet ist

Hyper-V-Speicherkomponente [cmdb_ci_hyper_v_storage_comp]

Feld	Beschreibung
object_id	UUID des virtuellen Datenträger-Images (VDI)
name	Name des virtuellen Datenträger-Images (VDI)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-Speicherkomponente [cmdb_ci_hyper_v_storage_comp] (Fortsetzung)

Feld	Beschreibung
Beschreibung	Beschreibung des Virtual Disk Image (VDI)
type	Typ der Speicherkomponente (VDI)
Kapazität	Gesamtkapazität des virtuellen Datenträger-Images (VDI)
location_id	Speicherort des virtuellen Datenträger-Images (VDI)
Ist_a_Snapshot	Angabe, ob das Image des virtuellen Laufwerks (Virtual Disk Image, VDI) ein Snapshot ist oder nicht
Snapshot_of	Angabe des VDI-Snapshots der Datenträger
Snapshot_time	Zeitpunkt der Snapshot-Erstellung
sr_object_ID	UUID des Speicher-Repositorys, dem das virtuelle Datenträger-Image (VDI) zugeordnet ist
vm_object_ID	UUID der virtuellen Maschine, die dem Image des virtuellen Laufwerks (Virtual Disk Image, VDI) zugeordnet ist

CI-Beziehungen

Von Citrix Xen Hyper-V-Erkennung erstellte Beziehungen

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_hyper_v_resource_pool	Enthält :: Enthalten in	cmdb_ci_hyper_v_server
cmdb_ci_hyper_v_server	Wird ausgeführt am :: Wird ausgeführt	cmdb_ci_linux_server
cmdb_ci_hyper_v_network	Stellt bereit: Bereitgestellt von	cmdb_ci_hyper_v_server
cmdb_ci_Hyper_V_Network_comp	Stellt bereit: Bereitgestellt von	cmdb_ci_hyper_v_server
cmdb_ci_hyper_v_instance	Verbunden durch :: Verbindet	cmdb_ci_Hyper_V_Network_comp
cmdb_ci_hyper_v_resource_pool	Referenz	cmdb_ci_hyper_v_storage
cmdb_ci_hyper_v_instance	Enthält :: Enthalten in	cmdb_ci_hyper_v_storage
cmdb_ci_Hyper_V_Storage_comp	Verwaltet von :: Verwaltet	cmdb_ci_hyper_v_storage
cmdb_ci_Hyper_V_Storage_comp	Referenz	cmdb_ci_hyper_v_instance
cmdb_ci_hyper_v_server	Ressourcen definieren für :: Ruft Ressourcen von ab	cmdb_ci_hyper_v_resource_pool
cmdb_ci_hyper_v_instance	Registriert am :: Hat registriert	cmdb_ci_hyper_v_server

Cloudian-Speicher-Erkennung

Das Erkennungsmuster Cloudian Storage wird von ServiceNow Discovery dazu verwendet, Cloudian-Server und zugehörige Laufwerke zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Patterns-Anwendung aus dem ServiceNow Store installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloudian Storage System-Muster werden von Discovery dazu verwendet, Cloudian Storage-Systemdaten zu finden. Die Erkennung dieser Ressourcen erfordert die Installation der Anwendungen Discovery- und Service-Mapping-Muster und CMDB-CI-Klassenmodelle aus dem ServiceNow Speichern, da jede Anwendung von der anderen abhängig ist. Sie können die Muster zur Erkennung von Cloudian Storage-Komponenten auf der ServiceNow AI Platform mit dem Paris-Release oder höher verwenden.

Cloudian ist ein Unternehmen im Bereich softwaredefinierter Datenspeicher. Cloudian bietet sofort einsatzbereite, verteilte, softwaredefinierte, S3-kompatible Objektspeicherlösungen.

Cloudian Hyperstore-Software : Stellen Sie das CentOS-Betriebssystem, zugehörige Pakete und Binärdateien der HyperStore-Software auf dem HyperStore-Knoten bereit.

Cloudian Hyperstore-Knoten: Dies ist ein unabhängiger Hardwareserver, auf dem Cloudian Hyperstore-Software auf einem Server nach Branchenstandard oder einer VM bereitgestellt oder auf einer Cloudian Hyperstore-Appliance vorinstalliert ist.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Damit ein Gerät als Cloudian-Server erkannt wird, muss der Befehl **/bin/systemctl status cloudian-s3** gültige Antworten zurückgeben und das **Cloudian HyperStore-Speichersystem** enthalten. Wenn dies nicht der Fall ist, wird das Gerät als Linux-Server erkannt.

- Vergewissern Sie sich, dass der Client Discover-Muster verwendet.
- Legen Sie **SSH**-Anmeldeinformationen für den Cloudian Storage-Server fest.
- Stellen Sie sicher, dass der MID Server Zugriff auf das Zielgerät hat.
- Stellen Sie sicher, dass der Discovery-Benutzer über die richtigen Berechtigungen zum Ausführen von Befehlen verfügt.
- Installieren Sie die folgenden Plugins:
- ○ Plugin „CMDB CI Class Models“ (Version 1.31.0 oder höher)
  - ○ Plugin „Discovery and Service Mapping Patterns“ (Version 1.0.84 oder höher)
  - ○ Discovery and Service Mapping Patterns: (sn_itom_pattern) Version 1.0.84 und abhängiges Plugin **CMDB CI Class Models** (sn_cmdb_ci_class) Version 1.31.0 (Content-Release von Oktober)

Berechtigungen

Stellen Sie sicher, dass die Cloudian Hyperstore-Software auf CentOS- oder RHEL-Servern bereitgestellt wird. Die Konfigurationen der Anmeldeinformationen sind dieselben wie für einen Linux-Server.

Konfigurieren Sie **SSH**-Anmeldeinformationen für den Cloudian Storage-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery ausführen

Um das Cloudian Storage-System zu erkennen, erstellen Sie einen Discovery-Zeitplan mit der IP-Adresse des Cloudian Storage-Servers als Ziel. Stellen Sie sicher, dass die von Ihnen konfigurierten **SSH**-Anmeldeinformationen auf den Cloudian-Server zugreifen können.

Von Discovery während der horizontalen Erkennung erfasste Daten

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
name	
serial_number	
ip_address	
manufacturer	
model_id	
short_description	
os_version	
os	
ram	
cpu_manufacturer	
CPU-Name	
cpu_core_count	
cpu_type	

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
name	
device_id	
storage_type	
size_bytes	
manufacturer	
model_id	
computer [Reference cmdb_ci_storage_server]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateisystem [cmdb_ci_file_system]

Feld	Beschreibung
name	
size_bytes	
free_space_bytes	
file_system	
mount_point	
computer [Reference cmdb_ci_storage_server]	
provided_by [Reference cmdb_ci_disk]	

Netzwerkadapter [cmdb_ci_network_adapter]

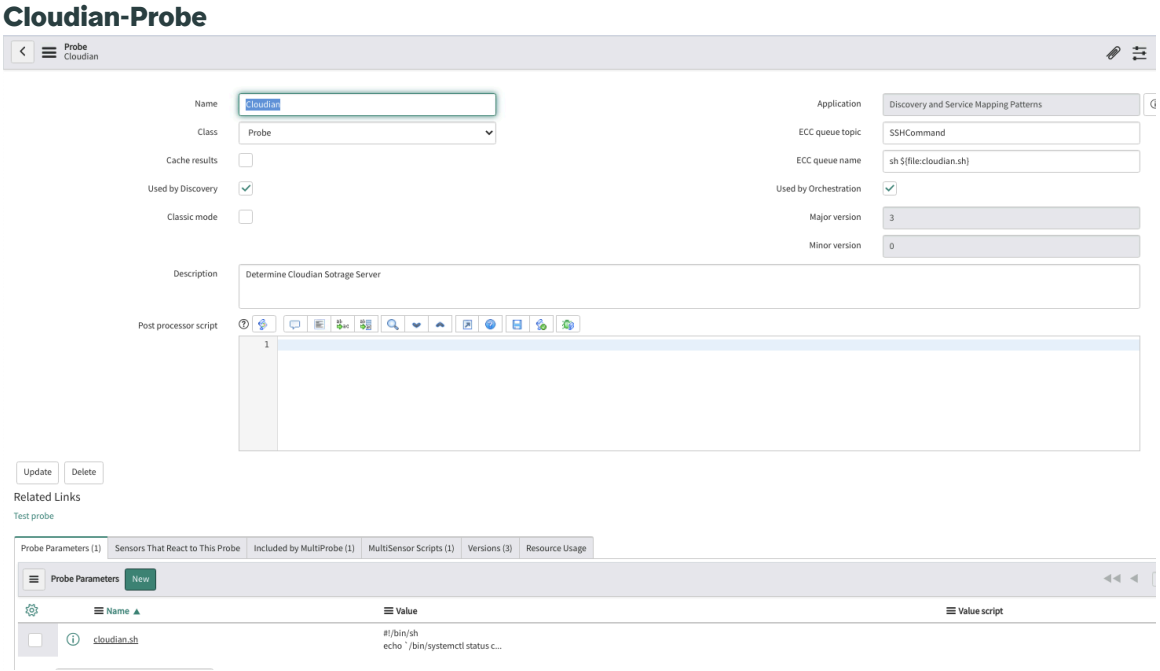
Feld	Beschreibung
name	
ip_address	
netmask	
mac_address	
cmdb_ci [Reference cmdb_ci_storage_server]	

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
ip_address	
netmask	
nic [Reference cmdb_ci_network_adapter]	

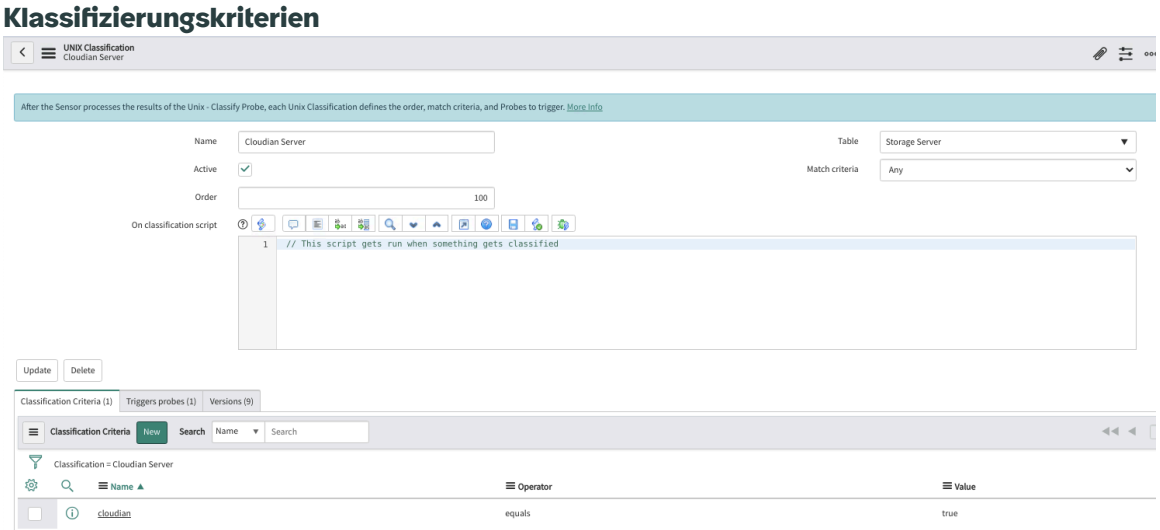
Die **Cloudian**-Probe wird in der Multi-Probe **Unix-Classify** erstellt. Die Probe **Cloudian** führt den Befehl **bin/systemctl status cloudian-s3** aus und prüft, ob die Ausgabe das **Cloudian HyperStore-Speichersystem** enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Bei der Unix-Klassifizierung wird der Klassifizierer **Cloudian-Server** vor dem **Linux-Klassifizierer** ausgeführt. Vom Cloudian-Klassifizierer werden Datensätze in der Tabelle [cmdb_ci_storage_server] erstellt. Von diesem Klassifizierer wird das Cloudian Storage System-Muster aufgerufen.

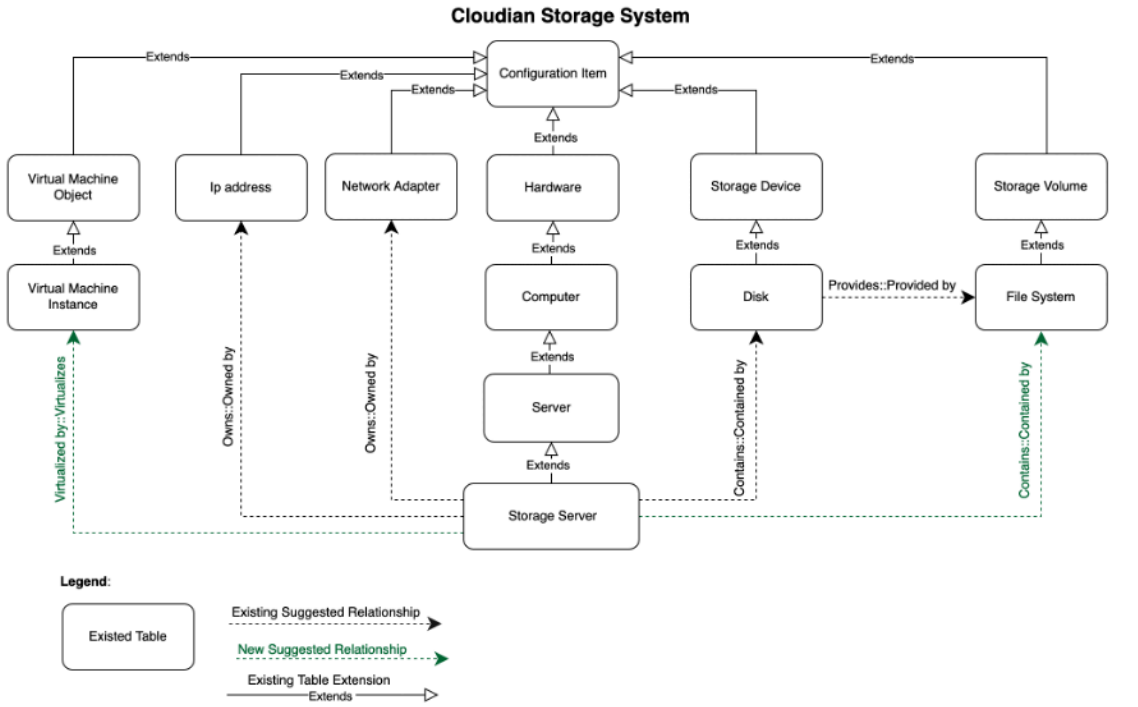
Klassifizierungskriterien



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

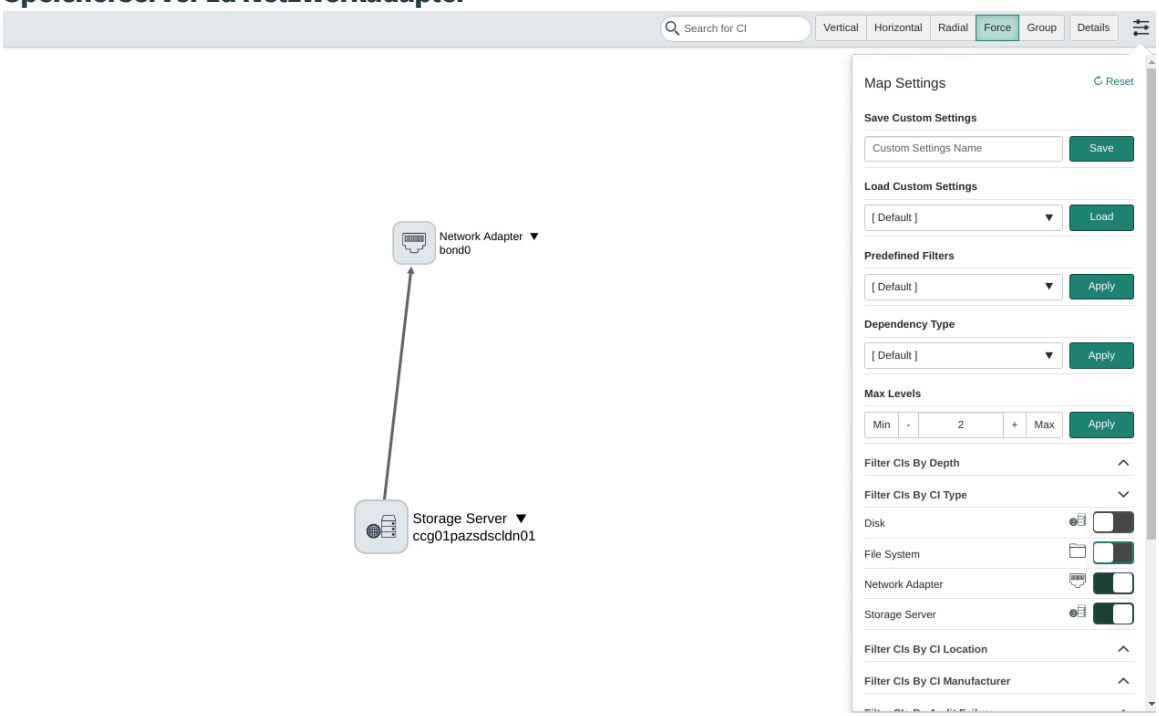
CMDB-Datenmodell

CMDB-Datenmodell



Speicherserver zu Netzwerkadapter

Speicherserver zu Netzwerkadapter

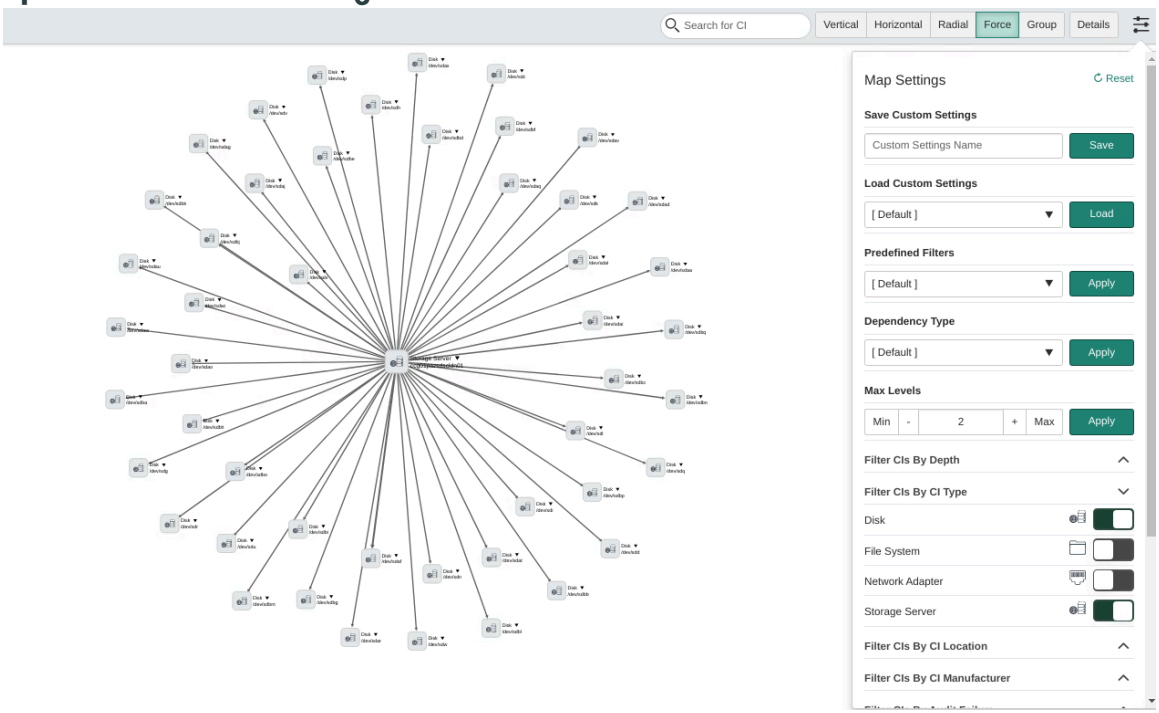


Speicherserver zu Datenträger

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

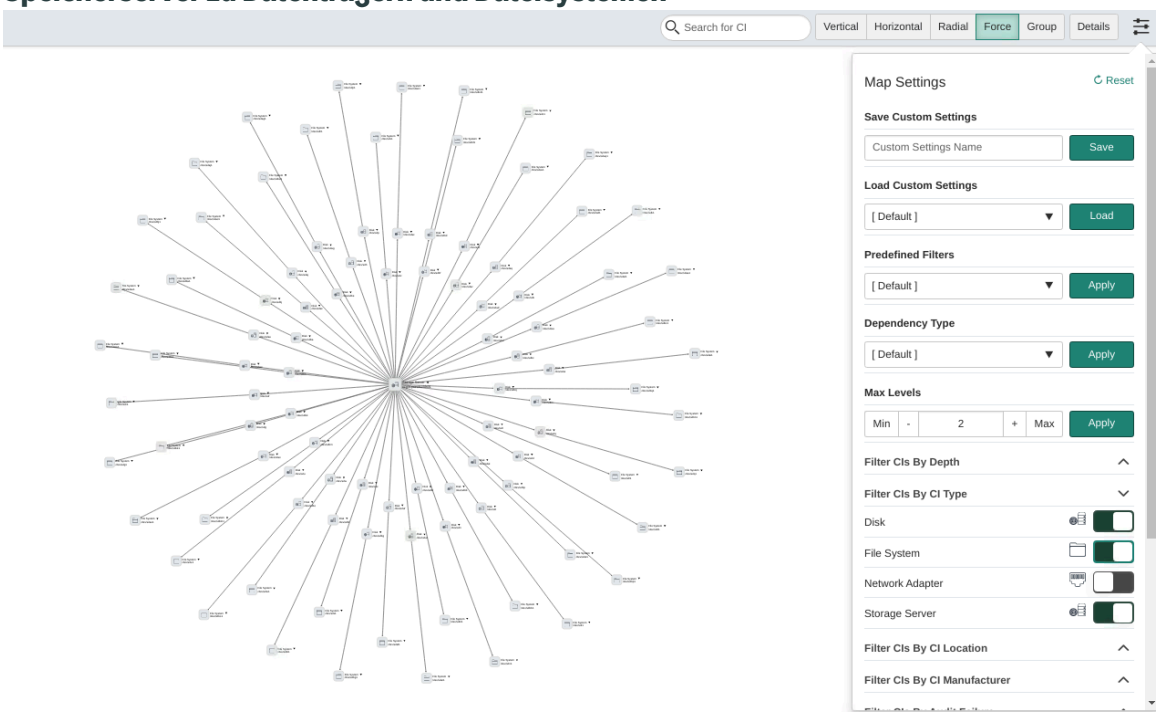
Automatische Übersetzung

Speicherserver zu Datenträger



Speicherserver zu Datenträgern und Dateisystemen

Speicherserver zu Datenträgern und Dateisystemen



CI-Beziehungen

Vom Cloudian Storage-Muster erstellte Beziehungen

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_network_adapter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_file_system
cmdb_ci_storage_server	Virtualisiert von::Virtualisiert	cmdb_ci_vm_instance
cmdb_ci_disk	Stellt bereit::Bereitgestellt von	cmdb_ci_file_system

Cohesity Speichersystem-Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Cohesity Storage System-Muster, um Cluster, Knoten und Gehäuse für zu finden Cohesity Datenplattform. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Cohesity Entwickelt Software, die zur Konsolidierung und Vereinfachung der Datenverwaltung verwendet wird, und umfasst Analytics-Funktionen. Ihre Software löst auch das Problem der Massendatenfragmentierung mit Daten, die sich über mehrere Systeme oder Cloud-Anbieter erstrecken.

Das Hauptprodukt des Unternehmens, DataPlatform, ist eine hyperkonvergierte Software, mit der Unternehmen eine Vielzahl von Arbeitsauslastungen konsolidieren können, einschließlich Sicherungen, Archiven, Tests, Entwicklung, und Analytics-Daten auf einer einzigen Cloud-nativen Plattform. Es funktioniert mit physischen Servern und virtuellen Computern.

Cohesity Erweitert Sicherungsfunktionen auf verteilte NoSQL-Arbeitsauslastungsdatenbanken wie MongoDB, Apache Cassandra, Couchbase und Apache HBase sowie Apache Hadoop-Daten in HDFS-Datenspeichern (Hadoop Distributed File System).

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- CMDB CI-Klassenmodelle, Ab Version 1.37.0
- Muster für Discovery und Service-Mapping, Ab Version 1.0.91

Verifizieren MID-Server Konfiguration

Verifizieren Sie MID-Server Ist auf „aktiv“ festgelegt und für erreichbar Cohesity Speichercluster.

Überprüfen Sie die API-Berechtigungen

Stellen Sie sicher, dass Sie über einen Standardauthentifizierungs-Account mit den richtigen Berechtigungen für die folgenden API-Aufrufe verfügen:

- `https://" + ${Cluster_ip} + "/irisservices/api/v1/public/Cluster?fetchStats=wahr`
- `https://" + ${Cluster_ip} + "/irisservices/api/v1/nexus/Cluster/Status`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- https://" + ${Cluster_ip} + "/irisservices/api/v1/public/nodes?fetchStats=wahr
- https://" + nodeIp + "/irisservices/api/v1/Nexus/node/Hardware_info

Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung

Weitere Informationen finden Sie unter Erstellen Sie einen Alias für Anmeldeinformationen für die Standardauthentifizierung Cohesity Speichersystem-Discovery.

Zeitplan für Erkennung ohne Server erstellen

Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für Cohesity Speichersystem-Discovery.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Cohesity Storage System-Musters.

Cohesity-Cluster [cmdb_ci_cohesity_Cluster]

Bezeichnung	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Clusters.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (FQDN) des Clusters.

Cohesity-Knoten [cmdb_ci_cohesity_node]

Bezeichnung	Feldname
Hersteller [manufacturer]	Hersteller des Clusterknotens, der sein könnte Cohesity Oder Drittpartei.
Vollständig qualifizierter Domänenname [fqdn]	FQDN des Knotens im Cluster.
Betriebsstatus [operational_status]	Betriebsstatus. Standardwert: Installiert.
Beschreibung [short_description]	Beschreibung des Clusterknotens: Cohesity Backup Server.

Gehäuse [cmdb_ci_Chassis]

Bezeichnung	Feldname
Hersteller [manufacturer]	Hersteller des Gehäuses.
Beschreibung [short_description]	Beschreibung des Gehäuses: Cohesity-Gehäuse.
Seriennummer [serial_number]	Seriennummer des Gehäuses.

IP-Adresse [cmdb_ci_ip_address]

Bezeichnung	Feldname
Name [name]	Name des Cohesity Knoten.
IP-Adresse [ip_address]	IP-Adresse des Cohesity Knoten.
IP-Version [ip_Version]	IP-Version von Cohesity Knoten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Cohesity Speichersystem-Discovery.

CI	Beziehungstyp	CI
Cohesity-Knoten [cmdb_ci_cohesity_node]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Cohesity-Knoten [cmdb_ci_cohesity_node]	Cluster von::Cluster	Cohesity-Cluster [cmdb_ci_cohesity_Cluster]
Cohesity-Knoten [cmdb_ci_cohesity_node]	Gehostet auf::Hostet	Gehäuse [cmdb_ci_Chassis]

Erstellen Sie einen Alias für Anmeldeinformationen für die Standardauthentifizierung Cohesity Speichersystem-Discovery

Erstellen Sie einen Alias, und fügen Sie ihn den Anmeldeinformationen für die Standardauthentifizierung hinzu, um es zu erkennen Cohesity Speichersysteme.

Vorbereitungen

Stellen Sie sicher, dass Sie über einen Standardauthentifizierungs-Account mit den richtigen Berechtigungen verfügen. Weitere Informationen finden Sie unter Überprüfen Sie die API-Berechtigungen Abschnitt in Cohesity Speichersystem-Discovery.

Erforderliche Rolle: discovery_admin

Prozedur

1. Erstellen Sie einen Alias.
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
   b. Wählen Sie **Neu**.
   c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie aus **Anmeldeinformationen** Für den Aliastyp in **Typ** Feld.
   d. Wählen Sie **Absenden**.
2. Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den neuen Alias.
   a. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
   b. Wählen Sie **Neu**.
   c. Klicken Sie auf **Basisanmeldedaten**.
   d. Entsperren Sie **Anmeldeinformationsalias** Feld und wählen Sie den erstellten Alias aus.
   e. Konfigurieren Sie den Rest von **Anmeldeinformationen Für Standardauthentifizierung** Formularfelder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie **Absenden**.
Weitere Informationen zu Formularfeldern mit Anmeldeinformationen für Standardauthentifizierung finden Sie unter Virtual Server Interface .

Nächste Maßnahme

Erstellen Sie einen Zeitplan für eine Erkennung ohne Server. Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für Cohesity Speichersystem-Discovery.

Zugehörige Informationen

Cohesity Speichersystem-Discovery

Erstellen Sie einen serverlosen Zeitplan für Cohesity Speichersystem-Discovery

Erstellen Sie einen serverlosen Discovery-Zeitplan für die Erkennung Cohesity Speichersysteme.

Vorbereitungen

- Verifizieren Sie MID-Server Ist auf „aktiv“ festgelegt und ist erreichbar für Cohesity Speichercluster.
- Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für Anmeldeinformationen für die Standardauthentifizierung Cohesity Speichersystem-Discovery.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Erstellen Sie den Discovery-Zeitplandatensatz.
   a. Wählen Sie **Neu**.
   b. Füllen Sie im Formular die Felder aus.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Erkannt	Scan-Typ, der serverlos sein muss.
MID-Server verwenden	Name des MID-Server Zur Verwendung für diesen Zeitplan.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

   c. Wählen Sie **Absenden**.
3. Erstellen Sie das Ausführungsmuster.
   a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.
   b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll. Dies sollte das Cohesity Storage System-Muster sein.
Proxyhost	Vollständig qualifizierter Domänenname des Computers, auf dem ein Proxy-Server installiert ist, falls zutreffend. Dieses Feld muss leer bleiben.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

d. Wählen Sie **Absenden**.

4. Legen Sie die Parameter des Musterstartprogramms fest.

a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.

b. Füllen Sie im Formular die Felder aus.

Parameter	Wert
Cluster_ip	Die Cohesity Cluster-URL oder IP-Adresse.
Anmeldeinformationsalias	Name des von Ihnen erstellten Anmeldeinformationsalias.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Zugehörige Informationen

Cohesity Speichersystem-Discovery

ColdFusion-Erkennung

Die ServiceNow Discovery-Anwendung findet Adobe ColdFusion-Server und die Instanzen der auf ihnen ausgeführten ColdFusion-Anwendungen. Nur die ColdFusion-Version 2016 wird unterstützt. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Komponenten

Discovery und Service-Mapping verwenden die Muster `ColdFusion Application` und `ColdFusion Application Server`, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Das Muster `ColdFusion Application Server` wird vom Prozessklassifizierer ColdFusion Application Server für die horizontale Erkennung ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen, je nachdem, auf welchem Typ von Hostcomputer der ColdFusion-Server installiert ist:

- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen (für Linux-Computer)

Dateizugriff

Das Muster muss auf diese ColdFusion-Dateien zugreifen können:

Datei	Beschreibung
neo-runtime.xml	Diese Datei stellt die Zuordnung zwischen der URL und dem Arbeitsverzeichnispfad der Anwendung bereit.
Anwendung.cfc Und Anwendung.cfm	Diese Dateien enthalten die Anwendungsnamen.
neo-datasource.xml	Diese Datei enthält den Namen der Datenquelle, die in der Konfiguration der ColdFusion-Anwendung verwendet wird. Die Datenquellenreferenz ist in den Dateien application.cfc und application.cfm konfiguriert. **Hinweis:** Die Datenquelle wird nur für die Erkennung von oben nach unten verwendet.

Eingabepunkt

Für die Erkennung von oben nach unten verwenden Sie die vollständige URL oder IP-Adresse der Webanwendung als HTTP(S)-Endpunkt. Beispiel: https://my-website-on-coldfusion/path oder https:10.120.255.2555:8500/path

Während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
ColdFusion-Server [cmdb_ci_coldfusion_server]	
Installationsverzeichnis [installation_directory]	Der Name und die Version des ColdFusion-Servers sowie das Verzeichnis, in dem er installiert ist.
Name [name]	
Version [version]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Installationsverzeichnis [installation_directory]	Der Name der Anwendung sowie das Verzeichnis, in dem sie installiert ist.
Name [name]	

Hinweis: Cold-Fusion-Anwendungen [cmdb_ci_cf_application] sind benutzerdefinierte Anwendungen, die dieses Muster nicht erkennt.

CI-Beziehungen

CI	Beziehung	CI
cmdb_ci_cf_application	Enthält::Enthalten in	cmdb_ci_coldfusion_server
cmdb_ci_coldfusion_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_linux_server cmdb_ci_win_server cmdb_ci_osx_server

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von Adobe ColdFusion von oben nach unten im Kontext von Anwendungsservices durch. Service-Mapping erkennt die ausgehenden Datenquellenverbindungen von ColdFusion-Servern zu Datenbankinstanzen.

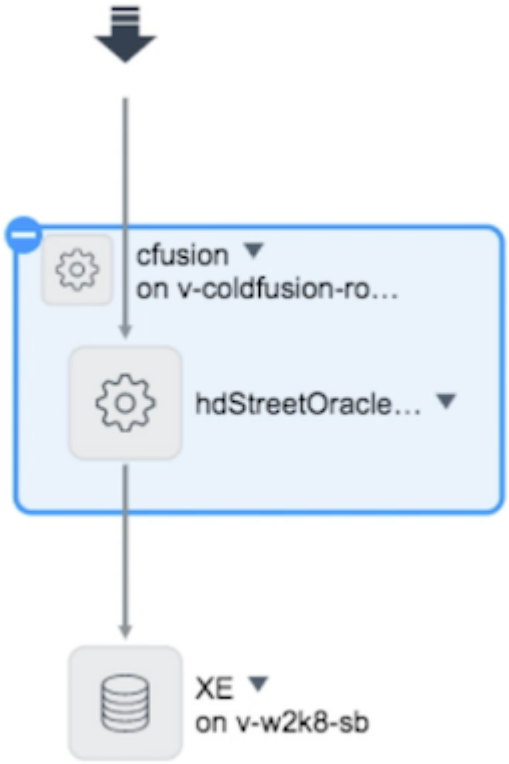
Beispiel

In diesem Beispiel zeigt die Anwendungsservicezuordnung die Ergebnisse einer Erkennung von oben nach unten des ColdFusion-Webanwendungsservices. Der Anwendungsservice besteht aus drei CIs:

- Der ColdFusion-Anwendungsserver heißt **cfusion**.
- Die ColdFusion-Anwendung **hdStreetOracle**.
- Eine Datenbank namens **XE**, mit der die ColdFusion-Anwendung eine Verbindung herstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ColdFusion-Servicezuordnung



Couchbase-Datenbankerkennung

Von der ServiceNow Discovery-Anwendung wird das Erkennungsmuster „Couchbase-Instanz“ dazu verwendet, Couchbase-Datenbankinstanzen und ihre Cluster zu finden und zuzuordnen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Die Couchbase-Datenbank ist eine verteilte Open Source-Datenbank, mit der JSON-Dokumente verwaltet werden. Mindestens eine Instanz eines Couchbase-Servers bildet einen Cluster. Daten und Services werden im gesamten Cluster gemeinsam genutzt.

Das Erkennungsmuster „Couchbase-Instanz“ wird von Discovery dazu verwendet, eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Sie können dieses Muster auf der ServiceNow AI Platform® mit Quebec-Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Die Couchbase-Datenbank muss auf einem Linux-Server installiert sein: Red Hat 7.9 oder Ubuntu 20.
- Stellen Sie sicher, dass auf den Servern CLI-Tools installiert sind.
- Konfigurieren Sie auf der ServiceNow AI Platform die SSH-Anmeldeinformationen . Konfigurieren Sie Anmeldeinformationen mit den folgenden Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Discovery-Berechtigungen
- Berechtigungen zum Auflisten von Dateien wie VERSION.txt in den Couchbase-Installationsordnern auf dem Linux-Server.
- Berechtigungen zum Ausführen des Befehls `systemctl status couchbase-server` auf dem Linux-Server.

Konfigurieren Sie auf der ServiceNow AI Platform Applicative-Anmeldeinformationen für die Tabelle cmdb_ci_couchbase_instance. Die Anmeldeinformationen müssen über ausreichende Berechtigungen verfügen, damit die folgenden Befehle auf dem Couchbase-Server ausgeführt werden können:

- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>/buckets`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>/remoteClusters`

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI (Couchbase-Instanz) [cmdb_ci_couchbase_instance]	
name	Name der Couchbase-Instanz.
install_directory	Der Installationsordner oder das Verzeichnis der Couchbase-Instanz.
config_file	Die Hauptkonfigurationsdatei der Couchbase-Instanz.
Version	Version der Couchbase-Instanz.
tcp_port	Der für den Zugriff auf die Befehlszeile und die REST-API verwendete Port.
Edition	Entweder die Basic- oder Enterprise-Edition der Couchbase-Instanz.
start_date	Das Datum, seit dem die Couchbase-Instanz aktiv ist.
Couchbase Cluster [cmdb_ci_couchbase_cluster]	
name	Name des Couchbase-Clusters.
cluster_id	ID des Couchbase-Clusters.
install_status	Installationsstatus, festgelegt auf „1“/„installiert“.
cluster_type	Betriebsstatus, festgelegt auf „1“/„funktionsfähig“.
Couchbase-Clusterknoten [cmdb _ci_couchbase_ cluster_node]	
name	Name des Clusterknotens.
install_status	Installationsstatus, festgelegt auf „1“/„installiert“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
operational_status	Betriebsstatus, festgelegt auf „1“/„funktionsfähig“.
node_status	Der Integritätsstatus des Clusterknotens.
node_encryption	Feld, das angibt, ob der Knoten verschlüsselt ist.
configured_host_name	Der konfigurierte Hostname des Clusterknotens.
host_name	Tatsächlicher Hostname des Clusterknotens.
total_memory	Der gesamte Speicher.
free_memory	Der freie Speicher.
mcd_reserved_memory	Der reservierte MCD-Speicher.
mcd_allocated_memory	Der zugeteilte MCD-Speicher.
couch_api_base	Die Couchbase-Basis-API-URL.
couch_api_base_https	Die Couchbase-HTTPS-API-URL.
recovery_type	Der Wiederherstellungstyp.
otpnode	Der OTP-Knoten.
node_uuid	Die UUID des Clusterknotens.
cluster_compatibility	Die Clusterkompatibilität des Clusterknotens.
Version	Die Version des Clusterknotens.
os	Das Betriebssystem des Clusterknotens.
cpu_count	Die CPU-Anzahl des Clusterknotens.
Edition	Die Clusterknoten-Edition. Die Edition ist die gleiche wie die der Couchbase-Instanz.
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	
name	Der Name des Couchbase-Buckets.
Cluster	Verweis auf das Couchbase-Cluster.
install_status	Installationsstatus, festgelegt auf „1“/„installiert“.
Couchbase-Clusterressource [cmdb_ci_couchbase_cluster_resource]	
name	Der Name des Couchbase-Service.
install_status	Installationsstatus, festgelegt auf „1“/„installiert“.
operational_status	Betriebsstatus, festgelegt auf „1“/„funktionsfähig“.
Cluster	Verweis auf das Couchbase-Cluster.

CI-Beziehungen

Diese Beziehungen sollen die Couchbase-DB-Erkennung unterstützen.

CI	Beziehung	CI
Couchbase-Instanz [cmdb_ci_couchbase_instance]	Wird ausgeführt auf::Wird ausgeführt	Linux-Server [cmdb_ci_linux_server]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Referenz	
Couchbase-Clusterknoten [cmdb_ci_couchbase_ cluster_node]	Cluster von::Cluster Referenz	Couchbase Cluster [cmdb_ci_couchbase_cluster]
Couchbase-Clusterknoten [cmdb_ci_couchbase_ cluster_node]	Gehostet auf::Hostet Referenz	Linux-Server [cmdb_ci_linux_server]
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	Verwendet::Verwendet von Referenz	Couchbase-Instanz [cmdb_ci_couchbase_instance]
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	Gehostet auf::Hostet Referenz	Couchbase Cluster [cmdb_ci_couchbase_cluster]
Couchbase Cluster [cmdb_ci_couchbase_cluster]	Repliziert zu::Repliziert von	Couchbase Cluster [cmdb_ci_couchbase_cluster]

CMDB-Datenmodell

CMDB-Datenmodell für die Couchbase-DB-Erkennung

Dell EMC XtremIO-Speicher-Array Discovery

ServiceNow Discovery Verwendet Dell EMC XtremIO-Speicher-Array Zu suchendes Muster Dell EMC XtremIO-Speicher-Array Komponenten. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Store-App Muster für Discovery und Service-Mapping

Verifizieren Sie Muster für Discovery und Service-Mapping Store-App, Version 1,0.96, ist installiert.

Verifizieren Sie CMDB CI-Klassenmodelle, Version 1.42.0, ist installiert.

Hinweis: Die Dell EMC XtremIO-Speicher-Array Die Store-Version von Muster 1.0.96 wurde nur für getestet XtremIO Clustertyp X2.

Anmeldeinformationen

Gewähren Sie Berechtigungen für die Standardauthentifizierung, indem Sie Anmeldeinformationen für die Standardauthentifizierung für die RESTful-API konfigurieren. Speichern Sie die Administratoranmeldeinformationen als Anmeldeinformationen für Standardauthentifizierung, um einen ordnungsgemäßen Zugriff sicherzustellen.

Ausführen Discovery

Führen Sie die schnelle Discovery nach Ziel-IP aus. Geben Sie die IP des XMS an (die den Speicher verwalten).

Berechtigungen für REST API-Abfragen

Während der Erkennung verwendet das Muster folgende API-Abfragen. Der Anwender, der den Anmeldeinformationen in der Instanz hinzugefügt wird, muss über Berechtigungen zum Ausführen dieser Abfragen verfügen.

- Ruft Details von XMS nach index_ID https ab://<IP>/api/JSON/v2/types/xms/<index_id>
- Ruft Details des Speicherservers (Clusters) nach index_ID https ab://<IP>/api/JSON/v2/types/Clusters/<index_id>
- Ruft Details des Speicherknotenelements (Bricks) nach index_ID https ab://<IP>/api/JSON/v2/types/Bricks/<index_id>
- Rufen Sie Details von Speicherdatenträgern (SSDs) nach index_ID https ab://<IP>/api/JSON/v2/types/ssds/<index_id>
- Rufen Sie Details zu Speichergehäuse (DAEs) nach index_ID https ab://<IP>/api/JSON/v2/types/daes/<index_id>
- Rufen Sie Details zu Speicher-Switches (Infiniband-Switches) nach index_ID https ab://<IP>/api/JSON/v2/types/infiniband-Switches/<index_id>
- Rufen Sie Details zu Batteriesicherungseinheiten (BBUS) nach index_ID https ab://<IP>/api/JSON/v2/types/bbus/<index_id>
- Rufen Sie Details zu Speicher-Controllern nach index_ID https ab://<IP>/api/JSON/v2/types/Storage-Controllers/<index_id>
- Rufen Sie Details zu Speicherports (Zielen) nach index_ID https ab://<IP>/api/JSON/v2/types/targets/<index_id>
- Ruft Details von Datenträgern (lokalen Datenträgern) anhand von index_ID https ab://<IP>/api/JSON/v2/types/local-Disks/<index_id>
- Ruft Details zu Initiatorgruppen nach index_ID https ab://<IP>/api/JSON/v2/types/initiator-groups/<index_id>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rufen Sie Details zu Fibre-Channel-Ports (Initiatoren) nach index_ID https ab://<IP>/api/JSON/v2/types/initiators/<index_id>
- Rufen Sie Details von Fibre Channel-Datenträgern (Volumes) nach index_ID https ab://<IP>/api/JSON/v2/types/Volumes/<index_id>

Das neue Konfigurationselement (Configuration Item, CI), das klassifiziert ist:

Initiatorgruppe.

Von Discovery während der horizontalen Erkennung erfasste Daten

Erkannte Dell EMC XtremIO-Speicher-Array Configuration Management Database (CMDB) Enthält die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_linux_Server]	
name	Der Name des Linux-/XMS-Servers
ip_address	Die IP-Adresse des Linux-/XMS-Servers
host_name	Der Hostname des Linux-/XMS-Servers
object_id	Das Bezeichnerattribut des Linux-/XMS-Servers
ram	Der insgesamt verfügbare RAM des Linux-/XMS-Servers
Speicherserver [cmdb_ci_storage_server]	
name	Der Name des Speicherservers (Cluster)
object_id	Die IP-Adresse des Speicherservers (Cluster)
serial_number	Die Seriennummer des Speicherservers (Cluster)
Speicherknotenelement [cmdb_ci_storage_node_element]	
name	Der Name des Speicherknotenelements (X-Brick)
object_id	Das Bezeichnerattribut des Speicherknotenelements (X-Brick)
serial_number	Die Seriennummer des Speicherknotenelements (X-Brick)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Speichercontroller [cmdb_ci_storage_controller]	
name	Der Name des Speicher-Controllers
device_id	Die Speicher-Controller-ID
serial_number	Die Seriennummer des Speicher-Controllers
model_number	Die Modellnummer des Speicher-Controllers
model_id	Die Modell-ID des Speicher-Controllers
Speicheranschluss [cmdb_ci_storage_port]	
wwpn	Der WWPN
name	Der Name des Speicherports (Ziel)
correlation_id	Die Korrelations-ID des Speicherports (Ziel)
speed	Die Geschwindigkeit des Speicherports (Ziel)
port_type	Der Speicherport-Typ (Ziel)
Speicher-Switch [cmdb_ci_storage_switch]	
object_id	Das Bezeichnerattribut des Speicher-Switches (Infiniband-Switch)
name	Der Name des Speicher-Switches (Infiniband-Switch)
serial_number	Die Seriennummer des Speicher-Switches (Infiniband-Switch)
model_id	Die Modell-ID des Speicher-Switches (Infiniband-Switch)
Speichergehäuse [cmdb_ci_Storage_Enclosure]	
name	Der Name des Speichergehäuses (Datenträger-Array-Gehäuse)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
object_id	Das Bezeichnerattribut des Speichergehäuses (Disk Array-Gehäuse)
serial_number	Die Seriennummer des Speichergehäuses (Disk Array-Gehäuse)
model_number	Die Modellnummer des Speichergehäuses (Disk Array-Gehäuse)
UPS [cmdb_ci_ups]	
name	Der Name der Battery Backup Unit (BBU)
serial_number	Die Seriennummer der Battery Backup Unit (BBU)
model_number	Die Modellnummer der Batteriesicherungseinheit (BBU)
model_id	Die Modell-ID der Battery Backup Unit (BBU)
Estimated_Charge_remaining	Die geschätzte Ladung blieb für die Batteriesicherungseinheit (BBU).
battery_voltage	Die Batteriespannung der Battery Backup Unit (BBU)
Initiatorgruppe [cmdb_ci_Initiator_Group]	
object_id	Das Bezeichnerattribut der Initiatorgruppe
name	Der Name der Initiatorgruppe
Number_of_initiators	Die Anzahl der Initiatoren in einer Gruppe
Anzahl_von_Volumes	Die Anzahl der Volumes
Fibre-Channel-Datenträger [cmdb_ci_fc_Disk]	
name	Der Name des Fibre Channel-Datenträgers (Volume)
device_id	Die ID des Fibre Channel-Datenträgers (Volume)
size	Die verfügbare Speichergröße des Fibre Channel-Datenträgers (Volume)
Fibre-Channel-Port [cmdb_ci_fc_Port]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
wwpn	Der WWPN
wwnn	Die WWNN.
name	Der Name des Fibre Channel-Ports (Initiator)
port_type	Der Porttyp des Fibre Channel-Ports (Initiator)

CI-Beziehungen

CI	Beziehungstyp	CI
cmdb_ci_linux_server	Verwalten::verwaltet von	cmdb_ci_storage_server
cmdb_ci_storage_switch	Stellt eine Verbindung her mit::Connected by	cmdb_ci_storage_server
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element
cmdb_ci_Storage_Enclosure	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_Storage_Port
cmdb_ci_ups	Stellt eine Verbindung her mit::Connected by	cmdb_ci_storage_node_element
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_Initiator_Group
cmdb_ci_Initiator_Group	Mitglied::Mitglied von	cmdb_ci_fc_port
cmdb_ci_Initiator_Group	Stellt eine Verbindung her mit::Connected by	cmdb_ci_fc_disk

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dell EMC Isilon-Discovery

Die ServiceNow Discovery-Anwendung verwendet Dell EMC Isilon-Muster, um Komponenten von zu finden Dell EMC Isilon. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Eine vollständige Liste der Geräte und Anwendungen, die ITOM-Transparenz erkennen kann, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Erstellen Sie SNMP-Community-Anmeldeinformationen

Erstellen Sie SNMP-Community-Anmeldeinformationen für den Isilon-Cluster. Der Erkennungsprozess beginnt mit der Verwendung von SNMP-basierten Abfragen zur Klassifizierung einer Anwendung als Isilon-Cluster. Weitere Informationen finden Sie unter SNMP-Community-Anmeldeinformationen in SNMP-Anmeldeinformationen .

Verifizieren Dell EMC Isilon-Anwenderberechtigungen und -Rollen

Sobald die Anwendung als Isilon-Cluster klassifiziert ist, verwendet der Erkennungsprozess REST-Abfragen, um Informationen darüber zu finden. Geben Sie an Dell EMC Isilon-Anwender mit den folgenden REST API-Endpunkten:

- "https://" + $host + ":8080/platform/3/cluster/config”
- "https://" + $host + ":8080/platform/3/network/interfaces”
- "https://" + $host_ip + ":8080/platform/3/cluster/nodes/”
- “https://” + $host + ":8080/platform/3/zones”
- "https://" + $host + ":8080/platform/3/network/pools”
- "https://" + $host + ":8080/platform/3/storagepool/nodepools”
- "https://" + $host + ":8080/platform/3/storagepool/storagepools”
- "https://" + $host + ":8080/platform/3/protocols/nfs/exports”
- "https://" + $host + ":8080/platform/3/protocols/smb/shares"

Die Dell EMC Der Isilon-Anwender muss auch über die folgenden Rollen verfügen:

- ISI_PRIV_LOGIN_PAPI
- ISI_PRIV_AUTH
- ISI_PRIV_DEVICES
- ISI_PRIV_NETWORK
- ISI_PRIV_NFS
- ISI_PRIV_SMARTPOOLS
- ISI_PRIV_SMB

Anmeldeinformationen für Standardauthentifizierung erstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Modul Anmeldeinformationen von ServiceNow Plattform, erstellen Sie für dieselbe Anmeldeinformationen für die Standardauthentifizierung Dell EMC Isilon-Anwender. Weitere Informationen finden Sie unter Virtual Server Interface .

Daten erfasst von Discovery Für Dell EMC Isilon

Discovery Füllt die Daten in aus CMDB Beim Ausführen des EMC Isilon-Musters.

Tabelle und Feld	Beschreibung
Speicherserver [cmdb_ci_storage_server]	Der Server, der den Isilon-Cluster hostet
short_description	Die während der Isilon-Serverinstallation konfigurierte Beschreibung
firmware_version	Die Version der auf dem Isilon-Server installierten Firmware
ip_address	Die IP-Adresse des Isilon-Servers
manufacturer	Das Unternehmen, das das Gerät hergestellt hat: EMC
model_id	Vorkonfigurierte Identifizierungszeichenfolge des Geräts
host_name	Der Hostname des Isilon-Servers
Speichercluster [cmdb_ci_storage_cluster]	Der Name der IP-Adresse des Clusters, den Isilon-Server bilden
name	
ip_address	
Speicherclusterknoten [cmdb_ci_storage_cluster_node]	Der Name und andere Attribute des Knotens, der Teil des Isilon-Speicherclusters ist
name	
Cluster	
operational_status	
Speicherknotenelement [cmdb_ci_storage_node_element]	Der Name und andere Attribute des physischen Knotens, der vom Speicherclusters gehostet wird
name	
manufacturer	
cpu_type	
model_id	
Netzwerkadapter [cmdb_ci_network_adapter]	Das Attribut, das anzeigt, ob der auf dem Clusterknoten installierte Netzwerkadapter aktiv ist
active	
name	
ip_address	
netmask	
IP-Adresse [cmdb_ci_ip_address]	Die Attribute der IP-Adresse des Clusterknotens
name	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

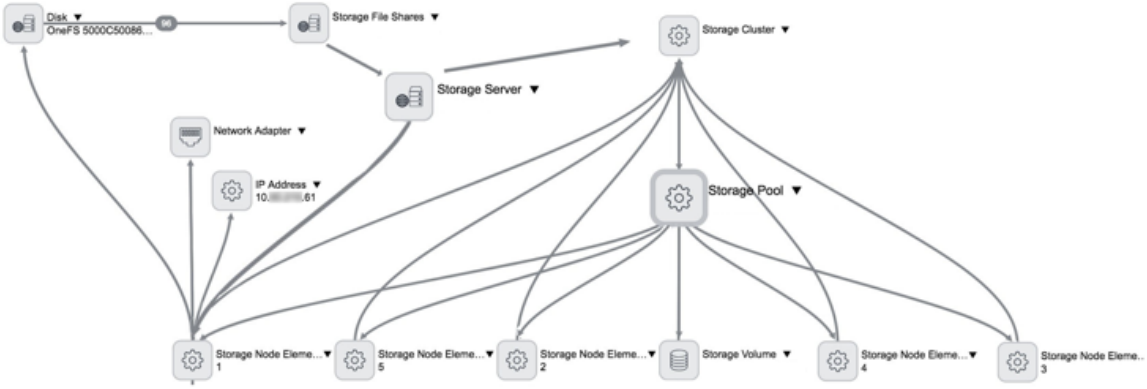
Tabelle und Feld	Beschreibung
netmask	
Datenträger [cmdb_ci_disk]	Der auf dem Isilon-Server installierte Speicherdatenträger
device_id	
name	
model_id	
Schnittstelle	
disk_interface	
Speicherdateifreigabe [cmdb_ci_storage_fileshare]	Die Serverattribute für die Dateifreigabe
Pfad	
name	
fileshare_id	
correlation_id	
Speichervolume [cmdb_ci_storage_volume]	Die Attribute des Speichervolume, das zum Speichercluster gehört
media_type	
object_id	
size_bytes	
free_space_bytes	
Speicherpool [cmdb_ci_storage_pool]	
pool_id	Die Attribute des Speicher-Pools, zu dem der Speichercluster gehört
free_space_bytes	
size_bytes	
name	
object_id	
Seriennummer [cmdb_serial_number]	Die Attribute der Seriennummer des Speicherknotens
serial_number	
serial_number_type	
valid	

Die Grafik zeigt CIs, die Teil der Isilon-Erkennung sind.

Hinweis: Diese Abhängigkeitsansichten-Zuordnung wurde der Übersichtlichkeit halber vereinfacht. Ihre Isilon-Bereitstellungen können viele weitere CIs enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeitsansichten mit Isilon-Komponenten



CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_storage_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element
cmdb_ci_storage_cluster_node	Cluster von::Cluster	cmdb_ci_storage_cluster (Referenz-`cluster`)
cmdb_ci_storage_cluster_node	Gehostet auf::Hostet	cmdb_ci_storage_node_element (Referenz-`server`)
cmdb_ci_storage_node_element	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_network_adapter	Eigentümer von::Eigentum von	cmdb_ci_storage_node_element (Referenz-`cmdb_ci`)
cmdb_ci_network_adapter	Verwendet von::Verwendet	cmdb_ci_storage_server (Referenz-`cmdb_ci`)
cmdb_ci_ip_address	Eigentümer von::Eigentum von	cmdb_ci_storage_node_element
cmdb_ci_ip_address	Verwendet von::Verwendet	cmdb_ci_storage_server
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_node_element (Referenz-`computer`)
cmdb_ci_storage_fileshare	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_server
cmdb_ci_storage_fileshare	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Verwendet::Verwendet von	cmdb_ci_storage_server
cmdb_ci_storage_volume	Eigentümer von::Eigentum von	cmdb_ci_storage_cluster
cmdb_ci_storage_pool	Eigentümer von::Eigentum von	cmdb_ci_storage_cluster (Referenz-`hosted_by`)

Dell Powermax-Speicher-Discovery mit Mustern

ServiceNow Discovery Verwendet **EMC PMAX-Phase1** Und **EMC PMAX-Phase2** Zu suchende Muster Dell Powermax-Speicherkomponenten. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu PowerMax-Speicherkomponenten und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Verifiziert die Erstellung des Anmeldeinformationsalias

1. Legen Sie den Bereich fest auf: **Global** .
2. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Alias ein. Beispiel: `powermax_Discovery_ceredential_Alias` . Notieren Sie sich den Aliasnamen, um ihn für die Konfiguration von zu verwenden **Standardauthentifizierung** Anmeldeinformationen.
Typ	Wählen Sie in der Liste aus **Anmeldeinformationen** .
ID	Die **ID** Das Feld wird beim Senden des Formulars automatisch ausgefüllt. Notieren Sie sich die Alias-ID, um sie zum Konfigurieren der Parameter für zu verwenden **EMC PMAX-Phase1** Muster. Beispiel: `powermax_credential_alias_ID` .

5. Wählen Sie **Absenden**.

Überprüfen Sie die Konfiguration von Standardauthentifizierung Anmeldeinformationen

Konfigurieren Sie **Standardauthentifizierung** Anmeldeinformationen zum Aktivieren der Verbindung mit der PowerMax REST API. Informationen zum Verfahren finden Sie unter Anmeldeinformationen für Standardauthentifizierung erstellen.

Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein. Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	powermax_Discovery_Basic_auth_ceredentials .
Anwendername	Geben Sie den Anwendernamen ein, der auf PowerMax zugreifen kann. Der Anwender muss über minimale schreibgeschützte Berechtigungen verfügen.
Passwort	Geben Sie das Passwort ein, das auf PowerMax zugreifen kann.

Verifiziert die Konfiguration eines serverlosen Discovery Zeitplan

Stellen Sie sicher, dass Sie auswählen Serverlos In **Erkennen** Feld. Informationen zum Verfahren finden Sie unter: Horizontale Erkennung planen

Ordnen Sie zu EMC PMAX-Phase1 Muster mit serverlosem Discovery Zeitplan

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder im Formular wie folgt aus:

Parameter	Beschreibung
IP-Adresse [emc_ip_address]	Die IP-Adresse der Navisphere, die als EMC Management Console dient, die mehrere Speicher verwalten kann.
Alias [credential_alias]	Die Alias-ID, die für die EMC PowerMax-Anmeldeinformationen konfiguriert ist. Beispiel: powermax_credential_alias_ID .

6. Wählen Sie **Absenden**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen von **EMC Powermax** Muster.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der vom Anwender zugewiesene Bezeichner oder die Bezeichnung für ein bestimmtes Speicher-Array oder eine bestimmte Komponente im System.
Modell-ID [model_id]	Die bestimmte Variante oder das bestimmte Modell des Speicher-Arrays.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
Seriennummer [serial_number]	Die Seriennummer, die jede einzelne Speicher-Array-Einheit eindeutig identifiziert.
Betriebssystem [bs]	Die auf dem Speicher-Array gehostete Betriebssystemumgebung. Zum Beispiel eingebettete Verwaltungssoftware oder Betriebssysteme.
BS-Version [os_Version]	Die Softwareversion, die auf dem Speicher-Array installiert ist, einschließlich des Kernbetriebssystems und der Verwaltungssoftware.
Firmware-Version [Firmware_Version]	Die in die Hardwarekomponenten des Speicher-Arrays eingebettete Software, einschließlich Controllern, Laufwerken und anderen Subsystemen.
Hersteller [manufacturer]	Das Unternehmen, das für das Entwerfen, die Herstellung und die Unterstützung des PowerMax-Speicher-Arrays verantwortlich ist Dell EMC.
Verwendete physische Kapazität [used_physical_Capacity]	Die Menge des derzeit zugewiesenen und im PowerMax-System genutzten Speicherplatzes. Gibt an, wie viele der verfügbaren physischen Speicherressourcen aktiv Daten oder andere Inhalte speichern.
Physische Kapazität [physical_Capacity]	Die maximale Kapazität, die zum Speichern von Daten oder anderen Inhalten verwendet werden kann.

Speicherclusterknoten [cmdb_ci_storage_cluster_node]

Feld	Beschreibung
Name [name]	Der Name des Clusterknotens.
Cluster [cluster]	Die diesem Clusterknoten in der PowerMax-Umgebung zugeordnete Hostgruppe.
Hersteller [manufacturer]	Der Herstellername, der lautet Dell EMC.

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Der Name des Speicherclusters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichercluster [cmdb_ci_storage_cluster] (Fortsetzung)

Feld	Beschreibung
Korrelations-ID [correlation_ID]	Kombiniert den Clusternamen und die Seriennummer des Speichers, um einen eindeutigen Bezeichner zu erstellen.

Speichercontroller [cmdb_ci_storage_controller]

Feld	Beschreibung
Name [name]	Die Kombination aus Asset und Asset-Tag.
Zugewiesen [zugewiesen]	Der Verfügbarkeitsstatus.
Asset [Asset]	Die Director-Steckplatznummer.
Asset-Tag [Asset_Tag]	Die Nummer des Direktors.
Geräte-ID [device_id]	Eine eindeutige Bezeichnung für den Controller.
Kurzbeschreibung [short_description]	Der Director-Slot und die Nummer.
Hersteller [manufacturer]	Der Herstellername, der lautet Dell EMC.

Speicheranschluss [cmdb_ci_storage_port]

Feld	Beschreibung
WWPN [wwpn]	Der World Wide Port Name (WWPN) des Speicherports.
Name [name]	Der Portbezeichner.
Bestellnummer [po_number]	Die Portnummer.
Status [state]	Der Portstatus.
Geschwindigkeit [Geschwindigkeit]	Die Übertragungsgeschwindigkeit des Ports.
Hersteller [manufacturer]	Der Herstellername, der lautet Dell EMC.
Kurzbeschreibung [short_description]	Eine Liste der Port-IP-Adressen.
IP-Adresse [ip_address]	Die verbundene IP-Adresse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Objekt-ID [object_id]	Der eindeutige Bezeichner des World Wide Name (WWN).
Status [state]	Der aktuelle Betriebsstatus des Volumes. Beispiel: **Schreiben Deaktiviert** Oder **Bereit** .
Größe [Größe]	Die Kapazität in Gigabyte (GB).

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Die Spindel-ID.
Hersteller [manufacturer]	Der Datenträgerhersteller.
Modell-ID [model_id]	Das Datenträgermodell.
Größe [Größe]	Die Datenträgerkapazität in Gigabyte (GB).
Geräte-ID [device_id]	Die Kombination der Seriennummer des Speichersystems mit dem Datenträgernamen, der jeden Datenträger in der PowerMax-Umgebung eindeutig identifiziert.

FC-Export [cmdb_ci_fc_Export]

Feld	Beschreibung
Export-ID [Export_ID]	Der Fibre Channel-Bezeichner.
Initiator-WWPN [Initiator_wwpn]	Ein eindeutiger Bezeichner, der die Direktor-ID, die Portnummer und die Initiator-ID kombiniert.
Bestellnummer [po_number]	Die Portnummer.
Zugewiesen an [assigned_to]	Der spezifische Host, der dem Export zugewiesen ist und die Fibre Channel-Verbindung verwaltet.
Attribute [Attribute]	Die Direktor-ID, die den spezifischen Direktor identifiziert, der für die Verwaltung der Fibre Channel-Exporte verantwortlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

FC-Export [cmdb_ci_fc_Export] (Fortsetzung)

Feld	Beschreibung
Name [name]	Die Initiator-ID.
Hersteller [manufacturer]	Der Herstellername, der lautet Dell EMC.
LUN [lun]	Die Logical Unit Number (LUN), die innerhalb von PowerMax-Systemen verbunden ist und die spezifische Speichereinheit angibt, die für den Fibre Channel-Export zugewiesen ist.
Asset-Tag [Asset_Tag]	Eine Kombination aus der Director-ID und der Portnummer, die das Asset innerhalb der Fibre Channel-Exporte eindeutig identifiziert.

ISCSI-Export [cmdb_ci_isci_Export]

Feld	Beschreibung
Export-ID [Export_ID]	Der eindeutige Bezeichner für einen iSCSI-Export in PowerMax-Systemen, der die Verwaltung und Nachverfolgung von iSCSI-Verbindungen erleichtert.
Initiator-WWPN [Initiator_wwpn]	Eine Kombination aus Director-ID, Portnummer und Initiator-ID, die einen eindeutigen Bezeichner für den Initiator innerhalb der iSCSI-Exporte bildet.
Name [name]	Die Initiator-ID in PowerMax-Systemen, die als eindeutiger Bezeichner für den Initiator im Kontext von iSCSI-Exporten dient.
Bestellnummer [po_number]	Die Portnummer, die den spezifischen Port identifiziert, der für den iSCSI-Export verwendet wird.
Attribute [Attribute]	Die Direktor-ID, die den spezifischen Direktor identifiziert, der für die Verwaltung des iSCSI-Exports verantwortlich ist.
Zugewiesen an [assigned_to]	Der Host, der dem iSCSI-Export in der PowerMax-Umgebung zugewiesen ist und das bestimmte Hostsystem angibt, das mit dem Export verbunden ist.

Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools.

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die PowerMax-Discovery mit zu unterstützen **EMC PMAX-Phase2** Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_server
cmdb_ci_fc_export	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume
cmdb_ci_fc_export	Exportieren nach::Importieren von	cmdb_ci_storage_cluster_node
cmdb_ci_isci_Export	Gehostet::Hosts	cmdb_ci_storage_server
cmdb_ci_isci_Export	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume
cmdb_ci_isci_Export	Exportieren nach::Importieren von	cmdb_ci_storage_cluster_node
cmdb_ci_storage_cluster_node	Cluster von::Cluster	cmdb_ci_storage_cluster
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_server
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_Storage_Port
cmdb_ci_Storage_Port	Eigentümer von::Eigentum von	cmdb_ci_fc_export
cmdb_ci_Storage_Port	Eigentümer von::Eigentum von	cmdb_ci_isci_Export
cmdb_ci_Storage_Port	Eigentümer von::Eigentum von	cmdb_ci_isci_Export
cmdb_ci_Storage_Port	Eigentümer von::Eigentum von	cmdb_ci_fc_export
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_Storage_Port
cmdb_ci_storage_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_cluster_node

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_pool

Dell Datendomänenspeicher-Discovery anhand von Mustern

Discovery Und Service-Mapping Verwenden Sie **Dell EMC-Datendomäne** serverloses Muster, um die im Data Domain Management Center (DDMC) registrierten Datendomänenspeichersysteme zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu Datendomänenkomponenten und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Verifiziert die Erstellung des Anmeldeinformationsalias

Rolle: DDMC-Administrator.

1. Legen Sie den Bereich fest auf: **Global** .
2. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Alias ein. Beispiel: Ddmc_Discovery_ceredential_alias . Notieren Sie sich den Aliasnamen, um ihn für die Konfiguration von zu verwenden **Standardauthentifizierung** Anmeldeinformationen.
Typ	Wählen Sie in der Liste aus **Anmeldeinformationen** .
ID	Die **ID** Das Feld wird beim Senden des Formulars automatisch ausgefüllt. Notieren Sie sich die Alias-ID, um sie zum Konfigurieren der Parameter für zu verwenden **Dell EMC-Datendomäne** Muster. Beispiel: Ddmc_credential_alias_ID .

5. Wählen Sie **Absenden**.

Überprüfen Sie die Konfiguration von Standardauthentifizierung Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle: DDMC-Administrator.

Hinweis: Um die Discovery mit Mustern auszuführen, können Sie nur eine Anmeldeinformation pro Alias erstellen.

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Suchen Sie in der Liste nach dem eindeutigen Alias-Namen, und öffnen Sie den Datensatz.
3. Wählen Sie in der Liste aus **Standardauthentifizierung** Anmeldeinformationen.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein. Beispiel: `Ddmc_Discovery_Basic_auth_ceredentials` .
Anwendername	Geben Sie den Anwendernamen ein, der auf das DDMC zugreifen kann. Dieser Anwender wird in DDMC erstellt. Der Anwender muss über minimale schreibgeschützte Berechtigungen verfügen. Alternativ können Sie die REST API-Schnittstelle für DDMC ausfüllen.
Passwort	Geben Sie das Passwort ein, das auf den DDMC zugreifen kann. Dieses Passwort wird in DDMC erstellt.
Aktiv	Standardmäßig aktiviert.
Anmeldeinformationsalias	Wenn Sie das Formular über den Alias eingegeben haben, müssen Sie dieses Feld nicht konfigurieren.

5. Wählen Sie **Absenden**.

Verifiziert die Konfiguration eines serverlosen Discovery Zeitplan

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie den Namen Ihrer Wahl ein.
Erkannt	Wählen Sie in der Liste aus `Serverlos` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wählen Sie die Suchschaltfläche aus, um die Liste der MID-Server zu öffnen, und wählen Sie den MID-Server aus, der Netzwerkzugriff auf das DDMC hat.
Aktiv	Standardmäßig aktiviert.
Anmeldeinformationsalias	Dieses Feld muss nicht konfiguriert werden.

Weitere Informationen zum Festlegen von **Max. Ausführungszeit** , **Ausführen** , Und **Zeit** Felder, siehe: Horizontale Erkennung planen

4. Wählen Sie **Absenden**.

Ordnen Sie zu **Dell EMC-Datendomäne** Muster mit serverlosem Discovery Zeitplan

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie den Namen Ihrer Wahl ein. Beispiel: dell_emc_Data_Domain_serverless_Discovery
Muster	Wählen Sie die Suchschaltfläche, um die Liste der Muster zu öffnen, und wählen Sie aus **Dell EMC-Datendomäne** Muster.
Proxyhost	Dieses Feld muss nicht konfiguriert werden.
Erweiterte Parameter	Dieses Feld muss nicht konfiguriert werden.

6. Wählen Sie **Absenden**.

Konfigurieren Sie die Parameter für **Dell EMC-Datendomäne** Muster

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie aus **Serverloses Ausführungsmuster** Registerkarte.
4. Wählen Sie den Datensatz aus, der für erstellt wurde **Dell EMC-Datendomäne** Muster.
5. In **Startprogramm-Parameter für Discovery-Muster** Legen Sie den Wert für die Felder wie folgt fest:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anmeldeinformationsalias	Geben Sie die für DDMC konfigurierte Alias-ID ein. Sie finden den Alias in **Aliasse Für Verbindungen Und Anmeldeinformationen** Liste. Beispiel: `Ddmc_credential_alias_ID` .
DDMC-Port	(Optional) standardmäßig verwendet das Muster Port 3009.
DDMC-IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse des DDMC ein. Diese Details können vom DDMC-Administrator bereitgestellt werden. Beispiel: `101.10.10.101` Oder `ddmc.demo.local` .

6. Um die Discovery auszuführen, können Sie auswählen **Entdecken Sie jetzt** Von **Zugehörige Links** Oder warten Sie auf die Laufzeit.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen von **Dell EMC-Datendomäne** Muster.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der eindeutige Bezeichner des Speicherservers. Der Name ist normalerweise der DNS-Hostname (Domain Name System) oder der Computername, der dem entspricht **Host_Name** Attribut.
Hostname [Host_Name]	Der DNS-Hostname des Datendomänensystems. Der Host, der zum Registrieren des Systems beim Data Domain Management Center (DDMC) verwendet wird.
FQDN [fqdn]	Der vollqualifizierte Domänenname des Datendomänensystems. Der vollständige Domänenname, der zum Registrieren des Systems beim DDMC verwendet wird.
IP-Adresse [ip_address]	Die IP-Adresse des Datendomänen-Speicherservers. Der Name ist die spezifische IP-Adresse, die zum Registrieren des Datendomänensystems beim DDMC verwendet wird.
BS-Version [os_Version]	Die Version des Betriebssystems, das auf dem Data Domain-System ausgeführt wird. Die unterstützten Versionen stammen ab DD OS 7,3.
Modell [model]	Das spezifische Modell des Data Domain (DD)-Systems. Beispielsweise lautet der Name für die DD Virtual Edition (VE) **DELL EMC DD VE** .
Hersteller [manufacturer]	Der Hersteller ist Dell EMC.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
Seriennummer [serial_number]	Die eindeutige Seriennummer, die dem DD-System zugewiesen ist.
Betriebssystem [os]	Das Betriebssystem der Datendomäne ist: **TT-BETRIEBSSYSTEM** .

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Der Name des DDMC, das dem Speichercluster zugeordnet ist.
Cluster-ID [cluster_id]	Der universelle Bezeichner (UUID) des DDMC, der den Cluster eindeutig identifiziert.
Clusterversion [Cluster_Version]	Die Softwareversion des DDMC, die derzeit auf dem Cluster installiert ist.
Seriennummer [serial_number]	Die eindeutige Seriennummer, die dem System Virtual Data Domain Management Center (VDDMC) zugewiesen ist.
Modell-ID [model_id]	Das spezifische Modell des verwendeten Datendomänensystems. Für den DDMC lautet die Modell-ID „DELL EMC DD Management Center“.
Hersteller [manufacturer]	Der Hersteller ist Dell EMC.

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Der Name, der dem Festplattengerät im Speichersystem zugewiesen ist.
Geräte-ID [device_id]	Der eindeutige Bezeichner für das Festplattengerät, der mit dem Gerätenamen identisch ist.
Modell-ID [model_id]	Das Modell des Datenträgergeräts. Beispiel: **VMware Virtual_Disk** .
Größe [Größe]	Die Kapazität des Festplattengeräts, gemessen in Gigabyte (GB).

Die Datenbank des Datenträgerregals-Gehäuses wird nur für physische DD-Systeme ausgefüllt, die Datenträger-Erweiterungsregale unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Festplattenregal-Gehäuse [cmdb_ci_diskshelf_Chassis_Cluster]

Feld	Beschreibung
Name [name]	Der Name des Datenträgererweiterungs-Shelfs.
Seriennummer [serial_number]	Die eindeutige Seriennummer des Datenträger-Erweiterungs-Shelfs.

Seriennummer [cmdb_ci_Serial_number]

Feld	Beschreibung
Seriennummer [serial_number]	Die eindeutige Seriennummer des Dell EMC Data Domain-Speichersystems, wie im DDMC registriert.
Seriennummerntyp [Serial_number_type]	Das Format der Seriennummer für das Dell EMC Data Domain-Speichersystem, das angibt, ob es sich um eine Systemseriennummer oder einen Universally Unique Identifier (UUID) handelt.
Gültig [valid]	Die Gültigkeit der Daten mit einem Wert von **Wahr** Bestätigt, dass die Seriennummer erfolgreich verifiziert wurde.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Der Bezeichner oder die Bezeichnung des Netzwerkadapters, z. B. **Eth1** .

Die DDMC-REST-API stellt die MAC-Adresse von Netzwerkadaptern nicht bereit. Daher bleibt das MAC-Adressfeld für Netzwerkadapter leer.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	Die IP-Adresse, die dem Gerät zugewiesen ist.
Netzmaske [netmask]	Die Netzmaske, die der IP-Adresse zugeordnet ist und das Subnetz definiert, zu dem die IP-Adresse gehört.

CI-Beziehungen

Muster für Discovery und Service-Mapping Erstellen Sie diese Beziehungen, um die Data Domain Discovery zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_storage_server	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_Disk_Shelf_Chassis	Gehostet auf: Hosts	cmdb_ci_storage_server
cmdb_ci_Serial_number	Referenz	cmdb_ci_storage_server
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_ip_address

Erkennung von F5-Zertifikaten

Die ServiceNow® Discovery Anwendungsverwendungen **Die F5-SSH-SSL-Zertifizierung** Mustererweiterung, um alle zugeordneten Zertifikate in F5-Lastenausgleichsmotoren zu finden, die IPv4-Adressen, IPv6-Adressen oder beides verwenden.

Die **Die F5-SSH-SSL-Zertifizierung** Mustererweiterung ist Teil von **F5-Lastenausgleichsmodul** Und **F5 Lastenausgleichsmodul SSH** Muster, die erkennen F5 BIG-IP-Lastenausgleichsmodul . Die **Die F5-SSH-SSL-Zertifizierung** Die Mustererweiterung erkennt F5-Lastenausgleichsmodul-Instanzen, die auf den Hosts über SNMP/SSH ausgeführt werden, und erkennt dann Zertifizierungen, die vom ausgeführten Knoten des Lastenausgleichsmoduls verwendet werden.

Hinweis: Für Lastenausgleichsmodule, die IPv6 ausführen, wird nur SSH unterstützt.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

Einschränkungen der IPv6-Unterstützung

- F5-SNMP wird nicht unterstützt.
- `MID-Server` REST APIs können nicht mit IPv6 ausgeführt werden.

  Informationen zum Ausführen der Discovery mit F5 REST finden Sie unter KB0864769 .

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen auf dem neuesten Stand sind

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die Konfiguration des F5-Lastenausgleichsmoduls

- Stellen Sie sicher, dass Instanzen des F5-Lastenausgleichsmoduls ausgeführt werden.
- Stellen Sie sicher, dass der Host (auf dem die F5-Instanz ausgeführt wird) mit den Anmeldeinformationen des Discovery-Benutzers erfolgreich erkennen kann.

Überprüfen Sie die Konfiguration von Discovery

Stellen Sie sicher, dass der in der ServiceNow AI Platform-Instanz hinzugefügte Discovery-Benutzer die folgenden Befehle ausführen kann:

Befehl	Beschreibung
modify	Ändert die TMSH-Komponenten. Sie können eine oder mehrere Eigenschaftseinstellungen in mehreren Komponenten ändern. Der Befehl *modify* verwendet die folgende Option: *display-threshold pager*.
display_threshold	Ermöglicht Ihnen, einen *display-threshold* in Ihrem Skript erneut zu aktivieren
list	Zeigt Komponenten an, zu deren Anzeige Sie berechtigt sind oder die als Argumente übergeben werden. Der Befehl *list* sucht nach den folgenden Argumenten: • *ssl-cert* • *certificate-key-size* • *checksum* • *create-time* • *expiration-string* • *issuer* • *subject* • *Version* • *fingerprint* • *serial-number* • *subject-alternative-name* • *size*

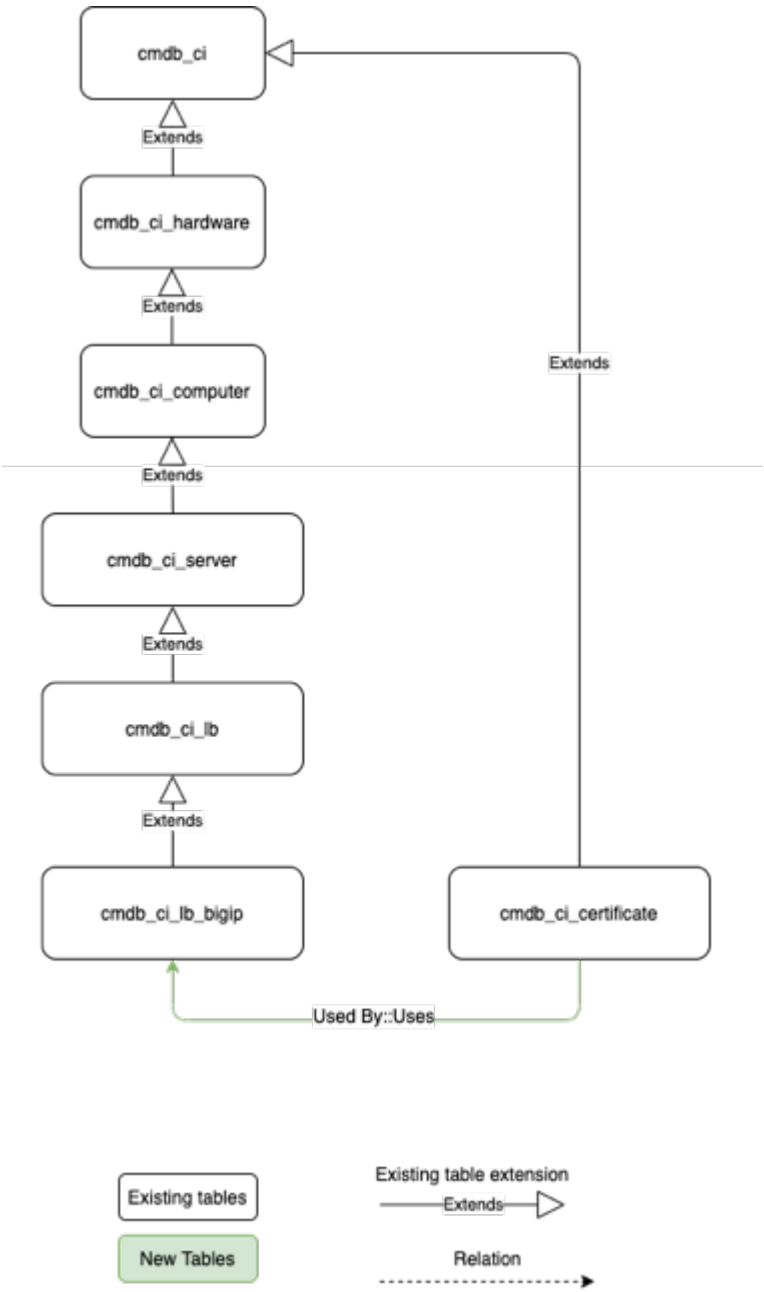
Überprüfen Sie die Konfiguration der Muster

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass **F5-SSH-SSL-ZERTIFIZIERUNG** Die gemeinsame Bibliothek wird dem Erweiterungsabschnitt von hinzugefügt **F5-Lastenausgleichsmodul** Und **F5 Lastenausgleichsmodul SSH** Muster, um die Zertifizierungsattribute zu erfassen.

Klassenmodell für die Erkennung von F5-Zertifikaten



Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Basiskonfigurationselement-Cluster [cmdb]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Konfigurationselement [cmdb_ci]	
operational_status	Betriebsstatus des Clusterknotens
Eindeutiges Zertifikat [cmdb_ci_unique_certificate]	
fingerprint	Hashwert des Zertifikats
Fingerabdruck-Algorithmus	Algorithmus, der zum Hashen des Zertifikats verwendet wird
Allgemeiner Antragstellername	Identifiziert den dem Zertifikat zugeordneten Hostnamen/die Domäne
Eindeutiger Antragstellername	Identifizierende Informationen des Antragstellers
Eindeutiger Ausstellername	Eindeutiger Name des Ausstellers
Anmerkungen	
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate erstellt werden sollen
Allgemeiner Ausstellername	Allgemeiner Name des Ausstellers
gültig ab	Gültigkeitsstartzeitraum des Zertifikats
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Antragstellerland	Der zweistellige Ländercode des Antragstellers.
Antragstellerorganisation	Organisation des Antragstellers
Version	X.509-Version des Zertifikats
Aussteller	Entität, die das Zertifikat signiert und ausgestellt hat
Antragsteller-Organisationseinheit	Organisationseinheit des Antragstellers
Alternativer Antragstellername	Liste vollqualifizierter Domänennamen, die durch das Zertifikat gesichert werden
gültig bis	Gültigkeitsendzeitraum des Zertifikats
name	
Status	Lebenszyklusstatus des Zertifikats
Stammaussteller	Stammentität, die das Zwischenzertifikat signiert und ausgestellt hat
Schlüsselgröße	Größe des vom Signaturalgorithmus verwendeten Schlüssels
Antragsteller-Ort	Ort des Antragstellers
Antragstellerstatus	Status des Antragstellers

CI-Beziehungen

Die **Die F5-SSH-SSL-Zertifizierung** Die Mustererweiterung erstellt keine CI-Beziehungen.

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Muster Fortinet Network Firewall der nächsten Generation – REST, um zu finden FortinetFirewalls über REST-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Aufrufe. Darüber hinaus findet die Mustererweiterung VDOM Discovery FortiGate Virtual Domains (VDOMs). Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Muster Fortinet Network Firewall der nächsten Generation – REST verwendet eine Reihe von REST-API-Aufrufen, um zu finden FortinetFirewalls. Discovery Verwendet das Muster zum Ausführen der horizontalen Discovery.

Hinweis: Nur REST-basiert FortinetDie Firewall-Discovery-Methode findet FortiGate-VDOMs. SNMP-basiert FortinetDie Firewall-Discovery-Methode erkennt sie nicht. Für Informationen zum standardmäßigen SNMP-basierten FortinetFirewall-Discovery, siehe Nächste Generation Fortinet SNMP-basierte Discovery der Netzwerk-Firewall.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über zu erfahren FortinetFirewalls und ihre Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Erstellen Sie ein API-Token

Erstellen Sie ein API-Token in Fortinet. Anweisungen zum Erstellen eines API-Tokens finden Sie unter Fortinet-Dokumentbibliothek Und suchen Sie in der FortiConverter-Tool-Produktfamilie nach dem artikel „FortiGate-Gerät über API-Token verbinden – Online-Hilfe“.

Überprüfen Sie den API-Zugriff und die Berechtigungen

- Überprüfen Sie, ob MID-Server Kann auf zugreifen Fortinet APIs.
- Stellen Sie sicher, dass das API-Token über ausreichende Berechtigungen verfügt, um die erforderlichen Informationen aus dem abzurufen Fortinet Geräte.

Erforderlich Fortinet APIs:

- `v2/cmdb/System/global`
- `api/v2/Monitor/System/Status`
- `api/v2/cmdb/System/ha`
- `api/v2/cmdb/Router/static`
- `/api/v2/cmdb/Firewall/Policy`
- `api/v2/cmdb/System/vdom-property`
- `api/v2/cmdb/System/Interface`
- `/api/v2/Monitor/System/Interface/select`

Deaktivieren Sie SNMP-basiert Fortinet Firewall-Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Deaktivieren Sie SNMP-basiert Fortinet Firewall-Discovery.

Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen

Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für Fortinet Firewall-REST-basierte Discovery.

Zeitplan für Erkennung ohne Server erstellen

Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für FortinetFirewall-REST-basierte Discovery.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Fortinet Network Firewall der nächsten Generation – REST.

Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Feld	Beschreibung
Name [name]	**Hostname** Feld von Fortinet Gerät.
Seriennummer [serial_number]	Seriennummer von Fortinet Gerät.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname des Fortinet Gerät.
Betriebsstatus [operational_status]	Gibt an, ob Fortinet Gerät befindet sich im Status „aktiv“.
IP-Adresse [ip_address]	IP-Adresse des Fortinet Gerät.
Hersteller [manufacturer]	Fortinet Gerätehersteller.
Beschreibung [short_description]	Kurzbeschreibung von Fortinet Gerät.
Modellnummer [model_number]	Fortinet Gerätemodellnummer.
Firmware-Version [Firmware-Version]	Fortinet Firmware-Version des Geräts.
Hardware-BS [Hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]

Feld	Beschreibung
Name [name]	**Hostname** Feld von Fortinet Firewall-Cluster.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname des Firewall-Clusters.
IP-Adresse [ip_address]	IP-Adresse des Firewall-Clusters.
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung des Firewall-Clusters.
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-BS [Hardware_os]	Auf der Hardware ausgeführtes Betriebssystem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet] (Fortsetzung)

Feld	Beschreibung
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „Fortinet-Firewall-Gerät“ [cmdb_ci_Firewall_device_fortinet].

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Fortinet Firewall.
Netzmaske [netmask]	Netzmaske von Fortinet Firewall.

Discovery Füllt die Daten in aus CMDB Bei der Ausführung der Erweiterung Fortinet Network Firewall – REST-Muster VDOM Discovery.

Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]

Feld	Beschreibung
Vdom-Index [vdom_index]	Index des VDOM in der Liste.
Name [name]	Name des VDOM.
Beschreibung [short_description]	Beschreibung der VDOM-Eigenschaft, die zusätzlichen Kontext oder Informationen zum Zweck der Eigenschaft bereitstellt.

Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_Firewall_Interface]

Feld	Beschreibung
ID [ID]	Eindeutiger Bezeichner für die Schnittstelle. Beispiel: Port1.
Name [name]	Name der Schnittstelle. Beispiel: LAN.
IP-Adresse [ip_address]	IP-Adresse, die der Schnittstelle zugewiesen ist.
Beschreibung [short_description]	Beschreibung der Schnittstelle, die häufig zu Dokumentations- oder Identifizierungszwecken verwendet wird. Beispiel: Haupt-LAN-Schnittstelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_Firewall_Interface] (Fortsetzung)

Feld	Beschreibung
MAC-Adresse [mac_address]	MAC-Adresse der Schnittstelle.
Zugriffstyp [Access_type]	Typ der Schnittstelle. Beispiel: Physisch, VLAN oder Aggregat.

Netzwerktopologie [cmdb_ci_Network_Topology]

Feld	Beschreibung
Name [name]	Virtual LAN (VLAN)-ID, die der Schnittstelle zugeordnet ist, falls zutreffend. Das Format ist: `VLAN:{VLAN-ID}` . Beispiel: VLAN-310.

Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_Firewall_Policy]

Feld	Beschreibung
Richtlinien-ID [Policy_ID]	Eindeutige ID, die der Richtlinie auf VDOM- oder Geräteebene zugewiesen ist.
UUID [UUID]	Globaler eindeutiger Bezeichner (GUID) für die Firewall-Richtlinie.
Name [name]	Name der Richtlinie
Source_Interface	Netzwerkschnittstelle, von der der Datenverkehr stammt.
Target_Interface	Netzwerkschnittstelle, an die der Datenverkehr weitergeleitet wird.
Quelladresse [Source_address]	Quelladresse oder Adressgruppe, aus der der Datenverkehr stammt.
Zieladresse [destination_address]	Zieladresse oder Adressgruppe, an die der Datenverkehr weitergeleitet wird.
Internetservice [Internet_Service]	Von der Richtlinie verwalteter Service oder Anwendung, häufig dargestellt durch eine Servicegruppe oder einen Namen.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Fortinet Firewall-Discovery.

CI	Beziehung	CI
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Routerschnittstelle [dscy_router_interface]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Seriennummer [cmdb_serial_number]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Discovery Erstellt diese Beziehungen zur Unterstützung der FortiGate VDOM-Discovery.

CI	Beziehung	CI
Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_Firewall_Interface]	Erstreckt sich von	Netzwerkschnittstelle [cmdb_ci_ni_Interface]
Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_Firewall_Policy]	Erstreckt sich von	Firewall-Sicherheitsrichtlinie [cmdb_ci_Firewall_sec_Policy]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Enthält::Enthalten in	Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_Firewall_Interface]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Enthält::Enthalten in	Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_Firewall_Policy]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Erstreckt sich von	IP-Firewall [cmdb_ci_ip_firewall]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Netzwerktopologie [cmdb_ci_Network_Topology]	Mitglieder::Mitglied von	Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_Firewall_Interface]

Deaktivieren Sie SNMP-basiert Fortinet Firewall-Discovery

Deaktivieren Sie die standardmäßige SNMP-basiert Fortinet Firewall-Discovery und REST-basierte Discovery stattdessen verwenden, um virtuelle FortiGate-Domänen (VDOMs) zu erkennen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **SNMP**an.
2. In **Name** Feld, suchen Sie nach Fortinet-Firewall .
3. Wählen Sie den Fortinet-Firewall-Datensatz aus.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
5. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Erstellen Sie einen Alias, und fügen Sie ihn einer API-Schlüssel-Anmeldeinformation hinzu. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für Fortinet Firewall-REST-basierte Discovery.

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für Fortinet Firewall-REST-basierte Discovery

Erstellen Sie einen Alias, und fügen Sie ihn zu einer API-Schlüssel-Anmeldeinformation hinzu, um sie zu erkennen Fortinet Firewalls und virtuelle FortiGate-Domänen (VDOMs) durch REST-basierte Discovery.

Vorbereitungen

Erstellen Sie ein API-Token in Fortinet. Weitere Informationen finden Sie unter Erstellen Sie ein API-Token Voraussetzung in Fortinet Firewall und FortiGate VDOM REST-basierte Discovery.

Erforderliche Rolle: discovery_admin

Prozedur

1. Erstellen Sie einen Alias.
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
   b. Wählen Sie **Neu**.
   c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie aus **Anmeldeinformationen** Für den Aliastyp in **Typ** Feld.
   d. Wählen Sie **Absenden**.
2. Konfigurieren Sie API-Schlüssel-Anmeldeinformationen für den neuen Alias.
   a. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
   b. Wählen Sie **Neu**.
   c. Wählen Sie Aus **API-Schlüssel-Anmeldeinformationen** .
   d. Entsperren Sie **Anmeldeinformationsalias** Feld und wählen Sie den erstellten Alias aus.
   e. Konfigurieren Sie den Rest von **API-Schlüssel-Anmeldeinformationen** Formularfelder.
   f. Wählen Sie **Absenden**.
   Weitere Informationen zu Formularfeldern für API-Schlüssel-Anmeldeinformationen finden Sie unter Anmeldeinformationen für API-Keys .

Nächste Maßnahme

Erstellen Sie einen serverlosen Zeitplan für Fortinet Firewall-REST-basierte Discovery. Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für FortinetFirewall-REST-basierte Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Erstellen Sie einen serverlosen Zeitplan für FortinetFirewall-REST-basierte Discovery

Erstellen Sie einen serverlosen Discovery-Zeitplan für die Erkennung Fortinet Firewalls und virtuelle FortiGate-Domänen (VDOMs) durch REST-basierte Discovery.

Vorbereitungen

- Stellen Sie sicher, dass Sie über die IP-Adresse für verfügen Fortinet Firewall-Gerät.
- Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für Fortinet Firewall-REST-basierte Discovery.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Erstellen Sie den Discovery-Zeitplandatensatz.
   a. Wählen Sie **Neu**.
   b. Füllen Sie im Formular die Felder aus.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Erkannt	Scan-Typ, der serverlos sein muss.
MID-Server verwenden	Name des MID-Server Zur Verwendung für diesen Zeitplan.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

   c. Wählen Sie **Absenden**.
3. Erstellen Sie das Ausführungsmuster.
   a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.
   b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .
   c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll. Dies sollte das Fortinet Network Firewall – REST-Muster der nächsten Generation sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren, der global sein muss.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

d. Wählen Sie **Absenden**.

4. Legen Sie die Parameter des Musterstartprogramms fest.

a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.

b. Füllen Sie im Formular die Felder aus.

Parameter	Wert
ip_address	IP-Adresse des Firewall-Geräts.
AnmeldeinformationsAlias	Name des von Ihnen erstellten Anmeldeinformationsalias.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Nächste Generation Fortinet SNMP-basierte Discovery der Netzwerk-Firewall

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Fortinet-Netzwerk-Firewall-Muster der nächsten Generation, um zu finden Fortinet Firewalls durch eine Reihe von SNMP-Aufrufen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Fortinet-Netzwerk-Firewall-Muster der nächsten Generation verwendet eine Reihe von SNMP-Aufrufen, um zu finden Fortinet Firewalls. Discovery Verwendet das Muster zum Ausführen der horizontalen Discovery.

Hinweis: Nur REST-basiert FortinetDie Firewall-Discovery-Methode findet FortiGate-VDOMs. SNMP-basiert FortinetDie Firewall-Discovery-Methode erkennt sie nicht. Für Informationen zu REST-basiert Fortinet Discovery von Firewall und FortiGate Virtual Domains (VDOMs), siehe Fortinet Firewall und FortiGate VDOM REST-basierte Discovery.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über zu erfahren Fortinet Firewalls und ihre Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen auf dem neuesten Stand sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Stellen Sie den SNMP-Zugriff sicher

Stellen Sie sicher, dass Ihr Fortinet Firewall-Gerät hat SNMP-Zugriff.

Konfigurieren Sie SNMP-Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .

Fügen Sie den SNMP-System-OID-Datensatz zu hinzu ServiceNow Instanz

Fügen Sie der ServiceNow-Instanz den OID-Datensatz des SNMP-Systems für das Fortinet-Gerät hinzu. Aktualisieren Sie Folgendes:

- Klassifizierer: Fortinet-Firewall
- Klasse: Fortinet-Firewall-Gerät

Führen Sie eine horizontale Discovery aus

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Fortinet-Netzwerk-Firewall-Musters der nächsten Generation.

Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]

Feld	Beschreibung
Name [name]	Hostname
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung von Fortinet Firewall-Cluster.
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Feld	Beschreibung
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet] (Fortsetzung)

Feld	Beschreibung
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung des Geräts.
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Fortinet Firewall.
Netzmaske [netmask]	Netzmaske von Fortinet Firewall.

Netzwerkadapter [cmdb_ci_network_adapter]

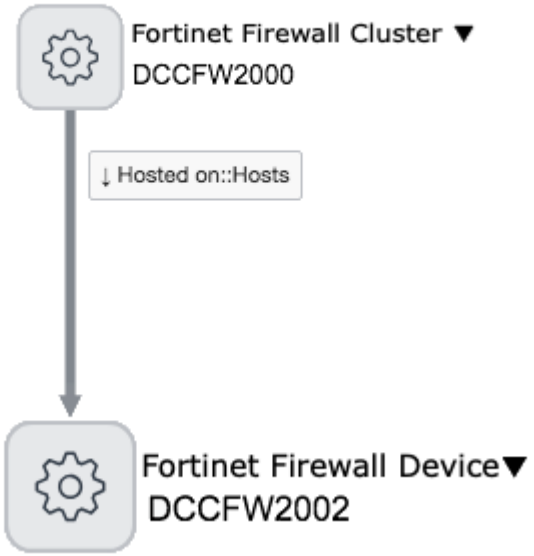
Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

Dies Abhängigkeitsansichten Ordnen Sie auf zu Fortinet Firewall-Geräte-CI zeigt an Fortinet Firewall-Cluster, zu dem er gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Fortinet Firewall-Discovery.

CI	Beziehung	CI
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Erstreckt sich von	Firewall-Cluster [cmdb_ci_firewall_cluster]
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Erstreckt sich von	Firewall-Gerät [cmdb_ci_firewall_device]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Routerschnittstelle [dscy_router_interface]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Seriennummer [cmdb_serial_number]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy Lastenausgleichsmodul-Discovery mit Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das HA-Proxy-Muster, um zu finden HAProxy Community-Lastenausgleichsmodule, die auf einem ausgeführt werden Linux Server. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

HAProxy Die Community-Edition ist ein Open Source-Lastenausgleichsmodul, das entweder im TCP- oder HTTP-Modus ausgeführt werden kann. Beachten Sie dies jedoch Discovery Unterstützt HAProxy Für den HTTP-Lastenausgleich wird der TCP-Lastenausgleich nicht unterstützt.

Beginnend mit Muster für Discovery und Service-Mapping Version 1.15.0, musterbasierte Discovery ist die Standardmethode für die Erkennung HAProxy Lastenausgleichsmodule. Für Informationen zu Probe-basiert HAProxy Discovery, siehe HAProxy Lastenausgleichsmodul-Discovery mithilfe von Probes.

Hinweis: HAProxy Discovery unterstützt die eins-zu-eins-Beziehungszuordnung zwischen einem Front-End-Port und einem Back-End-Port. Wenn mehrere Front-Ends mit demselben Back-End verbunden sind, ordnet der Discovery-Prozess nur die Beziehung von der niedrigsten Front-End-Portnummer in einem definierten Bereich dem Back-End-Port zu.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über zu erfahren HAProxy Lastenausgleichsmodule und ihre Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

Verifizieren HAProxy Ist auf installiert Linux Server

Verifizieren Sie HAProxy Software wird auf einem installiert und ausgeführt Linux Server.

Überprüfen Sie die Berechtigung zur Ausführung HAProxy Befehl

Stellen Sie sicher, dass Sie die Berechtigung zum Ausführen des folgenden Befehls haben: `<HAProxy-Installationspfad>/haproxy -V` .

Überprüfen Sie den Lesezugriff auf HAProxy Konfigurationsdatei

Überprüfen Sie, ob Sie Lesezugriff auf haben haproxy.cfg Datei.

SSH-Anmeldeinformationen erstellen

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des HA-Proxy-Musters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy Load Balancer [cmdb_ci_lb_haproxy]

Feld	Beschreibung
Name [name]	Name des HAProxy Lastenausgleichsmodul.
Version [version]	Version von HAProxy Lastenausgleichsmodul.
Beschreibung [short_description]	Beschreibung von HAProxy Prozess, der durch Ausführen des folgenden Befehls abgerufen wird: `haproxy: Version` .

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: `<LB name>:<LB port>` .
Port [port]	Port, auf dem der Lastenausgleichsmodul abhört.
IP-Adresse [ip_address]	IP-Adresse des Lastenausgleichsmodul-Service.
Letzter Port [Last_Port]	Höchste Portnummer, die vom Lastenausgleichsmodul-Service verwendet wird.
Load Balancer [load_balancer]	Verweist auf die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Name des Pools von Lastenausgleichsmodulen
Load Balancer [load_balancer]	Verweist auf die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].
Lastenausgleichsmethode [load_balancing_method]	Methode zum Lastenausgleich des Pools, z. B. Round Robin.
Neueste Discovery [Last_Discovered]	Zeitstempel der letzten Discovery.
Installationsstatus [install_status]	Installationsstatus des Lastenausgleichsmodul-Pools, z. B. installiert.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Name des Mitglieds des Lastenausgleichsmodul-Pools.
Service-Port [Service_Port]	Vom Poolmitglied verwendeter Port
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Pool [pool]	Verweist auf die Tabelle „Lastenausgleichsmodul-Pool“ [cmdb_ci_lb_Pool].
Load Balancer [load_balancer]	Verweist auf die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von HAProxy Lastenausgleichsmodul-Discovery.

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Zugeordnet zu::Zugeordnet von	Load Balancer-Service [cmdb_ci_lb_service]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer-Pool [cmdb_ci_lb_pool]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Pool [cmdb_ci_lb_pool]	Referenzen	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Service [cmdb_ci_lb_service]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Service [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	Hardware [cmdb_ci_hardware]

Erkennung „HPE BladeSystem Enclosure“

ServiceNow Discovery Verwendet das Discovery-Muster für HPE BladeSystem-Gehäuse, um BladeSystem zu erkennen, bei dem es sich um eine Reihe von Hewlett Packard Enterprise-Blade-Servercomputern handelt. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Sie die neueste Version von verwenden Muster für Discovery und Service-Mapping.
- Legen Sie SNMP-Anmeldeinformationen für das Gehäuse fest (vom Klassifizierer zu verwenden). Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .
- Legen Sie die SSH-Anmeldeinformationen für den Onboard-Administrator des Gehäuses fest (die von verwendet werden soll) Discovery Muster). Das für den Zugriff auf Onboard Administrator verwendete Konto muss über Berechtigungen zum Anzeigen aller Einschübe des Gehäuses verfügen, damit die Informationen der Blade-Server erfasst werden können. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .
- Überprüfen Sie die IP-Adresse des Onboard-Administrators, welche Discovery Wird für ausgeführt.
- Stellen Sie sicher, dass der Hostcomputer über erreichbar ist MID-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hervorhebungen und unterstützte Versionen

Das Muster wurde getestet anhand von:

- HPE BladeSystem c7000-Gehäuse G2 und G3
- HPE BladeSystem-Blades: HPE ProLiant BL460c
  - Generation 8, 9 und 10
  - ROM-Versionen: I31, I36, I41 (2014-2021)
  - Von einem Virtual Connect Manager/Virtual Connect Enterprise Manager (VCM/VCEM) verwaltete Blades haben eine logische Seriennummer. In diesem Fall ist die Seriennummer, die beispielsweise von WMI verfügbar gemacht wird, die logische und nicht die physische Nummer, wie es normalerweise der Fall ist. Beim Erstellen der Beziehung zwischen dem Blade- und dem BS-Server versucht das System, die physische und die logische Seriennummer mit denen des BS-Servers abzugleichen.
  - Bei der Erkennung von Blade-Servern mit logischen Seriennummern werden ihre logischen Seriennummern in **cmdb_serial_number** mit dem Typ **logisch** eingefügt. Dies ist ein neuer Seriennummerntyp, der zur Unterstützung dieser von HP eingeführten neuen Seriennummern erstellt wurde.

Hinweis: Die WMI stellt die logische Seriennummer als Bios-Seriennummer bereit. ESXi-Server werden von Probes erkannt. Das ESXiserver-CI erhält die logische Seriennummer als **Gehäuse**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des HPE BladeSystem Enclosure Discovery-Musters.

HPE BladeSystem-Gehäuse [cmdb_ci_hpe_bladesystem_Gehäuse]

Feld	Beschreibung
Name [name]	Name des Gehäuses.
UUID [UUID]	Eindeutiger Bezeichner des Gehäuses (proprietärer Bezeichner von HPE).
IP-Adresse [ip_address]	Management-IP des Gehäuses (Onboard Administrator-Adresse).
Modell-ID [model_id]	Typ des Gehäuses (Modell).
Hersteller [manufacturer]	Herstellername des Gehäuses („HP“ oder „HPE“, je nach Modell).
Seriennummer [serial_number]	Generierte Seriennummer gemäß der folgenden Konvention: **<Originalseriennummer des Gehäuses>::<UUID des Gehäuses>**.
Asset-Tag [asset_tag]	Asset-Tag, extrahiert aus den Daten des Gehäuses.
Modellnummer [model_number]	Teilenummer des Gehäuses (proprietär von HPE).
Midplane-Ersatzteilnummer [Midplane_spare_part_number]	Ersatzteilnummer (proprietär von HPE) der Mittelebene.
PDU-Typ [pdu_type]	Typ der Stromverteilungseinheit.
PDU-Ersatzteilnummer [pdu_spare_part_number]	Ersatzteilnummer der Stromverteilungseinheit (proprietär von HPE).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HPE BladeSystem-Gehäuse [cmdb_ci_hpe_bladesystem_Gehäuse] (Fortsetzung)

Feld	Beschreibung
Onboard-Administrator – Ablagetyp [onboard_admin_Tray_type]	Typ des Onboard Administrator-Tray.
Onboard-Administrator – Ersatzteilnummer des Trays [onboard_admin_tray_spare_part_number]	Ersatzteilnummer des Onboard Administrator-Tray (proprietär von HPE).
Seriennummer des Onboard-Administratorbereichs [Onboard_admin_Tray_Serial_number]	Seriennummer des Onboard Administrator-Tray.

HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]

Feld	Beschreibung
Name [name]	Generierter Wert gemäß der folgenden Konvention: **<Name des Gehäuses>/bay-<Positionsnummer>**
UUID [UUID]	Eindeutiger Bezeichner des Blade-Servers (proprietärer HPE-Bezeichner).
Logische UUID [uuid_logical]	Der logische eindeutige Bezeichner des HPE-Server-Blades (proprietärer Bezeichner von HPE).
Modell-ID [model_id]	Produktname des Blade-Servers (Modell).
Hersteller [manufacturer]	Herstellername des Blade-Servers („HP“ oder „HPE“, je nach Modell).
Seriennummer [serial_number]	Generierte Seriennummer gemäß der folgenden Konvention: **<Originalseriennummer des Blade>::<UUID des Blade>**.
Logische Seriennummer [Serial_number_logical]	Die logische Seriennummer des HPE-Server-Blades (proprietärer Bezeichner von HPE).
Asset-Tag [asset_tag]	Asset-Tag, extrahiert aus den Daten des Blade
Modellnummer [model_number]	Teilenummer des Blade (proprietär von HPE).
RAM (MB) [RAM]	RAM-Größe des Blade.
ROM-Version [rom_Version]	Version des ROM des Blade.
Ersatzteilnummer der Systemplatine [System_Board_spare_part_number]	Ersatzteilnummer der Hauptplatine des Blade-Systems (proprietär von HPE).
Startmodus [Boot_Mode]	Startmodus des Blade.
Status des sicheren Starts [Secure_Boot_Status]	Sicherer Platinenstatus des Blade.
Verwaltungsprozessortyp [Management_processor_type]	Verwaltungsprozessortyp des Blade (iLO-Version).
Name des Verwaltungsprozessors [Management_processor_Name]	Hostname des Verwaltungsprozessors des Blade.
Firmware-Version des Verwaltungsprozessors [Management_processor_Firmware_Version]	Version der Verwaltungsprozessor-Firmware des Blade.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade] (Fortsetzung)

Feld	Beschreibung
IP-Adresse des Verwaltungsprozessors [amanagement_processor_ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.
MAC-Adresse des Verwaltungsprozessors [Management_processor_mac_address]	MAC-Adresse des Verwaltungsprozessors des Blade.
Version des Energieverwaltungs-Controllers [Power_Management_Controller_Version]	Version des Energieverwaltungs-Controllers des Blade.
ILO Federation Capable [ILO_Federation_Capable]	iLofederation-Fähigkeit aktiviert/deaktiviert.
Bay-Nummer [Bay_number]	Positionsnummer des Gehäuses, in dem das Blade installiert ist.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
MAC-Adresse [mac_address]	Ethernet-Adresse des Blade-Verwaltungsprozessors (= MAC-Adresse der iLOnetwork-Schnittstelle).
Name [name]	Hostname des Verwaltungsprozessors des Blade.
IP-Adresse [ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „HPE BladeSystem Blade“ [cmdb_ci_hpe_bladesystem_Blade].

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
Name [name]	IPv4-IP-Adresse des Verwaltungsprozessors (iLO) des Blade.
IP-Adresse [ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.
NIC [nic]	Verweist auf die Tabelle „Netzwerkadapter“ [cmdb_ci_Network_Adapter].

Die Implementierung von HPE BladeSystem-Gehäuse CMDB Modell enthält drei neue CI-Klassen:

CMDB Modell: (Neue CI-Klassen)

Feld	Beschreibung
Gehäuse [cmdb_ci_Enclosure]	Allgemeine Klasse zur Darstellung einer beliebigen Gehäuseentität. Erweitert Hardware-CI-Klasse.
HPE BladeSystem-Gehäuse [cmdb_ci_hpe_bladesystem_Gehäuse]	CI-Klasse zur Darstellung der Gehäuse-Entität.
HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]	CI-Klasse zur Darstellung der Blade-Serverentität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Discovery Erstellt diese Beziehungen, um die Discovery von HPE BladeSystem Enclosure zu unterstützen.

CI	Beziehung	CI
HPE BladeSystem-Gehäuse [cmdb_ci_hpe_bladesystem_Gehäuse]	Enthält::Enthalten in	HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]
HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
IP-Adresse [cmdb_ci_ip_address]	references	Netzwerkadapter [cmdb_ci_network_adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	references	HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]
Seriennummer [cmdb_serial_number]	references	HPE BladeSystem-Gehäuse [cmdb_ci_hpe_bladesystem_Gehäuse]
Seriennummer [cmdb_serial_number]	references	HPE BladeSystem-Blade [cmdb_ci_hpe_bladesystem_Blade]

Zugehörige Informationen

SNMP-basierte Abfragen

IBM DB2 ein Linux Datenbank-Discovery

ServiceNow Discovery Verwendet das Discovery-Muster DB2 in Linux, um zu finden IBM DB2-Instanzen auf Linux Server.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung. Das Muster wird automatisch durch die Klassifizierung mit diesen DB2-Bezeichnern ausgelöst: tcp_Port, Name, installed_dir

Voraussetzungen

Konfigurieren Sie SSH-Anmeldeinformationen für Linux Server.

Stellen Sie außerdem sicher, dass der Benutzer über die Berechtigungen zum Ausführen der folgenden Befehle verfügt:

Identifikation für die DB2-UDB-Einstiegspunkttypen

```
". /" + $process.environmentVariables.HOME.value + "/sqllib/
db2profile; " + $process.environmentVariables.HOME.value +
"/sqllib/bin/db2level"

"source " + $installed_dir + "db2profile"

"db2 list database directory | grep \"Database name\" | grep -i
\"" + $entry_point.instance + "\" | head -1"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"db2level | grep \"DB2 v\""
```

Identifikation für die Db2-UDB-Einstiegspunkttypen # NONE

```
"cat " + $installed_dir + "/db2dump/db2diag.log | grep
\"INSTANCE:\" | grep " + $entry_point.instance + " | head -1"

"db2level | grep \"DB2 v\""
```

Identifikation für DB2 unter z/OS

```
"netstat -a | grep " + $entry_point.port

"ls -d /*/* |grep " + $id
```

Von Discovery während der horizontalen Erkennung erfasste Daten

In **Identifikation für DB2 UDB-Einstiegspunkttypen** und **Identifikation für DB2 UDB-Einstiegspunkttypen – NONE** werden die folgenden Tabellen und Felder erfasst:

DB2-Subsystem [cmdb_ci_DB_db2_instance]

Feld	Beschreibung
Name [name]	Der Name der DB2-Instanz.
TCP-Port(s) [tcp_port]	TCP-Port
Installationsverzeichnis [install_dir]	Installationsverzeichnis.
Version [version]	DB2-Version

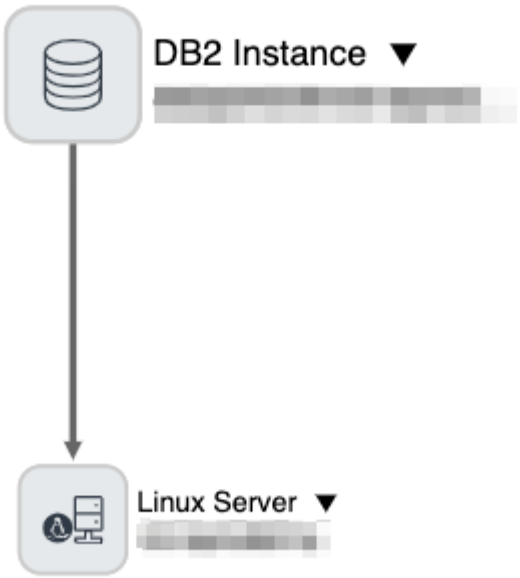
In „Identifikation für DB2 unter z/OS“ werden die folgenden Tabellen und Felder erfasst:

DB2-Subsystem [cmdb_ci_DB_db2_instance]

Tabelle und Feld	Beschreibung
Name [name]	Der Name der DB2-Instanz.
TCP-Port(s) [tcp_port]	TCP-Port
Installationsverzeichnis [install_dir]	Installationsverzeichnis.

Die Zuordnung der Abhängigkeitsansichten zeigt alle erkannten an IBM DB2-Instanzen in Ihrer Organisation und die Beziehungen zwischen ihnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Das Muster „IBM Db2 on Linux“ erstellt keine CI-Beziehungen.

IBM DB2 ein Windows Datenbank-Discovery

ServiceNow Discovery Verwendet das DB2-Discovery-Muster für Windows, um zu finden IBM DB2-Instanzen auf Windows Server.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung. Das Muster wird automatisch durch die Klassifizierung mit diesen DB2-Bezeichnern ausgelöst: tcp_Port, Name, installed_dir

Voraussetzungen

Stellen Sie sicher, dass der Benutzer über die Berechtigungen zum Ausführen der folgenden Befehle verfügt:

- `"\"" + $installed_dir + "\bin\db2cmd\" /c /w /i db2 list database directory"`
- `"\"" + $installed_dir + "\bin\db2cmd\" /c /w /i db2 list database directory | findstr \"Database name\" | findstr /i " + $entry_point.instance`
- `"\"" + $installed_dir + "\bin\db2level\""`

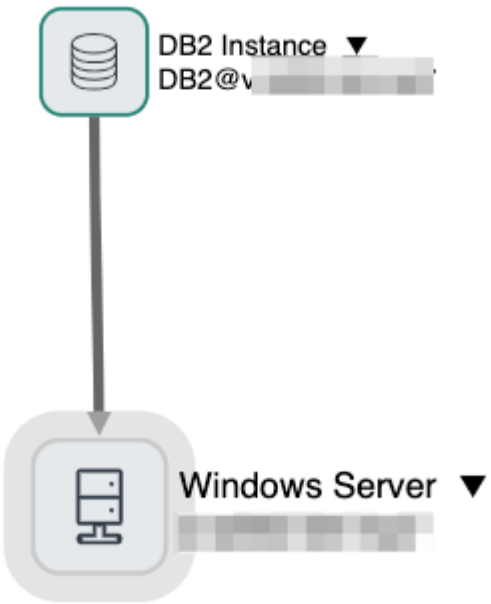
Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
name	Name der DB2-Instanz
tcp_port	TCP-Port
installed_dir	Installationsverzeichnis
Version	DB2-Version
db_name	Name der Datenbank.
pid	Prozess-ID der DB2-Instanz

Die Dependency Views-Zuordnung zeigt alle erkannten IBM DB2-Instanzen in Ihrer Organisation und die Beziehungen zwischen ihnen an.



CI-Beziehungen

Das Muster „IBM Db2 on Windows“ erstellt keine CI-Beziehungen.

IBM Informix Dynamic Server-Discovery

Die Anwendungen ServiceNow Discovery und Service-Mapping können den Informix Dynamic Server finden und zuordnen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anwender

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gewähren Sie dem Benutzer die Berechtigungen zum Ausführen der folgenden Befehle ohne erhöhte Rechte:

- $install_directory/bin/onstat -g dis

  Dieser Befehl ruft den Status und die Konfiguration des Informix Dynamic Servers ab.

- $install_directory/bin/dbaccess sysmaster

  Dieser Befehl führt eine SQL-Abfrage für das Master-Schema aus.

Derselbe Benutzer muss Leseberechtigung für die folgenden Verzeichnisse haben:

- install_directory + "/etc/sqlhosts

  Zugriff auf dieses Verzeichnis ist erforderlich, um Informationen über die Port-, Host- und Servicedefinition des Informix Dynamic Servers zu erhalten.

- /etc/services

  Zugriff auf dieses Verzeichnis ist erforderlich, um Informationen über die Host-Servicedefinition zu erhalten.

Berechtigungen

Konfigurieren Sie SSH-Anmeldeinformationen im Modul für Anmeldeinformationen der ServiceNow-Plattform für den Zugriff auf den Server, auf dem der Informix Dynamic Server gehostet wird.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Informix-Instanz [cmdb_ci_db_informix_instance]	Die Informix-Instanzattribute
tcp_port	
running_process	
Version	
install_directory	
config_file	
name	
Informix-Katalog [cmdb_ci_db_informix_catalog]	Die in der Informix-Instanz enthaltene Datenbank
Datenbank	

CI-Beziehungen

CI	Beziehung/Referenz	CI
Informix-Instanz [cmdb_ci_db_informix_instance]	Enthält::Enthalten in	Informix-Katalog [cmdb_ci_db_informix_catalog]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von oben nach unten

Während der Erkennung von oben nach unten erkennt Service-Mapping Verbindungen zwischen der Informix-Instanz und den Informix-Katalogen, die die Instanz enthält, und zeigt sie als Aufnahme in die Anwendungsservicezuordnung an.

IBM PowerHA SystemMirror für AIX Discovery

Die ServiceNow Discovery Die Anwendung verwendet das IBM PowerHA Cluster (HACMP)-Muster, um zu finden IBM PowerHA SystemMirror für AIX(Ehemals HACMP) Hochverfügbarkeitscluster auf AIX UNIX Und Linux Systeme, die auf ausgeführt werden IBM Plattformen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die folgende Anwendung aktuell ist

Muster für Discovery und Service-Mapping

Überprüfen Sie, ob sich das IBM PowerHA Cluster (HACMP)-Muster auf der Registerkarte Auslöser-Probes befindet

1. Navigieren zu **CI-Klassifizierung** > **UNIX**an.
2. Wählen Sie Aus **AIX** .
3. In **Löst Probes aus** Überprüfen Sie, ob das IBM PowerHA Cluster (HACMP)-Muster als Exploration aufgeführt ist, die nach dem AIX-Server-Muster ausgeführt wird.

Weitere Informationen zu finden AIX Server-Discovery, siehe Erkennung von AIX-Servern.

Überprüfen Sie die Server-IP-Adresse oder den Hostnamen

Überprüfen Sie, ob die Server-IP-Adresse oder der Hostname während der Discovery verwendet wird. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Verifizieren MID-Server Zugriff

Überprüfen Sie, ob MID-Server Hat Zugriff auf den Zielhost und kann alle Befehle ausführen, die im Muster implementiert sind.

Konfigurieren Sie ein UNIX Anwender mit den folgenden Berechtigungen

Konfigurieren Sie ein UNIX Anwender mit Berechtigungen zum Ausführen aller im offiziellen Ordner definierten Befehle IBM Dokumentation und die folgenden Befehle für AIX.

Befehl	Beschreibung
lssrc -s clstrmgrES	Überprüfen Sie, ob der clstrmgrES-Prozess ausgeführt wird
lslpp -l cluster.license	Rufen Sie die Lizenz- und Versionsdaten des Clusters ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
lslpp -l cluster.license | awk '{$1= $2=$3=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'	Ruft die Versionsdaten der Softwarebezeichnung des Clusters ab
/Usr/es/sbin/Cluster/Utilities/clRGinfo -A | awk „{print $1,$2}“ | grep -E -V „denied|error“	Rufen Sie den Namen und Typ der Ressourcengruppe ab
/Usr/es/sbin/Cluster/Utilities/clRGinfo -s | grep -E -V „verweigert|Fehler“	Rufen Sie weitere Informationen zu Ressourcengruppen ab
/Usr/es/sbin/Cluster/Utilities/clfindres -s | grep -E -V „verweigert|Fehler“	Alternativer Befehl zum Abrufen weiterer Informationen zu Ressourcengruppen
/Usr/es/sbin/Cluster/ Utilities/clshowres | grep -E „Ressourcengruppenname|Volume“ | grep -E -V „gleichzeitig|automatisch| Fehler|verweigert“ | sed „s/Volume-Gruppen/Volume-Gruppen-Namen/“ | awk „{print substr($0,$4)))}“ | sed „N;s/ \n/ /“	Ruft Volume-Gruppen ab, die Ressourcengruppen zugeordnet sind
/Usr/es/sbin/Cluster/clstat -o | grep „Ressourcengruppe“ | grep -E -V „Fehler|abgelehnt“ | awk „{print $3, $5, $6}“	Status der Ressourcengruppe(n) abrufen
/usr/es/sbin/cluster/utilities/cltopinfo -c	Rufen Sie den Clusternamen ab
/Usr/es/sbin/Cluster/Utilities/cllscf	Alternativer Befehl zum Abrufen des Clusternamens
lssrc -ls clstrmgrES	Aktuellen Status des Clusters abrufen
/usr/es/sbin/cluster/clstat -o | awk '{$1=$2=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'	Rufen Sie die Cluster-ID ab
/Usr/es/sbin/Cluster/Utilities/cllsclstr | grep -E -V „error|denied“ | awk „{print $1}“	Alternativer Befehl zum Abrufen der Cluster-ID
/Usr/bin/odmget HACMPcluster| grep -W ID | grep -E -V „error|denied“	Alternativer Befehl zum Abrufen der Cluster-ID
/Usr/es/sbin/Cluster/Utilities/cltopinfo -n | grep -E -V „error|denied“	Clusterknoten-Namen abrufen
/Usr/es/sbin/Cluster/Utilities/cllsnode | grep -E -V „error|denied“	Alternativer Befehl zum Abrufen des/der Namen des/der Clusterknoten
/Usr/es/sbin/Cluster/clstat -o | grep -i „Knoten:“ | awk „{print $2, $4}“	Clusterknoten-Status abrufen
Lscluster -m | grep -E „Knotenname| Status des Knotens“ | grep -E -V	Alternativer Befehl „Clusterknoten abrufen“-Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
„FEHLER|lscluster“ | awk „{print $2, $3, $4}“ | sed „N;s/\n/ /“	
/Usr/es/sbin/Cluster/Utilities/cllsif | grep -E -V „error|denied“ | awk „{print $1, $2, $6, $7}“	Rufen Sie Netzwerkschnittstelleninformationen ab
lspv | grep -E -V „Fehler|abgelehnt“	Rufen Sie Informationen zu physischen Volumes ab
Lsvg | grep -E -V „Fehler|abgelehnt“	Rufen Sie Informationen zu Volumegruppen ab
Lsvg -o | grep -E -V „Fehler|verweigert“	Rufen Sie Informationen zu den aktiven Volume-Gruppen ab
/usr/es/sbin/cluster/utilities/clshowres | grep 'Concurrent Volume Group' | awk '{$1=$2=$3=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'	Rufen Sie Informationen zu den gleichzeitigen Volumegruppen ab
hostname	Ruft den aktuellen Knotenhostnamen ab
Nslookup-Hostname	Konvertieren Sie den Hostnamen in FQDN

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des IBM PowerHA Cluster (HACMP)-Musters.

Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]

Feld	Beschreibung
Name [name]	Der Name der Ressourcengruppe, die im Clusterkontext konfiguriert ist.
Server [Server]	Der Name des PowerHA/HACMP-Clusters.
Ressourcengruppenstatus [resource_Group_Status]	Der Status der Ressourcengruppe im Clusterkontext. Beispiel: Online
Ressourcengruppentyp [resource_Group_type]	Typ der Ressourcengruppe. Beispiele: Gleichzeitig, nicht gleichzeitig
Cluster [cluster]	Der Name des PowerHA/HACMP-Clusters, zu dem die Ressourcengruppe gehört.

UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]

Feld	Beschreibung
Name [name]	Der Name der Volumegruppe im Clusterkontext.
Ressourcentyp [resource_type]	Der Ressourcentyp (Volumegruppe)
Ressourcenstatus [resource_Status]	Der Status der Volumegruppe. Beispiele: Online, Offline

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX-Clusterressource [cmdb_ci_unix_cluster_resource] (Fortsetzung)

Feld	Beschreibung
Cluster [cluster]	Der Name des PowerHA/HACMP-Clusters, zu dem die Volumegruppe gehört.

UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]

Feld	Beschreibung
Name [name]	Der Name des Knoten, der am Cluster teilnimmt
Knotenstatus [node_State]	Der Status des Clusterknotens im Kontext des CI-Status. Beispiel: NACH OBEN, UNTEN, UNBEKANNT.
Knotenstatus [node_Status]	Der Status des Knotens im Kontext der Ressourcengruppe, zu der er gehört
IP-Adresse [ip_address]	Die dem Knoten zugewiesenen IP-Adressen
Cluster [cluster]	Der Name des Clusters, zu dem der Clusterknoten gehört.

AIX-Server [cmdb_ci_aix_server]

Feld	Beschreibung
Name [name]	Name des AIX-Servers, der den Clusterknoten im Kontext des PowerHA/HACMP-Clusters darstellt.

UNIX-Cluster [cmdb_ci_unix_cluster]

Feld	Beschreibung
Name [name]	Der Name des PowerHA/HACMP-Clusters.
Cluster-ID [cluster_id]	Die ID des PowerHA/HACMP-Clusters. Beispiel: 0123456789
Clusterstatus [cluster_status]	Der aktuelle Status des PowerHA/HACMP-Clusters. Beispiele: ST_STABLE, NOT_CONFIGURED
Clusterversion [Cluster_Version]	Die Version des PowerHA/HACMP-Clusters. Beispiele: 5.5; 6.1; 7.2
Clustertyp [Cluster_type]	Der Typ des PowerHA/HACMP-Clusters. Nur relevant für Versionen 7.2 und höher. Beispiel: Gestreckt
Beschreibung [short_description]	Beschreibung des PowerHA/HACMP-Clusters (Version, ID).

Virtuelle Cluster-IP [cmdb_ci_cluster_vip]

Feld	Beschreibung
Name [name]	Der Schnittstellenname des Clusterknotens.
IP-Adresse [ip_address]	Hostname oder IP-Adresse, bei der der Hostname den Namen der Netzwerkschnittstelle des Clusterknotens und die IP-Adresse die IPv4-Adresse darstellt, die dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

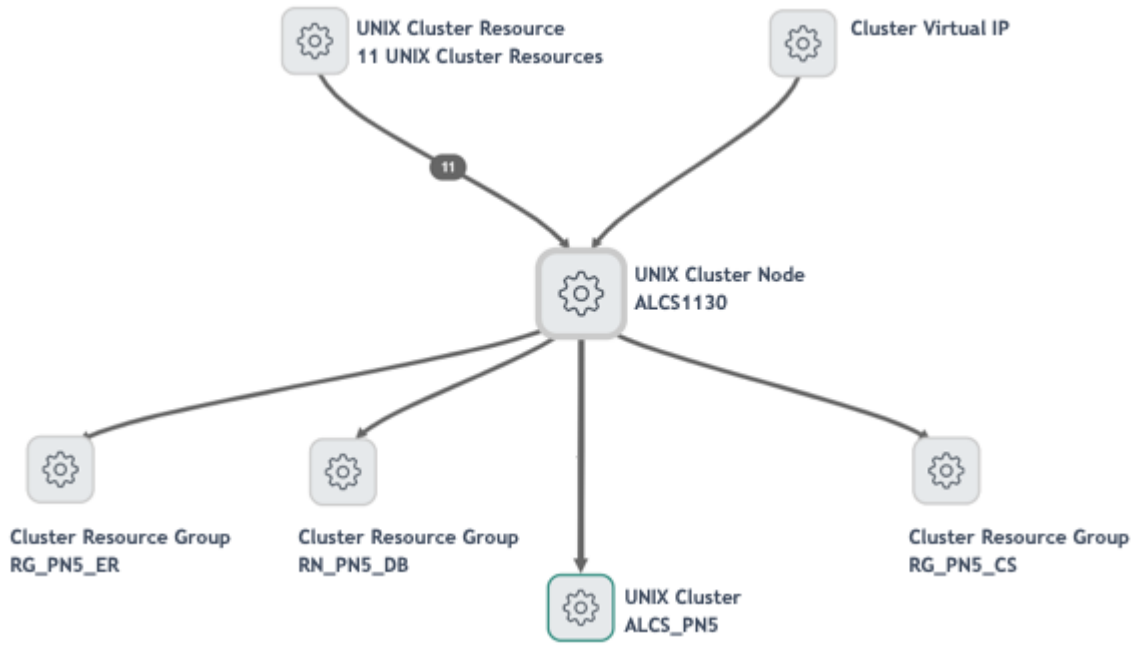
Virtuelle Cluster-IP [cmdb_ci_cluster_vip] (Fortsetzung)

Feld	Beschreibung
	Netzwerkschnittstellennamen zugeordnet ist. (Da der IBM PowerHA/HACMP-Cluster keine dedizierte VIP-Adresse hat).
Cluster [cluster]	Der Name des PowerHA/HACMP-Clusters.

Die Dependency Views-Zuordnung zeigt alle erkannten Cluster-CIs in Ihrer Organisation und die Beziehungen zwischen ihnen an.

In diesem Beispiel UNIX Clusterknoten stellt einen Cluster von dar UNIX Cluster. UNIX Clusterknoten ruft Ressourcen von ab UNIX Clusterressource und verwendet virtuelle Cluster-IP. UNIX Der Clusterknoten enthält drei Cluster-Ressourcengruppen.

Dependency Views-Beispielzuordnung



CI-Beziehungen

Die folgenden Beziehungen werden erstellt, um die Erkennung von IBM HACMP/PowerHA-Clustern zu unterstützen:

CI	Beziehung	CI
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	UNIX-Cluster [cmdb_ci_unix_cluster]
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Enthält::Enthalten in	Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]
Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]	Enthält::Enthalten in	UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	UNIX-Cluster [cmdb_ci_unix_cluster]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet von::Verwendet	UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]
UNIX-Cluster [cmdb_ci_unix_cluster]	Virtualisiert von::Virtualisiert	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
UNIX-Cluster [cmdb_ci_unix_cluster]	Enthält::Enthalten in	Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	AIX-Server [cmdb_ci_aix_server]

Erkennung der IBM-Virtualisierung und Hardware Management Console

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das IBM HMC Server-Muster, um Informationen zu Hardware Management Console (HMC), Frame- und LPAR-Servern zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery unterstützt die folgenden CIs:

- HMC-Server
- IBM-Frame
- LPAR-Instanz (Logische Partition)

  Eine LPAR ist das Äquivalent von IBM zu einem virtuellen Computer.

- LPAR-Ressource

Discovery wird auf dem HMC-Server und den einzelnen AIX-Maschinen (LPARs) verwendet.

Das IBM HMC Server-Muster wird mit SSH ausgeführt. Die Ausführung auf wird unterstützt IBM AIX-Betriebssystem für LPAR und unter Linux nur für HMC-Server.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die Berechtigungen für HMC- und AIX-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie, ob Sie über Berechtigungen für die folgenden HMC-Befehle verfügen:
  - `lssyscfg`
  - `lshmc`
  - `lshwres`
- Überprüfen Sie, ob Sie über Berechtigungen für den folgenden AIX-Befehl (LPAR) verfügen: `Lparstat: i` .

> **Hinweis:** Die `Lparstat: i` Der Befehl ist zusätzlich zu den für die AIX-Server-Discovery erforderlichen Befehlen. Weitere Informationen zur AIX-Server-Discovery finden Sie unter Erkennung von AIX-Servern. Eine Liste der AIX-Befehle finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Konfigurieren Sie SSH-Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen auf dem ServiceNow AI Platform. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Führen Sie eine horizontale Discovery für HMC-Server und LPARs aus

1. Führen Sie eine Discovery für die HMC-IP-Adresse aus.
2. Führen Sie nur dann eine Discovery für die LPARs mit der IP-Adresse des AIX-Computers aus, wenn die HMC-Server-Discovery erfolgreich abgeschlossen wurde.

Weitere Informationen zum Ausführen einer Discovery finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des IBM HMC Server-Musters.

IBM HMC-Server [cmdb_ci_hmc_Server]

Feld	Beschreibung
Name [name]	Name des HMC.
Frame-Anzahl [Frame_count]	Anzahl der für das HMC verwalteten Frames. Ein Frame ist der physische Computer, auf dem sich die LPARs befinden. Ein Frame entspricht einem ESX-Computer.
Seriennummer [Seriennummer]	Seriennummer des HMC-Servers.
IP-Adresse [ip_address]	IP-Adresse des HMC.
BS-Version [os_Version]	Betriebssystemversion.
CPU-Typ [cpu_type]	CPU-Typ
CPU-Geschwindigkeit (MHz) [cpu_Speed]	CPU-Geschwindigkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM HMC-Server [cmdb_ci_hmc_Server] (Fortsetzung)

Feld	Beschreibung
CPU-Anzahl [cpu_count]	CPU-Anzahl.
Anzahl der CPU-Kerne [cpu_Core_count]	Anzahl der CPU-Kerne.
RAM (MB) [RAM]	Arbeitsspeicher-RAM.

IBM-Frame [cmdb_ci_ibm_Frame]

Feld	Beschreibung
Name [name]	Name des Frames.
Seriennummer [Seriennummer]	Seriennummer des Frame-Servers.
Aktuell verfügbare Prozessoreinheiten [curr_avail_sys_proc_units]	Aktuell verfügbare Prozessoreinheiten.
Konfigurierbare Prozessoreinheiten [Configurable_sys_proc_units]	Konfigurierbare Prozessoreinheiten.
Installierte Prozessoreinheiten [installed_sys_proc_units]	Installierte Prozessoreinheiten.
Aktuell verfügbare Arbeitsspeichereinheiten [curr_avail_sys_mem]	Aktuell verfügbare Arbeitsspeichereinheiten.
Konfigurierbare Arbeitsspeichereinheiten [Configurable_sys_mem]	Konfigurierbare Arbeitsspeichereinheiten.
Installierte Arbeitsspeichereinheiten [installed_sys_mem]	Installierte Arbeitsspeichereinheiten.

IBM LPAR-Instanz [cmdb_ci_lpar_instance]

Feld	Beschreibung
Name [name]	Name der LPAR-Instanz.
Status [state]	Betriebsstatus. • Wird ausgeführt: Übersetzt in auf. • Nicht aktiviert und nicht verfügbar: In „aus“ übersetzen.
Seriennummer [serial_number]	Seriennummer der LPAR.
Objekt-ID [object_id]	Eindeutiger Objektbezeichner. Dieser Bezeichner wird aus der Seriennummer des Frames und dem LPAR-Bezeichner verkettet.
Ist VIO [is_vio]	Identifiziert die LPAR als VIO-Server Ein VIO-Server ist der LPAR, der die physischen Komponenten für andere LPARs verwaltet, z. B.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM LPAR-Instanz [cmdb_ci_lpar_instance] (Fortsetzung)

Feld	Beschreibung
	Netzwerkschnittstellenkarten (NICs) und optische Laufwerke.
VIO-Server [vio_Servers]	• Client-LPARs: Identifiziert die VIO-Server, die die Client-LPARs verwalten. • VIO-Server: Gibt die Client-LPARs an, die die VIO-Server verwalten.
Aktuelle min. Prozesseinheiten [curr_min_proc_units]	Mindestanzahl an Verarbeitungseinheiten, die der Partition dynamisch zugewiesen werden können
Laufende Prozesseinheiten [Run_proc_units]	Anzahl der Verarbeitungseinheiten, die für die Partition geändert werden
Aktueller Arbeitsspeicher [curr_mem]	Die der Partition zugewiesene Arbeitsspeichermenge in Megabyte (MB).
Ausgeführter Arbeitsspeicher [Run_mem]	Aktuelle Arbeitsspeichermenge in MB, in der sich die Partition geändert hat.

LPAR-Ressource [cmdb_ci_lpar_resource]

Feld	Beschreibung
Hohe Wasserzeichen-VCPU [High_Watermark_vcpu]	Höchster aufgezeichneter Wert von **Virtuelle Online-CPUs** Feld, wie von erfasst `Lparstat-i` Befehl. Da der Wert dynamisch ist, können sich die Ergebnisse einer Discovery auf den Wert auswirken: • Wenn der Wert von **Virtuelle Online-CPUs** Feld ist niedriger als der von erfasste Wert `Lparstat-i` Befehl, der Wert ändert sich nicht. • Wenn der Wert von **Virtuelle Online-CPUs** Feld ist höher als der von erfasste Wert `Lparstat-i` Befehl, der höhere Wert wird verwendet.
Knotenname [node_Name]	Name der Instanz zusammen mit dem Feld, das auf das LPAR-Instanz-CI verweist.

Seriennummer [cmdb_serial_number]

Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer des CI

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von IBM Virtualisierung und HMC-Discovery.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
IBM HMC-Server [cmdb_ci_hmc_Server]	Definiert Ressourcen für::Erhält Ressourcen von	IBM HMC-Prozessorpool [cmdb_ci_processor_Pool]
IBM LPAR-Instanz [cmdb_ci_lpar_instance]	Virtualisiert von::Virtualisiert	IBM-Frame [cmdb_ci_ibm_Frame]
IBM-Frame [cmdb_ci_ibm_Frame]	Verwaltet von::Verwaltet	IBM HMC-Server [cmdb_ci_hmc_Server]
IBM HMC-Prozessorpool [cmdb_ci_processor_Pool]	Mitglieder::Mitglied von	IBM LPAR-Instanz [cmdb_ci_lpar_instance]

IBM WebSEAL Discovery

Die ® Discovery-Anwendung verwendet IBM WebSEAL Zu suchende Muster WebSEAL Anwendungen, Webanwendungsserver und Verbindungen in Ihrer Infrastruktur. Um einige dieser Ressourcen zu erkennen, muss installiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ® Speichern.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Detaillierte Informationen zu IBM WebSEAL

Informationen finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Authentifizierung

Die WebSEAL Der Authentifizierungsprozess umfasst die HTTP-Headerauthentifizierung mit Standard-Anmeldeinformationen Virtual Server Interface .

Wenn Sie Discovery zum ersten Mal ausführen, konfigurieren Sie die Anmeldeinformationsaffinität für Discovery und Orchestration Anmeldeinformationsaffinität für Discovery und Orchestration .

Hinweis: Anmeldeinformationsaffinität ist im Debug-Modus nicht verfügbar.

Konfiguriert MID-Server

Stellen Sie sicher, dass MID-Server Hat Zugriff und Berechtigungen zum Senden von HTTPS-Anforderungen an die WebSEAL Anwendung.

Konfigurierte Anwenderberechtigungen zum Ausführen von API-Aufrufen

Stellen Sie sicher, dass der Anwender die Berechtigung zum Ausführen der folgenden API hat:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `/Net/General`
- `/Net/dns`
- `/wga/reverseProxy`
- `/wga/reverseProxy/<reverse_proxy_id>/Configuration/stanza/Junction/entry_Name/match-vhj-first`
- `/wga/reverseProxy/<reverse_proxy_id>/Junction`
- `/wga/reverseProxy/"<reverse_proxy_id>/Junction?junctions_ID=<junction_id>`
- `/wga/Widgets/Health.JSON`

HTTP-Klassifizierung aktiviert

Die IBM WebSEAL Das Muster wird ausgelöst, wenn Sie die Discovery auf dem Server ausführen, auf dem der ausgeführt wird WebSEAL Ist aktiviert. Stellen Sie sicher, dass die HTTP-Klassifizierung in der Instanz vorhanden ist. Weitere Informationen finden Sie unter HTTP-Klassifizierung erstellen Und Erkennung über einen HTTP- oder HTTPS REST-Aufruf ausführen

Während der horizontalen Erkennung erfasste Daten

Feld	Beschreibung
ISAM-Server [cmdb_ci_isam_Server]	
name	Der Name des Servers, wie von zurückgegeben `/Net/General` API-Aufruf. Wenn das Feld leer ist, `Nslookup` In der IP-Adresse wird versucht, dieses Feld auszufüllen.
IP-Adresse [ip_address]	Die IP-Adresse gemäß dem Discovery-Zeitplan/-Konfiguration.
fqdn	Die `Search_Domain` Zurückgegeben von `/Net/dns` API-Aufruf.
WebSeal [cmdb_ci_App_Server_webseal]	
name	Der Name des WebSEAL Server, wie von der API zurückgegeben.
IP-Adresse [ip_address]	Die IP-Adresse gemäß dem Discovery-Zeitplan/-Konfiguration.
fqdn	Die `Search_Domain` Zurückgegeben von `/Net/dns` API-Aufruf.
install_status	Der Status wird auf festgelegt **Installiert** Standardmäßig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
operation_status	Der Status wird auf festgelegt **Betriebsbereit** Standardmäßig.
install_directory	Gemäß der Identifizierungsanforderung wird dieses Feld mit dem FQDN des Servers ausgefüllt.
WebSeal-Reverse-Proxys [cmdb_ci_webseal_Reverse_Proxy]	
name	Der Name der Ressource gemäß der API-Antwort.
object_id	Die ID der Ressource, der API-Antwort.
install_status	Gibt an, ob die Installation aktiviert ist.
operational_status	Gibt an, ob der Vorgang gestartet wurde.
Service_type: Hartcodiert	Der Status wird auf festgelegt `Webseal-Reverse-Proxy` Standardmäßig.
webseal_Health_Status	Die WebSEAL Gemeldeter Integritätsstatus in Bezug auf `/wga/Widgets/Health.JSON` API-Aufruf
WebSeal-Verbindungen [cmdb_ci_webseal_Junction]	
name	Der Name der Ressource gemäß der API-Antwort.
object_id	Die ID der Ressource, erstellt als eindeutige Hash-Nummer, die dem Namen der Ressource entspricht, bei der Groß-/Kleinschreibung beachtet werden muss. **Hinweis:** Die Nichtberücksichtigung der Groß-/Kleinschreibung der Abfragen kann doppelte Felder erstellen, wenn der **Name** Wert ist identisch mit **Objekt-ID** Wert. Eines der Identifizierungsattribute muss geändert werden, um einen eindeutigen Wert zu haben.
install_status	Hartcodiert in Status „installiert“
operational_status	Hartcodiert in Betriebsstatus
Stateful_Junction	Boolescher Wert, der angibt, ob es sich um eine statusbehaftete Verbindung handelt
Transparent_path_Junction	Boolescher Wert, der angibt, ob es sich um eine transparente Pfadverbindung handelt
Junction_type	Liste für den Typ der Verbindung
WebSeal-Back-End-Server [cmdb_ci_webseal_Backend_Server]	
name	Der Name der Ressource gemäß API-Antwort
object_id	Die ID der Ressource gemäß API-Antwort
install_status	Der Status der Ressource gemäß dem Wert „aktiviert“ in der API-Antwort
operational_status	Der Status der Ressource gemäß dem Wert „Vorgangsstatus“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
server_id	Die UUID, die zur Identifizierung des Verbindungswebservers verwendet wird
http_Port	HTTP-Port des Back-End-Drittparteiservers. Gilt, wenn der Verbindungstyp tcp ist.
service_port	TCP-Port des Back-End-Drittparteiservers. Der Standardwert ist 80 für TCP-Verbindungen und 443 für SSL-Verbindungen
Priorität	Die Priorität des Servers (1–9). Der Standardwert ist 9.

Musterbeziehungen

CI	Beziehungstyp	CI
Webseal [cmdb_ci_app_server_webseal]	Wird ausgeführt auf::Wird ausgeführt	ISAM-Server [cmdb_ci_isam_Server]
WebSeal-Reverse-Proxy [cmdb_ci_webseal_Reverse_Proxy]	Gehostet auf::Hostet Referenz [load_Balancer]	Webseal [cmdb_ci_app_server_webseal]
WebSeal-Reverse-Proxy [cmdb_ci_webseal_Reverse_Proxy]	Wird ausgeführt auf::Wird ausgeführt Referenz [isam_Server]	ISAM-Server [cmdb_ci_isam_Server]
WebSeal-Verbindung [cmdb_ci_webseal_Junction]	Zugeteilt an::zugeteilt Referenz [Service]	WebSeal-Reverse-Proxy [cmdb_ci_webseal_Reverse_Proxy]
WebSeal-Verbindung [cmdb_ci_webseal_Junction]	Eigentümer von::Eigentum von Referenz [Pool]	Mitglied des Lastenausgleichsmodul-Pools [cmdb_ci_webseal_Backend_Server]
WebSeal-Verbindung [cmdb_ci_webseal_Junction]	Nur Referenz [load_Balancer]	Webseal [cmdb_ci_app_server_webseal]

Hinweis: Derzeit ist die Beziehung zwischen den Back-End-Servern und tatsächlichen Server-CIs in der CMDB für HD nicht möglich.

IBM WebSphere-Anwendungsserver-Discovery mithilfe von Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet Websphere unter Windows und Websphere in Unix-Mustern, um zu finden IBM WebSphere-Anwendungsserver. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die IBM WebSphere Application Server ist ein Software-Framework mit Middleware, das Java-basierte Webanwendungen hostet. Discovery Identifiziert und klassifiziert Informationen über IBM WebSphere-Anwendungsserver auf beiden Windows Und Linux Computer.

Hinweis: Beginnend mit Visibility Content Version 6,1.0, musterbasierte Discovery ist die Standardmethode für die Erkennung IBM WebSphere-Anwendungsserver. Die WebSphere-Probes sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter IBM WebSphere-Server-Discovery mithilfe von Probes.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen für Windows Discovery

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind:

- Muster für Discovery und Service-Mapping
- Visibility Content

Aktivieren Sie PowerShell auf dem MID-Server

Weitere Informationen finden Sie unter MID Server zur Verwendung von PowerShell einrichten.

Überprüfen Sie den Zugriff auf Dateien und Verzeichnisse

Überprüfen Sie den Zugriff auf die folgenden Dateien und Verzeichnisse:

- Installationsverzeichnis des Produkts
- Konfigurationsverzeichnis des Produkts
- versionInfo.bat
- WAS.product
- BASE.product
- Profil.Version
- Express.product
- application.xml
- server.xml
- cell.xml

Erstellen Windows Anmeldeinformationen

Weitere Informationen finden Sie unter Windows-Anmeldeinformationen .

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Voraussetzungen für Linux Discovery

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind:

- Muster für Discovery und Service-Mapping
- Visibility Content

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie SSH auf WebSphere-Anwendungsserver

Weitere Informationen finden Sie im artikel „SSH auf Linux- oder UNIX-Servern einrichten“ im Abschnitt „WebSphere-Automatisierung“ von IBM Dokumentation (https://www.ibm.com/docs/en/products).

Überprüfen Sie den Zugriff auf Dateien und Verzeichnisse

Überprüfen Sie den Zugriff auf die folgenden Dateien und Verzeichnisse:

- Installationsverzeichnis des Produkts
- Konfigurationsverzeichnis des Produkts
- Oeconsol
- WAS_HOME
- CONFIG_ROOT
- versionInfo.sh
- WAS.product
- BASE.product
- Profil.Version
- Express.product
- application.xml
- server.xml
- cell.xml

SSH-Anmeldeinformationen erstellen

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Überprüfen Sie erhöhte Rechte für IBM WebSphere Application Server-Befehle

Weitere Informationen finden Sie unter IBM WebSphere-Anwendungsserver (auf UNIX) Tabelle in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen von Websphere unter Windows und Websphere auf Unix-Mustern.

IBM Websphere [cmdb_ci_app_server_websphere]

Feld	Beschreibung
Name [name]	Name des WebSphere-Anwendungsservers.
Version [version]	Aktuelle Version des WebSphere-Anwendungsservers.
Knoten [node]	Name des Knotens, der den WebSphere-Anwendungsserver oder die Server gruppiert.
Zelle [Zelle]	Name der Zelle, die einen oder mehrere Knoten des WebSphere-Anwendungsservers gruppiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

WebSphere-EAR [cmdb_ci_App_Server_WS_ear]

Feld	Beschreibung
Name [name]	Name der Enterprise Application Archive-Datei (EAR).
Installationsverzeichnis [install_directory]	Installationsverzeichnis der EAR-Datei.

Webservice [cmdb_ci_Web_Service]

Feld	Beschreibung
Name [name]	Name des Webservice.
Service-ID [Service_ID]	ID des Webservice.
Attribute [Attribute]	Zusätzliche Attribute des Webservice.

WebSphere-Zelle [cmdb_ci_websphere_cell]

Feld	Beschreibung
Name [name]	Name der WebSphere-Zelle.
Zell-ID [CELL_ID]	ID der WebSphere-Zelle.
Zelltyp [cell_type]	Typ der WebSphere-Zelle.
Zell-Discovery-Protokoll [CELL_Discovery_Protocol]	Zell-Discovery-Protokoll.
Beschreibung [short_description]	Beschreibung der Zelle, falls eine angegeben wurde. Dieses Feld wird in ausgefüllt Linux Nur Discovery.

CI-Beziehungen

Discovery Erstellt diese Beziehungen, um die WebSphere Application Server-Discovery für beide zu unterstützen Windows Und Linux Systeme.

CI	Beziehung	CI
IBM Websphere [cmdb_ci_app_server_websphere]	Enthält::Enthalten in	WebSphere-Zelle [cmdb_ci_websphere_cell]
IBM Websphere [cmdb_ci_app_server_websphere]	Enthält::Enthalten in	WebSphere-EAR [cmdb_ci_App_Server_WS_ear]
Webservice [cmdb_ci_Web_Service]	Wird ausgeführt auf::Wird ausgeführt	IBM Websphere [cmdb_ci_app_server_websphere]

InfiniBox-Erkennung

ServiceNow Discovery verwendet das InfiniBox-Muster, um Instanzen zu suchen und zuzuordnen. Um diese Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Store installieren.

Die Erkennung verwendet mehrere Muster, um InfiniBox-Speichersystemdaten zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Anwendungen Muster für Discovery und Service-Mapping und CMDB CI Class Models aus dem ServiceNow Store installieren, da die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beiden Anwendungen voneinander abhängig sind. Sie können die Muster zur Erkennung von InfiniBox-Komponenten auf der ServiceNow AI Platform mit Paris-Release oder höher verwenden.

Das InfiniBox Enterprise-Speicher-Array bietet eine schnellere Performance, hohe Verfügbarkeit und eine Multi-Petabyte-Skalierung für gemischte Anwendungs-Arbeitsauslastung. Das Hardware-Redundanzdesign von InfiniBox ermöglicht eine schnelle Wiederherstellung nach Komponentenfehlern.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Hinweis: Die Erkennung von „Hosts“ und „Clustern“, die dem InfiniBox-System zugeordnet sind, wird ab Version 1.0.83 des Plugins „Muster für Discovery und Service-Mapping“ (sn_itom_pattern) nicht unterstützt.

- Installieren Sie die folgenden Plugins:
  - Plugin „CMDB CI Class Models“ (Version 1.28.0 oder höher)
  - Plugin „Discovery and Service Mapping Patterns“ (Version 1.0.81 oder höher)
- Legen Sie Anmeldeinformationen für die Standardauthentifizierung für das InfiniBox-Speichersystem fest.
- Legen Sie einen Anmeldeinformationsalias fest, und ordnen Sie ihn dem Anmeldedatensatz des InfiniBox-Systems zu.
- Setzen Sie den Erkennungszeitplantyp auf „Serverlos“.
- Stellen Sie sicher, dass der MID Server Zugriff auf das Zielgerät hat.

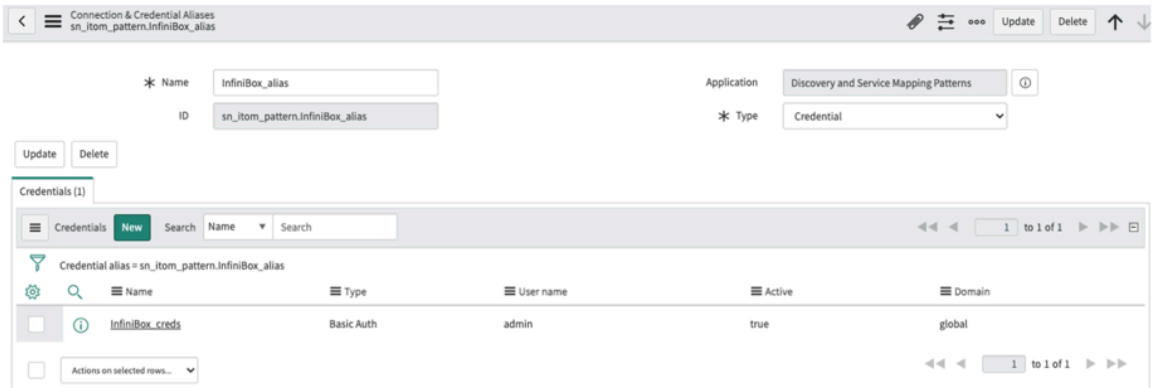
Authentifizierung

Konfigurieren Sie die Anmeldeinformationen der Standardauthentifizierung für die Authentifizierung der REST API-Aufrufe. Sie werden für die Erkennung der CI-Typen verwendet, die dem InfiniBox-Speichersystem zugeordnet sind.

1. Navigieren Sie zu **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen neuen **Anmeldeinformationsdatensatz**.
3. Erstellen Sie im Formular der zugehörigen Liste „Anmeldeinformationen“ einen neuen Anmeldeinformationendatensatz für die **Standardauthentifizierung**. Konfigurieren Sie die Parameter für die **Standardauthentifizierung**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aliasse für Verbindungen und Anmeldeinformationen



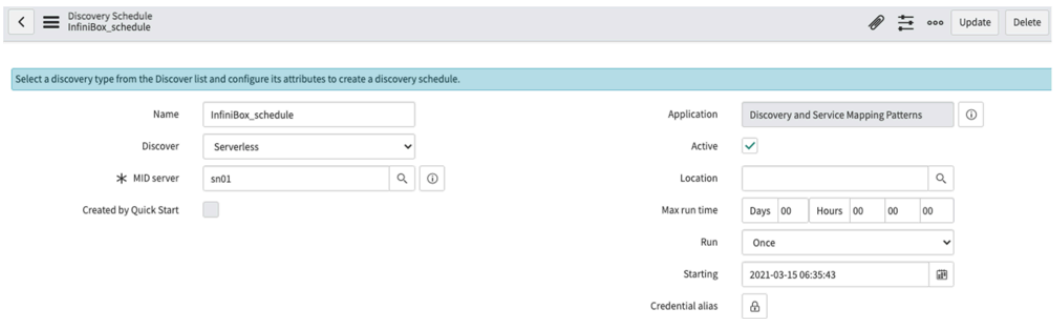
Konfigurieren Sie die Anmeldeinformationen des Typs **Standardauthentifizierung** und den dem Anmeldeinformationsdatensatz zugeordneten Anmeldeinformationsalias.

Sie können dieselbe Konfiguration über das Anmeldeinformationsdatensatzformular vornehmen, in dem Sie zuvor den Anmeldeinformationsalias erstellt haben. Ordnen Sie die Datensätze Aliasse für Verbindungen und Anmeldeinformationen zu.

Basisanmeldedaten

Discovery Zeitplan

1. Erstellen Sie den Erkennungszeitplan mit dem Typ „Serverlose Erkennung“.

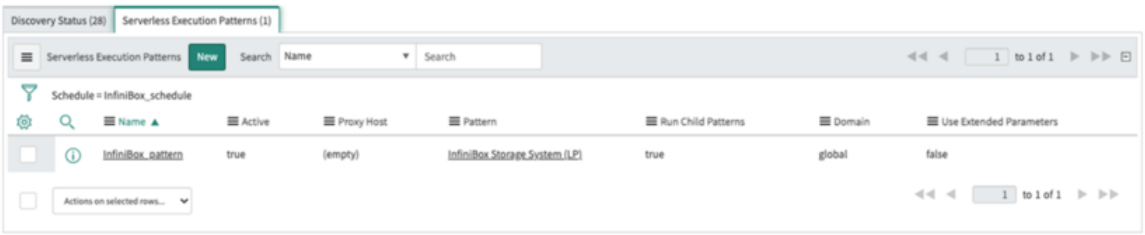


2. Für den Erkennungszeitplan mit dem Typ „Serverlose Erkennung“ konfigurieren Sie das InfiniBox-Speichersystem-LP-Muster auf der Registerkarte „Ausführungsmuster ohne Server“.
3. Legen Sie die Option „Untergeordnete Muster ausführen“ auf „True“ fest.

   Dadurch kann das System alle untergeordneten Muster auslösen, die dem InfiniBox-Speichersystem (LP) zugeordnet sind. Dies ist aufgrund des Large Payload (LP) -Mechanismus erforderlich. Dies wird für die Erkennung des InfiniBox-Speichersystems und aller entsprechenden CI-Typen verwendet.

Automatische Übersetzung

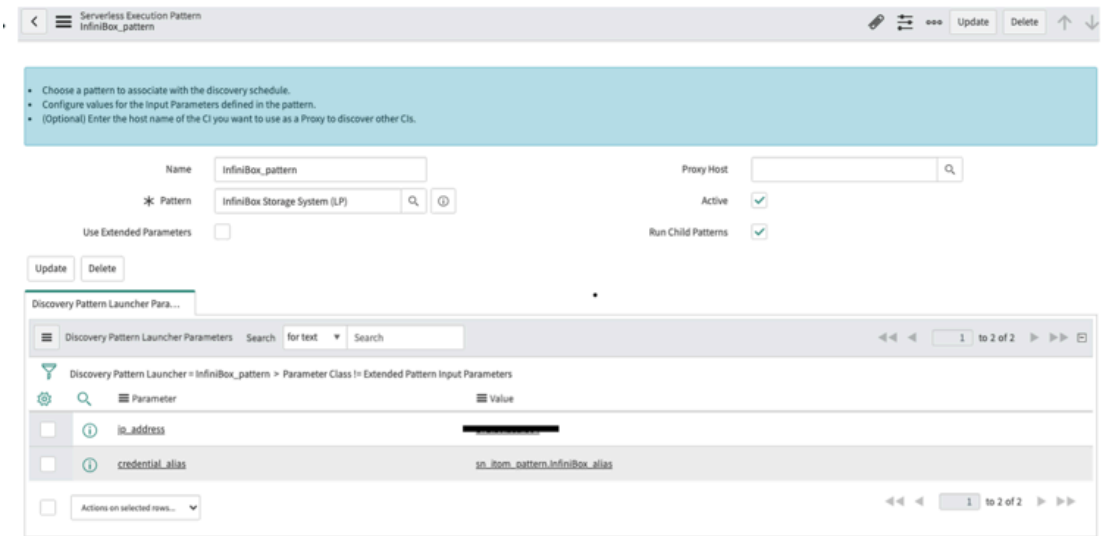
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Übernehmen Sie die Werte für **ip_address** und **credential_alias** aus dem zugehörigen Abschnitt „Ausführungsmuster ohne Server“. Diese dienen als Eingabeparameter zum Auslösen des Erkennungszeitplans und des zugehörigen InfiniBox-Erkennungsmusters.

Wenden Sie die IP-Adresse des InfiniBox-Systems und die ID des zuvor erstellten Datensatzes für Aliasse für Verbindungen und Anmeldeinformationen an. Diese beziehen sich auf die InfiniBox-Anmeldedaten für den Datensatz vom Typ **Standardauthentifizierung**.

Ausführungsmuster ohne Server



Von Discovery während der horizontalen Erkennung erfasste Daten

Speicherserver [cmdb_ci_storage_server]

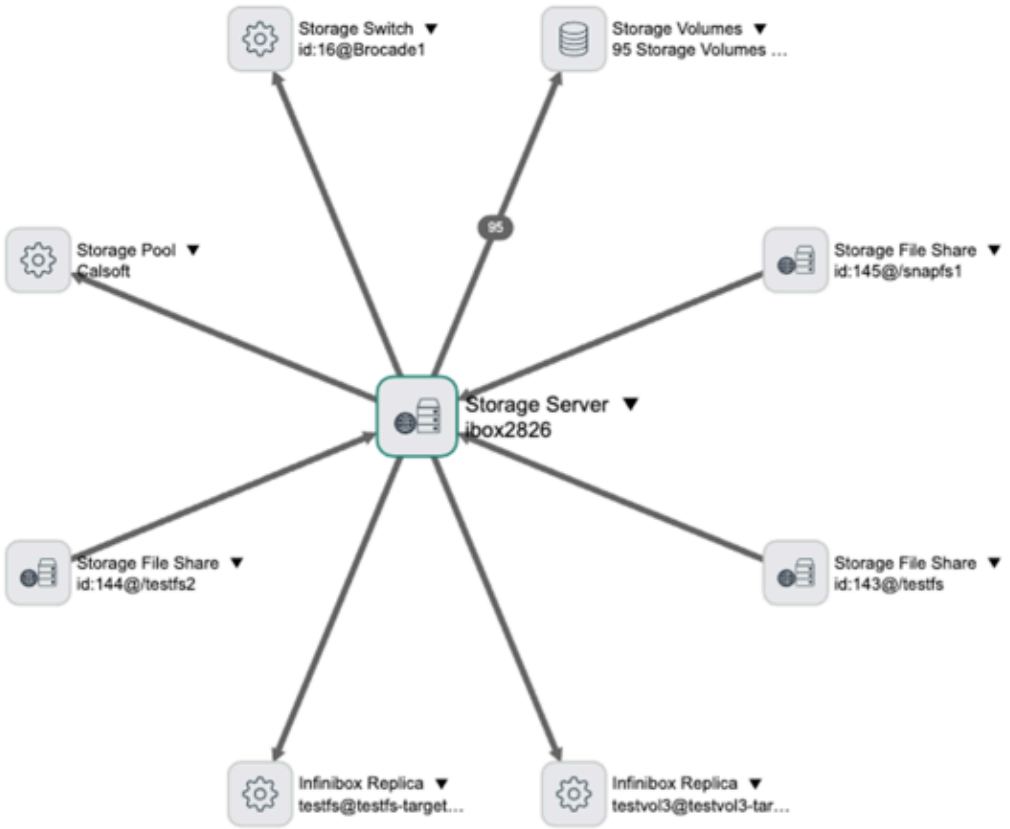
Feld	Beschreibung
ip_address	IP-Adresse des InfiniBox-Systems.
Name	Name des InfiniBox-Systems.
os_version	Aktuelle Version des InfiniBox-Systems.
model_id	Modell-ID des InfiniBox-Systems.
manufacturer	Produktbezeichnung des InfiniBox-Systems.
serial_number	Seriennummer des InfiniBox-Systems.
operational_status	Betriebszustand des InfiniBox-Systems.
physical_capacity	Physische Gesamtkapazität des InfiniBox-Systems in Gigabyte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
virtual_capacity	Virtuelle Gesamtkapazität des InfiniBox-Systems in Gigabyte.

Speicherserver-Ansichtszuordnung



Datenträger [cmdb_ci_disk]

Feld	Beschreibung
device id	ID des physischen Datenträgers, Kombination aus NODE_ID@DISK_ID.
Name	Name des physischen Datenträgers, Kombination aus INFINIBOX_NAME:NODE_ID@DISK_ID
drive_type	Laufwerkstyp des physischen Datenträgers.
model_id	Modell-ID des physischen Datenträgers.
manufacturer	Anbieter des physischen Datenträgers.
operational_status	Betriebsstatus des physischen Datenträgers.
serial_number	Seriennummer des physischen Datenträgers.
Computer	Verweis auf einen der physischen Knoten des InfiniBox-Systems.

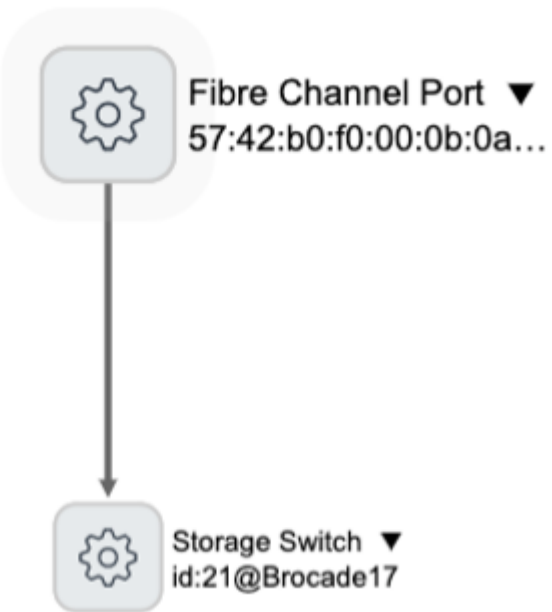
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre-Channel-Port [cmdb_ci_fc_port]

Feld	Beschreibung
wwpn	Weltweiter Port-Name des Fibre Channel-Ports.
name	Name des Fibre Channel-Ports (wwpn).
speed	Geschwindigkeitswert des Fibre Channel-Ports in Gigabit pro Sekunde, falls angewendet.
wwnn	Weltweiter Knotenname des Fibre Channel-Ports.
port_role	Rolle des Fibre Channel-Ports.
state	Status des Fibre Channel-Ports.
link_state	Verbindungsstatus des Fibre Channel-Ports.
manufacturer	Anbieter des Fibre Channel-Ports.
model_id	Modell-ID des Fibre Channel-Ports.
Computer	Verweis auf einen der physischen Knoten des InfiniBox-Systems.

Fibre Channel-Ansichtszuordnung



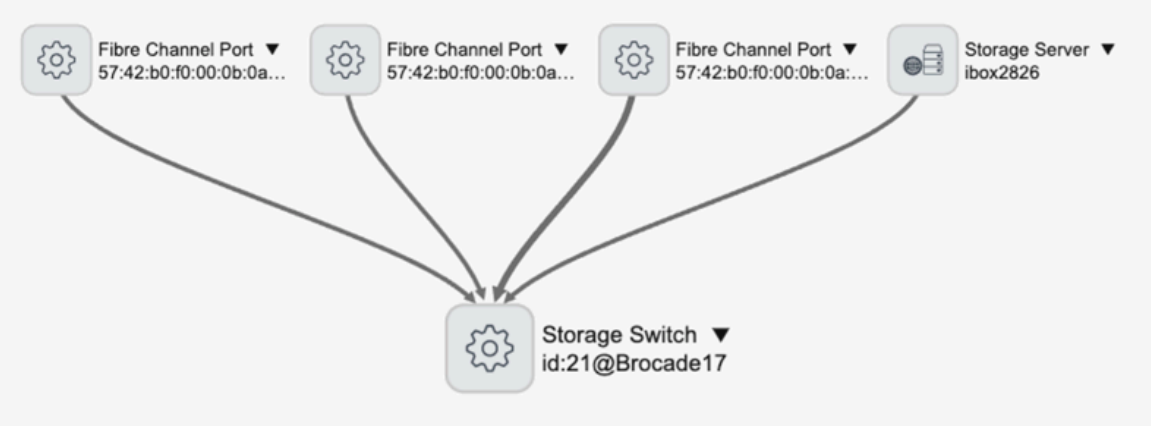
Speicher-Switch [cmdb_ci_storage_switch]

Feld	Beschreibung
object_id	ID des Speicher-Switches.
name	Name des Speicher-Switches, Kombination aus id:SWITCH_ID@SWITCH_NAME.
wwnn	Weltweiter Knotenname des Speicher-Switches.
manufacturer	Anbieter des Speicher-Switches.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

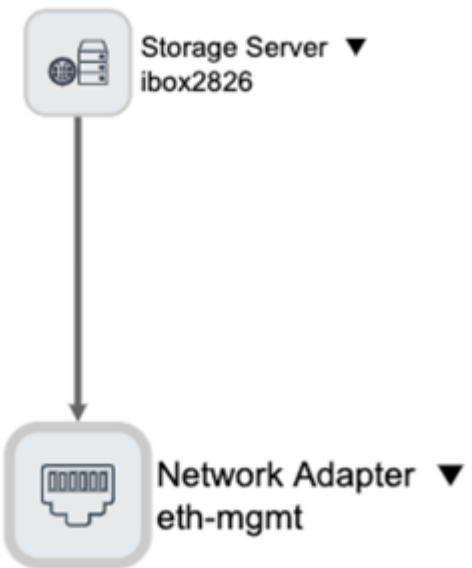
Speicher-Switch-Ansichtszuordnung



Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
mac_address	Ethernet-Adresse des Netzwerkadapters.
name	Ethernet-Name des Netzwerkadapters.
operational_status	Ethernet-Verknüpfungsstatus des Netzwerkadapters.
manufacturer	Ethernet-Anbieter des Netzwerkadapters.
model_id	Ethernet-Modell-ID des Netzwerkadapters.
ip_address	IPv4-IP-Adresse, die dem Ethernet-Netzwerkadapter zugeordnet ist.

Netzwerkadapter-Ansichtszuordnung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

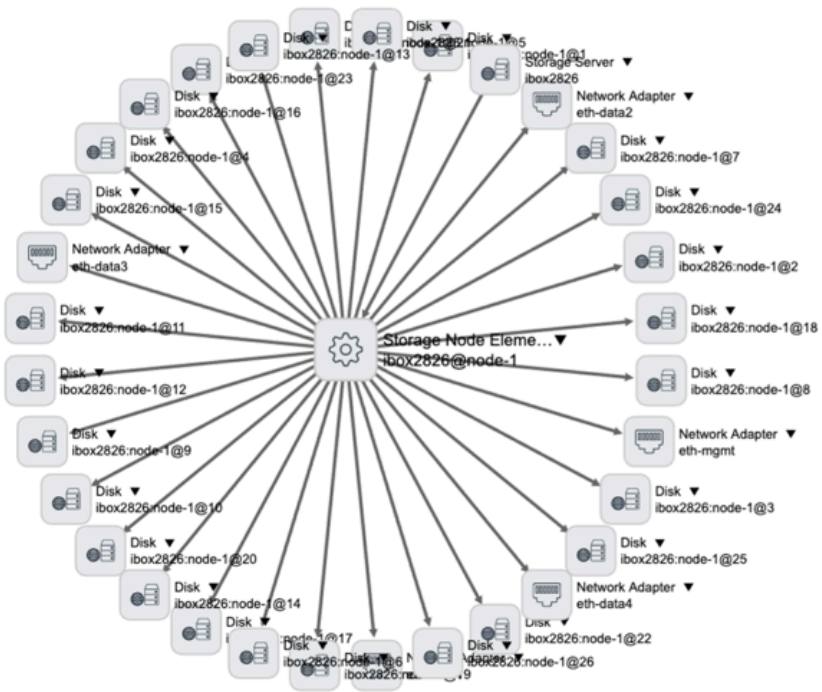
IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
netmask	Dem InfiniBox-Speichersystem zugeordnete Netzmaske.
name	IPv4-IP-Adresse eines der InfiniBox-Knoten oder des InfiniBox-Speichersystems.
ip_address	IPv4-IP-Adresse eines der InfiniBox-Knoten.

Speicherknotenelement [cmdb_ci_storage_node_element]

Feld	Beschreibung
object_id	Name des InfiniBox-Speicherknotens, Kombination aus id:NODE_ID@NODE_NAME.
name	Name des InfiniBox-Speicherknotens, Kombination aus INFINIBOX_NAME@NODE_NAME.
node_state	Betriebszustand des InfiniBox-Speicherknotens.
manufacturer	Anbieter des InfiniBox-Speicherknotens.
model_id	Modell des InfiniBox-Speicherknotens.
ip_address	Dem InfiniBox-Speicherknoten zugewiesene IPv4-Adresse.

Speicherknotenelement-Ansichtszuordnung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

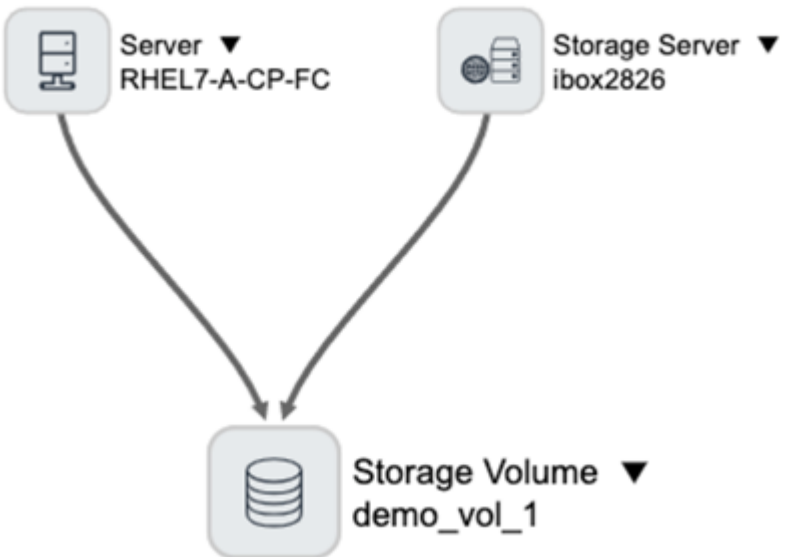
Seriennummer [cmdb_serial_number]

Feld	Beschreibung
serial_number	Dem InfiniBox-Speichersystem zugeordnete Seriennummer.
serial_number_type	Seriennummerntyp des InfiniBox-Speichersystems.
valid	Seriennummergültigkeitstyp des InfiniBox-Speichersystems.

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
object_id	ID des Speichervolume, Kombination aus id:VOLUME_ID@VOLUME_NAME.
volume_id	ID des Speichervolume, Kombination aus id:VOLUME_ID@VOLUME_NAME.
name	Name des Speichervolume.
storage_type	Rolle des Speichervolume.
size_bytes	Gesamtkapazität des Speichervolume in Byte.
serial_number	Seriennummer des Speichervolume.
pool_id	ID des Pools, dem das Speichervolume zugeordnet ist.
state	Sperrstatus des Speichervolume.
provisioning_type	Art der Bereitstellung des Speichervolume.
size	Gesamtkapazität des Speichervolume in Gigabyte
provided_by	Verweis zum Speicher-Pool, dem das Speichervolume zugeordnet ist.

Speichervolume-Ansichtszuordnung

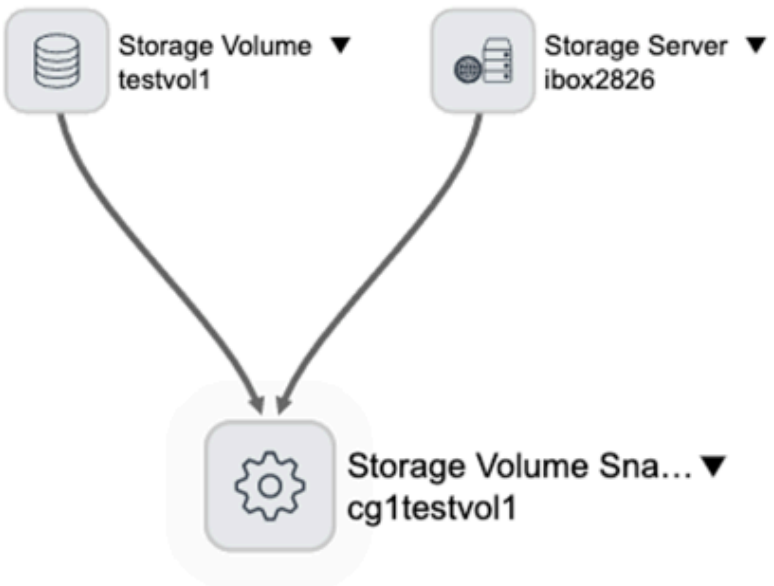


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Feld	Beschreibung
object_id	ID des Speichervolume-Snapshot, Kombination aus id:VOLUME_ID@VOLUME_NAME.
storage_server	Name des InfiniBox-Systems, dem der Volume-Snapshot zugeordnet ist.
name	Name des Speichervolume-Snapshots.
size_bytes	Gesamtkapazität des Speichervolume-Snapshots in Byte.
size	Gesamtkapazität des Speichervolume-Snapshots in Gigabyte.
serial_number	Seriennummer des Speichervolume-Snapshots.
pool_id	ID des Pools, dem der Speichervolume-Snapshot zugeordnet ist.
parent_id	ID des Speichervolume, das dem Snapshot des Speichervolume übergeordnet ist.
state	Sperrstatus des Speichervolume-Snapshots.
provisioning_type	Art der Bereitstellung des Speichervolume-Snapshots.
provided_by	Verweis zum Speicher-Pool, dem das Speichervolume zugeordnet ist.

Speichervolume-Snapshot

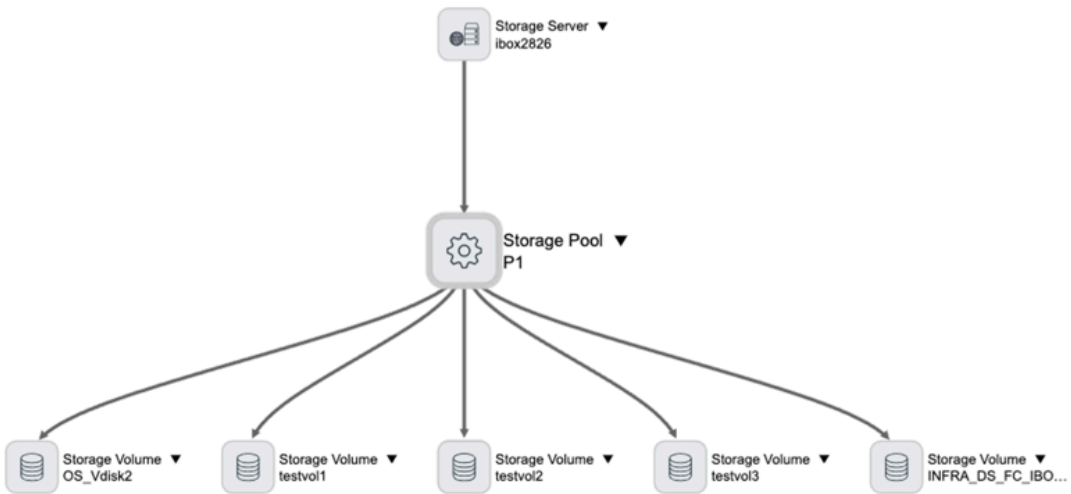


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
object_id	ID des Speichervolume, Kombination aus id:POOL_ID@POOL_NAME.
Name	Name des Speicherpools.
physical_capacity	Physische Gesamtkapazität des Speicherpools in Gigabyte.
virtual_capacity	Virtuelle Gesamtkapazität des Speicherpools in Gigabyte.
free_phys_capacity	Verfügbare physische Kapazität des Speicherpools in Gigabyte.
free_virt_capacity	Verfügbare virtuelle Kapazität des Speicherpools in Gigabyte.
num_vols	Anzahl der am Speicherpool beteiligten Volumes.
num_file_sys	Anzahl der am Speicherpool beteiligten Dateisysteme.
num_file_sys_snap	Anzahl der am Speicherpool beteiligten Dateisystem-Snapshots.
num_vol_snap	Anzahl der am Speicherpool beteiligten Volume-Snapshots.
pool_id	ID des Speicherpools.
pool_state	Status des Speicherpools.

Speicherpool-Ansichtszuordnung



Dateisystem [cmdb_ci_file_system]

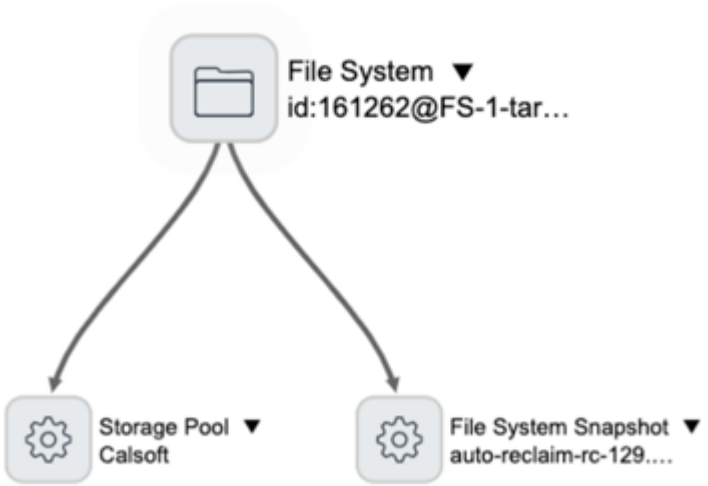
Feld	Beschreibung
object_id	ID des primären Dateisystems, Kombination aus id:FILE_SYSTEM_ID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateisystem [cmdb_ci_file_system] (Fortsetzung)

Feld	Beschreibung
server_name	Name des InfiniBox-Systems, dem das primäre Dateisystem zugeordnet ist.
name	Name des primären Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
size_bytes	Gesamtgröße des primären Dateisystems in Byte.
size	Gesamtgröße des primären Dateisystems in Gigabyte.
free_space_bytes	Freier Speicher des primären Dateisystems in Byte.
serial_number	Seriennummer des primären Dateisystems.
storage_type	Art des primären Dateisystems.
pool_id	ID des Pools, dem das primäre Dateisystem zugeordnet ist.
provisioning_type	Art der Bereitstellung des primären Dateisystems.
provided_by	Verweis auf den Speicherpool, dem das primäre Dateisystem zugeordnet ist.

Dateisystem-Ansichtszuordnung



Dateisystem-Snapshot [cmdb_ci_file_system_snapshot]

Feld	Beschreibung
object_id	ID des Snapshot-Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
volume_id	ID des Snapshot-Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
server_name	Name des InfiniBox-Systems, dem das Snapshot-Dateisystem zugeordnet ist.
name	Name des Snapshot-Dateisystems.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateisystem-Snapshot [cmdb_ci_file_system_snapshot] (Fortsetzung)

Feld	Beschreibung
size_bytes	Gesamtgröße des Snapshot-Dateisystems in Byte.
free_space_bytes	Freier Speicher des Snapshot-Dateisystems in Byte.
serial_number	Seriennummer des Snapshot-Dateisystems.
storage_type	Typ des Snapshot-Dateisystems.
pool_id	ID des Pools, dem das Snapshot-Dateisystem zugeordnet ist.
parent_id	ID des primären Dateisystems, dem das Snapshot-Dateisystem zugeordnet ist.
provisioning_type	Art der Bereitstellung des Snapshot-Dateisystems.

Dateisystem-Snapshot-Ansichtszuordnung

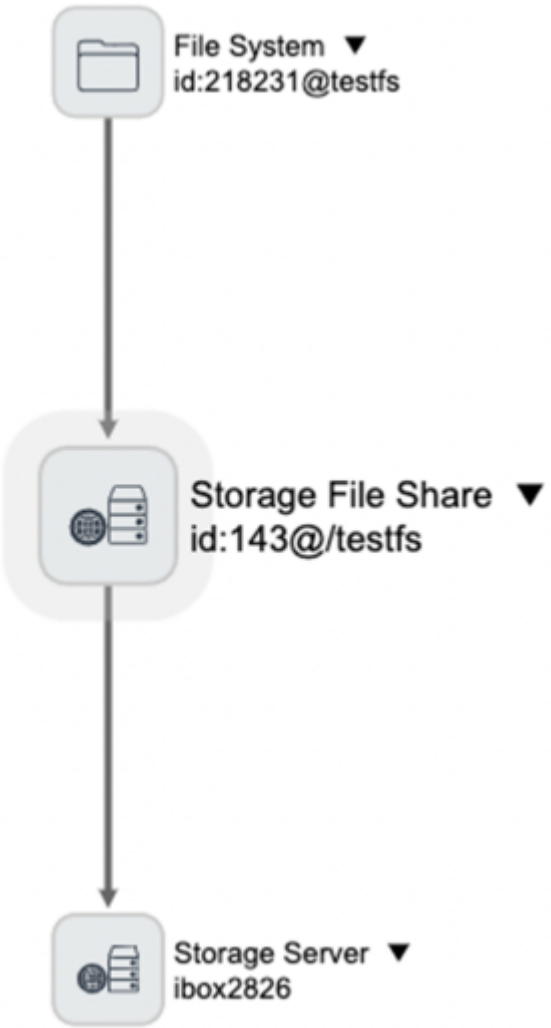
Speicherdateifreigabe [cmdb_ci_storage_fileshare]

Feld	Beschreibung
Pfad	Exportpfad der InfiniBox-Exportentität.
Name	Name der InfiniBox-Exportentität, Kombination aus id:EXPORT_ID@EXPORT_PATH.
fileshare_id	ID der Exportentität im Kontext des InfiniBox-Systems.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Export-Ansichtszuordnung



Primäre InfiniBox-Konsistenzgruppe [cmdb_ci_infinibox_cg]

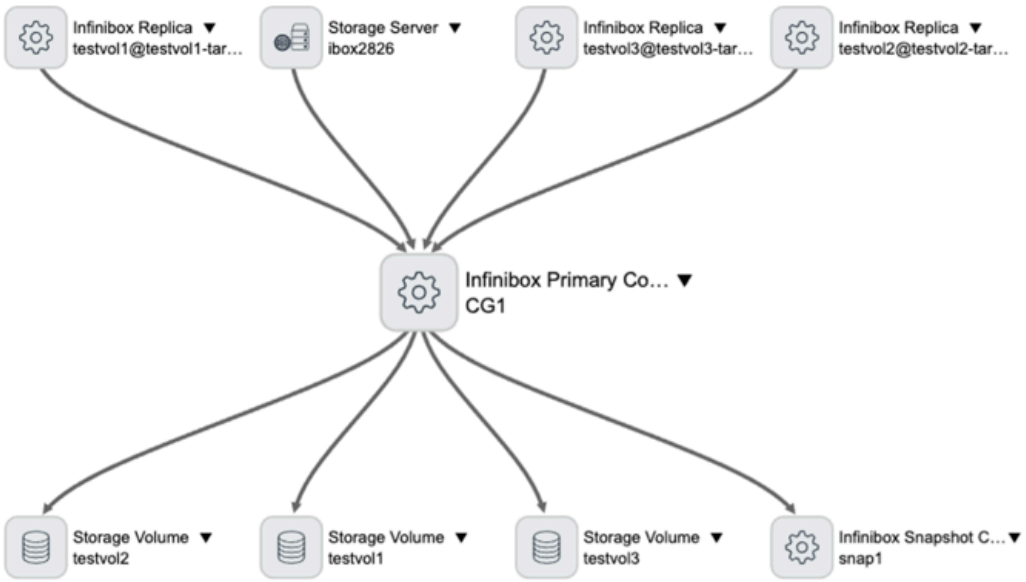
Feld	Beschreibung
object_id	ID der primären InfiniBox-Konsistenzgruppe, Kombination aus id:CONSISTENCY_GROUP_ID@ CONSISTENCY_GROUP_NAME.
created_time	Erstellungszeit der primären InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
updated_time	Aktualisierte Zeit der primären InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
name	Name der primären InfiniBox-Konsistenzgruppe.
type	Typ der primären InfiniBox-Konsistenzgruppe.
members_count	Anzahl der Entitäten, die an der primären InfiniBox-Konsistenzgruppe teilnehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Primäre InfiniBox-Konsistenzgruppe [cmdb_ci_infinibox_cg] (Fortsetzung)

Feld	Beschreibung
pool_id	ID des Pools, dem die primäre InfiniBox-Konsistenzgruppe zugeordnet ist.
lock_state	Sperrstatus der primären InfiniBox-Konsistenzgruppe.

Primäre Konsistenzgruppe – Ansichtszuordnung



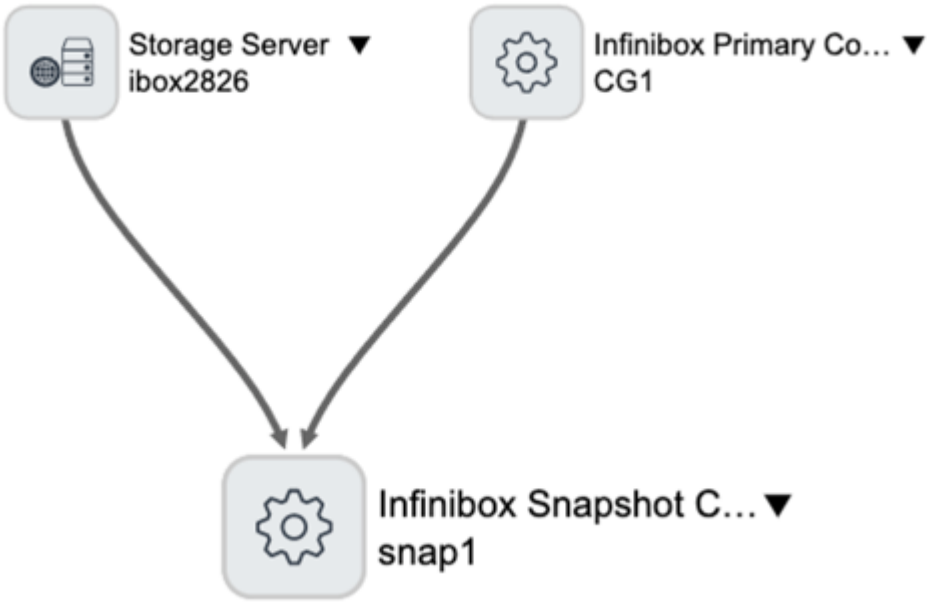
Snapshot der InfiniBox-Konsistenzgruppe[cmdb_ci_infinibox_snapshot_cg]

Feld	Beschreibung
object_id	ID des Snapshot der InfiniBox-Konsistenzgruppe, Kombination aus id:CONSISTENCY_GROUP_ID@ CONSISTENCY_GROUP_NAME.
created_time	Erstellungszeit für den Snapshot der InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
updated_time	Aktualisierte Zeit für den Snapshot der InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
name	Snapshot-Name der InfiniBox-Konsistenzgruppe.
type	Snapshot-Typ der InfiniBox-Konsistenzgruppe.
members_count	Anzahl der Entitäten, die an der Snapshot-InfiniBox-Konsistenzgruppe teilnehmen.
pool_id	ID des Pools, dem der Snapshot der InfiniBox-Konsistenzgruppe zugeordnet ist.
lock_state	Sperrstatus der Snapshot-InfiniBox-Konsistenzgruppe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansichtszuordnung – Snapshot-Konsistenzgruppe



InfiniBox-Verknüpfung [cmdb_ci_infinibox_link]

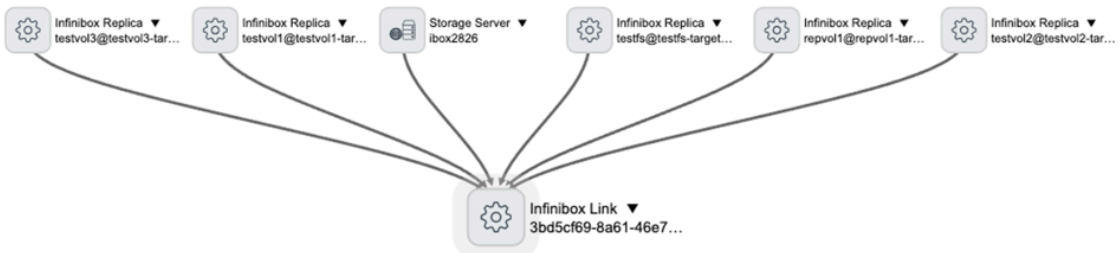
Feld	Beschreibung
object_id	ID der InfiniBox-Verknüpfung.
name	Name der InfiniBox-Verknüpfung.
remote_version	Version des InfiniBox-Remote-Speichersystems.
remote_host	Hostname oder die IP-Adresse des InfiniBox-Remote-Speichersystems.
remote_ip	IP-Adresse des InfiniBox-Remote-Speichersystems.
remote_link_id	Verknüpfungs-ID des InfiniBox-Remote-Speichersystems.
remote_serial_number	Seriennummerntyp des InfiniBox-Remote-Speichersystems.
remote_sys_name	Systemname des InfiniBox-Remote-Speichersystems.
link_state	Verknüpfungsstatus zwischen den InfiniBox-Speichersystemen.
link_config_id	ID der Verknüpfungskonfiguration des InfiniBox-Remote-Speichersystems im GUID-Format.
link_mode	Verknüpfungsmodus zwischen den InfiniBox-Speichersystemen.
resiliency_mode	Resilienzmodus zwischen den InfiniBox-Speichersystemen.
local_witness_state	Lokaler Zeugenstatus des InfiniBox-Speichersystems.
witness_address	Lokale Zeugenadresse des InfiniBox-Speichersystems, wenn zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

InfiniBox-Verknüpfung [cmdb_ci_infinibox_link] (Fortsetzung)

Feld	Beschreibung
last_connection_time	Zeitstempel der eingerichteten Verbindung zwischen den InfiniBox-Speichersystemen im Format JJ-MM-TT HH: MM::SS.
local_replica_net_space_id	ID des lokalen Replikat-Netzwerkspeichers des InfiniBox-Speichersystems.
link_replication_type	Replikationstyp der Verknüpfung zwischen den InfiniBox-Speichersystemen.

Verknüpfung-Ansichtszuordnung



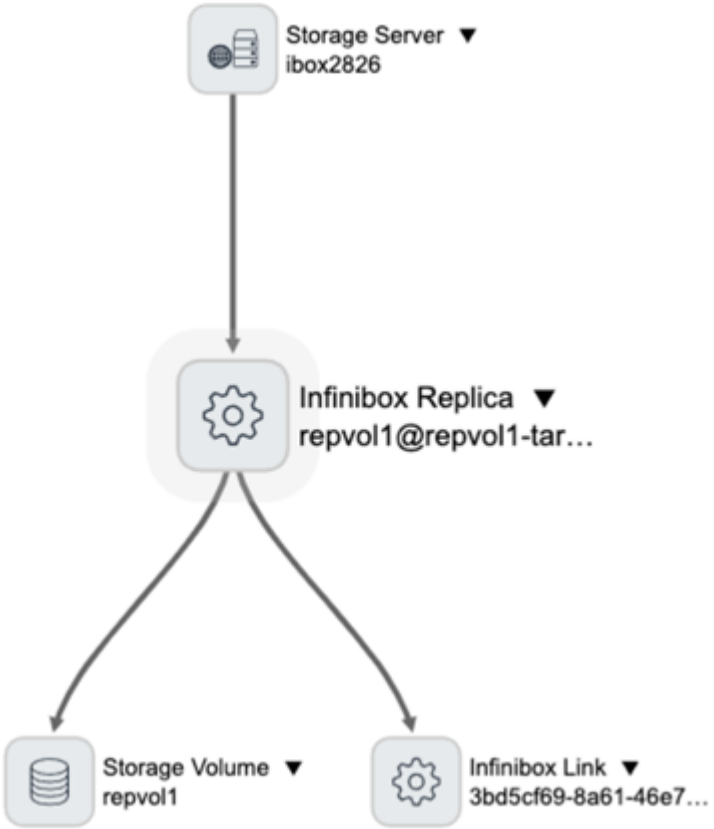
InfiniBox-Replikat [cmdb_ci_infinibox_replica]

Feld	Beschreibung
object_id	ID des InfiniBox-Replikats, Kombination aus LOCAL_ENTITY_NAME@REMOTE_ENTITY_NAME@replica:REPLICA_ID.
name	ID des InfiniBox-Replikats, Kombination aus LOCAL_ENTITY_NAME@REMOTE_ENTITY_NAME@replica:REPLICA_ID.
replica_role	Rolle des InfiniBox-Speichersystem-Replikats.
entity_type	Typ der replizierten Entität im Kontext des InfiniBox-Speichersystems.
replica_state	Status des Replikats im Kontext des InfiniBox-Speichersystems.
replication_type	Typ der Replizierung des Kontexts des InfiniBox-Speichersystems, wenn angewendet.
sync_state	Synchronisierungsstatus des InfiniBox-Speichersystem-Replikats.
link_id	ID der Verknüpfung, die dem Replikat im Kontext des InfiniBox-Speichersystems zugeordnet ist.
entity_id	ID der replizierten Entität im Kontext des InfiniBox-Speichersystems.
remote_entity_id	ID der replizierten Remote-Entität des InfiniBox-Speichersystems.
entity_name	Name der lokalen replizierten Entität im Kontext des InfiniBox-Speichersystems.
remote_entity_name	Name der replizierten Remote-Entität im Kontext des InfiniBox-Speichersystems.
dataset_type	Lokaler Datensatztyp im Kontext des InfiniBox-Speichersystems.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Replikat-Ansichtszuordnung



CI-Beziehungen

Vom InfiniBox-Speichersystem (LP)-Muster erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_switch
cmdb_ci_fc_port	Verbunden mit::Verbunden von	cmdb_ci_storage_switch
cmdb_ci_storage_server	Verwendet::Verwendet von	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_ip_address	Referenz nach Spaltennamen-NIC	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_fc_port
cmdb_ci_storage_server	Besitzt::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Enthält::Enthalten von	cmdb_ci_disk
cmdb_serial_number	Referenz	cmdb_ci_storage_server
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom InfiniBox-Speichervolume (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_volume	Bereitgestellt von::Bereitgestellt	cmdb_ci_storage_vol_snapshot
cmdb_ci_storage_pool	Referenz nach Spaltenname bereitgestellt von	cmdb_ci_storage_volume
cmdb_ci_storage_server	Enthält::Enthalten in und Verweis auf Spaltennamencomputer	cmdb_ci_storage_volume
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_vol_snapshot
cmdb_ci_infinibox_cg	Enthält::Enthalten von	cmdb_ci_storage_volume
cmdb_ci_infinibox_snapshot_cg	Enthält::Enthalten von	cmdb_ci_storage_vol_snapshot

Vom InfiniBox-Speicherpool (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_pool

Vom InfiniBox-Speicherexport (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_fileshare	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_server

Vom InfiniBox-Speicherdateisystem (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_file_system
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_file_system_snapshot
cmdb_ci_file_system	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_pool
cmdb_ci_file_system_snapshot	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_pool
cmdb_ci_file_system	Bereitgestellt von::Bereitgestellt	cmdb_ci_file_system_snapshot
cmdb_ci_file_system	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_fileshare
cmdb_ci_file_system_snapshot	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_fileshare

Vom InfiniBox-Speicherkonsistenzgruppen (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_cg
cmdb_ci_infinibox_cg	Bereitgestellt von::Bereitgestellt	cmdb_ci_infinibox_snapshot_cg
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_snapshot_cg
cmdb_ci_infinibox_cg	Enthält::Enthalten von	cmdb_ci_storage_pool
cmdb_ci_infinibox_snapshot_cg	Enthält::Enthalten von	cmdb_ci_storage_pool

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

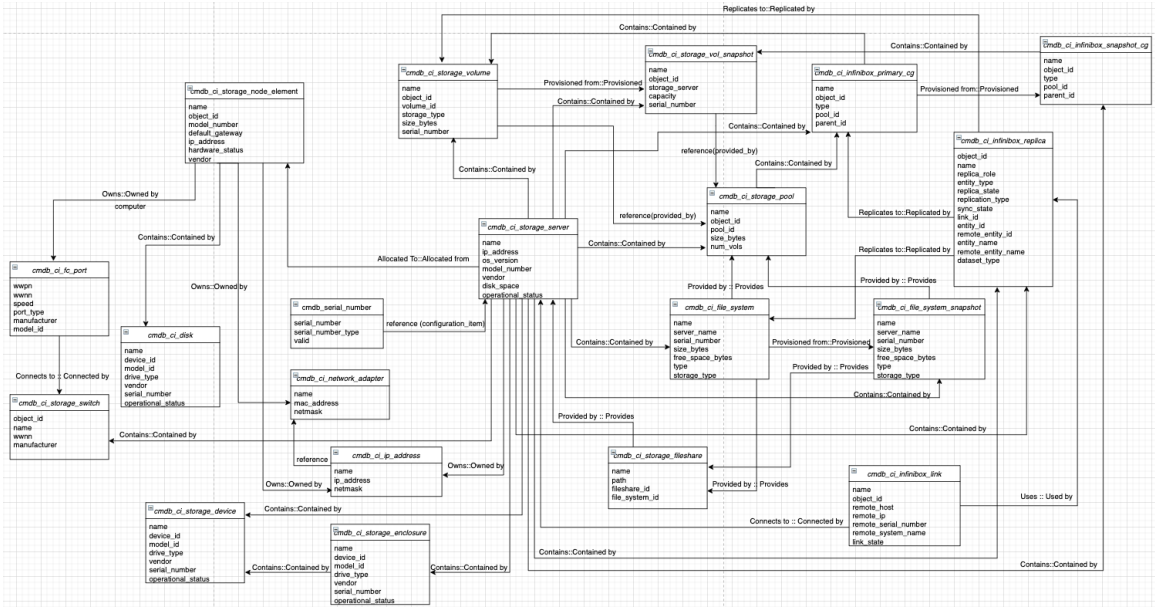
Vom InfiniBox-Speicherreplikat (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_replica
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_infinibox_cg
cmdb_ci_infinibox_replica	Verwendet::Verwendet von	cmdb_ci_infinibox_link
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_storage_volume
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_file_system

Vom InfiniBox-Speicherverknüpfungs (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_link

Infinibox-Klassenmodell



Next-Generation Juniper Network Firewall-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das Erkennungsmuster Next-Generation Juniper Network Firewall, um Juniper-Firewalls zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Juniper-Netzwerk-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der ServiceNow AI Platform® mit Madrid-Release oder höher verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz.
- Fügen Sie den SNMP-System-OID-Datensatz für das Juniper-Gerät der Instanz ServiceNow hinzu. Aktualisieren Sie Folgendes:
  - Klassifizierer: Juniper-Firewall
  - Klasse: Juniper-Firewall-Gerät

Stellen Sie das Muster wie folgt bereit:

1. Laden Sie CMDB CI Class Models: Release 1.10.0 aus dem ServiceNow Store herunter, und installieren Sie es. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind. Weitere Informationen finden Sie unter Firewall-Erweiterungsklassen .
2. Laden Sie das Erkennungsmuster aus dem ServiceNow Store herunter, und installieren Sie es.
3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
IP-Firewall [cmdb_ci_ip_firewall] – Enthält alle Netzwerk-Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Firewall-Gerät [cmdb_ci_firewall_device] – Abstrakte Klasse für herstellerspezifische Firewalls	
Name [name]	Hostname

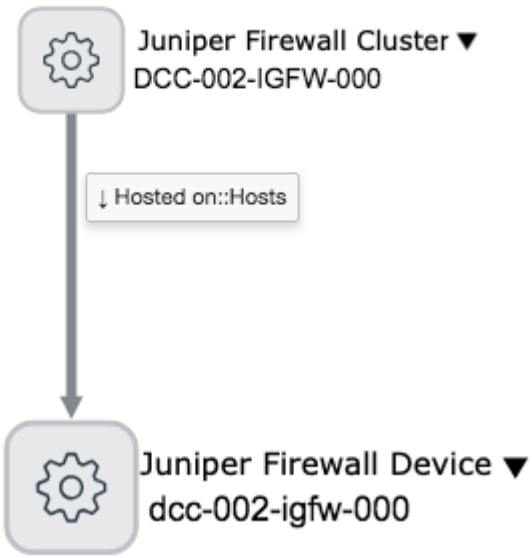
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Juniper-Firewall-Gerät [cmdb_ci_firewall_device_juniper] – Enthält physische Juniper-Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Firewall-Cluster [cmdb_ci_firewall_cluster] – Abstrakte Klasse für einen herstellerspezifischen Firewall-Cluster.	
Name [name]	Hostname
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Juniper-Firewall-Cluster [cmdb_ci_firewall_cluster_juniper] – Enthält Juniper-Firewall-Cluster	
Name [name]	Hostname

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Diese Abhängigkeitsansichtszuordnung auf dem Juniper-Firewall-Geräte-CI zeigt das Juniper-Firewall-Cluster, zu dem es gehört.



CI-Beziehungen

Diese Beziehungen sollen die Juniper-Netzwerk-Firewall-Erkennung unterstützen:

CI	Beziehung	CI
Firewall-Cluster [cmdb_ci_firewall_cluster]	Erstreckt sich von	Cluster [cmdb_ci_cluster]
Juniper-Firewall-Cluster [cmdb_ci_firewall_cluster_juniper]	Erstreckt sich von	Firewall-Cluster [cmdb_ci_firewall_cluster]
	Gehostet::Gehostet auf	Juniper-Firewall-Gerät [cmdb_ci_firewall_device]
Firewall-Gerät [cmdb_ci_firewall_device]	Erstreckt sich von	IP-Firewall [cmdb_ci_ip_firewall]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Juniper-Firewall-Gerät [cmdb_ci_firewall_device]	Erstreckt sich von	Firewall-Gerät [cmdb_ci_firewall_device]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Firewall-Gerätegruppe [cmdb_ci_firewall_device_group]	Erstreckt sich von	CMDB-CI [cmdb_ci]
	Mitglieder::Mitglied von	Firewall-Gerät [cmdb_ci_firewall_device]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Manager [cmdb_ci_firewall_manager]	Erstreckt sich von	CMDB-CI [cmdb_ci]
	Verwaltet::Verwaltet von	Firewall-Gerät [cmdb_ci_firewall_device]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]	Erstreckt sich von	CMDB-CI [cmdb_ci]

Linux Pacemaker-Cluster-Discovery

Die ServiceNow Discovery-Anwendung verwendet das Linux Pacemaker Cluster-Erkennungsmuster, um Clusterdaten mit hoher Verfügbarkeit zu finden und CMDB mit den erkannten Informationen auszufüllen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Dieses Muster ist ein Erweiterungsabschnitt des Linux-Server-Musters. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der ServiceNow AI Platform® mit Madrid-Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Konfigurieren Sie SSH-Anmeldeinformationen für den Linux-Server
- Gewähren Sie einem Benutzer die Berechtigung zum Lesen dieser Dateien:
  - `/etc/hosts`
  - `/etc/corosync/corosync.conf`
  - `/var/lib/heartbeat/crm/cib.xml` oder `/var/lib/pacemaker/cib/cib.xml` von Linux SP3
- Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der folgenden Befehle:

  `ps -ef | grep corosync | grep -v grep`

  `ps -ef | grep pacemaker | grep -v grep`

  `ifconfig | grep 'inet addr:' |awk '{print $1, $2 }'`

  `hostname -s`

  `hostname -f`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

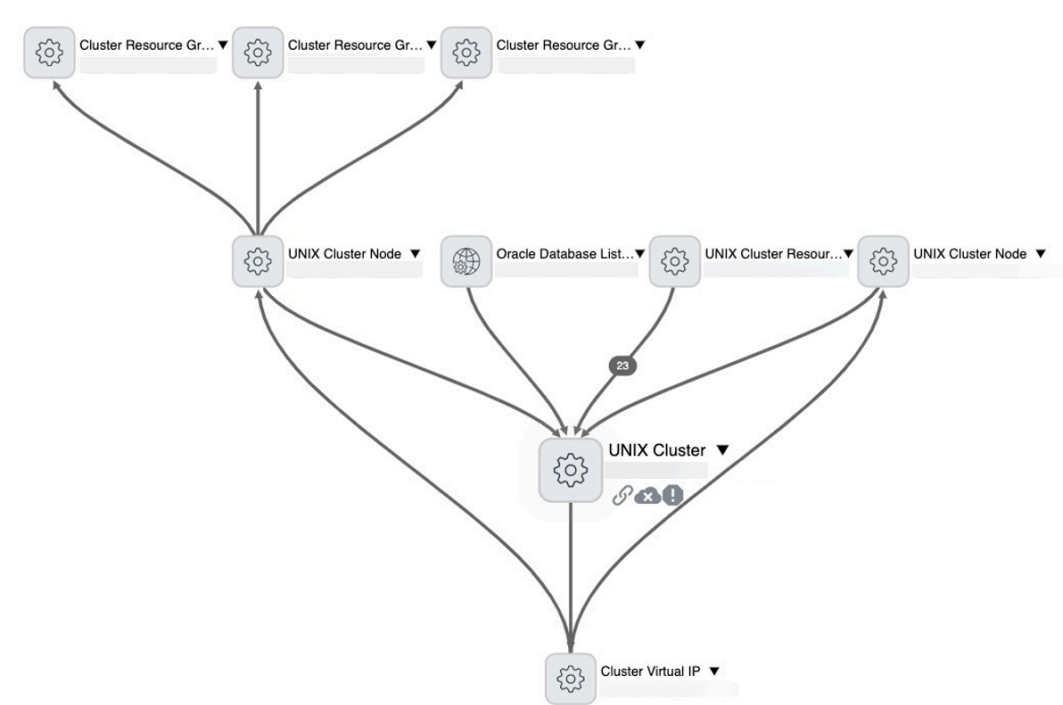
Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI – UNIX-Cluster [cmdb_ci_unix_cluster]	
name	Clustername
cluster_id	Cluster-ID. Enthält die Knoten-ID.
cluster_type	Clustertyp
cluster_status	Cluster-Status: Online / Offline
cluster_version	Clusterversion
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	
name	Ressourcenname
resource_type	Ressourcentyp
resource_status	Ressourcenstatus. Beispiel: Gestartet
ip_address	IP-Adresse des Computers, auf dem die Ressource ausgeführt wird
fqdn	FQDN des Computers, auf dem die Ressource ausgeführt
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	
name	Cluster-VIP-Name
ip_address	IP-Adresse der VIP
Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]	
name	Ressourcengruppenname
Knoten	Ressourcengruppenknoten
resource_group_status	Ressourcengruppenstatus
Server	Ressourcengruppenserver
fqdn	FQDN des Computers, auf dem die Ressourcengruppe läuft
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	
name	Knotenname und Knoten-ID
node_status	Knotenstatus
node_state	Knotenstatus
fqdn	FQDN des Computers, auf dem der Knoten ausgeführt wird

Die Karte Abhängigkeitsansichten zeigt entdeckte Lastenausgleichsmodul-CIs und die Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Diese Beziehungen sollen die Linux Pacemaker Cluster-Erkennung unterstützen:

CI	Beziehung	CI
cmdb_ci_unix_cluster	Hostet::Gehostet auf	cmdb_ci_linux_server
cmdb_ci_unix_cluster_node	Gehostet auf::Hostet	cmdb_ci_linux_server
	Cluster von::Cluster	cmdb_ci_unix_cluster
cmdb_ci_cluster_vip	Verwendet::Verwendet von	cmdb_ci_unix_cluster_node
	Virtualisiert von::Virtualisiert	cmdb_ci_unix_cluster
cmdb_ci_unix_cluster_resource	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_unix_cluster
	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_unix_cluster_node
cmdb_ci_cluster_resource_group	Enthält::Enthalten in	cmdb_ci_unix_cluster
	Enthält::Enthalten in	cmdb_ci_unix_cluster_node
	Enthält::Enthalten in	cmdb_ci_unix_cluster_resource

Microsoft Discovery von Zertifikaten der Zertifizierungsstelle (Certificate Authority, CA)

Die ServiceNow Discovery Anwendung kann erkennen Microsoft Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) mit dem Muster „Microsoft CA – Zertifikatverwaltung“. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Ab Version 1.27.0 Muster für Discovery und Service-Mapping Unterstützt die Erkennung des alternativen Antragstellernamen (SAN) für alle Anforderungs-IDs und die Discovery-Methoden der Vorlagen-ID.

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie den Prozess der Zertifizierungsstelle

Stellen Sie sicher, dass auf dem Hostcomputer der CA-Prozess ausgeführt wird.

Verifizieren Sie vorherige Windows Discovery

Verifizieren Sie einen Windows Host wurde während einer vorherigen horizontalen Discovery erkannt. Weitere Informationen finden Sie unter Erkennung von Windows.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Discovery-Zeitplan, um eine gezielte Discovery von durchzuführen Microsoft CA-Zertifikate, die den Host verwenden, auf dem der CA-Prozess ausgeführt wird. Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für Microsoft Discovery der Zertifizierungsstelle (Certificate Authority, CA).

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Microsoft CA – Zertifikatverwaltung“.

Eindeutiges Zertifikat [cmdb_ci_certificate]

Feld	Beschreibung
Fingerabdruck [Fingerabdruck]	Hashwert des Zertifikats
Fingerabdruckalgorithmus [Fingerprint_Algorithmus]	Algorithmus, der zum Hash des Zertifikats verwendetwird.
Allgemeiner Antragstellername [subject_common_Name]	Gibt den Hostnamen/die Domäne an, der/die dem Zertifikat zugeordnet ist und im Zertifikat aufgeführt ist **Betreff** Feld.
Eindeutiger Antragstellername [subject_Distinguished_Name]	Identifizierungsinformationen des Antragstellers, der im Zertifikat aufgeführt ist **Betreff** Feld.
Eindeutiger Ausstellername [issuer_Distinguished_Name]	Eindeutiger Name des Ausstellers.
Kommentare [comments]	Enthält eine lesbare Beschreibung für Benutzer
Verlängerungsnachverfolgung [Renewal_Tracking]	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate erstellt werden sollen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eindeutiges Zertifikat [cmdb_ci_certificate] (Fortsetzung)

Feld	Beschreibung
Zertifikatvorlage [cert_template]	Zertifikatvorlage, die die Richtlinien und Regeln definiert, die eine ZERTIFIZIERUNGSSTELLE verwendet, wenn eine Anforderung für ein Zertifikat empfangen wird.
Fingerabdruck des Zertifikats [Thumb_print]	Eindeutiger Bezeichner für Zertifikate in Anwendungen bei Vertrauensentscheidungen, in Konfigurationsdateien und bei Anzeige in Schnittstellen.
Allgemeiner Ausstellername [issuer_common_Name]	Allgemeiner Name des Ausstellers.
Gültig ab [valid_from]	Gültigkeitsstartzeitraum des Zertifikats
Seriennummer [serial_number]	Seriennummer des Zertifikats.
Antragstellerland [subject_Country]	Zweistelliger Ländercode im Zertifikat **Betreff** Feld.
Antragstellerorganisation [subject_Organization]	Organisation, die im Zertifikat aufgeführt ist **Betreff** Feld.
Aussteller [Aussteller]	Entität, die das Zertifikat signiert und ausgestellt hat.
Betrefforganisationseinheit [subject_Organization_unit]	Organisationseinheit, die im Zertifikat aufgeführt ist **Betreff** Feld.
Alternativer Antragstellername [subject_Alternative_Name]	Liste der vollqualifizierten Domänennamen, die durch das Zertifikat gesichertsind, aufgeführt im Zertifikat **Betreff** Feld.
Gültig bis [valid_to]	Gültigkeitsendzeitraum des Zertifikats
Name [name]	Name des CI.
Status [state]	Lebenszyklusstatus des Zertifikats. Beispiel: Installiert, ausgegeben oder widerrufen.
Stammaussteller [root_issuer]	Stammentität, die das Zwischenzertifikat signiert und ausgestellt hat
Betrefflokalität [subject_locality]	Ort, der im Zertifikat aufgeführt ist **Betreff** Feld.
Antragstellerstatus [subject_State]	Status, der im Zertifikat aufgeführt ist **Betreff** Feld.
Betriebsstatus [operational_status]	Gibt an, ob das Zertifikat gültig ist oder widerrufen wurde. Mögliche Werte: • **Betriebsbereit** : Gültiges Zertifikat • **Nicht Funktionsfähig** : Widerrufenes Zertifikat
Signaturalgorithmus [Signature_Algorithmus]	Signaturalgorithmus des Zertifikats. Beispiel: SHA-256, sha256RSA oder SHA1withRSA.
Anforderungstyp [Request_type]	Format, das zum anfordern des Zertifikats verwendet wird.
Datum der Anforderungsübermittlung [Request_submission_date]	Datum, an dem die Zertifikatanforderung übermittelt wurde.
Datum der Anforderungslösung [Request_Resolution_date]	Datum, an dem die Zertifikatanforderung von der ZERTIFIZIERUNGSSTELLE gelöst wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eindeutiges Zertifikat [cmdb_ci_certificate] (Fortsetzung)

Feld	Beschreibung
Datum des Widerrufs anfordern [Request_revocation_date]	Datum, an dem das Zertifikat widerrufen wurde. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Effektives Widerrufsdatum [effective_revocation_date]	Datum, an dem das Zertifikat effektiv widerrufen wurde, indem es der Zertifikatwiderrufliste (Certificate Revocation List, CRL) hinzugefügt wurde. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Sperrgrund [Revocation_reason]	Grund für den Widerruf des Zertifikats. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Name der anfordernden Person [requester_Name]	Name der Person, die das Zertifikat angefordert hat.
Vorlagenregistrierungskennzeichnungen [template_Enrollment_Flags]	Informationen zum Zertifikat, das von der CA oder dem Besitzer des Zertifikats bearbeitet werden muss. Suchen Sie in nach dem Fehlercode, um weitere Informationen zu erhalten Die offizielle Microsoft-Dokumentationswebsite .

CI-Beziehungen

Das Muster „Microsoft CA – Zertifikatverwaltung“ erstellt keine CI-Beziehungen.

Erstellen Sie einen serverlosen Zeitplan für Microsoft Discovery der Zertifizierungsstelle (Certificate Authority, CA)

Erstellen Sie einen serverlosen Discovery-Zeitplan für die Erkennung Microsoft Zertifikate der Zertifizierungsstelle (Certificate Authority, CA).

Vorbereitungen

- Stellen Sie sicher, dass der CA-Prozess auf dem Hostcomputer ausgeführt wird.
- Überprüfen Sie, ob ein Windows Host wurde während einer vorherigen horizontalen Discovery erkannt. Weitere Informationen finden Sie unter Erkennung von Windows.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Erstellen Sie den Discovery-Zeitplandatensatz.
   a. Wählen Sie **Neu**.
   b. Füllen Sie im Formular die Felder aus.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan. Beispiel: Erkennen Sie MS CA.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erkannt	Scan-Typ, der Zertifikate sein muss.
Discovery-Typ des Zertifikats	Zertifikattyp, der CA Trust Discovery sein muss.
MID-Server verwenden	Name des MID-Server Zur Verwendung für diesen Zeitplan.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

c. Wählen Sie **Absenden**.

3. Erstellen Sie das Ausführungsmuster.

a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.

b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .

Discovery verwendet jedes Ausführungsmuster, um bis zu 20.000 Zertifikate zu erkennen. Erstellen Sie für Bereitstellungen mit mehr als 20.000 Zertifikaten mehrere Ausführungsmuster.

c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz. Beispiel: Erkennen Sie MS CA.
Muster	Muster, das für diesen Zeitplan verwendet werden soll, wobei es sich um das Microsoft CA-Zertifikatverwaltungsmuster handeln muss.
Proxyhost	CI-Name des Windows Host, auf dem ausgeführt wird Microsoft CA-Service, der in einer vorherigen Discovery erkannt und in der ausgefüllt wurde CMDB.
Aktiv	Option zum Aktivieren dieses Zeitplans für die Discovery.

d. Wählen Sie **Absenden**.

4. Legen Sie die Parameter des Musterstartprogramms fest.

a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.

b. Füllen Sie im Formular die Felder aus.

Parameter	Beschreibung
template_list	Bestimmt, ob nach allen Anforderungs-IDs oder einer Vorlagen-ID gesucht werden soll, um Zertifikate zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
	▪ Alle: Schränkt die Discovery auf alle Zertifikatanforderungs-IDs in aufsteigender Reihenfolge ein, entweder basierend auf der standardmäßigen Beschränkung des Ausführungsmusters von 20.000 oder auf den in festgelegten Werten *start_offset*Oder *limit*. ▪ Vorlagen-ID: Sucht nur nach Zertifikaten in der spezifischen Vorlagen-ID.
start_offset	Dieser optionale Parameter gibt die Nummer des Zertifikats an, ab dem die Discovery gestartet werden soll, und ist nur relevant, wenn *template_list*Ist auf alle und für Bereitstellungen mit mehr als 20.000 Zertifikaten festgelegt. Wenn Sie mehrere serverlose Ausführungsmuster für Bereitstellungen mit mehr als 20.000 Zertifikaten erstellen, verwenden Sie 1 für die erste Ausführung, 20001 für die zweite usw. Wenn dieser Parameter leer bleibt, *start_offset*Standardwert ist 1.
limit	Dieser optionale Parameter begrenzt die Zertifikat-Discovery auf den angegebenen Wert und ist nur relevant, wenn *template_list*Ist auf alle festgelegt. Wenn der Parameter leer bleibt, beträgt der Grenzwert standardmäßig 20.000 Zertifikate.
ip	IP des Servers, auf dem der CA-Prozess (certsrv) ausgeführt wird.
Discover_SAN_for_template	Bei „wahr“ aktiviert dieser optionale Parameter die Erkennung des alternativen Antragstellernamen (SAN) der Zertifikate, wenn eine Vorlagen-ID in angegeben wird *template_list*Parameter. Dieser Parameter führt für jedes Zertifikat innerhalb der Vorlagen-ID separate Befehle aus, was sich auf die Leistung auswirken kann. Bei der Suche nach allen Anforderungs-IDs wird SAN automatisch erkannt, daher sollte dieser Parameter leer bleiben.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Zugehörige Informationen

Microsoft Discovery von Zertifikaten der Zertifizierungsstelle (Certificate Authority, CA)

NetApp Discovery des SolidFire-Speichersystems

ServiceNow Discovery Verwendet NetApp Discovery-Muster für das SolidFire-Speichersystem, um Cluster und Knoten im SolidFire-Speichersystem zu finden. Um einige dieser Ressourcen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.74) installiert ist.

Berechtigungen für Basisauthentifizierung

Stellen Sie sicher, dass zur Authentifizierung der Element-API-Aufrufe die Anmeldeinformationen für die Standardauthentifizierung konfiguriert sind. Speichern Sie die folgenden Anmeldeinformationen für den SolidFire Cluster-Administrator als Basisauthentifizierung, um einen ordnungsgemäßen Zugriff zu gewährleisten:

- „sys_user_group“
- clusterAdmins
- reporting
- drives

MID-Server

Stellen Sie sicher, dass der MID Server auf das Zielgerät zugreifen kann.

Discovery-Anmeldeinformationen

Stellen Sie sicher, dass Sie über die Anmeldeinformationen für die Ausführung von Discovery auf dem Hostcomputer verfügen, auf dem das SolidFire-Speichersystem ausgeführt wird.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan, um eine gezielte Erkennung von SolidFire-Clustern und -Knoten durchzuführen.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

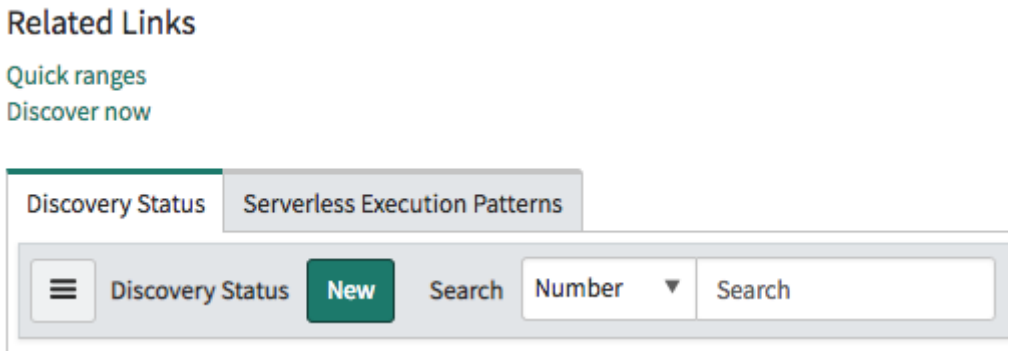
Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Zum Beispiel: Erkennung SolidFire.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Server s

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.



Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Zum Beispiel: Muster für SolidFire-Speicher.
Muster	Name des auszuführenden Musters: NetApp SolidFire Storage System
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Konfigurieren Sie unter **Startprogrammparameter für Discovery-Muster** die Startparameter mit den entsprechenden Werten. Stellen Sie sicher, dass die Management-IP des Clusters und der Alias für die Anmeldeinformationen definiert sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten SolidFire-Konfigurationsdaten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Hauptkonfigurationselement [cmdb_ci_storage_server]	
name	Name des CI

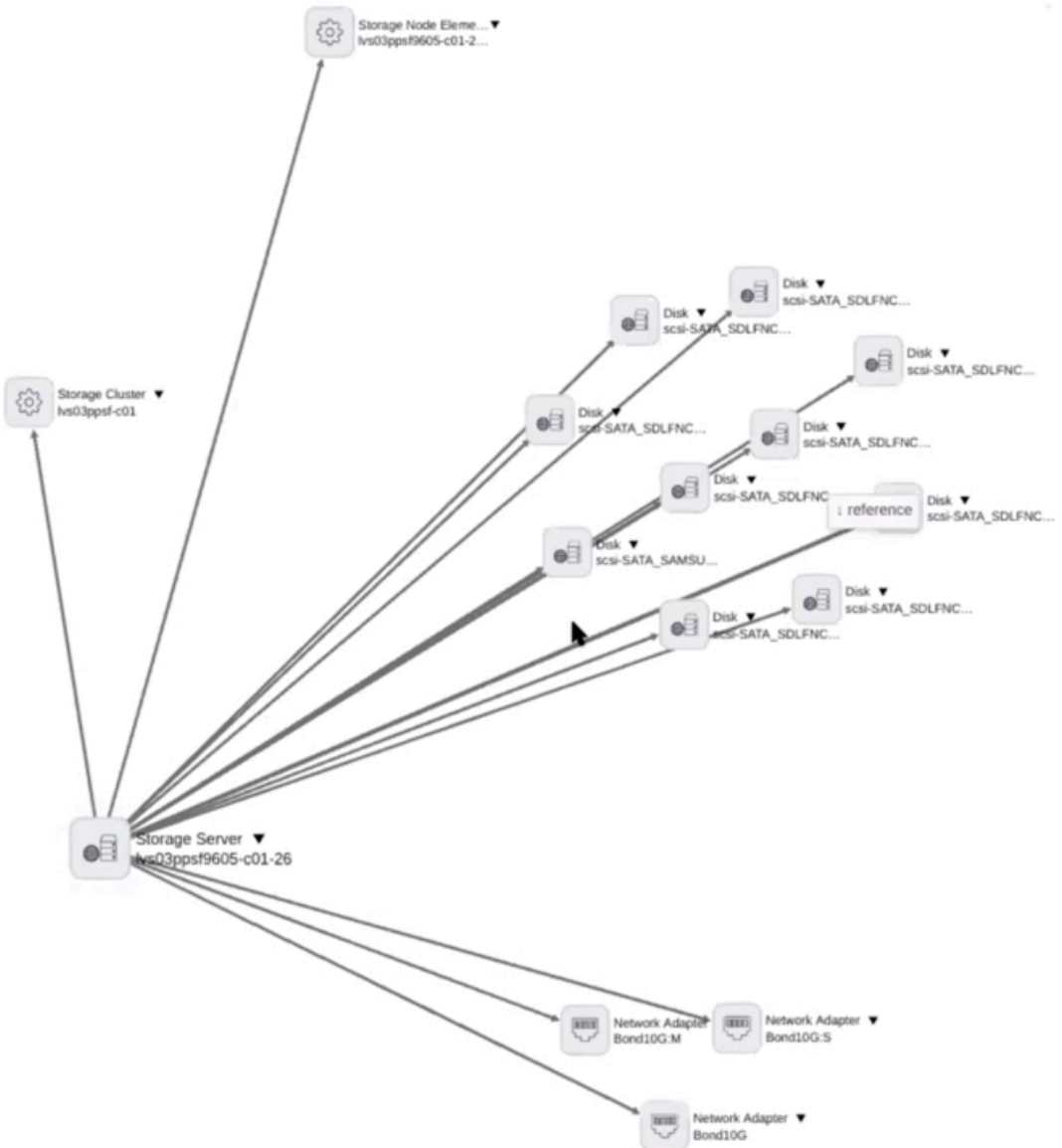
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
serial_number	Seriennummer, die dem CI zugeordnet ist
firmware_version	Firmwareversion des CI
ip_address	IP-Adresse für das CI
short_description	Kurze Textbeschreibung des CI
manufacturer	Hersteller des Geräts
model_id	Modell-ID des Geräts
os_version	Version des auf dem CI ausgeführten Betriebssystems
os	Auf dem CI ausgeführtes Betriebssystem
Speichercluster [cmdb_ci_storage_cluster]	
ip_address	IP-Adresse des Speicherclusters
manufacturer	Hersteller des Geräts
short_description	Kurze Textbeschreibung des CI
cluster_version	Version der Element-OS-API, die im Cluster ausgeführt wird
name	Name des CI
Speicherclusterknoten [cmdb_ci_storage_cluster_node]	
name	Name des CI
operational_status	Gibt an, ob sich das Gerät im aktiven Status befindet
Cluster	Referenz für das Cluster-CI
Speicherknotenelement [cmdb_ci_storage_node_element]	
short_description	Kurze Textbeschreibung des CI
manufacturer	Hersteller des Geräts
serial_number	Seriennummer, die dem CI zugeordnet ist
model_id	Modell-ID des Geräts
chassis_type	Typ des Gehäuses, das den Server enthält
ram	Speichergröße des CI
cpu_type	CPU-Typ
cpu_manufacturer	Hersteller der CPU
Speicherdatenträger [cmdb_ci_disk]	
name	Name des CI
device_id	ID des Geräts
serial_number	Seriennummer, die dem CI zugeordnet ist
storage_type	Speichertyp
size_bytes	Verfügbare Speichergröße in Byte
manufacturer	Hersteller des Geräts
model_id	Modell-ID des Geräts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Computer	Referenz für den Speicherserver
Netzwerkadapter [cmdb_ci_network_adapter]	
name	Name des CI
ip_address	IP-Adresse für das CI
netmask	Netzmaske des Servers, der den Netzwerkadapter hostet
mac_address	Die MAC-Adresse des Netzwerkadapters
IP-Adresse [cmdb_ci_ip_address]	
ip_address	IP-Adresse für das CI
netmask	Netzmaske des Servers, der das CI hostet

Die Dependency Views-Zuordnung zeigt alle erkannten Cluster und Knoten des SolidFire-Speichersystems in Ihrer Organisation und die Beziehungen zwischen ihnen an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

CI	Beziehung/Referenz	CI
Speichercluster	Cluster von::Cluster	Knoten des Speicherclusters
Knoten des Speicherclusters	Gehostet auf::Hostet	Element des Speicherknotens
Element des Speicherknotens	Verwaltet von::Verwaltet	Speichercluster
Speicherserver (Haupt-CI)	Zugeordnet zu::Zugeordnet von	Element des Speicherknotens
Speicherserver (Haupt-CI)	Wird ausgeführt auf::Wird ausgeführt	Speichercluster
Speicherserver (Haupt-CI)	Enthält::Enthalten in	Datenträger

Netzwerkrouter-Discovery anhand von Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Netzwerkrouter-Muster, um Netzwerkrouter in Ihrer Umgebung zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu Netzwerkroutern und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Informationen zur Probe-basierten Netzwerk-Switch- und Router-Discovery finden Sie unter Netzwerk-Switch- und Router-Discovery.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

Überprüfen Sie die IP-Adressinformationen

Der Router muss IP-Adressinformationen für eine erfolgreiche Discovery enthalten.

Stellen Sie sicher, dass Weiterleitungsregeln für Exit-Schnittstellen konfiguriert und erreichbar sind

Für den Router, der die IP-Adresse bereitstellt, müssen Weiterleitungsregeln für die Exit-Schnittstelle konfiguriert sein und für eine erfolgreiche Discovery erreichbar sein.

Erstellen von SNMP-Anmeldeinformationen

Erstellen Sie SNMP-Community-Anmeldeinformationen oder SNMPv3-Anmeldeinformationen. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .

Konfigurieren Sie Eigenschaften für die Router-Discovery

Navigieren Sie zu `sys_properties.list` Und verifizieren Sie, dass *`glide.discovery.L3_mapping`*Systemeigenschaft ist auf festgelegt **Wahr** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese zusätzlichen Eigenschaften für die Netzwerk-Router-Discovery konfigurieren.

Eigenschaft	Beschreibung
glide.discovery.max_concurrent_invocations_per_schedule	Legt eine maximale Anzahl geplanter Aufrufe für denselben Discovery-Zeitplan fest. Es wird ein Backlog geplanter Ausführungen verhindert, wenn Discovery nicht vor dem nächsten Start abgeschlossen wird. Der Wert ist eine Ganzzahl, die die maximale Anzahl automatisierter Aufrufe darstellt, die für denselben Zeitplan gleichzeitig ausgeführt werden können. Wenn der Grenzwert erreicht ist, werden nachfolgende geplante Aufrufe abgebrochen. Diese Eigenschaft wird durch den Wert 0 oder eine negative Zahl deaktiviert. • **Typ:** Ganzzahl • **Standardwert:** 3 • **Standort: Discovery-Definition** > **Eigenschaften** **Hinweis:** Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „auch wenn abgebrochen“ festgelegt ist.
glide.discovery.bgp_router_disable	Deaktiviert die Ausführung des SNMP – Routing-Musters, wenn ein Router erkannt wird, der das BGP-Protokoll ausführt. Wenn Sie die Tabelle „Gerätenachbarschaften“ [Discovery_device_neigh während der Erkennung der horizontalen Ebene 2 der BGP-fähigen Geräte ausfüllen müssen, legen Sie fest **BGP-Routererkundung deaktiviert** Eigenschaft bis **Nein** . Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	führen kann, einschließlich Problemen mit zu wenig Arbeitsspeicher auf dem MID-Server. • **Typ:** true | false • **Standardwert:** true • **Standort: Discovery-Definition** > **Eigenschaften**

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Netzwerkrouter-Musters.

IP-Router [cmdb_ci_ip_router]

Feld	Beschreibung
Name [name]	Name des Routers.
Modell-ID [model_id]	Hardwaremodell-ID des Routers.
Hersteller [manufacturer]	Router-Hersteller.
Seriennummer [serial_number]	Eindeutige Hardware-Seriennummer des Routers.
IP-Adresse [ip_address]	IP-Adressen, die Schnittstellen zugewiesen sind.
Beschreibung [short_description]	Gerätebeschreibung.
IP kann weitergeleitet werden [CAN_Route]	Gibt an, ob die IP-Taschen zwischen Netzwerken weitergeleitet werden können. Mögliche Werte sind „wahr“ oder „falsch“.
Kann VLANs partitionieren [CAN_partitionvlans]	Gibt an, ob das LAN (Local Area Network) partitioniert werden kann. Mögliche Werte sind „wahr“ oder „falsch“.
Kann IP wechseln [CAN_Switch]	Gibt an, ob ein Netzwerkgerät über Layer 2-Switching-Fähigkeiten verfügt. Mögliche Werte sind „wahr“ oder „falsch“.
Anzahl der physischen Schnittstellen [physical_Interface_count]	Anzahl der physischen Schnittstellen.
Ports [Ports]	Einzelne Netzwerkschnittstelle (physisch oder logisch), die zum Verbinden von Geräten wie Computern, Servern, Zugriffspunkten oder Uplinks mit Switches oder Routern verwendet wird.
Discovery-Protokoll-ID [Discovery_proto_ID]	Eindeutiger Bezeichner des Geräts, das an teilnimmt Cisco Discovery-Protokoll (CDP) oder LLDP-Protokoll (Link Layer Discovery Protocol).
Discovery-Protokolltyp [Discovery_proto_type]	Protokolltyp. Mögliche Werte sind CDP oder LLDP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Routers.
Netzmaske [netmask]	Netzmaske des Routers.
NIC [nic]	Verweist auf die Tabelle „Netzwerkadapter“ [cmdb_ci_Network_Adapter].

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Name des Netzwerkadapters
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „IP-Router“ [cmdb_ci_ip_Router].

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung der Netzwerkrouter-Discovery.

CI	Beziehung	CI
Schnittstellenweiterleitungsregel beenden [dscy_Route_Interface]	Referenzen	IP-Router [cmdb_ci_ip_router]
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
IP-Router [cmdb_ci_ip_router]	Enthält::Enthalten in	Weiterleitungsregel wechseln [dscy_swtch_fwd_rule]
IP-Router [cmdb_ci_ip_router]	Enthält::Enthalten in	Partition wechseln [dscy_swtch_Partition]
IP-Router [cmdb_ci_ip_router]	Enthält::Enthalten in	Switchport [dscy_switchport]
IP-Router [cmdb_ci_ip_router]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
IP-Router [cmdb_ci_ip_router]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
IP-Router [cmdb_ci_ip_router]	Verwendet::Verwendet von	Schnittstellenweiterleitungsregel beenden [dscy_Route_Interface]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
IP-Router [cmdb_ci_ip_router]	Verwendet::Verwendet von	Nächste Hop-Weiterleitungsregel [dscy_Route_next_Hop]
IP-Router [cmdb_ci_ip_router]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	IP-Router [cmdb_ci_ip_router]
Netzwerk-ARP-Tabelle [Discovery_net_arp_table]	Referenzen	IP-Router [cmdb_ci_ip_router]
Nächste Hop-Weiterleitungsregel [dscy_Route_next_Hop]	Referenzen	IP-Router [cmdb_ci_ip_router]
Routerschnittstelle [dscy_router_interface]	Referenzen	IP-Router [cmdb_ci_ip_router]
Seriennummer [cmdb_serial_number]	Referenzen	IP-Router [cmdb_ci_ip_router]
Bridge-Porttabelle wechseln [Discovery_Switch_Bridge_Port_table]	Referenzen	IP-Router [cmdb_ci_ip_router]
Weiterleitungsregel wechseln [dscy_swtch_fwd_rule]	Referenzen	IP-Router [cmdb_ci_ip_router]
Weiterleitungstabelle wechseln [Discovery_Switch_fwd_table]	Referenzen	IP-Router [cmdb_ci_ip_router]
Partition wechseln [sdcy_swtch_Partition]	Referenzen	IP-Router [cmdb_ci_ip_router]
Bereichsstrukturtabelle wechseln [Discovery_Switch_Spanning_Tree_table]	Referenzen	IP-Router [cmdb_ci_ip_router]
Switchport [dscy_switchport]	Referenzen	IP-Router [cmdb_ci_ip_router]

Netzwerk-Switch-Discovery anhand von Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Netzwerk-Switch-Muster, um Netzwerk-Switches in Ihrer Umgebung zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu Netzwerk-Switches und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Informationen zur Probe-basierten Netzwerk-Switch- und Router-Discovery finden Sie unter Netzwerk-Switch- und Router-Discovery.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster für Discovery und Service-Mapping
- Visibility Content

Überprüfen Sie die IP-Adressinformationen

Der Switch muss IP-Adressinformationen für eine erfolgreiche Discovery enthalten.

Stellen Sie sicher, dass Weiterleitungsregeln für Exit-Schnittstellen konfiguriert und erreichbar sind

Für den Switch, der die IP-Adresse bereitstellt, müssen Weiterleitungsregeln für die Exit-Schnittstelle konfiguriert sein und für eine erfolgreiche Discovery erreichbar sein.

Erstellen von SNMP-Anmeldeinformationen

Erstellen Sie SNMP-Community-Anmeldeinformationen oder SNMPv3-Anmeldeinformationen. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .

Konfigurieren Sie Eigenschaften für die Switch-Discovery

Navigieren Sie zu sys_properties.list Und verifizieren Sie, dass *glide.discovery.L3_mapping*Systemeigenschaft ist auf festgelegt **Wahr** .

Sie können diese zusätzlichen Eigenschaften für die Netzwerk-Switch-Discovery konfigurieren.

Eigenschaft	Beschreibung
glide.discovery.max_concurrent_invocations_per_schedule	Legt eine maximale Anzahl geplanter Aufrufe für denselben Discovery-Zeitplan fest. Es wird ein Backlog geplanter Ausführungen verhindert, wenn Discovery nicht vor dem nächsten Start abgeschlossen wird. Der Wert ist eine Ganzzahl, die die maximale Anzahl automatisierter Aufrufe darstellt, die für denselben Zeitplan gleichzeitig ausgeführt werden können. Wenn der Grenzwert erreicht ist, werden nachfolgende geplante Aufrufe abgebrochen. Diese Eigenschaft wird durch den Wert 0 oder eine negative Zahl deaktiviert. • **Typ:** Ganzzahl • **Standardwert:** 3 • **Standort: Discovery-Definition** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „auch wenn abgebrochen“ festgelegt ist.
glide.discovery.bgp_router_disable	Deaktiviert die Ausführung des SNMP – Routing-Musters, wenn ein Router erkannt wird, der das BGP-Protokoll ausführt. Wenn Sie die Tabelle „Gerätenachbarschaften“ [Discovery_device_neigh während der Erkennung der horizontalen Ebene 2 der BGP-fähigen Geräte ausfüllen müssen, legen Sie fest **BGP-Routererkundung deaktiviert** Eigenschaft bis **Nein** . Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen mit zu wenig Arbeitsspeicher auf dem MID-Server. • **Typ:** true | false • **Standardwert:** true • **Standort: Discovery-Definition** > **Eigenschaften**

Gestapelte Switches erkennen

Unterstützt die Netzwerk-Switch-Discovery Cisco Gestapelte Switches. Mehrere Switches im Stapel werden anhand der primären IP-Adresse identifiziert. Discovery identifiziert jedes Mitglied des Stapels anhand von Elementen wie der primären IP-Adresse, einem dem Switch zugeordneten Namen und dem Stapelmodus. Die Beziehung wird zwischen einem primären Switch und den sekundären Switches erstellt.

Der primäre Switch verfügt über alle Felder, die in der Tabelle „IP-Switch“ [cmdb_ci_ip_Switch] aufgeführt sind. Der sekundäre Switch hat Name, Serial_number, model_ID, Manufacturer, Stack, und Stack_Mode.

Hinweis: Wenn alle Ports an einem Switch für Port 161 offen sind, verfügt der Switch über eine IP pro Port, aber die gleiche Seriennummer wird für alle Ports verwendet. Die Identifizierung des Konfigurationselements (Configuration Item, CI) basiert auf der Seriennummer. Daher aktualisiert die Discovery den vorhandenen Datensatz jedes Mal, anstatt einen neuen zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Netzwerk-Switch“.

IP-Switch [cmdb_ci_ip_Switch]

Feld	Beschreibung
Name [name]	Name des Switches.
Modell-ID [model_id]	Hardwaremodell-ID des Switches.
Hersteller [manufacturer]	Hersteller wechseln.
Installationsstatus [install_status]	Installationsstatus des Geräts. Standardwert ist installiert.
Seriennummer [serial_number]	Eindeutige Hardware-Seriennummer des Routers.
IP-Adresse [ip_address]	IP-Adressen, die Schnittstellen zugewiesen sind.
Beschreibung [short_description]	Gerätebeschreibung.
IP kann weitergeleitet werden [CAN_Route]	Gibt an, ob die IP-Taschen zwischen Netzwerken weitergeleitet werden können. Mögliche Werte sind „wahr“ oder „falsch“.
Kann VLANs partitionieren [CAN_partitionvlans]	Gibt an, ob das LAN (Local Area Network) partitioniert werden kann. Mögliche Werte sind „wahr“ oder „falsch“.
Kann IP wechseln [CAN_Switch]	Gibt an, ob ein Netzwerkgerät über Layer 2-Switching-Fähigkeiten verfügt. Mögliche Werte sind „wahr“ oder „falsch“.
Anzahl der physischen Schnittstellen [physical_Interface_count]	Anzahl der physischen Schnittstellen.
Ports [Ports]	Einzelne Netzwerkschnittstelle (physisch oder logisch), die zum Verbinden von Geräten wie Computern, Servern, Zugriffspunkten oder Uplinks mit Switches oder Routern verwendet wird.
Discovery-Protokoll-ID [Discovery_proto_ID]	Eindeutiger Bezeichner des Geräts, das an teilnimmt Cisco Discovery-Protokoll (CDP) oder LLDP-Protokoll (Link Layer Discovery Protocol).
Discovery-Protokolltyp [Discovery_proto_type]	Protokolltyp. Mögliche Werte sind CDP oder LLDP.
Stapel [Stapel]	Gibt an, ob ein Netzwerkgerät Teil einer gestapelten Gruppe von Switches ist, die als eine Einheit arbeiten. Mögliche Werte sind „wahr“ oder „falsch“.
Stapelmodus [Stack_Mode]	Stapelarchitektur oder Rolle eines Netzwerkgeräts innerhalb eines Stapels. Beispiel: Standalone, Stack_Master oder Stack_member.
Standort [location]	Standort, an dem der Switch installiert ist.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerk-Switches.
Netzmaske [netmask]	Netzmaske des Netzwerk-Switches.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adresse [cmdb_ci_ip_address] (Fortsetzung)

Feld	Beschreibung
NIC [nic]	Verweist auf die Tabelle „Netzwerkadapter“ [cmdb_ci_Network_Adapter].

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Name des Netzwerkadapters
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „IP-Switch“ [cmdb_ci_ip_Switch].

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung der Netzwerk-Switch-Discovery.

CI	Beziehung	CI
Schnittstellenweiterleitungsregel beenden [dscy_Route_Interface]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
IP-Switch [cmdb_ci_ip_Switch]	Enthält::Enthalten in	Weiterleitungsregel wechseln [dscy_swtch_fwd_rule]
IP-Switch [cmdb_ci_ip_Switch]	Enthält::Enthalten in	Partition wechseln [dscy_swtch_Partition]
IP-Switch [cmdb_ci_ip_Switch]	Enthält::Enthalten in	Switchport [dscy_switchport]
IP-Switch [cmdb_ci_ip_Switch]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
IP-Switch [cmdb_ci_ip_Switch]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
IP-Switch [cmdb_ci_ip_Switch]	Verwendet::Verwendet von	Schnittstellenweiterleitungsregel beenden [dscy_Route_Interface]
IP-Switch [cmdb_ci_ip_Switch]	Verwendet::Verwendet von	Nächste Hop-Weiterleitungsregel [dscy_Route_next_Hop]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
IP-Switch [cmdb_ci_ip_Switch]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Netzwerk-ARP-Tabelle [Discovery_net_arp_table]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Nächste Hop-Weiterleitungsregel [dscy_Route_next_Hop]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Routerschnittstelle [dscy_router_interface]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Seriennummer [cmdb_serial_number]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Bridge-Porttabelle wechseln [Discovery_Switch_Bridge_Port_table]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Weiterleitungsregel wechseln [dscy_swtch_fwd_rule]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Weiterleitungstabelle wechseln [Discovery_Switch_fwd_table]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Partition wechseln [sdcy_swtch_Partition]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Bereichsstrukturtabelle wechseln [Discovery_Switch_Spanning_Tree_table]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]
Switchport [dscy_switchport]	Referenzen	IP-Switch [cmdb_ci_ip_Switch]

Nutanix Akropolis-Discovery

Die ServiceNow Discovery Die Anwendung verwendet das Nutanix-Komponentenmuster, um Komponenten von zu finden Nutanix Akropolis-Lösung enthält Nutanix PRISM Central Version 5,10 oder Nutanix Prism-Element 5,9. Das Nutanix VM-Ereignismuster sucht Ereignisse, die für virtuelle Maschinen (VMs) in erstellt wurden Nutanix Bereitstellung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Nutanix Components-Muster verwendet REST APIs, um Informationen über die Acropolis-Bereitstellungskomponenten zu sammeln.

Das Nutanix-VM-Event-Muster wird alle fünf Minuten ausgeführt. Wenn Ereignisse vorhanden sind, die auf die Statusänderung in einem der anzeigen Nutanix Komponenten, löst die erneute Discovery von aus Nutanix Komponenten, die das Nutanix-Komponentenmuster verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster für Discovery und Service-Mapping
- Visibility Content
- CMDB CI-Klassenmodelle

Verifizieren MID-Server Anforderungen

Stellen Sie eine dedizierte bereit, und verbinden Sie sie MID-Server Mit Netzwerkzugriff auf Prism-Element und Prism Central.

Um Ereignisse im Zusammenhang mit VMs in zu erkennen Nutanix Bereitstellung, legen Sie fest MID-Server Fähigkeit zu **Alle** Oder bis **Nutanix** .

Installieren Nutanix Endpunkt-SSL-Zertifikate für MID-Server JRE

1. Sammeln Sie die Zertifikate, indem Sie durchsuchen Nutanix PRISM-Konsole in Internet Explorer.
2. Fügen Sie SSL-Zertifikate für hinzu MID-Server, Wie in beschrieben Fügen Sie SSL-Zertifikate für den MID-Server hinzu .
3. Verwenden Sie den folgenden JRE keytool-Befehl, um die SSL-Zertifikate in zu importieren MID-Server Schlüsselspeicher von: <MID Installation>/JRE/bin/keytool -Import -V -Keystore <MID Installation>jre/lib/Security/cacerts .

   Wenn Sie ein Passwort eingeben müssen, geben Sie das anwenderdefinierte Passwort oder das Standardpasswort „changeit“ ein.
4. Installieren Nutanix Endpunkt-SSL-Zertifikate für MID-Server JRE.

Überprüfen Sie die API-Berechtigungen

Überprüfen Sie, ob der Anwender Lesezugriff auf die folgenden API-Anforderungen hat:

- /PrismGateway/services/rest/v1/vms
- /PrismGateway/services/rest/v1/storage_pools
- /PrismGateway/services/rest/v2.0/tasks/list
- /PrismGateway/services/rest/v2.0/hosts
- /PrismGateway/services/rest/v2.0/clusters
- /PrismGateway/services/rest/v2.0/vms
- /PrismGateway/services/rest/v2.0/storage_containers
- /api/nutanix/v3/clusters/list
- /api/nutanix/v3/categories/list
- /api/nutanix/v3/categories/{category_keys}/list
- /api/nutanix/v3/category/query

Konfigurieren Sie Anmeldeinformationen für Standardauthentifizierung

Weitere Informationen finden Sie unter Virtual Server Interface .

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Discovery-Zeitplan, um eine gezielte Discovery von durchzuführen Nutanix Komponenten. Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für Nutanix Akropolis-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) VMware-Komponenten erkennen

Zum Aktivieren der Anzeige von Beziehungen zwischen Nutanix Akropolis und VMware, Ausführen VMware Discovery vor Nutanix Akropolis-Discovery. Führen Sie die horizontale Discovery für aus VMware VCenter mit der Probe VMware – vCenter-Rechenzentren.

(Optional) CI-Tag-Erkennung deaktivieren

Das Muster „Nutanix-Komponenten“ erkennt Tags für Nutanix Hosts und virtuelle Computer. Wenn Ihre Bereitstellung Dutzende von Tags aufweist, kann dies die Erkennung verlangsamen und zu Leistungsproblemen führen. So können Sie die Erkennung von CI-Tags deaktivieren:

1. Navigieren zu **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf das Muster **Nutanix Components**.
3. Klicken Sie unter **Erweiterungsabschnitt** auf das Kontrollkästchen **Kategorien (Tags)** und anschließend auf **Entfernen**.
4. Klicken Sie auf **Speichern**.

Passen Sie die Batch-Größe zum Entfernen redundanter Beziehungsdaten an

Die *`sn_itom_pattern.nutanix_relations_deletion_batch_size`*Die Eigenschaft legt die Batch-Größe zum Löschen von Beziehungen zwischen fest Nutanix VM-Instanz und Nutanix Host. Der Standardwert ist 1000. Sie können diese Batchgröße nach Bedarf anpassen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Nutanix-Komponenten“.

Nutanix-Controller-VM [cmdb_ci_nutanix_controller_vm]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Controller-VM.
VM-ID [vm_ID]	Der universelle Bezeichner (UUID) des Nutanix Controller-VM.
Objekt-ID [object_id]	Die ID des Nutanix Controller-VM.
Arbeitsspeicher (MB) [Arbeitsspeicher]	Die Arbeitsspeichergröße von Nutanix Controller-VM in Megabyte (MB).
Status [state]	Der Stromstatus des Nutanix Controller-VM (ein/aus).
Hypervisor-Typ [Hypervisor_type]	Der Typ des Hypervisors, der für verwendet wird Nutanix Controller-VM.
Beschreibung [short_description]	Die Beschreibung, die für die virtuelle Maschine in definiert ist Nutanix Konsole: PRISM Central oder Prism-Element.

Nutanix-Cluster [cmdb_ci_nutanix_cluster]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Cluster.
IP-Adresse [ip_address]	Die IP-Adresse des Nutanix Cluster.
Cluster-ID [cluster_id]	Die ID des Nutanix Cluster.
Objekt-ID [object_id]	Die Objekt-ID des Nutanix Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix-Cluster [cmdb_ci_nutanix_cluster] (Fortsetzung)

Feld	Beschreibung
Version [version]	Die Nutanix Clusterversion.
Vollversion [Full_Version]	Die Vollversion von Nutanix Cluster.
Internes Subnetz [internal_Subnet]	Das Subnetz der internen IP-Adresse des Nutanix Cluster.
Externes Subnetz [external_Subnet]	Das Subnetz der externen IP-Adresse des Nutanix Cluster.
Zeitzone [Zeitzone]	Die Zeitzone des Nutanix Cluster.
Hypervisor-Typen [Hypervisor_types]	Der Typ des Hypervisors, der für verwendet wird Nutanix Cluster.
NTP-Server [ntp_Servers]	Die NTP-Server (Network Time Protocol), die sich auf beziehen Nutanix Cluster.
Anzahl der Knoten [num_nodes]	Die Anzahl der Knoten, die mit verbunden sind Nutanix Cluster.
NCC-Version [ncc_Version]	Die Nutanix Cluster Check (NCC)-Version.
Block-Seriennummern [Block_Serial_Numbers]	Die Seriennummern der Datenblöcke, die mit verbunden sind Nutanix Cluster.

Nutanix-Host [cmdb_ci_nutanix_host]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Host.
Objekt-ID [object_id]	Die ID des Nutanix Host.
Anzahl der CPU-Kerne [cpu_Core_count]	Die Anzahl von Nutanix Hostkerne.
CPU-Core-Thread [cpu_Core_Thread]	Die Anzahl der Threads von Nutanix Host.
CPU-Geschwindigkeit (MHz) [cpu_Speed]	Die CPU-Geschwindigkeit des Nutanix Host in MHz.
CPU-Anzahl [cpu_count]	Die Anzahl der CPU-Sockel des Nutanix Host.
RAM (MB) [RAM]	Der Arbeitsspeicher des Hosts in Megabyte (MB)
Seriennummer [serial_number]	Seriennummer von Nutanix Host.

Nutanix-Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Speicherpool.
Pool-ID [Pool_ID]	Die UUID des Nutanix Speicherpool.
Objekt-ID [object_id]	Die ID des Nutanix Speicherpool.
Größe [Größe]	Die Größe von Nutanix Speicherpool.

Nutanix-Speichercontainer [cmdb_ci_nutanix_storage_container]

Feld	Beschreibung
Objekt-ID [object_id]	Die ID des Nutanix Container.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix-Speichercontainer [cmdb_ci_nutanix_storage_container] (Fortsetzung)

Feld	Beschreibung
Container-ID [container_id]	Die UUID des Nutanix Container.
Name [name]	Der Name des Nutanix Container.
Replikationsfaktor [Replication_factor]	Die Anzahl der Kopien, die für die darin gespeicherten Daten erstellt wurden Nutanix Speichercontainer.
Deduplizierung [Deduplizierung]	Die Deduplizierung ist für aktiviert oder deaktiviert Nutanix Container.
Komprimierung [Komprimierung]	Die Komprimierung ist für aktiviert oder deaktiviert Nutanix Container.
Löschcode [Erasure_Code]	Das Löschen von Code ist für aktiviert oder deaktiviert Nutanix Container.
Größe [Größe]	Die Nutanix Containergröße wird während der Discovery dynamisch berechnet.

Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Controller-VM.
ID der VM-Instanz [vm_inst_id]	Der universelle Bezeichner (UUID) des Nutanix Controller-VM.
Objekt-ID [object_id]	Die ID des Nutanix Controller-VM.
CPUs [cpus]	Die Anzahl der CPUs der VM
Arbeitsspeicher (MB) [Arbeitsspeicher]	Die Arbeitsspeichergröße von Nutanix Controller-VM in Megabyte (MB).
Status [state]	Der Stromstatus des Nutanix Controller-VM (ein/aus).
Beschreibung [short_description]	Die Beschreibung, die für die virtuelle Maschine in definiert ist Nutanix Konsole: PRISM Central oder Prism-Element.

Nutanix Prism Central [cmdb_ci_nutanix_prism_central]

Feld	Beschreibung
Name [name]	Der Name des Nutanix PRISM Central Multi-Cluster-Manager. • **PrismCentral@<IP_ADDRESS>** : Wenn die IP-Adresse der Prism Central-Instanz zugeordnet ist. Dies gilt in den folgenden Szenarien: ○ Während der schnellen Discovery mithilfe der HTTP-Klassifizierung. ○ Während der serverlosen Discovery, wenn die IP-Adresse in eingegeben wurde **PRISM_Address** Parameterwert. • **PrismCentral@<DNS_NAME>** : Wenn der DNS-Name der Prism Central-Instanz zugeordnet ist. Dies gilt, wenn der DNS-Name in eingegeben wurde **PRISM_Address** Parameterwert während serverloser Discovery.
Objekt-ID [object_id]	Die ID des Nutanix Prism Central. Dieses Feld hat denselben Wert wie **Name** Feld.

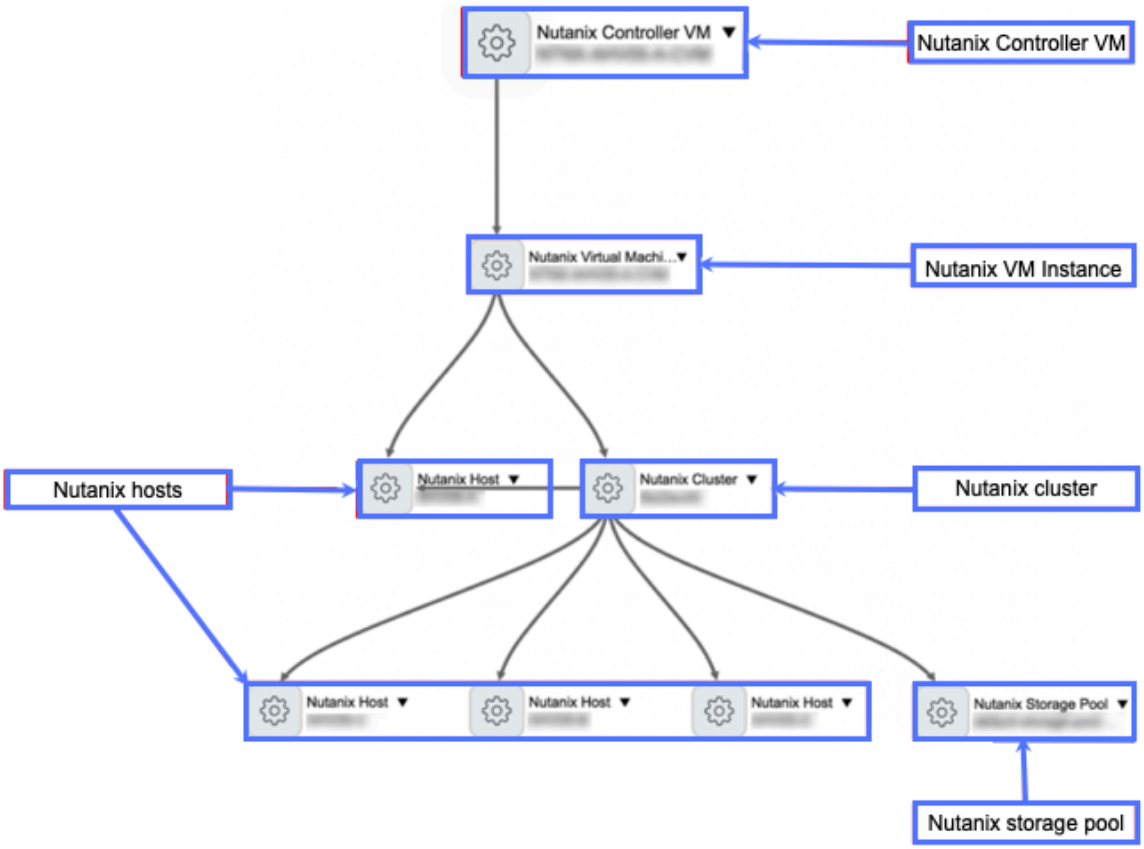
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix Prism Central [cmdb_ci_nutanix_prism_central] (Fortsetzung)

Feld	Beschreibung
	• **PrismCentral@<IP_ADDRESS>** : Wenn die IP-Adresse der Prism Central-Instanz zugeordnet ist. Dies gilt in den folgenden Szenarien: ○ Während der schnellen Discovery mithilfe der HTTP-Klassifizierung. ○ Während der serverlosen Discovery, wenn die IP-Adresse in eingegeben wurde **PRISM_Address** Parameterwert. • **PrismCentral@<DNS_NAME>** : Wenn der DNS-Name der Prism Central-Instanz zugeordnet ist. Dies gilt, wenn der DNS-Name in eingegeben wurde **PRISM_Address** Parameterwert während serverloser Discovery.

Die Grafik zeigt CIs, die Teil der Acropolis-Discovery in Bereitstellungen sind, die verwenden Nutanix AHV für Virtualisierung.

Nutanix-Komponenten

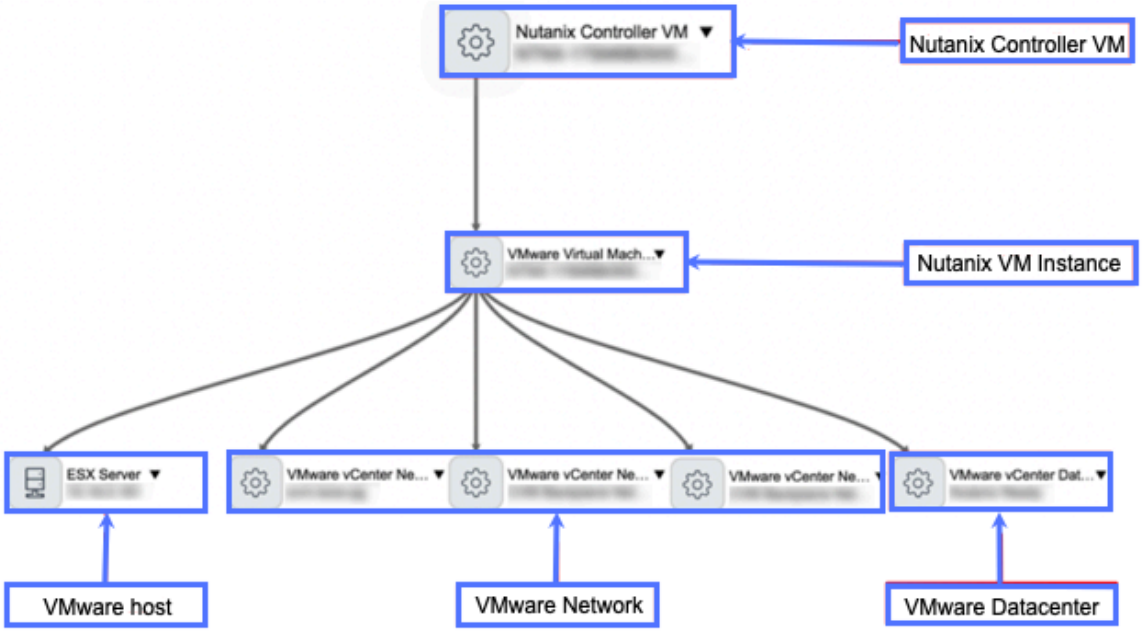


Die Grafik zeigt CIs, die Teil der Acropolis-Discovery in Bereitstellungen sind, die VMware-Software für die Virtualisierung verwenden.

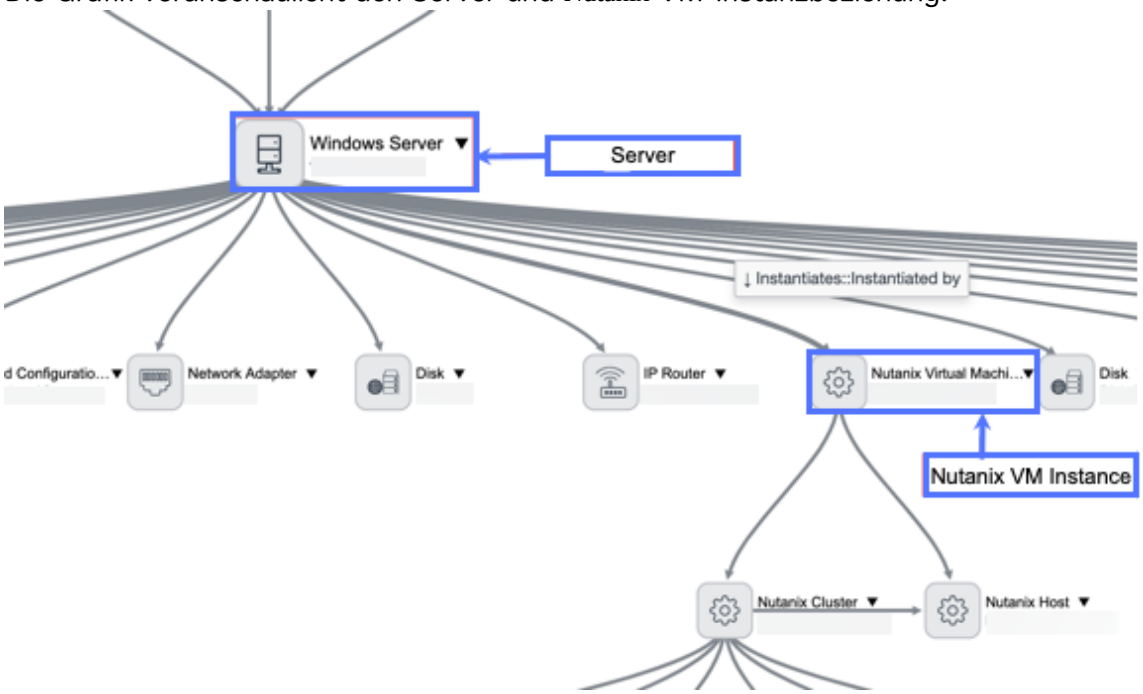
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix Komponenten in Bereitstellungen mit VM-Software



Die Grafik veranschaulicht den Server und Nutanix VM-Instanzbeziehung.



CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Nutanix Discovery:

CI	Beziehung	CI
Nutanix-Cluster [cmdb_ci_nutanix_cluster]	Definiert Ressourcen für::Erhält Ressourcen von	Nutanix-Speicherpool [cmdb_ci_storage_pool]
	Mitglieder::Mitglied von	Nutanix-Host [cmdb_ci_nutanix_host]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]	Registriert::Hat sich registriert	Nutanix-Host [cmdb_ci_nutanix_host]
	Gehostet auf::Hostet	Nutanix-Cluster [cmdb_ci_nutanix_cluster]
Nutanix-Controller-VM [cmdb_ci_nutanix_controller_vm]	Wird ausgeführt auf::Wird ausgeführt	Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]
	Wird ausgeführt auf::Wird ausgeführt	[cmdb_ci_vmware_instance]
	Gehostet auf::Hostet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]
Nutanix-Speicherpool [cmdb_ci_storage_pool]	Enthält::Enthalten in	Nutanix-Speichercontainer [cmdb_ci_nutanix_storage_container]
	Gehostet auf::Hostet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]
VMware-Cluster [cmdb_ci_vmware_cluster]	Definiert Ressourcen für::Erhält Ressourcen von	Nutanix-Speicherpool [cmdb_ci_storage_pool]
Server [cmdb_ci_server]	Instanziiert::Instanziiert von	Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]
Nutanix-Cluster [cmdb_ci_nutanix_cluster]	Verwaltet von::Verwaltet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]

Tag-Discovery

Das Muster „Nutanix-Komponenten“ erfasst Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Kategorieschlüssel
Wert [value]	Der Kategoriewert
Konfigurationselement [configuration_item]	Verweist auf die Tabelle „Nutanix-Host“ [cmdb_ci_nutanix_Host].

Dashboard

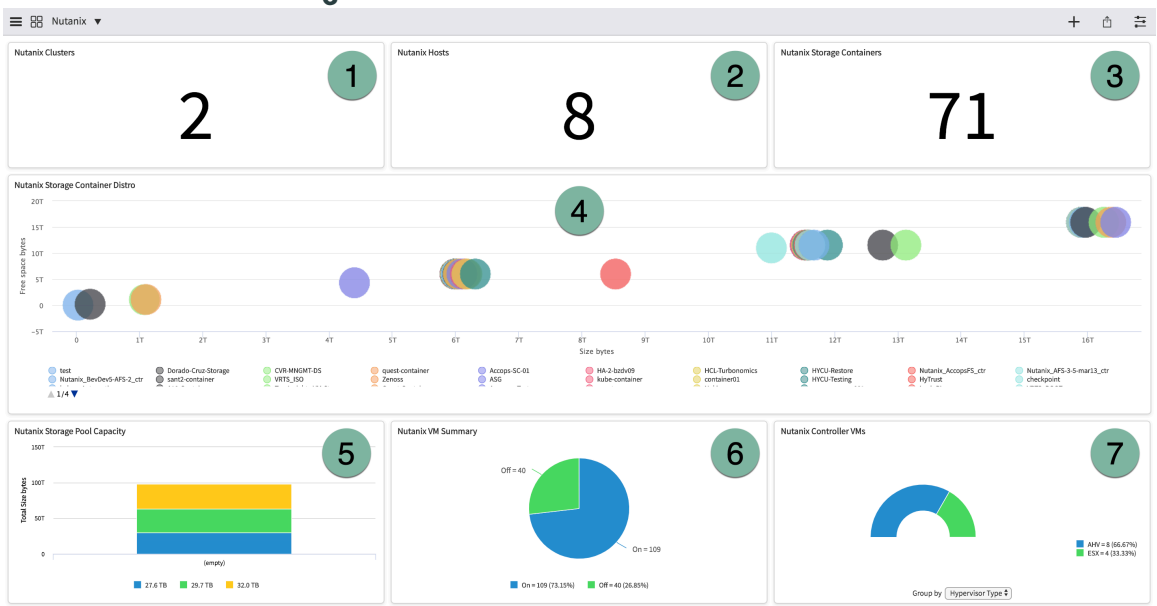
Das Dashboard enthält Berichte, die Anfragen an die Configuration Management Database (CMDB) stellen und die Ergebnisse anzeigen. Die Informationen werden erst angezeigt, nachdem das Muster die Infrastruktur erkannt hat.

Navigieren Sie zum Anzeigen des Dashboards zu **Self-Service** > **Dashboards** > **Alle** > **Nutanix**an.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (August 2024 Store), können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Und verwenden Sie das erweiterte Dashboard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard mit Erkennungsberichten



Die Berichte auf dem Dashboard enthalten die folgenden Informationen. Sie werden in der Tabelle anhand der in der Grafik angezeigten Nummern aufgelistet.

	Bericht	Beschreibung
1	Nutanix-Cluster	Nummer oder Nutanix Cluster gefunden.
2	Nutanix-Hosts	Anzahl von Nutanix Hosts gefunden.
3	Nutanix-Speichercontainer	Anzahl von Nutanix Speichercontainer gefunden.
4	Nutanix-Speichercontainer-Verteilung	Die Verteilung von Nutanix Speichercontainer freier Speicherplatz und Kapazität in Byte.
5	Nutanix-Speicherpool-Kapazität	Die Kapazität von Nutanix Speicherpool, in Byte.
6	Nutanix-VM-Zusammenfassung	Die Nutanix VMs gruppiert nach Status: Ein, aus, beendet.
7	Nutanix-Controller-VMs	Die Nutanix Controller-VMs gruppiert nach Hypervisor-Typ.

Erstellen Sie einen serverlosen Zeitplan für Nutanix Akropolis-Discovery

Erstellen Sie einen serverlosen Zeitplan zur Erkennung Nutanix Akropolis mit REST API.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.

2. Erstellen Sie den Discovery-Zeitplandatensatz.

a. Wählen Sie **Neu**.

b. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Erkannt	Scan-Typ, der serverlos sein muss.
MID-Server verwenden	Name des MID-Server Mit Zugriff auf Nutanix Umgebung.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.
Ausführen	Bestimmt den Ausführungszeitplan der Erkennung.

c. Wählen Sie **Absenden**.

3. Erstellen Sie das Ausführungsmuster.

a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.

b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .

c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll, der Nutanix-Komponenten sein muss.
Proxyhost	Vollqualifizierter Domänenname (FQDN) des Computers, auf dem der Proxy-Server installiert ist, der global sein muss. Dieses Feld ist optional.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

d. Wählen Sie **Absenden**.

4. Legen Sie die Parameter des Musterstartprogramms fest.

a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.

b. Füllen Sie im Formular die Felder aus.

Parameter	Wert
PRISM_Address	IP-Adresse oder der FQDN, der der Prism Central-Instanz zugeordnet ist.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Nutanix Akropolis-Discovery

NVIDIA GPU-Discovery mithilfe von Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet die Mustererweiterung Linux Server **Erkennen Sie Nvidia-GPU** Zu finden NVIDIA Grafikverarbeitungseinheiten (GPUs). Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Muster „Nvidia-GPU erkennen“ ist eine Erweiterung des Linux-Server-Musters. Weitere Informationen finden Sie unter Linux Discovery.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die Berechtigungen für den folgenden SSH-Befehl

Überprüfen Sie, ob Sie haben **Lesezugriff** Berechtigung für den SSH-Befehl: `nvidia-smi -q` .

SSH-Anmeldeinformationen erstellen

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Discover Nvidia GPU-Musters.

Grafikverarbeitungseinheit [cmdb_ci_gpu]

Feld	Beschreibung
Name [name]	Modellname der GPU.
Hersteller [manufacturer]	Lieferant der GPU.
Modell-ID [model_id]	Produktname der GPU.
Seriennummer [serial_number]	Seriennummer der GPU.

Darüber Hinaus Discovery Füllt die Daten in einem nicht- CMDB Tabelle beim Ausführen des Discover Nvidia GPU-Musters.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GPU-Details [gpu_Details]

Feld	Beschreibung
Tafel-ID [Board_ID]	Bezeichner für die GPU-Tafel, die zu Diagnosezwecken verwendet werden kann.
Tafelteilnummer [Board_part_number]	Die Teilenummer der GPU-Tafel.
Bus-ID [Bus_ID]	Bezeichner für den PCI-Bus (Peripheriekomponente Interconnect), auf dem sich die GPU befindet.
CUDA-Version [cuda_Version]	Version des CUDA-Toolkits, das von installiert wird NVIDIA Treiber.
Treiberversion [Driver_Version]	Version von NVIDIA Auf dem System installierter Treiber.
GSP-Firmware-Version [gsp_Firmware_Version]	Version der Firmware des GPU-Systemprozessors (GSP).
Index [index]	Indexnummer der GPU, wie vom System gemeldet.
Inforom-ECC [inforom_ecc]	Version des Fehlerkorrekturcodes (Error Correcting Code, ECC), der zum Aufzeichnen von Daten im InfoROM verwendet wird.
Inforom-IMG [inforom_img]	Globale Version des InfoROM-Images.
Inforom-OEM [inforom_oem]	Version der Konfigurationsdaten des ursprünglichen Geräteherstellers (OEM) im InfoROM.
Inforom-PWR [inforom_pwr]	Version der Energieverwaltungsdaten im InfoROM.
Freie Speichernutzung [Memory_free_usage]	Derzeit freier GPU-Arbeitsspeicher.
Gesamtauslastung des Arbeitsspeichers [Memory_total_usage]	Gesamtmenge des installierten GPU-Speichers.
Auslastung des verwendeten Arbeitsspeichers [Memory_used_usage]	Menge des derzeit verwendeten GPU-Speichers.
Name [name]	Offizieller Produktname der GPU.
Aktueller PCIE-Link [pcie_current_Link]	Aktuelle PCIe-Linkgenerierung (Interconnect Express) für Peripheriekomponenten.
Leistungsstatus [Performance_State]	Leistungs- und Leistungsstufen der GPU. Mögliche Werte werden von P0 bis P15 ausgeführt, wobei niedrigere Zahlen eine höhere Leistung anzeigen.
Status des Persistenzmodus [persistence_Mode_Status]	Gibt an, ob der Persistenzmodus für die GPU aktiviert ist. Mögliche Werte sind aktiviert oder deaktiviert.
Seriennummer [serial_number]	Seriennummer der GPU.
UUID [UUID]	Universally Unique Identifier (UUID) der GPU.
VBIOS-Version [vbios_Version]	Basic Input/Output System (BIOS) der GPU-Tafel.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von NVIDIA GPU-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Grafikverarbeitungseinheit [cmdb_ci_gpu]	Verwendet von::Verwendet	Linux-Server [cmdb_ci_linux_server]

Oracle Katalog-Discovery

Die Muster für Discovery und Service-Mapping-Anwendung verwendet **Rufen Sie Kataloginformationen ab** Mustererweiterung der zu suchenden Oracle DB in Unix- und Oracle DB in Windows-Mustern Oracle Katalotobjekte. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery Verwendet Oracle DB unter Unix und Oracle DB unter Windows-Mustern und die Mustererweiterung „Kataloginformationen abrufen“, um eine horizontale Discovery auszuführen.

Sie können dieses Muster auf der ServiceNow AI Platform® mit Madrid-Release oder höher verwenden.

Für Informationen zu Oracle Datenbank-Discovery, siehe Oracle-Datenbank-Discovery .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Geben Sie einem Anwender Berechtigungen zum Ausführen von Abfragen für ALL_TABLES

Geben Sie einem Anwender Berechtigungen zum Ausführen von Abfragen für ALL_TABLES.

Um die Tabellen anderer Anwender in ALL_TABLES anzuzeigen, muss ein Anwender über eine der folgenden Berechtigungen verfügen:

- Berechtigungen auf Objektebene, z. B.: AUSWÄHLEN.
- Rolle auf höherer Ebene, z. B.: WÄHLEN SIE EINE BELIEBIGE TABELLE aus.

Konfigurieren Sie anwendbare Anmeldeinformationen

Konfigurieren Sie anwendbare Anmeldeinformationen für den CI-Typ der Oracle-Instanz [cmdb_ci_DB_ora_instance]. Weitere Informationen finden Sie unter Anwendbare Anmeldeinformationen .

Konfigurieren Windows Anmeldeinformationen für Windows Betriebssystem (OS)

Weitere Informationen finden Sie unter Windows-Anmeldeinformationen .

Konfigurieren UNIX Anmeldeinformationen für UNIX BETRIEBSSYSTEM

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

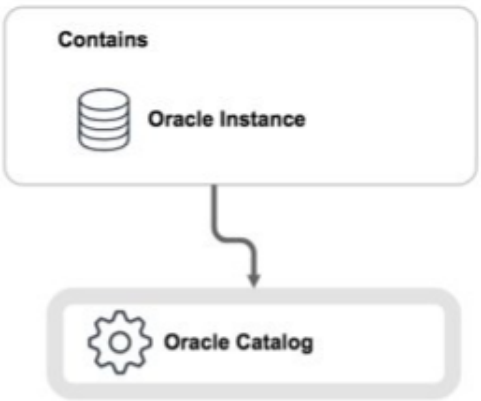
Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen der Erweiterung „Muster für Kataloginformationen abrufen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Oracle Catalog [cmdb_ci_db_ora_catalog]	
database_instance	Der Name der Datenbanksinstanz (SID)
name	Der Name des CI in der CMDB; Schema und SID
schema	Der Name des Katalogobjekts

Im Folgenden finden Sie eine Abhängigkeitsansicht der Beziehung zwischen einem Oracle Catalog und einer Oracle-Instanz.



CI-Beziehungen

Diese Beziehung wird zur Unterstützung erstellt Oracle Katalog-Discovery.

CI	Beziehung	CI
Oracle Catalog [cmdb_ci_db_ora_catalog]	Enthält::Enthalten in	Oracle-Instanz [cmdb_ci_db_ora_instance]

Oracle Datenbank 12c-Discovery

Die ServiceNow Discovery Die Anwendung kann Pluggable Datenbanken (PDBs) und Containerdatenbanken (CDBs) erkennen, die Funktionen von sind OracleDatenbank 12c. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Eine PDB ist eine portable Sammlung von Schemata, Schemaobjekten und Nicht-Schemaobjekten, die einem Oracle Net-Client als separate Datenbank angezeigt werden. Eine Sammlung von PDBs wird als Containerdatenbank (CDB) bezeichnet.

Weitere Informationen zu PDBs und CDBs finden Sie unter Was sind CDBs, PDBs und Container? .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Legen Sie die Benutzeranmeldeinformationen fest, und gewähren Sie Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren Sie Applicative-Anmeldeinformationen .
- Für Windows konfigurieren Sie Windows-Anmeldeinformationen .
- Für Unix konfigurieren Sie SSH-Anmeldeinformationen .
- Konfigurieren Sie für die Oracle-Datenbank die Discovery von Oracle-Datenbanken.
- Gewähren Sie einem Benutzer Berechtigungen zum Ausführen von Abfragen in den folgenden Tabellen:
  - V$DATAFILE
  - V$TEMPFILE
  - V$LOG
  - DBA_FREE_SPACE
  - V$DATABASE
  - V$PDBS
  - V$PARAMETER

Hinweis: Legen Sie Applicative-Anmeldeinformationen auf der CDB-Ebene fest, um nur Beziehungen für PDBs und die CDB-Größe zu ermitteln. Legen Sie alternativ Applicative-Anmeldeinformationen auf der CDB/PDB-Ebene fest, um Beziehungen für PDBs und die CDB/PDB-Größe zu ermitteln. Wenn Sie auf der CDB-Ebene keine Applicative-Anmeldeinformationen festlegen, werden keine PDB-Attribute erkannt.

Daten, die während der Erkennung erfasst wurden

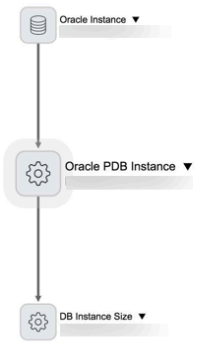
Discovery erfasst die folgenden Daten:

Tabelle und Feld	Beschreibung
cmdb_ci_db_ora_pdb_instance: Beziehungstyp: Verwaltet von	
sid	Name der PDB-Instanz
name	Name des CI in CMDB Dies ist eine Kombination aus SID und dem Hostname.
Version	Version der PDB aus der CDB-Instanz
Edition	Ausgabe der PDB aus der CDB-Instanz
install_directory	Installationsverzeichnis der PDB aus der CDB-Instanz
oracle_home	Oracle Home der PDB aus der CDB-Instanz
cdb_name	Name der CDB-SID, die die PDB enthält. Dies bezieht sich auf das Configuration Item (CI) der Oracle-Datenbankinstanz ().
cmdb_ci_db_instance_size: Beziehungstyp: Aufgenommen von	
sid	Name der CDB-/PDB-Instanz der Oracle-Datenbank
name	Name des CI in CMDB Dies ist eine Kombination aus SID und dem Hostnamen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
db_size	Gesamtgröße, die der Datenbankinstanz zugewiesen ist
used_size	Von der Datenbankinstanz verwendete Größe
free_size	Größe des freien Speicherplatzes in der Datenbankinstanz

Im Folgenden finden Sie eine Abhängigkeitsansicht der Beziehung zwischen PDBs, CDBs und Containern.



Oracle Global License Advisory Services (GLAS) – Datenerfassung anhand von Mustern

Von der Anwendung ServiceNow Discovery wird das von Oracle geprüfte Muster „GLAS Data Collection“ zur Erkennung von Oracle GLAS-Daten verwendet. Diese Daten enthalten erkannte Oracle Datenbank-, Middleware- und Java-Konfigurationselemente.

Das Muster „Oracle GLAS Data Collection“ ist eine Erweiterung der folgenden Muster:

- Oracle Datenbank auf UNIX Und Windows Muster
- Oracle Middleware ein Linux Für die folgenden Muster:
  - Oracle Tuxedo
  - WebLogic
  - Linux
- Oracle Java-on-Java-Installationsmuster

Die Oracle Datenbank- und Middleware-Muster führen die Mustererweiterungen aus, und die gesammelten Daten werden in gespeichert ServiceNow Tabellen für GLAS-Daten. Die Oracle Das Datenbankmuster DER GLAS-Datensammlung kann für verwendet werden ServiceNow AI Platform Beginnend mit Paris Release. Die Oracle Das GLAS-Datensammlungs-Middleware-Muster kann für verwendet werden ServiceNow AI Platform Beginnend mit Rome Release. Die Oracle Java-Muster kann auf verwendet werden ServiceNow AI Platform Beginnend mit Washington DC Release.

Einzelheiten zum Anzeigen und Herunterladen der gesammelten Oracle GLAS-Daten finden Sie unter Oracle GLAS-Daten (Global License Advisory Services) herunterladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über die unterstützten Versionen von zu erfahren Oracle, Siehe Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Installieren Sie Data Collection for Oracle Global Licensing and Advisory Services Store-App

Navigieren zu **Systemdefinition** > **Plugins** Und installieren Sie Data Collection for Oracle Global Licensing and Advisory Services App.

- Die Mindestversion für die Datenbanksammlung ist 1.4.0
- Die Mindestversion für die Middleware-Sammlung ist 1.7.1
- Die Mindestversion für die Java-Sammlung ist 1.8.4

Hinweis: Die Data Collection for Oracle Global Licensing and Advisory Services App erfordert Discovery(Com.snc.Discovery) Plugin, um ordnungsgemäß zu funktionieren.

Überprüfen Sie, ob die folgenden Anwendungen installiert sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die Betriebssystemberechtigungen

Überprüfen Sie, ob Ihr Windows Oder UNIX Anwender kann temporäre Dateien unter schreiben /Tmp .

Überprüfen Sie, ob Sie die folgenden Betriebssystembefehle ausführen können:

- ls
- cat
- ps

Erstellen Sie Betriebssystem-Anmeldeinformationen

Stellen Sie sicher, dass Sie über die folgenden Anmeldeinformationen für Ihr Betriebssystem verfügen, und erstellen Sie dann Anmeldeinformationen für sie im ServiceNow AI Platform:

- UNIX Anmeldeinformationen mit SSH. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .
- Windows Anmeldeinformationen mit PowerShell/WMI. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen .

Hinweis: PowerShell- und WMI-Anmeldeinformationen sind nur für die Datenbanksammlung erforderlich.

Überprüfen Sie Folgendes Oracle Berechtigungen

Stellen Sie sicher, dass Sie über anwendbare Anmeldeinformationen für verfügen Oracle Instanz (cmdb_ci_DB_ora_instance) mit den folgenden Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Leseberechtigungen für die Datei tnsnames.ora
- Berechtigungen zum Ausführen des Befehls *sqlplus*
- (Für Middleware-Sammlung) Sudo-Berechtigungen zum Ausführen des folgenden Befehls: Sudo su – oracle -c „$ORACLE_INSTANCE/bin/opmnctl Status“

Überprüfen Sie, ob Sie den Anwendernamen und das Passwort für den entsprechenden haben Oracle Datenbank mit Leseberechtigungen für die folgenden Tabellen:

DBA_ADVISOR_TASKS	DBA_USERS	SYS.MODEL$
DBA_CPU_USAGE_STATISTICS	MDSYS.DM$MODEL	SYS.REGISTRY$HISTORY
DBA_ENCRYPTED_COLUMNS	MDSYS.DM$OBJECT	SYSMAN.MGMT_INV_CONTAINER
DBA_FEATURE_USAGE_STATISTICS	MDSYS.DM$P_MODEL	SYSMAN.MGMT_LICENSES
DBA_FLASHBACK_ARCHIVE_TABLES	DVSYS.DBA_DV_REALM	SYSMAN.MGMT_LICENSE_DEFINITIONS
DBA_INDEXES	GV$IM_SEGMENTS	SYSMAN.MGMT_TARGETS
DBA_LOBS	GV$INSTANCE	SYSMAN.MGMT_VERSIONS
DBA_LOB_PARTITIONS	GV$PARAMETER	V $ ARCHIVE_DEST_STATUS
DBA_LOB_SUBPARTITIONS	MDSYS.SDO_FEATURE_USAGE	V $ BLOCK_CHANGE_TRACKING
DBA_OBJECTS	MDSYS.SDO_GEOM_METADATA_TABLE	V$CONTAINERS
DBA_RECYCLEBIN	MGMT$TARGET	V$DATABASE
DBA_REGISTRY	ODM.ODM_MINING_MODEL	V$DATAGUARD_CONFIG
DBA_SQLSET	ODM_DOCUMENT	V$LICENSE
DBA_SQLSET_REFERENCES	ODM_RECORD	V$OPTION
DBA_SQL_PROFILES	REDACTION_POLICIES	V$PARAMETER
DBA_TABLES	SCHEMA_VERSION_REGISTRY	V$VERSION
DBA_TABLESPACES	SYS.CDC_CHANGE_SETS$	dba_aws
DBA_TAB_PARTITIONS	SYS.CDC_CHANGE_TABLES $	
DBA_TAB_SUBPARTITIONS	SYS.DBA_MINING_MODELS	

Erstellen Sie anwendbare Anmeldeinformationen für die Oracle-Instanz

Erstellen Sie anwendbare Anmeldeinformationen auf der ServiceNow AI Platform. Weitere Informationen finden Sie unter Applicative-Anmeldeinformationen .

Für virtuelle Computer: Überprüfen Sie die Anmeldeinformationen für virtuelle Computer

Stellen Sie für virtuelle Computer sicher, dass Sie über die relevanten Anmeldeinformationen zum Sammeln von Hardwaredaten für Computer verfügen, die auf den folgenden virtuellen Anbietern gehostet werden:

- VMware
- Nutanix

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- IBM
- Hyper-V

Datenbank-CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_orcl_vsession	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_ora_lms_detail	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_ora_lms_overview	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_options	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_dba_users	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_vlicense	Enthält::Enthalten in	cmdb_ci_db_ora_instance

Tuxedo-Middleware-Erweiterung

Tuxedo-Lizenzkonfiguration und erfasste Protokolldateien:

- *_InstallLog.log
- *ubbc*
- bdmconfig*
- comps.xml
- dmconfig*
- JSconfig.xml
- lic.txt
- registry.xml
- tuxconfig*
- tuxwsvr.ini

Hinweis: Das Sternchen steht für ein oder mehrere Zeichen im Dateinamen.

Erfasste Prozesse:

- BBL
- DBBL
- GWWS
- JSH
- JSL
- TMJAVASVR
- TMMETADATA

WebLogic-Middleware-Erweiterung

Erfasste Dateien:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- beahomelist
- biee-domain.xml
- cluster.properties
- comps.xml
- config.xml
- domain-registry.xml
- opmn.xml
- portalconfig.xml
- pthome.xml
- registry.xml
- server.xml
- sessions.xml
- setupinfo.txt

WebLogic-Prozesse und -Dateien, die für die folgenden Middleware-Produkte erfasst werden:

- WebLogic
- OAS
- SOA
- OBI
- WebCenter
- FormularBerichte

Prozesse

WebLogic			OAS			OBI
startWebLogic	httpd	f90	iooomgrrmi	r30rbe32	rwrqm60	nqsserver
Java	Apache	frmweb	javaw	r30rqm32	rwrqm	sawserver
startWLS	Java	ifbld60	Java	r30run32	rwrun60	coreapplication_obijh1
nodemanager	opmn	ifbld90	jre	r30sxc32	rwserver	nqscheduler
beasvc	dis3	ifcgi60	oad	r30sxu32	rwsxc60	nqsclustercontroller
beasvc64	dis4	ifcmp60	odisrv	rwbld60	rwsxu60	essbase
beasvcX64	dis51pr	ifcmp90	ofcguard	rwbuilder	vdeserver	essvr
oraclesvc	dis51ws	ifctrl60	oidrepld	rwcgi60	webcachea	essbasestudio
opmn	dis51	ifdbg60	oidmon	rwcli60	webcached	hyperion
wlsvc	dwfde61	ifrun60	oidldapd	rwcon60	webcache	
wlsvc64	f45des	ifsrv60	opmn	rwconverter		
wlsvcX64	f45run	ifwdb60	r30cli32	rwisv60		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozesse (Fortsetzung)

WebLogic		OAS			OBI	
jmc	f50dbg32	ifweb60	r30con32	rwmts60		
httpd	f50run32	ifweb90	r30isv32	rwqmu60		
jrmc	f60	imapds	r30qmu32	rwrbe60		

Middleware-CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_ora_lms_overview	Enthält::Enthalten in	cmdb_ci_linux_server
cmdb_ci_config_file_tracked	Enthält::Enthalten in	cmdb_ci_linux_server

Diese Beziehungen werden durch eine Containment-Regel erstellt, die die gültigen Objekte beschreibt, die die Linux-CIs enthalten können.

Mit der Anwendung „Middleware-Datensammlung“ installierte Eigenschaften

Um auf die Eigenschaften der installierten Anwendung zuzugreifen, navigieren Sie zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an. Sie müssen über die Administratorrolle verfügen, um diese Eigenschaften zu ändern.

Systemeigenschaft	Standardwert	Beschreibung
sn_itom_oracleglas.isMaskingIp	*wahr*	Bestimmt, ob die IP-Adresse in maskiert werden soll Oracle middleware hat Dateien nachverfolgt, indem der Wert durch „Text_removed“ ersetzt wurde.
sn_itom_oracleglas.isMaskingUserName	*wahr*	Bestimmt, ob der Anwendername in maskiert werden soll Oracle middleware hat Dateien nachverfolgt, indem der Wert durch „Text_removed“ ersetzt wurde.
sn_itom_oracleglas.isMaskingPort	*wahr*	Bestimmt, ob der Port in maskiert werden soll Oracle middleware hat Dateien nachverfolgt, indem der Wert durch „Text_removed“ ersetzt wurde.

Steuern Sie DIE GLAS-Datensammlung

Folgendes MID-Server Die Eigenschaft steuert die GLAS-Datensammlung: *sn_itom_oracleglas.disable_glas_data_collection*

Diese Eigenschaft ist standardmäßig auf **false** festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In Data Collection for Oracle Global Licensing and Advisory Services Versionen vor 1.10.2, der Eigenschaftsname lautet *sn_itom_pattern.disable_glas_data_collection*.

Oracle Java-Prozess-Discovery

ITOM-Transparenz Kann Java-laufende Prozesse in Ihrer Infrastruktur erkennen, sodass Sie sich an halten können Oracle Lizenzvereinbarungen und Vorbereitung auf GLAS-Audits. Sie können die Discovery mithilfe des Java-Installationsmusters (IP-basiert) durchführen, Agent Client Collector Mit Anwendungsmustern, oder Agent Client Collector Mit dateibasierter Discovery.

Im Muster-Flow werden die Java-Prozesse von Application Dependency Mapping (ADM) erkannt. Wenn die Prozesse erkannt werden, wird das Java-Installationsmuster ausgelöst und erfasst die Daten.

Für Informationen zum privilegierten Anwenderzugriff , Siehe KB1705845 .

Weitere Informationen zu finden Agent Client Collector Informationen zu Mustern finden Sie unter Anwendungsmuster für Agent Client Collector.

Weitere Informationen zu finden Agent Client Collector Informationen zur dateibasierten Discovery finden Sie unter Erkennen Sie Java-Installationsdaten mit Agent Client Collector Visibility – Inhalt Dateibasierte Discovery.

Erfasste Daten

Java-Audit [ora_Java_Audit]

Feld	Beschreibung
Name	Name des Datensatzes. Beispiel: Java@Hostname
Name Des Physischen Computers	Name des Host-CI
Rechnertyp	Entweder Server(S) oder Desktop(D)
Java-Herausgeber/Runtime-Lieferant	Java-Lieferantenname
Betriebssystem	Betriebssystem, in dem die Java ausgeführt wird
Umgebungstyp	Produktions- oder Entwicklungs- oder QA-Umgebung
Java-Release/Version/Build	Java-Version
Installationspfad	Absoluter Installationspfad der Java-Binärdatei
Installationsdatum (Datum/Uhrzeit)	Datum und Uhrzeit der im Dateisystem erstellten Java-Binärdatei
Release-Datei (J/N)	Gibt an, ob A *Release.md* Datei ist in der Installation vorhanden
Prozessormarke/Modell	Name des Prozessormodells
Sockets (Ganzzahl)	Anzahl der CPU-Sockets
Kerne (Ganzzahl)	Anzahl der CPU-Kerne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Java-Audit [ora_Java_Audit] (Fortsetzung)

Feld	Beschreibung
V6 und früher	Gibt an, ob Sie haben eine Java-Version 6 oder früher
Open Source	Gibt an, ob Sie haben eine Open Source-Java-Installation
Schalten Sie kommerzielle Funktionen frei	Gibt an, ob Sie haben die kommerziellen Funktionen (z. B. JFR) aktiviert
Missionssteuerung	Gibt an, ob Das Plugin „Missionssteuerung“ ist aktiviert
AMC-Service Desk-Mitarbeiter	Gibt an, ob Das AMC Agent-Plugin ist aktiviert
Nutzungs-Tracker	Gibt an, ob Die Nutzungstracker-Funktion ist aktiviert
VM-Objekt-ID	Objekt-ID der VM-Instanz
PID	PID des laufenden Prozesses
IP-Adresse	IP-Adresse des Hosts/der VM
Zuerst erkannt	Das Datum der ersten Discovery
Neuester Discovery-Scan	Das Datum der letzten Discovery
Discovery-Quelle	Die Discovery-Methode.
Anwendung	Verweis auf die Tabelle [cmdb_ci_appl]
Softwareinstallation	Verweis auf die Tabelle [cmdb_sam_SW_install]
Java-Nachweis	Verweis auf die Tabelle [cmdb_ora_Java_evidence]
Host	Verweis auf die Tabelle [cmdb_ci]

Java-Nachweis [ora_Java_evidence]

Feld	Beschreibung
Laufender Prozess	Verweis auf die Tabelle [cmdb_running_Process]
Host-CI	Verweis auf die Tabelle [cmdb_ci_Computer]
Datei-Informationen	Stellt einen Verweis auf die Tabelle [cmdb_file_Information] bereit. Relevant nur für dateibasierte Discovery (FBD); in der musterbasierten Discovery bleibt dieses Feld leer.

Laden Sie herunter Oracle GLAS-Bericht in Discovery-Administratorarbeitsbereich. Weitere Informationen finden Sie unter Oracle GLAS-Daten (Global License Advisory Services) herunterladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle GLAS-Datenerfassung

Nach Discovery Schließt die Erkennung der Komponenten Ihrer Datenbank- oder Middleware-Bereitstellung ab. Sie können die relevanten Statistiken in anzeigen Oracle GLAS-Datensammlung.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (August 2024 Store), können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Um anzuzeigen und darauf zuzugreifen Oracle GLAS-Datensammlung.

Oracle GLAS-Daten (Global License Advisory Services) herunterladen

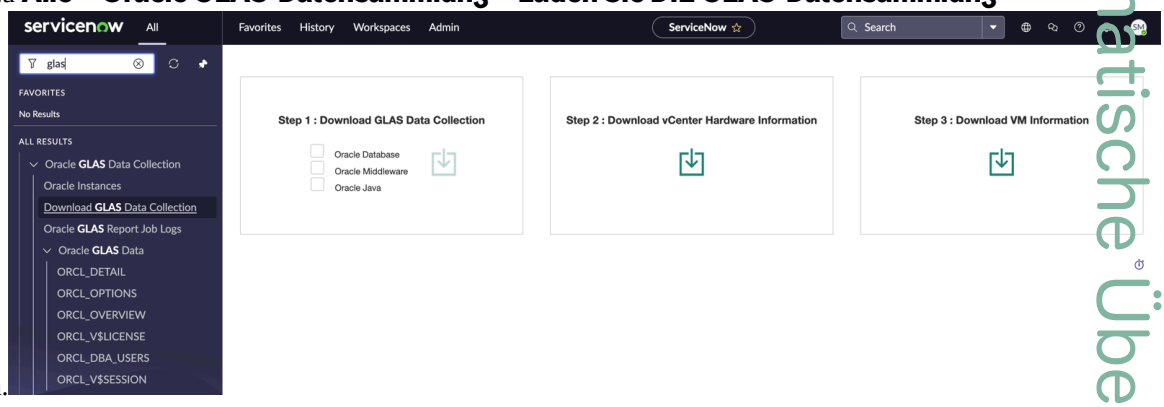
Herunterladen Oracle GLASDATEN im CSV-Format, um detaillierte Informationen zu Mustern und Konfigurationselementen zu erhalten. Sie können auch Berichte für herunterladen Oracle Datenbank, Middleware, Oracle Java-, VM- und vCenter-Hardwareinformationen.

Vorbereitungen

Erforderliche Rolle: admin oder glas_admin

Prozedur

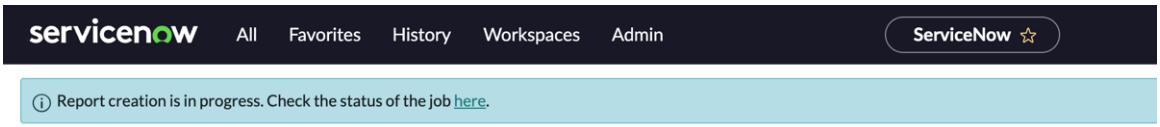
1. Navigieren zu **Alle** > **Oracle GLAS-Datensammlung** > **Laden Sie DIE GLAS-Datensammlung herunter**an.



2. Laden Sie die folgenden Berichte für herunter Oracle GLAS-Daten:
   - Zum Herunterladen Oracle Datenbank-, Middleware- und Java-Berichte, navigieren Sie zu **Schritt 1: Laden Sie die GLAS-Datensammlung herunter** Und wählen Sie Ihre Datensammlungsoptionen aus.
   - Um vCenter-Hardwareinformationen basierend auf dem Setup Ihrer Umgebung herunterzuladen, navigieren Sie zu **Schritt 2: Laden Sie vCenter-Hardwareinformationen herunter** .
   - Navigieren Sie zum Herunterladen von VM-Informationen zu **Schritt 3: VM-Informationen herunterladen** .
3. Wählen Sie das Download-Symbol ( ).
4. Geben Sie im Dialogfeld E-Mail-Adresse eingeben die E-Mail-Adresse ein, an die Sie eine Benachrichtigung erhalten möchten, wenn der Bericht bereit ist.
5. Wählen Sie **OK**.
   Nachdem die Statusmeldung für die Berichterstellung angezeigt wurde, können Sie den Status des Download-Auftrags überprüfen, indem Sie den in der Nachricht angegebenen Link auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Tabelle „Oracle GLAS Report Job Log“ [sn_itom_oracleglas_Job_log] wird in einem neuen Fenster geöffnet. Nachdem Ihr Bericht erfolgreich erstellt wurde, ändert sich der Status des Berichts in der Tabelle „Oracle GLAS-Berichtauftragsprotokolle“ in „Abgeschlossen“.

6. Wählen Sie einen Auftragsprotokolldatensatz aus, um seine Details anzuzeigen, einschließlich der eindeutigen Nummer, des Namens, der Beschreibung sowie des Datums und der Uhrzeit, zu der das Auftragsprotokoll erstellt und aktualisiert wird.
7. Laden Sie Ihren Bericht im Formular „Protokoll für Oracle GLAS-Berichtsauftrag“ herunter, indem Sie zu navigieren **Verwalten Sie Anhänge** Und auswählen **Herunterladen** .
   - Wenn Sie auswählen Oracle Datenbank, die folgenden CSV-Dateien werden heruntergeladen:
     - ORCL_V$SESSION.csv
     - ORCL_OPTIONS.csv
     - ORCL_DBA_USERS.csv
     - ORCL_DETAIL.csv
     - ORCL_V$LICENSE.csv
     - ORCL_OVERVIEW.csv
   - Wenn Sie auswählen Oracle Middleware, die folgenden Dateien werden in dem Format exportiert, das für den Servernamen und angezeigt wird Oracle Produkt installiert:
     - ORCL_OVERVIEW.csv
     - Collection-<Server Name>_<Oracle Product>.tar.bz mit den Dateien und Verzeichnissen des Formats FMW/u01/app/oracle/config/domains/soa_domain/config/config.xml.
   - Wenn Sie Oracle Java auswählen, werden die folgenden Ordner heruntergeladen:
     - Java-Ordner: Enthält Informationen zur Java-Installation
     - CPUQ-Ordner: Enthält CPUQ-Dateien, vCenter-Hardware- und VM-Informationen

   Hinweis: Sie können auch die CSV-Dateien für herunterladen Oracle Datenbank, indem Sie zu navigieren **Oracle GLAS-Datensammlung** > **Oracle GLAS-Daten**an. Wählen Sie in der Liste, die geöffnet wird, die Tabelle aus, die Sie herunterladen möchten, und wählen Sie dann aus **Laden Sie DEN GLAS-Bericht herunter** .

Ergebnis

Die heruntergeladenen Dateien werden an dem von Ihnen ausgewählten Speicherort angezeigt.

Trouble?

Wenn die Dateien leer sind oder eine Fehlermeldung enthalten, überprüfen Sie ihre Größe, um sicherzustellen, dass die in den folgenden Eigenschaften festgelegten Grenzwerte nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

überschritten wurden. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** Um die folgenden Eigenschaften zu finden.

Wichtig: Wenden Sie sich an ServiceNow Unterstützen Sie, bevor Sie diese Eigenschaften ändern.

Eigenschaft	Beschreibung
glide.discovery.file_tracking.max_file_size	Maximale Dateigröße für den Inhalt der verfolgten Konfigurationsdatei. Typ: Ganzzahl Standardwert: 500.000
glide.discovery.file_tracking.max_files_per_ci	Maximale Anzahl verfolgter Konfigurationsdateien pro CI. Typ: Ganzzahl Standardwert: 50
glide.discovery.file_tracking.change_limit_count	Anzahl der Änderungen, die für eine nachverfolgte Konfigurationsdatei im definierten Zeitfenster zulässig sind. Typ: Ganzzahl Standardwert: 4
glide.discovery.file_tracking.change_limit_days	Zeitfenster (in Tagen), das die Anzahl der Änderungen an einer verfolgten Konfigurationsdatei begrenzt. Typ: Ganzzahl Standardwert: 7

Wenn Sie einen Fehler erhalten Fehler: Sensor für horizontales Muster aufgrund eines Fehlers in der Nutzlast übersprungen: Nutzlastlänge 5056040 hat den Grenzwert von 300000 überschritten , Stellen Sie sicher, dass die Nutzlast das Systemlimit nicht überschritten hat. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** Um die folgenden Eigenschaften zu finden.

Eigenschaft	Beschreibung
mid.discovery.max_payload_size	Definiert die maximale Gesamt-Payload-Größe für den Payload von Ergebnissen, die aus Mustern stammen. Typ: Ganzzahl (Bytes) Standardwert: 300000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie einen SSH-Zeitüberschreitungsfehler erhalten, müssen Sie die folgenden Eigenschaften erstellen und festlegen. Siehe „MID-Server-Eigenschaft erstellen“ in MID-Server-Eigenschaften Für Details.

Eigenschaft	Beschreibung
mid.ssh.command_timeout_ms	Anzahl der Millisekunden, die ein SSH-Befehl vor einer Zeitüberschreitung ausgeführt werden darf (Standard ist konfigurierbar pro MID-Server). Typ: Ganzzahl
mid.sa.ssh.timeout	Die SSH-Zeitüberschreitung in Millisekunden. Typ: Ganzzahl
channel_timeout_ms	Der Zeitraum in Millisekunden, der von einem MID-Server während der Verarbeitung eines SSH-Befehls auf Aktivität gewartet wird. Wenn MID-Server Erkennt keine Aktivität innerhalb des angegebenen Fensters, beendet das System den Befehl. Typ: Ganzzahl

Oracle GoldenGate-Discovery

Die ServiceNow Discovery Und Service-Mapping Anwendungen finden Oracle Komponenten der GoldenGate-Version 12c, die verwenden Oracle Golden Gate Muster. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery verwendet das Muster Oracle Golden Gate, um eine horizontale Erkennung durchzuführen, um Daten in der Datei `$report_file` zu sammeln. Service-Mapping führt eine Erkennung von oben nach unten für die Datei `$report_file` durch, um ausgehende Oracle Golden Gate-Verbindungen zu finden.

Das Muster „Oracle Golden Gate“ unterstützt die folgenden Plattformen: AIX, Linux Hewlett Packard und Solaris.

Sie können dieses Muster auf der ServiceNow AI Platform mithilfe von Kingston, London oder Madrid verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die SSH-Anmeldeinformationen für das Betriebssystem des Servers, auf dem der Oracle Golden Gate-Server gehostet wird.

Benutzerzugriff

Erteilen Sie dem UNIX-Betriebssystembenutzer die Berechtigung zum Lesen der $report_file. Die $report_file ist die Berichtsdatei, die aus dem Prozess Oracle Golden Gate manager/replicat/extract-Prozess mit der Erweiterung .rpt extrahiert wird. Beispiel:

Konfigurationsdatei:

```
/base/ggs_beta/oracle/bt01pims/ggs/dirprm/mgr.prm REPORTFILE
```

Berichtsdatei:

```
/base/ggs_beta/oracle/bt01pims/ggs/dirrpt/MGR.rpt PROCESSID MGR
```

Berechtigungen zum Ausführen von Befehlen

Der Betriebssystembenutzer muss über Berechtigungen zum Ausführen der relevanten Betriebssystembefehle für jede unterstützte Plattform verfügen.

Geben Sie dem UNIX-Betriebssystembenutzer Berechtigungen, die folgenden Befehle gegen den Oracle Golden Gate-Server auszuführen:

Befehl	Obligatorisch/Optional	Beschreibung
$sudo + " ls -d " + $rpt_base_dir + "*.rpt | sort "	Obligatorisch	Listet alle Berichtsdateien im Oracle Golden Gate-Berichtsbasisverzeichnis auf
$sudo + " ls -d " + $prm_base_dir + "*.prm| sort "	Obligatorisch	Listet alle Parameterdateien im Oracle Golden Gate-Parameterbasisverzeichnis auf

Daten abrufen

Rufen Sie Daten ab, indem Sie folgende Elemente analysieren:

- Die Oracle Golden Gate Manager-Berichtsdatei (report_file) zum Abrufen zugehöriger Configuration Item-Namen (CI) und Zählerinformationen.
- Variablen in der Prozessbefehlszeile zum Abrufen des Installationsordners, des Manager-Prozessnamens, der Konfigurationsdatei und der Parameterdatei
- Variablen im Oracle Golden Gate-Installationsordner, um eine Liste von Parameter- und Konfigurationsdateien abzurufen

EVAL-Abschlussfunktionen

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um doppelte Einträge aus dem Extraktionsprozess und dem Replikationsprozess zu entfernen.

- var tableWithoutDuplicates = '';tableWithoutDuplicates = DuplicateRemover.removeDuplicates(${extracts}, ["name"]);CTX.setAttribute("extracts", tableWithoutDuplicates);
- var tableWithoutDuplicates = '';tableWithoutDuplicates = DuplicateRemover.removeDuplicates(${replicats}, ["name"]);CTX.setAttribute("replicats", tableWithoutDuplicates);

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um die Anzahl der Extraktionsprozesse und der Replikationsprozesse zu zählen.

```
return ${cmdb_ci_appl_ora_gg_replicat[*].config_file}.size()
return ${cmdb_ci_appl_ora_gg_extract[*].config_file}.size()
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um den privilegierten Befehl zurückzugeben.

```
return
 ${ctx}.getDiscoveryProvider(com.snc.sw.dto.ProviderType.SSH).getPrivilegedCom
mand();
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um den Erkennungstyp zurückzugeben.

```
ctx.getWork().getDiscoveryType();
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um die Version aus dem Installationsverzeichnispfad zu extrahieren, wenn sie leer ist.

```
inst_dir = ${install_directory}if(inst_dir.isEmpty()){return
 ${version}}if(inst_dir.startsWith('/')){return
 inst_dir.replaceAll('/.*/','')}if(!inst_dir.startsWith('/') && !inst_dir.isEmpty()){return
 inst_dir.replaceAll('.*\\\\','')}
```

Applicative-Anmeldeinformationen

1. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Applicative-Anmeldeinformationen**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Applicative-Anmeldeinformationen“

Feld	Beschreibung
Name	Name der Anmeldeinformationen Beispiel: oracle_db_user.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Anmeldeinformationen, die Sie auf **Alle MID Server** in Ihrem Netzwerk oder auf einen oder mehrere **Spezielle MID Server** anwenden oder nicht anwenden möchten. Wählen Sie **Spezielle MID Server** aus.
MID Servers	MID Server, für die die Anmeldeinformationen gelten. Wählen Sie den erforderlichen MID Server aus. Dieses Feld wird angezeigt, wenn Sie **Spezielle MID Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist **100**.
Benutzername	Name des Benutzers dieser Applicative-Anmeldeinformationen. Beispiel: oracle_db_user. Sie können einen beliebigen Benutzer für die Anmeldeinformationen für dieses Muster verwenden, da die Informationen aus einem lokalen Cache extrahiert werden.
Passwort	Nicht erforderlich. Sie können dieses Feld leer lassen oder einen beliebigen Wert eingeben.
CI-Typ	CI-Typ, für den diese Anmeldeinformationen verwendet wird: Speicherserver [cmdb_ci_storage_server] **Hinweis:** ServiceNow Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Konfigurationselemente (Configuration Items, CIs) umfassen.

5. Klicken Sie auf **Absenden**.

Eingabepunkt

Verwenden Sie für die Erkennung von oben nach unten die Oracle Golden Gate-IP-Adresse, und geben Sie den MID Server an.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery verwendet das Oracle Golden Gate-Muster zum Sammeln der in der folgenden Tabelle beschriebenen Daten.

Tabelle und Feld	Beschreibung
Haupt-CI cmdb_ci_appl_oracle_golden_gate	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Version [version]	Version der Installation von Oracle Golden Gate
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-Bezeichner (SID)
Anzahl der Replikate [count_replicat]	Zähler der Replikatprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden
Anzahl der Extrakte [count_extract]	Zähler der Extraktprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden.

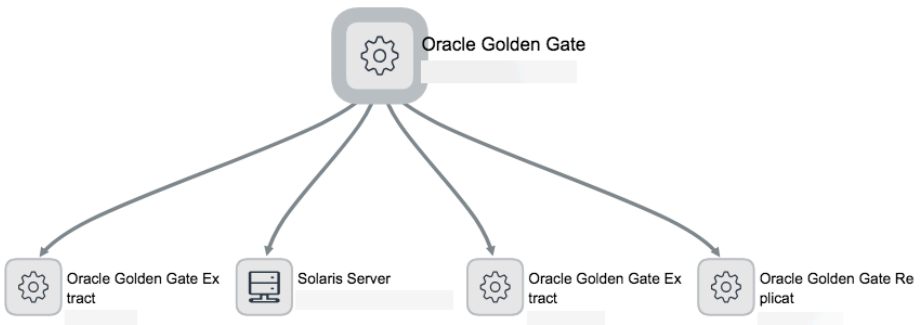
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Konfigurationsdatei [config_file]	Parameterdatei des Oracle Golden Gate-Prozesses. Geben Sie den Pfad zur Konfigurationsdatei und den Dateinamen an, <name>.prm.
Berichtsdatei [report_file]	Berichtsdatei des Oracle Golden Gate-Prozesses. Geben Sie den Pfad zur Berichtsdatei und den Dateinamen an, <name>.rpt.
Typ [type]	Typ der Oracle Golden Gate-Installation. Geben Sie Oracle Golden Gate für Oracle-Technologien an.
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Zugehöriges CI cmdb_ci_appl_ora_gg_replicat	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Berichtsdatei [report_file]	Replikat-Prozessberichtsdatei. Geben Sie den Pfad zur Berichtsdatei und den Dateinamen an, <name>.rpt.
Konfigurationsdatei [config_file]	Parameterdatei des Replikatsprozesses. Geben Sie den Pfad zur Konfigurationsdatei und den Dateinamen an, <name>.prm.
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Version [version]	Version der Installation von Oracle Golden Gate
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-SID
Betriebsstatus [operational_status]	Betriebsstatus des CI. Wählen Sie **Funktionsfähig** aus.
Zugehöriges CI cmdb_ci_appl_ora_gg_extract	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Berichtsdatei [report_file]	Berichtsdatei des Replikatprozesses
Konfigurationsdatei	Parameterdatei des Extraktprozesses

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
[config_file]	
Version [version]	Version der Installation von Oracle Golden Gate
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-SID
Betriebsstatus [operational_status]	Betriebsstatus des CI. Wählen Sie **Funktionsfähig** aus.

Die Dependency Views-Zuordnung zeigt die erkannten Lastenausgleichsmodul-CIs und deren Beziehung untereinander.



CI-Beziehungen

Diese Beziehungen sollen die Oracle Golden Gate-Erkennung unterstützen.

CI	Beziehung	CI
Haupt cmdb_ci_appl_oracle_golden_gate		
cmdb_ci_appl_oracle_golden_gate	Verwaltet::Verwaltet von	cmdb_ci_appl_ora_gg_replicat cmdb_ci_appl_ora_gg_extract
cmdb_ci_appl_oracle_golden_gate	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_oracle_golden_gate	Erstreckt sich von	cmdb_ci_appl
Zugehöriges CI cmdb_ci_appl_ora_gg_replicat		
cmdb_ci_appl_ora_gg_replicat	Verwaltet von::Verwaltet	cmdb_ci_appl_oracle_golden_gate

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_appl_ora_gg_replicat	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_ora_gg_replicat	Erstreckt sich von	cmdb_ci_appl
Zugehöriges CI cmdb_ci_appl_ora_gg_extract		
cmdb_ci_appl_ora_gg_extract	Verwaltet von::Verwaltet	cmdb_ci_appl_oracle_golden_gate
cmdb_ci_appl_ora_gg_extract	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_ora_gg_extract	Erstreckt sich von	cmdb_ci_appl

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Zum Erkennen des Oracle Golden Gate-Prozesses verwenden Sie den TCP-Einstiegspunkt mit dem richtigen Host und Port des Oracle Golden Gate-Prozesses.

Tabelle und Feld	Beschreibung
Haupt-CI cmdb_ci_appl_oracle_golden_gate	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Version [version]	Version der Installation von Oracle Golden Gate
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Konfigurationsdatei [config_file]	Parameterdatei des Oracle Golden Gate-Prozesses.
Berichtsdatei [report_file]	Berichtsdatei des Oracle Golden Gate-Replikatprozesses
Quelldatenbank [source_db]	Managerprozess-Quelldatenbanksystem-SID
Extraktprozesszähler [count_extract]	Zähler der Extraktprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden.
Replikatprozesszähler [count_replicat]	Zähler der Replikatprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Linux Virtualisierungsmanager und Red hat Virtualization Discovery

Die ServiceNow Discovery Anwendung verwendet Muster, um zu finden Oracle Linux Virtualisierungsmanager (OLVM) und Red hat Virtualization (RHV)-Komponenten. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Ab Version 1.28.0 Muster für Discovery und Service-Mapping Unterstützt sowohl OLVM als auch RHV-Discovery. Beachten Sie, dass die RHV-Muster, -Tabellen und zugehörigen Elemente in oVirt umbenannt wurden. Eine vollständige Liste der Namensänderungen finden Sie unter Zurich Release Release-Hinweise zur ITOM-Transparenz .

Discovery Verwendet die folgenden Muster für die OLVM- und RHV-Discovery:

- OVirt-Cluster und -Hosts
- OVirt – logische Rechenzentren erkennen
- OVirt Discover Manager-Instanz
- Virtuelle oVirt-Maschinen

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Stellen Sie bereit MID-Server

Stellen Sie das dedizierte bereit, und verbinden Sie es MID-Server Um entweder auf die OLVM- oder Red hat Virtualization Manager (RHV-M)-Instanzen zuzugreifen.

Erstellen Sie oVirt-Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

1. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Aus **OVirt-Anmeldeinformationen** , Füllen Sie das Formular aus, und wählen Sie dann aus **Übermitteln** .

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Anwendername	Name des Anwenders für die Durchführung dieser Discovery.
Passwort	Passwort für diesen Benutzer
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Discovery.
Bearer-Token	Option zum Aktivieren der Verwendung eines Bearer-Tokens.

Überprüfen Sie die API-Berechtigungen

Überprüfen Sie, ob der Anwender über schreibgeschützte Berechtigungen zum Senden der folgenden Abfragen verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- /ovirt-engine/api/
- /ovirt-engine/api/datacenters
- /ovirt-engine/api/clusters
- /ovirt-engine/api/hosts
- /ovirt-engine/api/vms

CMDB CI-Klassenmodelle hinzufügen

Fügen Sie Klassenmodelle hinzu, die erweitern CMDB Klassenhierarchie mit CMDB CI-Klassenmodelle Anwendung. Die App ist über verfügbar ServiceNow Store. Discovery Muster verwenden diese Klassenerweiterungen, um CIs auszufüllen. Weitere Informationen finden Sie unter Erweiterungsklassen für Red hat Virtualization (RHV) .

Cloud-Servicekonten erstellen

Erstellen Sie einen OLVM- oder RHV-Cloud-Service-Account auf der ServiceNow Instanz.

Hinweis: Bestätigen Sie das Discovery-Administratorarbeitsbereich Verwendet mindestens Version 1.10.0. Die **Discovery** > **Cloud-Service-Accounts** Das Navigationsmodul ist mit früheren Versionen nicht verfügbar. Um auf zuzugreifen **Cloud-Service-Accounts** Geben Sie bei einer früheren Version im Navigationsfilter Folgendes ein: cmdb_ci_Cloud_Service_Account.list .

1. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger Name für den Service-Account.
Konto-ID	Konto-ID, zu der diese Anmeldeinformationen gehören. Die API-url der Instanz muss angegeben werden, einschließlich des Ports. Beispiel: https://my-manager-instance.com:443 .
Discovery-Anmeldeinformationen	Die Erkennung-Anmeldeinformationen, die zuvor erstellt wurden
Datencenter-Typ	Der Rechenzentrumstyp, der oVirt LDC [cmdb_ci_rhv_ldc] sein muss.

Erkennungszeitpläne erstellen

Erstellen Sie einen Discovery-Zeitplan, um eine vollständige Discovery von OLVM- oder RHV-Komponenten durchzuführen.

1. Öffnen Sie den zuvor erstellten Cloud-Service-Account.
2. Unter **Zugehörige Links** , Wählen Sie aus **Erstellen Sie Einen Discovery-Zeitplan** .

   Unter dem Menüelement **Discovery-Zeitplan** wird ein neuer Zeitplan erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen der Muster.

OVirt LDC [cmdb_ci_rhv_ldc]

Feld	Beschreibung
Name [name]	Name des Rechenzentrums
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Beschreibung [short_description]	Beschreibung des Rechenzentrums, das Sie zur einfachen Identifizierung bereitstellen.
Kontingentmodus [Kontingent_Mode]	Kontingentmodusrichtlinie
URL [url]	API-URL für den Zugriff auf das Rechenzentrum.
Href-ID [href_ID]	Href-ID

OVirt-Cluster [cmdb_ci_rhv_Cluster]

Feld	Beschreibung
Name [name]	Name des Clusters.
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Beschreibung [short_description]	Beschreibung des Clusters, den Sie zur einfachen Identifizierung bereitstellen.
CPU-Typ [cpu_type]	CPU-Typ Beispiel: x86_64
CPU-Architektur [cpu_Architecture]	CPU-Architektur. Beispiel: Intel Broadwell IBRS SSBD MDS Family
KSM [ksm]	Aktivierungsstatus der Kernel-Richtlinie für das Zusammenführen derselben Seite (Kernel Same-Page Merging, KSM).
Fencing-Richtlinie [Fencing_Policy]	Fencing-Richtlinie
Arbeitsspeicher-Overcommit [Memory_overcommit]	Menge des im Cluster zulässigen Speichers mit Mehrfachvergabe
Transparente riesige Seiten [thp]	Richtlinie für transparente Seiten mit großem Arbeitsspeicher
Ballooning [Ballooning]	Arbeitsspeicher-Ballooning für Gäste
Kompatibilitätsversion [compatibility_Version]	Kompatibilitätsversion
URL [url]	API-URL für den Zugriff auf das Cluster
Href-ID [href_ID]	Href-ID

OVirt-Server [cmdb_ci_rhv_Server]

Feld	Beschreibung
Name [name]	Name des Servers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OVirt-Server [cmdb_ci_rhv_Server] (Fortsetzung)

Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Anzahl der CPU-Kerne [cpu_Core_count]	Gesamtzahl der Kerne
CPU-Anzahl [cpu_count]	Gesamtzahl der CPUs.
CPU-Typ [cpu_type]	CPU-Typ
CPU-Geschwindigkeit (MHz) [cpu_Speed]	CPU-Geschwindigkeit (MHz)
Hostname [host_name]	Hostname
IP-Adresse [ip_address]	IP-Adresse des Servers.
Modell-ID [model_id]	Modell-ID
Betriebssystem [os]	Betriebssystemfamilie
BS-Version [os_Version]	Version des Betriebssystems.
RAM (MB) [RAM]	Menge des Arbeitsspeichers (MB)
URL [url]	Verwendete API-URL, die für den Zugriff auf den Server verwendet wird

OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]

Feld	Beschreibung
Name [name]	Name der Instanz.
Status [state]	Status der Instanz.
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
IP-Adresse [ip_address]	IP-Adresse der Instanz.
Datenträger [Datenträger]	Anzahl der Datenträger
MAC-Adresse [mac_address]	MAC-Adresse der Instanz.
Verwaltungs-URL [mgmt_url]	Verwaltungs-API-URL
Beschreibung [short_description]	Beschreibung der Instanz, die Sie zur einfachen Identifizierung bereitstellen.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (Fully Qualified Domain Name, FQDN) der Instanz.
CPU-Architektur [cpu_Architecture]	CPU-Architektur. Beispiel: Intel Broadwell IBRS SSBD MDS-Familie.
Geschützt löschen [delete_protected]	Löschen Sie geschützte, mögliche Werte: Wahr oder falsch.
CPUs [cpus]	Anzahl an CPUs
HA-Priorität [ha_Priority]	Hochverfügbarkeits-Priorität (HA).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance] (Fortsetzung)

Feld	Beschreibung
Hochverfügbarkeit [High_Availability]	Hohe Verfügbarkeit, mögliche Werte: Wahr oder falsch.
Arbeitsspeicher MAX [Memory_Policy_max]	Maximaler Arbeitsspeicher in der dynamischen Arbeitsspeicherzuteilungsrichtlinie für die virtuelle Maschine (VM).
Arbeitsspeichergarantie (MB) [Memory_Policy_garantierte]	Garantierter Arbeitsspeicher für die VM (MB)
Mehrere Warteschlangen [Multi_Queues]	Mehrere Warteschlangen
Platzierungsrichtlinie [Placement_Policy]	Platzierungsrichtlinie
Statuslos [statuslos]	Statuslos, mögliche Werte: Wahr oder falsch.
Fehler bei Speicher [Storage_error_RESUME_Behaviour]	Verhalten einer VM, die aufgrund eines Speicher-E/A-Fehlers angehalten wird. Beispiel: AUTO_RESUME, LEAVE_PAUSED und KILL.
Startzeit [Start_time]	Startzeit der VM.
Endzeit [stop_time]	Endzeit der VM.
Threads [Threads]	Anzahl der Threads
Zeitzone [time_Zone]	Zeitzone der VM.
USB [usb]	USB-aktivierter Status
Einmal ausführen [Run_once]	Einmal ausführen
RHV-Typ [rhv_type]	OLVM- oder RHV-Typ.

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [Account_ID]	Konto-ID für dieses Cloud-Servicekonto
Objekt-ID [object_id]	Konto-ID für dieses Cloud-Servicekonto
Rechenzentrumstyp [datacenter_type]	Typ des Rechenzentrums: OVirt LDC [cmdb_ci_rhv_ldc].
Discovery-Anmeldeinformationen [Discovery_credentials]	Anmeldeinformationen für dieses Cloud-Servicekonto

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
Name [name]	Die IP-Adresse der Netzwerkschnittstellenkarte (NIC), die der VM zugewiesen ist.
IP-Adresse [ip_address]	Die IP-Adresse der NIC, die der VM zugewiesen ist.
IP-Version [ip_Version]	IP-Version: IPv4 oder IPv6.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VNIC-Endpunkt [cmdb_ci_endpoint_vnic]

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner für diese Ressource
Name [name]	Name für den Endpunkt der virtuellen Netzwerkschnittstellenkarte (vNIC).
IP-Adresse [ip_address]	IP-Adresse, die an die Netzwerkschnittstelle gebunden ist.

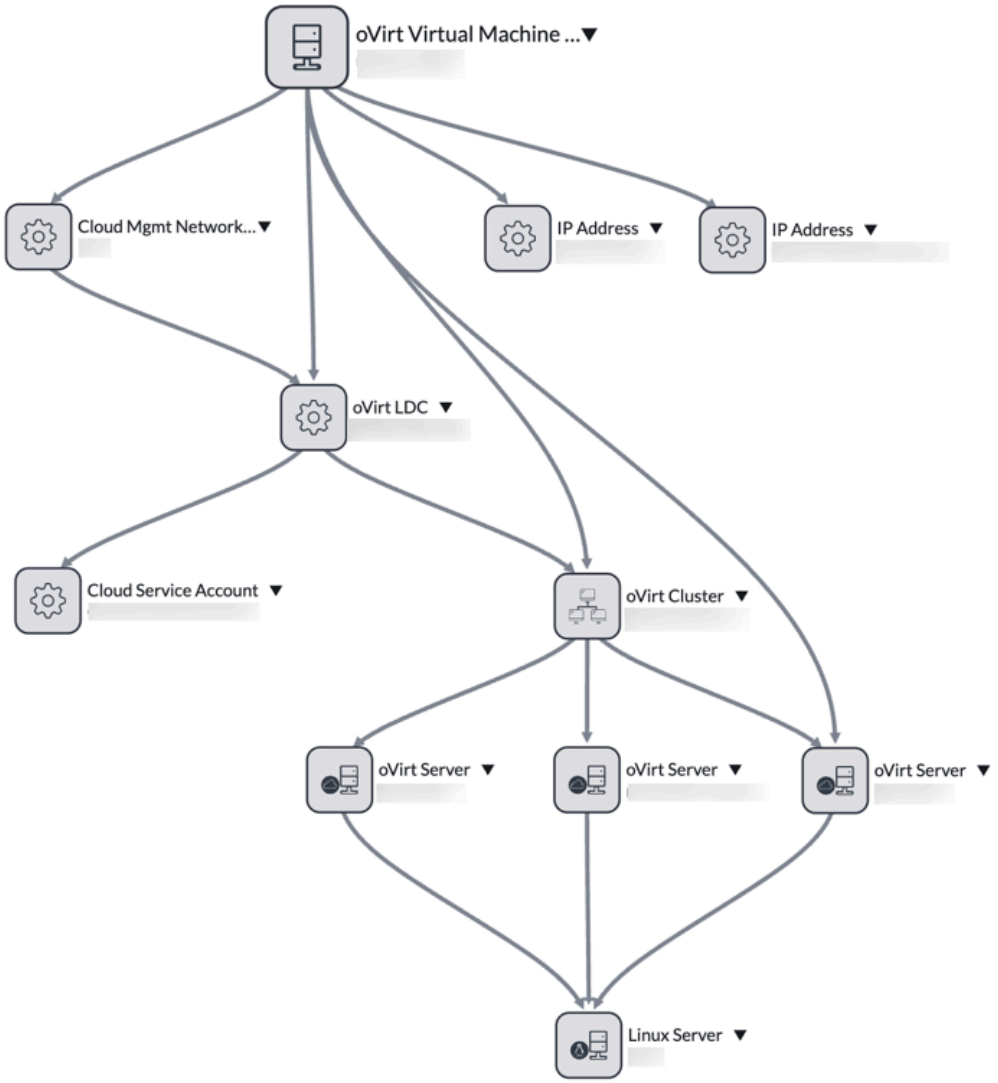
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Objekt-ID [object_id]	ID der Netzwerkschnittstelle.
Name [name]	Name der Netzwerkschnittstelle.
IP-Adresse [ip_address]	IP-Adresse, die an die Netzwerkschnittstelle gebunden ist.
Öffentliche IP [public_ip]	Öffentliche IP-Adresse, die an die Netzwerkschnittstelle gebunden ist.
Private IP [private_ip]	Private IP-Adresse, die an die Netzwerkschnittstelle gebunden ist.

In der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten OLVM- oder RHV-Ressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OLVM- oder RHV-Abhängigkeitsansicht



CI-Beziehungen

Die folgenden Beziehungen werden erstellt, um die OLVM- oder RHV-Discovery zu unterstützen.

CI	Beziehung	CI
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Gehostet auf::Hostet	OVirt LDC [cmdb_ci_rhv_ldc]
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Erstreckt sich von	Netzwerkadapter [cmdb_ci_network_adapter]
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
IP-Adresse [cmdb_ci_ip_address]	Erstreckt sich von	Konfigurationselement [cmdb_ci]
OVirt-Cluster [cmdb_ci_rhv_Cluster]	Mitglieder::Mitglied von	OVirt-Server [cmdb_ci_rhv_Server]
OVirt-Cluster [cmdb_ci_rhv_Cluster]	Erstreckt sich von	OVirt-Objekt [cmdb_ci_rhv_object]
OVirt LDC [cmdb_ci_rhv_ldc]	Enthält::Enthalten in	OVirt-Cluster [cmdb_ci_rhv_Cluster]
OVirt LDC [cmdb_ci_rhv_ldc]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
OVirt LDC [cmdb_ci_rhv_ldc]	Erstreckt sich von	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
OVirt-Server [cmdb_ci_rhv_Server]	Wird ausgeführt auf::Wird ausgeführt	Linux-Server [cmdb_ci_linux_server]
OVirt-Server [cmdb_ci_rhv_Server]	Erstreckt sich von	Virtualisierungsserver [cmdb_ci_virtualization_server]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Gehostet auf::Hostet	OVirt-Cluster [cmdb_ci_rhv_Cluster]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Gehostet auf::Hostet	OVirt LDC [cmdb_ci_rhv_ldc]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Registriert am::Registriert	OVirt-Server [cmdb_ci_rhv_Server]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
OVirt-VM-Instanz [cmdb_ci_rhv_vm_instance]	Erstreckt sich von	VM-Instanz [cmdb_ci_vm_instance]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Endpunkt implementieren in::Endpunkt implementieren von	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Erstreckt sich von	Endpunkt [cmdb_ci_Endpoint]

Oracle Listener-HD-Discovery

ServiceNow Discovery Verwendet Oracle Listener-HD-Muster, das gesucht und zugeordnet werden soll Oracle Echte Anwendungscluster-Komponenten. Um diese Ressourcen zu erkennen, installieren Sie CMDB CI-Klassenmodelle Und Muster für Discovery und Service-Mapping Von ServiceNow Speichern.

Oracle Mit RAC können Sie ein Cluster erstellen Oracle Datenbank. Oracle RAC verwendet Oracle Clusterware für die Infrastruktur, um mehrere Server zu binden, damit sie als ein einzelnes System funktionieren. Oracle Mit Clusterware können Sie einen geclusterten Speicherpool erstellen, der von einer beliebigen Kombination aus nicht-Cluster und verwendet werden kann Oracle RAC-Datenbanken. Discovery Verwendet Oracle Listener-HD-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster, um Informationen zu erkennen Oracle Datenbank-Listener und die Komponenten in Oracle RAC-Infrastruktur, wenn ein solches Setup konfiguriert ist.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass die folgenden Plugins installiert sind:
  - CMDB CI-Klassenmodelle Plugin (Version 1.29.0 oder höher).
  - Muster für Discovery und Service-Mapping Plugin (Version 1.0.82 oder höher).
- Stellen Sie sicher, dass Discovery Anwender befindet sich in Oracle DBA-Gruppe oder hat die richtigen Berechtigungen.
- Stellen Sie sicher, dass MID-Server Hat Zugriff auf das Zielgerät.
- Stellen Sie sicher, dass Oracle Clusterware/Grid-Infrastruktur ist installiert und die Oracle RAC-Datenbank ist konfiguriert. Wenn vorhanden ist Oracle Clusterware-Setup.
- Stellen Sie sicher, dass Oracle Listener-Prozess wird auf einem UNIX-BS-Host ausgeführt.
- Verwenden Oracle Clusterware-Mindestversion 12.2.X.X (Oracle Database 12c Release 2) oder höher, wenn vorhanden Oracle Clusterware-Setup.

  Hinweis: Dieses Muster wird von unterstützt Paris Release am. Mehr UNIX BS-Typen (AIX, Solaris, HP-UX) Werden ab Version 1.0.87 von unterstützt Muster für Discovery und Service-Mapping Plugins.

  Die folgenden Befehle werden während der Musterausführung ausgeführt. Durch die Ausführung der Befehle kann das Muster alle relevanten CMDB-Klassen mit den erforderlichen Informationen ausfüllen:

  - **Export TNS_ADMIN=<oracle_home_directory>/Network/admin** : Legt ORACLE_HOME auf die Umgebungsvariable TNS_ADMIN fest.
  - **ORACLE_BASE==<oracle_home_directory> exportieren** : Legt ORACLE_HOME auf die Umgebungsvariable ORACLE_BASE fest.
  - **Lsnrctl-Status LISTENER_NAME** : Überprüft den Status des Datenbank-Listeners.
  - **ps – ef | grep „d.bin“** : Sucht nach dem GRID_HOME-Pfad.
  - **Crsctl-Abfrage-Cluster-Site -Alle** : Listet die Knoten und Datenträger auf, die die Sites enthalten.
  - **LISTENER_NAME der lsnrctl-Services** : Listet die Services auf, die der Listener identifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

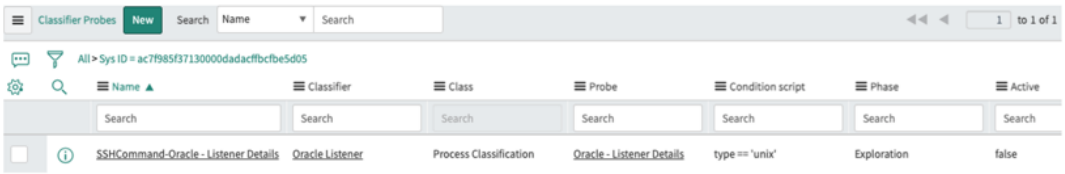
- **Crsctl stat res -f -W „((TYPE = ora.database.TYPE))“** : Listet den Datenbanknamen, den zugehörigen Knoten, den Typ und den aktiven Status auf.

  Hinweis: Wenn von **lsnrctl status LISTENER_NAME** keine Ausgabe abgerufen wird, wird das Muster **Oracle Listener HD** beendet.

Einschränkungen

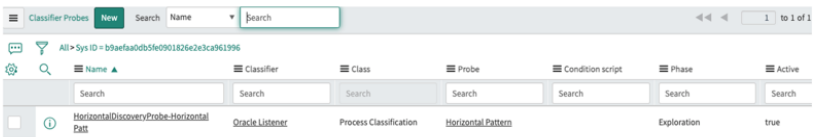
Das Oracle Clusterware-Setup wird nur für UNIX-Betriebssysteme unterstützt. Das Basissystem **SSH-Befehl – Oracle – Klassifiziererprobe für Listener-Details** Ist inaktiv (aktiv ist auf falsch festgelegt), wenn CMDB CI-Klassenmodelle Version 1.29.0 oder höher installiert werden.

Klassifizierungsprobes: Oracle-Listener-Details



Die **Oracle Listener-Prozessklassifizierung** löst das Muster „Oracle Listener HD“ aus.

Klassifizierungsprobes: Horizontales Muster



Von Discovery während der horizontalen Erkennung erfasste Daten

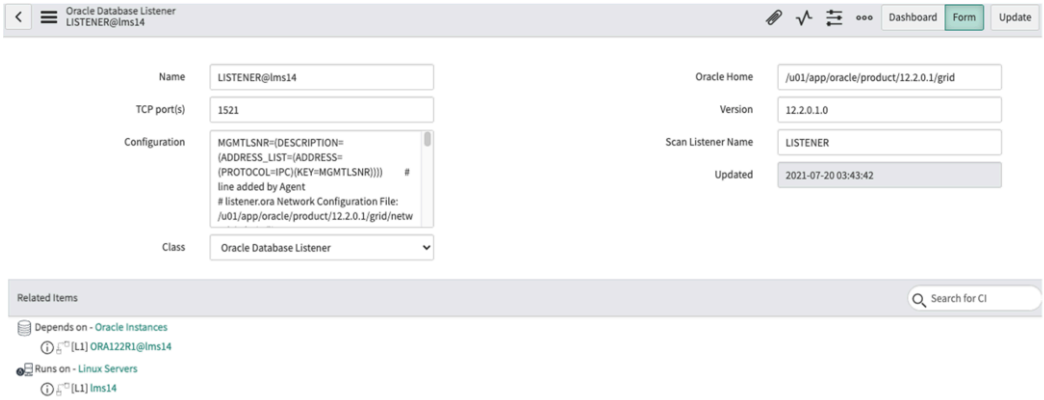
Das Muster „Oracle Listener HD“ füllt die folgenden CIs aus:

Haupt-CI (Oracle Database Listener) [cmdb_ci_db_ora_listener]

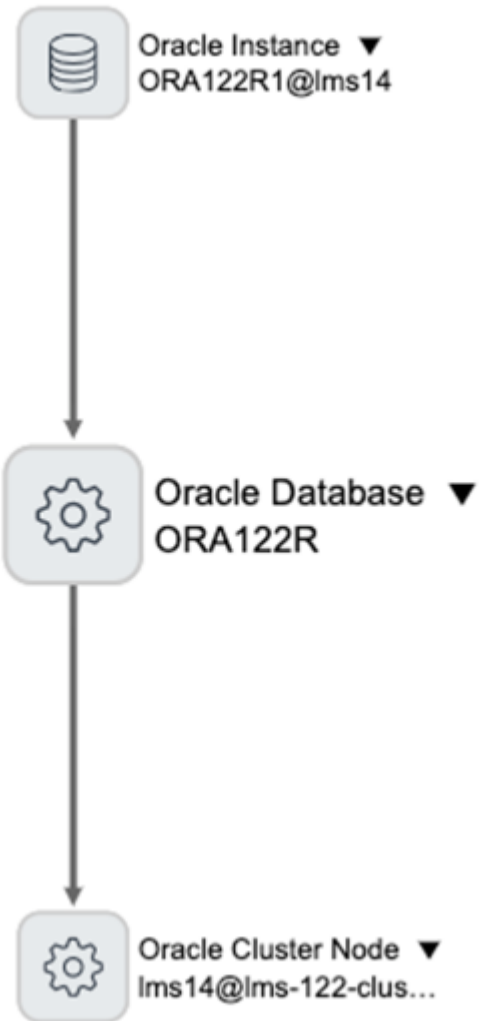
Feld	Beschreibung
name	Der Name des Oracle-Datenbanklisteners.
oracle_home	Das Oracle-Stammverzeichnis, in dem die Software installiert ist.
konfigurieren	Die Netzwerkkonfigurationsdatei listener.ora.
scan_listener_name	Der Name des SCAN LISTENER.
Version	Version des Oracle-Produkts.
tcp_port	Der Überwachungsport für Oracle-Client-Verbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Oracle-Datenbanklistener“



Oracle-Datenbanklistener-Ansichtszuordnung



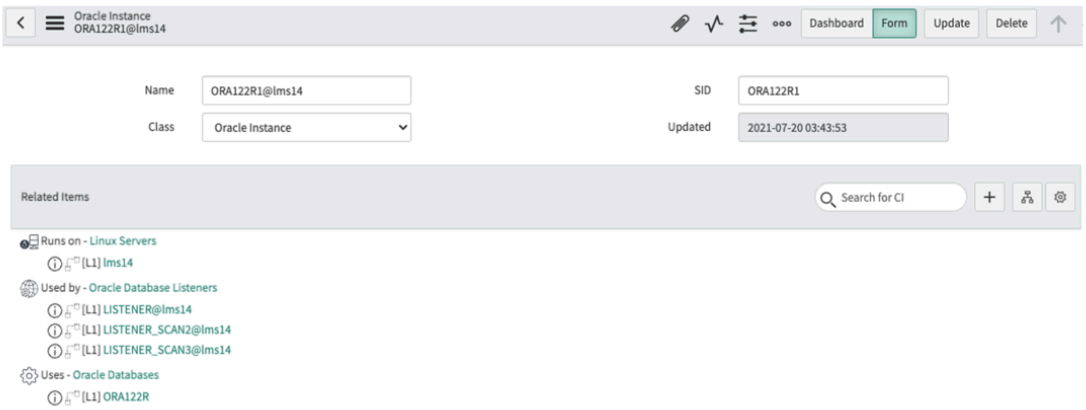
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

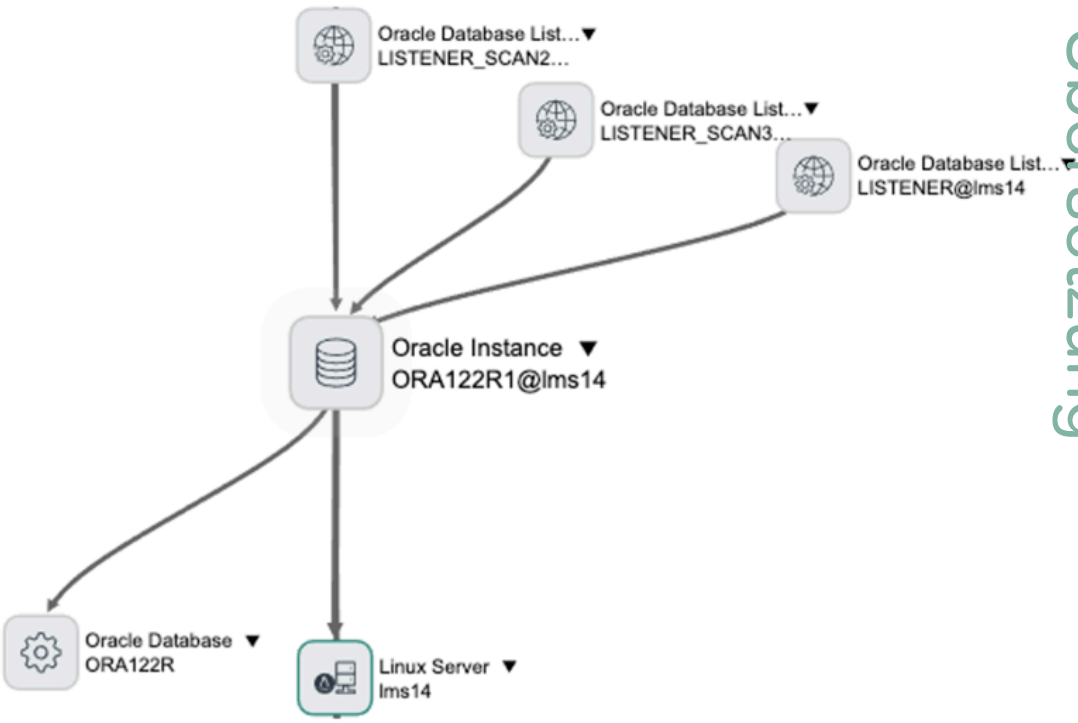
(Oracle-Instanz) cmdb_ci_db_ora_instance

Feld	Beschreibung
sid	Der spezifische Name, der die Instanz speziell identifiziert.
name	Der Name der Oracle-Instanzkombination von SID@HOST_NAME.

Formular „Oracle-Instanz“



Oracle-Instanz-Ansichtszuordnung



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

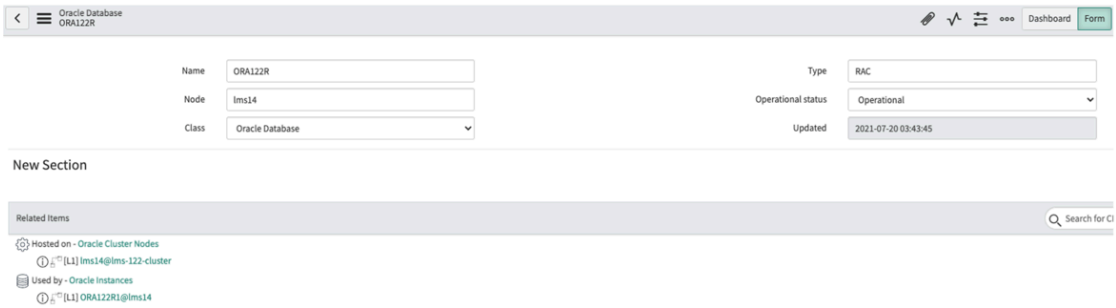
(Oracle-Datenbank) cmdb_ci_oracle_database

Feld	Beschreibung
name	Der eindeutige Name der Oracle-Datenbank.
Typ	Typ der Oracle-Datenbank
operational_status	Der aktive Status der Oracle-Datenbank.
Knoten	Der Hostname des Knotens, der die Oracle-Datenbank hostet.

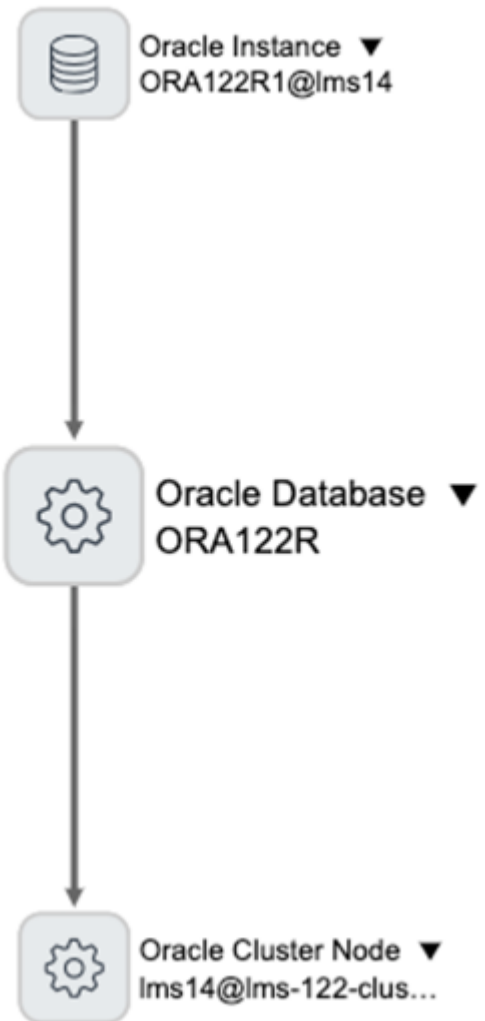
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Oracle-Datenbank“



Oracle-Datenbank-Ansichtszuordnung



(Oracle-Cluster) cmdb_ci_oracle_cluster

Feld	Beschreibung
name	Der Name des Oracle-Datenbankclusters.
cluster_id	Die GUID des Oracle-Datenbankclusters.
cluster_status	Der aktive Status des Oracle-Datenbankclusters.

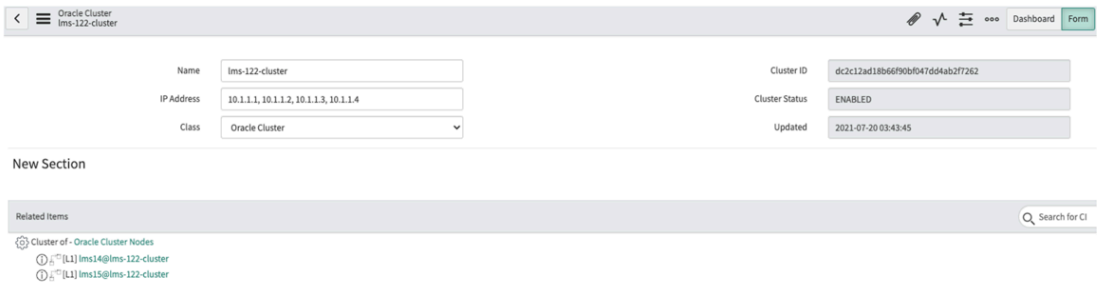
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

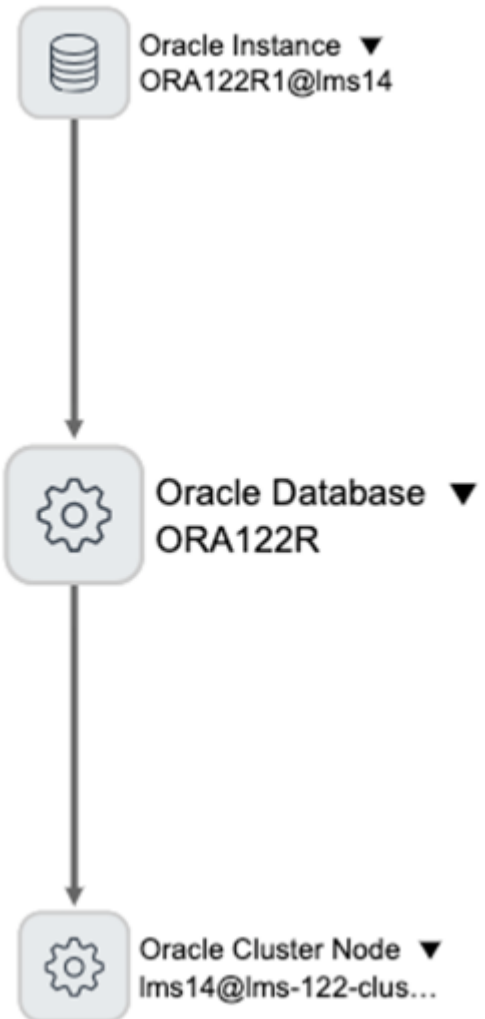
(Oracle-Cluster) cmdb_ci_oracle_cluster (Fortsetzung)

Feld	Beschreibung
ip_address	Die IP-Adressen der am Cluster teilnehmenden Knoten.

Formular „Oracle-Cluster“



Oracle-Cluster-Ansichtszuordnung



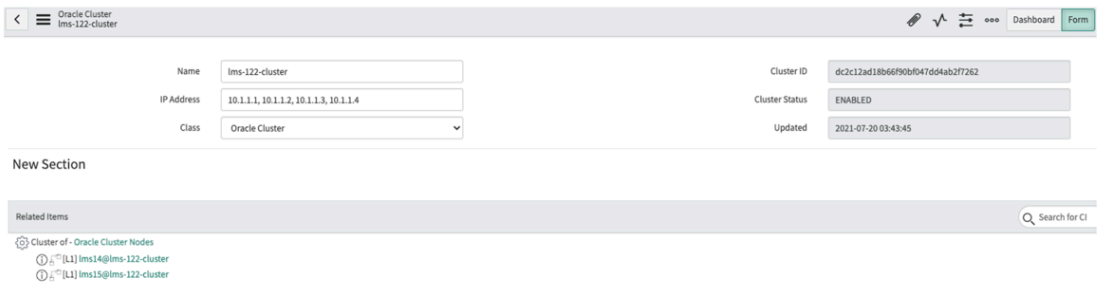
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Oracle-Clusterknoten) cmdb _ci_oracle_ cluster_node

Feld	Beschreibung
name	Der Hostname der Clusterknotenkombination HOSTNAME@CLUSTER_NAME.
ip_address	Die IP-Adresse des Clusterknotens, sofern durch DNS auflösbar.
Server	Der Hostname des Hosts, auf dem der Clusterknoten gehostet wird.
Cluster	Der Name des Clusters, dem der Clusterknoten zugewiesen ist.

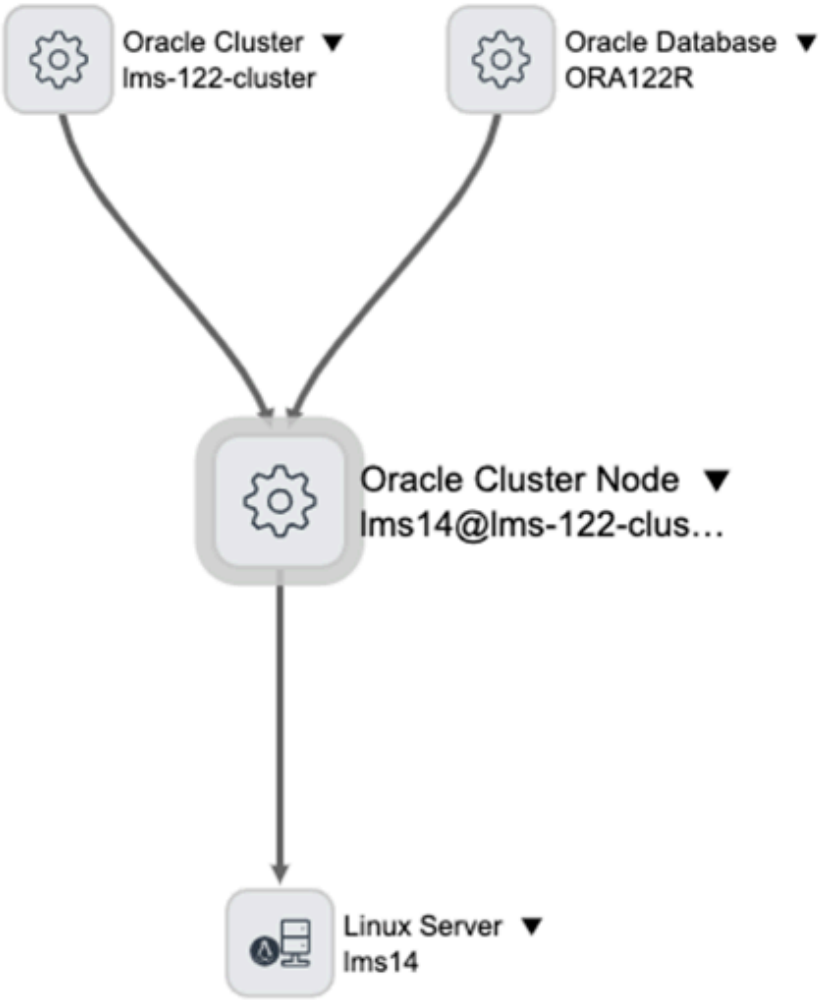
Formular „Oracle-Clusterknoten“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle-Clusterknoten-Ansichtszuordnung



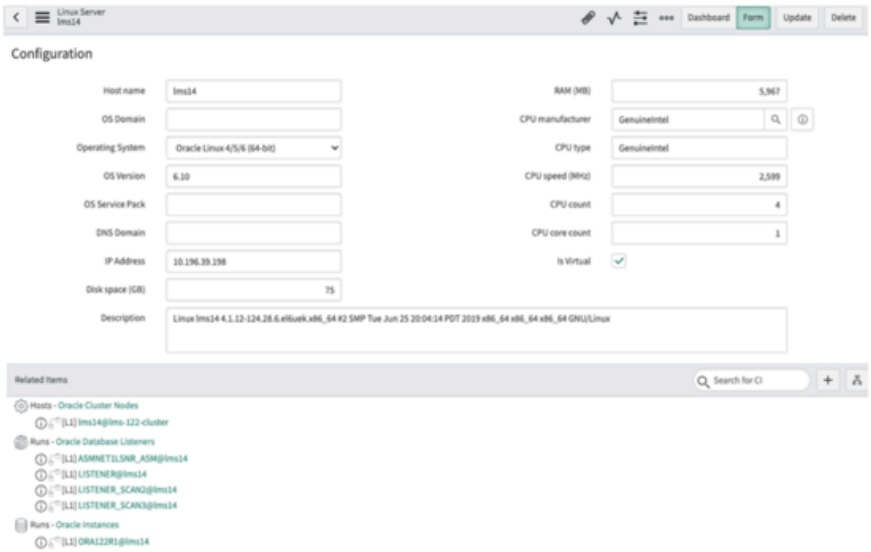
(Linux-Server) cmdb_ci_linux_server

Feld	Beschreibung
name	Der Hostname des Linux-Servers, auf dem der Oracle Listener-Prozess gehostet wird.

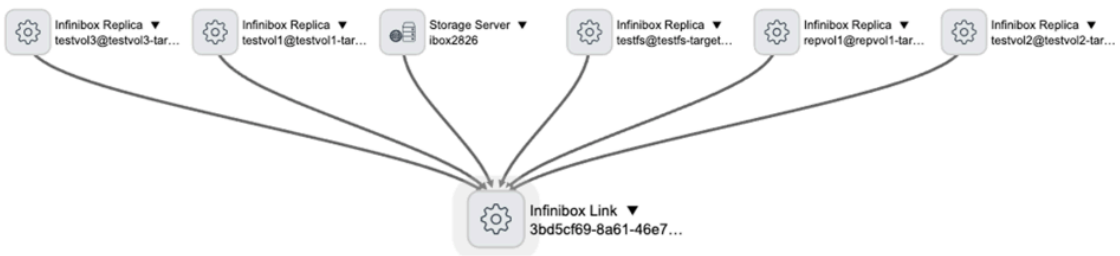
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Linux-Server“



Linux-Server-Ansichtszuordnung



(AIX-Server) cmdb_ci_aix_server

Feld	Beschreibung
name	Der Hostname des AIX-Servers, auf dem der Oracle Listener-Prozess gehostet wird.

(HPUX-Server) cmdb_ci_hpux_Server

Feld	Beschreibung
name	Der Hostname von HP-UX Server, der den Oracle Listener-Prozess hostet.

(Solaris-Server) cmdb_ci_solaris_server

Feld	Beschreibung
name	Der Hostname des Solaris-Servers, der den Oracle Listener-Prozess hostet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle DB-Service (cmdb_ci_DB_ora_Service)

Feld	Beschreibung
name	Der Name des Services
tcp_port	Der Port des Service.
Listener_Name	Der Name des Listeners, der den Service verwaltet.
Version	Die Version des Service.

CI-Beziehungen

Vom Oracle Listener HD-Muster erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_oracle_cluster	„Cluster of :: Cluster“	cmdb_ci_oracle_cluster_node
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_linux_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_linux_server
cmdb_ci_db_ora_listener	„Depends on :: Used by“	cmdb_ci_db_ora_instance
cmdb_ci_db_ora_instance	Verwendet::Verwendet von	cmdb_ci_db_oracle_database
cmdb_ci_oracle_database	„Hosted on :: Hosts“	cmdb_ci_oracle_cluster_node
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_aix_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_aix_server
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_solaris_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_solaris_server
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_hpux_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_hpux_server
cmdb_ci_DB_ora_Service	Verwaltet von::Verwaltet	cmdb_ci_db_ora_listener
cmdb_ci_db_ora_instance	Verwendet::Verwendet von	cmdb_ci_DB_ora_Service

Erkennung von Oracle Solaris LDOM

Discovery verwendet das Muster für die LDOM-Infrastruktur (Solaris Logical Domain) und das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek, um alle LDOM-Daten zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery verwendet diese Muster zum Ausführen einer horizontalen Erkennung: Sie können die Muster auf der ServiceNow AI Platform mit Release Zurich oder höher verwenden.

Das Muster für die Solaris LDOM-Infrastruktur wird bei der Solaris-Servererkennung automatisch ausgelöst. Das Muster überprüft, ob ein LDOM-Controller vorhanden ist, und stoppt die Ausführung, wenn kein Controller gefunden wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek wird als Erweiterungsabschnitt zum Solaris-Servermuster ausgeführt. Das Muster ändert die Seriennummer (SN) auf LDOM-Computern, sodass sie mit der SN übereinstimmt, die vom Muster für die Solaris LDOM-Infrastruktur gefüllt wird. Weitere Informationen zum Solaris-Server finden Sie unter Solaris-Erkennung.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

LDOM-Befehle beim Ausführen des Musters für die Solaris LDOM-Infrastruktur

Stellen Sie sicher, dass die relevanten Benutzer berechtigt sind, die folgenden benötigten Befehle für das Muster für die Solaris LDOM-Infrastruktur auszuführen:

- *"sudo /usr/sbin/virtinfo -a"*
- *"sudo /usr/sbin/ldm -V"*
- *"hostname"*
- *"svcs ldmd"*
- *"sudo /usr/sbin/ldm list-rsrc-group -a"*
- *"sudo /usr/sbin/sneep -T | grep ChassisSerialNumber 2> /dev/null"*
- *"/usr/sbin/prtdiag -v | awk '/Chassis Serial/{getline; getline; print}'"*
- *"sudo /usr/sbin/ldm list"*

Hinweis: Einige dieser Befehle werden mit Bedingungen verwendet und nicht bei jeder Erkennung ausgeführt. Beispielsweise können Sie die SN für Server in der Regel mit dem Befehl *sneep* abrufen. Dieser ist jedoch auf Solaris-Servern standardmäßig nicht verfügbar, daher wird *prtdiag* als alternative Methode zum Abrufen der SN verwendet.

Wichtige LDOM-Befehle beim Ausführen des Musters für die gemeinsam genutzte Solaris LDOM-Bibliothek

Stellen Sie sicher, dass die relevanten Benutzer berechtigt sind, die folgenden benötigten Befehle für das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek auszuführen:

- *"sudo /usr/sbin/virtinfo -a"*
- *"sudo /usr/sbin/sneep -T | grep ChassisSerialNumber 2> /dev/null"*
- *"hostname"*

Stellen Sie sicher, dass die relevanten Benutzer über die Berechtigungen zum Ausführen des LDOM-Befehls *virtinfo* verfügen. Dieser Befehl stellt sicher, dass die richtige LDOM-Rolle eingerichtet werden kann.

Stellen Sie sicher, dass die relevanten Benutzer über die Berechtigungen zum Ausführen des LDOM-Befehls *"sudo /usr/sbin/ldm list"* verfügen, um Gast-VMs auf dem LDOM-Controller aufzulisten. Dies ist erforderlich, um Beziehungen zwischen dem LDOM-Controller und den LDOM-Gast-VMs festzulegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einer der Seriennummernbefehle `sneep` oder `prtdiag` muss eine korrekte Antwort zurückgeben, um die SN korrekt festzulegen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die von beiden Mustern erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Solaris-Server [cmdb_ci_solaris_server]	
ldom_version	Auf dem LDOM-Controller installierte LDOM-Version
ldom_role	LDOM-Rolle; „Controller“ oder „Gast“
ldom_state	Status der LDOM-Implementierung auf dem LDOM-Controller
serial_number	Seriennummer des Computers
virtual	Gibt an, ob für den LDOM-Controller ein virtueller Computer (für Gast-VMs) verwendet wird oder nicht
ram	Auf dem LDOM-Controller verfügbarer Arbeitsspeicher
cpu_core_count	Anzahl der CPU-Kerne auf dem LDOM-Controller

CI-Beziehungen

CI	Beziehung	CI
LDOM-Controller	Gehostet auf::Hostet	LDOM-Gast-VM

Palo Alto Networks-Firewall-Erkennung

Die ServiceNow Discovery Die Anwendung verwendet das Palo Alto-Firewall-Muster der nächsten Generation, um zu finden Palo Alto Networks Firewalls. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Palo Alto Networks-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .
- Fügen Sie der ServiceNow-Instanz den OID-Datensatz des SNMP-Systems für das Palo Alto Networks-Gerät hinzu. Aktualisieren Sie Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klassifizierung: Palo-Alto-Firewall
- Klasse: Palo-Alto-Firewall-Gerät

- Stellen Sie das Muster wie folgt bereit:
  1. Herunterladen und installieren Firewall-Erweiterungsklassen Von ServiceNow Store. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind.
  2. Laden Sie das Erkennungsmuster aus dem ServiceNow Store herunter, und installieren Sie es.
  3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Palo Alto-Firewall-Musters der nächsten Generation.

Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Palo Alto-Geräts.
Seriennummer [serial_number]	Seriennummer des Palo Alto-Geräts.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (FQDN) des Palo Alto-Geräts.
Hersteller [manufacturer]	Palo Alto-Gerätehersteller.
Modell-ID [model_id]	Modell-ID des Palo Alto-Geräts.
Betriebsstatus [operational_status]	Gibt an, ob sich das Palo Alto-Gerät im Status „aktiv“ befindet.
Hardware-BS [Hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Beschreibung [short_description]	Kurzbeschreibung des Palo Alto-Geräts.
Firmware-Version [Firmware-Version]	Firmware-Version des Palo Alto-Geräts.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Alias [alias]	Der vom Anwender zugewiesene Name für den Netzwerkadapter.
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Konfigurationselement [cmdb_ci]	Verweist auf die Tabelle „Palo Alto-Firewall-Gerät“ [cmdb_ci_Firewall_device_palo_alto].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse der Palo Alto-Firewall.
Netzmaske [netmask]	Netzmaske der Palo Alto-Firewall.
NIC [nic]	Verweist auf die Tabelle „Netzwerkadapter“ [cmdb_ci_Network_Adapter].

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	DNS-Name (Domain Name System) des Palo Alto-Firewall-Geräts.
IP-Adresse [ip_address]	Host-IP-Adresse.

CI-Beziehungen

Diese Beziehungen sollen die Palo Alto Networks-Firewall-Erkennung unterstützen:

CI	Beziehung	CI
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_Network_Adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_Network_Adapter]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Erstreckt sich von	Firewall-Gerät [cmdb_ci_firewall_device]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_Network_Adapter]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
Routerschnittstelle [dscy_router_interface]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]
Seriennummer [cmdb_serial_number]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]

Erkennung von Pivotal Cloud Foundry

Die ServiceNow Discovery Anwendungsfunde Pivotal Cloud Foundry(PCF) Komponenten der Version 3, die verwenden Pivotal Cloud Foundry Muster. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können dieses Muster für verwenden ServiceNow AI Platform Kingston-Version wird gestartet .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Discovery von PCF V3-Komponenten wird unterstützt, wenn Muster für Discovery und Service-Mapping Plugin Version 1,0.99, März 2023 ist installiert. Das Muster unterstützt weiterhin die Discovery von PCF V2-Komponenten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Pivotal Cloud Foundry-Anmeldeinformationen

Erstellen Sie Pivotal Cloud Foundry Anmeldeinformationen.

1. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Aus **CloudFoundry-Anmeldeinformationen** .
4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Name der Anmeldeinformationen Beispiel: pcf_user-Anmeldeinformationen
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Anmeldeinformationen, die Sie auf **Alle MID Server** in Ihrem Netzwerk oder auf einen oder mehrere **Spezielle MID Server** anwenden oder nicht anwenden möchten. Wählen Sie **Spezielle MID Server** aus.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen versucht, während sie versucht, sich bei Geräten anzumelden. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste höher erscheinen. Legen Sie die Anmeldeinformationsreihenfolge fest, wenn eine große Anzahl von Anmeldeinformationen verwendet wird oder wenn die Sicherheit Anwender nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Benutzername	Name des Benutzers dieser Anmeldeinformationen. Vermeiden Sie führende oder nachgestellte Leerzeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Anwendernamen erkennt. Ein Beispiel ist `pcf_user`. Verwenden Sie die `client_id`, die zum Generieren des JWT-Tokens verwendet wird.
Passwort	Passwort des Benutzers dieser Anmeldeinformationen. Verwenden Sie das `client_secret`, das zum Generieren des JWT-Tokens verwendet wird.
Anmeldeinformationsalias	Alternativer Name für diese Anmeldeinformationen. Ein Beispiel ist `cf` Wenn dieses Feld geschlossen ist, wählen Sie das Entsperrsymbol, um das Feld zu entsperren.

5. Wählen Sie **Aktualisieren**.

JSON-Web-Token-Anmeldeinformationen

Führen Sie die folgenden Schritte zur Tokenvalidierung aus, um das JSON-Web-Token (JWT) zu überprüfen.

Das Format des JWT-Tokens ist: https://docs.cloudfoundry.org/api/uaa/version/4.27.0/index.html#jwt-bearer-token-grant .

1. Führen Sie das folgende cURL-Skript für die Server-API des Benutzerkontos und der Authentifizierung (UAA) aus, und überprüfen Sie die Ergebnisse:

   ```
   curl -s -k https://ip_address:port/oauth/token -X; POST -H ”Content-Type: application/x-www-form-urlencoded” -H “Accept: application/json” -d “client_id=<INSERT_USER_HERE>&client_secret=<INSERT_PASS_HERE>&grant_type=client_credentia
   ```

   Wenn dieser Befehl kein Token generiert, überprüfen Sie, ob die Anmeldeinformationen im enthalten sind ServiceNow Repository sind korrekt, andernfalls mit Schritt 2 fortfahren.

2. Führen Sie das folgende cURL-Skript für die Pivotal Cloud Foundry-API aus:

   ```
   Curl https://ip_address:port/v3/spaces -k -V -H „Accept: Application/JSON“ -H „Authorization: Bearer<INSERT TOKEN HERE>“
   ```

   Wenn dieser Befehl die PCF-Bereichsinformationen nicht abruft, überprüfen Sie die Anmeldeinformationen auf dem ServiceNow Anmeldeinformationen-Repository.

Anmeldeinformationen für V3-API-Elemente

Gewähren Sie einem leseberechtigten Benutzer die Berechtigung zur Verwendung der folgenden API-Elemente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- –/v3/Organizations
- –/v3/spaces
- –/v3/Domänen
- –/v3/Routen
- –/v3/Organization_Quoten
- –/v3/space_Quoten
- –/v3/Apps
- -/v3/Service_Offerings
- -/v3/Service_Plans
- -/v3/Service_instances
- -/v3/Tröpfchen

Hinweis: Die Pivotal Cloud Foundry Das Muster unterstützt auch die PCF V2-APIs.

Discovery-Zeitplan ohne Server erstellen

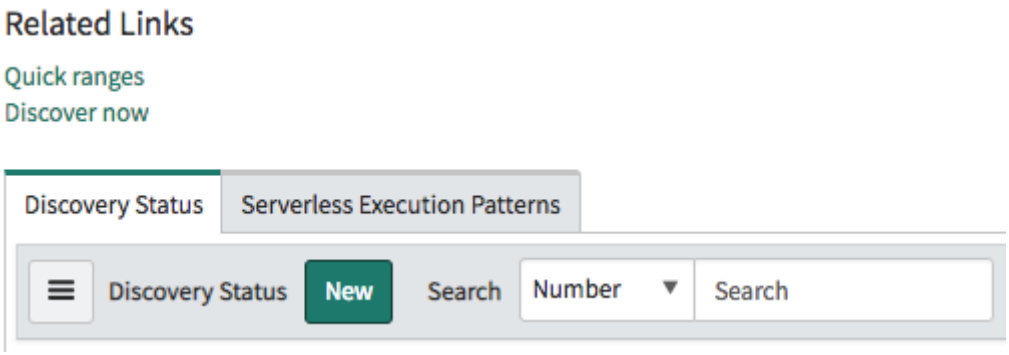
1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus:

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diesen Discovery-Zeitplan ein, z. B. `pcf`.
Erkennen	Wählen Sie als Erkennungstyp **ohne Server** aus.
MID-Server	MID Servers, für die die Anmeldeinformationen gelten. Geben Sie den erforderlichen MID-Server an, z. B. `Discovery_Server`.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Anmeldeinformationsalias	Alternativer Name für diese Anmeldeinformationen. Verwenden Sie den Alias, der sich auf bezieht Pivotal Cloud Foundry Anmeldeinformationen, die Sie zuvor erstellt haben.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie die Registerkarte Ausführungsmuster ohne Server.
6. Wählen Sie **Neu**.
7. Füllen Sie die Felder im Formular aus.

Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für dieses serverlose Ausführungsmuster ein, z. B. `Pcf1`
Muster	Wählen Sie **CloudFoundry** aus.
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Kontrollkästchen, um diesen Zeitplan für die Erkennung zu aktivieren. Aktivieren Sie das Kontrollkästchen.

8. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „serverlose Ausführungsmuster“, und wählen Sie aus **Speichern** .
9. Wählen Sie die Registerkarte serverlose Ausführungsmuster aus
10. Erstellen und definieren Sie das Ausführungsmuster ohne Server wie in der Produktdokumentation beschrieben.

    Konfigurieren Sie die für erforderlichen Parameter Pivotal Cloud Foundry Muster wie folgt:

Startprogrammparameter für Discovery-Muster

Parameter	Beschreibung
Organisation	Name der Organisation, die erkannt werden muss, oder aller, deren Eingabe „*“ ist.
CredentialAlias	Alternativer Name für diese Anmeldeinformationen. Verwenden Sie den Alias, der sich auf bezieht Pivotal Cloud Foundry Anmeldeinformationen, die Sie zuvor erstellt haben.
URL_CF	API-URL des Cloud-Controllers, der zum Abrufen der Informationen von verwendet wird Pivotal Cloud Foundry.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
URL_CF_AUTH	UAA-Server-API, die zum Generieren des Tokens verwendet wird. Geben Sie den Wert im folgenden Format ein: https://uaa.sys.dev.phx.pcf.example.com/oauth/token.

11. **Führen Sie eine Aktualisierung durch**.
12. Um die Discovery zu starten, navigieren Sie zu serverlos Discovery Definition und wählen Sie aus **Entdecken Sie Jetzt** .

EVAL-Abschlussfunktionen

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um alle Organisationen mit „,“ als Trennzeichen zu verketten.

```
var rtrn = '';
var organizations = ${organizations[*].name};
var beforeReturn = '';
var separator = '';
for (var i = 0; i < organizations.size(); i++)
 {
 beforeReturn += separator + organizations.get(i);
 separator = ',';
 }
rtrn = beforeReturn;
```

Verwenden Sie Folgendes EVAL Abschlussfunktionen, die 1 zurückgeben, wenn der Betriebsstatus aktiv ist, und 2, wenn er nicht aktiv ist.

```
var rtrn = '';
var currentOrgStatus = ${organizations[].operational_status};
var status = currentOrgStatus.toLowerCase();
if(status == "active"){
   rtrn = "1";
}
else {
   rtrn = "2";
}
```

Verwenden Sie Folgendes EVAL Abschlussfunktion, um 1 zurückzugeben, wenn der Betriebsstatus „gestartet“ ist, und 2, wenn er nicht gestartet wird.

```
var rtrn = '';
var currentAppStatus = ${apps[].state};
var status = currentAppStatus.toLowerCase();
if(status == "started"){
   rtrn = "1";
}
else {
   rtrn = "2";
}
```

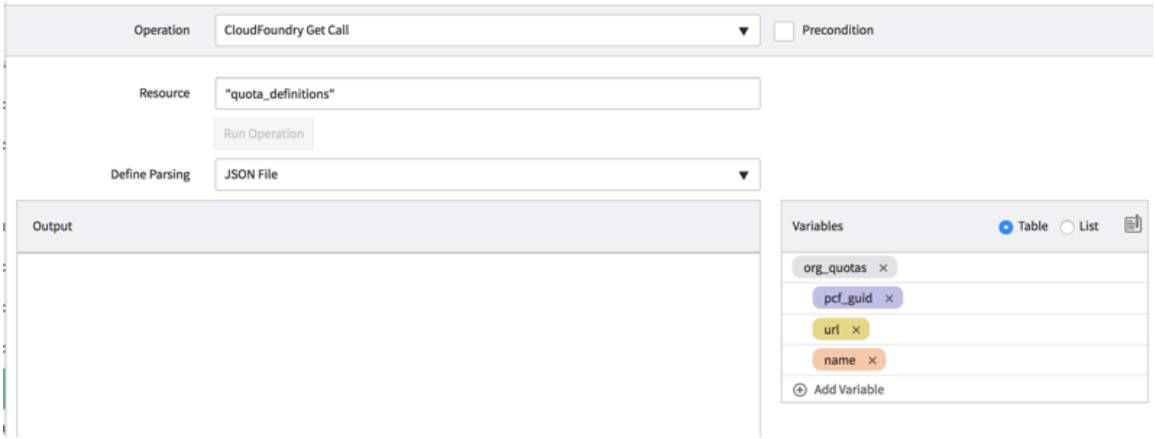
CloudFoundry Get Call

Der benutzerdefinierte Vorgang „CloudFoundry Get Call“ behandelt die Generierung von Token. Er verwendet die Anmeldeinformationen und die Kontextvariable URL_CF_AUTH, um ein Token zu generieren, das zum Erstellen von API-Aufrufen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Token generiert wird, wird URL_CF verwendet, um die im Feld **Ressource** definierten API-Aufrufe zu erstellen. Der benutzerdefinierte Vorgang behandelt auch die Paginierung, wenn die Antwort mehr als eine Seite umfasst.

CloudFoundry Get Call analysiert die Eingabe JSON, um die Tabellen und Variablen auszufüllen.



Pivotal Cloud Foundry BOSH Erweiterungsabschnitt

Die Pivotal Cloud Foundry BOSH ist ein Erweiterungsabschnitt von Pivotal Cloud Foundry Muster.

Die Erweiterung ist auf verfügbar ServiceNow® Store Für das Release Juni 2023 von Muster für Discovery und Service-Mapping1,6.0.

Anforderungen für Pivotal Cloud Foundry BOSH

Hinweis: Die folgenden Anforderungen gelten nur für den BOSH-Erweiterungsabschnitt.

Die Opsman-Authentifizierungs-URL muss als Musterparameter mit dem Namen angegeben werden *`URL_OPSMAN_AUTH`*. Beispiel: https://<opsman Einstiegspunkt>/uaa/oauth/Token

Die hinzugefügten Anmeldeinformationen müssen über die Berechtigung zum Ausführen der folgenden APIs verfügen:

- `/uaa/oauth/Token`
- `/api/v0/deploy/products`

Hinweis: Anwenderdefinierte APIs werden als hinzugefügt *`Tanzu Opsman – API abrufen`* Gehen Sie zum Muster.

Von Discovery während der horizontalen Erkennung erfasste Daten

Erfasste Informationen

Feld	Beschreibung
Haupt-CI: PCF-Grundlage [cmdb_ci_pcf_Foundation]	
Name	Pivotal Cloud Foundry Name des Clustereintrags <name>-<hostCf:<portCf>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Informationen (Fortsetzung)

Feld	Beschreibung
ip_address	Pivotal Cloud Foundry Host-IP.
port	Pivotal Cloud Foundry Service-Port.
short_description	Pivotal Cloud Foundry Service-Build-Nummer.
Organisation	Organisationsliste, verwaltet vom PCF-Cluster. Die Einträge werden durch Kommata „,“ getrennt.
PCF-Organisation [cmdb_ci_pcf_Organization]	
Name	Organisationsname
URL	Eindeutige Organisations-URL
pcf_guid	Organisations-UID in CF
operational_status	Organisationsstatus
PCF-Bereich [cmdb_ci_pcf_space]	
Name	Platzname
URL	Eindeutige Speicherplatz-URL
pcf_guid	Platz-UID in CF
PCF-Anwendung [cmdb_ci_pcf_appl]	
Name	Anwendungsname
URL	Eindeutige Anwendungs-URL
pcf_guid	Eindeutige Anwendungs-UID in CF
PCF-Route [cmdb_ci_pcf_Route]	
Name	Routenname
URL	Eindeutige Routen-URL
pcf_guid	Routen-UID in CF
port	Routenport
Typ	Routentyp
PCF-Kontingent [cmdb_ci_pcf_Kontingent]	
Name	Kontingentname
URL	Eindeutige Kontingent-URL
pcf_guid	Kontingent-UID in CF
PCF-Domäne [cmdb_ci_pcf_Domain]	
name	Domänenname
URL	Eindeutige Domänen-URL
pcf_guid	Domänen-UID in CF
PCF-Bereichsinstanz [cmdb_ci_pcf_space_instance]	
name	Name der Platzserviceinstanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Informationen (Fortsetzung)

Feld	Beschreibung
URL	Eindeutige Platzserviceinstanz-URL
pcf_guid	UID-Platzserviceinstanz in CF
PCF-Serviceplan [cmdb_ci_pcf_Service_Plan]	
name	Name der Serviceplaninstanz
URL	Eindeutige Serviceplan-URL
pcf_guid	UID-Platzserviceinstanz in CF
PCF-Service [cmdb_ci_pcf_Service]	
name	Servicename
URL	Eindeutige Service-URL
pcf_guid	Service-UID in CF
PCF-Droplet [cmdb_ci_pcf_Droplet]	
name	Ressourcen-URL
pcf_guid	Droplet-ID
URL	Droplet-URL
install_status	Installationsstatus: 1, „installiert“
operational_status	Betriebsstatus: 1, „operativ“
Schlüsselwert [cmdb_key_value]	
key	Ressourcen-Tag-Schlüssel **Hinweis:** Diese Daten werden nur für V3-API-Aufrufe erfasst.
Wert	Ressourcen-Tag-Wert. **Hinweis:** Diese Daten werden nur für V3-API-Aufrufe erfasst.

Von erkannte Daten Pivotal Cloud Foundry BOSH-Erweiterungsabschnitt

Feld	Beschreibung
BOSH-Bereitstellung (cmdb_ci_bosh_Deployment)	
Name	Der Installationsname der Ressource.
object_id	Die ID des bereitgestellten Produkts.
install_status	Hartcodiert auf den Wert: `1= installiert .`
operational_status	Hartcodiert auf den Wert: `1= betriebsbereit .`
Deployment_Version	Die Version des bereitgestellten Produkts.
deployment_type	Der Typ des bereitgestellten Produkts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Diese Beziehungen sollen die Pivotal Cloud Foundry-Erkennung unterstützen.

CI	Beziehung	CI
PCF-Bereich [cmdb_ci_pcf_space]		
cmdb_ci_pcf_space	Enthält::Enthalten in	cmdb_ci_pcf_organization
PCF-Anwendung [cmdb_ci_pcf_appl]		
cmdb_ci_pcf_appl	Enthält::Enthalten in	cmdb_ci_pcf_space
PCF-Route [cmdb_ci_pcf_Route]		
cmdb_ci_pcf_route	Enthält::Enthalten in	cmdb_ci_pcf_foundation
PCF-Kontingent [cmdb_ci_pcf_Kontingent]		
cmdb_ci_pcf_quota	Verwendet::Verwendet von	cmdb_ci_pcf_space cmdb_ci_pcf_organization
PCF-Domäne [cmdb_ci_pcf_Domain]		
cmdb_ci_pcf_domain	Verwendet::Verwendet von	cmdb_ci_pcf_route
	Eigentümer von::Eigentum von	cmdb_ci_pcf_organization
	Enthält::Enthalten in	cmdb_ci_pcf_foundation
PCF-Bereichsinstanz [cmdb_ci_pcf_space_instance]		
cmdb_ci_pcf_space_instance	Enthält::Enthalten in	cmdb_ci_pcf_space
PCF-Serviceplan [cmdb_ci_pcf_Service_Plan]		
cmdb_ci_pcf_service_plan	Verwendet::Verwendet von	cmdb_ci_pcf_space_instance
PCF-Service [cmdb_ci_pcf_Service]		
cmdb_ci_pcf_service	Verwendet::Verwendet von	cmdb_ci_pcf_service_plan
PCF-Droplet [cmdb_ci_pcf_Droplet]		
cmdb_ci_pcf_appl	Enthält::Enthalten in	cmdb_ci_pcf_Droplet
Schlüsselwert [cmdb_key_value]		
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_Droplet
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_organization
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_space
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_domain

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_route
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_appl
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_service
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_service_plan
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_space_instance

Pivotal Cloud Foundry BOSH-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Pivotal Cloud Foundry Discovery des BOSH-Erweiterungsabschnitts.

CI	Beziehung	CI
Cloud Foundry-Cluster [cmdb_ci_pcf_Foundation]	Enthält::Enthalten in	BOSH-Bereitstellung [cmdb_ci_bosh_Deployment]

Reiner Speicher FlashArray Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet das Pure Storage Flash Array-Muster, um Pure Storage zu finden FlashArray In Ihrer Infrastruktur. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Hinweis: Ab März 2024 ist die Musterausführung standardmäßig deaktiviert. Dient zum Erstellen eines CI für Pure Storage FlashArray, Synchronisieren Sie das Muster mit MID-Server.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung, um sie zu klassifizieren FlashArray. Weitere Informationen finden Sie unter Standardauthentifizierung .

Überprüfen Sie die Berechtigungen zum Ausführen von REST API-Aufrufen

Das Pure Storage Flash Array-Muster unterstützt die API 2,17-Version.

- `/api/1,17/auth/apitoken`
- `/api/2,17/auth/Session`
- `/api/2,17/Arrays`
- `/api/2,17/Volumes`
- `/api/2,17/Volume-groups`
- `/api/2,17/Host-groups`
- `/api/2,17/Hardware`
- `/api/2,17/dns`
- `/api/2,17/Ports`

Hinweis: Die Version des Pure Storage-Musters vom Februar 2024 unterstützt nur die iSCSI-Protokoll-Discovery.

Discovery wird ausgeführt.

Um die Discovery anhand von Mustern auszuführen, erstellen Sie einen Discovery-Zeitplan, der auf die Verwaltungs-IP-Adresse des abzielt FlashArray Speicher. Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Pure Storage Flash Array-Musters.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der vom Anwender zugewiesene Bezeichner oder die vom Benutzer zugewiesene Bezeichnung für FlashArray Speicher.
Seriennummer [serial_number]	Seriennummer, die jede Person eindeutig identifiziert FlashArray Speicher.
Betriebssystem [os]	Betriebssystem, das auf ausgeführt wird FlashArray Speicher.
BS-Version [os_Version]	Softwareversion, die auf installiert ist FlashArray Speicher.
Physische Kapazität (GB) [physical_Capacity]	Gesamtmenge des verfügbaren Speicherplatzes innerhalb von FlashArray System, gemessen in Gigabyte (GB). Diese Kapazität umfasst sowohl zugewiesene als auch nicht zugewiesene Speicherressourcen.
Freie Gesamtkapazität (GB) [total_free_Capacity]	Gesamtmenge des Speicherplatzes, der derzeit für die Verwendung auf verfügbar ist FlashArray Speichersystem, gemessen in GB.
IP-Adresse [ip_address]	IP-Adresse des FlashArray Speicher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
Hersteller [manufacturer]	Herstellername: Reiner Speicher.
Objekt-ID [object_id]	Anmeldeinformationsaffinität, die während der Discovery zugewiesen wurde FlashArray Speicher. Weitere Informationen zur Affinität von Anmeldeinformationen finden Sie unter Anmeldeinformationsaffinität für Discovery und Orchestration .
Modell-ID [model_id]	Modell-ID von FlashArray Speicher.
Verschlüsselung im Ruhezustand [Encryption_at_Rest]	Verschlüsselte Daten, die auf einem physischen Gerät oder in einer Datenbank gespeichert sind. Mögliche Werte: • aktiv • Deaktivieren
Verschlüsselungsalgorithmus [Encryption_algorithmus]	Typ des Algorithmus, den der Speicherserver verwendet. Mögliche Werte: • AES-256: Advanced Encryption Standard (AES) 256-Verschlüsselung • Mehrere Methoden: Pure Storage unterstützt derzeit nicht mehrere Methoden • Unbekannt: Wenn während einer vorherigen Discovery ein Algorithmustyp erkannt wurde, während der nächsten Discovery jedoch nicht erkannt wird, ist der Wert unbekannt

Speicherclusterknoten [cmdb_ci_storage_cluster_node]

Feld	Beschreibung
Name [name]	Clusterknotenname.
Cluster [cluster]	Hostgruppe, die diesem Clusterknoten in zugeordnet ist FlashArray Umgebung.
Change-Gruppe [Assignation_Group]	ISCSI- oder Fibre Channel-Initiatorverbindungen zwischen dem Speicher und dem Host.
Hersteller [manufacturer]	Herstellername: Reiner Speicher.
Kommentare [comments]	Alle Logical Unit Numbers (LUN), die mit dem Clusterknoten verbunden sind.

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Name des Speicherclusters.
Korrelations-ID [correlation_ID]	Kombiniert den Clusternamen und die Seriennummer des Speichers, um einen eindeutigen Bezeichner (UID) zu erstellen.
Hersteller [manufacturer]	Herstellername: Reiner Speicher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Name [name]	Volumename
Seriennummer [serial_number]	Seriennummer des Volumes.
Volume-ID [volume_id]	Volume-ID.
Installiert [install_date]	Datum, an dem das Volume installiert wurde.
Größe in Byte [size_bytes]	Volume-Größe in Byte.
Pool-ID [Pool_ID]	ID des Pools, der die Volumes enthält.
Attribute [Attribute]	Namen der Hosts, die mit den Volumes verbunden sind.
Hersteller [manufacturer]	Herstellername: Reiner Speicher.

Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Name des Speicherpools.
Objekt-ID [object_id]	ID des Speicherpools.
Hersteller [manufacturer]	Herstellername: Reiner Speicher.

Speichercontroller [cmdb_ci_storage_controller]

Feld	Beschreibung
Name [name]	Kombination aus Asset und Asset-Tag.
Modell-ID [model_id]	Modell-ID des Controllers.
Zugewiesen [zugewiesen]	Verfügbarkeitsstatus.
Geräte-ID [device_id]	Eine eindeutige Bezeichnung für den Controller.
Hersteller [manufacturer]	Herstellername: Reiner Speicher.

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Spindel-ID.
Größe in Byte [size_bytes]	Datenträgergröße in Byte.
Laufwerkstyp [Drive_type]	Typ des auf dem Datenträger installierten Laufwerks.
Geräte-ID [device_id]	Kombination der Seriennummer des Speichersystems mit dem Datenträgernamen, der jeden Datenträger innerhalb des eindeutig identifiziert FlashArray Umgebung.
Hersteller [manufacturer]	Datenträgerhersteller.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Name des Netzwerkadapters
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
IP-Standard-Gateway [ip_default_Gateway]	IP-Adresse des Standard-Gateways.
Alias [alias]	Der vom Anwender zugewiesene Name für den Netzwerkadapter.
Netzmaske [netmask]	Netzmaske des Netzwerkadapters

Fibre Channel-Export [cmdb_ci_fc_export]

Feld	Beschreibung
Initiator-WWPN [Initiator_wwpn]	UID, die die Director-ID, die Portnummer und die Initiator-ID kombiniert.

ISCSI-Export [cmdb_ci_iscsi_Export]

Feld	Beschreibung
Name [name]	Initiator-ID in FlashArray Systeme, die als UID für den Initiator im Kontext von iSCSI-Exporten dienen.
Export-ID [Export_ID]	UID für einen iSCSI-Export in FlashArray Systeme, die die Verwaltung und Nachverfolgung von iSCSI-Verbindungen erleichtern.
Initiator-IQN [Initiator_iqn]	Qualifizierter iSCSI-Name (IQN), der einem Initiator im iSCSI-Netzwerk zugewiesen ist.

CI-Beziehungen

CI	Beziehungstyp	CI
[cmdb_ci_disk]	Enthält::Enthalten in	[cmdb_ci_Storage_Server]
[cmdb_ci_iscsi_Export]	Gehostet auf::Hostet	[cmdb_ci_Storage_Server]
[cmdb_ci_iscsi_Export]	Referenz	[cmdb_ci_Storage_Cluster_node]
[cmdb_ci_Network_Adapter]	Eigentümer von::Eigentum von	[cmdb_ci_Storage_Server]
[cmdb_ci_Storage_Cluster_node]	Cluster von::Cluster	[cmdb_ci_Storage_Cluster]
[cmdb_ci_Storage_Controller]	Controller für::gesteuert von	[cmdb_ci_Storage_Server]
[cmdb_ci_Storage_Server]	Zugeordnet zu::Zugeordnet von	[cmdb_ci_Storage_Cluster_node]
[cmdb_ci_Storage_Server]	Enthält::Enthalten in	[cmdb_ci_Storage_Pool]
[cmdb_ci_Storage_Server]	Wird ausgeführt auf::Wird ausgeführt	[cmdb_ci_Storage_Cluster]
[cmdb_ci_storage_volume]	Enthält::Enthalten in	[cmdb_ci_Cluster_node]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
[cmdb_ci_storage_volume]	Enthält::Enthalten in	[cmdb_ci_Storage_Server]
[cmdb_ci_storage_volume]	Referenz	[cmdb_ci_Storage_Pool]

Pure Storage FlashBlade-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das FlashBlade Pure Storage-Muster, um FlashBlade-Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery kann Pure Storage FlashBlade Version 4 erkennen.

Hinweis:

Nur Linux MID Servers Werden für die Pure Storage FlashBlade-Discovery unterstützt. Windows MID Servers Werden nicht unterstützt.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Konfigurieren Sie Anwenderberechtigungen für UNIX BETRIEBSSYSTEM

Konfigurieren Sie einen Anwender für den Zugriff auf UNIX BETRIEBSSYSTEM.

- Definieren Sie den BS-Anwender mit Berechtigungen zum Ausführen der folgenden Befehle.

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
Pureman	-	Obligatorisch	Greift auf die Liste der Pure Storage-Befehle zu und verwendet sie für die Klassifizierung
Echo	$$username$$	Obligatorisch	Füllt den Benutzernamen für die temporäre Variable aus
"pureadmin list "	+ $usr + " --api-token --expose --csv"	Obligatorisch	Ruft das Benutzer-API-Token ab, um die x-auth für die REST-Aufrufbefehle zu generieren.

- Definieren Sie den BS-Anwender mit den erforderlichen Berechtigungen zum Ausführen der folgenden REST API-Aufrufe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- /api/login – Ruft den x-auth-Token-Leser aus der Antwort in Groovy ab.
- /api/1,2/file – Systeme – Ruft Informationen zu den Dateisystemen ab.
- /api/1,2/Blades – Ruft Informationen zu Blades ab.
- /api/1,2/dns – Ruft Informationen zu DNS ab.
- /api/1,2/Hardware – Ruft Informationen zur Speicherhardware ab.
- /api/1,4/Network-interface – Ruft Informationen zu Netzwerkschnittstellen ab.

Konfigurieren Sie SSH-Anmeldeinformationen

Auf der ServiceNow AI Platform, Konfigurieren Sie SSH-Anmeldeinformationen für den BS-Anwender. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Konfigurieren Sie anwendbare Anmeldeinformationen

Auf der ServiceNow AI Platform, Konfigurieren Sie anwendbare Anmeldeinformationen für den BS-Anwender. Das Passwortfeld ist nicht relevant. Sie können einen beliebigen Wert für das Passwort eingeben oder es leer lassen. Weitere Informationen finden Sie unter Applicative-Anmeldeinformationen .

Zugriff auf den für REST-Aufrufe verwendeten Port

Auf relevant Linux MID Servers, Gewähren Sie einem Anwender Zugriff auf den Port, der für REST-Aufrufe verwendet wird.

Daten erfasst von Discovery Für Pure Storage FlashBlade

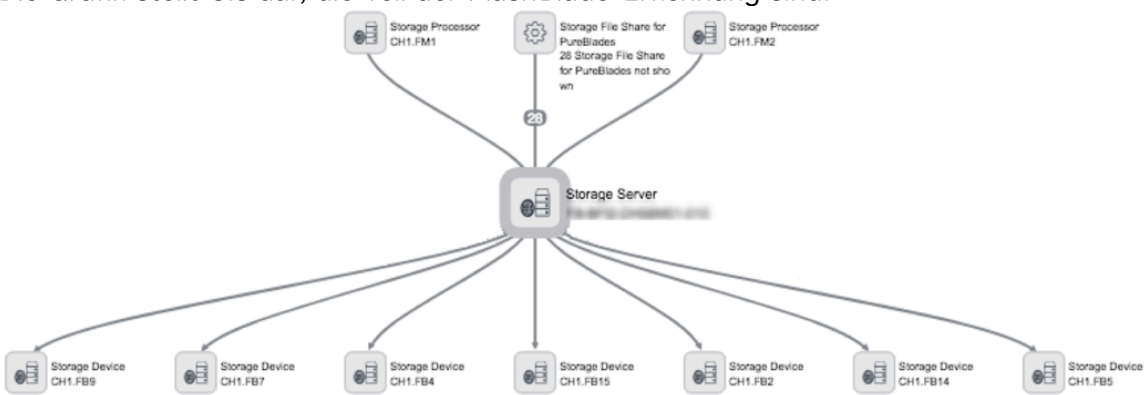
Discovery Füllt die Daten in aus CMDB Beim Ausführen des FlashBlade Pure Storage-Musters.

Tabelle und Feld	Beschreibung
Speicherserver [cmdb_ci_storage_server]	Die von FileShare for PureBlade bereitgestellten Attribute des Speicherservers
IP-Adresse [ip_address]	
Seriennummer [serial_number]	
Name [name]	
Pure Storage-Prozessor [cmdb_ci_storage_processor_pure]	Die Attribute des PureBlade-Speicherprozessors
Name [name]	
Seriennummer [serial_number]	
Geräte-ID [device_id]	
Modellnummer [model_number]	
Seriell [serial]	
Steckplatz [slot]	
Typ [type]	
Status [status]	
Pure Storage-Dateifreigabe [cmdb_ci_storage_fileshare_pure]	Die Attribute des FileShare-Speichers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Name [name]	
Pfad [path]	
Protokolle [protocols]	
Bereitgestellter Speicherplatz [provisioned_space]	
Eindeutiger Speicherplatz [unique_space]	
Snapshots-Speicherplatz [snapshots_space]	
Gesamter physischer Speicherplatz [total_physical_space]	
Freigegebener Speicherplatz [shared_space]	
Datenreduktion [data_reduction]	
Systemspeicherplatz [system_space]	
Speichergerät [cmdb_ci_storage_device]	Die Attribute des im Speicherserver enthaltenen Speichergeräts.
Geräte-ID [device_id]	
Name [name]	
Seriennummer [serial_number]	
Modellnummer [model_number]	
Speichertyp [storage_type]	

Die Grafik stellt CIs dar, die Teil der FlashBlade-Erkennung sind.



CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung der Pure Storage FlashBlade-Discovery.

CI	Beziehung	CI
Pure Storage-Dateifreigabe [cmdb_ci_storage_fileshare_pure]	Bereitgestellt von::Stellt bereit	Speicherserver [cmdb_ci_storage_server]
Speichergerät [cmdb_ci_storage_device]	Enthält::Enthalten in	Speicherserver [cmdb_ci_storage_server]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Speicherserver [cmdb_ci_storage_server]	Enthält::Enthalten in	Pure Storage-Prozessor [cmdb_ci_storage_processor_pure]

Red Hat JBoss Fuse-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können den Fuse-Anwendungsserver mithilfe des JBoss-Fuse-Musters finden und zuordnen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

Konfigurieren Sie SSH-Anmeldeinformationen im Modul für Anmeldeinformationen der ServiceNow-Plattform für den Zugriff auf den Server, auf dem der Fuse-Server gehostet wird.

Anwender

Gewähren Sie einem Benutzer die Leserechte für den Zugriff auf die folgenden Verzeichnisse:

- $install_directory + "/readme.txt"

  Der Zugriff auf dieses Verzeichnis ermöglicht das Abrufen von Versionsinformationen.

- /etc/services

  Der Zugriff auf dieses Verzeichnis ermöglicht das Lesen der Hostservice-Definition.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Jboss Fuse [cmdb_ci_appl_jboss_fuse]	
config_directory	Das Konfigurationsverzeichnis des Fuse-Servers
config_file	Die Konfigurationsdatei des Fuse-Servers
install_folder	Der Installationsordner des Fuse-Servers
Version	Die Version des Fuse-Servers
name	Der während der Installation für den Fuse-Server konfigurierte Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping erkennt die Verbindung zwischen dem JBoss Fuse-Server und dem IBM Informix Dynamic-Server.

Erkennung von Rubrik-Clustern

Discovery verwendet mehrere Muster, um sämtliche Daten über Rubrik-Cluster zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Anwendungen Discovery and Service Mapping Patterns und CMDB CI Class Models aus dem ServiceNow Store installieren, da die beiden Anwendungen voneinander abhängig sind.

Sie können die Muster zur Erkennung von Rubrik-Komponenten auf der ServiceNow AI Platform mit Release Paris oder höher verwenden.

Hinweis: Das in Version 1.0.78 von Discovery and Service Mapping Patterns angewendete Update behebt ein Problem mit doppelten CI-Typen in der CMDB. Wenn Sie Rubrik-Erkennungsmuster verwenden und bereits die Versionen 1.21.0, 1.23.0, 1.24.0 oder 1.25.0 der Store-App CMDB CI Class Models (sn_cmdb_ci_class) oder die Versionen 1.0.73, 1.0.74, 1.0.75 oder 1.0.76 der Anwendung Discovery and Service Mapping Patterns (sn_itom_pattern) installiert haben, sollten Sie den Anweisungen in KB0957523 folgen.

Alle Informationen für das Haupt-CI (Rubrik-Cluster) und die entsprechenden CI-Typen werden durch Aufrufe von REST APIs zurückgegeben.

Beachten Sie die folgenden Einschränkungen:

- Aufgrund der Einschränkungen des Mechanismus für große Nutzlasten werden in den Releases Paris und Quebec keine Referenzfelder unterstützt.
- Alle von der Rubrik REST API für Hosts (Server) zurückgegebenen Entitäten mit IP-Adressen, die nicht in Hostnamen aufgelöst werden, werden aus der Rubrik-Erkennung herausgefiltert (ausgeschlossen). Dies geschieht, um die Erstellung von Duplikaten in der CMDB zu verhindern.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App Discovery and Service Mapping Patterns

Stellen Sie Release 1.0.73 oder höher aus dem ServiceNow Store bereit.

Store-App „CMDB CI Class Models“

Stellen Sie Release 1.21.0 oder höher aus dem ServiceNow Store bereit.

Berechtigungen für Basisauthentifizierung

Stellen Sie sicher, dass zur Authentifizierung der REST API-Aufrufe die Anmeldeinformationen für die Basisauthentifizierung konfiguriert sind.

Anmeldeinformationsaliase, die den Rubrik-Anmeldeinformationen vom Typ Standardauthentifizierung zugeordnet sind, müssen ebenfalls erstellt werden. Diese Aliase dienen zusammen mit der IP-Adresse als Eingabeparameter.

Diese werden für die Erkennung aller CI-Typen verwendet, die dem Rubrik-Cluster zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sicherheitsschematyp: HTTP
- HTTP-Autorisierungsschema: Standard

MID-Server

Stellen Sie sicher, dass der MID Server auf die Ziel-Appliance zugreifen kann.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan ohne Server, um eine gezielte Erkennung von Rubrik-Clusterressourcen durchzuführen.

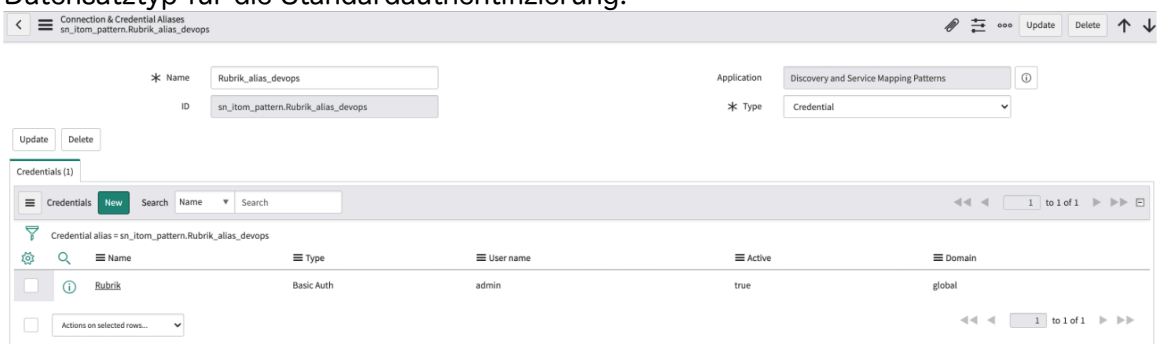
Hinweis: Der Discovery-Zeitplan, der alle mit Rubrik verknüpften Muster auslöst, unterstützt nur den Typ der serverlosen Erkennung. Außerdem muss für jedes Rubrik-Cluster (Brik) ein neuer Zeitplan für die serverlose Erkennung erstellt werden. Der Zeitplan muss die IP-Adresse aller Rubrik-Knoten enthalten, die dem Rubrik-Cluster zugeordnet sind, und den Anmeldeinformationsalias, der dem Anmeldeinformationsdatensatz der Rubrik-Standardauthentifizierung zugeordnet ist.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Zum Beispiel Erkennung Rubrik.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Server s
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

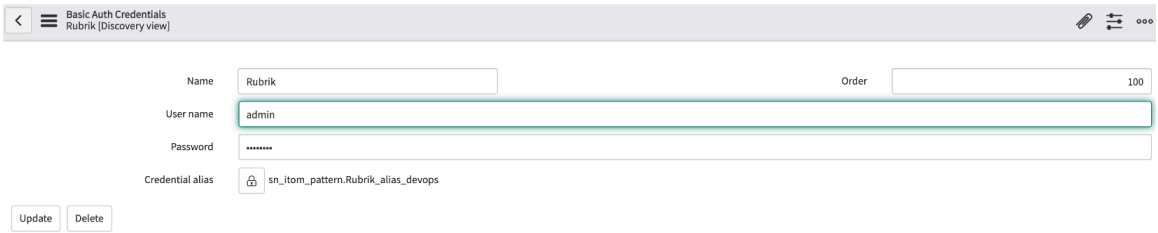
3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Navigieren Sie zu **Aliasse für Verbindungen und Anmeldeinformationen**, und erstellen Sie einen neuen Datensatztyp für Anmeldeinformationen. Erstellen Sie im Formular der zugehörigen Liste „Anmeldeinformationen“ einen neuen Datensatztyp für die Standardauthentifizierung.



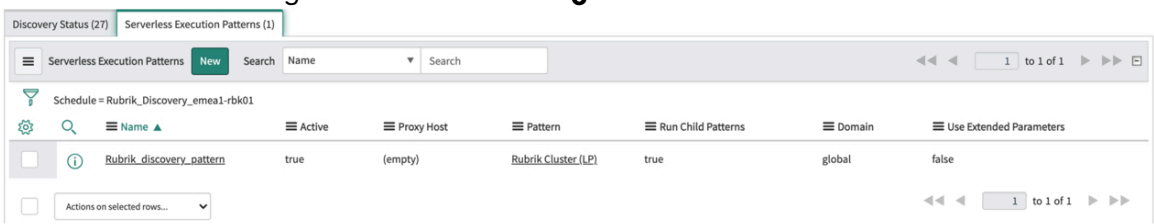
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Anmeldeinformationsalias kann vorhandenen Anmeldeinformationen zugeordnet werden. Beim Erstellen eines Anmeldeinformationsdatensatzes können Sie ihm auch den Anmeldeinformationsalias zuordnen. Klicken Sie auf das Schloss-Symbol **Anmeldeinformationsalias** im Datensatztyp „Aliasse für Verbindungen und Anmeldeinformationen“, den Sie oben angelegt haben, und ordnen Sie ihn nach Bedarf zu.

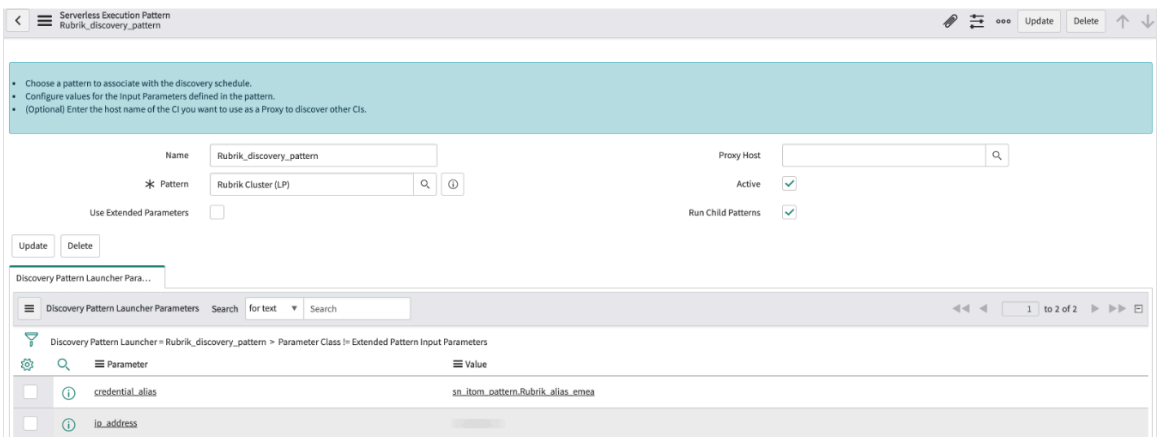


5. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**.



6. Stellen Sie sicher, dass die Spalte „Untergeordnete Muster ausführen“ für das Rubrik-Erkennungsmuster auf **true** gesetzt ist. Dadurch werden alle untergeordneten Muster ausgelöst, die dem Rubrik-Erkennungsmuster zugeordnet sind. Dies ist aufgrund des Mechanismus für große Nutzlasten erforderlich, der für die Erkennung des Rubrik-Clusters und aller entsprechenden CI-Typen verwendet wird.
7. Legen Sie unter **Startprogrammparameter für Discovery-Muster** die Parameter **credential_alias** und **ip_adresse** fest, die als Eingabeparameter für die Auslösung des Discovery-Zeitplans und das zugehörige Rubrik-Erkennungsmuster dienen.

   Setzen Sie den Parameter **ip_address** auf eine der IP-Adressen eines der Rubrik-Knoten, die dem Rubrik-Cluster zugeordnet sind. Setzen Sie **credential_alias** auf die ID des Anmeldeinformations-Datensatztyps, der in **Aliasse für Verbindungen und Anmeldeinformationen** erstellt wurde und mit dem Datensatztyp der Standardauthentifizierung für Rubrik-Anmeldedaten verwandt ist.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Rubrik AIX Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik AIX-Host [cmdb_ci_aix_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

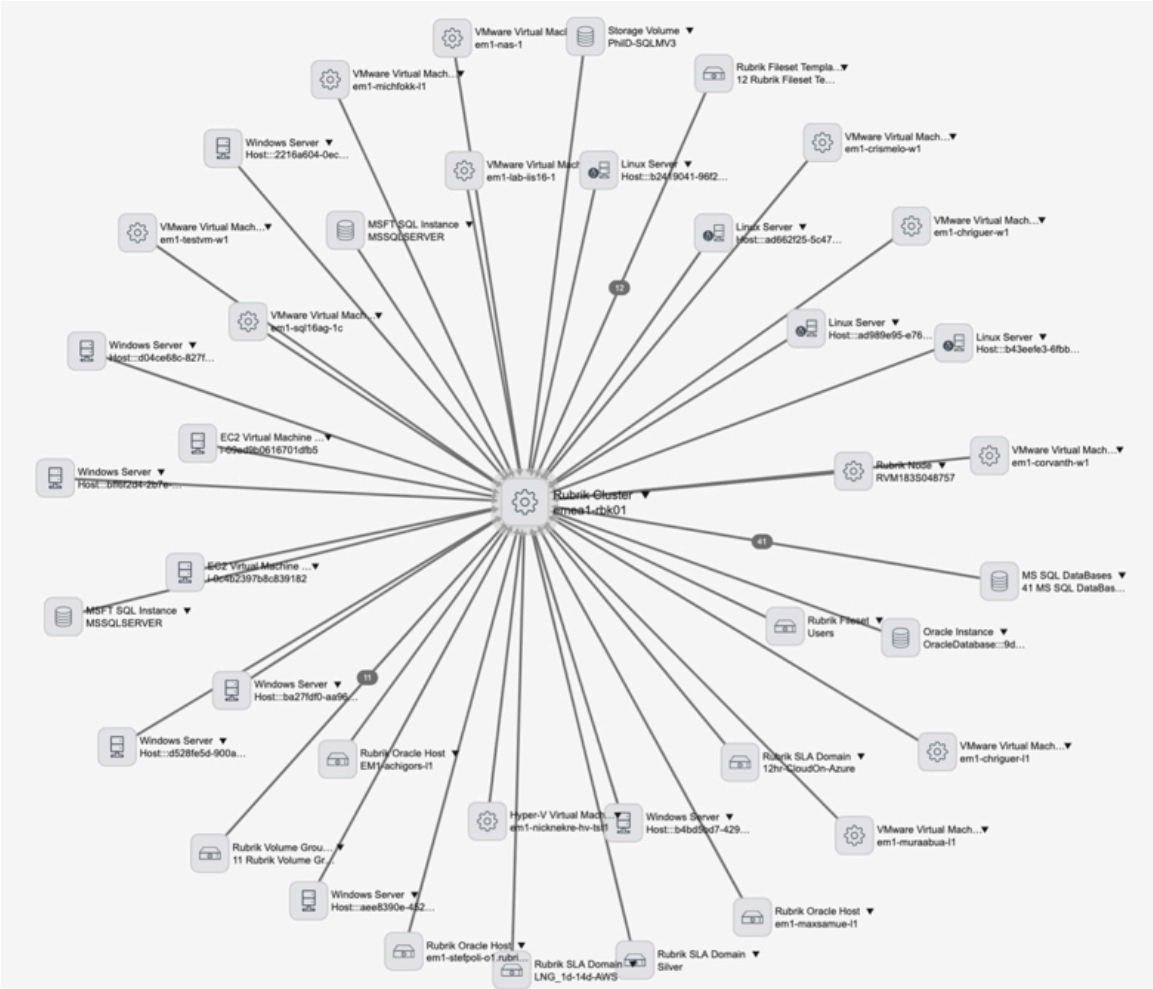
Ressourcen, die mithilfe des Musters „Rubrik Cluster (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Cluster [cmdb_ci_rubrik_cluster]	
cluster_id	Eindeutige ID des Rubrik-Clusters
name	Name des Rubrik-Clusters
cluster_version	Aktuelle Version des Rubrik-Clusters
api_version	API Version des Rubrik-Clusters
timezone	Vom Rubrik-Cluster verwendete Zeitzone

Die Dependency Views-Zuordnung zeigt die erkannten Clusterressourcen und deren Beziehungen untereinander.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



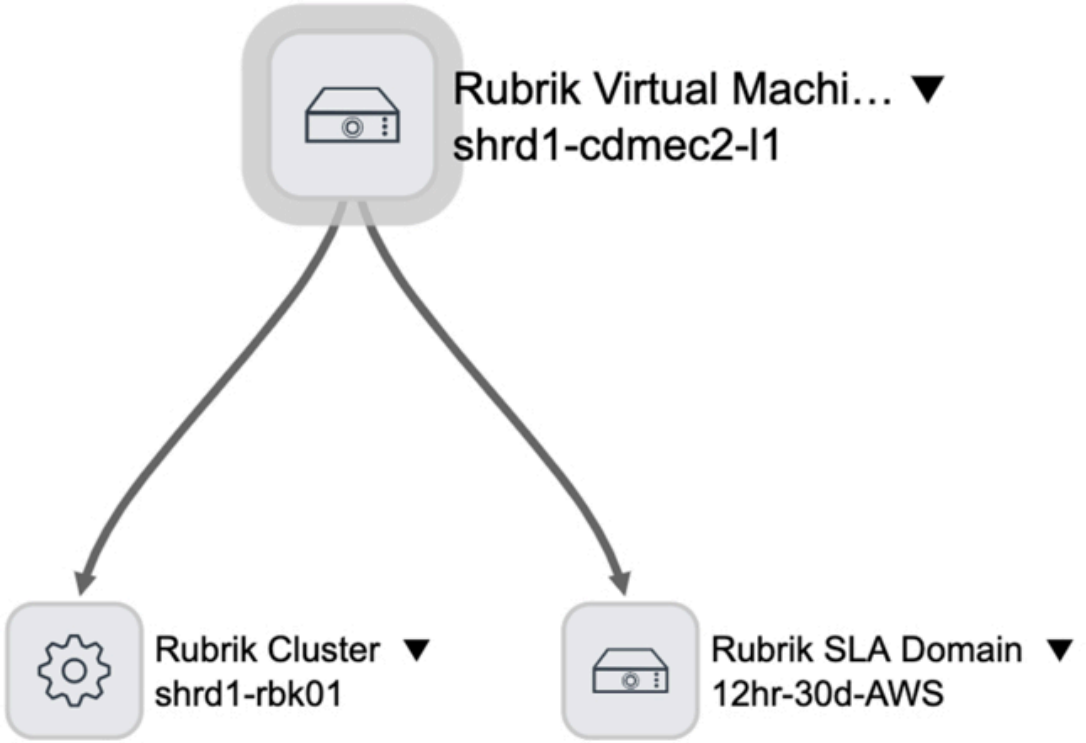
Ressourcen, die mithilfe des Musters „Rubrik EC2 Instance (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-EC2-Instanz [cmdb_ci_rubrik_vm_instance]	
object_id	ID der EC2-Instanz im Rubrik-Kontext
name	Name der EC2-Instanz im AWS-Kontext
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
account_id	ID des der EC2-Instanz zugeordneten AWS-Kontos
account_name	Name des der EC2-Instanz zugeordneten AWS-Kontos
instance_id	ID der EC2-Instanz im AWS-Kontext
instance_name	Name der EC2-Instanz im Rubrik-Kontext
instance_type	Vorlagentyp der EC2-Instanz
region	Geografische Region, in der sich die EC2-Instanz im AWS-Kontext befindet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Dependency Views-Zuordnung zeigt die erkannten EC2-Instanzen und deren Beziehungen untereinander.

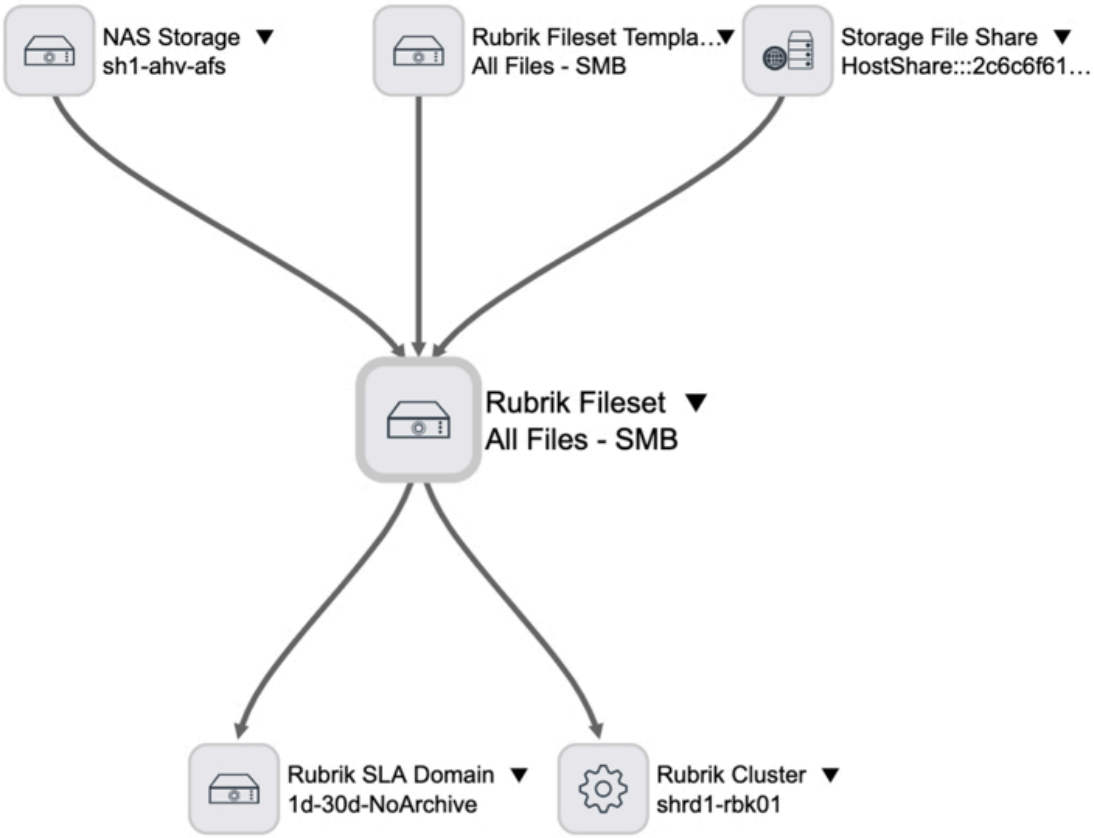


Ressourcen, die mithilfe des Musters „Rubrik Fileset (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Dateisatz [cmdb_ci_rubrik_fileset]	
object_id	ID des Rubrik-Dateisatzes
name	Name des Rubrik-Dateisatzes
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem der Rubrik-Dateisatz zugeordnet ist
template_id	ID der Rubrik-Dateisatzvorlage, aus der der Rubrik-Dateisatz die Ressourcen definiert
share_id	ID der Rubrik-Freigabe, die Besitzer des Rubrik-Dateisatzes ist

Die Dependency Views-Zuordnung zeigt die erkannten Dateisätze und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

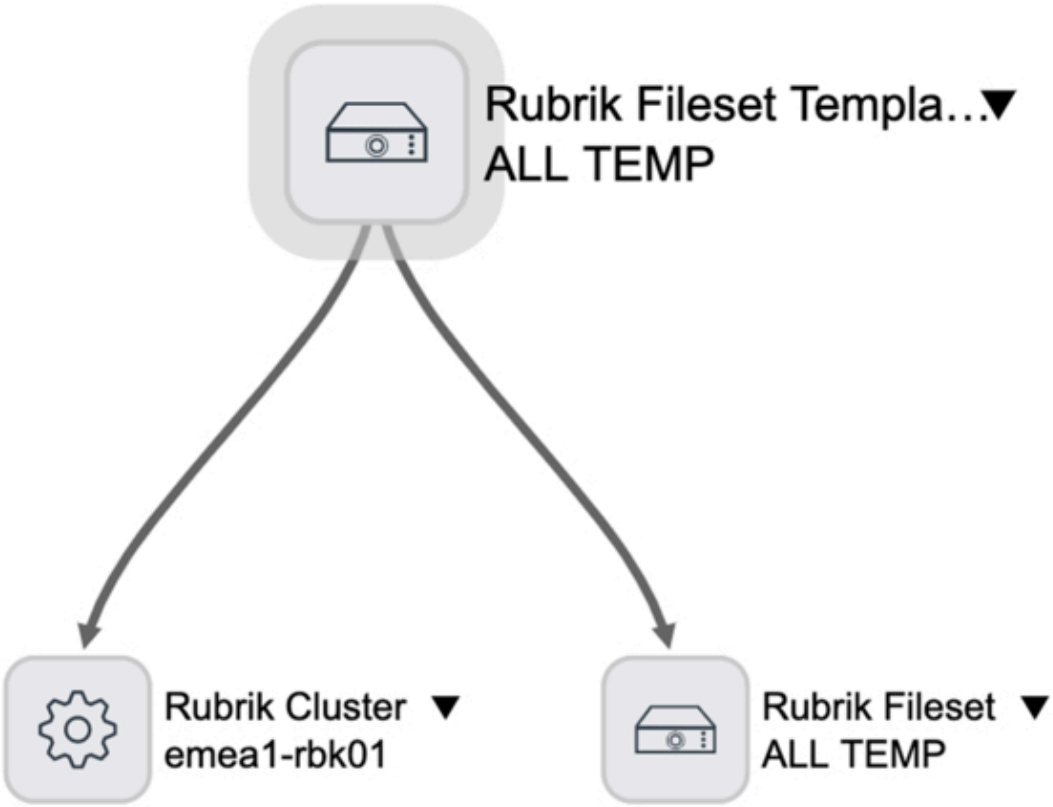


Ressourcen, die mithilfe des Musters „Rubrik Fileset Template (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Dateisatzvorlage [cmdb_ci_rubrik_fileset]	
object_id	ID der Rubrik-Dateisatzvorlage
name	Name der Rubrik-Dateisatzvorlage
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
share_count	Anzahl der Freigaben, die der Rubrik-Dateisatzvorlage zugeordnet sind
share_type	Typ der Freigaben, die der Rubrik-Dateisatzvorlage zugeordnet sind
host_count	Hostzähler, der der Rubrik-Dateisatzvorlage zugeordnet ist
os_type	Typ des Betriebssystems, das der Rubrik-Dateisatzvorlage zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Dateisatzvorlagen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



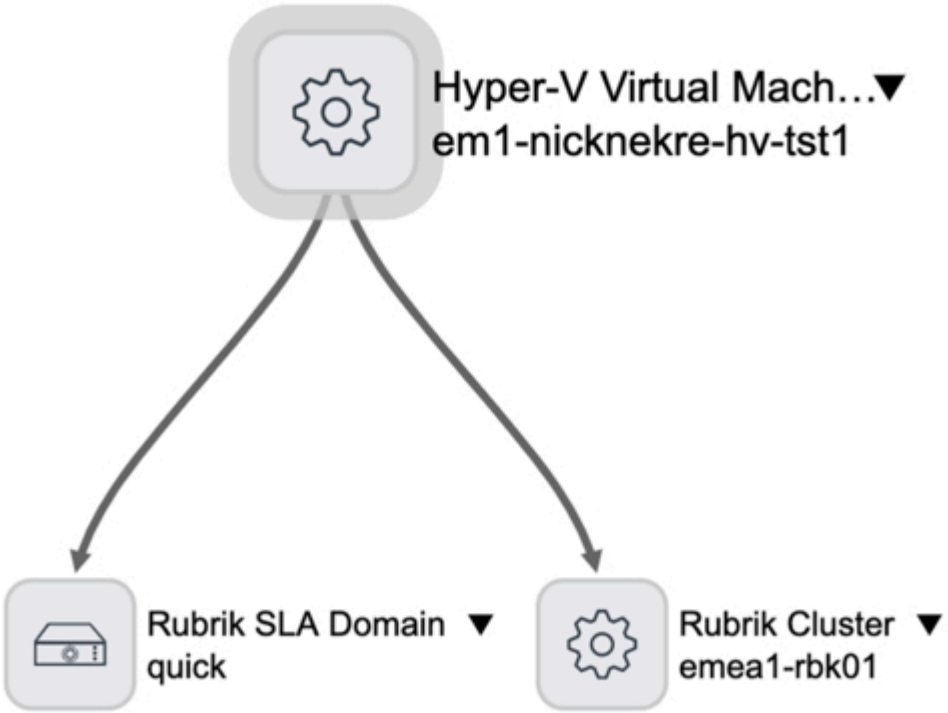
Ressourcen, die mithilfe des Musters „Rubrik Hyper-V Instance (LP)“ erkannt wurden

Hinweis: Bei der Erkennung von Hyper-V-Instanzen werden nur vorhandene CIs aktualisiert. Das liegt an einer Einschränkung in der Rubrik-REST API, die die GUID (object_id) der Hyper-V-Instanz nicht zurückgibt. Wenn keine Übereinstimmung zwischen den Daten aus der REST API und der CMDB besteht, werden keine CIs aktualisiert. Darüber hinaus wird das Muster „Rubrik Hyper-V Instance (LP)“ mit dem Status „Fehler“ abgeschlossen, wenn es keine Übereinstimmung gibt. Das ist das erwartete Verhalten.

Feld	Beschreibung
Rubrik Hyper-V-Instanz [cmdb_ci_hyper_v_instance]	
name	Name der Hyper-V-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem die Hyper-V-Instanz zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Hyper-V-Instanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

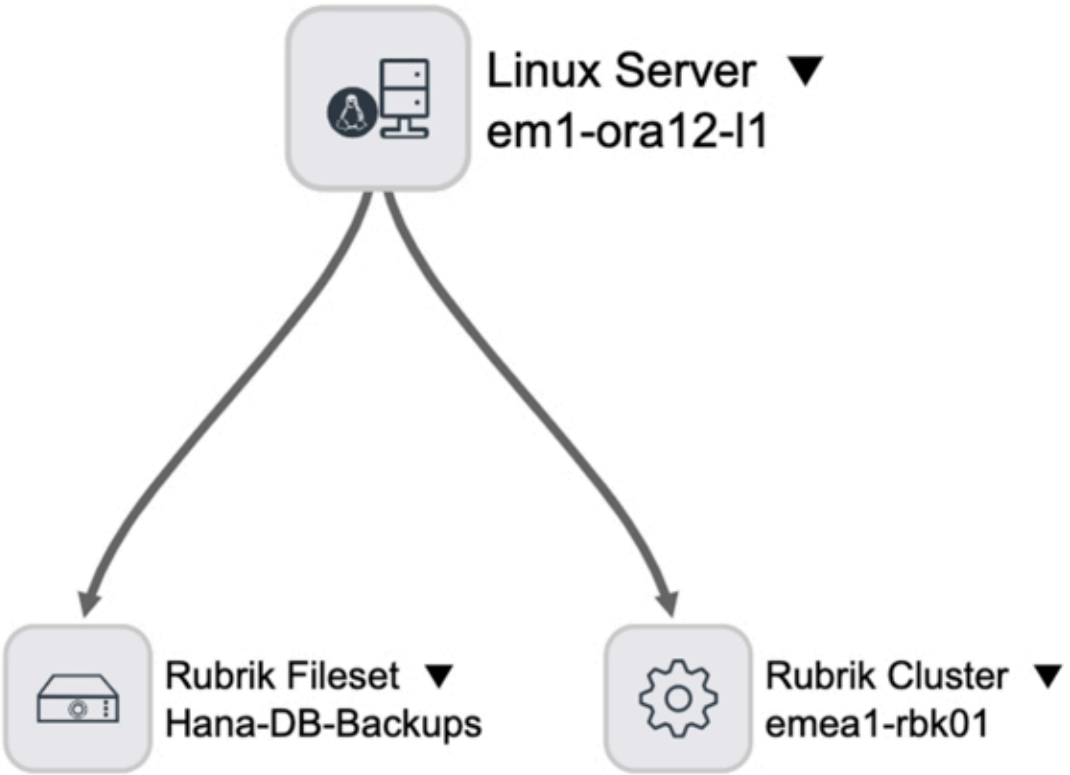


Ressourcen, die mithilfe des Musters „Rubrik Linux Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Linux-Host [cmdb_ci_linux_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

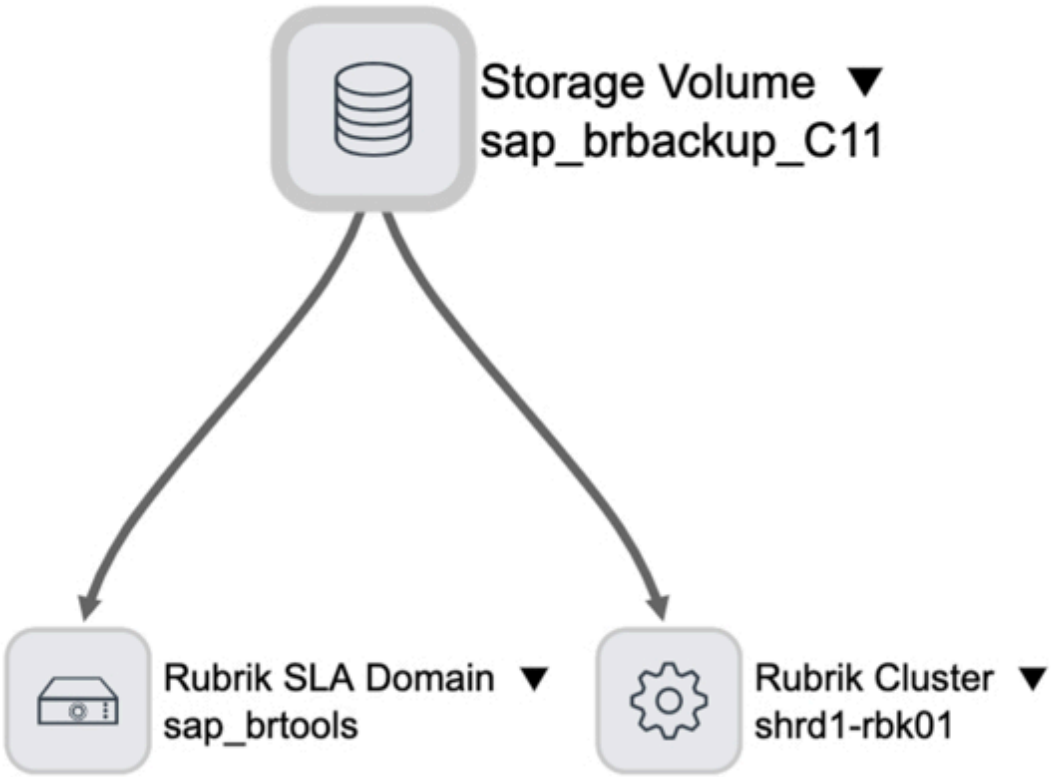


Ressourcen, die mithilfe des Musters „Rubrik Managed Volume (LP)“ erkannt wurden

Feld	Beschreibung
Verwaltetes Rubrik-Volume [cmdb_ci_storage_volume]	
object_id	ID des verwalteten Speichervolume
volume_id	Volume-ID des verwalteten Speichervolume
name	Name des verwalteten Speichervolume
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
size_bytes	Gesamtkapazität des Speichervolume in Byte
used_size_bytes	Größe der insgesamt genutzten Kapazität in Byte
snapshot_count	Snapshot-Zähler des verwalteten Speichervolume
share_type	Freigegebener Typ des verwalteten Speichervolume
state	Status des verwalteten Speichervolume

Die Dependency Views-Zuordnung zeigt die erkannten verwalteten Speicherinstanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ressourcen, die mithilfe des Musters „Rubrik MS SQL DB (LP)“ erkannt wurden

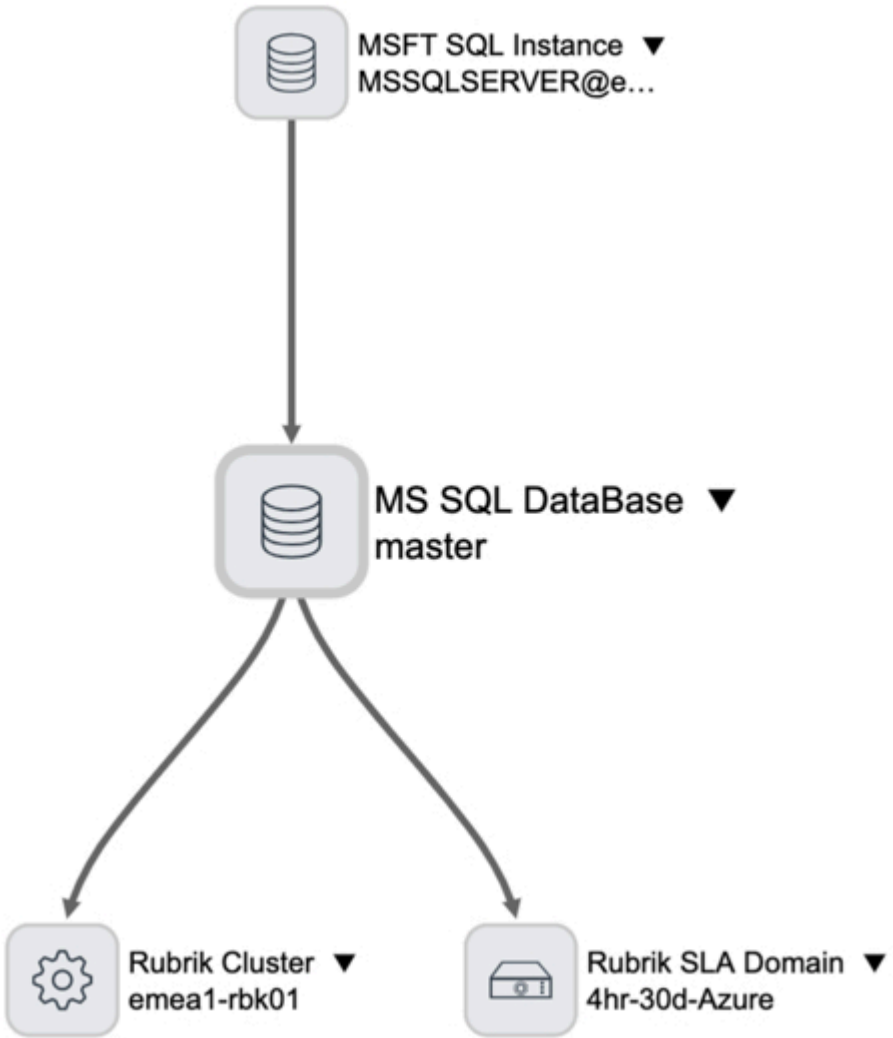
Hinweis: Beziehungen zwischen MS SQL-Instanzen, die in Windows-Clustern gehostet werden, und den zugeordneten MS SQL-Datenbanken werden ab Release 1.0.79 der Anwendung Discovery and Service Mapping Patterns nicht unterstützt. Das liegt an unzureichenden Informationen, die von der Rubrik-REST API für Windows-Cluster zurückgegeben werden. Die mit Windows-Clustern verknüpften MS SQL-Instanzen und MS SQL-Datenbanken werden aus den zugeordneten Mustern der Rubrik-Erkennung herausgefiltert.

Feld	Beschreibung
Rubrik MS SQL-DB [cmdb_ci_db_mssql_database]	
Datenbank	ID der MS SQL-Datenbank
name	Name der MS SQL-Datenbank
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, auf dem die MS SQL-Datenbank ausgeführt wird
instance_id	ID der Datenbankinstanz, der die MS SQL-Datenbank zugeordnet ist
state	Status der MS SQL-Datenbank

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
recovery_model	Typ des Wiederherstellungsmodells der MS SQL-Datenbank
last_snapshot	Letzter Snapshot der MS SQL-Datenbank im Format JJ-MM-TT HH-MM-SS
missed_snapshot_count	Anzahl der verpassten Snapshots der MS SQL-Datenbank

Die Dependency Views-Zuordnung zeigt die erkannten MS SQL-Datenbanken und deren Beziehungen untereinander.



Ressourcen, die mithilfe des Musters „Rubrik MS SQL Instance (LP)“ erkannt wurden

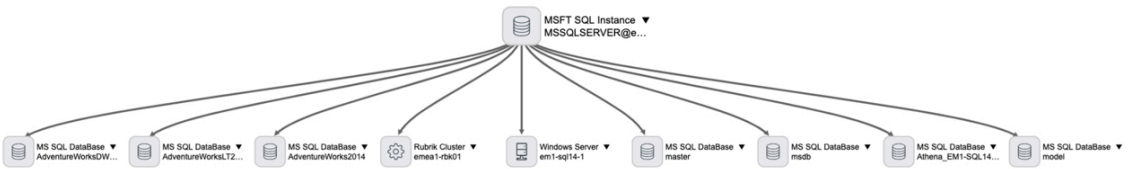
Hinweis: Beziehungen zwischen MS SQL-Instanzen, die in Windows-Clustern gehostet werden, und den zugeordneten MS SQL-Datenbanken werden ab Release 1.0.79 der Anwendung Discovery and Service Mapping Patterns nicht unterstützt. Das liegt an unzureichenden Informationen, die von der Rubrik-REST API für Windows-Cluster zurückgegeben werden. Die mit Windows-Clustern verknüpften MS SQL-Instanzen und MS SQL-Datenbanken werden aus den zugeordneten Mustern der Rubrik-Erkennung herausgefiltert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rubrik MS SQL-Instanz [cmdb_ci_db_mssql_instance]	
instance_name	ID der MS SQL-Instanz
name	Name der MS SQL-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
host_id	ID des Hosts, dem die MS SQL-Instanz zugeordnet ist
Version	Version der MS SQL-Instanz

Die Dependency Views-Zuordnung zeigt die erkannten MS SQL-Instanzen und deren Beziehungen untereinander.

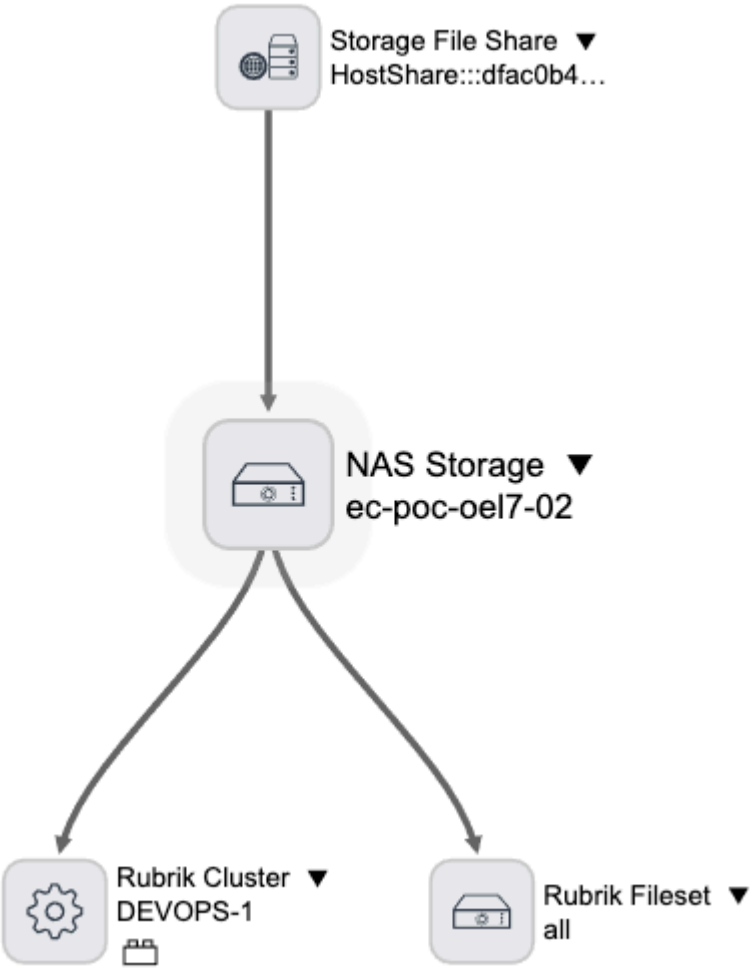


Ressourcen, die mithilfe des Musters „Rubrik NAS Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik NAS-Host [cmdb_ci_nas_storage]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
short_description	Lieferantentyp des NAS-Speichers.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ressourcen, die mithilfe des Musters „Rubrik Node (LP)“ erkannt wurden

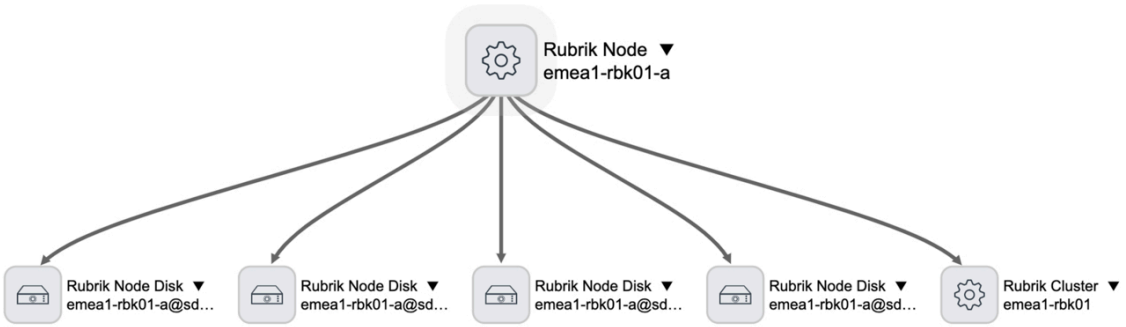
Feld	Beschreibung
Rubrik-Knoten [cmdb_ci_rubrik_node]	
brik_id	Gehäuse-ID des Rubrik-Knotens
name	Eindeutiger Name des Rubrik-Knotens, der als ID des Rubrik-Knotens dient
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
unavailable_disks	True/False. Gibt an, dass im Rubrik-Knoten nichtverfügbare Datenträger vorhanden sind
ip_address	IP-Adresse des Rubrik-Knotens, der dem Rubrik-Cluster zugeordnet ist
tunnel_enabled	True/False. Gibt an, ob für den Rubrik-Knoten Tunneling aktiviert ist
cpu_core_count	Anzahl der CPU-Kerne des Rubrik-Knotens
ram	Menge an RAM-Speicher (in MB), der für den Rubrik-Knoten reserviert ist
[cmdb_ci_rubrik_node_disk]	

Automatische Übersetzung

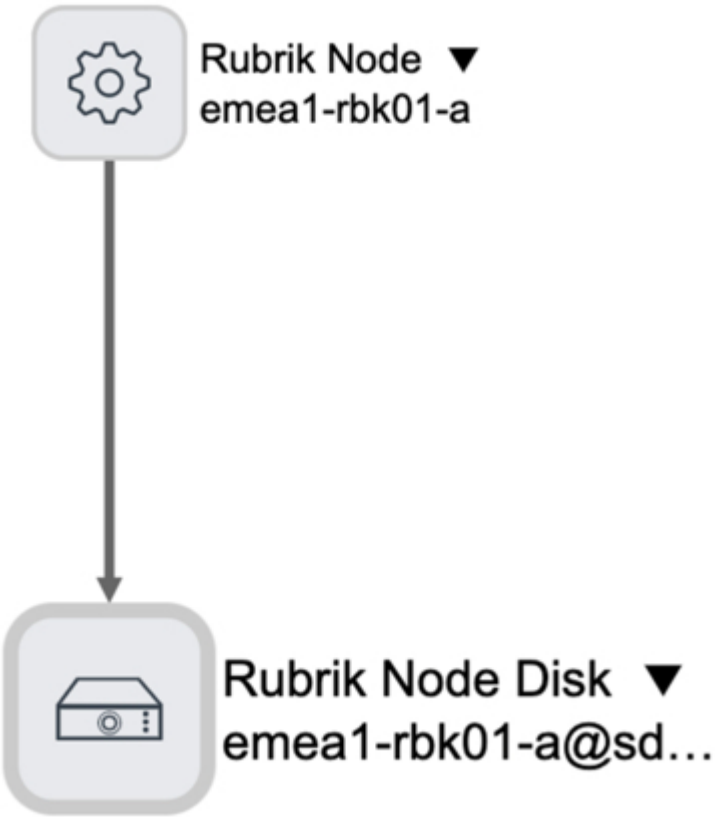
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
node_name	Name des Rubrik-Knotens, dem der Datenträger zugeordnet ist
device_id	Datenträger-ID und Name des Rubrik-Knotens, miteinander verkettet im Format ID@NODE_NAME.
name	Name des Datenträgers, der dem Rubrik-Knoten zugeordnet ist Der Name enthält die Verkettung des Rubrik-Knotennamens, die ID des Datenträgers und den Typ des Datenträgers im Format NODE_NAME@DISK_ID@DISK_TYPE.
size_bytes	Größe der Gesamtkapazität in Byte
unallocated_size_bytes	Größe der gesamten nicht zugeteilten Kapazität in Byte
usable_size_bytes	Größe der verfügbaren Gesamtkapazität in Byte
storage_type	Typ des Speicherdatenträgers: SSD oder HDD
storage_path	Verzeichnispfad des Speicherdatenträgers
operational_status	Betriebsstatus des Speicherdatenträgers

Die Dependency Views-Zuordnung zeigt die erkannten Knoten und Knotendatenträger und deren Beziehungen untereinander.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

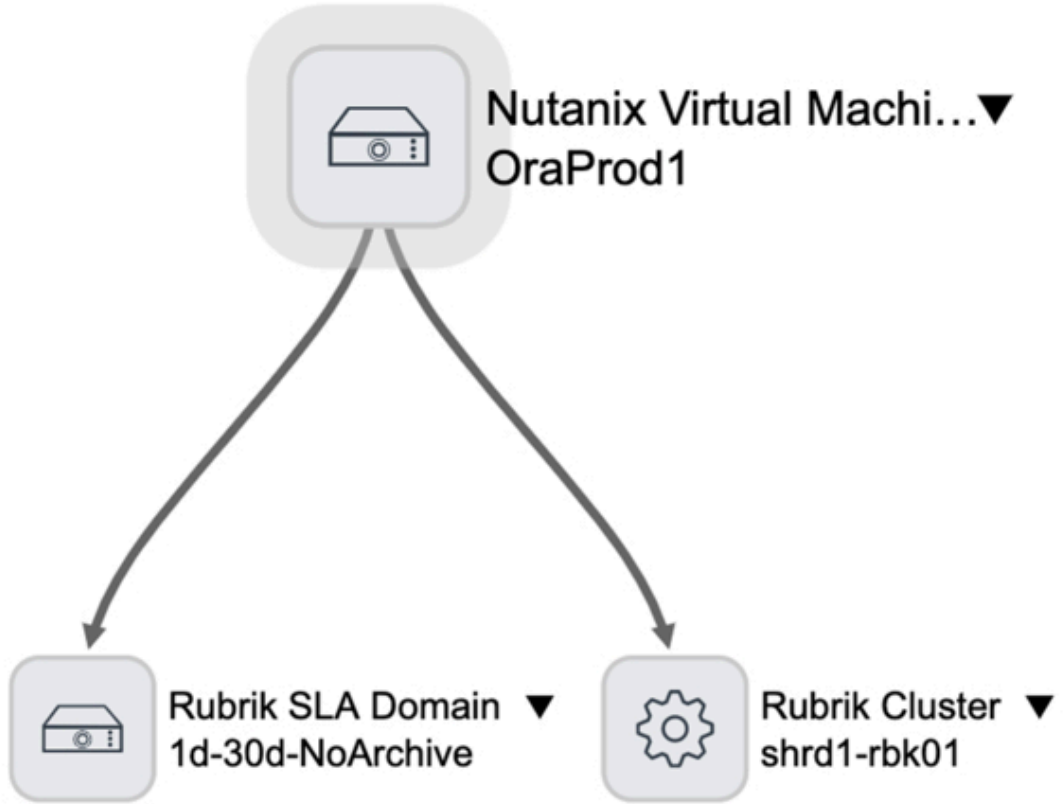


Ressourcen, die mithilfe des Musters „Rubrik Nutanix Instance (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Nutanix-Instanz [cmdb_ci_nutanix_vm_instance]	
object_id	ID der Nutanix VM-Instanz
vm_inst_id	ID der Nutanix VM-Instanz
name	Name der Nutanix VM-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
vm_cluster_id	ID des Clusters, zu dem die Nutanix VM-Instanz gehört
vm_cluster_name	Name des Clusters, zu dem die Nutanix VM-Instanz gehört
os_type	Der auf der Nutanix VM-Instanz konfigurierte Betriebssystemtyp

Die Dependency Views-Zuordnung zeigt die erkannten Nutanix-Instanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



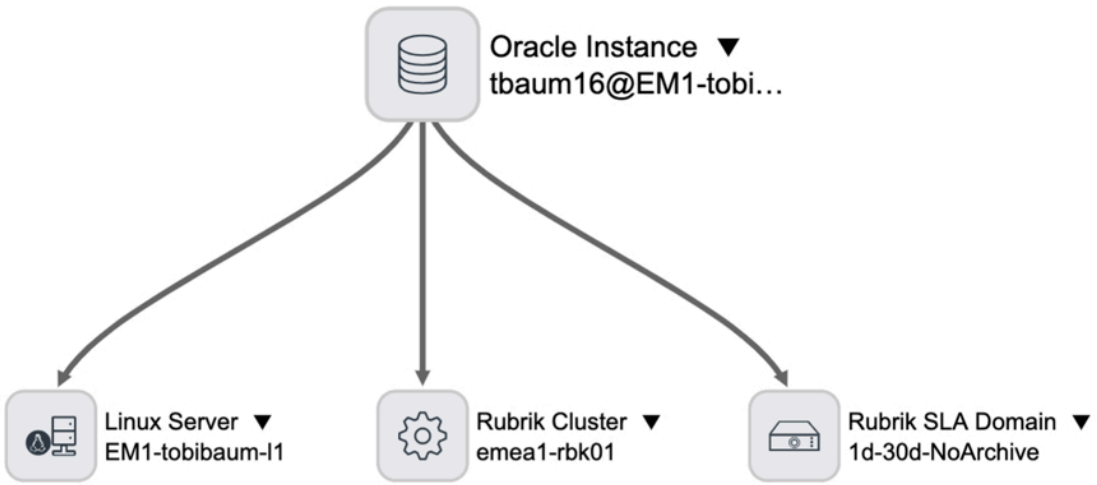
Ressourcen, die mithilfe des Musters „Rubrik Oracle DB (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Oracle-DB [cmdb_ci_db_ora_instance]	
sid	Oracle-System-ID der Datenbank
name	ID der Oracle-Datenbank im Rubrik-Kontext
database_name	Name der Oracle-Datenbank
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
rac_id	ID des Oracle RAC (Real Application Cluster), zu dem die Datenbank gehört
host_id	ID des Hosts, auf dem die Oracle-Datenbank ausgeführt wird
instance	ID der Oracle-Instanz, die die der Datenbank zugeordneten Daten verwaltet
Instance_count	Anzahl der Oracle-Instanzen, die die der Datenbank zugeordneten Daten verwalten
last_snapshot	Letzter Snapshot der Oracle-Datenbank im Format JJ-MM-TT HH-MM-SS

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
missed_snapshot_count	Anzahl der verpassten Snapshots der Oracle-Datenbank
tablespaces_count	Anzahl der logischen Speichereinheiten, die der Oracle-Datenbank zugeordnet sind

Die Dependency Views-Zuordnung zeigt die erkannten Oracle-Datenbanken und deren Beziehungen untereinander.

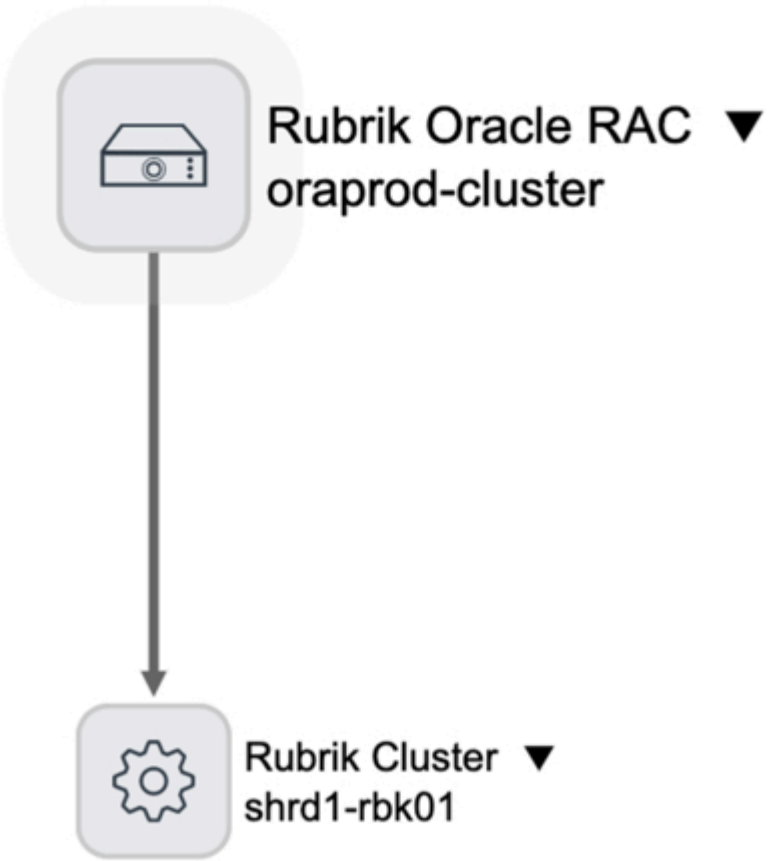


Ressourcen, die mithilfe des Musters „Rubrik Oracle RAC (Real Application Cluster) (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Oracle-RAC [cmdb_ci_rubrik_db_ora_rac]	
object_id	ID des Rubrik Oracle-RAC
name	Name des Rubrik Oracle-RAC
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
db_count	Anzahl der Datenbanken, die dem Rubrik Oracle-RAC zugeordnet sind
node_count	Anzahl der Knoten, die Teil des Rubrik Oracle-RAC sind
state	Status des Rubrik Oracle-RAC

Die Dependency Views-Zuordnung zeigt die erkannten Oracle-RACs und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

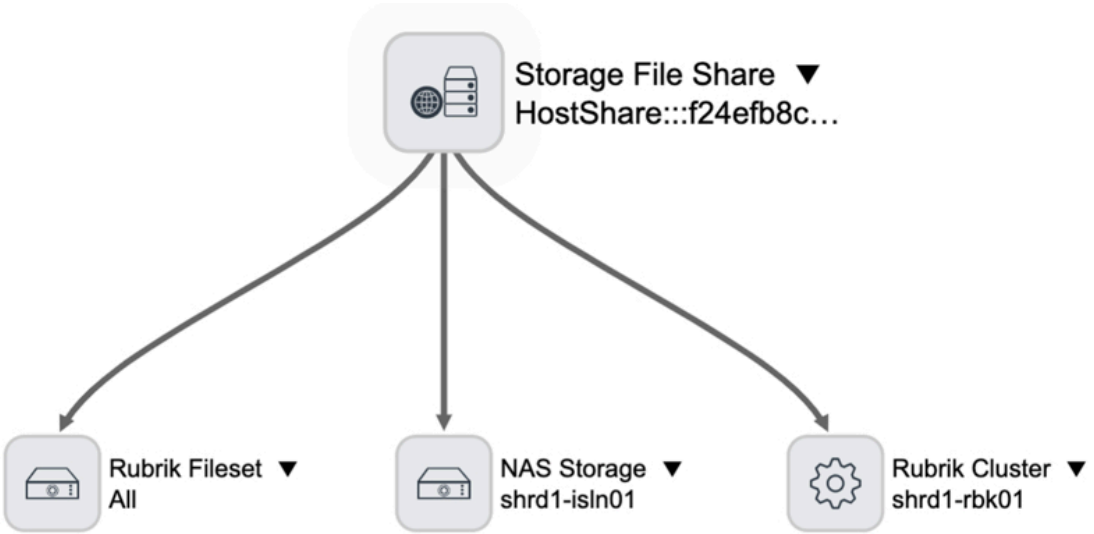


Ressourcen, die mithilfe des Musters „Rubrik Share (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Freigabe [cmdb_ci_storage_fileshare]	
name	ID der Hostfreigabe
Pfad	Exportpunkt der Hostfreigabe
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
host_id	ID des Hosts, dem die Hostfreigabe zugeordnet ist
share_type	Freigabetyp der Hostfreigabe
vendor_type	Typ des Anbieters der Hostfreigabe
Status	Aktueller Status der Hostfreigabe

Die Dependency Views-Zuordnung zeigt die erkannten Hostfreigaben und deren Beziehungen untereinander.

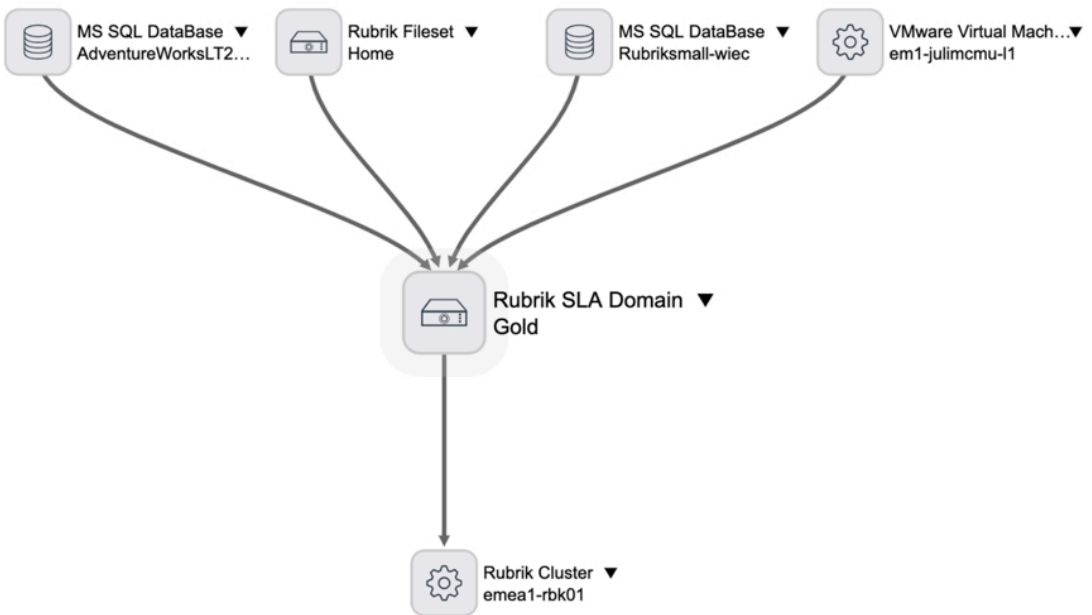
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ressourcen, die mithilfe des Musters „Rubrik SLA Domain (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-SLA-Domäne [cmdb_ci_rubrik_sla_domain]	
object_id	ID der Rubrik-SLA-Domänenrichtlinie
name	Name der Rubrik-SLA-Domänenrichtlinie
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
max_local_retention_limit	Maximale lokale Aufbewahrungsgrenze der SLA-Domänenrichtlinie

Die Dependency Views-Zuordnung zeigt die erkannten SLA-Domänen und deren Beziehungen untereinander.



Ressourcen, die mithilfe des Musters „Rubrik Solaris Host (LP)“ erkannt wurden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rubrik Solaris-Host [cmdb_ci_solaris_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

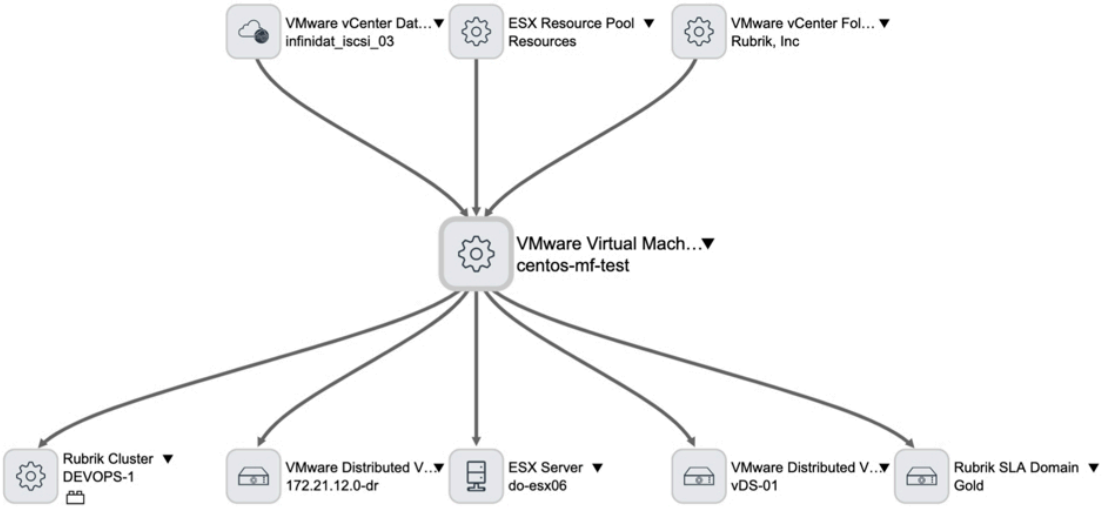
Ressourcen, die mithilfe des Musters „Rubrik VMware Instance (LP)“ erkannt wurden

Hinweis: Bei der Erkennung von VMware-Instanzen werden nur vorhandene CIs aktualisiert. Das liegt daran, dass bei der regulären vCenter-Erkennung die IRE (Identification and Reconciliation Engine) nicht verwendet wird und das Muster „Rubrik VMware“ Duplikate erzeugt. Wenn keine Übereinstimmung zwischen den Daten aus der REST API und der CMDB besteht, werden keine CIs aktualisiert. Darüber hinaus wird das Muster „Rubrik VMware Instance (LP)“ mit dem Status „Fehler“ abgeschlossen, wenn es keine Übereinstimmung gibt. Das ist das erwartete Verhalten.

Feld	Beschreibung
Rubrik VMware-Instanz [cmdb_ci_vmware_instance]	
object_id	ID der VMware-Instanz
name	Name der VMware-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Rubrik VMware-Hosts
host_name	Name des Rubrik VMware-Hosts
vm_cluster_name	Name des Clusters, zu dem die VM-Instanz gehört
ip_address	IP-Adresse der VMware-Instanz, falls zugewiesen
guest_os_fullname	Typ des Gastbetriebssystems
state	Status der VMware-Instanz

Die Dependency Views-Zuordnung zeigt die erkannten VMware-Instanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

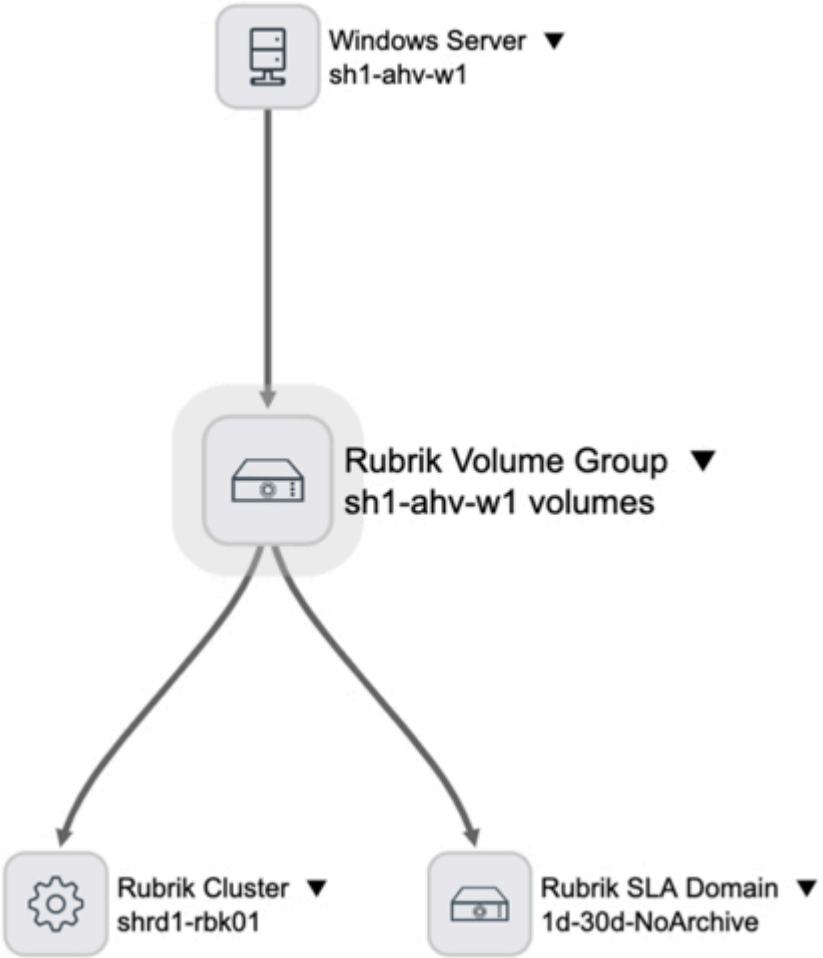


Ressourcen, die mithilfe des Musters „Rubrik Volume Group (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Volumegruppe [cmdb_ci_rubrik_volume_group]	
object_id	ID der Volumegruppe
volume_id	Volume-ID der Volumegruppe
name	Name der Volumegruppe
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem die Volumegruppe zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Volumegruppen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

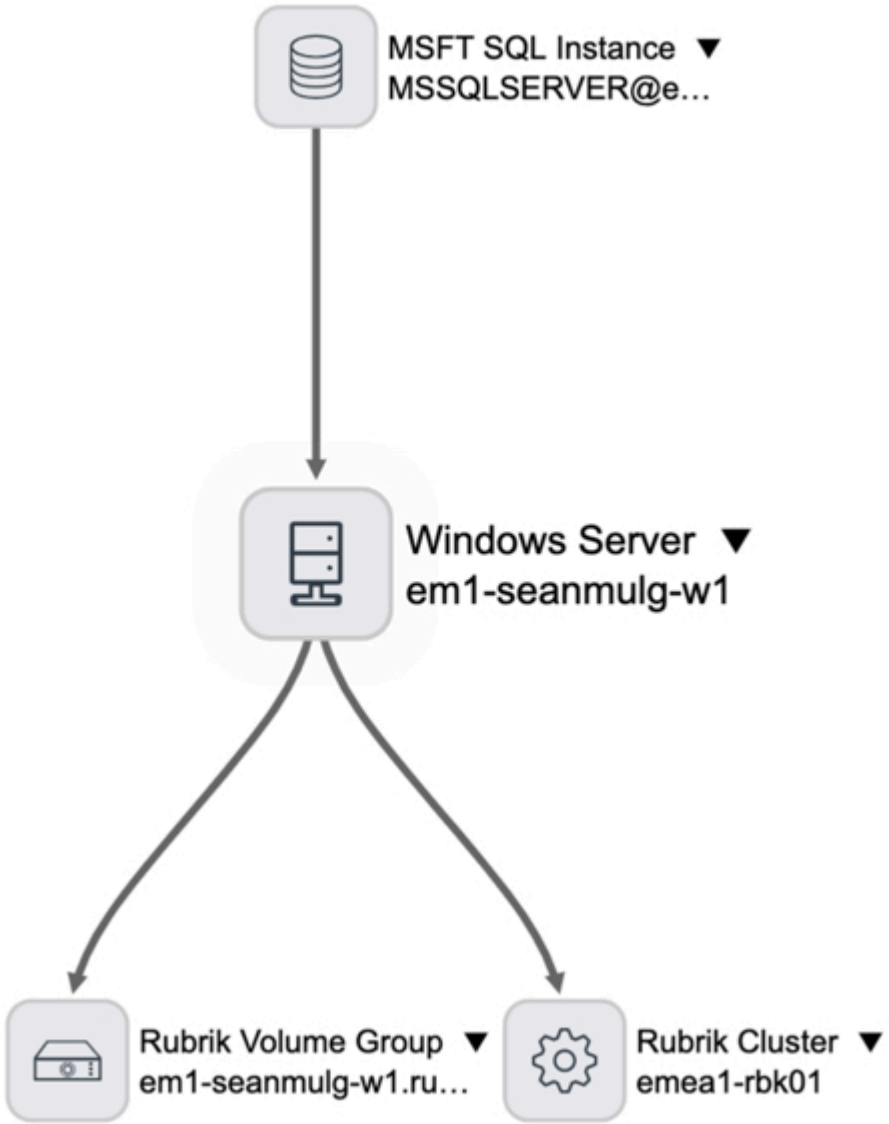


Ressourcen, die mithilfe des Musters „Rubrik Windows Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Windows-Host [cmdb_ci_win_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Ressourcen, die mithilfe des Musters „Rubrik AIX Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_aix_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik EC2 Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_vm_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_vm_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Fileset (LP)“ erkannt wurden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_server	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset
cmdb_ci_storage_fileshare	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset
cmdb_ci_rubrik_fileset_template	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_rubrik_fileset
cmdb_ci_rubrik_fileset	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_fileset	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_nas_storage	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset

Ressourcen, die mithilfe des Musters „Rubrik Fileset Template (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_fileset_template	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Hyper-V Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_hyper_v_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_hyper_v_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Linux Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_linux_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Managed Volume (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_storage_volume	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_storage_volume	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik MS SQL DB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_db_mssql_database	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_mssql_database	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_db_mssql_instance	Enthält::Enthalten in	cmdb_ci_db_mssql_database

Ressourcen, die mithilfe des Musters „Rubrik MS SQL Instance (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_db_mssql_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_mssql_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_server

Ressourcen, die mithilfe des Musters „Rubrik NAS Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nas_storage	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Node (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_node	Cluster von::Cluster	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_node	Verwendet::Verwendet von	cmdb_ci_rubrik_node_disk

Ressourcen, die mithilfe des Musters „Rubrik Nutanix Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nutanix_vm_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_nutanix_vm_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Oracle DB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_db_ora_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_ora_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_db_ora_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_server
cmdb_ci_db_ora_instance	Cluster von::Cluster	cmdb_ci_rubrik_db_ora_rac

Ressourcen, die mithilfe des Musters „Rubrik Oracle RAC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_db_ora_rac	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Share (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_storage_fileshare	Verwaltet von::Verwaltet	cmdb_ci_nas_storage
cmdb_ci_storage_fileshare	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen, die mithilfe des Musters „Rubrik SLA Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_sla_domain	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Solaris Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_solaris_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik VMware Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vmware_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_vmware_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Volume Group (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_volume_group	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_volume_group	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_server	Eigentümer von::Eigentum von	cmdb_ci_rubrik_volume_group

Ressourcen, die mithilfe des Musters „Rubrik Windows Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_win_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Erkennung von Veritas Cluster Server

Die Anwendung ServiceNow Discovery verwendet das Muster „Unix-Cluster – VERITAS Cluster“, um Veritas Cluster Server-Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können dieses Muster auf der ServiceNow AI Platform mithilfe von Kingston Patch 8, London oder Madrid verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

SSH-Anmeldeinformationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie auf ServiceNow AI Platform® die SSH-Anmeldeinformationen für einen Benutzer mit erhöhten Rechten für die Ausführung des Befehls `cat`. Weitere Informationen zu Befehlen finden Sie im Abschnitt zu Service-Mapping-Befehlen, die einen privilegierten Benutzer erfordern, in der Service-Mapping-Dokumentation.

Berechtigungen zum Lesen der Veritas Cluster Server-Konfigurationsdatei

Erteilen Sie dem Unix-Betriebssystembenutzer die Berechtigungen zum Lesen der folgenden Konfigurationsdatei: `/etc/VRTSvcs/conf/config/main.cf`.

Berechtigungen zum Ausführen von Veritas Cluster-Befehlen

Geben Sie dem Unix-Betriebssystembenutzer Berechtigungen, die folgenden Befehle gegen den Veritas Cluster-Server auszuführen:

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
“privilege user” + cat /etc/VRTSvcs/ conf/config/main.cf	-	Obligatorisch	Liest die Veritas Cluster Server-Konfigurationsdatei
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterUUID 2>/dev/ null	-	Obligatorisch	Ruft die Veritas Cluster Server-Cluster-UUID ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterName 2>/dev/ null	-	Obligatorisch	Ruft den Veritas Cluster Server-Clusternamen ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value EngineVersion	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusterversion ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterAddress	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusteradresse ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusState	-	Obligatorisch	Ruft den Veritas Cluster Server-Clusterstatus ab
“privilege user” + / opt/VRTSvcs/bin/ hasys -state	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusterknoten ab
“privilege user” + / opt/VRTSvcs/bin/ hares -state	-	Obligatorisch	Ruft die Cluster-Ressourcen des Veritas Cluster Servers ab
“privilege user” + /opt/VRTSvcs/ bin/hares -display |	-	Obligatorisch	Ruft den Cluster-Ressourcentyp des Veritas Cluster Servers ab.

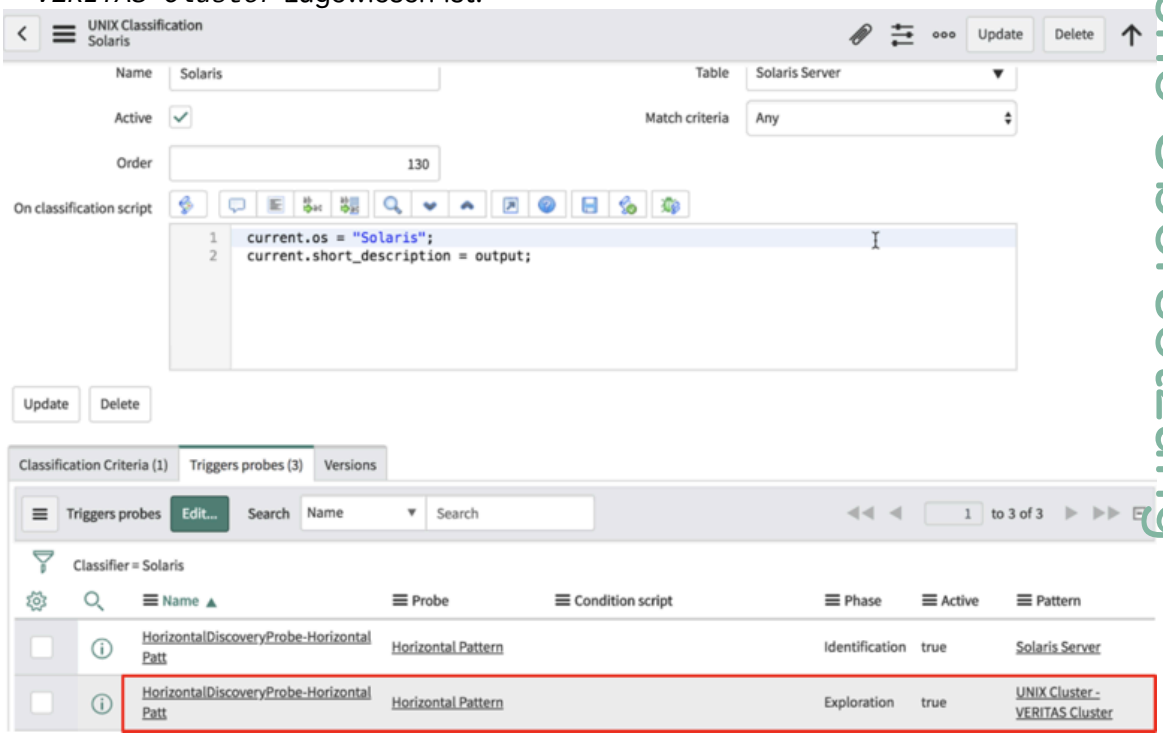
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
grep -w 'Type' |grep 'global' 2>/dev/null			
“privilege user” + / opt/VRTSvcs/bin/ hares -display | grep Group 2>/dev/null	-	Obligatorisch	Ruft die Cluster-Ressourcengruppe des Veritas Cluster Servers ab
“privilege user” + / opt/VRTSvcs/bin/ hagrp -state 2>/dev/ null	-	Obligatorisch	Ruft den Ressourcengruppennamen und Status des Veritas Cluster Servers ab

Klassifizierungs-Probe zum Auslösen des Musters „UNIX-Cluster – VERITAS Cluster“

So überprüfen Sie, ob die Klassifizierungs-Probe zum Auslösen des Musters „UNIX-Cluster – VERITAS Cluster“ festgelegt ist:

1. Navigieren zu **Discovery-Definition** > **CI-Klassifizierung** > **CI-Klassifizierung** > **UNIX**an.
2. Klicken Sie in der Liste **UNIX-Klassifizierung** auf **Solaris** oder **Linux**.
3. Überprüfen Sie auf der Registerkarte **Auslösertests**, ob die Probe *`HorizontalDiscoveryProbe-HorizontalPatt`* dem Muster *`UNIX Cluster – VERITAS Cluster`* zugewiesen ist.



Hinweis: Im Discovery-Protokoll wird der Fehler für den Schritt der Betriebssystemerkennung selbst dann angezeigt, wenn die Erkennung erfolgreich verläuft.

Systemeigenschaft für die neue Hostklasse

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie eine Systemeigenschaft [sys_property] `sa.host_classes` hinzu, und legen Sie den Wert auf cmdb_ci_unix_cluster fest. Das Erstellen einer neuen Hostklasse für Veritas Cluster-Server hilft bei der korrekten Identifizierung dieses Hosttyps.

Einschränkungen

Sie können das Muster „Unix-Cluster – VERITAS Cluster“ im Debug-Modus im Musterdesigner nicht anpassen.

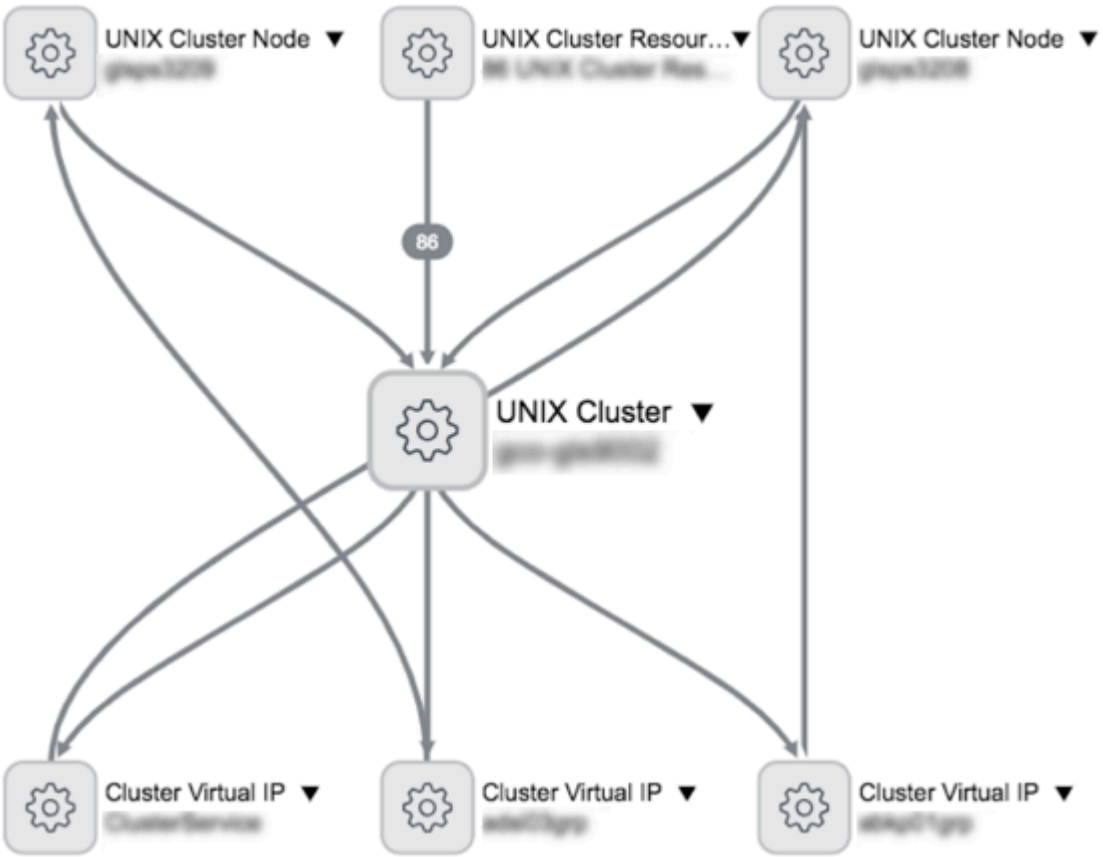
Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Unix-Cluster [cmdb_ci_unix_cluster]	Die Attribute des Unix-Clusters
IP-Adresse [ip_address]	
Clustertyp [cluster_type]	
Name [name]	
Clusterversion [cluster_version]	
Clusterstatus [cluster_status]	
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Die Attribute des Unix-Clusterknotens
Name [name]	
Cluster [cluster]	
Server [Server]	
Knotenstatus [node_status]	
IP-Adresse [ip_address]	
UNIX Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_resource_group]	Die Attribute der UNIX-Cluster-Ressourcengruppe
Name [name]	
Knoten [node]	
Server [Server]	
Cluster [cluster]	
Ressourcengruppenstatus [resource_group_status]	
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Die Attribute der UNIX-Cluster-Ressource
Ressourcentyp [resource_type]	
Name [name]	
Ressourcenstatus [resource_status]	
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Die Attribute der Cluster virtuellen IP-Adressen
IP-Adresse [ip_address]	
Name [name]	
Cluster [cluster]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Clusterstatus [cluster_status]	
Knoten [node]	

Die Grafik stellt CIs dar, die Teil der Veritas Cluster Server-Erkennung sind.



CI-Beziehungen

Das Muster „Unix Cluster – VERITAS Cluster“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet: Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Hostet: Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Virtualisiert von: Virtualisiert	Unix-Cluster [cmdb_ci_unix_cluster]
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Verwendet: Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von: Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für: Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für: Erhält Ressourcen von	Das Clusterfeld auf [cmdb_ci_unix_cluster]
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Das Clusterfeld auf UNIX-Cluster [cmdb_ci_unix_cluster]
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Das Knotenfeld auf Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Unix-Clusterressource [cmdb_ci_unix_cluster_resource]

VMware NSX Erweiterte Discovery des Lastenausgleichsmoduls

Die ServiceNow Discovery Die Anwendung verwendet das Discovery-Muster des VMware NSX Advanced Load Balancer, um zu finden VMware NSX Lastenausgleichsmodule. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Muster verwendet eine Reihe von REST-APIs, um die Lastenausgleichsmodule zu finden. Wird durch ausgelöst NSX HTTP-Klassifizierer, der auf antwortet **HTTP: Klassifizieren** Probe. Weitere Informationen finden Sie unter Erkennung von HTTP-Geräten.

Hinweis: Es sind zwei Muster verfügbar. Das veraltete Muster „VMware NSX Load Balancer“ gilt für die S-Serie. Das neue Muster „VMware NSX-T Load Balancer“ ist für die T-Serie. Die Funktionalität und die erfassten Informationen bleiben unverändert.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Aktivieren NSX Standardauthentifizierung

In VMware NSX, Aktivieren NSX Standardauthentifizierung.

Überprüfen Sie, ob die Anwendungen aktuell sind

- CMDB CI-Klassenmodelle
- Visibility Content
- Muster für Discovery und Service-Mapping

Konfigurieren Sie Anmeldeinformationen für Standardauthentifizierung

Auf der ServiceNow AI Platform, Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung. Die Anmeldeinformationen müssen über die folgenden API-Berechtigungen verfügen:

- NSX:
  - /api/4.0/edges
  - /api/4.0/edges/<edge_id>loadbalancer/config
- NSX-T: /api/v1/Edge-Cluster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Anmeldeinformationen für die Standardauthentifizierung finden Sie unter Virtual Server Interface .

Überprüfen Sie, ob die HTTP-Discovery für ausgelöst wird NSX Haupt-Controller-IP

Die HTTP-Discovery wird nur ausgelöst, wenn die SSH- oder SNMP-Discovery nicht erfolgreich ist.

Erkennungszeitpläne erstellen

Erstellen Sie den Discovery-Zeitplan für VMware NSX Load Balancer-Discovery, oder führen Sie eine schnelle Discovery für die IP-Adresse des aus NSX Haupt-Controller. Weitere Informationen zum Ausführen einer schnellen Discovery finden Sie unter Schnell-Discovery ausführen.

Daten erfasst von Discovery Für VMware NSX Erweiterter Lastenausgleichsmodul

Discovery Füllt die Daten in aus CMDB Beim Ausführen der Muster des erweiterten VMware NSX-Lastenausgleichsmoduls.

NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]

Feld	Beschreibung
Name [name]	Edge-Name
Objekt-ID [object_id]	Edge-ID
IP-Adresse [ip_address]	IP-Adresse des NSX Haupt-Controller.
Betriebsstatus [operational_status]	Lastenausgleichsmodulstatus: aktiv oder inaktiv

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des virtuellen Servers
IP-Adresse [ip_address]	IP-Adresse des virtuellen Servers
Objekt-ID [object_id]	Objekt-ID des virtuellen Servers
Port [port]	Virtueller Serverport, mit dem kommuniziert werden soll
Listener-Protokoll [listener_Protocol]	Listenerprotokoll. Beispiel: HTTP, HTTPS

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Poolname.
Objekt-ID [object_id]	Poolobjekt-ID

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Poolmitgliedsname
IP-Adresse [ip_address]	Poolmitglieds-IP-Adresse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

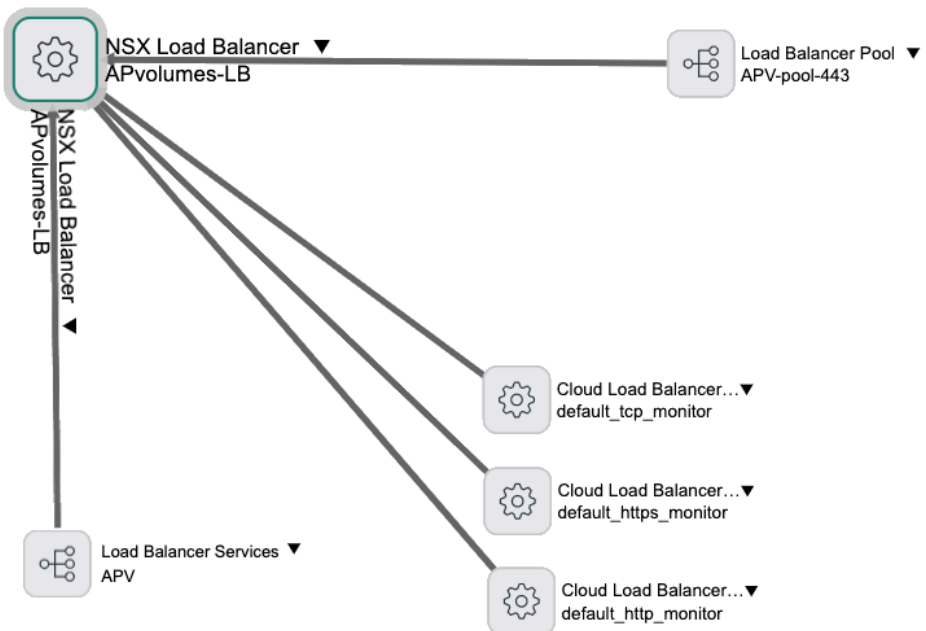
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Poolmitgliedsobjekt-ID
Service-Port [Service_Port]	Poolserverport, mit dem kommuniziert werden soll

Cloud-Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_Health_Service]

Feld	Beschreibung
Name [name]	Name des Monitors
Objekt-ID [object_id]	Objekt-ID des Monitors
Zeitüberschreitung in Sekunden [timeout_sec]	Zeit in Sekunden, die auf eine Antwort gewartet wird
Intervall in Sekunden [Check_interval_sec]	Intervall in Sekunden, nach dem der Monitor die Anforderung erneut sendet
Überwachungstyp-Protokoll [Monitor_type]	Monitortyp. Beispiel: HTTP, HTTPS, TCP
Anforderungspfad [Request_path]	Pfad, an den der Monitor die Anforderung sendet
Max. Wiederholungen [max_retries]	Die maximale Häufigkeit, mit der die Ressource getestet wird, bevor sie als „inaktiv“ deklariert wird.

Die Dependency Views-Zuordnung zeigt alle erkannten Lastenausgleichsmodul-CIs und ihre Beziehungen untereinander.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von VMware NSX Lastenausgleichsmodul-Discovery.

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]
Load Balancer-Service [cmdb_ci_lb_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Cloud-Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_Health_Service]	Gehostet auf::Hostet	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]
Cloud-Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_Health_Service]	Verwendet von::Verwendet	Load Balancer-Pool [cmdb_ci_lb_pool]

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Debugging auf (und nicht während der Discovery).	Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Verfügbare Cloud-Discovery-Muster

ITOM-Transparenz Enthält eine umfangreiche Bibliothek von Mustern, die Ihre Cloud-Umgebung erkennen können: AWS, Azure, GCP, IBM und OCI.

ServiceNow veröffentlicht monatlich neue Discovery-Muster im ServiceNow Store , um sicherzustellen, dass Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann. Hauptversionen von ServiceNow enthalten Muster, die zuvor im ServiceNow Store veröffentlicht wurden.

Eine vollständige Liste der Geräte und Anwendungen, die ITOM-Transparenz erkennen kann, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

AWS Discovery mithilfe von Mustern

Muster für Discovery und Service-Mapping Verwendet Muster, um Komponenten von zu erkennen Amazon AWS Cloud Bereitstellung während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind :

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Methode für Punkterkennung für AWS CFT-Stapel aktualisieren

Wenn Sie verwenden Cloud Provisioning and Governance, Sie müssen aktualisieren `getOperationGR(type)` Methode. Diese Aktualisierung stellt sicher, dass die Punkterkennung die Ressourcen für den AWS CloudFormation Template (CFT)-Stapel nach der Bereitstellung korrekt auflistet. Weitere Informationen zu den Schritten, die zum Aktualisieren dieser Methode erforderlich sind, finden Sie unter Knowledge Base Artikel KB0858437 .

Servicekonto in der AWS-Verwaltungskonsole

Eine AWS-Organisation ist eine Sammlung von AWS-Konten unter einem einzelnen Konto. Cloud-Discovery verweist auf AWS-Organisationen im Assistenten als *Verwaltungskonten*. Die Mitgliedskonten, die zu einem Verwaltungskonto gehören, werden als *Unterkonten* bezeichnet.

Hinweis: Cloud-Discovery Für AWS Organisationen werden in nicht vollständig unterstützt GovCloud Isolierte Region.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Verwendung von Verwaltungskonten hat folgende Vorteile:

Einfaches Füllen von Unterkonten

Nachdem Sie das Verwaltungskonto konfiguriert und die erforderlichen Anmeldeinformationen angegeben haben, können Sie die Verbindung mit dem Konto testen. Wenn der Test erfolgreich ist, Discovery Gibt eine Liste der Mitglieds-Accounts in diesem Verwaltungs-Account zurück. In dieser Liste können Sie mindestens ein Unterkonto auswählen, das in die Discovery des Verwaltungskontos aufgenommen werden soll.

(Optional für die Erkennung der gesamten AWS-Organisation) Erkennung von Unterkontenressourcen mithilfe dynamisch bezogener Anmeldeinformationen

Wenn Sie ausführen Discovery In Ihren Cloud-Ressourcen benötigen Sie nicht separate Anmeldeinformationen für jedes Unterkonto. Die Cloud-Discovery Prozess verarbeitet Anmeldeinformationen automatisch, indem über einen temporäre Anmeldeinformationen für jedes Unterkonto erworben werden AWS API. Sie können die Standardkonfiguration verwenden oder den MID-Server anpassen, um andere Rollen für zusätzliche Steuerungen und Sicherheitseinstellungen zu übernehmen.

IAM-Benutzerrichtlinie in der AWS-Verwaltungskonsole

Um während der Discovery die IAM-Anwenderrichtlinie anstelle von Anmeldeinformationen zu verwenden, konfigurieren Sie MID-Server Für AWS IAM-Rollen. Weitere Informationen finden Sie unter Konfigurieren Sie den MID-Server für AWS IAM-Rollen .

Normalerweise erstellen Sie die IAM-Benutzerrichtlinie für die Bereitstellung von AWS-Ressourcen in Cloud Provisioning and Governance, wie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern beschrieben. Stellen Sie sicher, dass die IAM-Benutzerrichtlinie die folgenden AWS-Ressourcen abdeckt:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
      "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeLoadBalancerPolicies",
      "elasticloadbalancing:DescribeInstanceHealth",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeLoadBalancerAttributes",
      "account:ListRegions",
      "elasticloadbalancing:Describe*",
      "ec2:Describe*",
      "ec2:DescribeNetworkInterfaceAttribute",
      "ec2:DescribeInstanceStatus",
      "ec2:DescribeCustomerGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeHosts",
      "ec2:DescribeImages",
      "ec2:DescribeVpcs",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeInstanceCreditSpecifications",

         ],
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
}
```

Zugriff auf AWS-Ressourcen konfigurieren

Um einen einzelnen Account zu erkennen, erstellen Sie im einen IAM-Account AWS Verwaltungskonsole und stellen Sie sicher, dass die Richtlinie „schreibgeschützter Zugriff“ angewendet wird. Um mehrere Mitglieds- oder untergeordnete Accounts zu erkennen, konfigurieren Sie die Anmeldeinformationen wie in beschrieben Zugriff für AWS-Servicekonten einrichten.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Support für AWS Services in der Region China

Die neueste Version von Muster für Discovery und Service-Mapping Unterstützt die Erkennung AWS Services in der Region China. Sie können diese Services in erkennen ServiceNow AI Platform, Beginnend ab Xanadu Patch 3 und Washington DC Patch 9-Instanzen.

Wird Erkannt AWS Services in der Region China erfordern die Verwendung einer Rechenzentrums-URL beim Einrichten von AWS Service-Account. Beispiel: `https://organizations.cn-northwest-1.amazonaws.com.cn` .

- Um mehr über zu erfahren AWS Master-Account- und Unteraccount-Support in der Region China, siehe KB1704526 .
- Zu identifizieren AWS In der Region China unterstützte Muster finden Sie in der Tabelle „Cloud Discovery-Muster“. Die **AWS – Support für Region China** Spalte hat den Wert „Ja“ für unterstützte Muster.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Amazon AWS - ACL (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk-ACL [cmdb_ci_network_acl]

Feld	Beschreibung
Name [name]	Name der Netzwerk-Zugriffssteuerungsliste (ACL)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

ACL-Endpunkt [cmdb_ci_Endpoint_acl]

Feld	Beschreibung
Name [name]	Name des Endpunkts.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Ressourcen, die mithilfe des Musters „Amazon AWS - Application and Network LB (LP)“ erkannt wurden

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmoduls
Vollständig qualifizierter Domänenname [fqdn]	IP-Adresse des vollständig qualifizierten Domänennamens des Lastenausgleichsmoduls.
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) des Lastenausgleichsmoduls
DNS-Name [dns_name]	Der öffentliche DNS-Name des Lastenausgleichmoduls
Name der kanonischen gehosteten Zone [canonical_hosted_zone_name]	Name der gehosteten Amazon Route 53-Zone, die dem Lastenausgleichsmodul zugeordnet ist.
ID der kanonischen gehosteten Zone [canonical_hosted_zone_id]	ID der gehosteten Amazon Route 53-Zone, die dem Lastenausgleichsmodul zugeordnet ist.
Status [state]	Der Status des Lastenausgleichsmoduls
Kurzbeschreibung [short_description]	Eine Verkettung einer Reihe von Attributen für die Lastenausgleichsmodule wie LB ARN, VPC ID, Typ und Zone
Kommentare [comments]	Bezeichner zur internen Verwendung (Löschungsstrategie)

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
Objekt-ID [object_id]	Name des DNS.
IP-Adresse [ip_address]	IP-Adresse des DNS.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DNS-Name [cmdb_ci_dns_name] (Fortsetzung)

Feld	Beschreibung
Kommentare [comments]	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Amazon AWS - Availability Zone (LP)“ erkannt wurden

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Status [state]	Der Status der Verfügbarkeitszone. Mögliche Werte: available, information, impaired und unavailable.

Ressourcen, die mithilfe des Musters „Amazon AWS - Classic LB (LP)“ erkannt wurden

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Name [name]	Der Name des Lastenausgleichsmoduls
Vollständig qualifizierter Domänenname [fqdn]	Der DNS-Name des Lastenausgleichmoduls
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
DNS-Name [dns_name]	Der DNS-Name des Lastenausgleichmoduls
Name der kanonischen gehosteten Zone [canonical_hosted_zone_name]	Der DNS-Name des Lastenausgleichmoduls
ID der kanonischen gehosteten Zone [canonical_hosted_zone_id]	ID der gehosteten Amazon Route 53-Zone für das Lastenausgleichsmodul.

Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]

Feld	Beschreibung
Name [name]	IP-Adresse des Lastenausgleichsmoduls.
Objekt-ID [object_id]	IP-Adresse des Lastenausgleichsmoduls.
IP-Adresse [ip_address]	IP-Adresse des Lastenausgleichsmoduls.
Kommentare [comments]	Kommentare im Zusammenhang mit dem Configuration Item (CI).

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DNS-Name [cmdb_ci_dns_name] (Fortsetzung)

Feld	Beschreibung
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools von Lastenausgleichsmodulen
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Der Name des Mitglieds des Lastenausgleichsmodul-Pools (bekannt in AWS Als Ziel).
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmodul-Services
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Port [port]	Der Port, den das Lastenausgleichsmodul abhört
Serviceport [service_port]	Der Port, den die Instanz abhört
Serverprotokoll [service_protocol]	Das für die Weiterleitung von Datenverkehr an Instanzen zu verwendende Protokoll: HTTP, HTTPS, TCP oder SSL
Listener-Protokoll [service_protocol]	Das Transportprotokoll des Lastenausgleichsmoduls, das zur Weiterleitung verwendet wird: HTTP, HTTPS, TCP oder SSL
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Mithilfe des Musters „Amazon AWS – LB Pool Member(LP)“ erkannte Ressourcen

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Ziel-ID, abhängig vom Zieltyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member] (Fortsetzung)

Feld	Beschreibung
	Beispiel: Instanz-ID, IP-Adresse, Lambda-ARN oder Anwendungslastenausgleichsmodul-ARN.
Service-Port [Service_Port]	Der Port, auf dem das Ziel abhört, falls verfügbar.
Objekt-ID [object_id]	Mögliche Werte: • Ziel-ID • Ziel-ID und Zielport, falls verfügbar, im folgenden Format: `<target ID>#<target port>` . Beispiel: `i-0123456789abcdef0#8080`
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.
Betriebsstatus [operational_status]	Betriebsstatus des Ziels. Mögliche Werte sind „betriebsbereit“ oder „nicht funktionsfähig“.
Installationsstatus [install_status]	Installationsstatus des Ziels. Mögliche Werte sind „installiert“ oder „deaktiviert“.
Pool [pool]	Verweist auf die Tabelle „Lastenausgleichsmodul-Pool“ [cmdb_ci_lb_Pool].

Hinweis: Standardmäßig führt das Muster „Amazon AWS – LB Pool Member(LP)“ keine Discovery aus. Um die Discovery von zu aktivieren AWS Anwendungslastenausgleichsmodul-Ziele festlegen `sn_itom_pattern.discover_aws_app_pool_members` MID-Server Eigenschaft bis **Wahr** . Weitere Informationen finden Sie unter Aktivieren AWS Ziel-Discovery des Anwendungslastenausgleichsmoduls.

Ressourcen, die mithilfe des Musters „Amazon AWS - Customer Gateway (LP)“ erkannt wurden

Kunden-Gateway [cmdb_ci_customer_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn beim Kunden-Gateway kein Name angegeben ist
Objekt-ID [object_id]	ID des Kunden-Gateways
Verbindungstyp [connection_type]	Typ der vom Kunden-Gateway unterstützten VPN-Verbindung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kunden-Gateway-Endpunkt [cmdb_ci_Endpoint_CUST_Gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn beim Kunden-Gateway kein Name angegeben ist
Objekt-ID [object_id]	ID des Kunden-Gateways

Mithilfe von erkannte Ressourcen Amazon AWS– Organisationsmuster erkennen

Cloud-Organisationen [cmdb_ci_Cloud_org]

Feld	Beschreibung
Name [name]	Der eindeutige Bezeichner (ID) des Management-Accounts einer Organisation.
Objekt-ID [object_id]	Der eindeutige Bezeichner (ID) des Management-Accounts einer Organisation.
Stamm-ID [root_ID]	Der eindeutige Bezeichner (ID) einer Organisation.
Master-E-Mail [Master_email]	Die E-Mail-Adresse, die dem zugeordnet ist AWS Account, der als Verwaltungsaccount für die Organisation festgelegt ist.
Installationsstatus [install_status]	Der Installationsstatus der Organisation basierend auf dem Status AvailablePolicyTypes.
Betriebsstatus [operational_status]	Der Betriebsstatus der Organisation basierend auf dem Status „Verfügbare PolicyTypes“.

Ressourcen, die mithilfe des Musters „Amazon AWS - Executable Template (LP)“ erkannt wurden

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Beispiel: **CentOS 7.0-64 minimal für VSI** .
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Gerätename des Root-Gerätevolumes (beispielsweise /dev/sda1)
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abschnitt „Mustererweiterung“ erkennt Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für virtuelle Windows-Maschinen (VMs) und RHEL-VMs.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel ist eine der folgenden Optionen: • Windows_OS_License_Type_Automatic • RHEL_OS_License_Type_Automatic
Wert [value]	Der Wert ist eine der folgenden Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist `Image`Oder `Cloud Image`.

Ressourcen, die mithilfe von erkannt wurden Amazon AWS– Muster des Hardwaretyps (LP)

Hardwaretyp [cmdb_ci_compute_template]

Feld	Beschreibung
Name [name]	Name dieses Image
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kern [core]	Die Standardanzahl der Kerne für den Instanztyp
Arbeitsspeicher MB [Memory_mb]	Speichergröße, die dieser Vorlage zugewiesen ist
vCPIs [vCPUs]	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne
Lokaler Speicher – GB [local_storage_gb]	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

Ressourcen, die mithilfe von erkannt wurden Amazon AWS– Host-Muster (LP)

Cloud-Host [cmdb_ci_Cloud_Host]

Feld	Beschreibung
Name [name]	Name dieses Hosts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Host [cmdb_ci_Cloud_Host] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Anzahl CPU-Kerne [cpu_core_count]	Anzahl der Hostkerne
Status [state]	Aktueller Status des Hosts
Hosttyp [host_type]	Typ des Hosts (instanceFamily)
Cloud-Anbieter [cloud_vendor]	Anbieter der Cloud: AWS
Virtuell [virtual]	Virtueller Host: False

Ressourcen, die mithilfe des Musters „Amazon AWS - Internet Gateway (LP)“ erkannt wurden

Internet-Gateway [cmdb_ci_internet_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Internet-Gateway kein Name angegeben ist.
Objekt-ID [object_id]	ID des Internet-Gateways

Internet-Gateway-Endpunkt [cmdb_ci_Endpoint_intGateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Internet-Gateway kein Name angegeben ist.
Objekt-ID [object_id]	ID des Internet-Gateways

Ressourcen, die mithilfe des Musters „Amazon AWS - IP Address (LP)“ erkannt wurden

IP-Adresse [cmdb_ci_cloud_ip_address]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
IP-Adresse [ip_address]	Falls verfügbar, die Adresse der Elastic-IP-Adresse, die an die Netzwerkschnittstelle gebunden ist. Wenn nicht verfügbar, die private IP.
Objekt-ID [object_id]	Die ID der Netzwerkschnittstelle
Öffentlicher DNS [public_dns]	Der öffentliche DNS-Name, falls verfügbar

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adresse [cmdb_ci_cloud_ip_address] (Fortsetzung)

Feld	Beschreibung
Private IP-Adresse [private_ip]	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
Instanz-ID [instance_id]	Die ID der Instanz

Ressourcen, die mithilfe von erkannt wurden Amazon AWS– Schlüsselpaar-Muster (LP)

Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]

Feld	Beschreibung
Name [name]	Der Name des Schlüsselpaars
Objekt-ID [object_id]	Die ID des Schlüsselpaars
Fingerabdruck [finger_print]	Wenn Sie verwendet haben KeyPair erstellen Zum Erstellen des Schlüsselpaars ist dieser Wert der SHA-1-Digest des DER-codierten privaten Schlüssels. Wenn Sie ImportKeyPair für die Bereitstellung verwendet haben AWS Der öffentliche Schlüssel. Dieser Wert ist der Fingerabdruck des öffentlichen MD5-Schlüssels, wie in Abschnitt 4 von RFC 4716 angegeben.

Ressourcen, die mithilfe des Musters „Amazon AWS - LB Pool (LP)“ erkannt wurden

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools von Lastenausgleichsmodulen
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Ressourcen, die mithilfe des Musters „Amazon AWS - LB Service (LP)“ erkannt wurden

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmodul-Services
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Port [port]	Der Port, den das Lastenausgleichsmodul abhört
Serviceport [service_port]	Der Port, den die Instanz abhört
Serverprotokoll [service_protocol]	Das für die Weiterleitung von Datenverkehr an Instanzen zu verwendende Protokoll: HTTP, HTTPS, TCP oder SSL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer-Service [cmdb_ci_lb_service] (Fortsetzung)

Feld	Beschreibung
Listener-Protokoll [service_protocol]	Das Transportprotokoll des Lastenausgleichsmoduls, das zur Weiterleitung verwendet wird: HTTP, HTTPS, TCP oder SSL
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Ressourcen, die mithilfe des Musters „Amazon AWS - NAT Gateway (LP)“ erkannt wurden

NAT-Gateway [cmdb_ci_nat_gateway]

Feld	Beschreibung
Name [name]	Name des NAT-Gateways
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Installationsstatus [install_status]	Bereitstellungsstatus des NAT-Gateway.

NAT-Endpunkt [cmdb_ci_Endpoint_nat]

Feld	Beschreibung
Name [name]	Der Name des NAT-Endpunkts
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Ressourcen, die mithilfe des Musters „Amazon AWS - Network (LP)“ erkannt wurden

Cloud-Netzwerk [cmdb_ci_network]

Feld	Beschreibung
Name [name]	Name des VPC-Netzwerks (Virtual Private Cloud)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Status [state]	Der aktuelle Status der VPC: ausstehend (pending) oder verfügbar (available).
CIDR [cidr]	CIDR-Darstellung des Subnetzes. Beispiel: 10.0.0.0/24
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Amazon AWS - NIC (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
Objekt-ID [object_id]	Die ID der Netzwerkschnittstelle
Status [state]	Der Status der Netzwerkschnittstelle Gültige Werte: verfügbar (available), zugeordnet (associated), hängt an (attaching), in Gebrauch (in-use) oder trennt (detaching).
Private IP [private_ip]	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
IP-Adresse [ip_address]	Falls verfügbar, die Adresse der Elastic-IP-Adresse, die an die Netzwerkschnittstelle gebunden ist. Wenn nicht verfügbar, die private IP.
Öffentliche IP [public_ip]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist

Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]

Feld	Beschreibung
Name [name]	IP-Adresse des Lastenausgleichsmoduls.
Objekt-ID [object_id]	Falls verfügbar, die Adresse der Elastic IP-Adresse, die an das Netzwerk gebunden ist. Wenn nicht verfügbar, die private IP.
IP-Adresse [ip_address]	Falls verfügbar, die Adresse der Elastic-IP-Adresse, die an die Netzwerkschnittstelle gebunden ist. Wenn nicht verfügbar, die private IP.
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

VNIC-Endpunkt [cmdb_ci_endpoint_vnic]

Feld	Beschreibung
Name [name]	Der Name des VNIC-Endpunkts (Virtual Network Machine Interface)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
IP-Adresse [ip_address]	Falls verfügbar, die Adresse der Elastic-IP-Adresse, die an die Netzwerkschnittstelle gebunden ist. Wenn nicht verfügbar, die private IP.
Host [host]	Die ID der Instanz

Mithilfe von erkannte Ressourcen Amazon AWS– Muster für Organisationseinheiten (Organizational Units, LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Organisationseinheit [cmdb_ci_aws_org_unit]

Feld	Beschreibung
Name [name]	Der anwenderfreundliche Name der Organisationseinheit (OU).
Objekt-ID [object_id]	Der eindeutige Bezeichner (ID), der dieser OE zugeordnet ist. Die ID ist für die Organisation eindeutig.
Organisations-ID [aws_org_ID]	Der eindeutige Bezeichner (ID), der dieser OE zugeordnet ist. Die ID ist für die Organisation eindeutig.
Übergeordnete ID der Organisationseinheit [org_unit_parent_ID]	Die ID der Stamm- oder unmittelbar übergeordneten OE.

Ressourcen, die mithilfe des Musters „Amazon AWS - Owned Template (LP)“ erkannt wurden

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Beispiel: **CentOS 7.0-64 minimal für VSI** .
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Der Typ des vom AMI verwendeten Root-Geräts. Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Der Abschnitt „Mustererweiterung“ erkennt Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows VMs und RHEL VMs.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel ist eine der folgenden Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value] (Fortsetzung)

Feld	Beschreibung
	• Windows_OS_License_Type_Automatic • RHEL_OS_License_Type_Automatic
Wert [value]	Der Wert ist eine der folgenden Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist `Image`Oder `Cloud Image`.

Ressourcen, die mithilfe des Musters „Amazon AWS - Public IP Address (LP)“ erkannt wurden

Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]

Feld	Beschreibung
Name [name]	Der Name oder die Zuteilungs-ID, wenn für die öffentliche IP-Adresse kein Name angegeben ist
Objekt-ID [object_id]	Die ID, die die Zuordnung der Adresse für die Verwendung mit EC2-VPC darstellt
Öffentliche IP-Adresse [public_ip]	Die Elastic IP-Adresse

Ressourcen, die mithilfe des Musters „Amazon AWS - Route Table (LP)“ erkannt wurden

Weiterleitungstabelle [cmdb_ci_route_table]

Feld	Beschreibung
Name [name]	Die ID der Weiterleitungstabelle
Status [state]	Wenn die Weiterleitungstabelle erkennbar ist, ist der Wert verfügbar.
Objekt-ID [object_id]	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist

Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist
Objekt-ID [object_id]	Die ID der Weiterleitungstabelle

Ressourcen, die mithilfe des Musters „Amazon AWS - Security Group (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Feld	Beschreibung
Name [name]	Der Name der Sicherheitsgruppe
Objekt-ID [object_id]	Die ID der Sicherheitsgruppe

Mithilfe von erkannte Ressourcen Amazon AWS– Muster für SSM-Cloud-Agents (LP)

Cloud-Systemmanagement-Agent [cmdb_ci_Cloud_System_Management_Agent]

Feld	Beschreibung
Cloud-Agent-Typ [Cloud_Agent_type]	Typ des Cloud-Agents: AWS SSM.
Installationsstatus [install_status]	Installationsstatus von AWS Systemmanager-Agent (SSM): • **Installiert** : Der Agent wird derzeit ausgeführt. • **Abwesend** : Der Agent wird derzeit nicht ausgeführt.
IP-Adresse [ip_address]	Adresse der VM-Instanz.
Name [name]	Name der VM-Instanz, auf der der SSM-Agent ausgeführt wird.
Objekt-ID [object_id]	ID der VM-Instanz.
Betriebsstatus [operational_status]	Betriebsstatus des Service Desk-Mitarbeiters. Mögliche Werte sind „betriebsbereit“ oder „nicht funktionsfähig“.
Betriebssystemplattform [Operating_System_Platform]	Betriebssystemtyp der VM-Instanz.
Ressourcentyp [resource_type]	Typ der von SSM verwalteten Ressource. Mögliche Werte sind „EC2Instance“ oder „ManagedInstance“.
Version [version]	Version des SSM-Agent.

Ressourcen, die mithilfe des Musters „Amazon AWS - Storage (LP)“ erkannt wurden

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Status [state]	Der Volumestatus. Die folgenden Werte sind gültig: wird erstellt (creating), verfügbar (available), in Gebrauch (in-use), löscht (deleting), gelöscht (deleted) oder Fehler (error).
Speichertyp [storage_type]	Beispiel: Hartcodierter Wert: **Blockieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume [cmdb_ci_storage_volume] (Fortsetzung)

Feld	Beschreibung
Volume-ID [volume_id]	Der Volumetyp. Beispiel: gp2 für Allzweck-SSD, io1 für bereitgestellte IOPS-SSD, st1 für durchsatzoptimierte Festplatte, sc1 für kalte Festplatte oder „Standard“ für magnetische Volumes.
Name [name]	Name oder ID, wenn für das Volume kein Name angegeben ist
Größe in Byte [size_bytes]	Die Größe des Volumes in Byte.
Objekt-ID [object_id]	Die ID des Volumes

Block-Endpunkt [cmdb_ci_endpoint_block]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Volume kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Volumes

Mithilfe von erkannte Ressourcen Amazon AWS– Muster für Unterkonto (LP)

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Konto-ID [account_id]	Eindeutiger Bezeichner (ID) des Accounts.
Objekt-ID [object_id]	Eindeutiger Bezeichner (ID) des Accounts.
Rechenzentrumstyp [datacenter_type]	Hartcodierter Wert: cmdb_ci_aws_Datacenter.
Name [name]	Anwenderfreundlicher Name des Accounts.
Ist Master-Konto [is_master_account]	Boolesches Attribut, das angibt, ob dieser Account der Verwaltungsaccount ist oder nicht.
Account-E-Mail [Account_email]	E-Mail-Adresse des AWS Service-Account.

Ressourcen, die mithilfe des Musters „Amazon AWS - Subnet (LP)“ erkannt wurden

Cloud-Subnetz [cmdb_ci_cloud_subnet]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Subnetz kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Subnetzes
CIDR [cidr]	Der IPv4 CIDR-Block, der dem Subnetz zugewiesen ist
Verfügbare IP-Anzahl [available_ip_count]	Die Anzahl der nicht verwendeten privaten IPv4-Adressen im Subnetz. Die IPv4-Adressen für angehaltene Instanzen gelten als nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Subnetz [cmdb_ci_cloud_subnet] (Fortsetzung)

Feld	Beschreibung
Status [state]	Der aktuelle Status des Subnetzes. Die folgenden Werte sind gültig: ausstehend (pending) oder verfügbar (available).

Ressourcen, die mithilfe des Musters „Amazon AWS – Virtual Server (LP)“ erkannt wurden

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Instanz kein Name angegeben ist
Objekt-ID [object_id]	Die ID der Instanz
Arbeitsspeicher [memory]	Für die Instanz verfügbare Arbeitsspeicher (MBs)
CPUs [cpus]	Anzahl der für die Instanz verfügbaren CPUs
Datenträger [disks]	Anzahl der Datenträger, die an die Instanz angeschlossen sind
ID der VM-Instanz [vm_inst_id]	Die ID der Instanz
Status [state]	Der aktuelle Status der Instanz
IP-Adresse [ip_address]	ID-Adresse der VM-Instanz
Netzwerkadapter [network_adapters]	Anzahl der für die Instanz verfügbaren NICs

Hinweis:

Wenn Sie eine stillgelegte VM erneut aktiviert haben und möchten, dass ihr aktiver Status in genau widergespiegelt wird **Betriebsstatus** Und **Installationsstatus** Felder in der Tabelle „VM-Instanz“ [cmdb_ci_vm_instance] festlegen `sn_itom_pattern.discover_aws_instance_statuses` MID-Server Eigenschaft bis **Wahr** . Beachten Sie, dass diese Einstellung zusätzliche API-Aufrufe umfasst – einen für jede Seite der Musterausführung –, die sich auf die Leistung auswirken können, wenn Sie eine große Anzahl von VMs verwalten.

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subnetzendpunkt [cmdb_ci_endpoint_subnet]

Feld	Beschreibung
Name [name]	Der Name des Subnetzendpunkts
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Beispiel: **CentOS 7.0-64 minimal für VSI** .
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Der Typ des vom AMI verwendeten Root-Geräts. Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Speicherzuordnung [cmdb_ci_storage_mapping]

Feld	Beschreibung
Name [name]	Die ID des Volumes
Objekt-ID [object_id]	Die ID des Volumes
Bereitstellungspunkt [Mount_Point]	Der Gerätename. Beispiel: **/Dev/sdh** Oder **Xvdh** .
Host [host]	Die öffentliche IPv4-Adresse, die der Instanz zugewiesen wurde, falls zutreffend
Zuordnungstyp [mapping_type]	Der Typ des vom AMI verwendeten Root-Geräts Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.

Ressourcen, die mithilfe des Musters „Amazon AWS - VPN Connections (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VPN-Verbindung [cmdb_ci_vpn_connection]

Feld	Beschreibung
Name [name]	Name des Projekts, das für die Erkennung verwendet wird
Objekt-ID [object_id]	Name oder ID, wenn für die VPN-Verbindung kein Name angegeben ist
Status [state]	Der aktuelle Status der VPN-Verbindung. Die folgenden Werte sind gültig: ausstehend (pending), verfügbar (available), löscht (deleting) oder gelöscht (deleted).

Mithilfe von erkannte Ressourcen Amazon AWS– VPN-Gateway (LP)-Muster

Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das VPN-Gateway kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Virtual Private Gateway
Verbindungstyp [connection_type]	Der Typ der vom Virtual Private Gateway unterstützten VPN-Verbindung

Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das VPN-Gateway kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Virtual Private Gateway
Verbindungstyp [connection_type]	Der Typ der vom Virtual Private Gateway unterstützten VPN-Verbindung

Mithilfe von erkannte Ressourcen Amazon AWS– Web-ACL (LP)-Muster

Web-ACL [cmdb_ci_Web_acl]

Feld	Beschreibung
Name [name]	Name der Web-Zugriffssteuerungsliste (Web-ACL).
Objekt-ID [object_id]	Eindeutige ID für die Web-ACL von AWS.
Standardaktion [defaul_action]	Standardaktion, wenn keine Regeln in der Web-ACL übereinstimmen. Mögliche Werte sind Allow oder Deny.
Beschreibung [short_description]	Beschreibung der Web-ACL, bereitgestellt von AWS.
Betriebsstatus [operational_status]	Gibt an, ob die Web-ACL aktiviert oder deaktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Web-ACL [cmdb_ci_Web_acl] (Fortsetzung)

Feld	Beschreibung
	Mögliche Werte sind „betriebsbereit“ oder „stillgelegt“.

Hinweis: Security Operations Anwender können die Integration mit nutzen Discovery Dient zum Importieren von Web-ACL-Regeln und Lastenausgleichsmodule mit angehängten Web-ACLs. Weitere Informationen zum Festlegen von ACL-Regeln und zur Verwendung der App „Überwachung der Risikominderungssteuerungen“ finden Sie unter Konfigurieren Sie AWS WAF-Integration für die Überwachung von Minderungssteuerungen .

Events, die während der horizontalen Erkennung mithilfe von Discovery erkannt wurden

Discovery verwendet Muster, um Events zu suchen, die für Amazon AWS Cloud-Komponenten erstellt wurden. Wenn Events vorhanden sind, die auf eine Statusänderung in einer der Amazon AWS Cloud-Komponenten hinweisen, wird die Erkennung von Amazon AWS Cloud-Komponenten anhand der Muster ausgelöst.

Muster, die für die Event-Erkennung verwendet wurden

Muster	CI
Amazon AWS Virtual Server Events	VM-Instanz [cmdb_ci_vm_instance]
Amazon AWS Security Group Events	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Amazon AWS Subnet Events	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Amazon AWS Storage Events	Speichervolume [cmdb_ci_storage_volume]
Amazon AWS Network Events	Cloud-Netzwerk [cmdb_ci_network]
Amazon AWS Classic LB Events	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Amazon AWS Application and Network LBs Events	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Amazon AWS - ACL (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Netzwerk-ACL [cmdb_ci_network_acl]
Netzwerk-ACL [cmdb_ci_network_acl]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Netzwerk-ACL [cmdb_ci_network_acl]	Endpunkt implementieren in::Endpunkt implementieren von	Netzwerk-ACL [cmdb_ci_network_acl]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt verwenden an::Endpunkt verwenden von	Netzwerk-ACL [cmdb_ci_network_acl]

Beziehungen, die mithilfe des Musters „Amazon AWS - Application and Network (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Beziehungen, die mithilfe des Musters „Amazon AWS - Availability Zone (LP)“ erkannt wurden

CI	Beziehung	CI
AWS-Rechenzentrum [cmdb_ci_aws_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]

Beziehungen, die mithilfe des Musters „Amazon AWS - Classic LB (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Beziehungen, die mit dem Muster „Amazon AWS – LB Pool Member(LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Referenzen	Load Balancer-Pool [cmdb_ci_lb_pool]

Hinweis: Standardmäßig führt das Muster „Amazon AWS – LB Pool Member(LP)“ keine Discovery aus. Um die Discovery von zu aktivieren AWS Anwendungslastenausgleichsmodul-Ziele festlegen `sn_itom_pattern.discover_aws_app_pool_members` MID-Server Eigenschaft bis **Wahr** . Weitere Informationen finden Sie unter Aktivieren AWS Ziel-Discovery des Anwendungslastenausgleichsmoduls.

Beziehungen, die mithilfe des Musters „Amazon AWS - Customer Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
Kunden-Gateway [cmdb_ci_customer_gateway]	Gehostet auf::Hostet	VM-Instanz [cmdb_ci_instance]
Kunden-Gateway [cmdb_ci_customer_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Kunden-Gateway [cmdb_ci_endpoint_cust_gateway]

Beziehungen, die mithilfe des Musters „Amazon AWS - Executable Template (LP)“ erkannt wurden

CI	Beziehung	CI
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Hardware Type (LP)“ erkannt wurden

CI	Beziehung	CI
Hardwaretyp [cmdb_ci_compute_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Host (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Host [cmdb_ci_cloud_host]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
VM-Instanz [cmdb_ci_vm_instance]	Wird ausgeführt auf::Wird ausgeführt	Host [cmdb_ci_cloud_host]

Beziehungen, die mithilfe des Musters „Amazon AWS - Internet Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
Internet-Gateway [cmdb_ci_internet_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Internet-Gateway [cmdb_ci_internet_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Internet-Gateway - EP [cmdb_ci_endpoint_intgateway]
Cloud-Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	Internet-Gateway - EP [cmdb_ci_endpoint_intgateway]

Beziehungen, die mithilfe des Musters „Amazon AWS - IP Address (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]	Enthält::Enthalten in	IP-Adresse [cmdb_ci_cloud_ip_address]

Beziehungen, die mithilfe des Musters „Amazon AWS - Key Pair (LP)“ erkannt wurden

CI	Beziehung	CI
Server [cmdb_ci_server]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - LB Pool (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Beziehungen, die mithilfe des Musters „Amazon AWS - LB Service (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Beziehungen, die mithilfe des Musters „Amazon AWS - NAT Gateway (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
NAT-Gateway [cmdb_ci_nat_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
NAT-Gateway [cmdb_ci_nat_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	NAT-EP [cmdb_ci_endpoint_nat]
Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	NAT-EP [cmdb_ci_endpoint_nat]

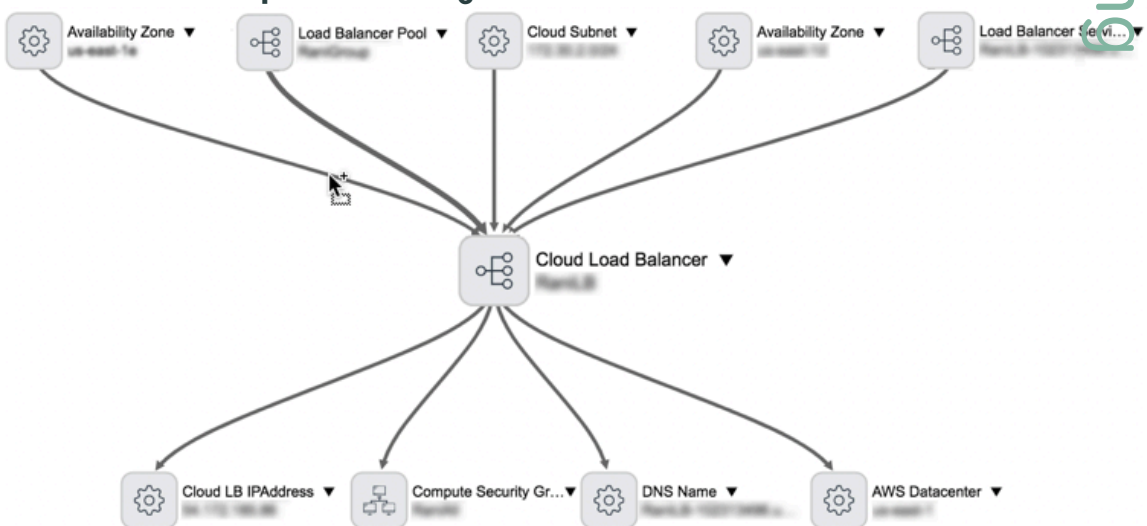
Beziehungen, die mithilfe des Musters „Amazon AWS - Network (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - NIC (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	NIC [cmdb_ci_nic]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Endpunkt implementieren in::Endpunkt implementieren von	NIC [cmdb_ci_nic]
NIC [cmdb_ci_nic]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Abhängigkeitsansichten, die das Cloud-Lastenausgleichsmodul und die verbundene Komponenten anzeigen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit erkannte Beziehungen Amazon AWS– Muster für Organisationseinheiten (Organizational Units, LP)

CI	Beziehung	CI
Cloud-Organisation [cmdb_ci_cloud_org]	Enthält::Enthalten in	AWS-Organisationseinheit [cmdb_ci_aws_org_unit]
AWS-Organisationseinheit [cmdb_ci_aws_org_unit]	Enthält::Enthalten in	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Nur Referenz	AWS-Organisationseinheit [cmdb_ci_aws_org_unit]

Beziehungen, die mithilfe des Musters „Amazon AWS - Owned Template (LP)“ erkannt wurden

CI	Beziehung	CI
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Public IP Address (LP)“ erkannt wurden

CI	Beziehung	CI
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Route Table (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Weiterleitungstabelle [cmdb_ci_route_table]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt verwenden an::Endpunkt verwenden von	Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]
Weiterleitungstabelle [cmdb_ci_route_table]	Endpunkt implementieren in::Endpunkt implementieren von	Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]

Beziehungen, die mithilfe des Musters „Amazon AWS - Security Group (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Mit erkannte Beziehungen Amazon AWS– Muster für SSM-Cloud-Agents (LP)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Cloud-Systemmanagement-Agent [cmdb_ci_Cloud_System_Management_Agent]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
Cloud-Systemmanagement-Agent [cmdb_ci_Cloud_System_Management_Agent]	Wird ausgeführt auf::Wird ausgeführt	VM-Instanz [cmdb_ci_vm_instance]

Beziehungen, die mithilfe des Musters „Amazon AWS - Storage Volume (LP)“ erkannt wurden

CI	Beziehung	CI
VM-Instanz [cmdb_ci_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
Block-Endpunkt [cmdb_ci_endpoint_block]	Endpunkt implementieren in::Endpunkt implementieren von	Speichervolume [cmdb_ci_storage_volume]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Speichervolume [cmdb_ci_storage_volume]
Speichervolume [cmdb_ci_storage_volume]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]

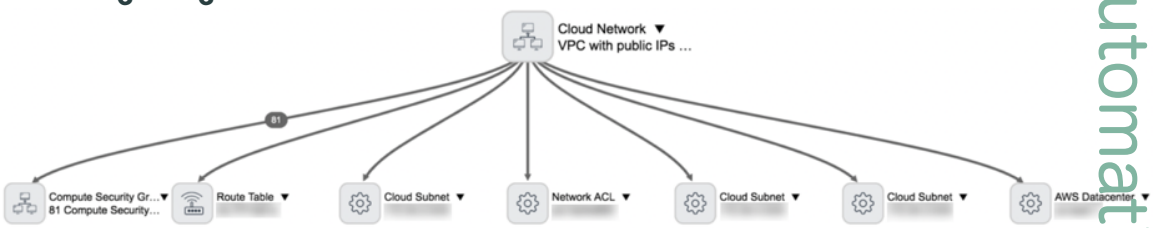
Beziehungen, die mithilfe des Musters „Amazon AWS – Virtual Server (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt implementieren in::Endpunkt implementieren von	Subnetzendpunkt [cmdb_ci_endpoint_subnet]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	VM-Instanz [cmdb_ci_vm_instance]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Subnetzendpunkt [cmdb_ci_endpoint_subnet]
VM-Instanz [cmdb_ci_vm_instance]	Enthält::Enthalten in	Speicherzuordnung [cmdb_ci_storage_mapping]

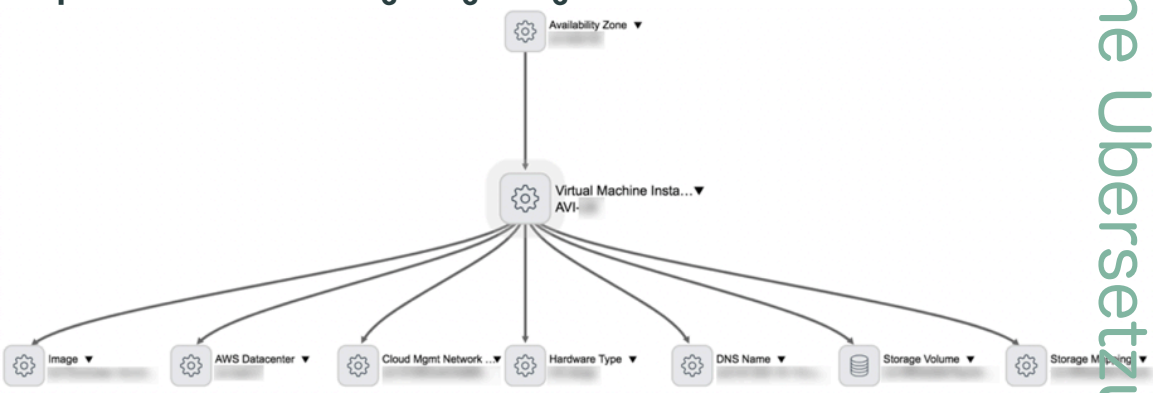
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Hardwaretyp [cmdb_ci_compute_template]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Image [cmdb_ci_os_template]
VM-Instanz [cmdb_ci_vm_instance]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Abhängigkeitsansichten, die Komponenten anzeigen, die in der AWS-Umgebung mit dem Cloud-Netzwerk verbunden sind



Abhängigkeitsansichten, die die VM und die verbundenen Komponenten in der AWS-Umgebung anzeigt



Beziehungen, die mithilfe des Musters „Amazon AWS - VPN Connections (LP)“ erkannt wurden

CI	Beziehung	CI
Kunden-Gateway [cmdb_ci_customer_gateway]	Enthält::Enthalten in	VPN-Verbindung [cmdb_ci_vpn_connection]
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Enthält::Enthalten in	VPN-Verbindung [cmdb_ci_vpn_connection]
VPN-Verbindung [cmdb_ci_vpn_connection]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - VPN Gateway (LP)“ erkannt wurden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]
Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]

Mit erkannte Beziehungen Amazon AWS– Web-ACL (LP)-Muster

CI	Beziehung	CI
Web-ACL [cmdb_ci_Web_acl]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
Web-ACL [cmdb_ci_Web_acl]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Hinweis: Security Operations Anwender können die Integration mit nutzen Discovery Dient zum Importieren von Web-ACL-Regeln und Lastenausgleichsmodule mit angehängten Web-ACLs. Weitere Informationen zum Festlegen von ACL-Regeln und zur Verwendung der App „Überwachung der Risikominderungssteuerungen“ finden Sie unter Konfigurieren Sie AWS WAF-Integration für die Überwachung von Minderungssteuerungen .

Services, die mithilfe von Mustern erkannt wurden

Bei der horizontalen Erkennung werden EC2- und VPC-Services gefunden, die auf AWS-Ressourcen ausgeführt werden.

Services, die von Discovery mithilfe von Mustern erkannt wurden

Servicename	CI-Klasse	Muster
AWS::EC2::SecurityGroup	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Amazon AWS Security Group Events
AWS::EC2::Subnet	Cloud-Subnetz [cmdb_ci_cloud_subnet]	Amazon AWS Subnet Events
AWS::EC2::VPC	Cloud-Netzwerk [cmdb_ci_network]	Amazon AWS Network Events
AWS::EC2::Instance	VM-Instanz [cmdb_ci_vm_instance]	Amazon AWS Virtual Server Events
EQS::EC2::Volume	Speichervolume [cmdb_ci_storage_volume]	Amazon AWS Elastic Block Storage
AWS::ElasticLoadBalancingV2::LoadBalancer	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Amazon AWS Application and Network LBs Events
AWS::ElasticLoadBalancing::LoadBalancer	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Amazon AWS Classic LBs Events

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Amazon ECS-Ressourcen-Discovery mit Mustern

Die ServiceNow Discovery-Anwendung verwendet Amazon AWS– ECS-Muster zum Suchen von Ressourcen, die von verwaltet werden Amazon Elastic Container-Service (Amazon ECS). Dies umfasst Ressourcen, die beim Starttyp Fargate ausgeführt werden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Amazon ECS ist ein hoch skalierbarer, schneller Containerverwaltungsservice, der das Ausführen, Stoppen und Verwalten vereinfacht Docker Container. AWS Fargate ist eine Rechnungs-Engine für Amazon ECS, die aktiviert AWS Kunden können Container ausführen, ohne Server oder Cluster verwalten zu müssen.

Discovery Verwendet Amazon AWS– ECS-Muster zum Ausführen der horizontalen Discovery.

Beginnend mit Muster für Discovery und Service-Mapping Version 1.18.0, die Amazon AWS– Das ECS-Muster unterstützt die Discovery von Amazon Elastische Container-Registrierung (Amazon ECR) Bilder. Weitere Informationen zum Scannen von Containern finden Sie unter Container-Images scannen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Erstellen AWS Anmeldeinformationen mit ECS-Ressourcen-Anzeigeberechtigungen

In AWS Konsole, erstellen AWS Anmeldeinformationen mit Berechtigungen zum Anzeigen von ECS-Ressourcen. Weitere Informationen finden Sie unter: https://docs.aws.amazon.com/en_pv/AmazonECS/latest/userguide/get-set-up-for-amazon-ecs.html .

Hinweis: Die API-Anforderungen verwenden AWS Signaturversion 4 zur Authentifizierung. Wenn die richtigen Anmeldeinformationen angegeben sind, erfolgt die Authentifizierung intern für die Musterschritte „Cloud API Call“.

Erstellen AWS Cloud-Anmeldeinformationsdatensätze oder temporäre Anmeldeinformationen verwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In ServiceNow AI Platform, Erstellen AWS Anmeldeinformationsdatensätze. Sie können auch temporäre Anmeldeinformationen verwenden, die von generiert wurden AWS Sicherheits-Token-Service (AWS STS) für IAM-Rollen. Weitere Informationen finden Sie unter Cloud-Anmeldeinformationen

Erstellen AWS Cloud-Service-Accounts

- In ServiceNow AI Platform, Erstellen AWS Cloud-Service-Accounts mit permanenten oder temporären Konten AWS Anmeldeinformationen. Weitere Informationen finden Sie unter Wird eingerichtet AWS Service-Accounts.
- Wählen Sie im Datensatz Cloud-Service-Account die Option aus **Erkennen Sie Rechenzentren** Zu finden AWS Rechenzentren (LDCs) für konfigurierte AWS Cloud-Service-Account.

Planen Sie einen AWS Discovery

In ServiceNow AI Platform, Planen Sie entweder ein vollständiges AWS Muster-Discovery oder nur eine ECS-Muster-Discovery.

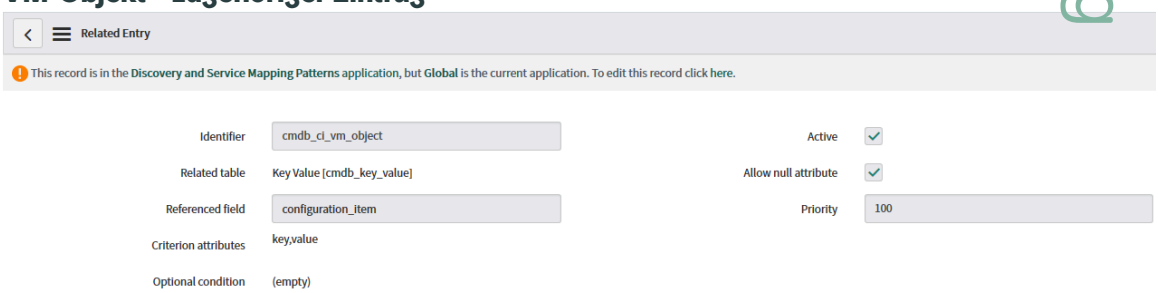
- Weitere Informationen zum Planen einer Cloud-Discovery finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.
- Weitere Informationen zum Erstellen eines serverlosen Zeitplans für Amazon ECS-Discovery, siehe Erstellen Sie einen serverlosen Zeitplan für Amazon ECS-Discovery.

Überprüfen Sie die Konfiguration des VM-Objektdatensatzes, um die Ressourcen-Tags zu finden

Damit das Muster die Ressourcen-Tags finden kann, muss die übergeordnete ECS-Tabelle (VM-Objekt) über einen zugehörigen Eintrag für die Tabelle cmdb_key_value verfügen:

1. In ServiceNow AI Platform Navigationsleiste, navigieren Sie zu **Alle** > **Konfiguration** > **Identifikation/Abgleich**, Und wählen Sie aus **CI-Bezeichner** .
2. Suchen Sie den Datensatz VM-Objekt, und öffnen Sie ihn.
3. Wählen Sie aus **Zugehörige Einträge** Registerkarte und stellen Sie sicher, dass sie wie in der Abbildung „Zugehöriger Eintrag für VM-Objekt“ angezeigt konfiguriert ist. Wenn nicht, geben Sie einen neuen zugehörigen Eintrag an: Wählen Sie in der zugehörigen Liste zugehörige Einträge die Option aus **Neu** , Füllen Sie das Formular aus, und wählen Sie dann aus **Übermitteln** .

VM-Objekt – zugehöriger Eintrag



Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen von Amazon AWS– ECS-Muster.

AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]

Feld	Beschreibung
Objekt-ID [object_id]	Die Amazon Ressourcenname (ARN), der den Cluster identifiziert.
Name [name]	Eine vom Benutzer generierte Zeichenfolge zur Identifizierung des Clusters
Anzahl der registrierten Containerinstanzen [registered_Container_instances_count]	Die Anzahl der im Cluster registrierten Container-Instanzen. Der Status dieser Container-Instanzen kann entweder „ACTIVE“ oder „DRAINING“ sein.

AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]

Feld	Beschreibung
Objekt-ID [object_id]	Die vollständige ARN der Aufgabendefinition
Name [name]	Der Name der Familie, für die diese Aufgabendefinition registriert ist.
Überarbeitung [Überarbeitung]	Die Überarbeitung der Aufgabe in einer bestimmten Familie. Dies ist die Versionsnummer der Aufgabendefinition in einer Familie.
Netzwerkmodus [Network_Mode]	Die Docker Netzwerkmodus, der für die Container in der Aufgabe verwendet werden soll. Gültige Werte: none, bridge, awsvpc, host.
CPU [cpu]	Die Anzahl der von der Aufgabe verwendeten CPU-Einheiten
Arbeitsspeicher [memory]	Die von der Aufgabe verwendete Arbeitsspeichermenge in Mebibyte (MIB).

AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]

Feld	Beschreibung
Objekt-ID [object_id]	Die ARN, die die Aufgabe identifiziert
Name [name]	Eine vom Benutzer generierte Zeichenfolge, um die Aufgabe zu identifizieren
Starttyp [Launch_type]	Der Starttyp, für den die Aufgabe ausgeführt wird
Betriebsstatus [Operation_Status]	Der Integritätsstatus der Aufgabe, der von der Integrität der darin enthaltenen wesentlichen Container bestimmt wird
CPU [cpu]	Die Anzahl der von der Aufgabe verwendeten CPU-Einheiten, wie in der Aufgabendefinition angegeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task] (Fortsetzung)

Feld	Beschreibung
Arbeitsspeicher [memory]	Die von der Aufgabe verwendete Speichermenge in MiB, wie in der Aufgabendefinition angegeben

AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]

Feld	Beschreibung
Objekt-ID [object_id]	Die ARN, die den Service identifiziert
Name [name]	Der Name des Services
Starttyp [Launch_type]	Der Starttyp, für den der Service ausgeführt wird
Planungsstrategie [Scheduling_Strategy]	Die für den Service zu verwendende Zeitplanstrategie

Docker-Container [cmdb_ci_docker_container]

Feld	Beschreibung
Container id [Container_ID]	Die ARN des Containers
Name [name]	Der Name des Containers
Status [status]	Der zuletzt bekannte Status des Containers
Betriebsstatus [operational_status]	Der Integritätsstatus des Containers
CPU [cpu]	Die Anzahl der für den Container festgelegten CPU-Einheiten
Arbeitsspeicher [memory]	Die feste Grenze des Arbeitsspeichers in MiB, die für den Container festgelegt ist

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Objekt-ID [object_id]	Der ARN, der die VM-Instanz identifiziert. **Hinweis:** Vollständige Informationen zur VM-Instanz werden in einem anderen EC2-Cloudmuster erkannt. In Amazon ECS-Ressourcen-Discovery, nur die object_ID wird analysiert, um die eindeutige Identifizierung des CI zu unterstützen.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Tag-Schlüssel
Wert [value]	Der Tag-Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Docker-Image [cmdb_ci_docker_image]

Feld	Beschreibung
Name [name]	Name des Docker Bild.
Image-Digest [image_digest]	Eindeutiger Bezeichner für Docker Bild.
Image-ID [image_id]	Eindeutiger Bezeichner mit 12 Zeichen für die Länge Docker Bild.

Container-Repository [cmdb_ci_container_repository]

Feld	Beschreibung
Name [name]	Vollqualifizierter Name des Repositorys, das den enthält Docker Bild.

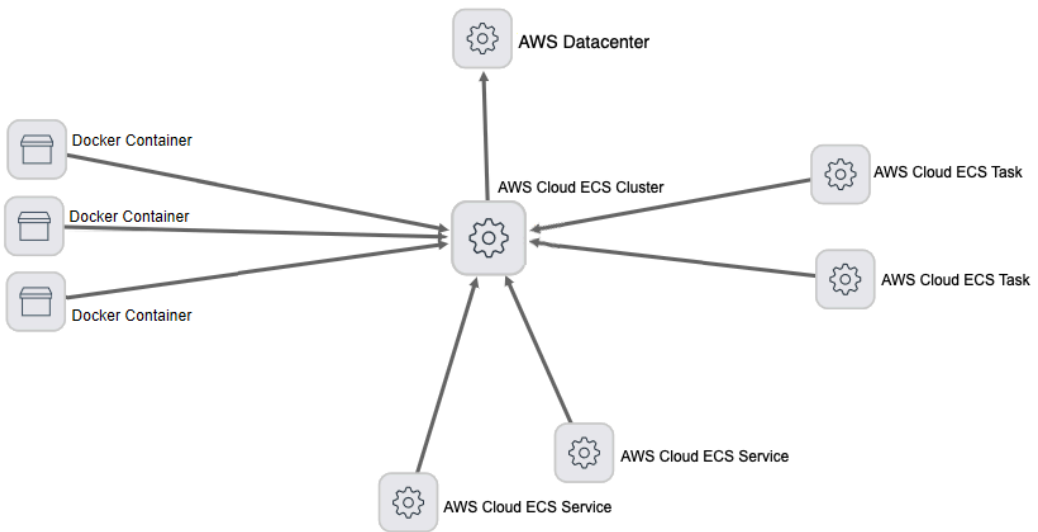
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]

Feld	Beschreibung
Name [name]	Die Docker Image-Tag.
Kategorie [category]	Vollqualifizierter Name des Repositorys, das den enthält Docker Bild.

Auf der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten Ressourcen in Ihrer Organisation anzeigen, die von verwaltet werden Amazon ECS und die Beziehungen zwischen ihnen.

In diesem Beispiel ist AWS Cloud-ECS-Cluster-CI wird auf einem gehostet AWS Rechenzentrum. Es wird zwei ausgeführt AWS Cloud-ECS-Aufgaben und zwei AWS Cloud-ECS-Services und verwendet drei Docker Container.

Dependency Views-Beispielzuordnung



CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Amazon Discovery der ECS-Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Verwendet::Verwendet von	VM-Instanz [cmdb_ci_vm_instance]
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Verwendet::Verwendet von	AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Wird ausgeführt auf::Wird ausgeführt	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	VM-Instanz [cmdb_ci_vm_instance]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	Docker-Container [cmdb_ci_docker_container]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Verwendet::Verwendet von	AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Verwendet von::Verwendet	AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Verwendet von::Verwendet	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Container-Repository [cmdb_ci_container_repository]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]
Docker-Container [cmdb_ci_docker_container]	Gehostet auf::Hostet	AWS-Rechenzentren
Docker-Container [cmdb_ci_docker_container]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]
Docker-Container [cmdb_ci_docker_container]	Verwendet von::Verwendet	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]

Erstellen Sie einen serverlosen Zeitplan für Amazon ECS-Discovery

Erstellen Sie einen serverlosen Zeitplan zur Erkennung Amazon Elastic Container-Service (Amazon ECS) und Amazon ECR-Ressourcen (Elastic Container Registry) in einer eigenständigen Discovery.

Vorbereitungen

Überprüfen Sie, ob Sie einen haben AWS Service-Account-ID und wurden erstellt AWS Anmeldeinformationen. Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Amazon ECS-Ressourcen-Discovery mit Mustern.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Erkennung von ECR-Ressourcen erfordert die Ausführung des Musters „Amazon AWS – ECS“, bevor Sie verwenden Aqua Trivy Zum Scannen von Containerbildern. Dient zum Erkennen nur ECS- und ECR-Ressourcen, ohne einen vollständigen auszuführen AWS Muster-Discovery: Erstellen Sie einen serverlosen Discovery-Zeitplan mit dem Amazon AWS – ECS-Muster.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Erstellen Sie den Discovery-Zeitplandatensatz.
   a. Wählen Sie **Neu**.
   b. Füllen Sie im Formular die Felder aus.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Erkannt	Scan-Typ, der serverlos sein muss.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server verwenden	Name des MID-Server Zur Verwendung für diesen Zeitplan.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.
Ausführen	Bestimmt den Ausführungszeitplan der Erkennung.

c. Wählen Sie **Absenden**.

3. Erstellen Sie das Ausführungsmuster.

a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.

b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .

c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll, der Amazon AWS – ECS sein muss.
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren, der global sein muss.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

d. Wählen Sie **Absenden**.

4. Legen Sie die Parameter des Musterstartprogramms fest.

a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.

b. Füllen Sie im Formular die Felder aus.

Parameter	Wert
cloud_account_id	AWS Cloud-Service-Account-ID.
cloud_cred_id	SYS_ID des AWS Anmeldeinformationen, die Sie auf erstellt haben ServiceNow AI Platform.
cloud_datacenter_type	Name der AWS-Rechenzentrumstabelle, die cmdb_ci_aws_Datacenter sein muss.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Amazon ECS-Ressourcen-Discovery mit Mustern

Container-Images scannen

Amazon Relativer Datenbankservice (Amazon RDS) Discovery mit Mustern

Die Anwendung ServiceNow® Discovery verwendet das Erkennungsmuster „Amazon AWS Relational Database Service“, um AWS RDS-Komponenten zu finden.

Amazon Relational Database Service (RDS) ist ein verwalteter relationaler Datenbankservice von Amazon Web Services (AWS). Er ermöglicht Benutzern das einfache Erstellen und Verwalten von relationalen Datenbankinstanzen in der Cloud.

Discovery verwendet das Erkennungsmuster, um eine horizontale Erkennung, Event-Erkennung und Tag-Erkennung auszuführen. Das Muster verwendet eine Reihe von Amazon REST APIs, um die RDS-Komponenten zu finden.

Von der ServiceNow AI Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ aus dem ServiceNow Store.
- Konfigurieren Sie auf der ServiceNow AI Platform die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Erstellen Sie ein Servicekonto. Legen Sie die **Konto-ID** auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances&DBInstanceIdentifier=<input_object_id> for events discovery
  - https://tagging.<REGION>.amazonaws.com/ for tags discovery
- Der MID-Server muss in der Amazon-Cloud platziert sein.
- Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-Mapping Von ServiceNow Store.
- Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Support für AWS Services in der Region China

Die neueste Version von Muster für Discovery und Service-Mapping Unterstützt die Erkennung AWS Services in der Region China. Sie können diese Services in erkennen ServiceNow AI Platform, Beginnend ab Xanadu Patch 3 und Washington DC Patch 9-Instanzen.

Wird Erkannt AWS Services in der Region China erfordern die Verwendung einer Rechenzentrums-URL beim Einrichten von AWS Service-Account. Beispiel: `https://organizations.cn-northwest-1.amazonaws.com.cn` .

- Um mehr über zu erfahren AWS Master-Account- und Unteraccount-Support in der Region China, siehe KB1704526 .
- Zu identifizieren AWS In der Region China unterstützte Muster finden Sie in der Tabelle „Cloud Discovery-Muster“. Die **AWS – Support für Region China** Spalte hat den Wert „Ja“ für unterstützte Muster.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Cloud-Datenbank [cmdb_ci_cloud_database]	
Kategorie [category]	Klasse der Datenbank. Enthält Vorlagen für CPU und Arbeitsspeicher
Objekt-ID [object_id]	Eindeutige Ressourcen-ID, die jedes logische Rechenzentrum (LDC) identifiziert
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
TCP-Port [tcp_port]	Port des Datenbankendpunkts
Name [name]	Name der Datenbank.
Version [version]	Version der Datenbank
Typ [type]	Typ der Datenbank. Kann Folgendes sein: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle-Datenbank, SQL Server.
Betriebsstatus [operational_status]	Status der Datenbank
IP-Adresse [ip_address]	IP-Adresse des vollständig qualifizierten Domänennamens (FQDN)
Anbieter [vendor]	Der Anbieter, Amazon
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse des Datenbankendpunkts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Name [name]	Name des Datenbankendpunkts
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
Kategorie [category]	Klasse der Datenbank. Enthält Vorlagen für CPU und Arbeitsspeicher
Netzmaske [netmask]	IP-Netzmaske
Betriebsstatus [operational_status]	Status der IP-Adresse

Amazon Redshift-Discovery mit Mustern

Die ServiceNow® Discovery Die Anwendung verwendet das Amazon AWS Redshift-Muster, um Redshift-Data Warehouse-Services zu finden, die in verfügbar sind Amazon Web Services(AWS). Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Redshift wird als Cluster von Compute-Knoten mit einem zusätzlichen Leader-Knoten ausgeführt. Der Leader-Knoten fungiert als Schnittstelle zu Clientanwendungen und wird dazu eingesetzt, die Kommunikation zwischen den Compute-Knoten zu koordinieren.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie AWS Abschnitt „Discovery-Voraussetzungen“ in AWS Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Amazon AWS Redshift-Musters.

Amazon Redshift [cmdb_ci_aws_redshift]

Feld	Beschreibung
Name [name]	Name des Redshift-Clusters.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner, der aus dem Redshift-Namespace erstellt wurde Amazon Ressourcenname (ARN) und der Clustername im folgenden Format: **arn:aws:redshift:<region>:<account-id>:Cluster:<cluster-name>** .
Startdatum [Start_date]	Zeitstempel, zu dem der Redshift-Cluster erstellt wurde.
Cluster-Verfügbarkeitsstatus [Cluster_Availability_Status]	Aktueller Verfügbarkeitsstatus des Redshift-Clusters. Beispiel: Verfügbar, nicht verfügbar oder Wartung.
VPC-ID [vpc_ID]	ID der Virtual Private Cloud (VPC), in der der Redshift-Cluster bereitgestellt wird.
Knotenanzahl [node_count]	Gesamtanzahl der Compute-Knoten im Redshift-Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Redshift [cmdb_ci_aws_redshift] (Fortsetzung)

Feld	Beschreibung
Knotentyp [node_type]	Typ der im Redshift-Cluster verwendeten Compute-Knoten.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (FQDN) des Redshift-Clusterendpunkts.
TCP-Port(s) [tcp_port]	TCP-Port, der vom Redshift-Cluster für Client-Verbindungen verwendet wird.
IP-Adresse [ip_address]	IP-Adresse, die dem Redshift-Cluster-Endpunkt zugeordnet ist.
Verfügbarkeitszone [Availability_Zone]	Verweist auf die Tabelle „Verfügbarkeitszone“ [cmdb_ci_Availability_Zone].

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone.
Objekt-ID [object_id]	Name der Verfügbarkeitszone.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Amazon Redshift-Discovery.

CI	Beziehung	CI
Amazon Redshift [cmdb_ci_aws_redshift]	Referenzen	Verfügbarkeitszone [cmdb_ci_av availability_zone]
AWS-Rechenzentrum [cmdb_ci_aws_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Schlüsselwert [cmdb_key_value]	Referenzen	Amazon Redshift [cmdb_ci_aws_redshift]

Tag-Discovery

Das Amazon AWS Redshift-Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.
Konfigurationselement [configuration_item]	Verweist auf die Tabelle „Amazon Redshift“ [cmdb_ci_aws_redshift].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Einfacher Speicherservice (Amazon S3) Discovery mit Mustern

Die ServiceNow Discovery-Anwendung verwendet das Muster „Amazon AWS S3“, um Buckets von öffentlichem und nicht öffentlichem Speicher des Amazon Simple Storage Service zu suchen. Das Muster verwendet eine Reihe von REST API-Aufrufen, um diese Ressourcen zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Zusätzlich zum Erkennungszeitplan löst die ServiceNow-Instanz das Muster „Amazon AWS S3“ aus, wenn AWS Config ein Event an die ServiceNow-Instanz sendet. Config ist ein Service, der AWS-Ressourcen kontinuierlich überwacht und jedes Mal Events an ServiceNow sendet, wenn erkannt wird, dass sich eine Ressourcenkonfiguration geändert hat.

Das Muster „Amazon AWS S3“ kann auch AWS S3-Buckets erkennen, die sich in der Region AWS GovCloud (US) befinden. Für AWS S3 in AWS GovCloud (SU) kann das Muster ausgehende AWS S3-Verbindungen zu anderen Cloud-Ressourcen wie der Lambda-Funktion nicht erkennen. Die Erkennung ausgehender Verbindungen für AWS S3 wird in zukünftigen Versionen unterstützt.

Sie können dieses Muster auf der ServiceNow-Plattform mit Jakarta Patch 10, Kingston Patch 8 oder London Patch 1 verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Wenn Sie Identity and Access Management (IAM) verwenden, um Benutzer auf der AWS-Plattform (Amazon Web Services) zu verwalten, stellen Sie sicher, dass Sie eine Benutzerrichtlinie für den AWS-Benutzer erstellt haben. Weitere Informationen finden Sie im Abschnitt zur Erstellung einer IAM-Benutzerrichtlinie für Cloud Provisioning and Governance in der ServiceNow Cloud Provisioning and Governance-Dokumentation.
- Konfigurieren Sie das AWS-Servicekonto.
- Konfigurieren Sie die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Benutzerberechtigungen für die AmazonS3ReadOnlyAccess-Richtlinie
- Erkennen Sie logische Rechenzentren, die S3-Buckets hosten, wie unter „Erkennung für ein AWS Cloud-Servicekonto ausführen“ in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.
- Erstellen Sie einen Zeitplan für das relevante AWS-Servicekonto, wie im Abschnitt zum Planen der Erkennung für ein Servicekonto in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.
- Zum Aktivieren der warnungsbasierten Discovery konfigurieren Sie den AWS Event-Service wie im Abschnitt zum Einrichten der AWS-Ereignisverarbeitung für Discovery und Service-Mapping in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-Mapping Von ServiceNow Store.
- Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

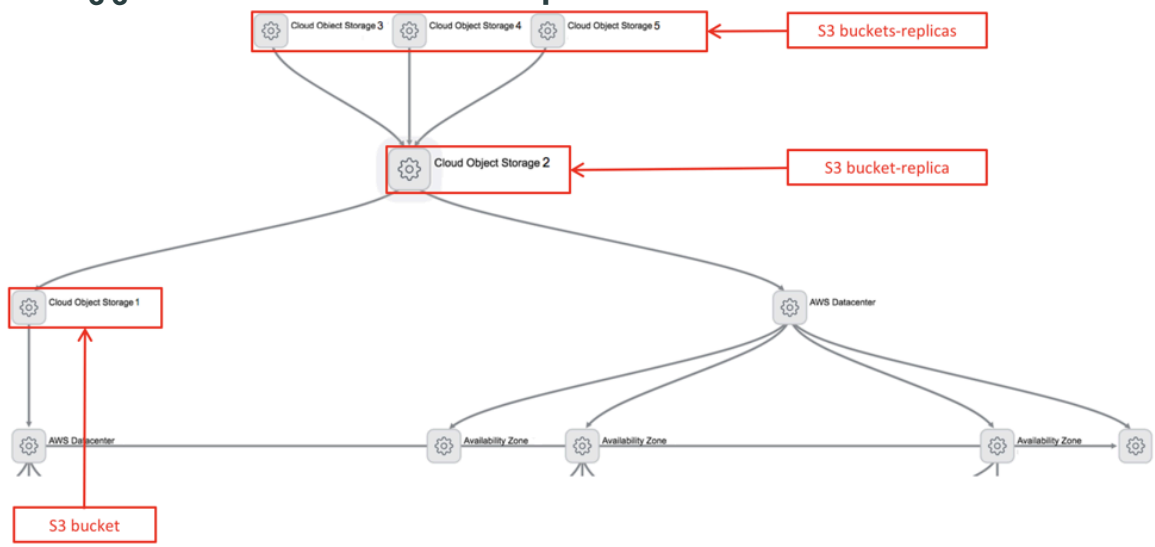
Tabelle und Feld	Beschreibung
Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]	
Bucket-Name [bucket_name]	Der Name des AWS S3-Bucket. Sie können alle in einem logischen Rechenzentrum gehosteten Buckets während eines Erkennungsprozesses erkennen.
Erstellungsdatum [creation date]	Erstellungsdatum des AWS S3-Bucket
Cloud-Anbieter [cloud_provider]	Amazon AWS
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: `arn:aws:s3:::<bucket name>`
Servicename [service_name]	Standardmäßig auf **S3** festgelegt
Eigentümer [owner]	Der Name des Eigentümers des AWS S3-Bucket
Verschlüsselungstyp [encryption_type]	Typ der Verschlüsselung für diesen Bucket. Die Auswahlmöglichkeiten sind: • Keine • AES-256 • AWS-KMS
ACL-Zugriffstyp [acl_access_type]	Auswahlmöglichkeiten für Zugriffssteuerungstypen: • Öffentlich • Nicht öffentlich
Richtlinie Zugriffstyp [policy_access_type]	Auswahlmöglichkeiten für Richtlinien-Zugriffstypen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	• Öffentlich • Nicht öffentlich
Replikationsziel [replication_destination]	Bucket-ARN des Bucket am Replikationsziel

In der Übersicht Abhängigkeitsansichten sehen Sie alle erkannten S3-Buckets in Ihrer Organisation, einschließlich S3-Buckets, die Sie als Repliken konfiguriert haben. In diesem Beispiel replizieren Cloudobjektspeicher 1, Cloudobjektspeicher 2 und Cloudobjektspeicher 3 Cloudobjektspeicher 2. Cloudobjektspeicher 2 wiederum repliziert Cloudobjektspeicher 1.

Abhängigkeitsansichten mit AWS S3-Komponenten



CI-Beziehungen

Diese Beziehungen sollen die Erkennung von AWS S3 unterstützen:

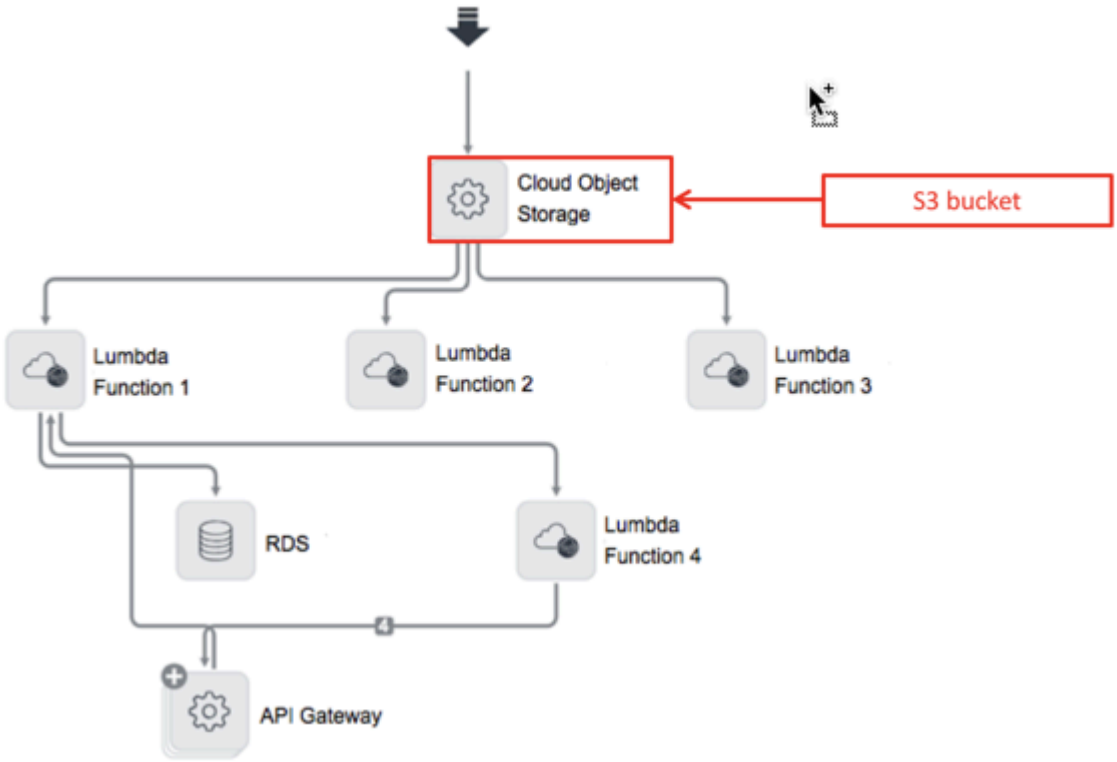
CI	Beziehung	CI
cmdb_ci_cloud_object_storage	Repliziert zu::Repliziert von	cmdb_ci_cloud_object_storage
cmdb_ci_cloud_object_storage	Gehostet auf::Hostet	cmdb_ci_logical_datacenter

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping kann ausgehende AWS S3-Verbindungen zu Cloud-Ressourcen erkennen, z. B. die Lambda-Funktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservicezuordnung mit einem S3-Bucket-CI



Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Debugging auf (und nicht während der Discovery).	Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

AWS API-Gateway-Discovery mit Mustern

Die ServiceNow Discovery Und Service-Mapping Anwendungen können AWS-API-Gateways und Verbindungen zu anderen Entitäten finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery und Service-Mapping verwenden das Muster *`Amazon AWS API Gateway`*, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen.

Dieses Muster können Sie auf der ServiceNow-Plattform in Version Kingston oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

AWS-Servicekonto mit Anmeldeinformationen

Richten Sie auf der ServiceNow AI Platform® das Servicekonto wie folgt ein:

- Eine **Konten-ID**, bei der es sich um die Amazon Konten-ID handelt, zu der das API-Gateway gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird. Sie können eine Erkennung über das Servicekonten-Formular ausführen.
- Die entsprechenden AWS-Anmeldeinformationen, die erforderlich sind, damit die Konten-ID die AWS-Cloud erreicht.

Weitere Informationen zu Servicekonten für Discovery und Service-Mapping finden Sie in der Produktdokumentation.

Update Set

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, importieren Sie das Update Set, das in „KB0679927 : AWS Lambda top-down discovery update set (Update Set für AWS Lambda-Erkennung von oben nach unten)“ bereitgestellt wird. Dieses Update Set ist für Service-Mapping erforderlich.

Benutzerzugriff

Erteilen Sie einem Benutzer auf der AWS-Konsole Berechtigungen zum Ausführen der Funktion `apigateway:GET` nur für die GET-Aktion in API Gateway.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Gateway [cmdb_ci_cloud_gateway]	
Objekt-ID	Die ID des Gateways
Kurzbeschreibung	Eine Kurzbeschreibung des Gateways
DNS-Name [cmdb_ci_dns_name]	
Name	Der eindeutige Name oder die IP-Adresse des DNS-Hosts
IP-Adresse	Die IP-Adresse des Hosts des DNS-Hosts
AWS-Ressourcenname des Endpunkts [cmdb_ci_endpoint_arn]	
Host	Der Host-Name oder die IP-Adresse des Endpunkts
ARN	Die ID (Amazon-Ressourcenname) anderer AWS-Entitäten, mit denen das Gateway eine Verbindung herstellt

Beziehungen von Konfigurationselementen

Diese Beziehungen sollen die AWS API Gateway-Erkennung unterstützen:

CI	Beziehung	CI
Cloud-Gateway [cmdb_ci_cloud_gateway]	Verwendet::Verwendet von	DNS-Name [cmdb_ci_dns_name]
	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter] Das AWS-Rechenzentrum hat Beziehungen zu anderen AWS-CIs, z. B. Verfügbarkeitszonen, Servicekonten usw. Weitere Details finden Sie unter AWS- und Azure Cloud-Erkennung in der Produktdokumentation.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten der AWS API-Gateways im Kontext von Anwendungsservices durch. Es erkennt ausgehende Verbindungen der AWS API-Gateways:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AWS Lambda – ARN
- VPC-Link für Virtual Private Cloud
- HTTP-Endpunkt, der als konfigurierte URL auf dem API-Gateway definiert ist

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Führen Sie die horizontale Erkennung und die Erkennung von oben nach unten mithilfe der Muster „Amazon AWS API Gateway“ [cmdb_ci_cloud_gateway] und „Amazon AWS Lambda“ [cmdb_ci_cloud_function] aus. Überprüfen Sie, ob das Ergebnis den Erwartungen entspricht.

Vorbereitungen

Stellen Sie sicher, dass Ihre Bereitstellung alle Voraussetzungen für AWS API-Gateway-Discovery mit Mustern und AWS Lambda-Discovery mit Mustern erfüllt.

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie einen Anwendungsservice mit den folgenden Eigenschaften für seinen Einstiegspunkt.

Feld	Beschreibung
CI-Typ	HTTPS
URL	Die URL zum Aufruf von API Gateway Normalerweise hat API GW das folgende Format: https://{restapi_id}.execute-api.{region}.amazonaws.com/{stage_name}/ Beispiel: https://k40o0l3af6.execute-api.us-east-1.amazonaws.com/prod/. Informationen zum URL-Format finden Sie unter https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-call-api.html . **Hinweis:** Der Standardwert für den Parameter stage_name lautet *prod*.

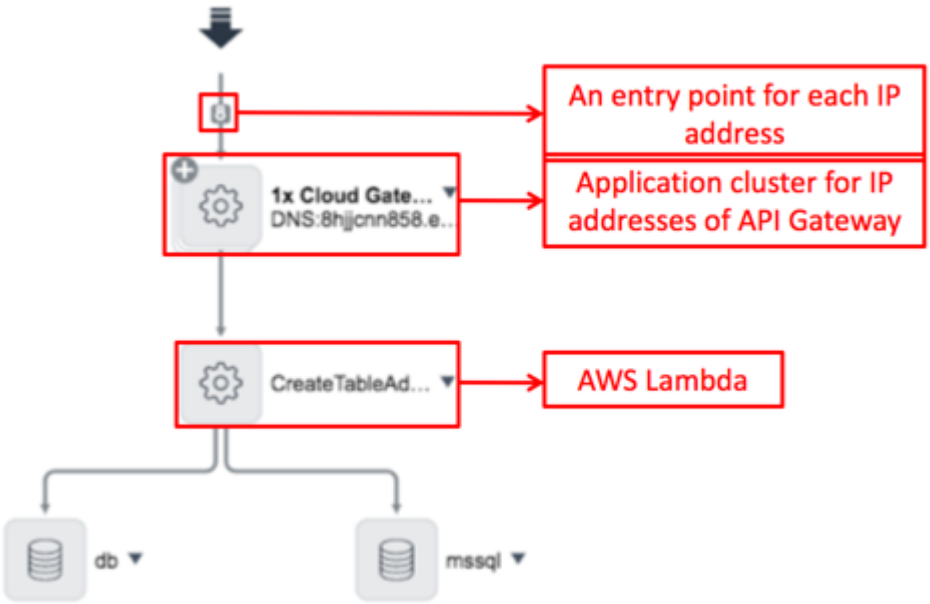
2. Klicken Sie auf **Erkennen**.
   Service-Mapping führt die Erkennung von oben nach unten mit dem Muster „Amazon AWS API Gateway“ [cmdb_ci_cloud_gateway] aus.

   Nachdem Service-Mapping die Identifizierung des API Gateway-Konfigurationselements (CI) abgeschlossen hat, führt es den Verbindungsabschnitt **Connection to APIs (Verbindung zu APIs)** aus und erkennt die Verbindung zu AWS Lambda. Anschließend wird das Muster „Amazon AWS Lambda“ [cmdb_ci_cloud_funktion] ausgeführt und das AWS Lambda-CI identifiziert.

3. Nachdem dieser Anwendungsservice von Service-Mapping erkannt wurde, überprüfen Sie, ob AWS-Komponenten richtig erkannt und identifiziert wurden.
   Überprüfen Sie, ob die folgenden Aktionen ausgeführt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Service-Mapping die URL korrekt auflöst, alle zugehörigen IP-Adressen findet und einen Einstiegspunkt für jede IP-Adresse erstellt.



- Service-Mapping identifiziert das AWS API Gateway und erstellt ein Anwendungscluster für die IP-Adresse.
- Im Bereich **Eigenschaften** werden die Eigenschaften für das AWS API Gateway angezeigt: Cloud-Gateway [cmdb_ci_cloud_gateway].
- Service-Mapping erkennt AWS Lambda, das mit dem Anwendungscluster für API Gateway verbunden ist.
- Service-Mapping erkennt die mit AWS Lambda verbundenen Datenbanken.

AWS Anwendungs-ELB-Service-Discovery mit Mustern

Discovery verwendet das Erkennungsmuster „Amazon AWS application ELB Service“, um alle Lastenausgleichsmodule in Ihrer Umgebung in einer Zuordnung anzuzeigen.

Elastic Load Balancing (ELB) verteilt eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele.

Das Erkennungsmuster „Amazon AWS application ELB Service“ unterstützt die Erkennung von oben nach unten. Dieses Muster erkennt alle Lastenausgleichsmodule mit diesen Eigenschaften:

- Ultrahochleistung, skaliertes TLS-Offloading und zentralisierte Zertifikatbereitstellung verwenden
- Unterstützung von UDP und statischen IP-Adressen für Ihre Anwendung

Für die Erkennung von oben nach unten lautet der Einstiegspunkt HTTP(s)-Endpunkt. Ausgehende Beziehungen bestehen zu Amazon EC2-Instanzen.

Von der ServiceNow AI Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können dieses Muster auf der ServiceNow-Plattform mit Version Kingston oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Führen Sie eine horizontale Erkennung mithilfe der Cloud-API (CAPI) aus. Dies ist erforderlich, da dieses Erkennungsmuster nur die Erkennung von oben nach unten unterstützt. Für Cloud-Discovery können Sie die horizontale Erkennung wie gewohnt ausführen.
- Wenn die Daten des Lastenausgleichsmoduls in der Configuration Management Database (CMDB) gespeichert wurden, erstellen Sie einen Anwendungsservice für jedes Lastenausgleichsmodul.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&LoadBalancerArns.member.1=<LB_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeListeners&LoadBalancerArn=<LB_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeRules&ListenerArn=<LISTENER_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeTargetHealth&TargetGroupArn=<TARGET_GROUP_ARN>&Version=2015-12-01
  - https://ec2.<REGION>.amazonaws.com/?Action=DescribeInstances&Version=2016-11-15&Filter.1.Name=instance-state-name&Filter.1.Value=running&Filter.2.Name=instance-id&Filter.2.Value=<INSTANCE_ID>
- Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-MappingVon ServiceNow Store.
- Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Load Balancer-Services [cmdb_ci_lb_service]	
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierte Domänenname (FQDN) des Lastenausgleichsmoduls. Der DNS-Name
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
Seriennummer [serial_number]	Seriennummer des Lastenausgleichsmoduls im folgenden Format: ##Object_ID=<LB_ARN>
Port [port]	Port des Lastenausgleichsmoduls
Objekt-ID [object_id]	Eindeutiger Bezeichner des Lastenausgleichsmoduls
IP-Adresse [ip_address]	IP-Adresse des FQDN

AWS Automatische Skalierung der Gruppen-Discovery mit Mustern

Die ® Discovery Die Anwendung verwendet das Muster „Amazon AWS – AutoScaling Groups (LP)“ und die Erweiterungen „Automatische Skalierung“, um zu finden AWS Gruppen für automatische Skalierung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Konfiguriert AWS Anmeldeinformationen

Konfigurieren Sie in Ihrer Instanz Anmeldeinformationen vom Typ **AWS-Anmeldeinformationen** Und legen Sie sie auf fest **Aktiv** . Weitere Informationen finden Sie unter Zugriffs-Setup für AWS-Service-Accounts .

Konfigurierter Cloud-Service-Account

Konfigurieren Sie AWS Service-Account gültig in ServiceNow Instanz. Weitere Informationen finden Sie unter Richten Sie AWS-Service-Accounts ein.

Konfigurierte Anwenderberechtigungen zum Ausführen des API-Aufrufs für automatische AWS-Skalierungsgruppen der Liste

Geben Sie die Anwenderberechtigung zum Ausführen der folgenden API an: https://autoscaling.amazonaws.com/?Action=DescribeAutoScalingGroups&Version=2011-01-01

Weitere Informationen finden Sie unter Discovery von Amazon AWS Cloud-Komponenten mithilfe von Mustern.

Konfigurierter Cloud-Discovery-Zeitplan

Erstellen Sie einen Cloud-Anwendungszeitplan für die Erkennung AWS Automatische Skalierung gruppiert und konfigurieren Sie die Attribute. Festlegen **Discovery** Bis **Cloud-**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung . Weitere Informationen finden Sie unter Erstellen Sie Zeitpläne für die Erkennung von Cloud-Ressourcen im Cloud-Discovery-Arbeitsbereich

Konfigurationen für AWS Gruppen für automatische Skalierung

Navigieren Sie zur Tabelle Haupt-CI (Instanzskalierungssatz), und stellen Sie sicher, dass die Konfigurationen wie folgt festgelegt sind:

Neue Felder für Tabelle – [cmdb_ci_instance_scale_Set]

Elementname	Typ	Bezeichnung	Max. Länge
Gewünschte_Kapazität	Ganzzahl	Gewünschte Kapazität	32
Min_size	Ganzzahl	Mindestgröße	32
max_size	Ganzzahl	Maximale Größe	32
Health_Check_type	Zeichenfolge	Integritätsprüfungstyp	128

AWS – Gruppen-Tags für automatische Skalierung

Die Mustererweiterung wird automatisch angezeigt und sammelt die Tags für automatische Skalierung (ab Release November 2022, Version 1,0.95).

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Amazon AWS – AutoScaling Groups (LP)“.

Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

Feld	Beschreibung
Objekt-ID [object_id]	Die Amazon Ressourcenname (ARN) der Gruppe „Automatische Skalierung“.
Name [name]	Die Amazon Ressourcenname (ARN) der Gruppe „Automatische Skalierung“.
Installationsstatus [install_status]	Installationsstatus der automatischen Skalierungsgruppe. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der automatischen Skalierungsgruppe. Der Standardwert ist betriebsbereit.
Gewünschte Kapazität [gewünschte_Kapazität]	Die gewünschte Größe der Gruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

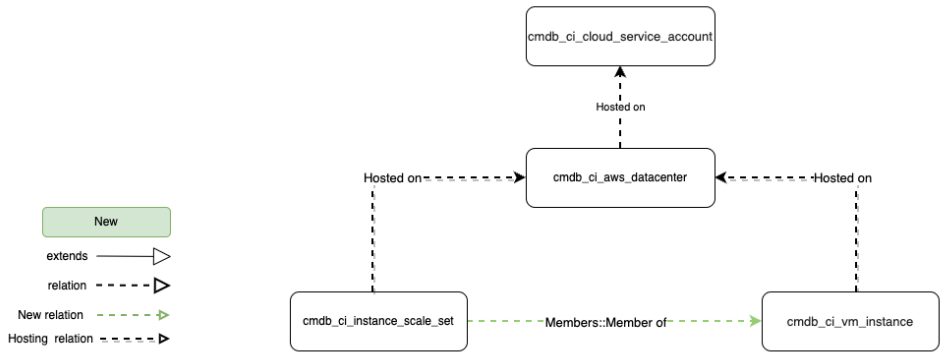
Instanzskalierungssatz [cmdb_ci_instance_scale_Set] (Fortsetzung)

Feld	Beschreibung
Maximale Größe [max_size]	Die maximale Größe der Gruppe.
Mindestgröße [min_size]	Die Mindestgröße der Gruppe.

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Objekt-ID [object_id]	Die Instanz-ID der virtuellen Maschine.

AWS Automatische EC2-Skalierung – Klassenmodell



CI-Beziehungen

CI	Beziehung	CI
AWS-Rechenzentrum [cmdb_ci_aws_datacenter]	Gehostet auf::Hostet	Service-Account [cmdb_ci_Cloud_Service_Account]
Instanzskalierungssatz [cmdb_ci_instance_scale_Set]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Instanzskalierungssatz [cmdb_ci_instance_scale_Set]	Mitglieder::Mitglied von	VM-Instanz [cmdb_ci_vm_instance] **Hinweis:** EC2-VM
Schlüsselwert [cmdb_key_value]	Nur Referenz	Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Discovery

Das Muster „Amazon AWS – AutoScaling Groups (LP)“ sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel des Ressourcen-Tags.
Wert [value]	Der Wert des Ressourcen-Tags.
Konfigurationselement [configuration_item]	Verweist auf den Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

AWS Discovery mithilfe von Mustern

AWS Klassische ELB-Service-Discovery mit Mustern

Discovery verwendet das Erkennungsmuster „Amazon AWS Classic ELB Service“, um alle Lastenausgleichsmodule zu finden, die HTTP- und HTTPS-Datenverkehr verwenden.

Elastic Load Balancing (ELB) verteilt eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele.

Das Erkennungsmuster „Amazon AWS Classic ELB Service“ unterstützt die Erkennung von oben nach unten. Die zwei möglichen Einstiegspunkte für die Erkennung von oben nach unten sind der HTTP(s)-Endpunkt und der TCP-Endpunkt. Ausgehende Beziehungen bestehen zu Amazon EC2-Instanzen.

Von der ServiceNow AI Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Sie können dieses Muster auf der ServiceNow-Plattform mit Version Jakarta oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Führen Sie eine horizontale Erkennung mithilfe der Cloud-API (CAPI) aus. Dies ist erforderlich, da dieses Erkennungsmuster nur die Erkennung von oben nach unten unterstützt. Für die Cloud-Erkennung können Sie die horizontale Erkennung wie gewohnt ausführen.
- Wenn die Daten des Lastenausgleichsmoduls in der Configuration Management Database (CMDB) gespeichert wurden, erstellen Sie einen Anwendungsservice für jedes Lastenausgleichsmodul.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&Version=2012-06-01&LoadBalancerNames.member.1=<LB_NAME>
- https://ec2.<REGION>.amazonaws.com/?Action=DescribeInstances&Version=2016-11-15&Filter.1.Name=instance-state-name&Filter.1.Value=running&Filter.2.Name=instance-id&Filter.2.Value=<INSTANCE_ID> (to create relation between LB and EC2 instance)

- Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-Mapping Von ServiceNow Store.
- Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Load Balancer-Services [cmdb_ci_lb_service]	
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierte Domänenname (FQDN) des Lastenausgleichsmoduls. Der DNS-Name
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
Back-End-Port [back_end_port]	Port der Instanz
Server-Port [server_port]	Port der Instanz
Port [port]	Port des Lastenausgleichsmoduls
Front-End-Port [front_end_port]	Port des Lastenausgleichsmoduls
Objekt-ID [object_id]	LB-Port
IP-Adresse [ip_address]	IP-Adresse des FQDN
Serverprotokoll [server_protocol]	Protokoll der Instanz.
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	Die IP-Adresse des Lastenausgleichsmodul-FQDN
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Netzmaske [netmask]	0.0.0.0

AWS Cognito-Discovery mit Mustern

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden das Muster „Amazon AWS Cognito“, um Authentifizierungs-, Autorisierungs- und Benutzerverwaltungsfunktionen für AWS-Kunden bereitzustellen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können dieses Muster auf der ServiceNow AI Platform mit London Patch 8, Madrid Patch 2 oder spätere Releases verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Benutzerberechtigungen

Gewähren Sie einem Benutzer eine Leseberechtigung, um die folgende API auszuführen:

- https://cognito-idp.<region>.amazonaws.com
- Methode: POST
- Body: {\"MaxResults\": 10}
- Headers: X-Amz-Target:AWSCognitoIdentityProviderService.ListUserPools,Content-Type:application/x-amz-json-1.0

AWS-Anmeldeinformationen

Konfigurieren Sie auf Ihrer Instanz Anmeldeinformationen des Typs **AWS-Anmeldeinformationen**, und setzen Sie sie auf **Aktiv**.

Cloud-Servicekonto

Konfigurieren Sie auf Ihrer Instanz das Cloud-Servicekonto vom Typ **AWS-Rechenzentrum**, und setzen Sie es auf **AWS-Konto-ID** . Verwenden Sie die zuvor in **AWS-Anmeldeinformationen** definierten Anmeldeinformationen.

Discovery Zeitplan

Erstellen Sie einen Cloud-Anwendungszeitplan für die Erkennung von AWS Cognito, und konfigurieren Sie die Attribute. Legen Sie Erkennung auf **Cloud-Anwendung** fest.

Ausführungsmuster

Erstellen und definieren Sie das Ausführungsmuster ohne Server für die Erkennung von Cloud-Anwendungen.

1. Erstellen Sie neue **Cloud-Ausführungsmuster**.
2. Definieren Sie den **Namen**.
3. Stellen Sie sicher, dass **Aktiv** auf „true“ gesetzt ist.
4. Stellen Sie sicher, dass die **Domäne** global ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie das **AWS-Muster** aus, das Sie ausführen möchten.
6. Erstellen Sie mehrere Datensätze, wenn Sie mehrere Muster ausführen möchten.

Erkennungszeitplan für vollständige AWS Discovery

Erstellen Sie einen Erkennungszeitplan aus dem **Cloud-Servicekonto**, das im vorherigen Verfahren erstellt wurde.

1. Klicken Sie auf **Discover Datacenter (Rechenzentren erkennen)**, und warten Sie, bis der Vorgang abgeschlossen ist.
2. Klicken Sie auf **Discovery Zeitplan erstellen**.
3. Dieser neue Zeitplan wird unter dem Discovery-Zeitplan erstellt und führt alle AWS-Muster aus.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery und Service-Mapping während der horizontalen Erkennung und der Erkennung von oben nach unten erfasste Daten

Das Muster „AWS Cognito“ sammelt Daten.

Vom Muster „AWS Cognito“ gesammelte Informationen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_authentication	
name	Ein beschreibender Name, der zur Identifizierung des Benutzer-Pools verwendet wird
object_id	Sie entspricht der account_id und wird von IRE-Identifizierungsregeln verwendet.
Fqdn	Beispiel für eine ARN: arn:aws:cognito-idp:eu-west-1:751200741520:userpool/eu-west-1_fim5E2mix

Tags werden auch von einem Erweiterungsabschnitt gesammelt, der dem Muster entsprechend ausgeführt wird. Die Tagging-API für AWS gibt den Ressourcentyp Cognito an.

Gesammelte Informationen aus den AWS Cognito-Tags

Feld	Beschreibung
cmdb_key_value	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gesammelte Informationen aus den AWS Cognito-Tags (Fortsetzung)

Feld	Beschreibung
key	Der tatsächliche Tag-Schlüssel
Wert	Der Tag-Wert
configuration_item	Die eindeutige Ressourcen-ID (ARN), die die Ressource in der AWS-Konsole identifiziert

CI-Beziehungen

Das Muster „AWS Cognito“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Cloud-Authentifizierung [cmdb_ci_cloud_authentication]	Hostet::Gehostet auf	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS DB-Cluster-Discovery mit Mustern

ServiceNow Discovery verwendet das Erkennungsmuster für AWS-DB-Cluster, um Aurora-DB-Cluster, serverlose Aurora-Ressourcen, Amazon Neptune-DB-Instanzen und Amazon DocumentDB-Instanzen zu suchen und zuzuordnen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Die erkannten DB-Cluster bilden neue Beziehungen mit den DB-Instanzen, die mit dem Muster „AWS Relational Database Service“ erkannt wurden. Daher wird das Muster für AWS-DB-Cluster während der Erkennung nach dem Muster „AWS Relational Database Service“ ausgelöst. Weitere Informationen finden Sie unter Amazon Relativer Datenbankservice (Amazon RDS) Discovery mit Mustern.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung Discovery and Service Mapping Patterns (Version 1.0.75) aus dem ServiceNow Store.
- Konfigurieren Sie auf der ServiceNow AI Platform die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Erstellen Sie ein Servicekonto. Legen Sie die **Konto-ID** auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBClusters
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances&DBInstanceIdentifier=<input_object_id> for events discovery
  - https://tagging.<REGION>.amazonaws.com/ for tags discovery
- Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-Mapping Von ServiceNow Store.
- Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Cloud-Datenbankcluster [cmdb_ci_cloud_db_cluster]	
Cluster-ID [cluster_id]	Enthält einen vom Benutzer angegebenen Bezeichner für das DB-Cluster. Dieser Bezeichner ist der eindeutige Schlüssel, der ein DB-Cluster identifiziert.
Name [name]	Enthält den Namen der ursprünglichen Datenbank des DB-Clusters, die bei der Erstellung angegeben wurde. Wenn kein Name angegeben wurde, wird der Clusterbezeichner als Name verwendet. Dieser Name wird für die Lebensdauer des DB-Clusters zurückgegeben.
FQDN [fqdn]	Gibt den Verbindungsendpunkt für die primäre Instanz des DB-Clusters an.
TCP-Port [tcp_port]	Port des Datenbankendpunkts
Anbieter [vendor]	Der Anbieter, Amazon
Clusterstatus [cluster_status]	Gibt den aktuellen Status dieses DB-Clusters an.
Betriebsstatus [operational_status]	Status der Datenbank; „Verfügbar“, wenn betriebsbereit.
Cloud-Datenbank [cmdb_ci_cloud_database]	
Objekt-ID [object_id]	Der Instanzbezeichner für dieses Mitglied des DB-Clusters. **Hinweis:** Für Datenbankinstanzen wird diese Tabelle nur mit dem Attribut object_id gefüllt. Dieses Attribut ist für die Identifizierung von CIs der Cloud-Datenbank erforderlich, um sicherzustellen, dass Beziehungen zwischen den CIs und den Cloud-Datenbankclustern hergestellt werden können.
Name [name]	Enthält den Namen der ursprünglichen Datenbank des DB-Clusters, die bei der Erstellung angegeben wurde. Wenn kein Name angegeben wurde, wird der Clusterbezeichner als Name verwendet. Dieser Name wird für die Lebensdauer des DB-Clusters zurückgegeben.
FQDN [fqdn]	Gibt den Verbindungsendpunkt für die primäre Instanz des DB-Clusters an.
TCP-Port [tcp_port]	Port des Datenbankendpunkts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Anbieter [vendor]	Der Anbieter, Amazon
Betriebsstatus [operational_status]	Status der Datenbank; „Verfügbar“, wenn betriebsbereit.
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse des Cloud DB Cluster Writer-Endpunkts.
Name [name]	IP-Adresse.
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
Netzmaske [netmask]	IP-Netzmaske [0.0.0.0].

CI-Beziehungen

CI	Beziehung	CI
cmdb_ci_cloud_db_cluster	Cluster aus::Cluster	cmdb_ci_cloud_database
cmdb_ci_cloud_database	Gehostet auf::Hostet	cmdb_ci_aws_datacenter
cmdb_ci_cloud_db_cluster	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_ci_cloud_database	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_db_cluster
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_database

AWS DynamoDB-Discovery mit Mustern

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden das Muster „Amazon AWS DynamoDB“, um Komponenten von DynamoDB zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Amazon AWS DynamoDB-Muster stellt REST-APIs zum Abrufen von Informationen zu DynamoDB bereit. Sie können auch konfigurieren Service-Mapping Und Discovery Um zu erkennen AWS DynamoDB-Komponenten mit AWS Ereignisse.

Von der ServiceNow AI Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anwenderzugriff

Auf der AWS Konsole, gewähren Sie einem Anwender die folgenden Berechtigungen: AmazonDynamoDBReadOnly Access und AWSLambdaInvocation-DynamoDB.

Cloud-Serviceaccount

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Servicekonto auf der ServiceNow AI Platform® mit den folgenden Eigenschaften ein:

- Ein **Account-ID** , Welches ist Amazon Account-ID, zu der DynamoDB gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
- Das entsprechende AWS Anmeldeinformationen, die für die Account-ID erforderlich sind, um zu erreichen AWS Cloud.

AWS Anmeldeinformationen

Auf der ServiceNow AI Platform®, Konfigurieren AWS Anmeldeinformationen mit einem geheimen Schlüssel und einem Zugriffsschlüssel.

Einstiegspunkt für einen Service, der DynamoDB enthält

Verwenden *AWS***Ressourcenname – Endpunkt** Als Einstiegspunkttyp beim Erstellen eines Service mit DynamoDB. Geben Sie den Amazon-Ressourcennamen (ARN) und den Host für den Einstiegspunkt an.

(Für Top Down-Discovery durch Service-Mapping) Führen Sie eine Horizontal-Discovery der logischen Rechenzentren durch.

Erkennen Sie logische Rechenzentren, die DynamoDBs hosten, wie unter Discovery auf ausführen beschrieben AWS Cloud-Service-Account in ServiceNow Cloud Provisioning and Governance Dokumentation.

Cloud-Discovery

Laden Sie für Cloud-Discovery das Muster für Discovery und Service-Mapping aus dem ServiceNow Store herunter.

MID-Server

Wenn Sie den MID-Server installieren, vergewissern Sie sich, dass der Hostcomputer die Systemanforderungen für den MID-Server erfüllt oder übertrifft.

Discovery-Zeitplan

Erstellen Sie einen Zeitplan für das relevante AWS Service-Account wie unter Discovery für einen Service-Account planen in beschrieben ServiceNow Cloud Provisioning and Governance Dokumentation.

Konfigurieren AWS Ereignisservice

Um die warnungsbasierte Discovery zu aktivieren, konfigurieren Sie AWS Ereignisservice wie unter „Setup“ beschrieben AWS Ereignisverarbeitung für Discovery Und Service-Mapping In ServiceNow Cloud Provisioning and Governance Dokumentation.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: *arn:aws:dynamodb::xxxxxxxxxxxx:table:<table name>*
DynamoDB-Tabelle [cmdb_ci_dynamodb_table]	
Name [name]	Tabellenname.
Erstellungsdatum [creation date]	Erstellungsdatum der DynamoDB gemäß der Zeitzone des MID-Server s, der diese DynamoDB erkennt.
Cloud-Anbieter [cloud_provider]	Amazon AWS
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: *arn:aws:dynamodb:<region>:xxxxxxxxxxxx:table:<tab name>*
Globale ARN [global_arn]	Die globale ARN der Tabelle für die globale DynamoDB-Tabelle. Dieses Feld ist leer, wenn die DynamoDB nicht global ist.
Stream-ARN [stream_arn]	Die Auswahlmöglichkeiten sind: • Stream-ARN • Deaktiviert
Servicename [service_name]	Standardmäßig auf **DynamoDB** festgelegt
Verschlüsselung [encryption]	Verschlüsselungskonfiguration auf der DynamoDB Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Replikationsgruppe [replication_group]	Tabellen-ARN der verbundenen globalen DynamoDB-Tabellen
Automatische Skalierung lesen [read_autoscaling]	Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Einheiten lesen [read_units]	Die Anzahl der gelesenen Einheiten in der DynamoDB-Tabelle
Max. Einheiten zum Lesen [read_max_units]	Die maximal zulässige Anzahl der gelesenen Einheiten in der DynamoDB-Tabelle
Min. Einheiten zum Lesen [read_min_units]	Die zulässige Mindestzahl an gelesenen Einheiten in der DynamoDB-Tabelle

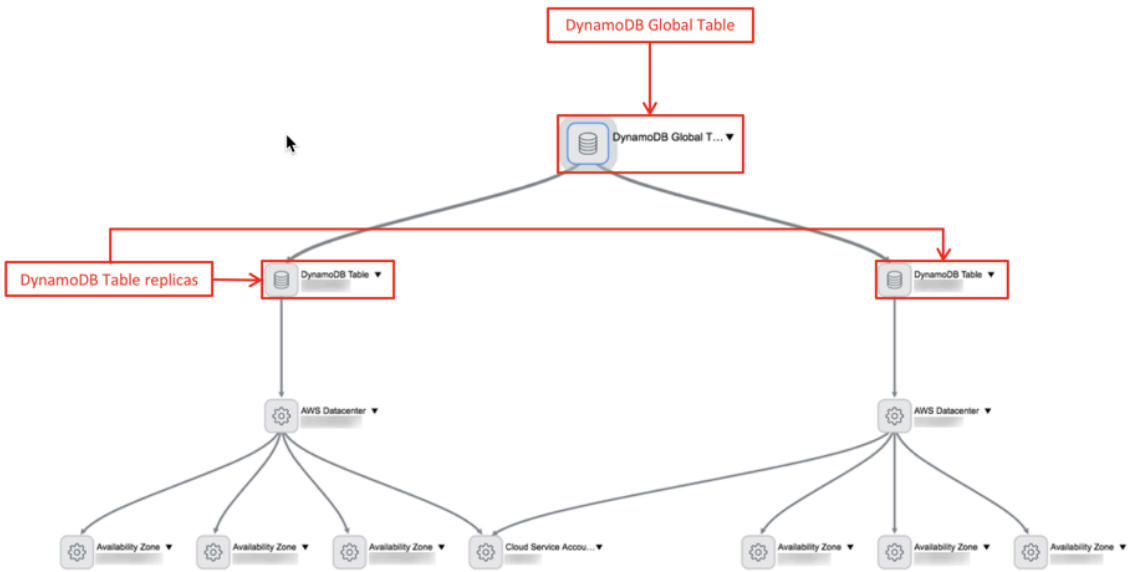
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Einheiten zum Schreiben [write_units]	Die Anzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Max. Einheiten zum Schreiben [write_max_units]	Die maximal zulässige Anzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Min. Einheiten zum Schreiben [write_min_units]	Die zulässige Mindestzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Tabellengröße [table_size]	Die derzeit bereitgestellte Größe der DynamoDB-Tabelle in Byte
Automatische Skalierung schreiben [write_autoscaling]	Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Zeitpunkt [point_in_time]	Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert

Die Grafik zeigt CIs, die Teil der DynamoDB-Erkennung sind.

Abhängigkeitsansichten mit DynamoDB-Komponenten



CI-Beziehungen

Das Muster „Amazon AWS DynamoDB“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	Cluster von::Cluster	DynamoDB-Tabelle [cmdb_ci_dynamodb_table]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Das Muster „Amazon AWS DynamoDB“ identifiziert Verbindungen von der DynamoDB zu AWS Lambda-Funktionen.

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Als Teil der Erstellung oder Änderung eines Erkennungsmusters können Sie den Vorgang **Cloud-REST-Abfrage** verwenden, um Informationen aus Konfigurationselementen (CIs) des PaaS-Typs (Platform as a Service) zu extrahieren, z. B. Microsoft Azure oder Amazon Web Services.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfen Sie, ob das Betriebssystem des CI, für das Sie den Vorgang „Cloud-REST-Aufruf“ verwenden möchten, den Betriebssystemtyp des logischen Datenzentrums [cmdb_ci_logical_datacenter] erweitert:
  1. Navigieren zu **Musterdesigner** > **Discovery-Muster**an.
  2. Doppelklicken Sie auf das relevante Muster, um es im Musterdesigner zu öffnen.
  3. Klicken Sie auf die Registerkarte **Standard**.
  4. Beachten Sie das Betriebssystem für dieses CI.
  5. Navigieren zu **Systemdefinition** > **Tabellen**an.
  6. Legen Sie das Suchfeld auf **Bezeichnung** fest und geben Sie den Namen des Betriebssystems ein, wie auf der Registerkarte **Standard** des Musters angegeben.
  7. Suchen Sie das Betriebssystem in der Liste, und stellen Sie sicher, dass das logische Rechenzentrum in der Spalte **Erweitert Tabelle** angezeigt wird.
- Navigieren Sie zu dem entsprechenden Pattern-Schritt:
  1. Wählen Sie auf dem Musterformular den entsprechenden Identifikationsteil für aus Discovery .

     Alternativ wählen Sie den entsprechenden Identifikations- oder Verbindungsabschnitt für aus Service-Mapping .
  2. Wählen Sie den entsprechenden Musterschritt aus, oder klicken Sie auf das Symbol **Schritt darüber hinzufügen**, um einen Schritt hinzufügen.

Grundkenntnisse in der Programmierung sind wünschenswert.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie den Cloud-REST-Aufrufvorgang in Mustern für die Erkennung von PaaS-CIs bereit. Dieser auf Java-Skript basierende benutzerdefinierte Vorgang ist nur verfügbar, nachdem Musterversion 1.0.24 oder höher aus dem ServiceNow Store heruntergeladen wurde. Verwenden Sie diesen Vorgang anstelle des im Standardsystem verfügbaren Cloud-REST-Aufrufvorgangs.

In der offiziellen Dokumentation der API-Hersteller finden Sie die Abfragesyntax für das Gerät, das Sie mit dem Vorgang Cloud-REST-Abfrage abfragen möchten. Beispiel:

- http://docs.aws.amazon.com/AWSEC2/latest/APIReference/Welcome.html
- https://docs.microsoft.com/en-us/rest/api/apimanagement/

Prozedur

1. Wählen Sie **Cloud-REST-Abfrage** aus der Liste **Vorgang** aus.
2. Definieren Sie Abfrageparameter nach Bedarf:

> **Hinweis:** Wenn Sie diesen Vorgang angepasst haben, können die Abfrageparameter unterschiedlich sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
URL	Geben Sie die URL wie in der offiziellen Microsoft Azure- oder Amazon Web Services-Dokumentation beschrieben an. Sie können Variablen verwenden. Sie können auch einen Wert aus einem bestimmten Feld in einer tabellarischen Variable eingeben.
Methode	Geben Sie den Methodenwert als Zeichenfolge in Großbuchstaben ein, z. B. „GET“. Unterstützte Methoden: ○ GET ○ POST ○ PUT Weitere Informationen finden Sie im entsprechenden API-Leitfaden. Wenn die HTTP-Abfragemethode in der API-Dokumentation nicht ausdrücklich erwähnt wird, verwenden Sie die GET-Methode.
Textkörper	(Optional) Geben Sie einen Anforderungstext als Zeichenfolge ein. Wenn die Zeichenfolge Anführungszeichen enthält, verwenden Sie den umgekehrten Schrägstrich vor den Anführungszeichen, um anzugeben, dass die Zeichenfolge nicht bei den Anführungszeichen endet.
Header	(Optional) Wenn die relevante API-Dokumentation besagt, dass HTTP-Header gesendet werden müssen, geben Sie diese Header im folgenden Format ein: Header_name1:header_value1,header_name2:header_value Zum Beispiel: Content-Type:xml.
Formatiert	JSON formatiert oder nicht

Automatische Übersetzung

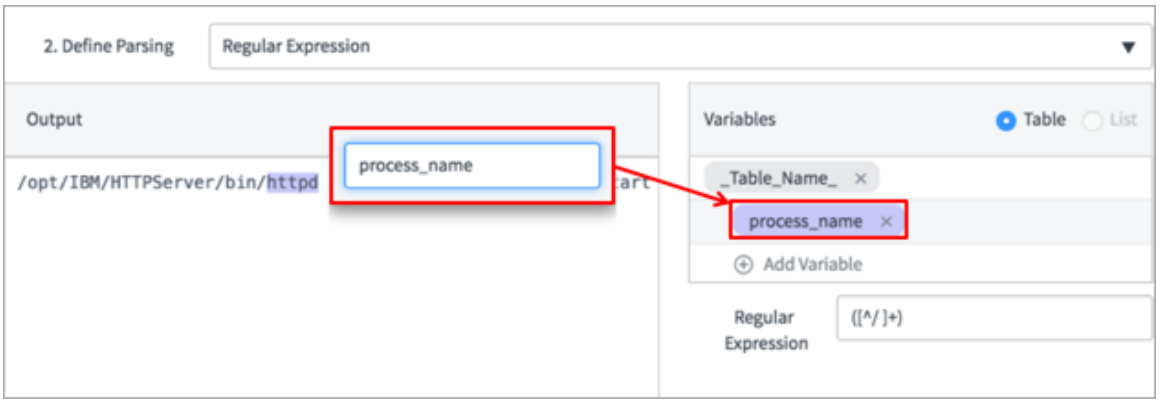
3. Wenn Sie die gesamte Befehlsausgabe als Variable speichern möchten, klicken Sie in der Liste **Analyse definieren** auf KEINE, und definieren Sie die Variable.
4. Wählen Sie die Parsing-Strategie aus der Liste **Analyse definieren** aus.
5. Wenn Sie im Debug-Modus arbeiten, definieren Sie die Analysekriterien wie folgt:

   a. Klicken Sie auf **Vorgang ausführen**, um das Ergebnis im Bereich **Ausgabe** anzuzeigen.

   b. Im Feld **Ausgabe** markieren Sie Text oder Symbole, der/die eine Variable enthalten soll/sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie im Feld Variablenname den Namen für die neue Variable ein, beispielsweise 'process_name'.

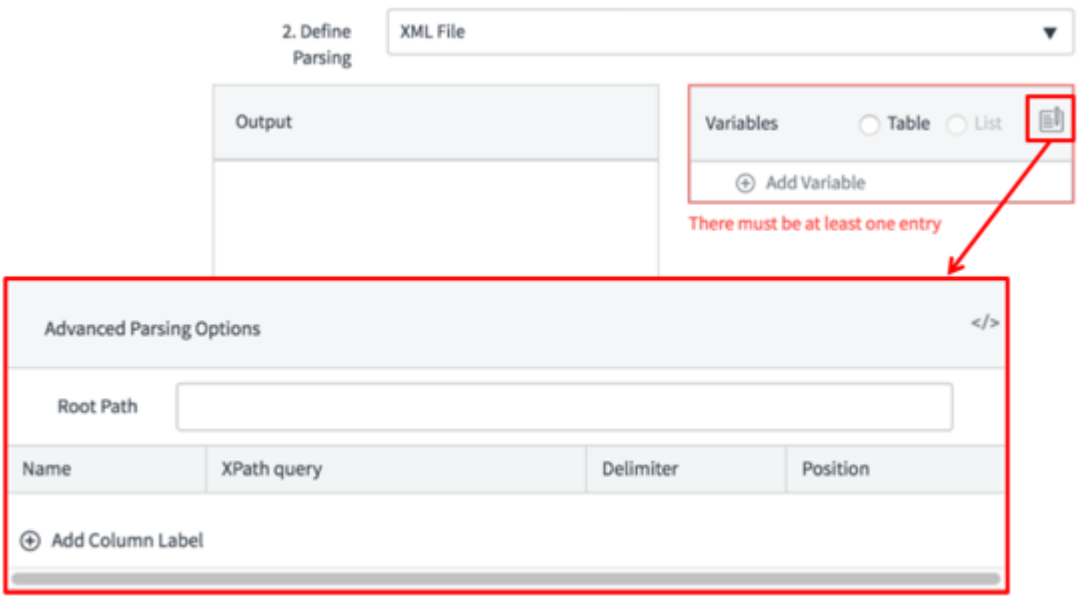


d. Drücken Sie die **Eingabetaste**.
Die neue Variable wird im Feld **Variablen** hinzugefügt.

6. Wenn Sie nicht im Debug-Modus arbeiten, definieren Sie die Analysekriterien wie folgt:

a. Klicken Sie im Variablenbereich auf **Variable hinzufügen**, und geben Sie den Namen für die neue Variable ein.

b. Klicken Sie auf das Symbol **Erweitert**.



c. Klicken Sie auf **Spaltenbezeichnung hinzufügen**.

d. Geben Sie die Analyse-Abfrage ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

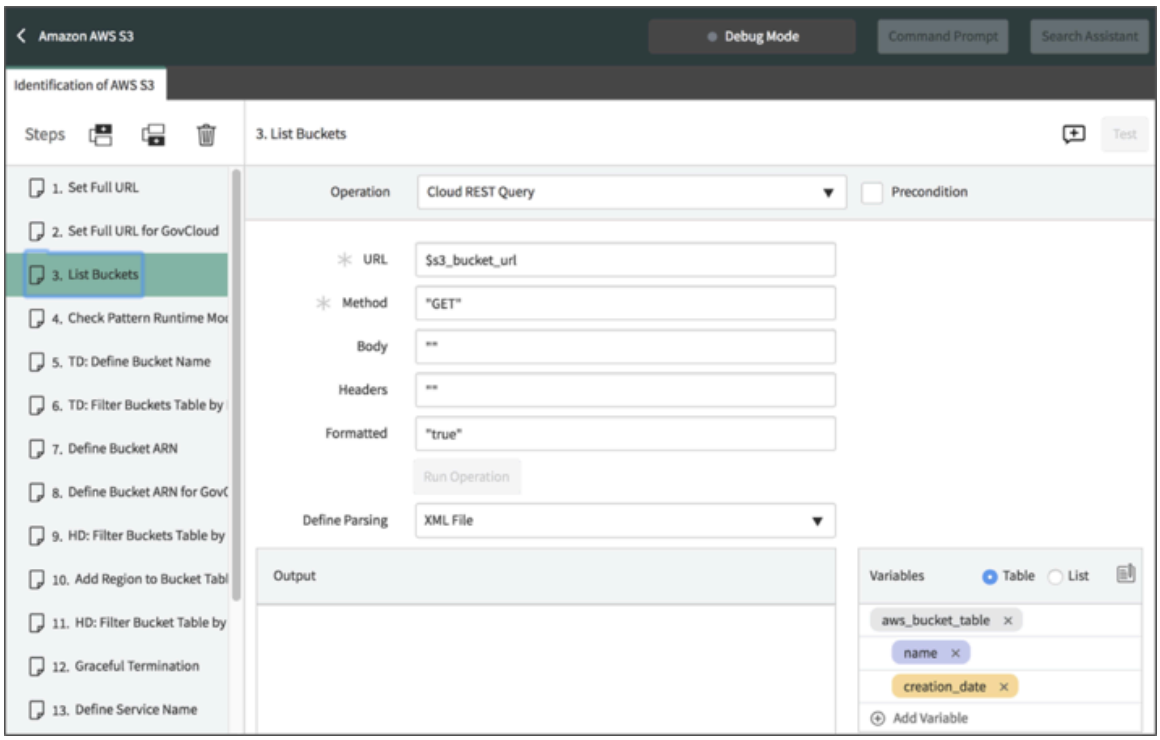
e. Geben Sie einen Wert für das Trennzeichen ein.

f. Geben Sie einen Wert für die Position ein.

7. Wählen Sie **Beenden**, um die Erkennung zu stoppen, wenn keine Ergebnisse gefunden werden.

Example:

Diese Operation wird verwendet in	Dieses Objekt
Hierarchie	Applikation
CI-Typ	Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]
Muster	Amazon AWS S3
Abschnitt	Identifizierung von AWS S3
Schrittnummer und -Name	3. Buckets auflisten



Verwenden Sie den Cloud-REST-Abfragevorgang, um Informationen zu AWS-Buckets, deren Namen und Erstellungsdaten zu extrahieren.

AWS ElastiCache-Discovery mit Mustern

Von der Anwendung ServiceNow® Discovery wird das Amazon ElastiCache-Erkennungsmuster dazu verwendet, Redis-Cluster zu ermitteln, die als Teil des ElastiCache-Service bereitgestellt werden. ElastiCache ist sowohl mit Redis als auch mit Memcached kompatibel, mit dem Muster werden jedoch nur Informationen für Redis gesammelt.

Amazon ElastiCache ist ein vollständig verwalteter In-Memory Caching-Service, der in AWS verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - https://elasticache.{region}.amazonaws.com?Action=DescribeReplicationGroups&Version=2015-02-02
  - https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Replikationsgruppen werden in der Tabelle „Cloud-Datenbankcluster“ [cmdb_ci_cloud_db_cluster] gespeichert, und Knotengruppenmitglieder werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name der Ressource für jede Replikationsgruppe und jedes Knotengruppenmitglied.
FQDN	Vollqualifizierter Domänenname für jedes Knotengruppenmitglied.
Port	Port, der von jedem Knotengruppenmitglied verwendet wird.

AWS Keyspaces-Discovery mit Mustern

Von der Anwendung ServiceNow® Discovery wird das Amazon Keyspaces-Erkennungsmuster dazu verwendet, den mit Amazon Keyspaces verwalteten Apache Cassandra-kompatiblen Datenbankservice zu ermitteln.

Amazon Keyspaces ist ein verwalteter Apache Cassandra-kompatibler Datenbankservice. Von einem Keyspace werden zugehörige Tabellen gruppiert, die für mindestens eine Anwendung relevant sind. Der Keyspace enthält mindestens eine Tabelle und definiert die Replikationsstrategie für alle enthaltenen Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Installieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - https://cassandra.{region}.amazonaws.com {Content-Type:application/x-amz-json-1.0, , X-Amz-Target: KeyspacesService.ListKeyspaces}
  - https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Keyspaces werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name des Keyspace
FQDN	Vollqualifizierter Domänenname der Region, in der sich der Keyspace befindet.
Port	Port für eingehende TLS-Verbindungen (9142).

AWS Kinesis-Discovery mit Mustern

Die ServiceNow® Discovery-Anwendung verwendet Amazon Kinesis-Discovery-Muster, um verfügbare Kinesis-Services zu finden Amazon Web Services(AWS).

Kinesis ist ein verwaltetes, skalierbares, AWS Cloud-basierter Service, der die Echtzeitverarbeitung von Streaming großer Datenmengen pro Sekunde ermöglicht. AWS Kinesis enthält vier Arten von Services:

- Kinesis-Video-Streams: Erfassen, verarbeiten und speichern Sie Video-Streams für Analytics und maschinelles Lernen.
- Kinesis-Datenströme: Ein vollständig verwalteter Streaming-Datenservice.
- Kinesis-Daten-Firehose: Lädt Datenströme in AWS-Datenspeicher.
- Kinesis Data Analytics: Verarbeiten und analysieren Sie Streaming-Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ aus dem ServiceNow Store.
- Überprüfen Sie die folgenden Plugin-Versionen:
  - Muster für Discovery und Service-Mapping 1.0.93 oder höher (sn_itom_pattern)
  - CMDB CI-Klassenmodelle Version 1.40.0 oder höher (sn_cmdb_ci_class)

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten enthalten die folgenden Felder in der Tabelle „Cloud-Datenbank“ [cmdb_ci_aws_Kinesis].

Feld	Beschreibung
Objekt-ID	Name der Streamressource.
Name	Der Name des Streams. • Kinesis-Daten: cmdb_ci_aws_Kinesis_Data • Kinesis-Video: cmdb_ci_aws_Kinesis_Video • Kinesis-Firehose: cmdb_ci_aws_Kinesis_Firehose • Kinesis-Daten-Analytics: cmdb_ci_aws_Kinesis_Data_Analytics
Status	Der Status des Streams.

Konfigurationselement (CI)-Beziehungen

CI	Beziehung	CI
AWS Kinesis Data	Gehostet auf::Hostet	AWS-Rechenzentrum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
AWS Kinesis – Video	Gehostet auf::Hostet	AWS-Rechenzentrum
AWS Kinesis Firehose	Gehostet auf::Hostet	AWS-Rechenzentrum
AWS Kinesis – Daten-Analytics	Gehostet auf::Hostet	AWS-Rechenzentrum

AWS Lambda-Discovery mit Mustern

Die Anwendungen ServiceNow Discovery und Service-Mapping können Lambda-Funktionen suchen und zuordnen, die in Ihrer AWS-Cloud ausgeführt werden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery und Service-Mapping verwenden das Muster „Amazon AWS Lambda“, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Wenn Sie die Cloud-Erkennung ausführen, fragt Ihre Instanz Ihr AWS-Servicekonto mit den erforderlichen Anmeldeinformationen ab und führt dann eine Abfrage aus, um Lambda-Informationen zu erhalten. Das Muster analysiert diese Informationen, die dann in der CMDB gespeichert werden.

Sie können dieses Muster auf der ServiceNow-Plattform mit Jakarta Patch 10, Kingston Patch 8 oder London Patch 1 verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Update Set

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, importieren Sie das Update Set, das in „KB0679927 : AWS Lambda top-down discovery update set (Update Set für AWS Lambda-Erkennung von oben nach unten)“ bereitgestellt wird. Dieses Update Set ist für Service-Mapping erforderlich.

Benutzerrichtlinie für AWS-Benutzer

Wenn Sie Identity and Access Management (IAM) verwenden, um Benutzer auf der AWS-Plattform (Amazon Web Services) zu verwalten, stellen Sie sicher, dass Sie eine Benutzerrichtlinie für den AWS-Benutzer erstellt haben. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern in der Dokumentation zu ServiceNow Cloud Provisioning and Governance.

AWS-Servicekonto mit Anmeldeinformationen

Sie müssen Ihr Servicekonto mit den entsprechenden AWS-Anmeldeinformationen einrichten. Sie führen die Erkennung über das Servicekonten-Formular aus.

Weitere Informationen zu Servicekonten für Discovery und Service-Mapping finden Sie in der Produktdokumentation.

Servicekonto

Erstellen Sie ein Servicekonto auf der ServiceNow-Plattform. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der AWS Lambda gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird. Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Logische Rechenzentren mithilfe der horizontalen Erkennung erkennen

Klicken Sie im Formular „Cloud-Servicekonto“ unter **Zugehörige Links** auf **Rechenzentren erkennen**.

Benutzerberechtigungen

Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der ListFunctions-API mit der Ressource: arn:aws:lambda:region:account-id: function:function-name. Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der GetFunction-API mit der Ressource: „*“.

Amazon-Ressourcenname (ARN)

(Optional für Anwendungsservices, die ARN als Einstiegspunkt verwenden) Stellen Sie sicher, dass Sie den ARN für das zu erkennende AWS Lambda kennen. ARNs dienen als Ressourcenbezeichner für Amazon Web Services.

Host

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, verwenden Sie den folgenden Host: 127.0.0.1.

Cloud-Discovery

Für Cloud-Discovery, Laden Sie herunter Muster für Discovery und Service-Mapping Von ServiceNow Store.

MID-Server

Bei der Installation von MID-Server, Stellen Sie sicher, dass der Hostcomputer die erfüllt oder überschreitet Systemanforderungen des MID-Servers Veröffentlicht am ServiceNow Dokumentationswebsite.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Horizontale Erkennung trägt diese Daten in die CMDB ein:

Tabelle und Feld	Beschreibung
Cloud-Funktion [cmdb_ci_cloud_function]	
Name [name]	Der Name der Funktion
Objekt-ID [object_id]	Die ID (Amazon-Ressourcenname) der AWS Lamdba-Funktion, z. B. `arn:aws:lambda:{datacenter}1:751200741520:function:{function-name}`
Version [version]	Die Version der Funktion. Beispielsweise steht `$Latest` für die neueste veröffentlichte Version.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Sprache [language]	Die Laufzeitumgebung oder Sprache und Version, in der die Funktion geschrieben ist, z. B. `Node.js6.10` für JavaScript Version 6.10.
Code-Speicherort-URL [code_location_url]	Die URL der Funktion, die Sie über die API Gateway-Konsole erstellt haben
CodeSha256 [codesha256]	Die kryptografische Hash-Signatur für die Funktion
Codegröße [code_size]	Die Größe des Funktionscodes in MB
Letzte Änderung an der Funktion [function_last_modified]	Das Datum, an dem die Funktion in Ihrer AWS Lamdba-Umgebung zuletzt geändert wurde

Hinweis: Um alle diese Felder anzuzeigen, müssen Sie das Formularlayout wie in der Produktdokumentation beschrieben konfigurieren.

CI-Beziehungen

Diese Beziehungen sollen die AWS Lambda-Erkennung unterstützen:

CI	Beziehung	CI
Cloudfunktion [cmdb_ci_cloud_function]	Verwendet::Verwendet von	Cloud-Datenbank [cmdb_ci_cloud_database]
	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter] Das AWS-Rechenzentrum hat Beziehungen zu anderen AWS-CIs, z. B. Verfügbarkeitszonen, Servicekonten usw. Weitere Informationen finden Sie unter AWS und Azure Cloud-Erkennung in der Produktdokumentation.
	Stellt bereit::Bereitgestellt von	Cloud Event-Quelle [cmdb_ci_cloud_event_source] Dieses CI kann eine beliebige Event-Quelle sein, die die Cloud-Funktion oder das API-Gateway auslöst.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten von AWS Lambda im Kontext von Anwendungsservices durch. Es erkennt ausgehende Verbindungen von AWS Lambda:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AWS API-Gateway
- Amazon Relational Database Service (RDS)
- Weitere Instanz von AWS Lambda innerhalb oder außerhalb der aktuellen Region, die ARN verwendet

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

AWS MemoryDB für Redis-Discovery mit Mustern

Die ® Discovery-Anwendung verwendet AWS MemoryDB für Redis-Muster und Erweiterungen zu finden AWS Arbeitsspeicher-DB für Redis. Um einige dieser Ressourcen zu erkennen, muss installiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ® Speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Konfiguriert AWS Anmeldeinformationen

Konfigurieren Sie in Ihrer Instanz Anmeldeinformationen vom Typ **AWS-Anmeldeinformationen** . Weitere Informationen finden Sie unter Zugriffs-Setup für AWS-Service-Accounts .

Konfigurierter Cloud-Service-Account

Konfigurieren Sie AWS Service-Account gültig in ServiceNow Instanz. Weitere Informationen finden Sie unter Richten Sie AWS-Service-Accounts ein.

Konfigurierte Anwenderberechtigungen zum Ausführen der Liste AWS MemoryDB für Redis-API-Aufrufe

Geben Sie die Anwenderberechtigung zum Ausführen der folgenden API an:

- https://memory-db.{region}.amazonaws.com?Action=DescribeClusters&ShowShardDetails=true
- https://memory-db.{region}.amazonaws.com?Action=ListTags&ResourceArn={ARN}

Weitere Informationen finden Sie unter Discovery von Amazon AWS Cloud-Komponenten mithilfe von Mustern.

Konfigurierter Cloud-Discovery-Zeitplan

Erstellen Sie einen Cloud-Anwendungszeitplan für die Erkennung AWS Rechenzentren. Festlegen **Discovery** Bis **Cloud-Discovery** . Weitere Informationen finden Sie unter: Erstellen Sie Zeitpläne für die Erkennung von Cloud-Ressourcen im Cloud-Discovery-Arbeitsbereich

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten, die während erfasst wurden AWS Arbeitsspeicher-DB für Redis Horizontale Discovery

Feld	Beschreibung
Haupt-CI [cmdb_ci_Cloud_database]	
ARN	Der Amazon-Ressourcenname eines einzelnen Knotens im Cluster. Die Werte werden in der Spalte Objekt-ID [object_ID] ausgefüllt.
Name	Der Name eines einzelnen Knotens im Cluster.
FQDN	Der vollqualifizierte Domänenname jedes Knotens im Cluster.
TCP_Port	Der TCP-Port, von dem ein einzelner Knoten im Cluster Datenverkehr erhält.
Typ	Der Typ der Datenbank ist MemoryDB.
Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	
ARN	Der Amazon-Ressourcenname des Clusters. Die Werte werden in der Spalte Objekt-ID [object_ID] ausgefüllt.
Name	Name des Clusters
FQDN	Der vollqualifizierte Domänenname des Clusters.
TCP_Port	Der TCP-Port, von dem der Cluster Datenverkehr erhält.

Musterbeziehungen

CI	Beziehungstyp	CI
[cmdb_ci_appl]	Erstreckt sich von	[cmdb_ci]
[cmdb_ci_cloud_database]	Erstreckt sich von	[cmdb_ci_DB_instance]
[cmdb_ci_Cloud_DB_Cluster]	Cluster::Cluster von	[cmdb_ci_Cloud_DB_Cluster]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbeziehungen (Fortsetzung)

CI	Beziehungstyp	CI
[cmdb_ci_Cloud_DB_Cluster]	Nur Referenz (Configuration_item)	[cmdb_key_value]

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

AWS Discovery mithilfe von Mustern

AWS OpenSearch-Discovery mit Mustern

Von der Anwendung ServiceNow® Discovery wird das Amazon OpenSearch-Erkennungsmuster dazu verwendet, Amazon OpenSearch-Servicedomänen zu ermitteln.

OpenSearch ist eine Such- und Analyse-Engine auf Open-Source-Basis für Anwendungsfälle wie Protokollanalysen, Echtzeit-Anwendungsüberwachung und Clickstream-Analysen. OpenSearch funktioniert als Cluster von Knoten, die vom Endbenutzer abstrahiert werden. Eine OpenSearch-Servicedomäne ist gleichbedeutend mit einem OpenSearch-Cluster. Domänen sind Cluster mit Einstellungen, Instanztypen, Instanzanzahlen und Speicherressourcen.

Voraussetzungen

- Installieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - https://es.{region}.amazonaws.com/2021-01-01/domain
  - https://es.{region}.amazonaws.com/2021-01-01/opensearch/domain-info{"DomainNames":[]}
  - https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

OpenSearch-Servicedomänen werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name der Servicedomäne.
FQDN	Vollqualifizierter Domänenname der Region, in der sich der Keyspace befindet.

AWS Ressourcenbestands-Discovery mit Mustern

Die ServiceNow Discovery Und Service-Mapping-Anwendungen können finden und zuordnen AWS Vom AWS Config Service verfügbare Ressourcen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery Verwendet das AWS-Ressourcenbestandsmuster, um die über verfügbaren Ressourcen zu erkennen AWS. Verwenden Sie dieses Muster für AWS Ressourcen, die kein dediziertes Muster haben, z. B. AWS Lambda oder EC2. Dieses Muster ist auf Ressourcen beschränkt, die über den AWS-Konfigurationsservice verfügbar sind, wie im AWS Config Developer Guide beschrieben.

Sie können dieses Muster auf der ServiceNow-Plattform mit der Version London (Patch 8), Madrid (Patch 2) oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Erstellen Sie AWS-Anmeldeinformationen.
- Erstellen Sie einen AWS Cloud-Service-Account.

  Sie können nur verwenden AWS Verwaltungsservice-Account für Discovery, nicht seine Unterkonten.

  Hinweis: Die Cloud Discovery-Benutzeroberfläche bezeichnet Mitgliedskonten als Unterkonten.

- Erkennen AWS Rechenzentren (LDC)
- Planen Sie ein vollständiges AWS Ermitteln oder verwenden Sie ein bestimmtes Bestandsmuster
- Feinabstimmung AWS Ressourcen-Discovery mithilfe der Ressourcenaufnahmeliste.

  Wenn Ihre Bereitstellung anwenderdefinierte Muster für die AWS-Discovery aufweist, stellen Sie sicher, dass Sie nicht erkennen AWS Ressourcen zweimal.

1. Stellen Sie sicher, dass der Anwendungsbereich ist Muster für Discovery und Service-Mapping:
   a. Navigieren zu **Einstellungen** > **Entwickler**an.
   b. Wählen Sie Discovery and Service Mapping Patterns aus der Liste **Anwendung** aus.
2. Navigieren zu **Systemdefinitionen** > **Tabellen**an.
3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option Löschen aus.

Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Liste um zusätzliche Ressourcentypen erweitern, die das Muster erkennen soll. Die Namen dieser Ressourcentypen müssen den Benennungskonventionen der entsprechenden Anbieter entsprechen.

Hinweis: Wenn Sie die sofort einsatzbereite Aufnahmeliste ändern, wird sie in Anwendungsupdates nicht mehr automatisch aktualisiert. Sie müssen die benutzerdefinierte Liste selbst verwalten.

1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Cloud-Anbieter	Der Lieferant des Ressourcentyps: AWS.
Ressourcentyp	Die AWS Ressourcentypwert. Zum Beispiel: AWS::CloudWatch::Alarm.
Anwendung	Der Anwendungsbereich: Muster für Discovery und Service-Mapping.

Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

- Zum Erkennen der Ressourcen, von denen der AWS-Konfigurationsservice unterstützt wird, wird vom Muster folgende API verwendet: https://config.[AWS region].amazonaws.com. Vom Muster wird der Ressourcentyp in der API-Anforderung im folgenden Format angegeben: {"resourceType":"AWS::[RESOURCE]::[TYPE]"}.

  Die POST-Methode erfordert die folgenden Header:

  - X-Amz-Target - StarlingDoveService.ListDiscoveredResources☒
  - Accept - application/json
  - Content-Type - application/x-amz-json-1.1☒
- Zum Erkennen der Ressourcen-Tags für Ressourcen, die Tags unterstützen, wird vom Muster folgende API verwendet: https://tagging.[AWS region].amazonaws.com. Vom Muster wird der Ressourcentyp in der API-Anforderung im folgenden Format angegeben: {"ResourceTypeFilters": [“[resource]:[type]"]}.

  Die POST-Methode erfordert die folgenden Header:

  - X-Amz-Target - ResourceGroupsTaggingAPI_20170126.GetResources☒
  - Accept - application/json
  - Content-Type - application/x-amz-json-1.1☒

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_cmp_resource]	
object_id	Die ID des Elements. Dies ist normalerweise der Amazon-Ressourcenname (Amazon Resource Name, ARN).
name	Name der Ressource
resource_type	Der Asset-Ressourcentyp, basierend auf dem Inhalt der JSON-Datei
Beschreibung	Kurzbeschreibung, wie das CI mit Daten gefüllt wird

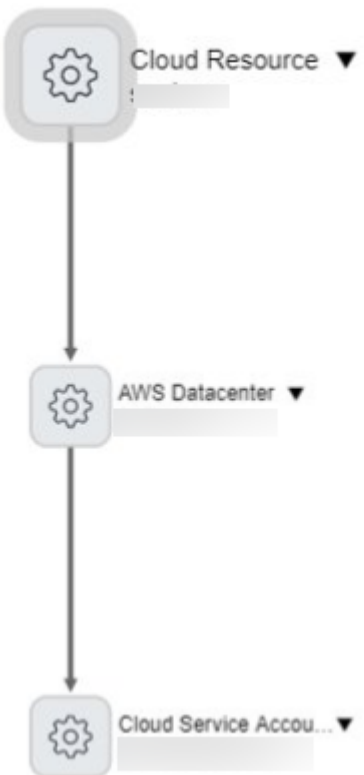
CI-Beziehungen

Das Muster „AWS Resource Inventory“ erstellt die folgenden CI-Beziehung:

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]

Im Folgenden finden Sie eine Abhängigkeitsansicht des gesammelten Daten-Flows.

AWS Resource Inventory –Abhängigkeitsansicht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS Services-Discovery mithilfe von Mustern

Muster für Discovery und Service-Mapping Anwendungsverwendungen Amazon AWS Zu erkennende Servicemuster Amazon AWS Services während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Die neueste Version von Muster für Discovery und Service-Mapping Unterstützt die Erkennung folgender Elemente Amazon AWS Services:

- AppSync-API
- Athena-Arbeitsgruppe
- Sicherungsplan
- Sicherungsresor
- CloudFront-Verteilung
- Cloudwatch-Protokolle
- CodeDeploy-Bereitstellung
- CodePipeline-Pipeline
- Endpunkte des Datenbankmigrationsservice (DMS)
- Elastische Bohnenalk-Anwendung
- EMR-Cluster (wird auf EC2 ausgeführt)
- EventBridge-Ereignisbus
- FSX-Sicherung
- FSX-Dateisystem
- Klebe-Datenbank
- IAM-Richtlinie
- IAM-Rolle
- IAM-Anwender
- KMS-Schlüssel
- MQ-Broker
- MQ-Konfiguration
- S3-Glacier Vault
- SageMaker-Notebook-Instanz
- Secrets Manager Secret
- SES-Identität (Simple Email Service)
- SQS-Warteschlange
- Schrittfunktionen – Status-Computer
- Speicher-Gateway
- System Manager-Dokument
- Systemmanager-Parameterspeicher
- Familienserver übertragen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- VPC-Flow-Protokoll
- Von VPC verwaltete Präfixliste
- Röntgen-Stichprobenregel

Muster für Discovery und Service-Mapping Unterstützt AWS GovCloud (USA)-Accounts für die folgenden Services:

- AppSync-API
- Elastische Bohnenalk-Anwendung
- EventBridge-Ereignisbus
- MQ-Broker
- SQS-Warteschlange
- Schrittfunktionen – Status-Computer
- Speicher-Gateway

Wird Erkannt AWS Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich AWS Service-Account. Weitere Informationen finden Sie unter Wird eingerichtet AWS Service-Accounts.

Voraussetzungen

Verifizieren Amazon AWS Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in AWS Discovery mithilfe von Mustern.

Entfernen Sie Ressourcen aus der Tabelle „Ressourceneinschlussliste“

Stellen Sie sicher, dass die relevante Ressource nicht in der Tabelle „Ressourceneinschlussliste“ [sa_Cloud_Inventory_resource_Whitelist] aufgeführt ist, um eine doppelte Discovery zu vermeiden. Weitere Informationen zum Entfernen von Ressourcen aus der Ressourceneinschlussliste finden Sie unter AWS Ressourcenbestands-Discovery mit Mustern.

Aktivieren Sie das entsprechende Muster

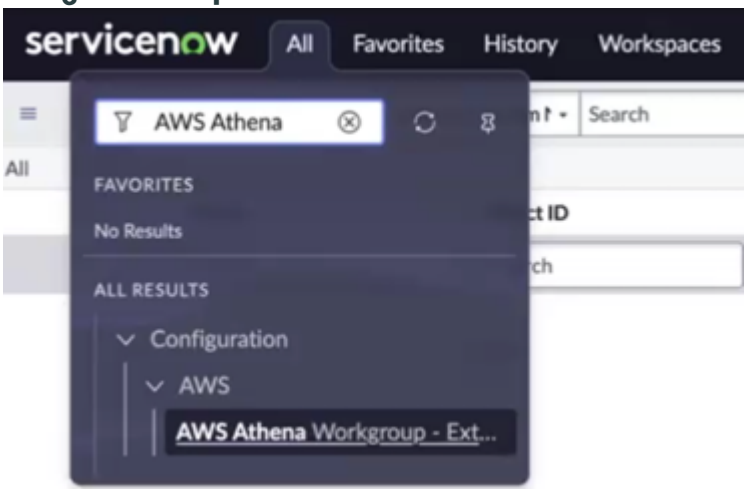
Die Muster für Discovery und Service-Mapping Für diese Services sind standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird.Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt Daten für jedes der Muster in nicht- CMDB Tabellen. Diese Tabellen sind unter aufgeführt **Alle** > **Konfiguration** > **AWS**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigationsbeispiel für nicht- CMDB Tabelle AWS Athena Workgroup



Discovery Füllt Daten in der Cloud-Ressource [cmdb_ci_CMP_resource] aus CMDB Tabelle beim Ausführen der folgenden Muster:

- Amazon AWS – Athena Workgroup – Erweiterter Bestand (LP)
- Amazon AWS – Sicherungssicherungsplan – Erweiterter Bestand (LP)
- Amazon AWS – Sicherungsresor – Erweiterter Bestand (LP)
- Amazon AWS – CloudFront-Distribution – Erweiterter Bestand (LP)
- Amazon AWS – CloudWatch-Protokoll – Erweiterter Bestand (LP)
- Amazon AWS – CodeDeploy-Bereitstellung – Erweiterter Bestand (LP)
- Amazon AWS – CodePipeline-Pipeline – Erweiterter Bestand (LP)
- Amazon AWS – DMS-Endpunkt – Erweiterter Bestand (LP)
- Amazon AWS – EMR-Cluster – Erweiterter Bestand (LP)
- Amazon AWS – FSX-Sicherung – Erweiterter Bestand (LP)
- Amazon AWS – FSX-Dateisystem – Erweiterter Bestand (LP)
- Amazon AWS – Glue Database – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Richtlinie – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Rolle – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Anwender – Erweiterter Bestand (LP)
- Amazon AWS – KMS-Schlüssel – Erweiterter Bestand (LP)
- Amazon AWS – MQ-Konfiguration – Erweiterter Bestand (LP)
- Amazon AWS – S3 Glacier Vault – Erweiterter Bestand (LP)
- Amazon AWS – SageMaker-Notebook-Instanz – Erweiterter Bestand (LP)
- Amazon AWS – Secret Manager Secret – Erweiterter Bestand (LP)
- Amazon AWS – Simple Email Service Identity – Erweiterter Bestand (LP)
- Amazon AWS – Systems Manager-Dokument – Erweiterter Bestand (LP)
- Amazon AWS – Systemmanager-Parameterspeicher – Erweiterter Bestand (LP)
- Amazon AWS – Familienserver übertragen – Erweiterter Bestand (LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon AWS – VPC-Flow-Protokoll – Erweiterter Bestand (LP)
- Amazon AWS – von VPC verwaltete Präfixliste – Erweiterter Bestand (LP)
- Amazon AWS – XRay-Stichprobenregel – Erweiterter Bestand (LP)

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Name [name]	Name des AWS Ressource.
Objekt-ID [object_id]	Amazon-Ressourcenname (ARN) für AWS Ressource.
Ressourcentyp [resource_type]	Typ der Ressource im folgenden Format – **Lieferant::Service::Component** . Beispiel: Für die DMS-Endpunktressource wird der Wert auf festgelegt **AWS::DMS::Endpunkt** .
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert: Installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Standardwert: Operativ.

Discovery Füllt die Daten in verschiedenen aus CMDB Tabellen, wenn die folgenden Muster ausgeführt werden.

Amazon AWS – AppSync-API – Erweiterter Bestand (LP)

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Name [name]	Name der AWS AppSync-API, bei der es sich um die GraphQL-Schnittstelle handelt.
Objekt-ID [object_id]	ARN für die API.
Typ [type]	Typ der Ressource im folgenden Format – **Lieferant::Service::Component** . Der Wert ist auf festgelegt **AWS::AppSync::API** .

Amazon AWS – Elastic Beanstalk-Anwendung – Erweiterter Bestand (LP)

Cloud-App-Server [cmdb_ci_Cloud_appserver]

Feld	Beschreibung
Name [name]	Name der Anwendung.
Objekt-ID [object_id]	ARN der Anwendung.

Amazon AWS – EventBridge-Ereignisbus – Erweiterter Bestand (LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Name [name]	Name des Ereignisbusses.
Objekt-ID [object_id]	ARN des Ereignisbusses.
Typ [type]	Typ der Ressource im folgenden Format – **Lieferant::Service::Component** . Der Wert ist auf festgelegt **AWS::EventBridge::EventBus** .

Amazon AWS – MQ-Broker – Erweiterter Bestand (LP)

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Name [name]	Name des MQ-Brokers. Dieser Wert muss im AWS-Account eindeutig sein, zwischen 1-50 Zeichen lang sein und nur Buchstaben, Zahlen, Bindestriche und Unterstriche enthalten. Beispiel: MyActiveMQBroker.
Objekt-ID [object_id]	ARN des MQ-Brokers.
Typ [type]	Typ der Broker-Engine. Beispiel: ACTIVEMQ oder RABBITMQ.
Version [version]	Version der Broker-Engine.

Amazon AWS – SQS-Warteschlange – Erweiterter Bestand (LP)

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Name [name]	Name der Warteschlange, für die Sie die URL abrufen möchten. Der Name kann bis zu 80 Zeichen lang sein.
Objekt-ID [object_id]	ARN der Warteschlange.
Typ [type]	Typ der Ressource im folgenden Format – **Lieferant::Service::Component** . Der Wert ist auf festgelegt **AWS::SQS::Warteschlange** .

Amazon AWS – Schrittfunktionen-Statuscomputer – Erweiterter Bestand (LP)

Cloud-Funktion [cmdb_ci_cloud_function]

Feld	Beschreibung
Name [name]	Name des Statuscomputers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Funktion [cmdb_ci_cloud_function] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	ARN des Statuscomputers.
Edition [edition]	Edition des Statuscomputers. Mögliche Werte: STANDARD oder EXPRESS.

Amazon AWS – Storage Gateway – Erweiterter Bestand (LP)

Cloud-Gateway [cmdb_ci_cloud_gateway]

Feld	Beschreibung
Name [name]	Name, den Sie für Ihr Gateway konfiguriert haben.
Objekt-ID [object_id]	ARN des Gateways.
Umgebung [Environment]	Typ der Hardware- oder Softwareplattform, auf der das Gateway ausgeführt wird.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Amazon AWS Services-Discovery.

Diese Beziehungen unterstützen die Discovery von AWS Services, wenn die folgenden Muster ausgeführt werden.

- Amazon AWS – Athena Workgroup – Erweiterter Bestand (LP)
- Amazon AWS – Sicherungssicherungsplan – Erweiterter Bestand (LP)
- Amazon AWS – Sicherungsresor – Erweiterter Bestand (LP)
- Amazon AWS – CloudFront-Distribution – Erweiterter Bestand (LP)
- Amazon AWS – CloudWatch-Protokoll – Erweiterter Bestand (LP)
- Amazon AWS – CodeDeploy-Bereitstellung – Erweiterter Bestand (LP)
- Amazon AWS – CodePipeline-Pipeline – Erweiterter Bestand (LP)
- Amazon AWS – DMS-Endpunkt – Erweiterter Bestand (LP)
- Amazon AWS – EMR-Cluster – Erweiterter Bestand (LP)
- Amazon AWS – FSX-Sicherung – Erweiterter Bestand (LP)
- Amazon AWS – FSX-Dateisystem – Erweiterter Bestand (LP)
- Amazon AWS – Glue Database – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Richtlinie – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Rolle – Erweiterter Bestand (LP)
- Amazon AWS – IAM-Anwender – Erweiterter Bestand (LP)
- Amazon AWS – KMS-Schlüssel – Erweiterter Bestand (LP)
- Amazon AWS – MQ-Konfiguration – Erweiterter Bestand (LP)
- Amazon AWS – S3 Glacier Vault – Erweiterter Bestand (LP)
- Amazon AWS – SageMaker-Notebook-Instanz – Erweiterter Bestand (LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon AWS – Secret Manager Secret – Erweiterter Bestand (LP)
- Amazon AWS – Simple Email Service Identity – Erweiterter Bestand (LP)
- Amazon AWS – Systems Manager-Dokument – Erweiterter Bestand (LP)
- Amazon AWS – Systemmanager-Parameterspeicher – Erweiterter Bestand (LP)
- Amazon AWS – Familienserver übertragen – Erweiterter Bestand (LP)
- Amazon AWS – VPC-Flow-Protokoll – Erweiterter Bestand (LP)
- Amazon AWS – von VPC verwaltete Präfixliste – Erweiterter Bestand (LP)
- Amazon AWS – XRay-Stichprobenregel – Erweiterter Bestand (LP)

Regionale Services

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Globale Services

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Diese Beziehungen unterstützen die Discovery von AWS Services, wenn die folgenden Muster ausgeführt werden.

Amazon AWS – AppSync-API – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – Elastic Beanstalk-Anwendung – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud-App-Server [cmdb_ci_Cloud_appserver]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – EventBridge-Ereignisbus – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – MQ-Broker – Erweiterter Bestand (LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – SQS-Warteschlange – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – Schrittfunktionen-Statuscomputer – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud-Funktion [cmdb_ci_cloud_function]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Amazon AWS – Storage Gateway – Erweiterter Bestand (LP)

CI	Beziehung	CI
Cloud-Gateway [cmdb_ci_cloud_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

AWS Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

AWS Tag-Discovery mit Mustern

Die ServiceNow Discovery Und Service-Mapping Anwendungen können Muster verwenden, um die Tags für zu erkennen AWS Ressourcen und Konfigurationselementtypen (CI), und füllen Sie dann aus CMDB Mit diesen Erkennungen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Dieses Tag-spezifische Discovery-Muster ist zusätzlich zum anderen AWS Muster, die auf verfügbar sind ServiceNow Store.Dieses Muster erweitert die für die Erkennung der jeweiligen verwendeten AWS Ressourcen.

Discovery Füllt aus CMDB Mit Tags für Folgendes AWS Muster und CI-Typen:

- Amazon AWS – ACL (LP) [cmdb_ci_Network_acl]
- Amazon AWS API-Gateway [cmdb_ci_Cloud_Gateway]
- Amazon AWS – Anwendungs- und Netzwerk-LB (LP) [cmdb_ci_Cloud_load_Balancer]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon AWS Application and Network LBs Events
- Amazon AWS – Classic LB (LP) [cmdb_ci_Cloud_load_Balancer]
- Amazon AWS Classic LB-Ereignisse
- Amazon AWS Cognito [cmdb_ci_Cloud_authentication]
- Amazon AWS – Kunden-Gateway (LP) [cmdb_ci_Customer_Gateway]
- Amazon AWS DB-Cluster
- Amazon AWS DynamoDB [cmdb_ci_dynamodb_table]
- Amazon AWS ElastiCache
- Amazon AWS – ECS [cmdb_ci_Cloud_Service_Account]
- Amazon AWS – ausführbare Vorlage (LP) [cmdb_ci_os_template]
- Amazon AWS – Host (LP)
- Amazon AWS – Internet Gateway (LP)
- Amazon AWS-Keyspace
- Amazon AWS – Schlüsselpaar (LP)
- Amazon AWS Lambda [cmdb_ci_Cloud_function]
- Amazon AWS – LB-Pool (LP)
- Amazon AWS – NAT-Gateway (LP)
- Amazon AWS – Netzwerk (LP)
- Amazon AWS Network Events
- AMAZON AWS – NIC (LP)
- Amazon AWS – Owned Template (LP)
- Amazon AWS – öffentliche IP-Adresse (LP)
- Amazon AWS Redshift
- Amazon AWS Relational Database Service [cmdb_ci_Cloud_database]
- Amazon AWS-Ressourcenbestand
- Amazon AWS – Weiterleitungstabelle (LP)
- Amazon AWS S3 [cmdb_ci_Cloud_object_Storage]
- Amazon AWS – Sicherheitsgruppe (LP)
- Amazon AWS Security Group Events
- Serverlose Amazon AWS-Datenbank
- Amazon AWS – Speicher (LP)
- Amazon AWS Storage Events
- Discovery des Amazon AWS-Unterkontos
- Amazon AWS – Subnetz (LP)
- Amazon AWS – Virtual Server (LP)
- Amazon AWS Virtual Server Events

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon AWS – VPN-Verbindungen (LP)
- Amazon AWS – VPN-Gateway (LP)

Hinweis: Weitere Informationen zu den Tags und Mustern für jede dieser Ressourcen finden Sie in der Dokumentation für spezifische AWS Ressource.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

AWS Anmeldeinformationen

- Konfigurieren Sie auf der ServiceNow AI Platform die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Haben Sie einen Amazon **Account-ID** . Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird. Sie können Discovery über das Servicekonten-Formular ausführen.
- Legen Sie schreibgeschützte Berechtigungen für die folgende URL fest: https//tagging.<region>.amazonaws.com.

Discovery-Zeitplan

Erstellen Sie einen Zeitplan für das relevante AWS Service-Account. Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Musteraufgaben

Bei Erkennung AWS Tags, das Muster schließt die folgenden allgemeinen Aufgaben ab:

- Legt den Filter für Ressourcentypen fest: Filtert die Tags nur nach Tags, die mit dem Muster-CI-Typ in Verbindung stehen.
- Initiiert den Cloud API-Aufruf: Der API-Aufruf der Cloud-Umgebung, die die Tags sammelt und ihre Attribute in der Tag-Tabelle analysiert.
- Analysiert den Ressourcennamen aus dem Amazon-Ressourcennamen (ARN). Jeweils Amazon Der Ressource wird ein Name und ein eindeutiger Bezeichner zugewiesen.

  Hinweis: Das Analysieren des Ressourcennamens ist nur für Muster erforderlich, bei denen der Hauptidentifizierungsabschnitt nicht mit dem ARN von funktioniert AWS Ressource. Wenn dies der Fall ist, muss ein Beziehungsattribut aus analysiert werden AWS ARN.

- Enthält Verweise auf den Cloud-Ressourcentyp. Stellt die Beziehung zwischen dem Tag und dem Cloud-Ressourcentyp her.

Cloud-REST-Aufruf

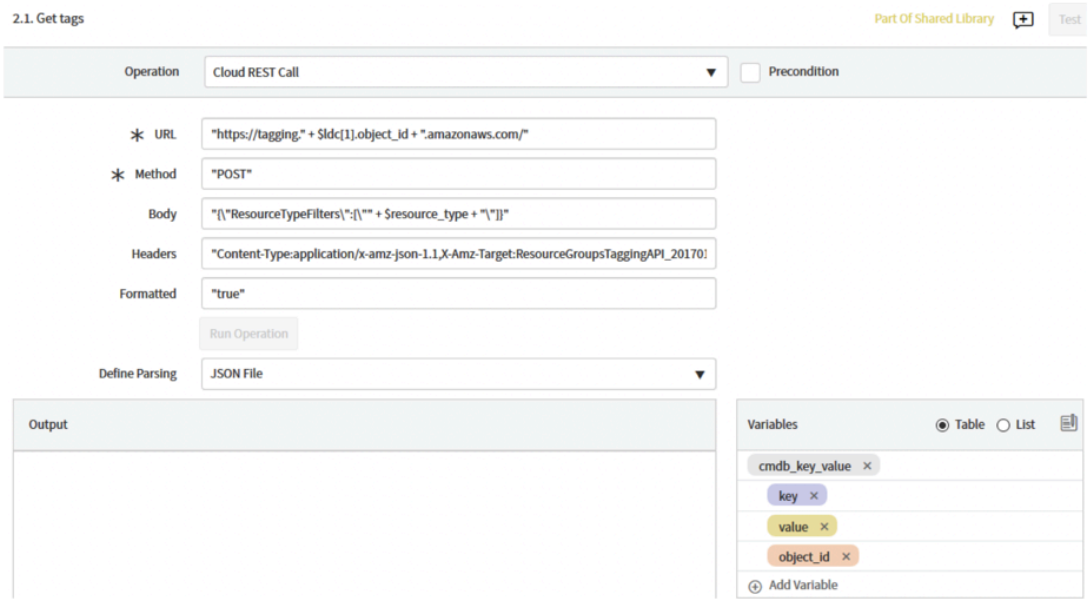
Das Muster enthält eine API mit dem Namen „Cloud Rest Call“ Post Call, die zum Sammeln der folgenden Daten verwendet wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- API-URL, die zum Abrufen der Daten verwendet wird — "https://tagging." + $ldc[1].object_id + ".amazonaws.com/“
- API-Hauptteil — "{\"ResourceTypeFilters\":[\"" + $resource_type + "\"]}“
- Header — "Content-Type:application/x-amz-json-1.1,X-Amz-Target:ResourceGroupsTaggingAPI_20170126.GetResources"

Diese Daten werden wie im folgenden Fenster angezeigt.

Daten aus dem Cloud REST-Aufruf



Von Discovery während der horizontalen Erkennung erfasste Daten

Das Muster erfasst während der horizontalen Discovery die folgenden Daten:

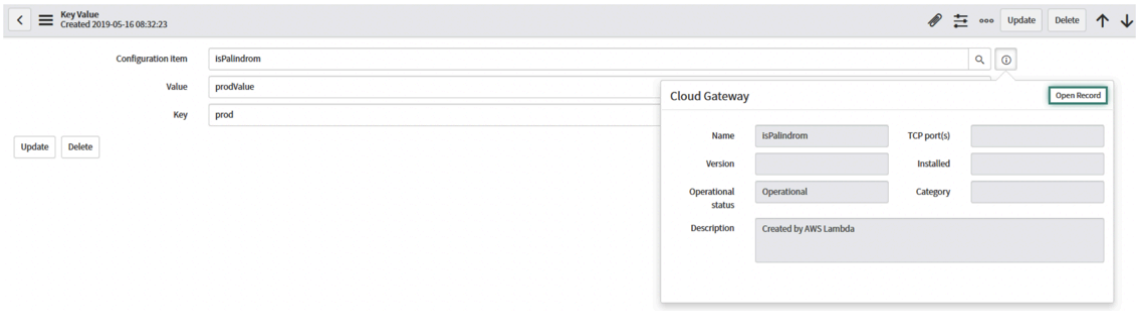
Tabelle und Feld	Zusätzliche Informationen
CI-Typ [cmdb_key_value]	
Schlüssel	Tag-Schlüssel
Wert	Tag-Wert
Object_id	Eindeutige Ressourcen-ID, die die Ressource in identifiziert AWS Konsole.
Klassenmodell [cmdb_key_value]	
Erweitert Tabelle	Nicht zutreffend
Bezeichner – Object_id	Zugehörige Einträge zu den Cloud-Ressourcen
Metadatenregeln	Nicht zutreffend

Diese Daten werden wie im folgenden Fenster angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der horizontalen Erkennung erfasste Daten



AWS Discovery-Muster verwendet die folgende Auswertung:

```
var rtrn;
var name = ${cmdb_key_value[].object_id}
name = name.substring(name.lastIndexOf("restapis/")+9,name.lastIndex);
name = name.substring(0,name.indexOf("/"));
rtrn = name;
```

Ähnliche EVALS sind für Muster verfügbar, bei denen der Hauptidentifizierungsabschnitt keine ARN-Informationen in der Tabelle des Haupt-CI-Typs enthält. Wenn diese Informationen nicht verfügbar sind, muss der Tag-Erweiterungsabschnitt eine eindeutige ARN analysieren, die zum Herstellen der Beziehung zur zugehörigen Cloud-Ressource verwendet wird.

Aktivieren AWS Ziel-Discovery des Anwendungslastenausgleichsmoduls

Aktivieren Sie *sn_itom_pattern.discover_aws_app_pool_members* MID-Server Zu erkennende Eigenschaft AWS Anwendungslastenausgleichsmodul-Ziele.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **MID-Server** > **Eigenschaften**an.
2. In **Name** Feld, suchen Sie nach sn_itom_pattern.Discover_aws_App_Pool_members .
3. Wählen Sie die Eigenschaft *sn_itom_pattern.discover_aws_app_pool_members* aus.
4. Im Feld **Wert** geben Sie wahr ein.
5. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

AWS Discovery mithilfe von Mustern

Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern

Muster für Discovery und Service-Mapping Verwendet Muster, um Komponenten von zu erkennen Google Cloud Platform (GCP) Bereitstellung während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping Startversion 1.8.0 (September 2023)
- CMDB CI-Klassenmodelle Startversion 1.49.0 (September 2023)
- Visibility Content Startversion 6.13.0 (September 2023)

Verifizieren Sie MID-Server Anforderungen

- Verwenden Sie zur Cloud-Erkennung einen dedizierten MID-Server. Der MID-Server muss über 16 Kerne und 8 GB mit 4 GB Java Memory Model (JVM)-Speicherzuweisung verfügen. Für Informationen zur Verifizierung MID-Server Spezifikationen siehe KB-artikel KB2156327 .
- Stellen Sie den dedizierten MID-Server mit Internetzugang bereit und stellen Sie die Verbindung her.
- Weitere Informationen zu finden MID-Server Konfigurationen, siehe Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen.

Verifizieren Google Cloud BigQuery und Google Cloud-Bigtable-Anforderungen

Um zu erkennen Google Cloud BigQuery und Google Cloud-Bigtable, navigieren Sie zu **Alle** > **Discovery** > **MID-Server** > **Eigenschaften** Und stellen Sie sicher, dass die `sn_itom_pattern.google_dbservice_table_collection`Eigenschaft ist auf festgelegt **Wahr** .

Überprüfen Sie die Anwenderrolleneinstellungen

Legen Sie die Benutzerberechtigung für das Google Cloud Platform-Mitglied auf **Betrachter** fest:

1. Navigieren Sie in der Google Cloud Platform-Konsole zu **IAM**.
2. Wählen Sie das entsprechende Mitglied aus der Liste aus, und klicken Sie auf das Symbol **Bearbeiten**.
3. Wählen Sie im Fenster „Bearbeitungsberechtigungen“ in der Liste **Rolle** Betrachter aus.
4. Klicken Sie auf **Speichern**.

Konfigurieren Google API-Anmeldeinformationen

Weitere Informationen finden Sie unter Konfigurieren Sie Google API-Anmeldeinformationen für Cloud-Discovery.

Erstellen Sie einen Google Cloud Platform Service-Account

Weitere Informationen finden Sie unter Erstellen GCP Service-Accounts.

Sammeln von Cloud-Protokollierungs-Events aktivieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Google Cloud Platform-Muster können Cloud-Protokollierungs-Events sammeln, die von den nativen Google Cloud-APIs generiert werden. Konfigurieren Sie Google Stackdriver LoggingService zum automatischen Aktualisieren von CMDB.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Überprüfen Sie, ob ein Discovery Zeitplan ist konfiguriert

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die von allen zur Erkennung von GCP-Produkte entwickelten Mustern erkannt werden

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [Account_ID]	Name des Projekts, das für die Discovery verwendet wird.
Objekt-ID [object_id]	Name des Projekts, das für die Discovery verwendet wird.
Rechenzentrumstyp [datacenter_type]	Rechenzentrumstyp: Google-Rechenzentrum [cmdb_ci_google_Datacenter].

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Beschreibung [short_description]	Beschreibung der Verfügbarkeitszone.
Status [state]	Status der Verfügbarkeitszone. Mögliche Werte sind verfügbar oder beendet.

Google-Rechenzentrum [cmdb_ci_google_datacenter]

Feld	Beschreibung
Name [name]	Name des Rechenzentrums oder der Region
Region [Region]	Name des Rechenzentrums oder der Region

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Google-Rechenzentrum [cmdb_ci_google_datacenter] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von zugewiesen wurde GCP Für diese Ressource.
Beschreibung [short_description]	Beschreibung des Rechenzentrums oder der Region.

Ressourcen, die von der Säule Google Cloud Platform Discovery Computer erkannt wurden

Virtuelle Maschine [cmdb_ci_vm_instance]

Feld	Beschreibung
Name [name]	Name des virtuellen Computers (VM)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Status [state]	VM-Status. Eine der folgenden Möglichkeiten: • An • Wird ausgeführt • Aus • Beendet • Angehalten
Datenträger [Datenträger]	Anzahl der Datenträger, die dieser VM zugewiesen sind
Netzwerkadapter [nics]	Anzahl der Netzwerkschnittstellen-Controller (NICs), die dieser VM zugewiesen sind.
CPUs [cpus]	Anzahl der CPU-Kerne, die dieser VM zugewiesen sind
Arbeitsspeicher (MB) [Arbeitsspeicher]	Anzahl der dieser VM zugewiesenen Arbeitsspeichergröße.

Instanzvorlage [cmdb_ci_instance_template]

Feld	Beschreibung
Name [name]	Name der Instanzvorlage
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Beschreibung [short_description]	Beschreibung der Instanzvorlage

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Name [name]	Name des NIC

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der aus einer Verkettung von vm_id + „:“ + nic_name besteht.
IP-Adresse [ip_address]	Primäre interne IP-Adresse des NIC
Status [state]	Feld mit demselben Wert wie das GCP-Statusfeld

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Name [name]	Name des Datenträgers
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Größe [Größe]	Datenträgergröße in GB
Beschreibung [short_description]	Beschreibung, die Sie zur einfachen Identifizierung angeben
Status [state]	Status des Datenträgers. Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.
Installationsstatus [install_status]	Installiert
Speichertyp [storage_type]	Datenträgertyp. Beispielsweise „pd-standard“ oder „lokale SSD“.

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Image-Typ [image_type]	Image-Typ
Image-Quelle [image_source]	Image-Quelle, z. B. Quelldatenträger / Snapshot + „/“ + Quelldatenträger-/Snapshot-ID

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwaretyp [cmdb_ci_compute_template]

Feld	Beschreibung
Name [name]	Name des Image.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
VCPUs [vcpus]	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne
Arbeitsspeicher MB [Memory_mb]	Speichergröße, die dieser Vorlage zugewiesen ist
Lokaler Speicher – GB [local_storage_gb]	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

Ressourcen, die von der Säule Google Cloud Platform Discovery External IP erkannt wurden

Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]

Feld	Beschreibung
Name [name]	Name der externen IP
Öffentliche IP-Adresse [public_ip_address]	Adresse der öffentlichen IP
Status [state]	Status der externen IP-Adresse. Eine der folgenden Möglichkeiten: • In Gebrauch • Verfügbar Verwenden Sie „In Gebrauch“, wenn die externe IP verwendet wird, oder „Verfügbar“, wenn sie für eine spätere Verwendung reserviert ist.

Ressourcen entdeckt durch das Google Cloud Platform Discovery-Lastenausgleichsmodul

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Name [name]	Name des load_balancer
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer-Services [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmodul-Services
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Servicetyp [service_type]	Servicetyp. Einer der folgenden: • Benutzeroberfläche (HTTP/TCP/UDP LB) • Back-End (nur HTTP-LB)
Port [port]	Listener-Protokoll-Portnummer (Back-End)
Front-End-Port [front_end_port]	Listener-Protokoll-Portnummer (Front-End)
Listener-Protokoll [listener_Protocol]	Listener-Protokoll Einer von • TCP • HTTP • HTTPS
Pool [pool]	Pool, der vom LB-Service verwendet wird

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Poolname. Für TCP-/UDP-LBs ohne Pools der Name, der den LB-Namen **-Pool** enthält.
Objekt-ID [object_id]	Der eindeutige Bezeichner des LB-Pools Für TCP-/UDP-LBs ohne Pools der Name, der den LB-Namen **-Pool** enthält.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Name des Poolmitglieds
Objekt-ID [object_id]	Eindeutiger Bezeichner des Poolmitglieds, erstellt aus der ID der Instanz object_id

Cloud-Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_Health_Service]

Feld	Beschreibung
Name [name]	Name des Integritätsservice
Objekt-ID [object_id]	Eindeutiger Bezeichner der Integritätsdienstprüfung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_Health_Service] (Fortsetzung)

Feld	Beschreibung
Überwachungstyp-Protokoll [Monitor_type]	Typ der Integritätsprüfung. Einer der folgenden: • TCP • HTTP • HTTPS
Zeitüberschreitung in Sekunden [timeout_sec]	Zeit in Sekunden, die auf die Antwort der Integritätsprüfung gewartet wird
Intervall in Sekunden [Check_interval_sec]	Intervall in Sekunden zum Ausführen der Integritätsprüfung
Fehlerfreier Schwellenwert [Healthy_threshold]	Anzahl der sequenziellen erfolgreichen Probe-Ergebnisse, damit eine VM-Instanz als fehlerfrei gilt
Fehlerhafter Schwellenwert [unhealthy_threshold]	Anzahl der sequenziellen fehlerhaften Probe-Ergebnisse, damit eine VM-Instanz als fehlerhaft gilt
Anforderungspfad [Request_path]	URL-Pfad, zu dem GCP Sendet Proben-Anforderungen für Integritätsprüfung. Wenn ausgelassen, GCP Sendet Probe-Anforderungen an den Stammpfad.
Port [port]	Protokoll und Port, um zu bestimmen, wie GCP Integritätsprüfungssysteme wenden sich an die VMs.

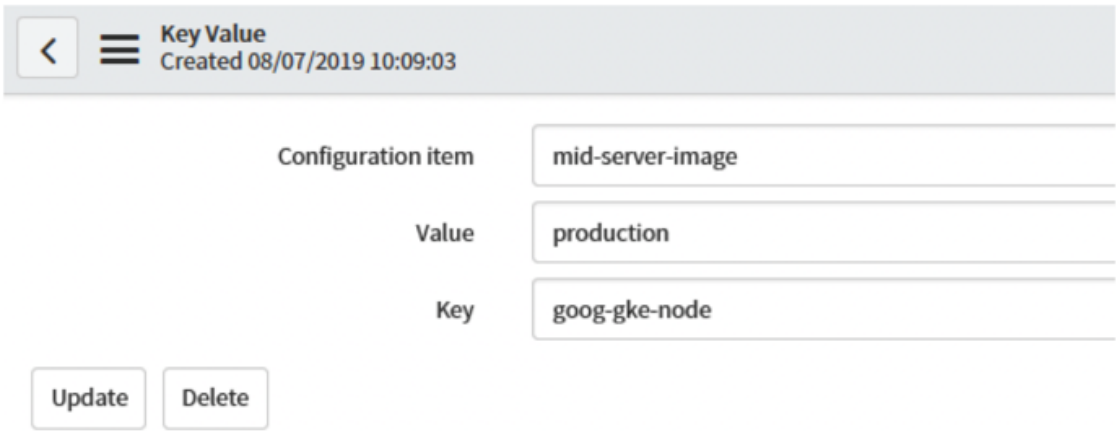
Ressourcen, die von Google Cloud Platform Discovery anhand von Bezeichnungen erkannt wurden

Wenn Google Cloud Platform Discovery während der Erkennung Bezeichnungen verwendet, werden die folgenden Daten aus dem Schlüsselwertformular gesammelt:

- Schlüssel
- Wert
- Konfigurationselement

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

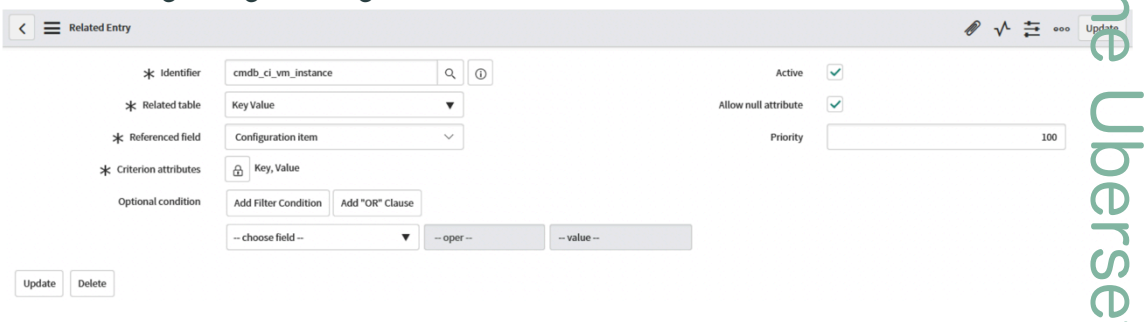
Schlüsselwertformular



Diese Daten werden im Formular „Zugehöriger Eintrag“ für Folgendes identifiziert CMDB Tabellen:

- Virtuelle Maschine [cmdb_ci_vm_instance]
- Image [cmdb_ci_os_template]
- Speichervolume [cmdb_ci_storage_volume]
- Speicher-Snapshot [cmdb_ci_storage_vol_snapshot], wie vom übergeordneten Element übernommen

Formular „Zugehörige Einträge“



Ressourcen, die von der Säule Google Cloud Platform Discovery Network erkannt wurden

Cloud-Netzwerk [cmdb_ci_network]

Feld	Beschreibung
Name [name]	Name des VPC-Netzwerks (Virtual Private Cloud)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Standard-Gateway [default_Gateway]	Gateway-Adresse für Standardweiterleitung aus dem Netzwerk
Status [state]	Status des Netzwerks Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Subnetz [cmdb_ci_Cloud_Subnet]

Feld	Beschreibung
Name [name]	Name der Instanzvorlage
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
CIDR [cidr]	Kombination aus Subnetz-CIDR, sekundärer CIDR und IPV6-CIDR. Beispiel: 10.0,0.0/16,10.2,0.0/16,fd20:957:65cb:bc00:0:0:0/64,10.1,0.0/16,fd20:957:65cb:bc00:0:0:0:0:0:0/64
Subnetzmaske [Subnet_mask]	Darstellung der Subnetzmaske mit Punkten. Beispiel: 255.255.255.0
Gateway [Gateway]	Gateway-Adresse für Standardweiterleitung aus dem Netzwerk
Broadcast-Adresse [Broadcast_address]	Broadcast-Adresse des Subnetzes
Verfügbare IP-Anzahl [available_ip_count]	Anzahl der IPs, die im Subnetz verfügbar sind. Dieser Wert enthält keine Netzwerk- und Broadcast-Adressen.

Netzwerk-ACL [cmdb_ci_network_acl]

Feld	Beschreibung
Name [name]	Name der Zugriffssteuerungsliste (ACL)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Beschreibung [short_description]	ACL-Beschreibung, die Sie angeben

Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule]

Feld	Beschreibung
Name [name]	ACL-Regelname. Dieser Name ist mit dem Namen von cmdb_ci_network_acl identisch.
Ablehnung zulassen [allow_deny]	ACL-Regelverhalten Einer der folgenden: • Zugelassen • Abgelehnt
Ausgehend [is_outbound]	Regel für ausgehenden Datenverkehr. Verwenden Sie eine der folgenden Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule] (Fortsetzung)

Feld	Beschreibung
	• „True“, wenn die Regel für ausgehenden Datenverkehr ist • „False“, wenn die Regel für eingehenden Datenverkehr ist
Quellbereiche [Source_Ranges]	JSON-Blobservice, der Quellen enthält, die CIDR-Darstellungen (Classless Inter-Domain Routing) sind, für die die Regel den Datenverkehr vom Service zulässt oder blockiert
Zielbereiche [destination_Ranges]	JSON-Blobservice, der Ziele enthält, die CIDR-Darstellungen sind, für die die Regel den Datenverkehr vom Service zulässt oder blockiert
Ziel-Tags [target_Tags]	JSON-Blobservice, der die Liste der Tags darstellt, die steuern, für welche Instanzen die Firewall-Regel gilt
Zulässiger/abgelehnter Datenverkehr [allowed_deny_Traffic]	JSON-Blobservice, der die Regeln enthält, die von dieser ACL-Regel entweder zugelassen oder verweigert werden

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Image-Typ [image_type]	Image-Typ
Image-Quelle [image_source]	Image-Quelle, z. B. Quelldatenträger / Snapshot + „/“ + Quelldatenträger-/Snapshot-ID

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Hardwaretyp [cmdb_ci_compute_template]

Feld	Beschreibung
Name [name]	Name des Image.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
VCPUs [vcpus]	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwaretyp [cmdb_ci_compute_template] (Fortsetzung)

Feld	Beschreibung
Arbeitsspeicher MB [Memory_mb]	Speichergröße, die dieser Vorlage zugewiesen ist
Lokaler Speicher – GB [local_storage_gb]	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

Ressourcen, die von der Säule Google Cloud Platform Discovery Storage erkannt wurden

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Name [name]	Name des Speicherdatenträgers
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Größe [Größe]	Datenträgergröße in GB
Status [state]	Status des Netzwerks Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.
Status [status]	Datenträgerstatus: Installiert
Speichertyp [storage_type]	Datenträgertyp. Beispielsweise „pd-standard“ oder „local-ssd“.

Cloud-Datenträgertyp [cmdb_ci_Disk_type]

Feld	Beschreibung
Name [name]	Name des Datenträgers im Format: <Datenträgertyp-Name>@<Zonenname>
Objekt-ID [object_id]	Datenträgertyp ist pro Zone eindeutig. Verwendetes Format: <Zone>:<Datenträgertyp-Name>
Beschreibung [short_description]	Beschreibung des Datenträgertyps. Beispielsweise „lokale SSD“.
Gültige Datenträgergröße (GB) [valid_Disk_size]	Datenträgergrößen, die für diesen Datenträgertyp gültig sind
Standard-Datenträgergröße (GB) [default_Disk_size_gb]	Standard-Datenträgergröße (in GB) für diesen Datenträgertyp

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Feld	Beschreibung
Name [name]	Name des Snapshots
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Beschreibung [short_description]	ACL-Beschreibung, die Sie angeben
Status [state]	Feld mit demselben Wert wie das GCP-Statusfeld
Volume-Name [Volume_Name]	Name des Quelldatenträgers: Speichervolume [cmdb_ci_storage_volume]
Kapazität [Kapazität]	Anzahl der im Snapshot gespeicherten Bytes

Ressourcen erkannt für Google Cloud BigQuery, Google Cloud-Bigtable, Google Cloud-Spanner, und Google Cloud-SQL

Cloud-Datenbank [cmdb_ci_cloud_database]

Feld	Beschreibung
Name [name]	Name der Datenbank, die Sie in erstellt haben GCP.
Objekt-ID [object_id]	Identifizierungsname der Datenbank.
Installationsstatus [install_status]	Installationsstatus der Datenbank. Standard ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Datenbank Der Standardwert ist „betriebsbereit“.
Status [state]	Gibt an, ob die Datenbank verfügbar oder beendet ist.
Typ [type]	Typ der Datenbank.
Verarbeitungseinheiten [processing_units] (nur für Cloud-Spanner)	Anzahl der Rechenverarbeitungseinheiten, die jeder Spanner-Instanz zugeordnet sind

Datenbank [cmdb_ci_database]

Feld	Beschreibung
Name [name]	Name der Datenbank.
Typ [type]	Typ der Datenbank.
Installationsstatus [install_status]	Installationsstatus der Datenbank.

Für Google Cloud Firebase erkannte Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Datenbank [cmdb_ci_cloud_database]

Name [name]	Name der Datenbank, die Sie in erstellt haben GCP.
Objekt-ID [object_id]	Identifizierungsname der Datenbank.
Installationsstatus [install_status]	Installationsstatus der Datenbank. Standard ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Datenbank Der Standardwert ist „betriebsbereit“.
Status [state]	Gibt an, ob die Datenbank verfügbar oder beendet ist.
Typ [type]	Typ der Datenbank.

Für Google Cloud Firebase Datastore erkannte Ressourcen

Datenbank [cmdb_ci_database]

Feld	Beschreibung
Name [name]	Name der Datenbank.
Typ [type]	Typ der Datenbank.
Installationsstatus [install_status]	Installationsstatus der Datenbank.

Von Virtual erkannte Ressourcen Google Cloud Platform (GCP)– VM-Lizenz und Google Cloud Platform (GCP)– Virtuelle Servermuster

Diese Mustererweiterungsabschnitte erkennen Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows VMs und RHEL VMs.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel ist eine der folgenden Optionen: • Windows_OS_License_Type_Automatic • RHEL_OS_License_Type_Automatic • SQL_Server_License_Type_Automatic
Wert [value]	Der Wert ist eine der folgenden Optionen: • BYOL • Lizenz enthalten
Konfigurationselement [configuration_item]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *`Virtual Machine Instance`*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Diese Beziehungen sollen die Google Cloud Platform-Erkennung unterstützen.

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform Computer erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Virtuelle Maschine [cmdb_ci_vm_instance]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Virtuelle Maschine [cmdb_ci_vm_instance]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Instanzvorlage [cmdb_ci_instance_template]	Host::Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Instanzvorlage [cmdb_ci_instance_template]	Verwendet::Verwendet von	Hardwaretyp [cmdb_ci_compute_template]
Instanzvorlage [cmdb_ci_instance_template]	Verwendet::Verwendet von	Image [cmdb_ci_os_template]
NIC [cmdb_ci_nic]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter]
NIC [cmdb_ci_nic]	Endpunkt implementieren auf	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
NIC [cmdb_ci_nic]	Endpunkt implementieren von	Virtuelle Maschine [cmdb_ci_vm_instance]
Speichervolume [cmdb_ci_storage_volume]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Speichervolume [cmdb_ci_storage_volume]	Endpunkt implementieren auf	Block-Endpunkt [cmdb_ci_endpoint_block]
Speichervolume [cmdb_ci_storage_volume]	Endpunkt implementieren von:	Virtuelle Maschine [cmdb_ci_vm_instance]
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Hardwaretyp [cmdb_ci_compute_template]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_ google_Datacenter]
Hardwaretyp [cmdb_ci_compute_template]	Bereitgestellt von	Hardwaretyp [cmdb_ci_compute_template]

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform IP erkannt werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Beziehungen für Ressourcen, die vom Google Cloud Platform-Lastenausgleichsmodul erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer-Services [cmdb_ci_lb_service]	Gehostet auf::Host	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Load Balancer-Services [cmdb_ci_lb_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Integritätsservice [cmdb_ci_lb_health_service]	Verwendet::Verwendet von	Load Balancer-Services [cmdb_ci_lb_service]
Integritätsservice [cmdb_ci_lb_health_service]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Integritätsservice [cmdb_ci_lb_health_service]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Integritätsservice [cmdb_ci_lb_health_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform Network erkannt werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Netzwerk [cmdb_ci_network]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten	Cloud-Netzwerk [cmdb_ci_network]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Netzwerk-ACL [cmdb_ci_network_acl]	Enthält::Enthalten	Cloud-Netzwerk [cmdb_ci_network]
Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule]	Enthält::Enthalten	Netzwerk-ACL [cmdb_ci_network_acl]

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform Storage erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Speichervolume [cmdb_ci_storage_volume]	Enthält::Enthalten	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Speichervolume [cmdb_ci_storage_volume]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Datenträgertyp [cmdb_ci_disk_type]	Host::Gehostet auf	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Datenträgertyp [cmdb_ci_disk_type]	Host::Gehostet auf	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	Bereitgestellt von::Bereitgestellt mit	Speichervolume [cmdb_ci_storage_volume] Diese Beziehung bedeutet, dass dieser Datenträger von diesem Snapshot erstellt wurde.
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	Repliziert zu::Repliziert von	Speichervolume [cmdb_ci_storage_volume]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
		Diese Beziehung bedeutet, dass dieser Snapshot von diesem Datenträger erstellt wurde.

Für die VM-Instanz erkannte Beziehungen

CI	Beziehung	CI
Server [cmdb_ci_server]	Virtualisiert von::Virtualisiert	VM-Instanz [cmdb_ci_instance]

Für Google Cloud BigQuery, Google Cloud SQL, Google Cloud Spanner und Google Cloud Bigtable erkannte Ressourcen

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Enthält::Enthalten in	Datenbank [cmdb_ci_database]
Schlüsselwert [cmdb_key_value]	Nur Referenz	Cloud-Datenbank [cmdb_ci_cloud_database]

Für Google Cloud Platform Firebase erkannte Beziehungen

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]

Beziehungen für Google Cloud Platform Firestore

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	Ci
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Google Cloud Platform (GCP) AlloyDB für PostgreSQL-Discovery mit Mustern

Muster für Discovery und Service-Mapping Verwendet das Muster Google Cloud Platform (GCP) – AlloyDB für PostgreSQL, um AlloyDB für PostgreSQL während der horizontalen Discovery zu erkennen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie GCP Abschnitt „Discovery-Voraussetzungen“ in Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Google Cloud Platform (GCP) – AlloyDB für PostgreSQL.

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [Account_ID]	Name des Projekts, das für die Discovery verwendet wird.
Objekt-ID [object_id]	Name des Projekts, das für die Discovery verwendet wird.
Rechenzentrumstyp [datacenter_type]	Rechenzentrumstyp: Google-Rechenzentrum [cmdb_ci_google_Datacenter].

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Beschreibung [short_description]	Beschreibung der Verfügbarkeitszone.
Status [state]	Status der Verfügbarkeitszone. Mögliche Werte sind verfügbar oder beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Google-Rechenzentrum [cmdb_ci_google_datacenter]

Feld	Beschreibung
Name [name]	Name des Rechenzentrums oder der Region
Region [Region]	Name des Rechenzentrums oder der Region
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von zugewiesen wurde GCP Für diese Ressource.
Beschreibung [short_description]	Beschreibung des Rechenzentrums oder der Region.

Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]

Feld	Beschreibung
Cluster-ID [cluster_id]	Die GCP Vom System generierter eindeutiger Bezeichner (UID) der Ressource.
Name [name]	Name der Clusterressource.
Automatisierte Sicherungen [Automated_Backup]	Bestimmt, ob automatisierte Sicherungen aktiviert sind. Mögliche Werte sind aktiviert oder deaktiviert.
Installationsstatus [install_status]	Installationsstatus des Clusters. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus des Clusters. Der Standardwert ist betriebsbereit.
Clusterstatus [cluster_status]	Aktueller Status dieses Clusters. Beispiel: BEREIT oder GESTOPPT.
Clusterversion [Cluster_Version]	Optionales Feld, das die Hauptversion der Datenbank-Engine anzeigt.
Clustertyp [Cluster_type]	Typ des Clusters. Mögliche Werte sind „AlloyDB – Primäres Cluster“ oder „AlloyDB – sekundärer Cluster“.

Cloud-Datenbank [cmdb_ci_cloud_database]

Feld	Beschreibung
Objekt-ID [object_id]	Die GCP Vom System generierte UID der Ressource.
Name [name]	Name der Instanzressource.
Installationsstatus [install_status]	Installationsstatus der Datenbank. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Datenbank Der Standardwert ist betriebsbereit.
Status [state]	Status der Datenbank Mögliche Werte sind verfügbar oder beendet.
CPU-Anzahl [cpu_count]	Anzahl der zentralen Verarbeitungseinheiten (CPUs) in der VM-Instanz.

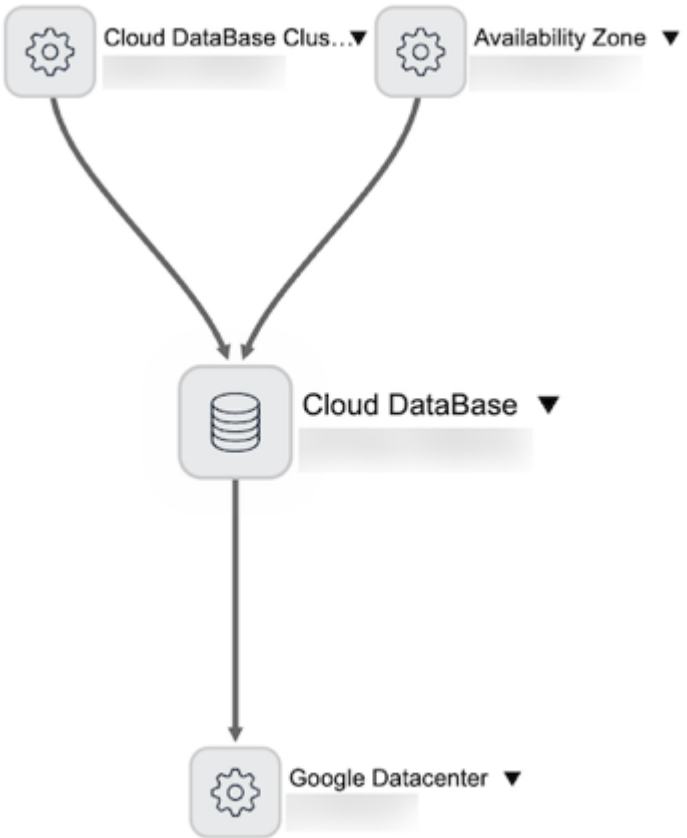
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Datenbank [cmdb_ci_cloud_database] (Fortsetzung)

Feld	Beschreibung
Typ [type]	Typ der Datenbank: AlloyDB – PostgreSQL.
Replikationstyp [Replication_type]	Typ der bei der Erstellung angegebenen Instanz. Beispiel: Primäre Instanz, Lesepool-Instanz oder sekundäre Instanz.
IP-Adresse [ip_address]	IP-Adresse für die Instanz, die der Endpunkt für eine Endanwenderanwendung ist.

In der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten AlloyDB for PostgreSQL-Ressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen anzeigen.

AlloyDB für PostgreSQL-Instanzabhängigkeitsansicht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AlloyDB für PostgreSQL-Clusterabhängigkeitsansicht

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung der AlloyDB für PostgreSQL-Discovery.

CI	Beziehung	CI
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Datenbank [cmdb_ci_cloud_database]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	Cluster von::Cluster	Cloud-Datenbank [cmdb_ci_cloud_database]
Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	Repliziert::repliziert von	Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]
Schlüsselwert [cmdb_key_value]	Referenzen	Cloud-Datenbank [cmdb_ci_cloud_database]
Schlüsselwert [cmdb_key_value]	Referenzen	Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]

Tag-Discovery

Das Google Cloud Platform (GCP) – AlloyDB for PostgreSQL-Muster sammelt Tags und füllt sie in zwei Einträge in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus. Ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eintrag verweist auf die Cloud-Datenbanktabelle, der andere auf die Cloud-Datenbank-Clustertabelle.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Schlüssel.
Wert [value]	Tag-Wert.
Konfigurationselement [configuration_item]	Verweist auf die Cloud-Datenbank-Tabelle [cmdb_ci_Cloud_database]
Konfigurationselement [configuration_item]	Verweist auf die Tabelle „Cloud-Datenbank-Cluster“ [cmdb_ci_Cloud_DB_Cluster]

Google Cloud Platform (GCP) Asset-Bestandserkennung mit Mustern

Die ServiceNow Discovery-Anwendung verwendet Google Cloud Platform (GCP) Zu suchendes Asset-Bestandsmuster GCP Ressourcen und Richtlinien. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Das Muster bietet Sichtbarkeit für Services, die von der Asset Inventory-API unterstützt werden, sowie zum Sammeln von Bestandsdaten zu den bereitgestellten GCP-Services und zum Aktualisieren der CMDB.

Das Muster sammelt Bestandsdaten entweder für alle von GCP unterstützte Ressourcen oder für eine vorkonfigurierte Aufnahmeliste von Ressourcen. Die Aufnahmeliste für Ressourcen des Cloud-Bestands enthält alle Ressourcentypen, die vom Bestand von GCP-Cloud-Assets unterstützt werden, mit Ausnahme von Compute Engine-Ressourcen und IAM-Richtlinien. Ihren Anforderungen entsprechend können Sie die Aufnahmeliste um zusätzliche Ressourcentypen erweitern. Weitere Informationen zu Google Cloud-Assets finden Sie unter https://cloud.google.com/resource-manager/docs/cloud-asset-inventory/overview .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Beginnend mit Muster für Discovery und Service-Mapping Version 1.18.1 können Sie erkennen GCP Speicher nach zwei Discovery-Typen: Serverlose und Cloud-Discovery. Durch das Ausführen von Cloud-Discovery-Zeitplänen können Sie einen Zeitplan für alle ausführen GCP Projekte, ohne separate Zeitpläne manuell zu konfigurieren. Sie können die serverlose Discovery auch wie zuvor verwenden.

Erweitert Google Cloud Platform (GCP) Das Asset-Bestandsmuster führt Abfragen aus, um die Konfigurationen in Ihrem System zu überprüfen und eine Discovery gemäß Ihren Konfigurationen auszulösen. Die Abfragen nach Reihenfolge:

1. Wenn Sie haben **Startprogramm-Parameter Für Discovery-Muster** Konfiguriert löst das Muster einen serverlosen Discovery-Zeitplan aus.

2. Wenn die vorherige Abfrage keine Ergebnisse enthält, wird die Abfrage des Musters fortgesetzt, wenn Sie über verfügen `mid.gcp_resource_inventory_bucketpath`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-ServerEigenschaft konfiguriert. Wenn Sie dies tun, führt das Muster einen Cloud-Discovery-Zeitplan nach Cloud-Accounts aus.

3. Wenn die vorherige Abfrage keine Ergebnisse enthält, wird die Abfrage des Musters fortgesetzt, wenn Sie über verfügen `mid.gcp_resource_inventory_bucketpath.default` MID-ServerEigenschaft konfiguriert. Wenn Sie dies tun, löst das Muster einen standardmäßigen Cloud-Discovery-Zeitplan aus.
4. Wenn keine dieser Eigenschaften konfiguriert ist, wird das Muster ordnungsgemäß beendet.

Voraussetzungen

Überprüfen Sie, ob die Store-Apps aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

GCP Autorisierung für Discovery zur Verwendung der Cloud-Asset-API

- API-Endpunkt: `https://cloudasset.googleapis.com/v1/projects/<account_id>: ExportAssets`
- Mindestens eine der folgenden IAM-Berechtigungen für das angegebene übergeordnete Ressourcenelement erforderlich:
  - cloudasset.assets.exportResource
  - cloudasset.assets.exportIamPolicy

Service-Account-Anwender für die Cloud-Speicher-API

Die ServiceNow Cloud-Service-Account muss über verfügen Schreibgeschützte Berechtigung von GCP Bis Greifen Sie auf den API-Endpunkt zu – https://www.googleapis.com/storage/v1.

Hinweis: Mit den Headern auf der Verschlüsselungsseite können Sie Folgendes tun:

- Laden Sie ein Objekt herunter, das mit einem vom Kunden bereitgestellten Verschlüsselungsschlüssel verschlüsselt ist.
- Rufen Sie Objektmetadaten mit Inhalts-Hashes ab.

Berechtigung zum Lesen und Schreiben in einen Cloud-Speicher-Bucket

- Speicherobjekt-Ersteller
- Speicherobjekt-Viewer
- Speicherobjekt-Administrator

Erstellen Sie einen Cloud-Speicher-Bucket mit der Google Cloud-Konsole

1. Wechseln Sie zu **Google Cloud-Konsole** .
2. Von **Navigationsmenü** , Wählen Sie aus **Cloudspeicherung** > **Buckets**an.
3. Um einen neuen Bucket zu erstellen, wählen Sie aus **+ Erstellen** .
4. Auf der **Erstellen Sie einen Bucket** Seite, geben Sie die Bucket-Informationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Benennen Sie Ihren Bucket	Geben Sie einen global eindeutigen Namen für Ihren Bucket ein.
Wählen Sie aus, wo Ihre Daten gespeichert werden sollen	Wählen Sie einen Standorttyp und einen Standort aus, an dem die Bucket-Daten dauerhaft gespeichert werden. ○ Standorttyp: Multi-Region, für globalen Speicher (z. B. USA, eu, asien). ○ Speicherort: Liste der Cloud-Speicherorte, die zum Speichern Ihrer Daten verfügbar sind.
Wählen Sie eine Speicherklasse für Ihre Daten aus	Wählen Sie die entsprechende Speicherklasse für Ihre Anforderungen aus (z. B. Standard, Nearline, Coldline oder Archiv).
Wählen Sie aus, wie der Zugriff auf Objekte gesteuert werden soll	Wählen Sie aus, ob Ihr Bucket die Verhinderung des öffentlichen Zugriffs erzwingt.
Wählen Sie aus, wie Objektdaten geschützt werden sollen	Konfigurieren Sie bei Bedarf Schutztools.

5. Wählen Sie **Erstellen** aus.

Hinweis: Weitere Informationen finden Sie unter Google Cloud Storage-Dokumentation .

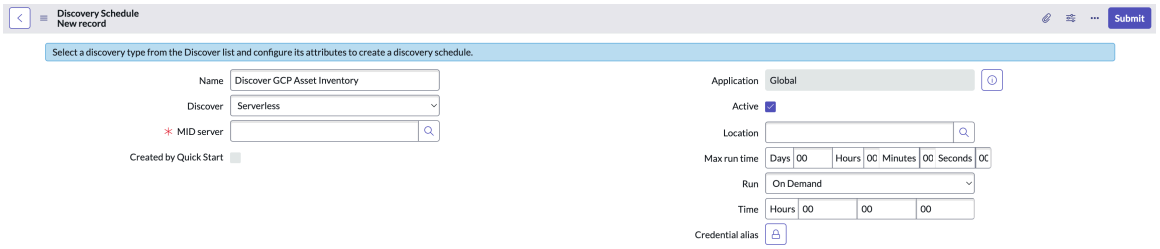
Aufbewahrungsrichtlinie für den Speicher-Bucket

Stellen Sie sicher, dass die Aufbewahrungsrichtlinie für den Speicher-Bucket nicht aktiv ist. Wenn die Aufbewahrungsrichtlinie aktiv ist, kann die automatisch generierte Bestandsdatendatei nicht durch das Muster gelöscht werden.

Erstellen Sie einen serverlosen Discovery-Zeitplan

Erstellen Sie einen Discovery-Zeitplan, um eine gezielte Discovery von durchzuführen GCP Asset-Bestand.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular



aus.

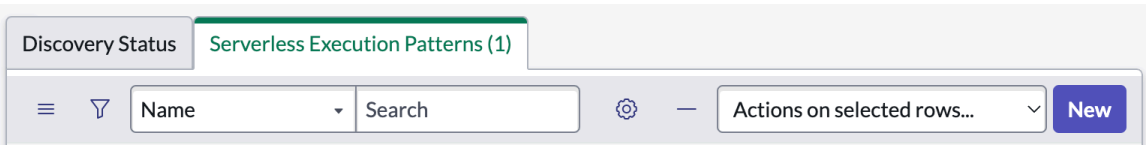
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Beispiel: `GCP-Asset-Bestand erkennen` .
Erkannt	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Server s
Ausführen	Option zum Auswählen, wann die nächste Discovery ausgeführt werden soll.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.



Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispiel: `GCP-Asset-Bestand erkennen` .
Muster	Wählen Sie aus **Google Cloud Platform (GCP) – Ressourcenbestand** Muster.
Proxyhost	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Wählen Sie **Absenden**.
6. In **Startprogramm-Parameter Für Discovery-Muster** Konfigurieren Sie die folgenden Parameter mit den relevanten Werten:

Parameter	Wert
cloud_account_id	Projekt-ID in GCP
Full_path_file	Der vollständige Dateipfad des Speicher-Buckets. Beispiel: `gs://<bucketname>` .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
cloud_cred_id	Sysid der GCP-Anmeldeinformationen
cloud_datacenter_type	cmdb_ci_google_datacenter

Speicher-Discovery-Konfigurationen mit MID-Server Eigenschaften

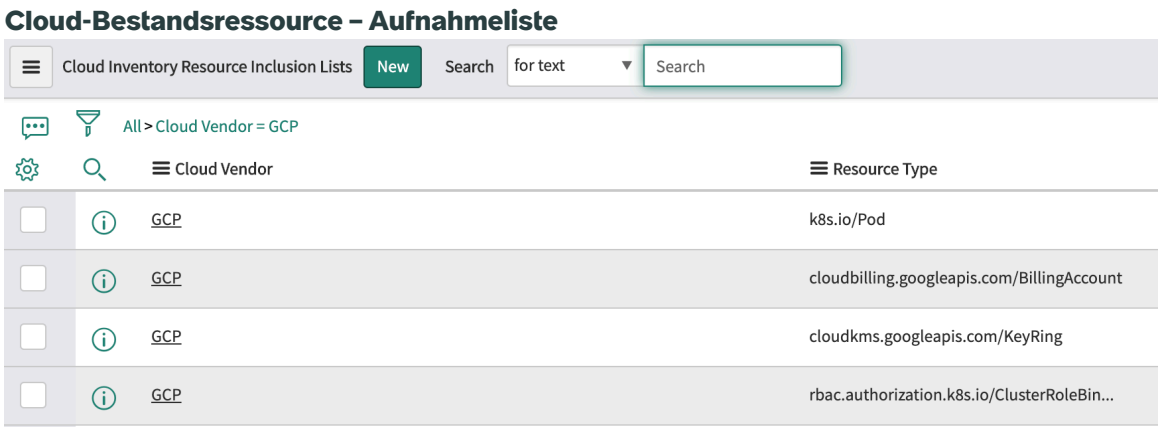
1. Konfigurieren Sie die Eigenschaft *mid.gcp_resource_inventory_bucketpath*.
   a. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** Und filtern Sie die Liste nach Name beginnt mit Mid.gcp .
   b. Wählen Sie *mid.gcp_resource_inventory_bucketpath*.
   c. Füllen Sie das Formular aus.
      i. Konfigurieren Sie die Eigenschaft **Name** Feld zum Einfügen Ihrer Account-ID wie folgt: Mid.gcp_resource_Inventory_bucketpath.<Cloud-Account-ID> .
      ii. Füllen Sie aus **Wert** Feld mit dem Bucket-URI, das der vollständige Dateipfad des Speicher-Buckets ist. Beispiel: gs://<bucketname> .
      iii. In **MID-Server** Feld leer lassen, um festzulegen MID-ServerEigenschaft, die sich auf alle MID-Server auswirkt. Zum Festlegen von MID-ServerEigenschaft für eine bestimmte MID-Server, Wählen Sie den bevorzugten Server aus.
      iv. Wählen Sie **Aktualisieren**.
2. Konfigurieren Sie die Eigenschaft *mid.gcp_resource_inventory_bucketpath.default*.
   a. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** Und filtern Sie die Liste nach Name beginnt mit Mid.gcp .
   b. Wählen Sie *mid.gcp_resource_inventory_bucketpath.default*.
   c. Füllen Sie aus **Wert** Feld mit dem Bucket-URI, das der vollständige Dateipfad des Speicher-Buckets ist. Beispiel: gs://<bucketname> .
   d. Wählen Sie **Aktualisieren**.

Weitere Informationen finden Sie unter Exportieren Sie Asset-Metadaten aus einem Projekt in ein anderes

Cloud-Bestandsressource-Aufnahmeliste

- Dient zum Sammeln von Bestandsdaten für Ressourcen, die von unterstützt werden GCP, In ServiceNow AI Platform, Navigieren Sie zu **Cloud-Bestandsressource – Aufnahmeliste** Und löschen Sie alle GCP Tabellendatensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Feintunen Sie die Erkennung von GCP-Ressourcen mithilfe der Aufnahmeliste von Cloud-Bestandsressourcen.

  Wenn Ihre Bereitstellung benutzerdefinierte Muster für die GCP-Erkennung hat, stellen Sie sicher, dass Sie GCP-Ressourcen nicht zweimal entdecken:

  1. Stellen Sie sicher, dass der Anwendungsbereich „Discovery and Service Mapping Patterns“ ist:
     a. Navigieren zu **Einstellungen** > **Entwickler**an.
     b. Wählen Sie Discovery and Service Mapping Patterns aus der Liste **Anwendung** aus.
  2. Navigieren zu **Systemdefinitionen** > **Tabellen**an.
  3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
  4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
  5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option Löschen aus.

  Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Liste wie folgt mit zusätzlichen Ressourcentypen erweitern, die vom Muster erkannt werden sollen:

  Hinweis: Wenn Sie die im Basissystem bereitgestellte Liste ändern, wird sie in Anwendungs-Updates nicht mehr automatisch aktualisiert. Sie müssen anwenderdefinierte Listen selbst verwalten.

  1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
  2. Klicken Sie auf **Neu**.
  3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

  Hinweis: Die Namen der zusätzlichen Ressourcentypen müssen den entsprechenden Namenskonventionen der Lieferanten entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Cloud-Anbieter	Der Lieferant des Ressourcentyps: GCP
Ressourcentyp	Wert des GCP-Ressourcentyps
Anwendung	Der Anwendungsbereich: Discovery and Service Mapping Patterns

Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Dieses Muster erkennt Daten, die Sichtbarkeit für alle GCP-Services in Ihrer Organisation bieten. Die erkannten Daten umfassen die folgenden Tabellen und Felder.

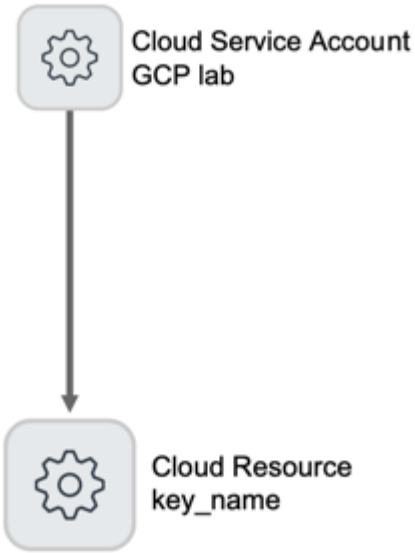
Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_cmp_resource]	
object_id	Die ID des Elements. Das Element wird mit dieser URL aufgerufen.
name	Der Name der Ressource
resource_type	Der Asset-Ressourcentyp gemäß den Daten in der JSON-Datei
Schlüsselwert [cmdb_key_value]	
Schlüssel	Der Name des GCP-Tag-Schlüssels.
Wert	Der Name des GCP-Tag-Werts.

Die Dependency Views-Zuordnung zeigt die erkannten Konfigurationselemente (CIs) in Ihrer Organisation und die Beziehungen zwischen ihnen an. Hier ist die einzige bedeutungsvolle Beziehung zwischen den CIs die, mit der Discovery sie identifizieren kann.

Jedes GCP-Bestand-CI ist entweder einem Logischen Datenzentrum (LDC)-CI oder einem Cloud-Servicekonto-CI zugeordnet. In diesem Beispiel bezieht sich das Bestand-CI auf ein Cloud-Servicekonto-CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dependency Views-Zuordnung mit Cloud-Servicekonto-CI



CI-Beziehungen

Diese Beziehungen sollen die GCP-Asset-Bestandserkennung unterstützen:

CI	Beziehung	CI
Für globale Ressourcen:		
Haupt-CI [cmdb_ci_cmp_resource]	Enthalten in::Enthält	Cloud-Servicekonten
Für regionale Ressourcen:		
Haupt-CI [cmdb_ci_cmp_resource]	HostedOn::Hosts	Logisches Rechenzentrum (LDC)

Google Cloud Platform (GCP) Discovery von Cloud-Funktionen mithilfe von Mustern

Muster für Discovery und Service-Mapping Verwendet das Muster „Google Cloud Platform (GCP) – Cloud-Funktionen“, um Cloud-Funktionen in einem zu erkennen Google Cloud Platform (GCP) Bereitstellung während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie GCP Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Google Cloud Platform (GCP) – Cloud-Funktionen“.

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [Account_ID]	Name des Projekts, das für die Discovery verwendet wird.
Objekt-ID [object_id]	Name des Projekts, das für die Discovery verwendet wird.
Rechenzentrumstyp [datacenter_type]	Rechenzentrumstyp: Google-Rechenzentrum [cmdb_ci_google_Datacenter].

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Beschreibung [short_description]	Beschreibung der Verfügbarkeitszone.
Status [state]	Status der Verfügbarkeitszone. Mögliche Werte sind verfügbar oder beendet.

Google-Rechenzentrum [cmdb_ci_google_datacenter]

Feld	Beschreibung
Name [name]	Name des Rechenzentrums oder der Region
Region [Region]	Name des Rechenzentrums oder der Region
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von zugewiesen wurde GCP Für diese Ressource.
Beschreibung [short_description]	Beschreibung des Rechenzentrums oder der Region.

Cloud-Funktion [cmdb_ci_cloud_function]

Feld	Beschreibung
Version [version]	Versions-ID der Funktion, nur verfügbar für Gen1-Cloud-Funktionen.
Objekt-ID [object_id]	Name, der aus der API-Antwort abgerufen wird. Beispiel: Projects/Automation-226410/locations/US-central1/Functions/Auto-labeller .
Name [name]	Name, der aus der API-Antwort analysiert wurde. Beispiel: automatische Etikettierung .
Letzte Änderung an der Funktion [function_last_modified]	Zeitstempel, der angibt, wann die Funktion zuletzt aktualisiert wurde.

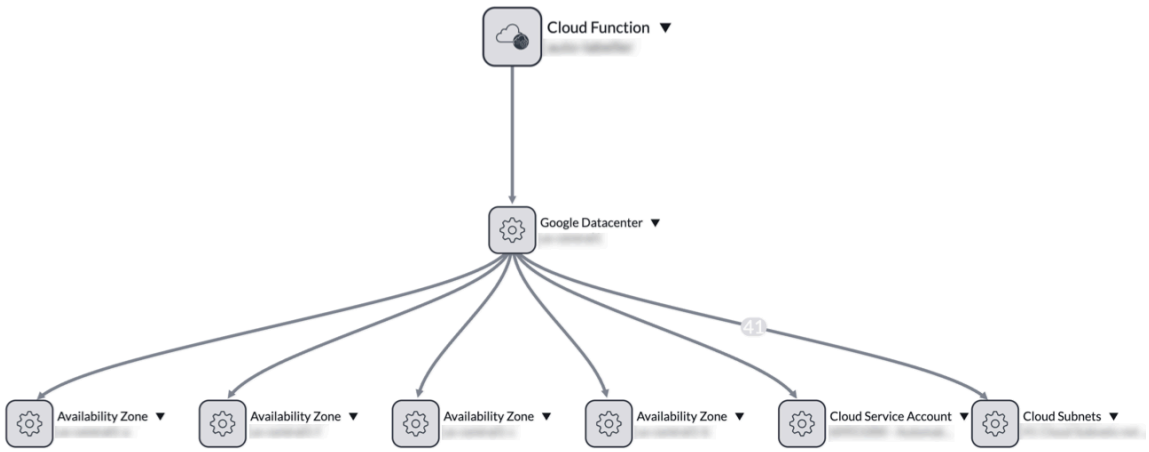
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Funktion [cmdb_ci_cloud_function] (Fortsetzung)

Feld	Beschreibung
CodeSha256 [codesha256]	SHA-256-Hash-Algorithmus des Codes der Funktion, der zum Überprüfen der Integrität des Builds verwendet wird. Beispiel: `273a583f-ef1c-49c2-9bae-7d21bf3b5f7a` .
Sprache [language]	Laufzeitumgebung oder Programmiersprache, die für die Funktion verwendet wird.
Installationsstatus [install_status]	Installationsstatus der Funktion. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Funktion. Der Standardwert ist betriebsbereit.

Auf der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten anzeigen GCP Cloud-Funktionsressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen.

GCP Abhängigkeitsansicht für Cloud-Funktionen



CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von GCP Discovery von Cloud-Funktionen.

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Cloud-Funktion [cmdb_ci_cloud_function]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Schlüsselwert [cmdb_key_value]	Referenzen	Cloud-Funktion [cmdb_ci_cloud_function]

Tag-Discovery

Das Muster „Google Cloud Platform (GCP) – Cloud-Funktionen“ erfasst Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.
Konfigurationselement [configuration_item]	Verweist auf die Tabelle „Cloud-Funktion“ [cmdb_ci_Cloud_function].

Google Cloud Platform (GCP) Speicher-Discovery mit Mustern

Muster für Discovery und Service-Mapping Verwendet das Google Cloud Platform (GCP) – Memorystore DB-Muster, um den Memorystore für Memcached und den Memorystore für Redis während der horizontalen Discovery zu erkennen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie GCP Abschnitt „Discovery-Voraussetzungen“ in Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Google Cloud Platform (GCP) – Memorystore DB.

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [Account_ID]	Name des Projekts, das für die Discovery verwendet wird.
Objekt-ID [object_id]	Name des Projekts, das für die Discovery verwendet wird.
Rechenzentrumstyp [datacenter_type]	Rechenzentrumstyp: Google-Rechenzentrum [cmdb_ci_google_Datacenter].

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Beschreibung [short_description]	Beschreibung der Verfügbarkeitszone.
Status [state]	Status der Verfügbarkeitszone. Mögliche Werte sind verfügbar oder beendet.

Google-Rechenzentrum [cmdb_ci_google_datacenter]

Feld	Beschreibung
Name [name]	Name des Rechenzentrums oder der Region
Region [Region]	Name des Rechenzentrums oder der Region

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Google-Rechenzentrum [cmdb_ci_google_datacenter] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von zugewiesen wurde GCP Für diese Ressource.
Beschreibung [short_description]	Beschreibung des Rechenzentrums oder der Region.

Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]

Feld	Beschreibung
Name [name]	Name des Clusters.
Cluster-ID [cluster_id]	ID des Clusters.
Installationsstatus [install_status]	Installationsstatus des Clusters. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus des Clusters. Der Standardwert ist betriebsbereit.
Clusterstatus [cluster_status]	Aktueller Status dieses Clusters. Beispiel: BEREIT oder GESTOPPT.
Clustertyp [Cluster_type]	Typ des Clusters: Redis-Cluster.
Festplattenspeicher (GB) [Disk_space]	Speicherplatz in Gigabyte (GB).
IAM-Authentifizierung aktiviert [iam_authentication_enabled]	Bestimmt, ob die IAM-Authentifizierung aktiviert ist. Mögliche Werte sind „wahr“ oder „falsch“.
Knotenanzahl [node_count]	Anzahl der Replikatknoten pro Shard.
Löschschutz aktiviert [DELETION_Protection_enabled]	Bestimmt, ob der Löschschutz aktiviert ist. Mögliche Werte sind „wahr“ oder „falsch“.
Asset-Tag [asset_tag]	Knotentyp eines Redis-Clusterknotens. Beispiel: REDIS_SHARED_CORE_NANO oder REDIS_HIGHMEM_MEDIUM.

Cloud-Datenbank [cmdb_ci_cloud_database]

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Name der Ressource in diesem Bereich, einschließlich Projekt und Standort.
Name [name]	Eindeutiger Name der Ressource, analysiert aus der Objekt-ID.
Typ [type]	Typ der Datenbank. Mögliche Werte sind „memCache-instance“ oder „redis-instance“.
Installationsstatus [install_status]	Installationsstatus der Datenbank. Standardwert ist installiert.

Automatische Übersetzung

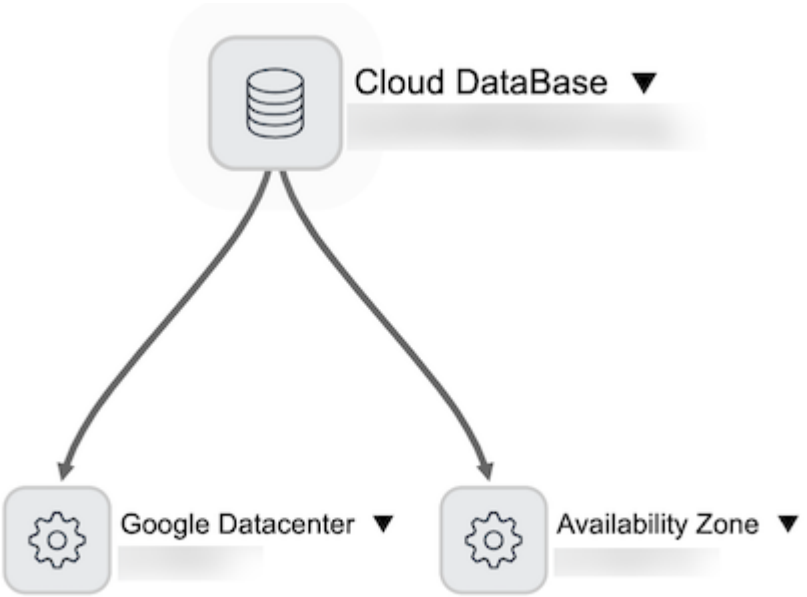
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Datenbank [cmdb_ci_cloud_database] (Fortsetzung)

Feld	Beschreibung
Betriebsstatus [operational_status]	Betriebsstatus der Datenbank Der Standardwert ist betriebsbereit.
Status [state]	Status der Datenbank Mögliche Werte sind verfügbar oder beendet.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (FQDN) für den Ressourcentyp.
IP-Adresse [ip_address]	Hostname oder IP-Adresse des exponierten Endpunkts, der von Clients für die Verbindung mit dem Service verwendet wird.

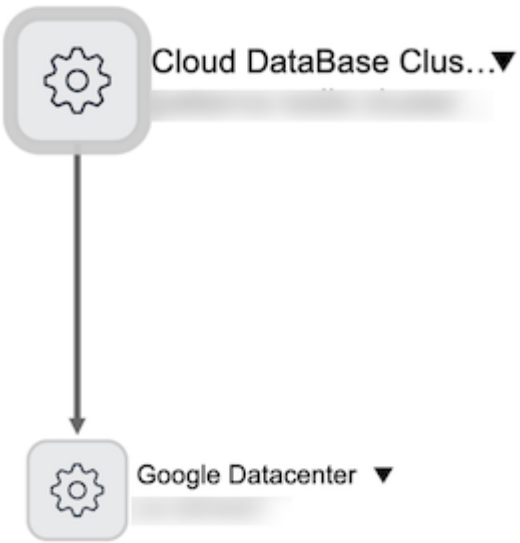
In der Zuordnung „Abhängigkeitsansichten“ können Sie alle erkannten Arbeitsspeicher für Arbeitsspeicher oder Arbeitsspeicher für Redis-Ressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen anzeigen.

Arbeitsspeicher für Arbeitsspeicher oder Arbeitsspeicher für Abhängigkeitsansicht der Redis-Instanz



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsspeicher für Redis-Clusterabhängigkeitsansicht



CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung der Memorystore-Discovery.

CI	Beziehung	CI
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	Erstreckt sich von	Cluster [cmdb_ci_cluster]
Cloud-Datenbank-Cluster [cmdb_ci_Cloud_DB_Cluster]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Referenzen	Cloud-Datenbank [cmdb_ci_cloud_database]

Tag-Discovery

Das Google Cloud Platform (GCP) – Memorystore DB-Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value] (Fortsetzung)

Feld	Beschreibung
Wert [value]	Tag-Wert.
Konfigurationselement [configuration_item]	Verweist auf die Cloud-Datenbank-Tabelle [cmdb_ci_Cloud_database].

Google Cloud Platform (GCP) Organisations-Discovery mit Mustern

Die Anwendung ServiceNow Discovery verwendet das Google Cloud Platform (GCP)-Organisationserkennungsmuster, um GCP-Organisationsprojekte und -ressourcen zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

GCP-Organisationsstruktur

Vergewissern Sie sich, dass eine GCP-Organisationsressource ordnungsgemäß strukturiert ist und sich die Projekte in einer anderen Hierarchie darunter befinden.

Stellen Sie sicher, dass für alle Projekte unter der GCP-Organisationsressource die Compute Engine-API aktiviert ist.

Servicekonto-Benutzereinstellungen

Überprüfen Sie, ob Benutzer des Servicekontos Zugriff auf den Ressourcenknoten der GCP-Organisation haben.

Stellen Sie sicher, dass Servicekonto-Benutzer Mitglieder aller anderen Projekte sind, die sich unter dem GCP -Organisationsressourcenknoten befinden.

Stellen Sie sicher, dass Servicekonto-Benutzer über die folgenden Cloud-Identitäts- und Zugriffsverwaltungs-Anmeldeinformationen für Projekte unter der GCP-Organisationsressource verfügen:

- resourcemanager.folders.list
- resourcemanager.organizations.get
- resourcemanager.projects.get
- resourcemanager.projects.list

Anmeldeinformationen für API-Elemente

Während der Erkennung verwendet das Muster folgende API-Elemente. Der Benutzer, der den Anmeldeinformationen in der Instanz hinzugefügt wurde, muss über Berechtigungen zum Senden dieser Abfragen verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- https://cloudresourcemanager.googleapis.com/v1/{name=organizations/*}
- https://cloudresourcemanager.googleapis.com/v1/projects
- https://cloudresourcemanager.googleapis.com/v2/folders:search

Anmeldeinformationen für die Erstellung eines Erkennungszeitplans

Konfigurieren Sie die folgenden Anmeldeinformationen:

1. Erstellen Sie GCP-Anmeldeinformationen.
2. Erstellen Sie ein GCP-Servicekonto:
   a. Anmeldeinformationen: Die GCP-Anmeldeinformationen
   b. Konto-ID: Die Google-Servicekonto-ID
   c. Rechenzentrumstyp: Wählen Sie **cmdb_ci_google_datacenter** aus.
3. Erstellen Sie einen Erkennungszeitplan.

(Optional) Erkennungszeitplan ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan, um eine gezielte Erkennung von GCP-Organisationsressourcen durchzuführen.

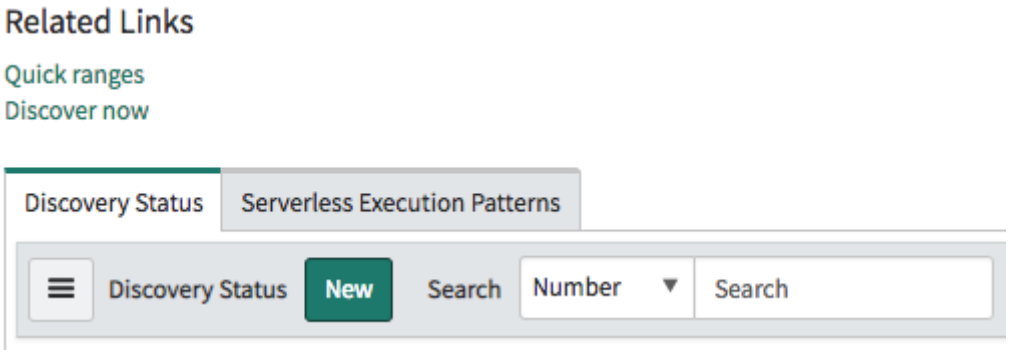
1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Beispielsweise GCP-Organisation erkennen.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Server s
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Formular „Ausführungsmuster ohne Server“

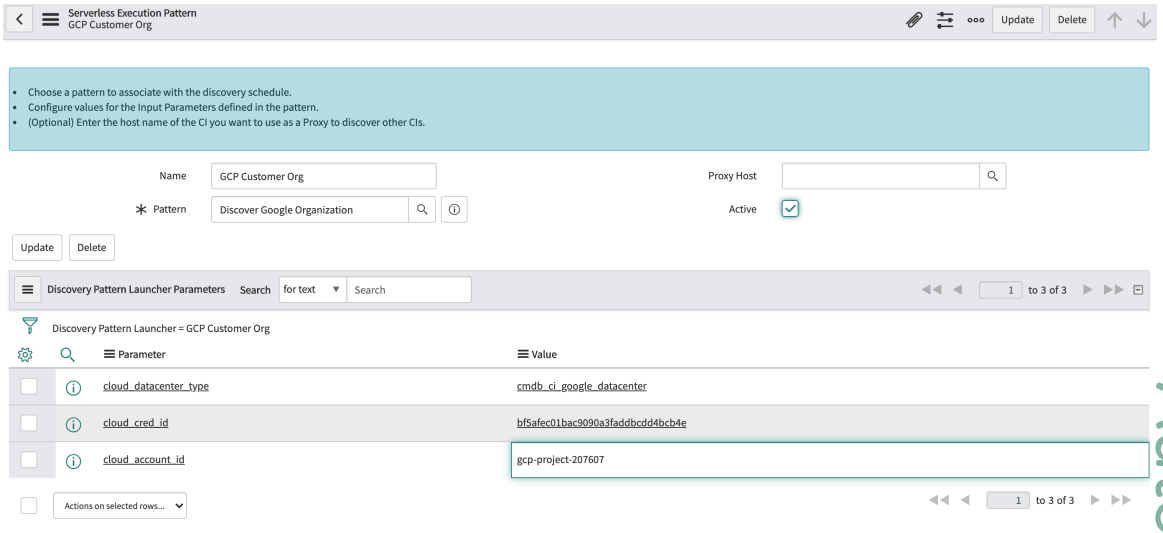
Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispielsweise GCP-Organisation erkennen.
Muster	Name des auszuführenden Musters: GCP Organization.
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Konfigurieren Sie unter **Startprogrammparameter für Discovery-Muster** die folgenden Parameter mit den entsprechenden Werten:

Parameter	Wert
cloud_account_id	Projekt-ID in GCP
cloud_cred_id	Sysid der GCP-Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
cloud_datacenter_type	cmdb_ci_google_datacenter



Kunden mit frühem Zugriff auf das Muster „GCP Organization“

Stellen Sie sicher, dass die geplante Aufgabe „Discover-GCP-SubAccounts“ in Ihrer Instanz nicht aktiviert ist.

1. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**an.
2. Klicken Sie auf die geplante Aufgabe „Discover-GCP-SubAccounts“.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **Aktualisieren**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Organisation [cmdb_ci_cloud_org]	
name	Der Name der Organisationsressource
object_id	Die ID der Organisationsressource
time	Die Zeit, zu der die Organisationsressource in GCP erstellt wurde
operational_status	Aktueller Betriebsstatus. Eine der folgenden Möglichkeiten: • Operativ • Nicht funktionsfähig • Reparatur in Bearbeitung • DR-Standby • Bereit • Stillgelegt
Ordner [cmdb_ci_gcp_folder]	
name	Der Name des Organisationsordners

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
parent_id	Die ID der übergeordneten Ressource
parent_type	Der Typ der übergeordneten Ressource. Kann `Organisation` oder `Ordner` sein.
time	Die Zeit, zu der die Ressource in GCP erstellt wurde
Status	Der Status des Ordners gemäß dem `Lebenszyklusstatus` in GCP
object_id	Die ID des Organisationsordners
Projekt [cmdb_ci_gcp_project]	
name	Der Name des Projekts
project_id	Die ID des Projekts
parent_id	Die ID der übergeordneten Ordnerressource
parent_type	Der Typ der übergeordneten Ressource. Kann `Organisation` oder `Ordner` sein.
time	Die Zeit, zu der die Ressource in GCP erstellt wurde
operational_status	Der Status des Ordners gemäß dem `Lebenszyklusstatus` in GCP
object_id	Die ID des Projekts
discovery_credentials	GCP-Kontoanmeldeinformationen
Ressource [cmdb_key_value]	
key	Der Schlüssel oder die Bezeichnung, die dem GCP-Projekt zugeordnet ist. Beispiel: `Land`.
Wert	Der dem GCP-Projekt zugewiesene Projektbezeichnungswert. Beispiel: `ca`.
configuration_item	Die URL oder der Pfad des CI.

CI-Beziehungen

CI	Beziehung	CI
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Servicekonto
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Google-Ordner [cmdb_ci_gcp_folder]
Servicekonto	Eigentümer von::Eigentum von	Google-Projekt [cmdb_ci_gcp_project]
Google-Ordner [cmdb_ci_gcp_folder]	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]
Google-Ordner [cmdb_ci_gcp_folder]	Enthalten in::Enthält	Untergeordneter Google-Ordner
Untergeordneter Google-Ordner	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM Cloud Platform-Erkennung

Die ServiceNow Discovery-Anwendung findet IBM Cloud Platform-Komponenten (Softlayer API v3 und v3.1 und Bluemix-API v2) mithilfe der IBM Cloud Platform-Muster. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können die Muster auf ServiceNow AI Platform mithilfe der Versionen London Patch 7, Madrid Patch 2 oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

MID-Server

Verwenden Sie zur Cloud-Erkennung einen dedizierten MID-Server. Der MID-Server muss über 16 Kerne und 8 GB mit 4 GB Java Memory Model (JVM)-Speicherzuweisung verfügen.

Stellen Sie den dedizierten MID-Server mit Internetzugang bereit und stellen Sie die Verbindung her.

Berechtigungen

Die Cloud-Ressourcen befinden sich in einer IBM-Cloud. Erstellen Sie die IBM-Anmeldeinformationen für den Zugriff auf Ihr IBM-Konto.

1. Navigieren zu **Discovery** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **IBM-Anmeldeinformationen**, und füllen Sie das Formular aus:

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen Ein Beispiel ist ibm-cred.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	in zufälliger Reihenfolge durch. Der Standardwert ist 100.
SoftLayer-API-Benutzer	Benutzername für die Softlayer-API. Verwenden Sie den Softlayer-API-Benutzernamen, der in der Softlayer-Konsole definiert ist.
SoftLayer-API-Schlüssel	Schlüssel für die Softlayer-API. Verwenden Sie den Softlayer-API-Schlüssel, der in der Softlayer-Konsole definiert ist.
Bluemix-API-Schlüssel	Schlüssel für die Bluemix-API. Verwenden Sie den in der IBM Cloud-Konsole definierten Bluemix-API-Schlüssel.

4. Klicken Sie auf **Absenden**.

IBM Cloud-Servicekonto erstellen

Verwenden Sie die im vorherigen Verfahren definierten Anmeldeinformationen, um das IBM Cloud-Servicekonto zu erstellen.

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Konten**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus:

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Name der Anmeldeinformationen Ein Beispiel ist ibm-snow.
Konto-ID	IBM Konto-ID-Name. Geben Sie die IBM-Konto-ID ein.
Discovery Anmeldeinformationen	Discovery-Anmeldeinformationen, die Sie zuvor definiert haben
Datencenter-Typ	Datencenter-Typ. Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]

4. Klicken Sie auf **Absenden**.

Discovery-Zeitplan ohne Server erstellen

Konfigurieren Sie eine Discovery ohne Server.

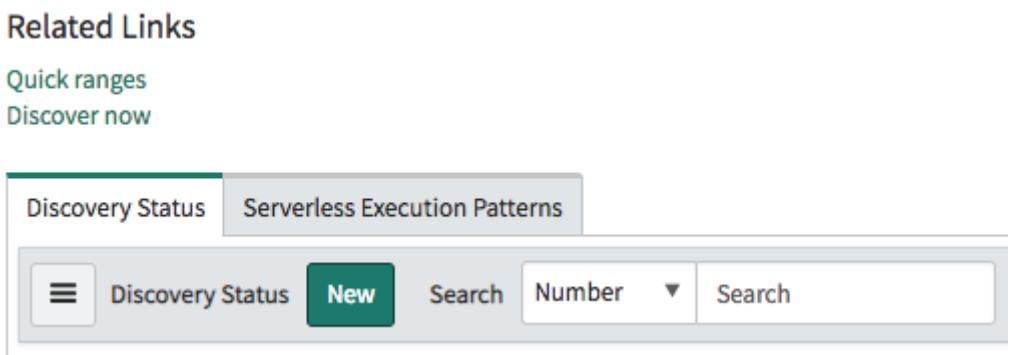
1. Auf der ServiceNow AI Platform, Navigieren Sie zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name für diesen Discovery-Zeitplan. Beispiel: Muster ohne Server
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Server s Beispiel: Discovery_Server
Aktiv	Option zur Aktivierung dieses Zeitplans für Discovery. Aktivieren Sie dieses Kontrollkästchen, um Discovery zu aktivieren.
Ausführen	Gibt an, wie häufig der Discovery-Zeitplan ausgeführt werden soll

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.

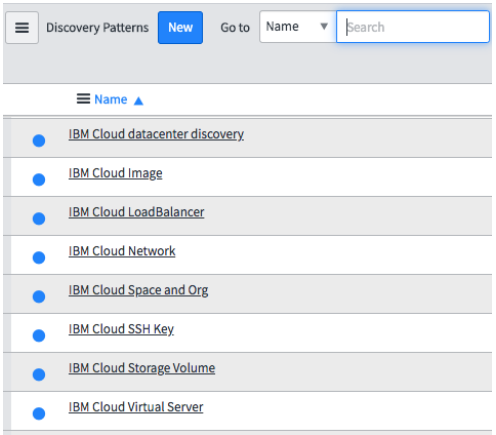


5. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**.
6. Klicken Sie auf **Neu**.
7. Füllen Sie die Felder im Formular aus:

Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispiel: IBM1.
Muster	Name des Musters, das Sie ausführen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	 Wenn Sie mehrere Muster ausführen möchten, erstellen Sie mehrere Datensätze.
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zur Aktivierung dieses Zeitplans für Discovery. Aktivieren Sie dieses Kontrollkästchen, um Discovery zu aktivieren.

8. Konfigurieren Sie die Parameter, die vom IBM Cloud Platform-Muster erforderlich sind, wie folgt:

Startprogrammparameter für Discovery-Muster

Parameter	Beschreibung
cloud_cred_id	Die sys_id der IBM-Anmeldeinformationen, die in der Konfiguration angegeben ist.
cloud_account_id	Die IBM-Konto-ID
cloud_datacenter_type	cmdb_ci_ibm_datacenter

9. **Führen Sie eine Aktualisierung durch**.
10. Um Discovery zu starten, navigieren Sie zur Discovery-Definition ohne Server, und klicken auf **Discovery starten**.

IBM Flow – horizontale Erkennung

- Wenn Sie die Erkennung mithilfe eines Zeitplans ohne Server ausführen möchte, werden die ausgewählten IBM Cloud-Platform-Muster ausgeführt und IBM Cloud-Platform-Ressourcen erkannt.
- Wenn Sie die Erkennung mit einem Servicekonto durchführen möchten, wird ein vollständiger IBM Cloud Platform-Discovery-Zeitplan ausgeführt, der alle unterstützten IBM Cloud Platform-Ressourcen erkennt.

Automatische Übersetzung

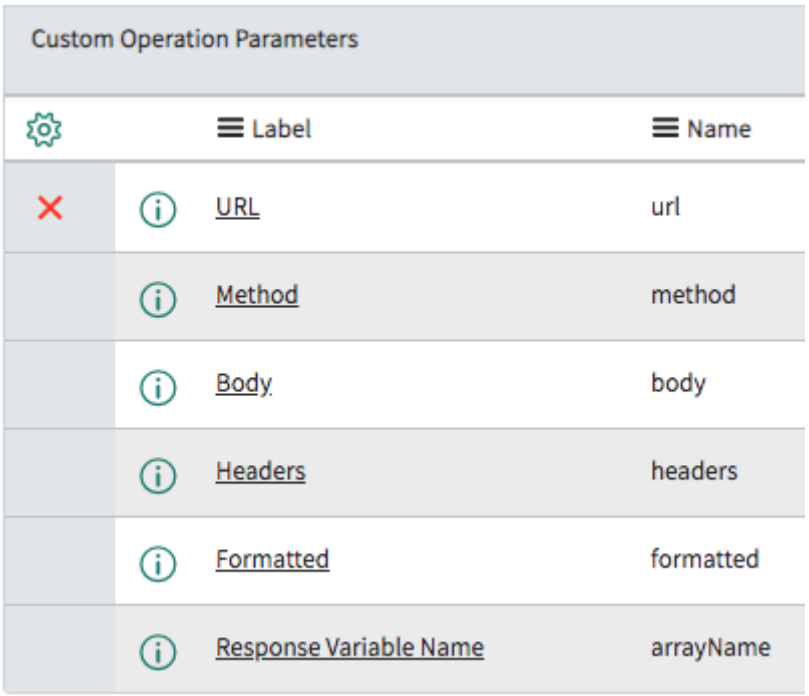
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefinierter Cloud-Vorgang

Cloud-REST – Antwort zu Kontext hinzufügen

Vorgang für Cloud-REST-Abfragen, der umfangreiche Antworten und eine bessere Speichernutzung unterstützt.

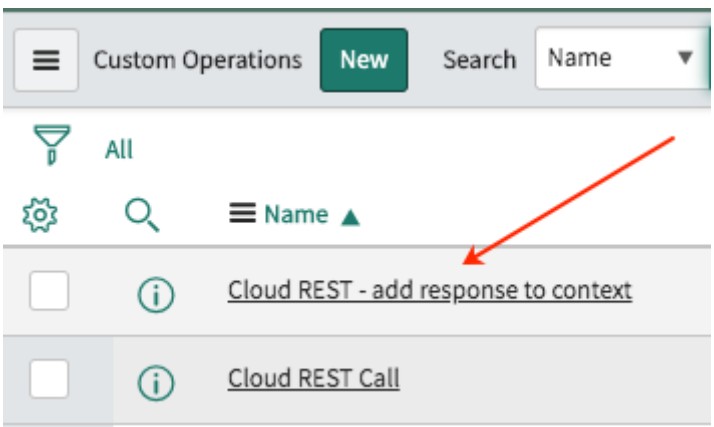
- Geben Sie alle Felder mit denselben Werten wie im benutzerdefinierten Vorgang „Cloud-REST-Abfrage“ an, mit Ausnahme der Tabelle für die Antwort, die im Feld **Name der Antwortvariablen** festgelegt ist.



- Legen Sie **Analyse definieren** als „Keine“ fest.

Methoden zum Abrufen von Daten für das IBM-Konto

1. Navigieren zu **Musterdesigner** > **Anwenderdefinierte Vorgänge**an.



2. Klicken Sie auf **Cloud-REST – Antwort zu Kontext hinzufügen**.

Methode: Get-Aufruf

API-URLs, die zum Abrufen der Daten verwendet werden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lastenausgleichsmodul *https://api.softlayer.com/rest<api_version>/SoftLayer_Network_LBaaS_LoadBalancer/getAllObjects?objectMask=mask[listeners[defaultPool],members,healthMonitors]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getNetworkVlans?objectMask=mask[primaryRouter.datacenter,name,id,vlanNumber,networkSpace]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getSubnets?objectMask=mask[datacenter]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getSecurityGroups?objectMask=mask[rules]*
- Organisationen und Bereiche *https://api.<region>.bluemix.net/v2/organizations*
- *https://api.<region>.bluemix.net/v2/spaces*
- SSH-Schlüssel *https://api.softlayer.com/rest/v3/SoftLayer_Account/SoftLayer_Account/getSshKeys*
- Speicher *https://api.softlayer.com/rest/<api_version>/SoftLayer_Account/getNetworkStorage*
- Virtueller Server *https://api.softlayer.com/rest/v3.1/SoftLayer_Account/getSecurityGroups*
- *http://api.softlayer.com/rest/v3.1/SoftLayer_Account/getSecurityGroups?objectMask=mask[id,name,networkComponentBindings[networkComponentId,networkCompon*
- *https://api.softlayer.com/rest/v3.1/SoftLayer_Account/getVirtualGuests?objectMask=mask[hostname,domain,powerState,fullyQualifiedDomainName,notes,id,stat*

EVAL-Funktionen

Verwenden Sie die folgende EVAL-Funktion, um die Lastenausgleichsmodul-API-Antwort in ein vollständiges JSON-Format umzuwandeln. Die Standardantwort hat das Format „[<resource objects>]”.

```
var cloud_lb_response = ${cloud_lb_response};
for (var i = 0; i < cloud_lb_response.size(); i++){
    cloud_lb_response.set(i, '{"result":[' + cloud_lb_response.get(i) + ']}');
}
CTX.setAttribute("cloud_lb_response", cloud_lb_response;
```

Verwenden Sie die folgende EVAL-Funktion, um die Netzwerk-API-Antwort in ein vollständiges JSON-Format umzuwandeln. Die Standardantwort hat das Format „[<resource objects>]”.

```
var network_response = ${network_response};
for (var i = 0; i < network_response.size(); i++){
    network_response.set(i, '{"result":[' + network_response.get(i) + ']}');
}
CTX.setAttribute("network_response", network_response);
```

Verwenden Sie die folgende EVAL-Funktion, um die IBM-Region aus der LB-Verfügbarkeitszone (Rechenzentrum) abzurufen. Dieselbe Funktion wird für andere Ressourcen im Muster verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var res = "";
res =
 IbmCloudDcToRegion.convertDctoRegion(${cloud_lb[].cloud_lb_az_short_name});
```

Verwenden Sie die folgende EVAL-Funktion, um den erforderlichen Algorithmus im Muster auszuwählen.

```
var rtrn
var lb_algorithm = ${cloud_lb_pools[].lb_algorithm}.toString();
switch (lb_algorithm){
  case "ROUNDROBIN":
    lb_algorithm = "round-robin";
    break;
  case "WEIGHTED_RR":
    lb_algorithm = "round-robin";
    break;
  case "LEASTCONNECTION":
    lb_algorithm = "least-connections";
    break;
  default: break;
```

Verwenden Sie die folgende EVAL-Funktion, um die eindeutige Region für das Konto zu analysieren, das die Organisationen und die entsprechenden Bereiche hostet.

```
var tableWithoutDuplicates = '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${account_region},["region_name"]);
CTX.setAttribute("account_region_unique",  tableWithoutDuplicates);
```

Verwenden Sie die folgende EVAL-Funktion, um Informationen für alle Organisationen abzurufen, die dem IBM Cloud-Konto zugewiesen sind, bei dem die Iteration zum Abrufen der eindeutigen Region durchgeführt wird.

```
var cloudcall = new CloudRestAPIClient();
var resourceTable = ${account_region_unique[*].region_name};
var tableSize = resourceTable.size();
var tmp_response = new Packages.java.util.ArrayList();
var all_organizations_response = new Packages.java.util.ArrayList();
for (var i = 0; i < tableSize ; i++){
  if  (!resourceTable.get(i)) continue;
  var url = "https://api."+resourceTable.get(i)+".bluemix.net/v2/organizations";
  tmp_response = cloudcall.arrayListExecute(${service_account}, null, url, null,
 'GET', null, 'true', CTX);

  for (var j = 0; j < tmp_response.size(); j++){
    all_organizations_response.add('{"result":[' + tmp_response.get(j) + ']}');
  }
}
CTX.setAttribute("all_organizations_response", all_organizations_response);
```

Verwenden Sie die folgende EVAL-Funktion, um Informationen für alle Bereiche abzurufen, die dem IBM Cloud-Konto zugewiesen sind, bei dem die Iteration zum Abrufen der eindeutigen Region durchgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var rtrn = '';
var cloudcall = new CloudRestAPIClient();
var resultList = new Packages.java.util.ArrayList();
var rest = '';
var resourceTable = ${account_region_unique[*].region_name};
var result = new Packages.java.util.ArrayList();
var all_organizations_response = ${all_organizations_response}
for (var i = 0; i < resourceTable.size() ; i++){
   var url = "https://api."+resourceTable.get(i)+".bluemix.net/v2/spaces";
   result = cloudcall.arrayListExecute(${service_account}, null, url, null, 'GET', null,
 'true', CTX);
   for (var z = 0; z < all_organizations_response.size(); z++){
      var jsonObj = JSON.parse(result.get(z));
      ms.log("length "+jsonObj.resources.length);
for(var j=0;j<jsonObj.resources.length;j++){
         var guid = jsonObj.resources[j].metadata.guid;
         var url = jsonObj.resources[j].metadata.url;
         var name = jsonObj.resources[j].entity.name;
         var organization_guid = jsonObj.resources[j].entity.organization_guid;
         var allow_ssh = jsonObj.resources[j].entity.allow_ssh ? "true" : "false";
         var row = new Packages.java.util.HashMap();
 Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug(">>>>>>>>>>>>>>|||||||||||>>>>>> region alias=" +
 resourceTable.get(i));
         Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug(">>>>>>>>>>>>>>|||||||||||>>>>>> region full name=" +
 IbmCloudDcToRegion.regionNamebyAlias(resourceTable.get(i)));
         row.put("region",
 IbmCloudDcToRegion.regionNamebyAlias(resourceTable.get(i)));
         row.put("space_guid",guid);
         row.put("space_url",url);
         row.put("space_name",name);
         row.put("space_organization_guid",organization_guid);
         row.put("space_allow_ssh",allow_ssh);
         row.put("rest", rest);
         resultList.add(row);
      }
   }
   CTX.setAttribute('spaces_table', resultList);
}
```

Verwenden Sie die folgende EVAL-Funktion, um alle Bereiche nach eindeutiger Region zu filtern.

```
var space_region = ${spaces_table[].region};

Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug("filtering space according to LDC. space_region=" + space_region);
var regions = ${cmdb_ci_ibm_datacenter[*].region};
Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug("input regions list=" + regions.toString());

var rtrn = "false";
if(regions.contains(space_region)) {
   rtrn = "true";
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
}
rtrn;
```

Verwenden Sie die folgende EVAL-Funktion, um alle Bereiche nach Speichererkennung zu filtern.

```
var storage_response = ${storage_response};
for (var i = 0; i < storage_response.size(); i++){
     storage_response.set(i, '{"result":[' + storage_response.get(i) + ']}');
}
CTX.setAttribute("storage_response", storage_response);
```

Verwenden Sie die folgende EVAL-Funktion, um die API-Antwort in das vollständige JSON-Format zu konvertieren, da die unberührte Antwort als „[<resource objects>]" formatiert ist.

```
var ssh_key = ${ssh_key_json};
for(var i = 0; i < ssh_key.size(); i++){
   ssh_key.set(i,'{"result\" : ' + ssh_key.get(i) + "}");
}
CTX.setAttribute("ssh_key_json", ssh_key);
```

Verwenden Sie die folgende EVAL-Funktion, um die Verfügbarkeitszone in die Speichervolume-Tabelle einzufügen.

```
var rtrn;
var resource_group = ${network_storage[].resource_name};
var regex = /.*-(\w{3}\d{2}).*/;
var az_name = regex.exec(resource_group);
if (az_name) {
   rtrn = az_name[1];
} else {
   rtrn;
}
```

Verwenden Sie die folgende EVAL-Funktion, um die Region in die Speichervolume-Tabelle einzufügen.

```
var res = "";
res =
 IbmCloudDcToRegion.convertDctoRegion(${network_storage[].availability_zone});
```

Verwenden Sie die folgende EVAL-Funktion, um die Größe der Speicher von Gigabyte in Byte zu konvertieren.

```
var rtrn = '';

var size = ${network_storage[].size};

rtrn = (parseInt(size) * 1073741824) + '';
```

Verwenden Sie die folgende EVAL-Funktion, um die Größe der Speicher von Gigabyte in Byte zu konvertieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var cloudcall = new CloudRestAPIClient();
var resourceTable = ${network_storage[*].storage_object_id};
var tableSize = resourceTable.size();
var allResources = new Packages.java.util.ArrayList();
var response = new Packages.java.util.ArrayList();
for (var i = 0; i < tableSize ; i++){
  if  (!resourceTable.get(i)) continue;
  var url =
 "https://api.softlayer.com/rest/"+${api_version}+"/SoftLayer_Network_Storage/"
+resourceTable.get(i)+"/getObject?objectMask=mask[snapshots]";
  // the commented out code is to call the "Cloud Rest Call" API

  allResources = cloudcall.arrayListExecute(${service_account}, null, url, null,
 'GET', null, 'true', CTX);
  for (var j = 0; j < allResources.size(); j++){
    response.add('{"result":[' + allResources.get(j) + ']}');
  }
}
CTX.setAttribute("all_snapshots_response", response);
```

Verwenden Sie den folgenden EVAL-Abschluss, der die von der API empfangene JSON-Datei in ein Format umwandelt, mit dem der JSON-Parser arbeiten kann. Die Standard-JSON wird unter `$vm_json_array` gespeichert, die neue JSON unter $vm_json.

```
var vm_json = new Packages.java.util.ArrayList();
vm_json.addAll(${vm_json_array});

for (var i = 0 ; i < vm_json.size(); i++){
    vm_json.set(i, '{\"result\":[' + vm_json.get(i) + ']}');
}

CTX.setAttribute("vm_json", vm_json);
```

Verwenden Sie den folgenden EVAL-Abschluss, der „on“ zurückgibt, wenn der Stromversorgungsstatus aktiv ist. Der Wert „off“ wird zurückgegeben, wenn der Stromversorgungsstatus deaktiviert ist.

```
var power = ${cmdb_ci_vm_instance[].state};
var rtrn = '';

if (power == 'Running'){
  rtrn = "on";
}
else {
  rtrn = "off"
}
```

Verwenden Sie den folgenden EVAL-Abschluss, der die Region des CI basierend auf dem angegebenen Verfügbarkeitszonennamen zurückgibt.

```
var az = ${cmdb_ci_vm_instance[].avail_zone};
var rtrn = '';
rtrn = IbmCloudDcToRegion.convertDctoRegion(az);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie den folgenden EVAL-Abschluss, der eine HashMap aus HashSets erstellt und VMs mit ihren Netzwerkspeichern verbindet. Der folgende Schlüssel wird verwendet:

- P = Seite
- V = VM
- N = Netzwerkspeicher

```
var rtrn = '';
var vmJson = ${vm_json_array};
var VMtoStorageHashMap = new Packages.java.util.HashMap();

for (var p = 0 ; p < vmJson.size(); p++){
  var page = JSON.parse(vmJson.get(p));
  for (var now_V in page){
    if (page[v].allowedNetworkStorage.length > 0){
      var vm_id = page[v].id + '';
      var storageSet = new Packages.java.util.HashSet();
      for (var n in page[v].allowedNetworkStorage){
        storageSet.add(page[v].allowedNetworkStorage[n].id + '');
      }
      VMtoStorageHashMap.put(vm_id,storageSet);
    }
  }
}
CTX.setAttribute("VMStorageCache", VMtoStorageHashMap);
```

Verwenden Sie den folgenden EVAL-Abschluss, um doppelte Einträge aus Tabellen zu entfernen.

```
var tableWithoutDuplicates = '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${cmdb_ci_os_template},["object_id"]);
CTX.setAttribute("cmdb_ci_os_template", tableWithoutDuplicates);
```

Verwenden Sie den folgenden EVAL-Abschluss, der eine Liste von VM-IDs erstellt, die sich auf die aktuelle Sicherheitsgruppen-ID beziehen.

```
var rtrn = '';
//get the Security Group ID of the current record in the table for comparison
var current_table_id = ${security_groups[].sec_group_id};
var current_table_id_string = current_table_id + '';

// get the list of instance's ID that will be then added to Security Group table
var needed_value_id_list = ${sec_group_network_components[*].vm_instance_id};
//get the list of Security Group IDs in the Network Component table, which will
 then be compared one by one to the current record of the security_groups table
var compare_id_list = ${sec_group_network_components[*].sec_group_id};

var beforeReturn = '';
var separator = '';
for (var i = 0; i <  compare_id_list.size(); i++)   {

  if   (current_table_id_string == compare_id_list.get(i)){

     beforeReturn += separator + needed_value_id_list.get(i);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    separator = ',';
  }
}
rtrn = beforeReturn;
```

Verwenden Sie den folgenden EVAL-Abschluss, der eine HashMap von HashSets zwischen Sicherheitsgruppen und den VMs erstellt, die für ihre Verwendung konfiguriert sind.

```
rtrn = '';
var secGroupTable = ${cmdb_ci_endpoint_comp_security};
var secToVMHashSet = new Packages.java.util.HashMap();

// this loop worst case O(N*M) M = security groups, N = VMs
for(var i=0; i<secGroupTable.size(); i++){
  var securityTableId = secGroupTable.get(i).get('object_id');
  var vmListStr = secGroupTable.get(i).get('instance_list');
  var vmList = vmListStr.split(",");

  var vmSet = new Packages.java.util.HashSet();
  for (var j in vmList){
    vmSet.add(vmList[j]);
  }

  secToVMHashSet.put(securityTableId,vmSet);
}
CTX.setAttribute("securityVMCache",  secToVMHashSet);
```

Verwenden Sie den folgenden EVAL-Abschluss, der „true“ zurückgibt, wenn die aktuelle VM die aktuelle Sicherheitsgruppen-ID verwendet.

```
var rtrn = '';
var vm_id = ${cmdb_ci_vm_instance[].object_id};
var vmHashSet =
 ${securityVMCache}.get(${cmdb_ci_endpoint_comp_security[].object_id});
rtrn = vmHashSet.contains(vm_id);
```

Verwenden Sie den folgenden EVAL-Abschluss, der „true“ zurückgibt, wenn die aktuelle VM das aktuelle Speichervolume verwendet.

```
var rtrn = '';
var vm_id = ${cmdb_ci_vm_instance[].object_id};
var vol_id = ${cmdb_ci_endpoint_iscsi[].object_id};
var vmHashSet = ${VMStorageCache}.get(vm_id);
if (vmHashSet){
  rtrn = vmHashSet.contains(vol_id);
}
else {
  rtrn = 'false'
}
```

Verwenden Sie die folgende EVAL-Funktion, um die API-Antwort in das vollständige JSON-Format zu konvertieren, da die unberührte Antwort als „[<resource objects>]” formatiert ist.

```
var cloud_response = ${location_groups_response}
for (var i = 0; i < cloud_response.size(); i++){
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    cloud_response.set(l, '{"result":[' + cloud_response.get(i) + ']}');
}
CTX.setAttribute("location_groups_response", cloud_response);
```

Analysiert die eindeutigen Standortgruppen in der Tabelle „location_groups_az“ in der Spalte „lg_id“ und erstellt eine neue Tabelle „location_groups_az_unique“, die das Ergebnis enthält

```
var tableWithoutDuplicates= '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${location_groups_az},["lg_id"]);
CTX.setAttribute("location_groups_az_unique", tableWithoutDuplicates);
```

Erstellt eine Liste von Verfügbarkeitszonen pro Standortgruppe, die in einer neuen Spalte in „llocation_groups_az_uniquetable“ gespeichert ist. Die Listendatensätze sind absichtlich durch Kommas unterteilt, sodass im nachfolgenden Schritt eindeutige Beziehungen hergestellt werden können.

```
var current_table_id= ${location_groups_az_unique[].lg_id};
var current_table_id_string = current_table_id+ '';
var needed_v alue_id_list = ${location_groups_az[*].lg_az_id};
var compare_id_list= ${location_groups_az[*].lg_id};
var beforeReturn= '';
var separator = ',';
for (var i= 0; i< compare_id_list.size(); i++)  {
    if (current_table_id_string == compare_id_list.get(i)){
    beforeReturn += separator + needed_v alue_id_list.get(i) + separator;
  }
}
rtrn = beforeReturn;
```

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Von Discovery während der horizontalen Erkennung erfasste Daten

Daten werden mithilfe der folgenden Muster gesammelt:

- IBM Cloud-Lastenausgleichsmodul
- IBM Cloud-Standortgruppen
- IBM Cloud-Netzwerk
- IBM Cloud-Organisationen und -Bereiche
- IBM Cloud-Ressourcengruppen
- IBM Cloud-SSH-Schlüssel
- IBM Cloud-Speicher
- IBM Cloud virtueller Server

Daten, die für IBM-Komponenten erfasst wurden:

Vom IBM Cloud-Lastenausgleichsmodul erkannte Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_load_balancer	
name	Name des Lastenausgleichmoduls
object_id	Eindeutiger Bezeichner des Lastenausgleichmoduls
fqdn	Lastenausgleichsmoduladresse (Hostname)
dns_name	Domänenservername des Lastenausgleichmoduls
short_description	Beschreibung des Lastenausgleichmoduls, das Sie zur einfachen Identifizierung angeben
operational_status	Status des Lastenausgleichmoduls, einer der folgenden: • ONLINE • OFFLINE
location	Standort des Rechenzentrums
state	Bereitstellungsstatus des Lastenausgleichmoduls
Zugehöriges CI: cmdb_ci_lb_service	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • Ressourcentyp-Listener
object_id	Eindeutiger Bezeichner des Lastenausgleichmoduls
port	Portnummer des Listeners
front_end_port	Protokollportnummer des Listeners
listener_protocol	Protokoll des Listeners Eines der folgenden Protokolle: • TCP • HTTP • HTTPS
operational_status	Bereitstellungsstatus des Listeners
Zugehöriges CI: cmdb_ci_lb_pool	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • port • Ressourcentyp „Pool“
object_id	Eindeutiger Bezeichner des Lastenausgleichmodulpools

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
port	Protokoll-Port des Back-End
pool_status	Pool-Bereitstellungsstatus des Lastenausgleichmoduls
load_balancing_method	Lastenausgleichsmethode. Einer der folgenden Algorithmen: • "ROUNDROBIN" • "WEIGHTED_RR" • "LEASTCONNECTION"
Zugehöriges CI: cmdb_ci_lb_pool_member	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • IP-Adresse des Poolmitglieds
object_id	Eindeutiger Bezeichner des Lastenausgleichmodul-Poolmitglieds, bestehend aus: • Mitglieds-ID • Listener-ID
ip_address	IP-Adresse des Lastenausgleichsmodulmitglieds
server_id	ID des Mitglieds in IBM Cloud
load_balancer	Name des zugehörigen Lastenausgleichmoduls
Zugehöriges CI: cmdb_ci_lb_health_service	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • Ressourcentyp: **Integritätsprüfung** • resource ID
object_id	Eindeutiger Bezeichner der Integritätsdienstprüfung
monitor_type	Integritätsprüfungstyp Eine der folgenden Möglichkeiten: • TCP • HTTP • HTTPS
timeout_sec	Zeit in Sekunden, die auf die Antworten der Integritätsprüfung gewartet wird
check_interval_sec	Intervall in Sekunden zum Ausführen der Integritätsprüfung

Von den IBM Cloud-Standortgruppen erkannte Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_location_group	
name	Ein beschreibender Name zur Identifizierung einer Standortgruppe
object_id	Die ID des Standortgruppen-Datensatzes
locationGroupType Name	Der Name des Standortgruppentyps
short_description	Ein kleiner Hinweis zu einer Standortgruppe, den Sie nach Belieben verwenden können.
locationGroup Type ID	Die ID des Standortgruppentyps

Vom IBM Cloud-Netzwerk erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_network	
name	VLAN-Nummer
object_id	Eindeutiger Netzwerk-Bezeichner
access_port_vlan	VLAN-Nummer
is_external	Netzwerkspeicherplatzwert. Der Wert ist entweder: • „true“, wenn network_space „PUBLIC“ ist • „false“, wenn network_space „PRIVATE“ ist
state	Status hat den Wert „verfügbar“.
Zugehöriges CI: cmdb_ci_cloud_subnet	
name	Name, bestehend aus: „network_identifier/cidr“
object_id	Eindeutiger Subnetz-Bezeichner
subnet_mask	Netzmaske des Subnetzes
gateway	Gateway-IP-Adresse
cidr	Methode für die Zuweisung von IP-Adressen und IP-Routing: „network_identifier/cidr“
Kategorie	Subnetztyp
broadcast_address	Broadcast-Adresse des Subnetzes
available_ip_count	Anzahl der IP-Adressen, die im Subnetz verfügbar sind
Zugehöriges CI: cmdb_ci_compute_security_group	
name	Name der Sicherheitsgruppe
object_id	Eindeutiger Bezeichner der Sicherheitsgruppe
short_description	Beschreibung der Sicherheitsgruppe, die Sie zur einfachen Identifizierung angeben
Zugehörige CI: cmdb_ci_compute_security_group_rule	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
name	Feld mit demselben Wert wie das Feld „object_id“ der Sicherheitsgruppenregel
object_id	Eindeutiger Bezeichner der Sicherheitsgruppenregeln
erstellt	Datum, an dem das CI erstellt wurde
direction	Richtung der Informationen. Eine der folgenden Möglichkeiten: • eingehend • ausgehend
EtherType	EtherType Eine der folgenden Möglichkeiten: • IPv4 • IPv6
port_range_min	Der erste Port des Bereichs, für den die Regel gilt
port_range_max	Der letzte Port des Bereichs, für den die Regel gilt
protocol	Protokoll, auf das die Regel angewendet wird
remote_group_id	Sicherheitsgruppen-ID für die Quell-/Ziel-Sicherheitsgruppe. Dies bedeutet, dass diese Regel für alle IP-Adressen gilt, die in dieser Sicherheitsgruppe konfiguriert wurden.

Von IBM Cloud-Organisationen und -Bereichen erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_org	
name	Name der Cloud-Organisation
guid	Eindeutiger Bezeichner der Organisation
url	Eindeutige URL der Organisation
billing_enabled	Von der Organisation verwendete Abrechnungsmethode. Eine der folgenden: • Aktiviert / (TRUE) • Deaktiviert / (FALSE)
quota_definition_url	Ressourcen, die einer Organisation zur Verfügung stehen
spaces_url	Eindeutige URL des Speicherplatzes, der einer Organisation zugewiesen ist
operational_status	Betriebsstatus der Organisation
Zugehöriges CI: cmdb_ci_cloud_space	
name	Eindeutiger Name des Bereichs
object_id	Eindeutiger Bereichsbezeichner (GUID)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
allow_ssh	Zugriff auf die Anwendung über SSH ist entweder erlaubt oder nicht erlaubt. Boolesch, einer der folgenden Werte: • WAHR • FALSCH
URL	URL des Bereichs aus der Metadatenbeschreibung

Von den IBM Cloud-Ressourcengruppen erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_resource_group	
name	Name der Ressourcengruppe
object_id	Eindeutiger Bezeichner der Ressourcengruppe
quota_id	Wert, der die der Ressourcengruppe zugeordnete Kontingent-ID angibt

Vom IBM Cloud-SSH-Schlüssel erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_key_pair	
name	Name zur Identifizierung eines SSH-Schlüssels
object_id	ID des SSH-Schlüsseldatensatzes
key	SSH-Schlüsseldatensatz
finger_print	Kurze Sequenz von Bytes, die zur Authentifizierung oder zum Nachschlagen eines längeren SSH-Schlüssels verwendet wird. Dieser Wert wird automatisch generiert, wenn der SSH-Schlüssel hinzugefügt oder bearbeitet wird. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
created _date	Datum, an dem der SSH-Schlüssel hinzugefügt wurde. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
modify_date	Datum, an dem der SSH-Schlüssel modifiziert wurde. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
short_description	Beschreibung des SSH, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums
Zugehöriges CI: cmdb_ci_cloud_service_account	
name	Name des Cloud-Servicekontos

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der logischen Rechenzentren (LDCs)
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“

Vom IBM Cloud-Speicher erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_storage_volume	
name	Benutzername für folgende Aktionen: • Zugriff auf ein Nicht-EVault-Speichervolume • Registrierung des EVault-Server-Agent mit dem Vault-Sicherungssystem
object_id	Eindeutiger Bezeichner für Speicherkonto
size	Kapazität des Speicherkontos, gemessen in Gigabyte
size_bytes	Kapazität des Speicherkontos, gemessen in Byte
Bezeichnung	Name der Speichernetzwerkressource
storage_type	Beschreibung des Speichertyps. Beispiel: NAS
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
Gerät	Eindeutige Identifikationsnummer des Geräts, das dem Speichervolume zugeordnet ist
Zugehöriges CI: cmdb_ci_storage_vol_snapshot	
name	Name der Speicher-Netzwerkressource
object_id	Eindeutiger Speicher-Bezeichner
Kapazität	Kapazität des Snapshot-Volume in Gigabyte
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
location	Eindeutige Verfügbarkeitszone, in der sich das Speichervolume befindet
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums
Zugehöriges CI: cmdb_ci_cloud_service_account	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
name	Name des Cloud-Servicekontos
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der LDCs
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“
Zugehöriges CI: cmdb_ci_availability_zone	
name	Name der Verfügbarkeitszone (AZ)
object_id	Eindeutiger Bezeichner für diese Ressource
short_description	Verfügbarkeitszonenbeschreibung, die Sie angeben

Vom IBM Cloud virtuellen Server erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_vm_instance	
name	Name der VM
object_id	Eindeutiger Bezeichner der VM
dns_domain	Name des VM-Domänenservers
fqdn	VM-IP-Adresse
short_description	Beschreibung in einer Notiz, die der VM auf der IBM-Konsole angehängt wird
CPUs	Anzahl der CPU-Kerne, die dieser VM zugewiesen sind
memory	Speichergröße, die dieser VM zugewiesen ist
disks	Anzahl der Datenträger, die dieser VM zugewiesen sind
state	Der Ausführungsstatus der VM. • On – Wird von der API als „ausgeführt“ zurückgegeben • Off – Wird von der API als „angehalten“ zurückgegeben
placement_group_id	Platzierungsgruppen-ID
nics	Anzahl der NICs
Zugehöriges CI: cmdb_ci_nic	
name	Name, bestehend aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Name des Lastenausgleichmoduls • Port
object_id	Eindeutiger Bezeichner der NIC
ip_address	IP, die auf der NIC konfiguriert ist
mac_address	NIC-MAC-Details
netmask	Maske zur Unterteilung der IP-Adresse in Subnetze und zur Angabe der verfügbaren Hosts im Netzwerk
Status	Status der NIC
Zugehörige CI: cmdb_ci_endpoint_vnic	
name	Name für den VNIC-Endpunkt
object_id	Eindeutiger Bezeichner des VNIC-Endpunkts
host	Bezeichner des Hosts
Zugehöriges CI: cmdb_ci_storage_volume	
name	Benutzername für folgende Aktionen: • Zugriff auf ein Nicht-EVault-Speichervolume • Registrierung des EVault-Server-Agent mit dem Vault-Sicherungssystem
object_id	Eindeutiger Bezeichner für Speicherkonto
size	Kapazität des Speicherkontos, gemessen in Gigabyte
size_bytes	Kapazität des Speicherkontos, gemessen in Byte
Bezeichnung	Name der Speichernetzwerkressource
storage_type	Beschreibung des Speichertyps. Beispiel: NAS
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
Gerät	Eindeutige Identifikationsnummer des Gastes, der dem Speichervolume zugeordnet ist
Zugehöriges CI: cmdb_ci_endpoint_nfs	
name	Name für den NFS-Endpunkt
host	Bezeichner des Hosts
protocol	Angewendetes Protokoll
Typ	NFS-Endpunkttyp
erstellt	Datum, an dem der NFS-Endpunkt erstellt wurde
aktualisiert	Datum, an dem der NFS-Endpunkt aktualisiert wurde
discovery_source	Quelle der Erkennung. Beispiel: ServiceWatch
host_name	Hostname des NFS-Endpunkts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugehöriges CI: cmdb_ci_endpoint_iscsi	
host	Host-Bezeichner für den ISCSI-Endpunkt
port	Port, um festzulegen, wie GCP-ISCSI Kontakt zu den VMs herstellt
protocol	Angewendetes Protokoll
Typ	ISCSI-Endpunkttyp
erstellt	Datum, an dem der ISCSI-Endpunkt erstellt wurde
aktualisiert	Datum, an dem der ISCSI-Endpunkt aktualisiert wurde
discovery_source	Quelle der Erkennung. Beispiel: ImportSet
host_name	Hostname des ISCSI-Endpunkts
Zugehörige CI: cmdb_ci_endpoint_block	
name	Name für den Block-Endpunkt
object_id	Eindeutiger Bezeichner des Block-Endpunkts
host	Bezeichner des Hosts
Zugehöriges CI: cmdb_ci_os_template	
name	Name des Image. Zum Beispiel: CentOS 7.0-64 Minimal for VSI
object_id	Eindeutiger Bezeichner des Images
guest_os	Vom Image verwendetes Betriebssystem Beispiel: Linux
root_device_type	Typ des von Root verwendeten Geräts
image_source	Image-Quelle
image_type	Image-Typ
infuse_key	Schlüssel, der zur Eingabe des Image verwendet wird
update_host_name	Update-Hostname für das Image
Anmeldeinformationen	Anmeldeinformationen für das Image
Version	Version des Betriebssystems. Beispiel: „7.0-64 Minimal for VSI“
Zugehöriges CI: cmdb_ci_cloud_key_pair	
name	Name zur Identifizierung eines Schlüssels (Schlüsselbezeichnung)
object_id	ID des Schlüsseldatensatzes
key	Schlüsseldatensatz
finger_print	Kurze Sequenz von Bytes, die zum Authentifizieren oder Nachschlagen eines Schlüssels verwendet wird. Dieser Wert wird automatisch generiert, wenn der Schlüssel hinzugefügt oder bearbeitet wird. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
created _date	Datum, an dem der Schlüssel hinzugefügt wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.

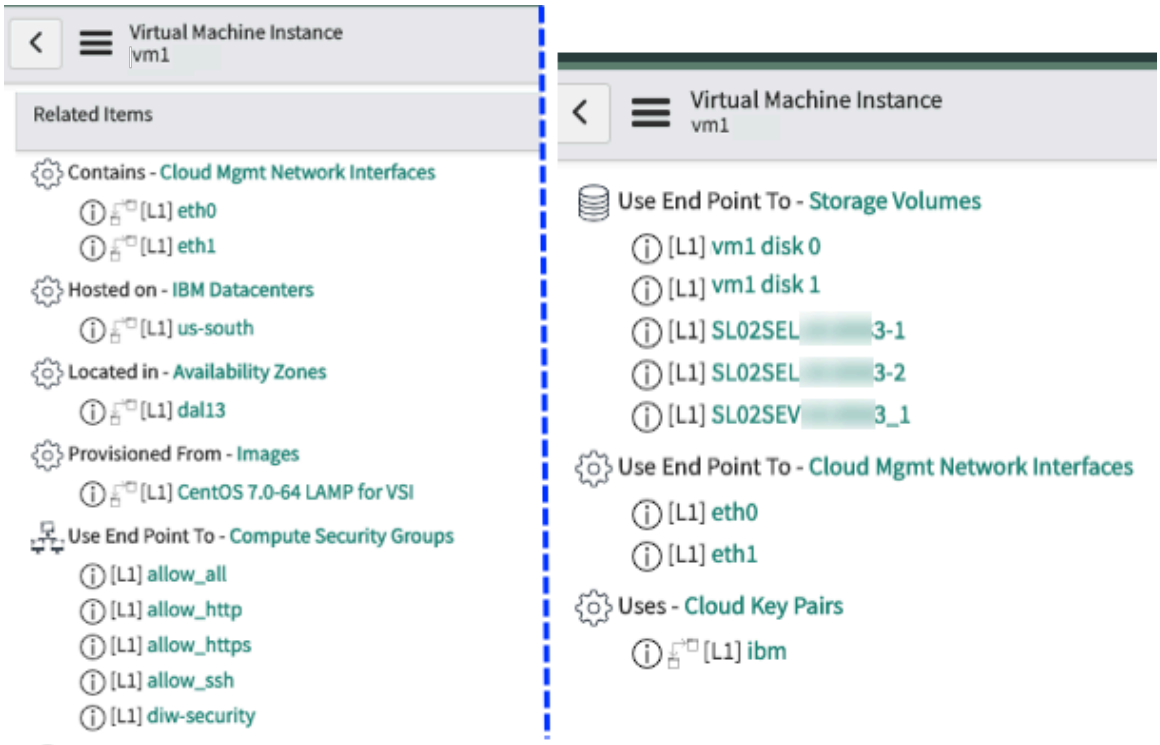
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
modify_date	Datum, an dem der Schlüssel modifiziert wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
short_description	Beschreibung, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_compute_security_group	
name	Name der Sicherheitsgruppe
object_id	Eindeutiger Bezeichner der Sicherheitsgruppe
short_description	Beschreibung der Sicherheitsgruppe, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_endpoint_comp_security	
host	Host-Bezeichner des Sicherheitsendpunkts der Berechnung
port	Eindeutiger Host-Bezeichner des Sicherheitsendpunkts der Berechnung
protocol	Angewendetes Protokoll
Typ	Typ des Sicherheitsendpunkts der Berechnung
erstellt	Datum, an dem der Sicherheitsendpunkt der Berechnung hinzugefügt wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
aktualisiert	Datum, an dem der Sicherheitsendpunkt der Berechnung geändert wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
discovery_source	Quelle der Erkennung. Beispiel: Manuelle Eingabe
host_name	Host-Name des Sicherheitsendpunkts der Berechnung
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums
Zugehöriges CI: cmdb_ci_availability_zone	
name	Name der Verfügbarkeitszone (AZ)
object_id	Eindeutiger Bezeichner für diese Ressource
short_description	Verfügbarkeitszonenbeschreibung, die Sie angeben
Zugehöriges CI: cmdb_ci_cloud_service_account	
name	Name des Cloud-Servicekontos
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der LDCs
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“

IBM Cloud virtueller Server – Ansicht „Zugehörige Elemente“



CI-Beziehungen

Diese Beziehungen sollen die IBM Cloud Plattform-Erkennung unterstützen.

Beziehungen für vom IBM Cloud-Lastenausgleichsmodul erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_cloud_load_balancer		
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_health_service
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_lb_service
Zugehöriges CI: cmdb_ci_lb_service		
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Enthält::Enthalten in	cmdb_ci_lb_pool
Zugehöriges CI: cmdb_ci_lb_pool		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member
Zugehöriges CI: cmdb_ci_lb_health_service		
cmdb_ci_lb_health_service	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen für von den IBM Cloud-Standortgruppen erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehörige CI: cmdb_ci_cloud_location_group		
cmdb_ci_cloud_location_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_location_group	Enthält::Enthalten in	cmdb_ci_availability_zone

Beziehungen für vom IBM Cloud-Netzwerk erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_network		
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
Zugehöriges CI: cmdb_ci_compute_security_group		
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_compute_security_group	Enthält::Enthalten in	cmdb_ci_compute_security_group_rule

Beziehungen für von den IBM Cloud-Ressourcegruppen erkannte Ressourcen

CI	Beziehung	CI
Zugehörige CI: cmdb_ci_resource_group		
cmdb_ci_resource_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen für vom IBM Cloud-SSH-Schlüssel erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_cloud_key_pair		
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Beziehungen für vom IBM Cloud-Speicher erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_storage_volume		
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Bereitgestellt::Bereitgestellt von	cmdb_ci_storage_vol_snapshot
Zugehöriges CI: cmdb_ci_storage_vol_snapshot		
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_vol_snapshot	Positioniert in Zone::Zone beinhaltet	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_storage_volume

Beziehungen für vom IBM Cloud virtuellen Server erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_vm_instance		
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_vm_instance	Standort::Häuser	cmdb_ci_availability_zone
cmdb_ci_vm_instance	Verwendet::Verwendet von	cmdb_ci_cloud_key_pair
cmdb_ci_vm_instance	Enthält::Enthalten in	cmdb_ci_nic
cmdb_ci_vm_instance	endpoint	cmdb_ci_nic

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_nic		
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_os_template		
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_os_template	Bereitgestellt::Bereitgestellt von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_compute_security_group		
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_compute_security_group	Implementieren::Implementiert von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_storage_volume		
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Implementieren::Implementiert von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_cloud_key_pair		
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Für die VM-Instanz erkannte Beziehungen

CI	Beziehung	CI
Server [cmdb_ci_server]	Virtualisiert von::Virtualisiert	VM-Instanz [cmdb_ci_instance]

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter `mid.sa.cloud.request_timeout` gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter `mid.sa.cloud.request_timeout` auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter `sa.debugger.max_timeout` auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Microsoft Azure Cloud-Discovery mithilfe von Mustern

Discovery Verwendet mehrere Muster, um Komponenten von zu erkennen Microsoft Azure Cloud Bereitstellung während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Konfiguration von Cloud-Discovery Für Microsoft Azure

- Verwenden Sie Cloud-Discovery Einzurichtender Arbeitsbereich Cloud-Discovery. Weitere Informationen finden Sie unter Cloud-Discovery Setup mit Cloud Operations Workspace
- Aktivieren Cloud-Discovery Um auf zuzugreifen Azure Umgebung. Weitere Informationen finden Sie unter Azure-Servicekonten einrichten.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen einzubeziehen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von verwendet werden Service-Mapping. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Tag-basierte Discovery-Konfiguration.

Azure-Verfügbarkeitssatz

Warten Sie auf **Bereinigungsauftrag für Verfügbarkeitszone, um den Verfügbarkeitssatz-Datensatz zu löschen** Planen Sie die Aufgabe, um alle Configuration Items (CI) des vorab ausgefüllten Verfügbarkeitssatzes in zu löschen **cmdb_ci_Azure_Availability_Set** Tabelle.

Azure-Verfügbarkeitszone

Um eine Discovery mit der Azure-Verfügbarkeitszone auszuführen, registrieren Sie die Abonnement-ID für **VerfügbarkeitZonePeering** Funktion mit AZ CLI mit `az-Funktionsregister -n AvailabilityZonePeering --Namespace Microsoft.Resources` Dient zur Verwendung der API zum Prüfen von Zonen-Peering. Überprüfen Sie den Status mit `az-Funktion zeigt -n AvailabilityZonePeering --Namespace Microsoft.Resources an` Vor Ausführung der Discovery.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Azure Ressourcen-Discovery nach Rechenzentren

Azure Verfügt über Dutzende von Rechenzentren auf der ganzen Welt. Ihre Ressourcen wie Lastenausgleichsmodule und virtuelle Maschinen befinden sich normalerweise nicht in allen Rechenzentren, sondern nur in einigen davon. Die **Discovery Des Azure-Rechenzentrums** Muster wird vor allen anderen ausgeführt Azure Muster zur Identifizierung der Rechenzentren, die Ressourcen im Zusammenhang mit Ihrem Service-Account („aktiv“) haben, und der Rechenzentren, die nicht über Ihre Ressourcen verfügen („passiv“). Dieses Modell verbessert die Leistung von Azure Discovery. Dieses Ausführungsmodell ist effizienter als das vorherige, bei dem alle Rechenzentren erkannt wurden, unabhängig davon, ob relevante Ressourcen vorhanden sind.

Nachdem Sie die „aktiven“ und „passiven“ Rechenzentren identifiziert haben Discovery Der Zeitplan setzt die Ausführung aller fort Azure Muster nur für die „aktiven“ Rechenzentren, um zu erkennen Azure Cloud-Ressourcen, die Sie haben. Die „passiven“ Rechenzentren werden beim Ausführen des Zeitplans ignoriert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglicherweise bemerken Sie Unterschiede in Azure Discovery-Protokoll, in Discovery-Zeit und in CMDB, Abhängig vom Service-Account und MID-Server Eigenschaftseinstellungen.

Rechenzentren, die bereits vor erkannt wurden Muster für Discovery und Service-MappingVersion 1.15.0, verbleiben in **Azure-Rechenzentren** Tabelle . Das Discovery-Laufzeitverhalten wird jetzt jedoch durch den Wert von bestimmt Die MID-Server Eigenschaft `mid.cloud.discovery.sonar.discover_all_azure_datacenters`.Die Eigenschaft ist auf festgelegt **Falsch** Standardmäßig, um die Discovery-Ausführung auf die „aktiven“ Rechenzentren und nicht auf alle Rechenzentren zu beschränken. Sie können alle Rechenzentren für einen Service-Account erkennen, einschließlich „passiver“, indem Sie die Eigenschaft auf festlegen **Wahr** . Weitere Informationen finden Sie unter: MID-Server-Eigenschaften erstellen

Unterschiede gemäß der Service-Account-Discovery nach der Bereitstellung Muster für Discovery und Service-Mapping Version 1.15.0:

- Für neu erkannten Service-Account:
  - Wenn MID-Server Eigenschaft ist auf festgelegt **Falsch** (Standard), Discovery Erfasst Azure Ressourcen Nur für „aktive“ Rechenzentren. Die **Azure-Rechenzentren** Die Tabelle enthält nur „aktive“ Rechenzentrumsdatensätze für den Service-Account. Das Discovery-Protokoll (Registerkarte „Geräte“) zeigt nur „aktive“ Rechenzentren an.
  - Wenn MID-Server Eigenschaft ist auf festgelegt **Wahr** , Discovery Erfasst Azure Ressourcen Für alle Rechenzentren. Die Azure Die Tabelle „Rechenzentren“ enthält alle Rechenzentrumsdatensätze für den Service-Account. Das Discovery-Protokoll (Registerkarte „Geräte“) zeigt alle Rechenzentren („aktiv“ und „passiv“) an.
- Für einen Service-Account, der vor erkannt wurde Muster für Discovery und Service-Mapping Version 1.15.0:
  - Wenn MID-Server Eigenschaft ist auf festgelegt **Falsch** (Standard), Discovery Erfasst Azure Ressourcen Nur für „aktive“ Rechenzentren. Die **Azure-Rechenzentren** Die Tabelle enthält alle Rechenzentrumsdatensätze für den Service-Account. Das Discovery-Protokoll (Registerkarte „Geräte“) zeigt nur „aktive“ Rechenzentren an .
  - Wenn MID-Server Eigenschaft ist auf festgelegt **Wahr** , Discovery Erfasst Azure Ressourcen Für alle Rechenzentren. Die **Azure-Rechenzentren** Die Tabelle enthält alle Rechenzentrumsdatensätze für den Service-Account. Das Discovery-Protokoll (Registerkarte „Geräte“) zeigt alle Rechenzentren („aktiv“ und „passiv“) an.

Für Verwaltungsgruppen: Azure Cloud-Discovery Erkennt alle Azure Rechenzentren.

Azure Hardwaretyp-Discovery

Die Hardware-Typ-Discovery hat in den letzten Jahren drei Modelländerungen unterzogen. Die 1.15.0 Modell löst aus **Hardwaretyp** Muster und **Virtuelle Maschine** Muster nach **Discovery Des Azure-Rechenzentrums** Muster. Wird Gestartet Muster für Discovery und Service-MappingPlugin-Version 1.15.0, Cloud-Discovery Gibt an, welches Hardwaretypmodell verwendet wird, und startet nur eines der beiden Muster: **Hardwaretyp (LP)** Oder **Cloud-Hardwaretyp (LP)** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Migration zum neuen Azure Hardwaretyp-Discovery-Modell: Anwendungsfälle

Muster für Discovery und Service-Mapping Version	Migrationsstatus des Hardwaretyps	Welches Muster ausgeführt wird S	Discovery-Ergebnis
Vor 1.0.75	Wurden nicht zum neuen Modell migriert	**Hardwaretyp (LP)** Muster	Der erstellte CI-Typ: [cmdb_ci_Compute_template]
Muster für Discovery und Service-Mapping Version 1.0.75	Die Migration zum neuen Modell erfolgt über das Migrationsskript. Siehe KB0955939	**Hardwaretyp (LP)** Muster	Der erstellte CI-Typ: [cmdb_ci_Cloud_Hardware_type]
Muster für Discovery und Service-Mapping Version 1.6.0	Das neue Modell des Hardwaretyps wird OOB bereitgestellt, aktiviert mit der Systemeigenschaft: *sn_itom_pattern.use a single hardware type for cloud datacenters*. Weitere Informationen finden Sie unter KB1285337 .	Gemäß KB1285337 Flow-Diagramm	Der erstellte CI-Typ: Gemäß KB1285337
Muster für Discovery und Service-Mapping 1.15.0	Das neue Modell des Hardwaretyps wird OOB bereitgestellt, das mit der Systemeigenschaft aktiviert ist: *sn_itom_pattern.use a single hardware type for cloud datacenters*. Weitere Informationen finden Sie unter KB1285337 .	Der Flow ist wie in beschrieben KB1285337 . Es wird jedoch nur ein Muster ausgeführt. Das Muster, das zum ordnungsgemäßen Beenden verwendet wurde, wird nicht ausgeführt.	Entweder **Hardwaretyp (LP)** Muster oder **Cloud-Hardwaretyp (LP)** Musterausführung S .

Azure SQL Managed Instance License Discovery

Die Azure Datenbankmustererweiterung (LP) **Azure SQL Managed Instance-Lizenz** Erkennt Azure Lizenzinformationen für SQL Managed Instance und füllt den Lizenztyp in der Tabelle „Schlüsselwert“ [cmdb_key_value] des Cloud-Datenbank-CI [cmdb_ci_Cloud_database] aus.

Erforderliche Plugins und Anwendungen

- Software Asset Management Professional Für Microsoft
- Visibility Content

Erkannte Ressourcen und Beziehungen

Mithilfe von erkannte Ressourcen Azure Datenbankmustererweiterung (LP): Azure SQL Managed Instance-Lizenz

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit erkannte Beziehungen Azure Datenbankmustererweiterung (LP): Azure SQL Managed Instance-Lizenz

Azure Marktplatz-Discovery

Das Muster Azure – Marketplace LB (LP) erkennt Folgendes Azure Marktplatzprodukte:

- SaaS
- Azure-Anwendung
- Virtuelle Maschine

Hinweis: Das Muster erkennt nur virtuelle Computer (VMs), die aus Images von Drittparteien oder gewerblichen Marktplätzen erstellt wurden.

Erkannte Ressourcen und Beziehungen

Vom Muster Azure – Marketplace LB (LP) erkannte Ressourcen

Beziehungen, die mithilfe des Musters Azure – Marketplace LB (LP) erkannt wurden

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Microsoft Azure - Application LB (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Lastenausgleichsmodul kein Name angegeben ist
location	Pfad des Lastenausgleichsmoduls
state	Aktueller Status des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
ip_address	IP-Adresse des Lastenausgleichsmodul.
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
dns_name	Der DNS-Name des Lastenausgleichmoduls
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
IP-Adresse des Cloud-Lastenausgleichsmoduls [cmdb_ci_cloud_lb_ipaddress]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
lb_id	Ein eindeutiger Bezeichner für den Lastenausgleichsmodul.
ip_address	IP-Adresse des Lastenausgleichsmoduls
ip_address_type	Der Typ der IP-Adresse, die privat oder öffentlich sein kann.
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)
install_status	Bereitstellungsstatus der Ressource

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Load Balancer-Pool [cmdb_ci_lb_pool]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Pool des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Pools des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Load Balancer-Service [cmdb_ci_lb_service]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Service des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Services des Lastenausgleichsmoduls
port	TCP-Port, den der Service des Lastenausgleichsmoduls abhört
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Classic LB (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Lastenausgleichsmodul kein Name angegeben ist
location	Pfad des Lastenausgleichsmoduls
state	Aktueller Status des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
IP-Adresse des Cloud-Lastenausgleichsmoduls [cmdb_ci_cloud_lb_ipaddress]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
lb_id	Ein eindeutiger Bezeichner für den Lastenausgleichsmodul.
ip_address	IP-Adresse des Lastenausgleichsmoduls
ip_address_type	Typ der IP-Adresse, kann privat oder öffentlich sein
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
install_status	Bereitstellungsstatus der Ressource
Load Balancer-Service [cmdb_ci_lb_service]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Service des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Services des Lastenausgleichsmoduls
port	TCP-Port, den der Service des Lastenausgleichsmoduls abhört
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Load Balancer-Pool [cmdb_ci_lb_pool]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Pool des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Pools des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Hardware Type (LP)“ erkannt wurden

Feld	Beschreibung
Hardwaretyp [cmdb_ci_Hardware_type]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Hardwaretyp kein Name angegeben ist
local_storage_gb	Speicher, der dieser Vorlage zugewiesen ist
cores	Die Standardanzahl der Kerne für den Instanztyp
memory_mb	Speichergröße, die dieser Vorlage zugewiesen ist
vcpus	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne

Ressourcen, die mithilfe des Musters „Microsoft Azure - Host (LP)“ erkannt wurden

Feld	Beschreibung
Host [cmdb_ci_cloud_host]	
name	Name oder ID, wenn für den Host kein Name angegeben ist
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
host_type	Typ des Hosts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
cloud_vendor	Anbieter der Cloud: Microsoft Azure
virtual	Virtueller Host: False

Ressourcen, die mithilfe des Musters „Microsoft Azure - Image (LP)“ erkannt wurden

Feld	Beschreibung
Image-Tabelle [cmdb_ci_os_template]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Image kein Name angegeben ist
location	Pfad des Image
guest_os	Betriebssystem, das sekundär zum Betriebssystem ist
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
image_source	Quelle des Betriebssystem-Image

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Ressourcen, die mithilfe des Musters „Microsoft Azure - Network and Subnet (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Netzwerk [cmdb_ci_network]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Cloud-Netzwerk kein Name angegeben ist
location	Pfad des Netzwerks
state	Aktueller Status des Netzwerks
install_status	Bereitstellungsstatus der Ressource
cidr	CIDR-Darstellung des Netzwerks Beispiel: 10.0.0.0/24
Cloud-Subnetz [cmdb_ci_cloud_subnet]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Cloud-Subnetz kein Name angegeben ist
location	Bezeichner zur internen Verwendung (Löschungsstrategie)
state	Der aktuelle Status des Subnetzes.
install_status	Bereitstellungsstatus der Ressource
cidr	CIDR-Darstellung des Subnetzes. Beispiel: 10.0.0.0/24

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen, die mithilfe des Musters „Microsoft Azure - NIC (LP)“ erkannt wurden

Feld	Beschreibung
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
location	Pfad der Netzwerkschnittstelle
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status der Netzwerkschnittstelle
public_ip	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist
private_ip	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
Primär	True/False. Definiert, ob die Netzwerkschnittstelle die primäre Netzwerkschnittstelle ist oder nicht
mac_address	MAC-Adresse der Netzwerkschnittstelle
public_dns	Öffentlicher DNS-Name der Netzwerkschnittstelle

Ressourcen, die mithilfe des Musters „Microsoft Azure - Private Gateway (LP)“ erkannt wurden

Feld	Beschreibung
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das private Gateway kein Name angegeben ist
location	Pfad des privaten Gateway
connection_type	Typ der vom Gateway unterstützten VPN-Verbindung
operational_status	Status der Ressource
install_status	Bereitstellungsstatus der Ressource
Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts
connection_type	Typ der vom Gateway unterstützten VPN-Verbindung

Ressourcen, die mithilfe des Musters „Microsoft Azure - Public IP (LP)“ erkannt wurden

Feld	Beschreibung
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die IP-Adresse kein Name angegeben ist
location	Pfad der IP-Adresse
state	Aktueller Status der IP-Adresse
public_ip_address	Adresse der Elastic IP-Adresse
public_dns	Öffentlicher DNS-Name
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - Resource Group (LP)“ erkannt wurden

Feld	Beschreibung
Ressourcengruppe [cmdb_ci_resource_group]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die Ressourcengruppe kein Name angegeben ist
location	Pfad der Ressourcengruppe
state	Aktueller Status der Ressourcengruppe
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - Route Table (LP)“ erkannt wurden

Feld	Beschreibung
Weiterleitungstabelle [cmdb_ci_route_table]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist
location	Pfad der Weiterleitungstabelle
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status der Weiterleitungstabelle

Ressourcen, die mithilfe des Musters „Microsoft Azure - Security Group (LP)“ erkannt wurden

Feld	Beschreibung
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die Sicherheitsgruppe kein Name angegeben ist
location	Pfad der Sicherheitsgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
state	Aktueller Status der Sicherheitsgruppe
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - SQL Server (LP)“ erkannt wurden

Feld	Beschreibung
VM-Instanz [cmdb_ci_vm_instance]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
location	Pfad der VM-Instanz

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Account (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Speicherkonto [cmdb_ci_cloud_storage_account]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Speicherkonto kein Name angegeben ist
location	Pfad des Speicherkontos
sku_name	Name der SKU (für Sicherungshäufigkeit)
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status des Speicherkontos

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Containers (LP)“ erkannt wurden

Feld	Beschreibung
Speichervolume [cmdb_ci_storage_volume]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist
location	Pfad des Speichervolume
volume_id	Bezeichner, der die Volume-ID als Wert enthält
volume_container	Name des Containers
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Status	Status der Ressource
Block-Endpunkt [cmdb_ci_endpoint_block]	
name	Name oder ID, wenn für den Block-Endpunkt kein Name angegeben ist
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Volume (LP)“ erkannt wurden

Feld	Beschreibung
Speichervolume [cmdb_ci_storage_volume]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist
volume_id	Der Volumetyp. Beispiel: • `gp2` für Allzweck-SSD • `io1` für bereitgestellte IOPS-SSD • `st1` für durchsatzoptimierte HDD • `sc1` für Cold-HDD • `standard` für magnetische Volumes
location	Pfad des Speichervolume
state	Aktueller Status des Speichervolume
install_status	Bereitstellungsstatus der Ressource
size	Größe des Volume
size_bytes	Die Größe des Volumes (Byte)
storage_type	Beispiel: Hartcodierter Wert „Block“.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Sub Account (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
account_id	Der eindeutige Bezeichner (ID) des Kontos
name	Name oder ID, wenn für das Servicekonto kein Name angegeben ist
datacenter_type	cmdb_ci_azure_datacenter
discovery_credentials	Referenzfeld zu den zugehörigen Microsoft Azure-Anmeldeinformationen.
datacenter_url	URL des Rechenzentrums
parent_account	Verweis auf das Primärkonto, falls vorhanden
is_master_account	Boolesches Attribut, das angibt, ob es sich hierbei um das Primärkonto handelt oder nicht

Ressourcen, die mithilfe des Musters „Microsoft Azure - Virtual Machine (LP)“ erkannt wurden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
VM-Instanz [cmdb_ci_vm_instance]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für die Instanz kein Name angegeben ist
location	Pfad der Instanz
install_status	Bereitstellungsstatus der Ressource
state	Der aktuelle Status der Instanz
vm_inst_id	Die ID der Instanz
nics	Anzahl der für die Instanz verfügbaren NICs
disks	Anzahl der Datenträger, die an die Instanz angeschlossen sind
disks_size	Gesamtgröße der angehängten Datenträger
memory	Für die Instanz verfügbare Arbeitsspeicher (MBs)
CPUs	Anzahl der für die Instanz verfügbaren CPUs
Block-Endpunkt [cmdb_ci_endpoint_block]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts
host	Die öffentliche IPv4-Adresse, die der Instanz zugewiesen wurde, falls zutreffend
Speichervolume [cmdb_ci_storage_volume]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist
location	Pfad des Speichervolume
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
location	Pfad der Netzwerkschnittstelle
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	
object_id	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts

Der Abschnitt „Mustererweiterung“ erkennt Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows VMs und Red hat Enterprise Linux (RHEL) VMs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Windows VM mit einem anwenderdefinierten Image, Discovery Füllen Sie Schlüsselwerte nur aus, wenn die Details des primären BS-Datenträgers verfügbar sind.
- Für RHEL-VMs werden Informationen nur für VMs ausgefüllt, die Marketplace-Images verwenden.

Feld	Beschreibung
Schlüsselwert [cmdb_key_value]	
Schlüssel [key]	Der Schlüssel ist eine der folgenden Optionen: • Windows_OS_License_Type_Automatic • RHEL_OS_License_Type_Automatic • SQL_Server_License_Type_Automatic
Wert [value]	Der Wert ist eine der folgenden Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *`Virtual Machine Instance`*.

Von erkannte Ressourcen Microsoft Azure Website-Muster (LP) und Microsoft Azure Websitemuster

Feld	Beschreibung
Cloud-Ressource [cmdb_ci_Cloud_Webserver]	
Name[Name]	Der Name des Azure Webserver.
Objekt-ID [object_id]	Die ID von Azure Webserver.
IP-Adresse [ip_address]	Die IP-Adresse des Webservers.
FQDN [fqdn]	Der vollqualifizierte Domänenname (FQDN) des Webservers.
Anbieter [vendor]	Der Lieferant ist Microsoft.
Installationsstatus [install_status]	Der Installationsstatus des Webservers.
Status [state]	Der Betriebsstatus des Webservers.
Betriebsstatus [operational_status]	Der Betriebsstatus des Webservers.
IP-Adresse [cmdb_ci_ip_address]	
Name [name]	Die IP-Adresse des Webservers.
IP-Adresse [ip_address]	Die IP-Adresse des Webservers.
FQDN [fqdn]	Der vollqualifizierte Domänenname (FQDN).
Anbieter [vendor]	Der Lieferant ist Microsoft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Installationsstatus [install_status]	Der Installationsstatus.
Betriebsstatus [operational_status]	Der Betriebsstatus.
Schlüsselwert [cmdb_key_value]	
Schlüssel [key]	Die Azure Schlüsselwertname.
Wert [value]	Die Azure Schlüsselwertwert.

Mithilfe von erkannte Ressourcen Azure Datenbankmuster (LP)

Cloud-Datenbank [cmdb_ci_cloud_database]

Feld	Beschreibung
Vollständig qualifizierter Domänenname [fqdn]	Der FQDN, den Microsoft Azure Ihrer Datenbank zugewiesen hat.
Name [name]	Der Name der Datenbank, die Sie in Microsoft Azure erstellt haben.
Objekt-ID [object_id]	Der Identifizierungsname der Datenbank.
Betriebsstatus [operational_status]	Der Betriebsstatus der Datenbank.
Typ [type]	Der Typ der von Ihnen erstellten Datenbank.
Status [state]	Der Status der Datenbank: Ob sie verfügbar oder beendet ist.
Anbieter [vendor]	Der Lieferantenname lautet Azure.
Version [version]	Die Version der Datenbank.
Kategorie [category]	Die SKU-Familie (Stock Keeping Unit).

Cloud-Hardwaretyp [cmdb_ci_Cloud_Hardware_type]

Feld	Beschreibung
Objekt-ID [object_id]	Ein eindeutiger Bezeichner für den Hardwaretyp.
Name [name]	Name für den Hardwaretyp.
VCPUs [vcpus]	Anzahl der virtuellen CPU-Kerne.
Anbieter [Provider]	Anbieter für den Hardwaretyp: Azure.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
Netzmaske [netmask]	Netzmaske von Azure Datenbank.

Mithilfe von erkannte Ressourcen Azure Datenbankmustererweiterung (LP): Azure SQL Managed Instance-Lizenz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	SQL_Server_PaaS_Managed_Instance_License_Type_Automatic
Wert [value]	Lizenztyp. Die folgenden ordnen zu Azure Portallizenz für ServiceNow Werte: • **Azure-Hybrid-Vorteil** : BYOL • **Pay-as-you-go** : Lizenz Enthalten • **Hybrid Failover-Rechte** : Hybrid-Failover
Konfigurationselement [configuration_item]	cmdb_ci_cloud_database

Serverlose Hardware [cmdb_ci_serverless_Hardware]

Feld	Beschreibung
Objekt-ID [object_id]	Objekt-ID von Azure Cloud-Datenbank.
Name [name]	SKU-Name.
Cloud-Anbieter [cloud_vendor]	Cloud-Lieferant der serverlosen Hardware: MS Azure.
Anzahl der CPU-Kerne [cpu_Core_count]	Anzahl der virtuellen Kerne (vCores).
CPU-Core-Thread [cpu_Core_Thread]	Anzahl der vCores.
CPU-Anzahl [cpu_count]	Anzahl der vCores.
Kategorie [category]	Vcore-Kaufmodell.
Unterkategorie [Unterkategorie]	SKU-Stufe.
Hosttyp [host_type]	Hosttyp: PaaS.

Vom Muster Azure – Marketplace LB (LP) erkannte Ressourcen

Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]

Feld	Beschreibung
Name [name]	Name der Cloud-Ressource, normalerweise das Marktplatzangebot oder der SKU-Name.
Objekt-ID [object_id]	Eine eindeutige Ressourcen-ID der Cloud-Ressource.
Ressourcentyp [resource_type]	Service in Cloud Marketplace. Beispiel: microsoft.compute/virtualmachines.
Planname [Plan_Name]	Abrechnungs- oder SKU-Plan für eine Ressource aus dem Cloud Marketplace. Beispiel: Pay as you go.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product] (Fortsetzung)

Feld	Beschreibung
Markt [Markt]	ISO-Code (International Organization for Standardization) des geografischen Marktes, auf dem die Ressource im angegebenen Markt verkauft wird. Beispiel: US oder EU.
Organisations-ID [Organization_ID]	Ein eindeutiger Bezeichner für die Organisation oder den Herausgeber, die die Marktplatzressource besitzt.

Marktplatz-Produktdetails [Marketplace_Product_Details]

Feld	Beschreibung
Produktcode [Product_Code]	Ein eindeutiger Produktcode der Ressource im Cloud Marketplace.
Herausgebername [Publisher_Name]	Organisation oder Person, die für die Erstellung und das Angebot des Produkts oder Service verantwortlich ist.
Version [version]	Release-Nummer oder Iteration des Produkts.
Bereitgestellt am [deploy_on]	Verweist auf die Tabelle „bereitgestelltes Marktplatzprodukt“ [cmdb_ci_deploy_Marketplace_Product].

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Azure Schlüsselwertname.
Wert [value]	Azure Schlüsselwertwert.

Von der Mustererweiterung Azure – Unterkonto (LP) erkannte Ressourcen: Azure-Verwaltungsgruppen

Cloud-Organisationen [cmdb_ci_Cloud_org]

Feld	Beschreibung
Name [name]	Mandanten-ID oder Name. • Mandanten-ID: Bei Verwendung von Anmeldeinformationen auf Verwaltungsebene • Mandantenname: Bei Verwendung von Anmeldeinformationen auf Mandantenebene
Objekt-ID [object_id]	Mandanten-ID.
DNS-Domäne [dns_Domain]	Bei der Registrierung eingegebener Domänenname. Beispiel: `servicenow.com` . Dieses Feld wird nur ausgefüllt, wenn Anmeldeinformationen auf Mandantenebene verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]

Feld	Beschreibung
Name [name]	Name der Verwaltungsgruppe.
Objekt-ID [object_id]	Verwaltungsgruppenname und Mandanten-ID im folgenden Format: `Name +@+TenantId` . Beispiel: `ItomMgmtGroup@8bcff-vdc-btrv` .
Übergeordnet [parent]	Verweist auf die direkt übergeordnete Tabelle „Azure-Verwaltungsgruppe“ [cmdb_ci_Azure_Management_Group].

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Microsoft Azure - Application LB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Eigentümer von::Eigentum von	cmdb_ci_cloud_lb_ipaddress
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_cloud_subnet	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen, die mithilfe des Musters „Microsoft Azure - Classic LB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Eigentümer von::Eigentum von	cmdb_ci_cloud_lb_ipaddress
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_lb_service
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen, die mithilfe des Musters „Microsoft Azure - Hardware Type (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Host (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_cloud_host	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_host
cmdb_ci_vm_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_cloud_host

Beziehungen, die mithilfe des Musters „Microsoft Azure - Image (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_os_template

Beziehungen, die mithilfe des Musters „Microsoft Azure - Network and Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_network

Beziehungen, die mithilfe des Musters „Microsoft Azure - NIC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_nic
cmdb_ci_cloud_subnet	Enthält::Enthalten in	cmdb_ci_nic

Beziehungen, die mithilfe des Musters „Microsoft Azure - Private Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_endpoint_vpg	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_virtual_pvt_gateway
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_virtual_pvt_gateway
cmdb_ci_virtual_pvt_gateway	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_network	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vpg

Beziehungen, die mithilfe des Musters „Microsoft Azure - Public IP (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_public_ipaddress	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_nic	Enthält::Enthalten in	cmdb_ci_cloud_public_ipaddress
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_public_ipaddress

Beziehungen, die mithilfe des Musters „Microsoft Azure - Resoure Group (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_resource_group

Beziehungen, die mithilfe des Musters „Microsoft Azure - Route Table (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_route_table	Enthält::Enthalten in	cmdb_ci_route
cmdb_ci_route_table	Enthält::Enthalten in	cmdb_ci_network
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_route_table
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_route_table

Beziehungen, die mithilfe des Musters „Microsoft Azure - Security Group (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_subnet	Verwendet::Verwendet von	cmdb_ci_compute_security_group
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_compute_security_group
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_compute_security_group
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Account (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_storage_account
cmdb_ci_cloud_storage_account	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Containers (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume
cmdb_ci_cloud_storage_account	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Volume (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Sub Account (LP)“ erkannt wurden

Mit dem Muster „Microsoft Azure - Sub Account (LP)“ werden keine Beziehungen erkannt.

Beziehungen, die mithilfe des Musters „Microsoft Azure - Virtual Machine (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vnic
cmdb_ci_endpoint_vnic	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_nic
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_vm_instance
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_block
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_Availability_Set	Enthält::Enthalten in	cmdb_ci_vm_instance

Mit erkannte Beziehungen Microsoft Azure Website (LP) und Microsoft Azure Website-Muster

CI	Beziehung	CI
cmdb_ci_cloud_webserver	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_cloud_webserver	Besitzt::Im Besitz	cmdb_ci_ip_address
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_webserver

Mit erkannte Beziehungen Azure Datenbankmuster (LP).

CI	Beziehung	CI
cmdb_ci_cloud_database	Besitzt:Im Besitz Von	cmdb_ci_ip_address
cmdb_ci_cloud_database	Enthält::Enthalten in	cmdb_ci_database
cmdb_ci_cloud_database	Gehostet Auf::Hosted	cmdb_ci_azure_datacenter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_database	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_database	Bereitgestellt von::Bereitgestellt	cmdb_ci_Cloud_Hardware_type
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_Cloud_Hardware_type

Mit erkannte Beziehungen Azure Datenbankmustererweiterung (LP): Azure SQL Managed Instance-Lizenz

CI	Beziehung	CI
cmdb_ci_cloud_database	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_serverless_Hardware
cmdb_ci_serverless_Hardware	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_database

Beziehungen, die mithilfe des Musters Azure – Marketplace LB (LP) erkannt wurden

CI	Beziehung	CI
Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]	Erstreckt sich von	VM-Objekt [cmdb_ci_vm_object]
Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]	Gehostet auf::Hostet	Cloud-Service-Account [cmdb_ci_Cloud_sevice_Account]
Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Marktplatz-Produktdetails [Marketplace_Product_Details]	Referenzen	Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Bereitgestelltes Marktplatzprodukt [cmdb_ci_deploy_Marketplace_Product]

Beziehungen, die mit der Mustererweiterung Azure – Unterkonto (LP) erkannt wurden: Azure-Verwaltungsgruppen

CI	Beziehung	CI
Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]	Enthält::Enthalten in	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Cloud-Organisationen [cmdb_ci_Cloud_org]	Enthält::Enthalten in	Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]
Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]	Enthält::Enthalten in	Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]
* Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]	Referenzen	Azure-Verwaltungsgruppe [cmdb_ci_Azure_Management_Group]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

* Verweist nur auf die direkte über- und untergeordnete Verwaltungsgruppenbeziehung.

Events, die während der horizontalen Erkennung mithilfe von Discovery erkannt wurden

Discovery verwendet Muster, um Events zu suchen, die für Microsoft Azure-Komponenten erstellt wurden. Wenn Events vorhanden sind, die auf eine Statusänderung in einer der Microsoft Azure-Komponenten hinweisen, wird die Erkennung von Microsoft Azure-Komponenten anhand der Muster ausgelöst.

Muster, die für die Event-Erkennung verwendet wurden

Muster	CI-Klasse
Azure Application LB Event	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Azure Availability Set Event	Verfügbarkeitssatz [cmdb_ci_Availability_Set]
Azure Classic LB-Ereignis	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Azure-Datenbankereignis	Cloud-Datenbank [cmdb_ci_cloud_database]
Azure Express-Routenkreisereignis	Cloud Direct Connect [cmdb_ci_Cloud_direct_Connect]
Azure-Funktionsereignis	Cloud-Funktion [cmdb_ci_cloud_function]
Azure – Gateway-Ereignis Für Lokales Netzwerk	Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]
Azure-NAT-Gateway-Ereignis	NAT-Gateway [cmdb_ci_nat_gateway]
Azure-Netzwerkereignis	Cloud-Netzwerk [cmdb_ci_network]
Azure NIC Event	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]
Ereignis der privaten Azure-DNS-Zone	DNS-Zone [cmdb_ci_dns_Zone]
Azure Public IP Event	Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]
Azure Resource Group Event	Ressourcengruppe [cmdb_ci_resource_group]
Azure Security Group Event	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Azure-Speicher-Account-Ereignis	Cloud-Speicherkonto [cmdb_ci_cloud_storage_account]
Azure-Vm-Ereignis	VM-Instanz [cmdb_ci_vm_instance]
Azure Virtual Network Gateway-Verbindungsereignis	Gateway-Verbindung für virtuelles Netzwerk [cmdb_ci_vpc_Gateway_connection]
Peerings-Ereignis Des Virtuellen Azure-Netzwerks	Peering für virtuelles Netzwerk [cmdb_ci_vnet_Peering]
Azure VM-Skalierungssatz-Ereignis	Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

Von Discovery während der horizontalen Erkennung erfasste Tag-Informationen

Beim Ausführen der Muster werden Tag-Informationen erfasst, um die Tabelle „cmdb_key_value“ zu füllen. Jedes Tag bezieht sich auf ein CI, das während der Erkennung erkannt wurde. Die Tag-Erkennung erfolgt im Erweiterungsabschnitt jedes Musters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping Verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Azure App-Konfiguration – Musterbasierte Discovery im Store

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Die Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – App Configuration Store – Extended Inventory (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-App-Konfiguration – Konfigurationsspeicher [cmdb_Azure_App_Configuration_Store]

Feld	Beschreibung
Authentifizierungsmodus [authentication_Mode]	Die Methode oder Strategie für die Authentifizierung des Zugriffs.
Lokale Authentifizierung deaktivieren [disable_local_auth]	Gibt an, ob lokale Authentifizierungsmethoden deaktiviert sind.
Löschschutz aktivieren [enable_purge_Protection]	Gibt an, ob der Löschschutz für die Ressource aktiviert ist.
Endpunkt [Endpunkt]	Der URL-Endpunkt, über den auf den Service zugegriffen wird.
Key Vault-Eigenschaften [key_Vault_properties]	Eigenschaften im Zusammenhang mit der Konfiguration von Key Vault-Services.
Standort [location]	Die Azure Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Delegierung von privatem Link [private_Link_delegation]	Konfigurationen im Zusammenhang mit der Delegierung privater Links.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Status des Ressourcenbereitstellungsprozesses.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
SKU-Name [sku_name]	Die Lagerhaltungseinheit (Stock Keeping Unit, SKU), die die Preisstufe der Ressource darstellt.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner von Azure Active Directory-Mandant.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Die Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – App Configuration Store – Extended Inventory (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die Azure Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource] (Fortsetzung)

Feld	Beschreibung
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.appConfiguration/ConfigurationStores** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-App-Konfiguration – Konfigurationsspeicher [cmdb_Azure_App_Configuration_Store]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery für App-Service-App-Serviceplan

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Anwendung – Daten ausfüllen in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – App-Service-App-Serviceplan – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure App-Service – App-Serviceplan [cmdb_Azure_App_Service_App_Service_Plan]

Feld	Beschreibung
Art [Art]	Die Kategorie oder Spezialisierung der Ressource, häufig spezifisch für bestimmte Azure Services.
Standort [location]	Die Azure Region, in der die Ressource gehostet wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Status [status]	Der Betriebsstatus oder die Integrität der Ressource.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner des Azure Active Directory-Mandant, der der Ressource zugeordnet ist.
Stufe [Stufe]	Die der Ressource zugewiesene Leistungs- oder Preisstufe.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-App-Server“ [cmdb_ci_Cloud_appserver].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – App-Service-App-Serviceplan – Erweiterter Bestand (LP)“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-App-Server [cmdb_ci_Cloud_appserver]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die Azure Region, in der die Ressource gehostet wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Typ [type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.Web/Serverfarmen** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-App-Server [cmdb_ci_Cloud_appserver]
Cloud-App-Server [cmdb_ci_Cloud_appserver]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure App-Service – App-Serviceplan [cmdb_Azure_App_Service_App_Service_Plan]	Referenzen	Cloud-App-Server [cmdb_ci_Cloud_appserver]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Microsoft Azure Anwendungs-Gateway-Discovery mit Mustern

Die ServiceNow Discovery-Anwendung verwendet das Azure Application Gateway HD-Muster für die Erkennung dieses Produkts, während die Service-Mapping-Anwendung das Application Gateway mithilfe des Azure Application Gateway TD-Musters (LBS) erkennt. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure-Prinzipal-Anmeldeinformationen

Erstellen Sie auf der ServiceNow Platform ein Servicekonto für die Cloud-Erkennung. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.

Berechtigungen

Weisen Sie in der Microsoft Azure-Konsole einem Benutzer die Leserrolle zu.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
name	Name des Azure Application Gateway
Fqdn	Vollqualifizierter Domänenname des Azure Application Gateway
Object_id	Die ID des Gateways
Install_status	Installationsstatus des Azure Application Gateway
state	Status des Azure Application Gateway
Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]	
name	IP-Adresse des Azure Application Gateway
Object_id	ID des Azure Application Gateway
ipaddress _type	Typ der IP-Adresse, kann privat oder öffentlich sein
ip_address	IP-Adresse des Azure Application Gateway
state	Status der IP-Adresse des Azure Application Gateway
operational_state	Betriebsstatus der IP-Adresse des Azure Application Gateway
install_status	Installationsstatus der IP-Adresse des Azure Application Gateway
Load Balancer-Service [cmdb_ci_lb_service]	
Seriennummer	ID des Azure Application Gateway-Service
port	TCP-Port, den der Azure Application Gateway-Service abhört
name	FQDN mit der Portnummer des Azure Application Gateway-Service gemäß dieser Syntax: <fqdn>:<port>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Zusätzliche Informationen
ip_address	IP-Adresse des Azure Application Gateway, auf dem der Service ausgeführt wird
object_id	ID des Azure Application Gateway-Service
operational_state	Betriebsstatus des Azure Application Gateway-Service

CI-Beziehungen

Diese Beziehungen sollen die Azure Application Gateway-Erkennung unterstützen:

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten des Azure Application Gateway im Kontext von Anwendungsservices durch. Service-Mapping erkennt die ausgehenden http-Verbindungen vom Azure Application Gateway-Service zu Poolmitgliedern, z. B. virtuellen Computern.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Azure Musterbasierte Discovery der Anwendungseinblickkomponente

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Anwendung – Daten ausfüllen in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Anwendungseinblickkomponente – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Application Insight – Komponente [cmdb_Azure_Application_Insight_component]

Feld	Beschreibung
App-ID [App_ID]	Der Bezeichner für die Anwendung, die mit dieser Ressource verknüpft ist.
Anwendungstyp [Application_type]	Der Typ der Anwendung, mit der die Ressource verknüpft ist.
Verbindungszeichenfolge [connection_string]	Die Zeichenfolge, die für die Verbindung mit dem Ressourcenendpunkt verwendet wird.
Instrumentierungsschlüssel [Instrumentation_key]	Der Schlüssel, der für Anwendungseinblicke zum Protokollieren von Telemetriedaten verwendet wird.
Art [Art]	Der spezifische Untertyp oder die spezifische Variation der Ressource.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Aufbewahrung in Tagen [Retention_in_days]	Die Anzahl der Tage, die Protokolle oder Daten aufbewahrt werden.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Verzeichnismandant, zu dem die Ressource gehört.
Version [version]	Die Versionsnummer der Ressource oder des Service.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Anwendungseinblickkomponente – Erweiterter Bestand (LP)“.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.insights/components** .
Beschreibung [short_description]	Beschreibung der Ressource oder des Service.
Version [version]	Die Versionsnummer der Ressource oder des Service.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Application Insight – Komponente [cmdb_Azure_Application_Insight_component]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Musterbasierte Discovery der Anwendungssicherheitsgruppe

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Anwendungssicherheitsgruppe – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure-Anwendungssicherheitsgruppe [cmdb_Azure_Application_Security_Group_Application_Security_Group]

Feld	Beschreibung
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource in Azure.
Bereitstellungsstatus [Provisioning_State]	Aktueller Status des Bereitstellungsprozesses für die Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner für den Mandanten, zu dem die Ressource gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Anwendungssicherheitsgruppe [cmdb_Azure_Application_Security_Group_Application_Security_Group] (Fortsetzung)

Feld	Beschreibung
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Anwendungssicherheitsgruppe – Erweiterter Bestand (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource in Azure.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.network/ applicationsecuritygroups** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Anwendungssicherheitsgruppe [cmdb_Azure_Application_Security_Group_Application_Security_Group]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery des Automatisierungs-Accounts

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Automatisierungs-Account – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure-Automatisierungs-Account [cmdb_Azure_Automation_Account]

Feld	Beschreibung
Lokale Authentifizierung deaktivieren [disable_local_auth]	Eine Einstellung, die angibt, ob die lokale Authentifizierung für die Ressource deaktiviert ist.
Identität [Identität]	Die verwaltete Identität, die der Ressource zugeordnet ist.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Automatisierungs-Account [cmdb_Azure_Automation_Account] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Der Konfigurationsstatus des öffentlichen Netzwerkzugriffs für die Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner für Azure Active Directory-Mandant, der der Ressource zugeordnet ist.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Automatisierungsaccount – Erweiterter Bestand (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.automation/automationaccounts** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Automatisierungs-Account [cmdb_Azure_Automation_Account]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Verfügbarkeit legt Discovery anhand von Mustern fest

Muster für Discovery und Service-Mapping Verwendet das Muster Azure – Verfügbarkeitssatz (LP) zur Erkennung Azure Verfügbarkeitssätze während der horizontalen Discovery. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Azure Abschnitt „Discovery-Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Azure – Verfügbarkeitssatz (LP).

Verfügbarkeitssatz [cmdb_ci_Availability_Set]

Feld	Beschreibung
Objekt-ID [object_ID]	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
Name [name]	Name oder ID, wenn für die Verfügbarkeitszone kein Name angegeben ist
Installationsstatus [install_Status]	Bereitstellungsstatus der Ressource

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Azure Discovery der Verfügbarkeitssätze.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Verfügbarkeitssatz [cmdb_ci_Availability_Set]
Azure-Rechenzentrum [cmdb_ci_azure_datacenter]	Enthält::Enthalten in	Verfügbarkeitssatz [cmdb_ci_Availability_Set]

Azure Discovery von Verfügbarkeitszonen anhand von Mustern

Muster für Discovery und Service-Mapping Verwendet das Muster Azure – Verfügbarkeitszonen (LP) zur Erkennung Azure Verfügbarkeitszonen während der horizontalen Discovery. Um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Azure Abschnitt „Discovery-Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Azure – Verfügbarkeitszonen (LP).

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Objekt-ID [object_ID]	Name der Verfügbarkeitszone im folgenden Format: **{Standort} + „-“ + {ZoneNum}** .
Name [name]	Name der Verfügbarkeitszone im folgenden Format: **{Standort} + „-“ + {ZoneNum}** .
Installationsstatus [install_status]	Installationsstatus der Verfügbarkeitszone. Standardwert ist installiert.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von Azure Verfügbarkeitszonen-Discovery.

CI	Beziehung	CI
Azure-Rechenzentrum [cmdb_ci_azure_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]

Azure Musterbasierte Discovery für Galeriebilddefinition berechnen

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Compute Gallery Image Definition – Extended Inventory (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Compute-Galerie – Bilddefinition [cmdb_Azure_Compute_Gallery_image_Definition]

Feld	Beschreibung
Architektur [Architektur]	Architektur der zentralen Verarbeitungseinheit (CPU) der Ressource, z. B. x86 oder ARM.
Hyper-V-Generierung [Hyper_V_Generation]	Die Hyper-V-Generierungsversion der virtuellen Maschine.
Art [Art]	Die spezifische Unterkategorie oder der Variationstyp der Ressource.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
BS-Typ [os_type]	Der Betriebssystemtyp, der der Ressource zugeordnet ist.
Bereitstellungsstatus [Provisioning_State]	Aktueller Bereitstellungsstatus der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
SKU [sku]	Die Lagerhaltungseinheit (Stock Keeping Unit, SKU), die die Preisstufe der Ressource definiert.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner für Azure Active Directory-Mandant.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Compute Gallery Image Definition – Extended Inventory (LP).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.compute/galleries/images** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Compute-Galerie – Bilddefinition [cmdb_Azure_Compute_Gallery_image_Definition]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Snapshot-Musterbasierte Discovery berechnen

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Compute Snapshot – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Compute – Snapshot [cmdb_Azure_Compute_Snapshot]

Feld	Beschreibung
Datenträgerstatus [Disk_State]	Der aktuelle Status des Datenträgers. Beispiel: Angehängt oder nicht angehängt.
Verschlüsselungstyp [Encryption_type]	Der auf die Ressourcendaten angewendete Verschlüsselungsmechanismus. Beispiel: EncryptionAtRestWithCustomerKey oder EncryptionAtRestWithPlatformKey.
DC-Standort [Standort]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Netzwerkzugriffsrichtlinie [Network_Access_Policy]	Die Richtlinie, die den Netzwerkzugriff auf die Ressource steuert.
Objekt-ID [object_ID]	Ein eindeutiger Bezeichner für die abgefragte Ressource.
BS-Typ [os_type]	Der Typ des Betriebssystems, das der Ressource zugeordnet ist.
Bereitstellungsstatus [Provisioning_State]	Aktueller Bereitstellungsstatus der Ressource. Beispiel: Erfolgreich oder Fehlgeschlagen.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Gibt an, ob auf die Ressource über das öffentliche Netzwerk zugegriffen werden kann.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
SKU-Stufe [sku_Tier]	Die Stufe der Lagerhaltungseinheit (Stock Keeping Unit, SKU), die die Ressourcenleistung und -Kosten bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Compute – Snapshot [cmdb_Azure_Compute_Snapshot] (Fortsetzung)

Feld	Beschreibung
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner des Mandanten, der die Ressource besitzt.
Typ [type]	Der Typ oder die Kategorie der Ressource.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Speichervolume-Snapshot“ [cmdb_ci_Storage_vol_Snapshot].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Snapshot berechnen – Erweiterter Bestand (LP)“.

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Feld	Beschreibung
Kapazität [Kapazität]	Die Größe des Datenträgers in Bezug auf die Speicherkapazität.
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Ein eindeutiger Bezeichner für die abgefragte Ressource im folgenden Format: **/Subscriptions/ {subscriptionId}/resourceGroups/ {resouceGroupName}/Provider/ Microsoft.Compute/snapshots/ {snapshotName}** .
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Status [state]	Der aktuelle Status des Datenträgers. Beispiel: Angehängt oder nicht angehängt.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Azure Compute – Snapshot [cmdb_Azure_Compute_Snapshot]	Referenzen	Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery der Container-Registrierung

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Container-Registrierung – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Container-Registrierung [cmdb_Azure_Container_Registry_Registry]

Feld	Beschreibung
Admin-Anwender aktiviert [admin_user_enabled]	Gibt an, ob der Administrator-Anwenderaccount für die Ressource aktiviert ist.
Verschlüsselungsstatus [Encryption_Status]	Der aktuelle Verschlüsselungsstatus der Ressource, der angibt, ob Daten verschlüsselt sind.
Identität [Identität]	Die Identitätsinformationen für die Ressource, die für Authentifizierung und Autorisierung verwendet werden.
Art [Art]	Die spezifische Art oder Untertyp der Ressource, falls zutreffend.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Gibt an, ob öffentlicher Netzwerkzugriff für die Ressource zulässig ist.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Die Azure Active Directory-Mandanten-ID, die der Ressource zugeordnet ist.
Stufe [Stufe]	Die Service- oder Ressourcenebene, die das Leistungs- oder Kostenniveau angibt.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Container-Registrierung – Erweiterter Bestand (LP)“.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource] (Fortsetzung)

Feld	Beschreibung
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.containerregistrierung/ Registrierungen** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Container-Registrierung [cmdb_Azure_Container_Registry_Registry]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Data Factory-Discovery

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Data Factory – Extended Inventory (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Data Factory [cmdb_Azure_Data_Factory_Data_Data_Factory]

Feld	Beschreibung
Identität [Identität]	Informationen zur Identität, die der Ressource zugeordnet ist.
Art [Art]	Die spezifische Art oder Lagerhaltungseinheit (SKU) der Ressource.
Standort [location]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Der Status der Zugänglichkeit des öffentlichen Netzwerks für die Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner des Mandanten, der die Ressource enthält.
Version [version]	Die Version der Ressource.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Data Factory – Extended Inventory (LP)“.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource] (Fortsetzung)

Feld	Beschreibung
Standort [location]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.datafactory/Fabrics** .
Beschreibung [short_description]	Beschreibung der Ressource oder des Service.
Version [version]	Die Version der Ressource.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Data Factory [cmdb_Azure_Data_Factory_Data_Data_Factory]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery für Sicherungsresor für Datenschutz

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Datenschutz-Sicherungsresor – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Data Protection – Sicherungsresor [cmdb_Azure_Data_Protection_Backup_Vault]

Feld	Beschreibung
Art [Art]	Der Typ oder die Kategorie der Ressource.
Standort [location]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner des Azure Active Directory-Mandant.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Datenschutz-Sicherungsresor – Erweitertes Inventar (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource] (Fortsetzung)

Feld	Beschreibung
Standort [location]	Der geografische Standort, an dem die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource.
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.Datenschutz/Backupvaults** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Data Protection – Sicherungsresor [cmdb_Azure_Data_Protection_Backup_Vault]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery des Arbeitsbereichs „Databricks“

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Databricks-Arbeitsbereich – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure-Databricks – Arbeitsbereich [cmdb_Azure_databricks_Workspace]

Feld	Beschreibung
Art [Art]	Der Modell- oder Konfigurationstyp der Ressource.
Standort [location]	Geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Gibt an, ob der öffentliche Netzwerkzugriff für die Ressource aktiviert ist.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
SKU-Name [sku_Name]	Die Lagerhaltungseinheit (Stock Keeping Unit, SKU), die die Preisstufe der Ressource definiert.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner für Azure Active Directory-Mandant.
Arbeitsbereich-ID [Workspace_ID]	Der eindeutige Bezeichner für den Arbeitsbereich, der der Ressource zugeordnet ist.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Databricks-Arbeitsbereich – Erweiterter Bestand (LP)“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.databricks/Arbeitsbereiche** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Databricks – Arbeitsbereich [cmdb_Azure_databricks_Workspace]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery für Datenträgerverschlüsselungssatz

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Datenträgerverschlüsselungssatz – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure-Datenträgerverschlüsselungssatz [cmdb_Azure_Disk_Encryption_Set_Disk_Encryption_Set]

Feld	Beschreibung
Verschlüsselungstyp [Encryption_type]	Die zum Verschlüsseln der Ressourcendaten verwendete Methode.
Identitätstyp [Identity_type]	Die Klassifizierung der Identität, die der Ressource zugewiesen ist. Beispiel: SystemAssigned oder UserAssigned.
Schlüssel-URL [key_url]	Die URL, in der der Verschlüsselungsschlüssel gespeichert oder zugänglich ist.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Status des Ressourcenbereitstellungsprozesses.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Mandanten-ID [Mandant_ID]	Der Bezeichner für den Mandanten, der die Ressource besitzt.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Datenträgerverschlüsselungssatz – Erweitertes Inventar (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.compute/diskencryptionsets** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Datenträgerverschlüsselungssatz [cmdb_Azure_Disk_Encryption_Set_Disk_Encryption_Set]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure DNS Zonen- und Datensatzsätze Discovery anhand von Mustern

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet die Muster Azure – DNS Zones (LP) und Azure – DNS Zone Recordsets (LP) zur Erkennung Azure Domain Name System (DNS) Definitionen (Zonen und ihre jeweiligen Datensatzsätze). Um einige dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über zu erfahren Azure DNS-Zonen und Datensatzsätze und ihre Version, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Weitere Informationen zu finden Azure Cloud-Discovery, siehe Erkennung von Azure-Clouds.

Voraussetzungen

Überprüfen Sie die Berechtigungen

Auf der Microsoft Azure Konsole, stellt einem Anwender die Rolle API-Management-Service-Leser bereit.

Erstellen Azure Service-Prinzipal-Anmeldeinformationen

Weitere Informationen finden Sie unter: Anmeldeinformationen für Azure-Cloud erstellen.

Konfigurieren Azure Service-Account

Weitere Informationen finden Sie unter Richten Sie ein Cloud-KontoFür Azure.

Discovery-Zeitplan erstellen

Erstellen Sie einen Zeitplan für die relevanten Azure-Service-Accounts. Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen der Muster Azure – DNS Zones (LP) und Azure – DNS Zone Recordsets (LP).

Vom Muster Azure – DNS Zones (LP) erkannte Ressourcen

DNS-Zone [cmdb_ci_dns_Zone]

Feld	Beschreibung
Name [name]	Der Name der DNS-Zone.
Anzahl der Datensatzsätze [number_of_Record Sets]	Die Anzahl der in der DNS-Zone definierten Datensatzsätze.
Betriebsstatus [operational_status]	Der Betriebsstatus der DNS-Zone.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DNS-Zone [cmdb_ci_dns_Zone] (Fortsetzung)

Feld	Beschreibung
Status [state]	Der Status der DNS-Zone.
Installationsstatus [install_status]	Der Installationsstatus der DNS-Zone.
Kommentare [comments]	Das Feld für allgemeine Kommentare.

Ressourcen, die vom Muster Azure – DNS Zone Recordsets (LP) erkannt wurden

DNS Alias [cmdb_ci_dns_Alias]

Feld	Beschreibung
Name [name]	Der Name des DNS-Alias-Datensatzes.
IP-Adresse [ip_address]	IP-Adresse des DNS-Alias-Datensatzes.
Kommentare [comments]	Eindeutiger Bezeichner für Azure DNS-Zone, die Service-Account-ID, DNS-Zonenname und ein festes Hash-Suffix kombiniert.
Betriebsstatus [operational_status]	Der Betriebsstatus des DNS-Alias-Datensatzes.

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Der Name des DNS-Namensdatensatzes.
Betriebsstatus [operational_status]	Der Betriebsstatus des DNS-Datensatzes.
Kommentare [comments]	Eindeutiger Bezeichner für Azure DNS-Zone, die Service-Account-ID, DNS-Zonenname und ein festes Hash-Suffix kombiniert.

CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Azure DNS Zonen-Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	DNS-Zone [cmdb_ci_dns_Zone]

Diese Beziehungen werden zur Unterstützung erstellt Azure DNS Discovery des Zonendatensatzes.

CI	Beziehung	CI
DNS-Zone [cmdb_ci_dns_Zone]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
DNS-Zone [cmdb_ci_dns_Zone]	Enthält::Enthalten in	DNS-Alias [cmdb_ci_dns_alias]
DNS-Name [cmdb_ci_dns_name]	Verwendet von::Verwendet	DNS-Alias [cmdb_ci_dns_alias]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Ereignis-Grid-Systemthema-Discovery mit Mustern

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Ereignisrastersystem – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure-Ereignisraster – Systemthema [cmdb_Azure_event_Grid_System_topic]

Feld	Beschreibung
Art [Art]	Die spezifische Art oder Lagerhaltungseinheit (SKU) der Ressource, die ihre Fähigkeiten oder Konfiguration beschreibt.
Metrikressourcen-ID [metric_resource_ID]	Der Bezeichner, der für den Zugriff auf Metriken verwendet wird, die sich auf die Ressource beziehen.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource in Azure.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Status des Bereitstellungsprozesses der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner für Azure Active Directory-Mandant.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Ereignisraster – Systemthema [cmdb_Azure_event_Grid_System_topic] (Fortsetzung)

Feld	Beschreibung
Thementyp [topic_type]	Die Kategorie oder der Typ des Ereignisthemas.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud Messaging-Service“ [cmdb_ci_Cloud_Messaging_Service].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Ereignisrastersystem – Erweiterter Bestand (LP).

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource gehostet wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource in Azure.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Typ [type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.eventraster/systemthemen** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure-Ereignisraster – Systemthema [cmdb_Azure_event_Grid_System_topic]	Referenzen	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value] (Fortsetzung)

Feld	Beschreibung
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery des Ereignis-Hub-Namespace

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Ereignis-Hub-Namespace – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Event Hub – Namespace [cmdb_Azure_event_Hub_Namespace]

Feld	Beschreibung
Art [Art]	Die Art oder der Untertyp der Ressource, häufig die spezifische Rolle oder Variation.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Minimale TLS-Version [Minimum_tls_Version]	Die minimale TLS-Version (Transport Layer Security), die für die Ressource für sichere Verbindungen erforderlich ist.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Event Hub – Namespace [cmdb_Azure_event_Hub_Namespace] (Fortsetzung)

Feld	Beschreibung
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Status des Ressourcenbereitstellungsprozesses.
Öffentliches Netzwerk #ccess [public_Network_Access]	Gibt an, ob auf die Ressource über das öffentliche Netzwerk zugegriffen werden kann.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner des Azure Active Directory-Mandant.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud Messaging-Service“ [cmdb_ci_Cloud_Messaging_Service].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Ereignis-Hub-Namespace – Erweitertes Inventar (LP).

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Name [name]	Der Name der Ressource.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Typ [type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.eventhub/namespaces** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Event Hub – Namespace [cmdb_Azure_event_Hub_Namespace]	Referenzen	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Microsoft Azure Funktionen-Discovery mit Mustern

Die Muster für Discovery und Service-Mapping-Anwendung verwendet Azure – Funktionen (LP) Und Azure: Funktionen TD Zu erkennende Muster Azure Functions Apps und ordnen Sie sie im Kontext von Anwendungsservices zu. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure Functions Detaillierte Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Azure Service-Account

Konfigurieren Sie Azure Service-Account. Weitere Informationen finden Sie unter Richten Sie ein Cloud-KontoFür Azure

Azure-Prinzipal-Anmeldeinformationen

Erstellen Sie auf der ServiceNow AI Platform ein Servicekonto für die Cloud-Erkennung. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird. Weitere Informationen finden Sie unter: Anmeldeinformationen für Azure-Cloud erstellen

Berechtigungen

Weisen Sie in der Microsoft Azure-Konsole einem Benutzer die API-Management-Service-Leserrolle zu.

Ausführen Azure Cloud-Discovery

Detaillierte Informationen finden Sie unter: Erkennung von Azure-Clouds

Discovery-Zeitplan erstellen

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Azure Function [cmdb_ci_cloud_function]	
name	Der Name der Funktions-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Object_id	Die ID der Funktions-App.
ip_address	Die IP-Adresse der Funktions-App.
fqdn	Der vollqualifizierte Domänenname (FQDN) der Funktions-App.
Code_location_url	Die URL des Quellcodes der Funktions-App.
app_function_state	Der Status der Funktions-App.
operational_status	Der Betriebsstatus der Funktions-App.
install_status	Der Installationsstatus der Funktions-App.

CI-Beziehungen

Diese Beziehungen sollen die Azure Functions-Erkennung unterstützen:

CI	Beziehung	CI
Azure Functions [cmdb_ci_cloud_function]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_Azure_Datacenter]

Verbindungen, die von Service-Mapping während der Erkennung von oben nach unten gefunden werden

Service-Mapping kann die folgenden Verbindungen erkennen:

- Verbindungen mit den folgenden Datenbanken: MSSql, MySql, MongoDB und Documentum
- HTTP-Verbindungen, die zur Azure Functions-Umgebung gehören, z. B. https://scenario4-hop1-azure-funktion.azurewebsites.net

> **Hinweis:** Service-Mapping durchsucht Java-Klassen/JAR-Dateien und Binärdateien nicht nach möglichen Informationen über ausgehende HTTP-Verbindungen von Azure Functions. Wenn Java-Klassen/JAR-Dateien und Binärdateien die einzige Informationsquelle zu einigen ausgehenden HTTP-Verbindungen sind, findet Service-Mapping diese HTTP-Verbindungen nicht.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Azure Musterbasierte Key Vault-Discovery

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Key Vault – Extended Inventory (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Key Vault [cmdb_Azure_key_Vault_key_Vault]

Feld	Beschreibung
Art [Art]	Das spezifische Formular oder die spezifische Variante des Ressourcentyps.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Öffentlicher Netzwerkzugriff [public_Network_Access]	Gibt an, ob die Ressource über ein öffentliches Netzwerk zugänglich ist.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner von Azure Active Directory-Mandant, zu dem die Ressource gehört.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Key Vault – Erweitertes Inventar (LP)“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.keyVault/Vault** .
Beschreibung [short_description]	Beschreibung der Ressource oder des Service.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Key Vault [cmdb_Azure_key_Vault_key_Vault]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery der Logic-App

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Logic App – Erweiterter Bestand“ (LP).

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Logic-App [cmdb_Azure_Logic_App_Logic_App]

Feld	Beschreibung
Zugriffsendpunkt [Access_Endpoint]	Die Endpunkt-URL, die für den Zugriff auf die Ressource verwendet wird.
Identität [Identität]	Die Identität, die der Ressource zu Zugriffs- und Sicherheitszwecken zugeordnet ist.
Art [Art]	Die spezifische Unterkategorie oder Variante der Ressource.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungsstatus der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Status [state]	Der aktuelle Gesamtbetriebsstatus der Ressource.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner des Mandanten, der die Ressource besitzt.
Typ [type]	Der Typ oder die Kategorie der Ressource.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Funktion“ [cmdb_ci_Cloud_function].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Logic App – Extended Inventory (LP)“.

Cloud-Funktion [cmdb_ci_cloud_function]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource im folgenden Format: **/Subscriptions/ {subscriptionId}/resourceGroups/ {resouceGroupName}/Provider/ Microsoft.Logic/Workflows/ {workflowname}** .
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Funktion [cmdb_ci_cloud_function]
Cloud-Funktion [cmdb_ci_cloud_function]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Logic-App [cmdb_Azure_Logic_App_Logic_App]	Referenzen	Cloud-Funktion [cmdb_ci_cloud_function]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Verwaltete Identität – vom Anwender zugewiesene Identität – musterbasierte Discovery

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – verwaltete Identität – zugewiesene Identität des Anwenders – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure – verwaltete Identität – vom Anwender zugewiesene Identität [cmdb_Azure_Managed_Identity_user_assigned_Identity]

Feld	Beschreibung
Client-ID [Client_ID]	Der eindeutige Bezeichner für einen Azure Active Directory (Azure AD) Anwendung, auch als Client bezeichnet.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Prinzipal-ID [Principal_ID]	Der eindeutige Bezeichner des Prinzipalservice oder Anwenders, der der Ressource zugeordnet ist.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Mandanten-ID [Mandant_ID]	Der eindeutige Bezeichner von Azure AD-Mandant.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure – verwaltete Identität – vom Anwender zugewiesene Identität [cmdb_Azure_Managed_Identity_user_assigned_Identity] (Fortsetzung)

Feld	Beschreibung
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – verwaltete Identität – zugewiesene Identität des Anwenders – Erweitertes Inventar (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.managedidentity/ userassignedidentities** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure – verwaltete Identität – vom Anwender zugewiesene Identität [cmdb_Azure_Managed_Identity_user_assigned_Identity]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery für Netzwerke

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Netzwerke-IP-Gruppe – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Networks – IP-Gruppe [cmdb_Azure_Networks_ip_Group]

Feld	Beschreibung
Standort [location]	Die geografische Region, in der die Ressource gehostet wird.
Objekt-ID [object_ID]	Ein eindeutiger Bezeichner für die Ressource in Azure.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Networks – IP-Gruppe [cmdb_Azure_Networks_ip_Group] (Fortsetzung)

Feld	Beschreibung
Mandanten-ID [Mandant_ID]	Der Bezeichner für Azure Active Directory-Mandant, der der Ressource zugeordnet ist.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Netzwerke-IP-Gruppe – Erweiterter Bestand (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource gehostet wird.
Name [name]	Der Name, der der Ressource zugewiesen ist.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner für die Ressource in Azure.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.network/ipgroups** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Networks – IP-Gruppe [cmdb_Azure_Networks_ip_Group]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery für privaten Link

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – privater Link – privater Endpunkt – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Privater Azure-Link – privater Endpunkt [cmdb_Azure_private_Link_private_endpoint]

Feld	Beschreibung
Art [Art]	Die spezifische Kategorie oder Variante des Ressourcentyps.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Privater Azure-Link – privater Endpunkt [cmdb_Azure_private_Link_private_endpoint] (Fortsetzung)

Feld	Beschreibung
Bereitstellungsstatus [Provisioning_State]	Der aktuelle Bereitstellungs- oder Bereitstellungsstatus der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Mandanten-ID [Mandant_ID]	Der Bezeichner für den Mandanten, der der Ressource zugeordnet ist.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – privater Link – privater Endpunkt – Erweiterter Bestand (LP)“.

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Ressource bereitgestellt wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.network/privateendpoints** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Privater Azure-Link – privater Endpunkt [cmdb_Azure_private_Link_private_endpoint]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Microsoft Azure Ressourcenbestands-Discovery

Die ServiceNow Discovery Die Anwendung verwendet das Azure Resource Inventory (LP)-Muster, um Ressourcen zu finden, die über verfügbar sind Azure Die kein dediziertes Muster haben. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Sie können bis zu 10.000 Ressourcen mithilfe des Azure Resource Inventory (LP)-Musters erkennen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure Service-Prinzipal

Verifizieren Sie Azure Serviceprinzipal ist konfiguriert. Weitere Informationen finden Sie unter Erkennung von Azure-Clouds

Berechtigungen

Für Versionen 1.3.0 und höher:

Weisen Sie einem Anwender in der Microsoft Azure-Konsole die Rolle API Management Service Reader mit Berechtigungen zum Ausführen der folgenden REST-POST-Anforderung zu:

„https://management.<resource url>/Provider/microsoft.resourcegraph/resources?api-Version=2022-10-01“

<resource url>: Die URL variiert je nach Azure-Kontotyp, z. B. „azure.com“ oder Adresse der Behördenwebsite.

Für Versionen 1.0.99 und früher:

Stellen Sie in der Microsoft Azure-Konsole einem Benutzer die Rolle „API Management Service-Leser“ mit Berechtigungen zum Ausführen der folgenden REST GET-Anforderung zur Verfügung:

"https://management.azure.com/subscriptions/<subscription id>/resources"

Cloud Discovery-Zeitplan erstellen

Erstellen Sie einen Zeitplan für den entsprechenden Azure-Service-Account, wie in beschrieben Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung des Azure-Bestands mithilfe der Aufnahmeliste für Ressourcen feintunen

Wenn Ihre Bereitstellung anwenderdefinierte Muster für die Azure-Discovery aufweist, stellen Sie sicher, dass Sie Azure-Ressourcen nicht zweimal erkennen.

Hinweis: Wenn Sie die Tabelle [pre_resource_Whitelist] leer lassen, werden alle Ressourcen vom Muster ausgefüllt, was zu Leistungsproblemen führen kann.

1. Stellen Sie sicher, dass der Anwendungsbereich ist Muster für Discovery und Service-Mapping:
   a. Navigieren zu **Einstellungen** > **Entwickler**an.
   b. Wählen Sie Discovery and Service Mapping Patterns aus der Liste **Anwendung** aus.
2. Navigieren zu **Systemdefinitionen** > **Tabellen**an.
3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option Löschen aus.

Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Aufnahmeliste um zusätzliche Ressourcentypen erweitern, die das Muster erkennen soll. Die Namen dieser Ressourcentypen müssen den Benennungskonventionen der entsprechenden Anbieter entsprechen.

Hinweis: Wenn Sie die sofort einsatzbereite Aufnahmeliste ändern, wird sie in Anwendungsupdates nicht mehr automatisch aktualisiert. Sie müssen die anwenderdefinierte Liste selbst verwalten.

1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Cloud-Anbieter	Der Lieferant des Ressourcentyps: Azure.
Ressourcentyp	Die Azure Ressourcentypwert.
Anwendung	Der Anwendungsbereich: Discovery and Service Mapping Patterns

Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

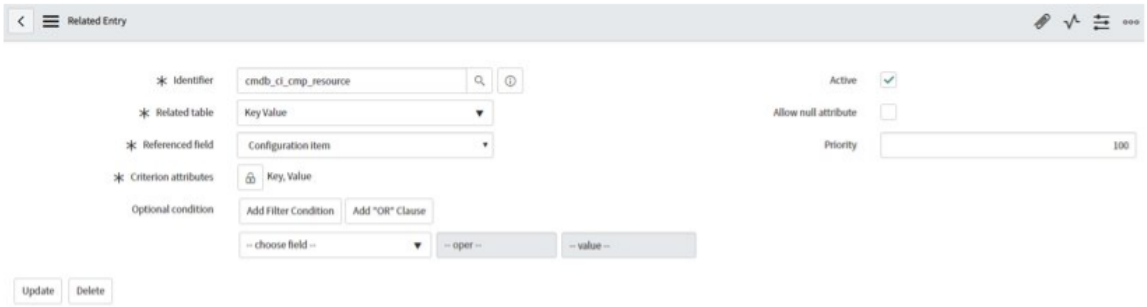
Ändern Sie die mit ServiceNow verbundenen Einträge.

1. Navigieren Sie zu **Zugehörige Einträge**.
2. Klicken Sie auf **Neu**.
3. Geben Sie als Bezeichner **cmdb_ci_cmp_resource** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie für die zugehörige Tabelle **Schlüsselwert [cmdb_key_value]** aus.
5. Wählen Sie für das referenzierte Feld **Configuration Item** aus.
6. Fügen Sie für die Kriteriumsattribute **Schlüssel** und **Wert** hinzu.

   Möglicherweise müssen Sie auf das Schlosssymbol klicken, um die Kriteriumsattribute anzuzeigen und zu ändern.



Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Ressource [cmdb_ci_cmp_resource]	
Name	Ein beschreibender Name zum Erkennen der Azure-Ressource
Ressourcentyp	Der Typ der Ressource, z. B. Netzwerk, Lastenausgleichsmodul
Objekt-ID	Die ID der Azure-Ressource.
Beschreibung	Der während der Erkennung ausgefüllte Text, der angibt, dass diese Ressource in Azure verfügbar ist
Schlüsselwert [cmdb_key_value]	
Schlüssel	Der Name des Azure-Tag-Schlüssels.
Wert	Der Name des Azure-Tag-Werts.

CI-Beziehungen

Diese Beziehungen werden zur Unterstützung erstellt Azure Ressourcenbestands-Discovery:

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_Azure_Datacenter]

Zugehörige Informationen

https://learn.microsoft.com/en-us/azure/governance/resource-graph/reference/supported-tables-resources

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Musterbasierte Discovery des Service Bus-Namespace

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Service Bus-Namespace – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Service Bus – Namespace [cmdb_Azure_Service_Bus_Namespace]

Feld	Beschreibung
Identität [Identität]	Die Identitätsinformationen, die der Ressource zugeordnet sind und häufig für Authentifizierung oder Zugriffssteuerung verwendet werden.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Objekt-ID [object_ID]	Der eindeutige Bezeichner der Ressource.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Status [status]	Der aktuelle Status oder Status der Ressource.
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Ressource“ [cmdb_ci_CMP_resource].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters Azure – Service Bus-Namespace – Erweitertes Inventar (LP).

Cloud-Ressource [cmdb_ci_cmp_resource]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Der geografische Standort, an dem die Ressource gehostet wird.
Name [name]	Der Name der Ressource
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Ressourcentyp [resource_type]	Typ der Ressource. Der Wert ist auf festgelegt **microsoft.servicebus/namespaces** .
Beschreibung [short_description]	Beschreibung der Ressource oder des Service.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Ressource [cmdb_ci_cmp_resource]
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Service Bus – Namespace [cmdb_Azure_Service_Bus_Namespace]	Referenzen	Cloud-Ressource [cmdb_ci_cmp_resource]

Microsoft Azure Tag-Discovery

Das Muster sammelt Tags und füllt sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Azure Musterbasierte Discovery in der Servicebus-Warteschlange

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Service Bus-Warteschlange – Erweitertes Inventar (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Service Bus – Warteschlange [cmdb_Azure_Service_Bus_Queue]

Feld	Beschreibung
Batchvorgänge aktivieren [enable_Batched_Operations]	Gibt an, ob Batchvorgänge für die Warteschlange aktiviert sind.
Partitionierung aktivieren [enable_partitioning]	Gibt an, ob die Nachrichtenpartitionierung für die Lastverteilung über mehrere Nachrichten-Broker aktiviert ist.
DC-Standort [Standort]	Die geografische Region, in der die Service Bus-Warteschlange bereitgestellt wird.
Max. Nachrichtengröße in KB [max_message_size_in_kb]	Die maximal zulässige Größe einer einzelnen Nachricht in Kilobyte (KB).
Max. Größe in MB [max_size_in_mb]	Die maximale Speichergröße der Warteschlange in Megabyte (MB).
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Service Bus-Warteschlange.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Status [status]	Der aktuelle Status der Service Bus-Warteschlange.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Service Bus – Warteschlange [cmdb_Azure_Service_Bus_Queue] (Fortsetzung)

Feld	Beschreibung
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud Messaging-Service“ [cmdb_ci_Cloud_Messaging_Service].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Service Bus-Warteschlange – Erweiterter Bestand (LP)“.

Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der die Service Bus-Warteschlange bereitgestellt wird.
Name [name]	Der Name der Service Bus-Warteschlange.
Objekt-ID [object_id]	Der eindeutige Bezeichner für die Service Bus-Warteschlange.
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Typ [type]	Typ der Ressource. Der Wert ist auf festgelegt **Microsoft.ServiceBus/Namespaces/Warteschlangen** .

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Enthält::Enthalten in	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]
Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Service Bus – Warteschlange [cmdb_Azure_Service_Bus_Queue]	Referenzen	Cloud Messaging-Service [cmdb_ci_Cloud_Messaging_Service]

Azure Musterbasierte Discovery des Service Bus-Themas

Muster für Discovery und Service-Mapping Findet Microsoft Azure Services in Ihrer Cloud-Umgebung. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbasierte Discovery- und Zuordnungsanforderungen

Verifizieren Sie Microsoft Azure Discovery-Voraussetzungen

Weitere Informationen finden Sie im Abschnitt „Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Aktivieren Sie das entsprechende Muster

Das Muster für diesen Service ist standardmäßig deaktiviert. Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird. Weitere Informationen zum Aktivieren von Mustern finden Sie unter Aktivieren Sie ein deaktiviertes Muster.

Konfigurieren Sie Discovery Zeitplan für die Unterstützung von GovCloud

Wird Erkannt Microsoft Azure Für GovCloud-Accounts (USA) ist die Verwendung einer Rechenzentrum-URL beim Einrichten eines erforderlich Microsoft Azure Service-Account. Weitere Informationen finden Sie unter Cloud-Discovery Referenz des Service-Account-Formulars.

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in beiden aus CMDB Und nicht- CMDB Tabellen.

Daten gespeichert in nicht- CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in nicht- CMDB Tabelle beim Ausführen des Musters „Azure – Service Bus-Thema – Erweiterter Bestand (LP)“.

Sie können die nicht- CMDB Azure Tabellen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Azure**an. Sie können auch im Navigationsfilter nach dem bestimmten Musternamen suchen.

Azure Service Bus – Thema [cmdb_Azure_Service_Bus_topic]

Feld	Beschreibung
Batchvorgänge aktivieren [enable_Batched_Operations]	Gibt an, ob Batchvorgänge für das Thema aktiviert sind.
Partitionierung aktivieren [enable_partitioning]	Gibt an, ob das Thema partitioniert ist, um die Skalierbarkeit zu unterstützen.
DC-Standort [Standort]	Die geografische Region, in der das Thema bereitgestellt wird.
Max. Nachrichtengröße in KB [max_message_size_in_kb]	Die maximale Größe einer Nachricht, die an das Thema gesendet werden kann, gemessen in Kilobyte (KB).
Max. Größe in MB [max_size_in_mb]	Die maximale Speichergrenze für das Thema in Megabyte (MB).
Objekt-ID [object_ID]	Der eindeutige Bezeichner für die Themenressource.
Status [status]	Der aktuelle Status der Themenressource. Beispiel: Aktiv oder deaktiviert.
Abonnementanzahl [Subscription_count]	Die Anzahl der aktiven Abonnements, die dem Thema zugeordnet sind.
Ressourcengruppe [resource_Group]	Name der Ressourcengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Service Bus – Thema [cmdb_Azure_Service_Bus_topic] (Fortsetzung)

Feld	Beschreibung
Abonnement-ID [Subscription_ID]	Die Abonnement-ID.
Konfigurationselement [Configuration_item]	Verweist auf die Tabelle „Cloud-Thema“ [cmdb_ci_Cloud_topic].

Daten in gespeichert CMDB Tabellen

Muster für Discovery und Service-Mapping Die Anwendung füllt Daten in aus CMDB Beim Ausführen des Musters „Azure – Service Bus-Thema – Erweiterter Bestand (LP)“.

Cloud-Thema [cmdb_ci_Cloud_topic]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus der Ressource. Standardwert ist installiert.
Standort [location]	Die geografische Region, in der das Thema bereitgestellt wird.
Name [name]	Der Name des Themas im Service Bus-Namespace.
Objekt-ID [object_id]	Der eindeutige Bezeichner der Ressource im folgenden Format: **/Subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/Provider/Microsoft.ServiceBus/namespaces/{namespaceName}/topics/{topicName}**
Betriebsstatus [operational_status]	Betriebsstatus der Ressource. Der Standardwert ist betriebsbereit.
Beschreibung [short_description]	Beschreibung der Ressource oder des Service.

CI-Beziehungen

Das Muster erstellt diese Beziehungen zur Unterstützung der Discovery.

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Enthält::Enthalten in	Cloud-Thema [cmdb_ci_Cloud_topic]
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Thema [cmdb_ci_Cloud_topic]
Cloud-Thema [cmdb_ci_Cloud_topic]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Azure Service Bus – Thema [cmdb_Azure_Service_Bus_topic]	Referenzen	Cloud-Thema [cmdb_ci_Cloud_topic]

Azure Virtual Machine Scale Sets (VMSS) Instanz-Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet die Muster Azure – VM Scale Set (LP) und Azure VM Instance – Uniform Scale Set (Azure VM Scale Set), um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu finden Azure Virtual Machine Scale Sets (VMSS). Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

VMSS Ermöglicht das Erstellen und Verwalten einer Gruppe von virtuellen Maschinen mit Lastenausgleich (VMs). Die Anzahl der VM-Instanzen kann als Reaktion auf den Bedarf oder einen definierten Zeitplan automatisch erhöht oder verringert werden. Dort Einheitlich Orchestration-Modi flexibel und erreichen.

- VMSS Mit flexibler Orchestration wird bei identischen oder mehreren VM-Typen eine hohe Verfügbarkeit im Maßstab erreicht. Mit flexibler Orchestration Azure Bietet eine einheitliche Experience für den Azure VM-Ökosystem.
- VMSS Mit Uniform Orchestration, optimiert für große statuslose Arbeitsauslastungen mit identischen Instanzen. VMSS Verwenden Sie bei einheitlicher Orchestration ein VM-Profil oder eine Vorlage, um die gewünschte Kapazität zu erreichen. Es gibt zwar einige Möglichkeiten, einzelne VM-Instanzen zu verwalten oder anzupassen, aber Uniform verwendet identische VM-Instanzen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Um mehr über zu erfahren VMSS Und deren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Verifizieren Sie Azure Abschnitt „Discovery-Voraussetzungen“ in Microsoft Azure Cloud-Discovery mithilfe von Mustern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters Azure – VM Scale Set (LP).

Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

Feld	Beschreibung
Installationsstatus [install_status]	Installationsstatus des Instanzskalierungssatzes. Standardwert ist installiert.
Status [state]	Bereitstellungsstatus des Instanzskalierungssatzes. Mögliche Werte sind verfügbar oder beendet.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner für den Instanzskalierungssatz.
Name [name]	Name des Instanzskalierungssatzes.

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Musters „Azure VM-Instanz – einheitlicher Skalierungssatz“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Netzwerkadapter [nics]	Anzahl der Netzwerkschnittstellenkarten (Network Interface Cards, NICs), die an die VM-Instanz angehängt sind.
Status [state]	Aktueller Status der Instanz. Beispiel: Ein, aus oder beendet.
Installationsstatus [install_status]	Installationsstatus der Instanz. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Instanz. Der Standardwert ist betriebsbereit.
Datenträger [Datenträger]	Anzahl der an die Instanz angehängten Datenträger.
Datenträgergröße (GB) [Disk_size]	Gesamtspeicherkapazität aller an die VM angeschlossenen Datenträger in Gigabyte (GB).

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Name [name]	Name oder ID für das Speichervolume.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
Installationsstatus [install_status]	Installationsstatus des Speichervolumes. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus des Speichervolumes. Der Standardwert ist betriebsbereit.

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Name [name]	Name oder ID für die Netzwerkschnittstelle.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
Installationsstatus [install_status]	Installationsstatus der Netzwerkschnittstelle. Der Standardstatus ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus der Netzwerkschnittstelle. Der Standardstatus ist „betriebsbereit“.

VNIC-Endpunkt [cmdb_ci_endpoint_vnic]

Feld	Beschreibung
Name [name]	Name oder ID für den Endpunkt.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name oder ID für das Image.
Objekt-ID [object_id]	Ein eindeutiger Bezeichner, zugeordnet von Microsoft Azure Für diese Ressource.
Installationsstatus [install_status]	Installationsstatus des Image. Standardwert ist installiert.
Betriebsstatus [operational_status]	Betriebsstatus des Image. Der Standardwert ist betriebsbereit.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktivieren Sie die Cloud-BS-Image-Discovery.

Hardwaretyp [cmdb_ci_compute_template]

Feld	Beschreibung
Name [name]	Name des Hardwaretyps.

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

CI-Beziehungen

Discovery Erstellt diese Beziehungen zur Unterstützung von VMSS Discovery beim Ausführen des Musters Azure – VM Scale Set (LP).

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Instanzskalierungssatz [cmdb_ci_instance_scale_Set]
Instanzskalierungssatz [cmdb_ci_instance_scale_Set]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Instanzskalierungssatz [cmdb_ci_instance_scale_Set]	Verbraucht::verbraucht von	Load Balancer-Pool [cmdb_ci_lb_pool]

Discovery Erstellt diese Beziehungen zur Unterstützung von VMSS Discovery beim Ausführen des Musters „Azure – VM Scale Set“ (LP).

CI	Beziehung	CI
VM-Instanz [cmdb_ci_vm_instance]	Verwaltet von::Verwaltet	Instanzskalierungssatz [cmdb_ci_instance_scale_Set]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Speichervolume [cmdb_ci_storage_volume]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Block-Endpunkt [cmdb_ci_endpoint_block]	Endpunkt implementieren in::Endpunkt implementieren von	Speichervolume [cmdb_ci_storage_volume]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Hardwaretyp [cmdb_ci_compute_template]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Hardwaretyp [cmdb_ci_compute_template]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Cloud-Hardwaretyp [cmdb_ci_Cloud_Hardware_type]
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt implementieren in::Endpunkt implementieren von	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Image [cmdb_ci_os_template]
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Tag-Discovery

Sowohl die Muster „Azure – VM Scale Set“ (LP) als auch „Azure VM Instance – Uniform Scale Set“ erfassen Tags und füllen sie in der Tabelle „Schlüsselwert“ [cmdb_key_value] aus.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Tag-Name.
Wert [value]	Tag-Wert.

Oracle Cloud Infrastructure (OCI)-Discovery

ServiceNow Discovery Verwendet die Discovery-Muster von Oracle Cloud Infrastructure (OCI), um Enterprise-Anwendungen durch Kombination in Echtzeit elastisch zu machen Oracle Autonome Services, integrierte Sicherheit und Cloud-Computing. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen installiert sind

Überprüfen Sie, ob die folgenden Anwendungen installiert und auf dem neuesten Stand sind:

- Cloud-Zugriffsschnittstelle (ab Version 1,0.0)
- Visibility Content
- CMDB CI-Klassenmodelle
- Muster für Discovery und Service-Mapping

Konfigurieren Sie Oracle API-Anmeldeinformationen

Stellen Sie sicher, dass Ihre OCI-Anmeldeinformationen konfiguriert sind und dass Ihre privaten und öffentlichen Schlüssel in das RSA-Format konvertiert werden. Weitere Informationen finden Sie unter Erstellen Oracle API-Anmeldeinformationen.

Erstellen Sie einen OCI-Service-Account

Weitere Informationen finden Sie unter Erstellen Sie OCI-Service-Accounts.

Erstellen Sie einen Cloud-Discovery-Zeitplan

Informationen zum Ausführen einer Cloud-Discovery im Maßstab finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Erstellen Sie einen Erkennungszeitplan für die Ausführung in LRZs.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**an.
2. Klicken Sie auf die Schaltfläche **Cloud Discovery**.
3. Wählen Sie im Feld **Provider** die Option **OCI** aus. Füllen Sie das Formular aus, um ein neues Konto zu erstellen, oder wählen Sie ein vorhandenes Konto aus. Weitere Informationen finden Sie unter Erstellen Sie OCI-Service-Accounts.
4. Filtern Sie auf der Seite **Rechenzentren auswählen**, für welche LZRs Sie die Erkennung ausführen möchten.
5. Wählen Sie auf der Seite **Virtuelle Computer erkennen (optional)** aus, ob Sie die Erkennung von Betriebssystemen für virtuelle Computer ausführen möchten.
6. Wenn Sie fertig sind, navigieren Sie zur Seite **Zeitplan erstellen**, und klicken Sie auf die Schaltfläche **Beenden und ausführen.**

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Oracle-Konfigurationsdaten umfassen die folgenden Tabellen und Felder.

Feld	Beschreibung
Cloud-Datenbank (cmdb_ci_cloud_database)	
name	Name der Datenbank
object_id	Eindeutiger Bezeichner der Datenbank
operational_status	Betriebsstatus der Datenbank
Lieferant	Der Anbieter: **Oracle**.
Typ	Typ der Oracle-Datenbank
Version	Version der Datenbank
state	Status der Datenbank
Anmerkungen	Das Attribut wird für die Löschstrategie ausgegeben.
install_status	Status der Installation
Image (cmdb_ci_os_template)	
name	Image-Name
object_id	Eindeutiger Bezeichner des Images
Version	Version des Gastbetriebssystems
guest_os	Name des Gastbetriebssystems
Servicekonto (cmdb_ci_cloud_service_account)	
name	Name des Kontos
datacenter_type	Datencenter-Typ.
account_id	Eindeutiger Bezeichner des Kontos
object_id	Eindeutiger Bezeichner des Kontos (gleicher Wert wie die Konto-ID)
discovery_credentials	Anmeldeinformationen im Zusammenhang mit dem Servicekonto
is_master_account	**true**, wenn es sich um das Stamm-Compartment handelt. **false**, wenn es sich nicht um das Stamm-Compartment handelt.
Netzwerk (cmdb_ci_network)	
name	Name des Netzwerks
object_id	Eindeutiger Bezeichner des Netzwerks
cidr	CIDR des Netzwerks
domain_name	Name der Domäne
state	Status des Netzwerks
NIC (cmdb_ci_nic)	
name	NIC-Name
object_id	Eindeutiger Bezeichner der NIC

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
public_ip	Öffentliche IP-Adresse
mac_address	MAC-Adresse
Primär	Legen Sie entsprechend der Konfiguration **true**/**false** fest.
private_ip	Private IP-Adresse
state	Status der NIC
Speichervolume (cmdb_ci_storage_volume)	
name	Name des Speichervolume.
object_id	Eindeutiger Bezeichner des Speichervolume
state	Status des Speichervolume
volume_id	Eindeutiger Bezeichner des Speichervolume (gleicher Wert wie Konto-ID)
size	Größe des Speichervolume
size_bytes	Größe des Speichervolume in Byte
Subnetz (cmdb_ci_cloud_subnet)	
name	Name des Subnetzes
object_id	Eindeutiger Bezeichner des Subnetzes
cidr	CIDR des Subnetzes
domain_name	Name der Domäne
state	Status des Subnetzes
Virtuelle Maschine (cmdb_ci_vm_instance)	
name	Name der VM
object_id	Eindeutiger Bezeichner der VM
state	Status der VM
memory	Größe des Arbeitsspeichers
CPUs	Anzahl an CPUs

Tags werden in die Tabelle **cmdb_key_value** eingetragen und beziehen sich auf die relevante CMDB-CI-Ressource. Um dies zu unterstützen, wurden Erweiterungsabschnitte für die folgenden Ressourcen erstellt:

- Autonomous DB
- Exadata-DB
- Bild
- Netzwerk
- NIC
- Speicher-Laufwerk
- Account
- Subnetz
- Virtueller Computer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Oracle OCI - Availability Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Enthält::Enthalten in	cmdb_ci_availablity_zone

Beziehungen, die mithilfe des Musters „Oracle OCI - Block (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_block
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume

Beziehungen, die mithilfe des Musters „Oracle OCI - Fault Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone

Hinweis: Wenn Sie für einen Teil der LZRs einen Cloud Discovery-Zeitplaner konfigurieren, wird das Muster „Oracle OCI - Fault Domain (LP)“ nicht ausgelöst.

Beziehungen, die mithilfe des Musters „Oracle OCI - Image (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - LDC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Beziehungen, die mithilfe des Musters „Oracle OCI - Network (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen, die mithilfe des Musters „Oracle OCI - NIC Attachment (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_subnet
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vnic
cmdb_ci_endpoint_vnic	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_nic
cmdb_ci_cloud_subnet	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_endpoint_subnet

Beziehungen, die mithilfe des Musters „Oracle OCI - NIC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - Storage Volume (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_availablity_zone	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet

Beziehungen, die mithilfe des Musters „Oracle OCI - Virtual machine (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_oci_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_vm_instance	DR bereitgestellt von::Stellt DR bereit für	cmdb_ci_avaliability_zone
cmdb_ci_avaliability_zone	Enthält::Enthalten in	cmdb_ci_vm_instance

OpenStack-Ressourcenerkennung

Die ServiceNow Discovery-Anwendung verwendet OpenStack-Ressourcen-Erkennungsmuster, um OpenStack-Ressourcen über REST API-Aufrufe zu finden. Um einige dieser Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Discovery Verwendet OpenStack-Ressourcen-Discovery-Muster, um eine horizontale Discovery auszuführen.

Beginnend mit Muster für Discovery und Service-Mapping Store-Release August 2024. OpenStack-Ressourcen-Discovery-Muster unterstützen sowohl die private als auch die öffentliche Cloud-Discovery.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

OpenStack-Anforderungen

- Suchen Sie im OpenStack Identity-Servicekatalog die Zugriffs-URL, die als OpenStack Identity-Service-Endpunkt verwendet wird. Beispiel: https://<openstack dns>:<port>.
- Konfigurieren Sie einen OpenStack-Anwender mit Berechtigungen zum Generieren eines Projektbereichstoken. Zum Generieren eines Tokens ist das Festlegen der Werte „Domänen-ID“, „Anwendername“, „Projektname“ und „Passwort“ erforderlich.

MID Server-Anforderungen

Stellen Sie einen dedizierten MID-Server für Cloud-Erkennung bereit und verbinden Sie ihn.

Der dedizierte MID-Server muss Zugriff auf OpenStack und einen offenen Port haben, damit jeder OpenStack-Service erkannt werden kann.

Anmeldeinformationen

Auf der ServiceNow AI Platform, Erstellen Sie OpenStack-Anmeldeinformationen für ServiceNow Cloud-Service-Account. Geben Sie die Werte für Domänen-ID, Anwendername, Projektname und Passwort ein, die Sie in OpenStack-Anforderungen konfiguriert haben. Weitere Informationen finden Sie unter Anmeldeinformationen erstellen und testen .

Servicekonto

Auf der ServiceNow AI Platform, Konfigurieren Sie ein ServiceNow Cloud-Service-Account mit den erstellten OpenStack-Anmeldeinformationen und den OpenStack-Rechenzentrumsdetails. In **Account-Id** Feld die Projekt-ID des zu erkennenden OpenStack-Projekts angeben.

Erkennungszeitpläne erstellen

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Erstellen Sie einen automatischen Discovery-Zeitplan für OpenStack-Service-Accounts – nur für private Cloud

Erstellen Sie einen automatischen serverlosen Discovery-Zeitplan für OpenStack-Servicekonten mithilfe des Musters OpenStack – Servicekonten erkennen. Weitere Informationen finden Sie unter Zeitplan für automatische Cloud-Discovery für offenen Stapel [KB1638685] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen der OpenStack-Ressourcen-Discovery-Muster.

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Objekt-ID [object_id]	Server-UUID
Name [name]	Servername
Status [status]	Serverstatus
Beschreibung [short_description]	(Optional) Serverbeschreibung
CPUs [cpus]	Anzahl der virtuellen CPUs (vCPUs) aus der Variante, mit der die VM-Instanz bereitgestellt wird.
Datenträger [Datenträger]	Anzahl aller von Cinder verwalteten Volumes, die von der VM-Instanz zurückgegeben werden.
Datenträgergröße (GB) [Disk_size]	Gesamtmenge aller von Cinder verwalteten Volumes, die von der VM-Instanz verwendet werden, gemessen in Gigabyte (GB).
Arbeitsspeicher (MB) [Arbeitsspeicher]	Die **RAM** Wert aus der Variante, mit der die VM-Instanz bereitgestellt wird, gemessen in Megabyte (MB).
Netzwerkadapter [nics]	Anzahl der eindeutigen Schnittstellen, die in der VM-Instanz konfiguriert sind.
Status [state]	Zugeordneter Statuswert, der für die VM-Instanz zurückgegeben wird. Die OpenStack-Server-Status Und ihre zugehörigen ServiceNow **Status** Werte sind: • AKTIV: Ein • GERETTET: Am • ANGEHALTEN: Angehalten • ANGEHALTEN: Aus • GESTOPPT: Aus • SOFT_DELETED: Beendet • HARD_DELETED: Beendet • GRÖSSE GEÄNDERT: Aus • FEHLER: Fehler • INITIALISIERT: Wird gestartet Für beliebig **Status** Wert nicht aufgeführt, der Standardwert ist aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Schlüsselpaare [cmdb_ci_cloud_key_pair]

Feld	Beschreibung
Objekt-ID [object_id]	Schlüsselpaar-UUID
Name [name]	Schlüsselpaarname, der zum Verweisen verwendet wird
Fingerabdruck [finger_print]	Schlüsselpaar-Fingerabdruck

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Objekt-ID [object_id]	ID des Lastenausgleichsmoduls
Name [name]	Visuell lesbarer Ressourcenname
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus

Lastenausgleichsmodul-Listener [cmdb_ci_lb_listener]

Feld	Beschreibung
Objekt-ID [object_id]	Listener-ID
Name [name]	Visuell lesbarer Name der Ressource
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Listener-Protokoll [listener_Protocol]	Protokoll für die Ressource. Entweder HTTP, HTTPS, TCP, TERMINATED_HTTPS oder UDP
Listener-Port [listener_Port]	Protokollportnummer für die Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Objekt-ID [object_id]	Pool-ID
Name [name]	Visuell lesbarer Ressourcenname
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer-Pool [cmdb_ci_lb_pool] (Fortsetzung)

Feld	Beschreibung
Lastenausgleichsmethode [load_balancing_method]	Lastenausgleichsalgorithmus für den Pool. Einer der folgenden Werte: LEAST_CONNECTIONS, ROUND_ROBIN, SOURCE_IP oder SOURCE_IP_PORT

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Objekt-ID [object_id]	Poolmitglieds-ID
Name [name]	Visuell lesbarer Ressourcenname
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
IP-Adresse [ip_address]	Back-End-Mitgliedsserver-IP-Adresse

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Objekt-ID [object_id]	Volume-UUID
Name [name]	Volumename
Status [status]	Volumestatus
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Speichertyp [storage_type]	Zugeordneter Volumetyp

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Feld	Beschreibung
Objekt-ID [object_id]	Volume-UUID
Name [name]	Volumename
Status [status]	Volumestatus
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Image [cmdb_ci_os_template]

Feld	Beschreibung
Objekt-ID [object_id]	Benutzerdefinierte Image-UUID
Name [name]	Image-Name. Der Wert kann null sein (der JSON-Null-Datentyp).
Status [status]	Image-Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Netzwerk [cmdb_ci_network]

Feld	Beschreibung
Objekt-ID [object_id]	Netzwerk-ID
Name [name]	Visuell lesbarer Netzwerkname
Betriebsstatus [operational_status]	Netzwerkstatus. Mögliche Werte: ACTIVE, DOWN, BUILD oder ERROR
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Cloud-Subnetz [cmdb_ci_cloud_subnet]

Feld	Beschreibung
Objekt-ID [object_id]	Subnetz-ID
Name [name]	Visuell lesbarer Ressourcenname
DHCP aktiviert [is_dhcp_enabled]	Ob DHCP für das Subnetz aktiviert oder deaktiviert ist
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Feld	Beschreibung
Objekt-ID [object_id]	Sicherheitsgruppen-ID
Name [name]	Visuell lesbarer Ressourcenname
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Sicherheitsgruppenregel [cmdb_ci_compute_security_group_rule]

Feld	Beschreibung
Name [name]	Dieses Feld hat den gleichen Wert wie das Feld object_id.
Objekt-ID [object_id]	Sicherheitsgruppenregel-ID
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Ethertyp [ethertype]	EtherType Muss IPv4 oder IPv6 sein. In CIDR dargestellte Adressen müssen den Eingangs- oder Ausgangsregeln entsprechen.
Portbereich max. [port_range_max]	Der letzte Port des Bereichs, für den die Regel gilt. Dieser Wert ist die maximale Portnummer in dem Bereich, der der Sicherheitsgruppenregel entspricht. • Wenn das Protokoll TCP, UDP, DCCP, SCTP oder UDP-Lite ist, muss dieser Wert größer oder gleich dem Attributwert port_range_min sein. • Wenn das Protokoll ICMP ist, muss dieser Wert ein ICMP-Code sein.
Portbereich min. [port_range_min]	Der erste Port des Bereichs, für den die Regel gilt. Dieser Wert ist die minimale Portnummer in dem Bereich, der der Sicherheitsgruppenregel entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsgruppenregel [cmdb_ci_compute_security_group_rule] (Fortsetzung)

Feld	Beschreibung
	• Wenn das Protokoll TCP, UDP, DCCP, SCTP oder UDP-Lite ist, muss dieser Wert kleiner oder gleich dem Attributwert port_range_max sein. • Wenn das Protokoll ICMP ist, muss dieser Wert ein ICMP-Typ sein.

OpenStack-Domäne [cmdb_ci_cloud_openstack_domain]

Feld	Beschreibung
Objekt-ID [object_id]	Domänen-ID
Name [name]	Domänenname
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Aktiviert [enabled]	Definiert, ob die Domäne aktiviert oder deaktiviert ist. • „True“ – Die Domäne ist aktiviert. • „False“ – Die Domäne ist deaktiviert.

OpenStack-Service [cmdb_ci_cloud_openstack_service]

Feld	Beschreibung
Objekt-ID [object_id]	Service-ID
Name [name]	Servicename
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Typ [type]	Servicetyp. Beschreibt die vom Service implementierte API. Mögliche Werte: Berechnen, EC2, Identität, Image, Netzwerk oder Volume
Katalog aktiviert [enabled]	Definiert, ob der Service und seine Endpunkte im Servicekatalog angezeigt werden. • True – Der Service und seine Endpunkte werden im Servicekatalog angezeigt. • False – Der Service und seine Endpunkte werden nicht im Servicekatalog angezeigt.

OpenStack-Endpunkt [cmdb_ci_Cloud_openstack_Endpoint]

Feld	Beschreibung
Objekt-ID [object_id]	Endpunkt-ID
Name [name]	Servicename
Schnittstelle [interface]	Schnittstellentyp, der die Sichtbarkeit des Endpunkts beschreibt. Mögliche Werte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OpenStack-Endpunkt [cmdb_ci_Cloud_openstack_Endpoint] (Fortsetzung)

Feld	Beschreibung
	• Öffentlich – Für Endbenutzer auf einer öffentlich verfügbaren Netzwerkschnittstelle sichtbar • Intern – Für Endbenutzer auf einer nicht zertifizierten internen Netzwerkschnittstelle sichtbar • Administrator – Für Administratoren auf einer sicheren Netzwerkschnittstelle sichtbar
Katalog aktiviert [enabled]	Definiert, ob der Service und seine Endpunkte im Servicekatalog angezeigt werden. • True – Der Service und seine Endpunkte werden im Servicekatalog angezeigt. • False – Der Service und seine Endpunkte werden nicht im Servicekatalog angezeigt.

Cloud-Hardwaretyp [cmdb_ci_Cloud_Hardware_type]

Feld	Beschreibung
Name [name]	Die **Name** Feld der OpenStack-Variante.
Objekt-ID [object_id]	Die **id** Feld der OpenStack-Variante.
VCPUs [vcpus]	Die **vcpus** Feld der OpenStack-Variante.
Arbeitsspeicher MB [Memory_mb]	Die **RAM** Feld der OpenStack-Variante.
Lokaler Speicher – GB [local_storage_gb]	Die **Datenträger** Feld der OpenStack-Variante.

Die erkannten Daten enthalten die Tabelle „OpenStack-Hypervisor-Ansicht“ [cmdb_ci_openstack_Hypervisor_View] und ihre Felder nur für private Cloud.

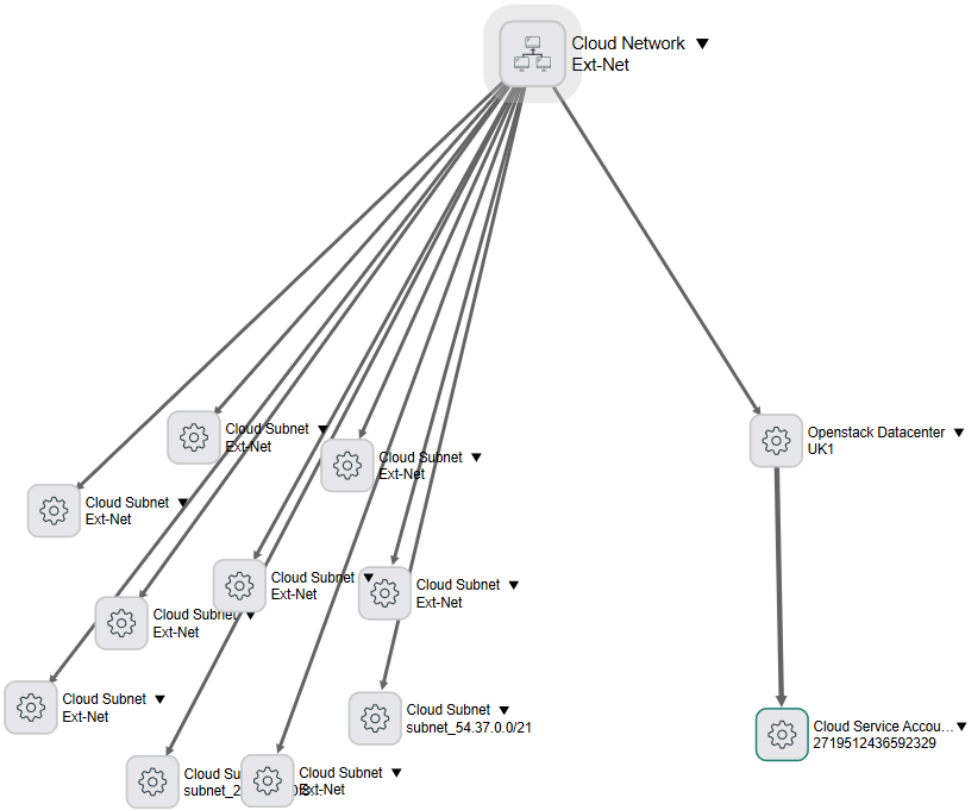
OpenStack-Hypervisor-Ansicht [cmdb_ci_openstack_Hypervisor_View] Tabellenfelder

Feld	Beschreibung
Name [name]	Verketteter Wert von **Hypervisor_type** Und **Hypervisor_hostname** Felder. Beispiel: QEMU@host.acmecorp.com.
IP-Adresse [ip_address]	Der Wert von **Host_ip** Feld.
Hypervisor-Technologie [Hypervisor_Technology]	Der Wert von **Hypervisor_type** Feld.
Objekt-ID [object_id]	Der Wert von **id** Feld.
Status [state]	Der Wert von **status** Feld.
Version [version]	Der Wert von **Hypervisor_Version** Feld.

Die Zuordnung „Abhängigkeitsansichten“ zeigt alle erkannten OpenStack-Ressourcen in Ihrer Organisation, die über REST-API-Aufrufe verfügbar sind, und die Beziehungen zwischen ihnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

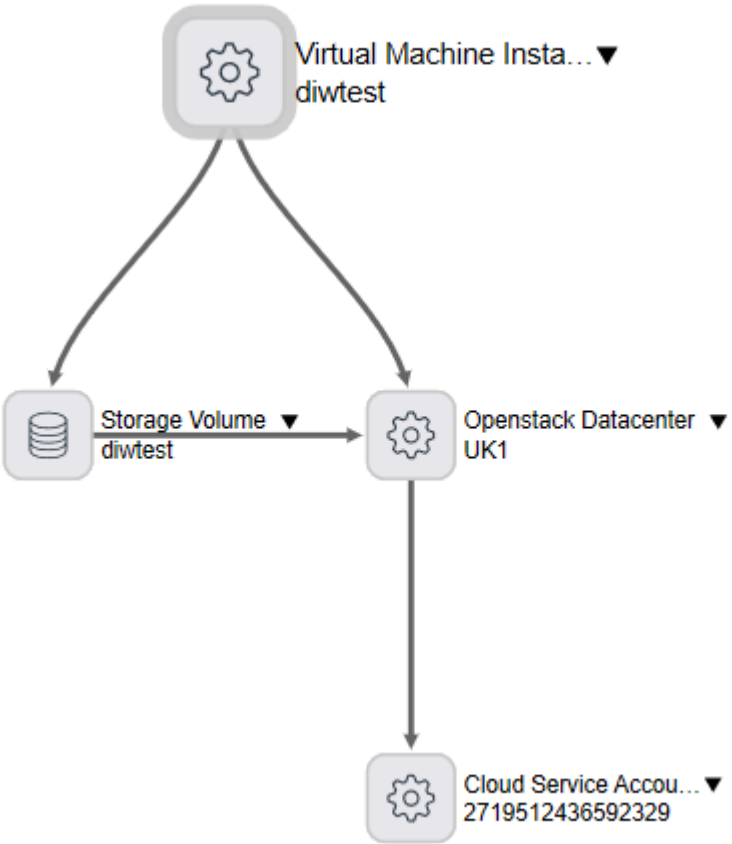
OpenStack-Netzwerkabhängigkeit



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OpenStack-VM-Abhängigkeit



CI-Beziehungen

Die in der folgenden Tabelle aufgeführten Beziehungen werden erstellt, um die OpenStack-Ressourcen-Discovery zu unterstützen.

CI	Beziehung	CI
cmdb_ci_openstack_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_openstack_service	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_openstack_endpoint	Endpunkt verwenden bis::Endpunkt verwenden ab	cmdb_ci_cloud_openstack_service
cmdb_ci_cloud_openstack_endpoint	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_cloud_openstack_domain	Eigentümer von::Eigentum von	cmdb_ci_cloud_service_account
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_compute_security_group	Enthält::Enthalten in	cmdb_ci_compute_security_group_rule
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_listener
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_vm_instance	Verwendet::Verwendet von	cmdb_ci_storage_volume
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_storage_vol_snapshot	Bereitgestellt von::Bereitgestellt	cmdb_ci_storage_volume
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_vm_instance	Virtualisiert von::Virtualisiert	cmdb_ci_server

Die in der folgenden Tabelle aufgeführten Beziehungen werden erstellt, um die OpenStack-Ressourcen-Discovery nur in der privaten Cloud zu unterstützen.

CI	Beziehung	CI
cmdb_ci_vm_instance	Registriert auf::Hat sich registriert	cmdb_ci_openstack_Hypervisor_View
cmdb_ci_openstack_Hypervisor_View	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_openstack_Hypervisor_View	Verwendet::Hosts verwendet von	cmdb_ci_server

Musterdesigner und zugehörige Anwendungen konfigurieren

Installieren Sie die neuesten verfügbaren Versionen der ServiceNow-Anwendungen, um die neuesten Discovery-Muster zu verwenden.

Von der Anwendung Musterdesigner (com.snc.pattern.designer) wird die Benutzeroberfläche zum Erstellen oder Anpassen von Discovery-Mustern bereitgestellt. Musterdesigner wird automatisch mit Discovery oder Service-Mapping installiert. Die Muster selbst werden mit dedizierten Musteranwendungen veröffentlicht.

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

Visibility Content (sn_pattern_design)

Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Sie können die neuesten verfügbaren Versionen der Musteranwendungen aus dem ServiceNow Store installieren. Alternativ können Sie diese Anwendungen als Plugins auf Ihrer Instanz von ServiceNow installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugins auf darin enthaltene erforderliche Muster überprüfen

Da ServiceNow Discovery-Muster mithilfe von zwei verschiedenen Plugins veröffentlicht, müssen Sie möglicherweise überprüfen, welches Plugin installiert oder aktualisiert werden soll.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

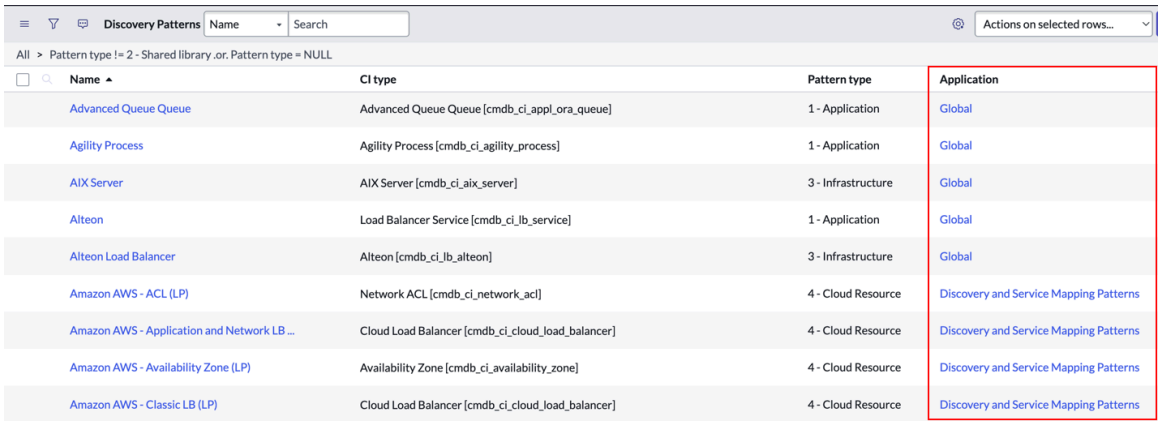
Visibility Content (sn_pattern_design)

Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Zeigen Sie die Spalte **Anwendung** an.
   a. Klicken Sie auf **Liste personalisieren**.
   b. Wählen Sie im Dialogfeld „Listenspalten personalisieren“ unter **Verfügbar** die Option **Anwendung** aus, und klicken Sie auf den Rechtspfeil.
3. **Wahlweise:** Sie können gemeinsam genutzte Bibliotheken herausfiltern, um nur Muster in der Liste anzuzeigen.
4. Suchen Sie in der Liste nach dem entsprechenden Muster.
5. Überprüfen Sie, zu welcher Anwendung das Muster gehört.

Global steht für Visibility Content.



Muster für Discovery und Service-Mapping installieren

Sie können die Anwendung Muster für Discovery und Service-Mapping (sn_itom_pattern) installieren, wenn Sie über die Administratorrolle verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie den Eintrag der Anwendung Discovery and Service Mapping Patterns im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Mit Muster für Discovery und Service-Mapping werden mehrere Tabellen installiert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie über die Filterkriterien und die Suchleiste nach der Anwendung Muster für Discovery und Service-Mapping (sn_itom_pattern).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Visibility Content installieren

Sie können die Anwendung Visibility Content (sn_pattern_design) installieren, wenn Sie über die Administratorrolle verfügen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie den Eintrag der Anwendung Visibility Content im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Mit Visibility Content werden mehrere Tabellen installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie über die Filterkriterien und die Suchleiste nach der Anwendung Visibility Content (sn_pattern_design).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Password2-Verschlüsselung für Muster

Das Passwort (Zwei -Way verschlüsselt) Feldtyp wird zum Verschlüsseln und Entschlüsseln von Daten verwendet. Der Feldtyp funktioniert gemäß den NIST 800-57-Richtlinien und bietet FIPS 140-2-L3-Schutz.

Passwort2 ist ein Textfeld, in dem vertrauliche Daten gespeichert werden Zwei -Way-Verschlüsselung. Die Zwei -Wie die Verschlüsselung die Daten als sicheren verschlüsselten Wert speichert, der innerhalb von entschlüsselt werden kann ServiceNow AI Platform Instanz.

Ab Quebec können Sie mit Key Management Framework Schlüssel verwalten, die für Password2-Felder verwendet werden. Auf einer ServiceNow AI Platform mit Release Rome oder höher ist die Implementierung von Password2 jedoch verbindlich vorgeschrieben.

Hinweis: Nur neu erstellte Datensätze mit Passwort2-Feldern sind Zwei -Way verschlüsselt. Vorhandene Daten werden nicht automatisch zur Verwendung der Password2-Verschlüsselung konvertiert.

Password2-Implementierung überprüfen

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.76) installiert ist.

Sicherstellen, dass Password2 in XML-Datensätzen enthalten ist

Zeigen Sie die XML-Datensätze in der ServiceNow AI Platform-Instanz an, und überprüfen Sie, ob die Verschlüsselung diesem Beispiel ähnelt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Typen für Service-Mapping und Discovery erstellen

Erstellen Sie CI-Typen (oder CI-Klassen) für Anwendungen und Geräte, die Service-Mapping und Discovery standardmäßig nicht unterstützen.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin, Personalize_dictionary oder admin

Stellen Sie sicher, dass kein CI-Typ für diese Anwendung oder dieses Gerät vorhanden ist.

Warum und wann dieser Vorgang ausgeführt wird

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden.

Hinweis: Die Discovery- und CMDB-Benutzeroberfläche beziehen sich auf CI-Typen als CI-Klassen.

Ihnen steht eine große Auswahl vorkonfigurierter CI-Typen zur Verfügung, die die am häufigsten verwendeten Anwendungen abdecken. Wenn Ihre Organisation eine weniger bekannte oder eine proprietäre Anwendung verwendet, die über keinen entsprechenden CI-Typ verfügt, müssen Sie ihn erstellen.

Ein CI-Typ ist ein generischer Begriff, der von mehreren ServiceNow-Anwendungen verwendet wird, es gibt jedoch einige spezifische Attribute für Service-Mapping und Discovery.

Ein CI-Typ (oder eine Klasse) enthält mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten. Beispiel:

- CI-Attribute werden den CMDB-Tabellen als Felder hinzugefügt.
- Bezeichner helfen Service-Mapping und Discovery bei der Unterscheidung zwischen neuen und vorhandenen CIs. Wenn beispielsweise in der CMDB ein Apache-Webserver-CI-Typ definiert ist und sowohl Service-Mapping als auch Discovery ein Apache-Webserver-CI erkennen, verarbeitet sie es mit Bezeichnern. Sie erkennt es dann als aktualisierte Version des Apache-Webserver-CI, das bereits im System vorhanden ist, und nicht als neues Apache-Webserver-CI.
- Es gibt Abgleichsregeln , die der ServiceNow-Plattform helfen, CI-Attribute korrekt zu konsolidieren, die aus verschiedenen Anwendungen eingegangen sind. Diese Regeln sind für Organisationen erforderlich, in denen mehr als eine Anwendung Gegenstand des Discovery-Prozesses ist. Abgleichsregeln definieren, wie Attribute desselben CI, die von verschiedenen Erkennungsquellen erkannt wurden, zusammengeführt werden. Zum Beispiel entdeckt Service-Mapping Versions- und Startverzeichnisattribute eines Apache-Webserver-CI, während Discovery die Versions- und Patch-Ebenen-Attribute für das gleiche Apache-Webserver-CI entdeckt. Mit ServiceNow AI Platform wird die Abgleichsregel angewendet, und Service-Mapping überschreibt daher nicht die von Discovery gefundenen Attribute.
- Zugehörige Elemente, sowohl CIs als auch Nicht-CIs, dienen als Referenz und liefern zusätzliche Informationen zum CI. Beispielsweise können Sie eine Seriennummer, einen Port und eine Netzwerk-APR-Tabelle als zugehörige Elemente für einen Hardwareserver definieren. Diese Elemente werden vom System nicht zur Identifizierung verwendet. Nachdem Sie zugehörige Elemente für den CI-Typ konfiguriert haben, können Sie die Horizontal-Discovery für CIs dieses Typs zusammen mit den zugehörigen Elementen verwenden. Diesbezügliche Informationen finden Sie unter Zugehörige Elemente zusammen mit dem Haupt-CI erkennen.

  Hinweis: Nicht-CIs sind Elemente, die die Konfigurationselement-Tabelle [cmdb_ci] nicht erweitern. Beispiele für Nicht-CIs sind Ports, Seriennummern oder Netzwerk-ARP-Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet. In diesem Beispiel ist das Apache-Webserver-CI dem Webserver-CI untergeordnet und leitet viele Attribute vom übergeordneten Element ab, z. B. Name, Version, Modell-ID. Standardmäßig übernehmen untergeordnete CI-Klassen Bezeichner von ihren übergeordneten CI-Klassen.

Zusätzlich zu diesen CI-Typ-Definitionen verwendet der horizontale Erkennungsprozess eine CI-Klassifizierung, um zu definieren, zu welchem CI-Typ ein CI gehört. Erstellen Sie eine Geräte-CI-Klassifizierung, wenn Sie einen CI-Typ für Geräte mit SNMP und eine Prozess-CI-Klassifizierung für einen Anwendungs-CI-Typ erstellen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**an.
2. Wenn Sie einen vorhandenen CI-Typ als übergeordnetes Element für den neuen CI-Typ verwenden möchten, klicken Sie auf **Hierarchie**, um die Liste der CI-Klassen anzuzeigen.
3. Klicken Sie auf das Kontextmenü für den erforderlichen CI-Typ und wählen Sie **Untergeordnete Klasse hinzufügen** aus.
4. Eine Tabelle erstellen So speichern Sie die CI-Typattribute:

Formular „Neue Tabelle“

Feld	Beschreibung
Bezeichnung	Name des CI-Typs. Beispiel: Apache-Webserver
Name	Der Tabellenname. Beispiel: cmdb_ci_apache_web_server. Verwenden Sie einen Namen, der den anderen CMDB-Klassen ähnlich ist (z. B. `u_cmdb_ci_laptop`).
Erweitert Tabelle	Der Tabellenname des übergeordneten CI-Typs. Alle CI-Typen sind Erweiterungen der Konfigurationselement-Tabelle [cmdb_ci] oder ihrer untergeordneten Tabellen. Beispiel: Wenn die neue Klasse Laptops ist, was eine Unterklasse von Computern ist, wählen Sie die Tabelle cmdb_ci_computer aus. Wenn die neue Klasse eine Klasse der obersten Ebene ist, wählen Sie die Tabelle cmdb_ci aus. Die am häufigsten verwendeten übergeordneten CI-Typen sind: ◦ cmdb_ci - Standard ◦ cmdb_ci_database - für Datenbanken ◦ cmdb_ci_app_server - für Anwendungsserver ◦ cmdb_ci_infra_service - für Infrastrukturservices ◦ cmdb_ci_endpoint_inclusion - für Einstiegspunkte des Integrationstyps ◦ cmdb_ci_appl - für Anwendungen ◦ cmdb_ci_web_server - für Webserver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ cmdb_ci_lb - für Lastenausgleichsmodule ○ cmdb_ci_endpoint - für Einstiegspunkte

5. Konfigurieren Sie, wie die Instanz bestimmt, ob ein erkanntes CI ein aktualisiertes CI in der Instanz oder ein brandneues CI ist.
Die Einzelheiten des Verfahrens finden Sie unter CI-Identifizierungsregel erstellen oder bearbeiten .

> ⚠ **Warnung:** Wenn keine CI-Identifizierungsregel für einen CI-Typ vorhanden ist, erkennt Service-Mapping CIs, die zu diesem Typ gehören, kann die Ergebnisse des Erkennungsprozesses jedoch nicht interpretieren. In diesem Fall lehnt ServiceNow AI Platform die Erkennungsergebnisse für diese CIs ab, und ihre Informationen werden nicht aktualisiert.

a. Konfigurieren Sie auf der Seite **Bezeichner** die Parameter wie folgt:

Bezeichner-Formular

Feld	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen an.
Betrifft	Geben Sie den CI-Typ ein.
Aktiv	Aktivieren Sie das Kontrollkästchen .
Unabhängig	Deaktivieren Sie das Kontrollkästchen .

b. Konfigurieren Sie die Bezeichner-Eintragsparameter wie folgt:

Bezeichnereintrags-Formular

Feld	Beschreibung
Kriteriumsattribute	Wählen Sie das Attribut aus, das Sie zum Identifizieren des CI verwenden möchten. Beispielsweise **Klasse**, **Installationsverzeichnis** oder **Seriennummer**.
Null-Attribut unterstützen	Aktivieren Sie das Kontrollkästchen .
Priorität	Wenn mehr als ein Bezeichnet-Eintrag vorhanden ist, fügen Sie die Priorität hinzu, um die Reihenfolge zu bestimmen, in der Service-Mapping diese Einträge anwendet. Wenn keines der Identifizierungskriterien mit dem erkannten CI übereinstimmt, ist dieses CI neu.

6. **Wahlweise:** Konfigurieren Sie Verweise auf andere CIs oder Nicht-CIs als zugehörige Elemente für den CI-Typ.

Formular „Zugehörige Einträge“

Feld	Beschreibung
Aktiv	Kontrollkästchen, das angibt, dass der zugehörige Eintrag aktiv ist.
Zugehörige Tabelle	Eine zugehörige Tabelle, die auf das CI verweist, das abgeglichen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Referenziertes Feld	Ein referenziertes Feld in der **Zugehörigen Tabelle**, das das referenzierte CI speichern soll. Dieses Feld verweist immer auf die Tabelle „cmdb_ci“ oder auf eine untergeordnete Tabelle der Tabelle „cmdb_ci“.
Priorität	Priorität des zugehörigen Eintrags für die angegebene **Zugehörige Tabelle**. Regeln mit niedrigeren Prioritätszahlen werden bei der Abgleichung eines zugehörigen Elements mit einer bestimmten zugehörigen Tabelle mit höherer Priorität behandelt. Zugehörige Einträge für die angegebene zugehörige Tabelle von identischer Priorität werden nach dem Zufallsprinzip angewendet. Sie können zwischen den Prioritätszahlen Lücken lassen, um die Zuweisung ungenutzter Zahlen für neue Einträge zu ermöglichen, ohne die bestehende Prioritätsreihenfolge verändern zu müssen.
Kriteriumsattribute	Der Satz von Attributen, um das zugehörige Element eindeutig zu identifizieren. Attribute gehören entweder zu der aktuellen Klasse oder einer übergeordneten Klasse. **Hinweis:** Das Hinzufügen von Referenzfeldern als Kriteriumsattribute ist möglich. Solche Felder sind jedoch möglicherweise nicht immer wirksam: ○ In Referenzfeldern werden *sys_id*s gespeichert, die auf einen Datensatz in einer anderen Tabelle verweisen. Somit gelten Referenzfelder (bezüglich der Eindeutigkeit) als schwache Kriteriumsattribute für die aktuelle Tabelle. ○ Vom System werden ungültige Werte in einem Referenzfeld erkannt und dann durch „Unbekannt“ ersetzt. Beispielsweise wird ein ungültiger Wert für *Model ID* durch den Wert „Unbekannt“ ersetzt. Wenn für mehrere CIs dasselbe Referenzfeld auf „Unbekannt“ festgelegt ist, werden diese CIs auch zu doppelten CIs. Wählen Sie das Schlosssymbol aus, um Attribute der Identifizierungsregel anzuzeigen, hinzuzufügen oder daraus zu entfernen.
Null-Attribut unterstützen	Wenn mindestens ein Kriteriumsattribut in der zugehörigen Tabelle nicht null ist, lassen Sie den Versuch zu, eine Übereinstimmung mit einem Bezeichner-Eintrag zu erzielen, selbst wenn Kriteriumsattribute vorliegen, die null sind.
Filterbedingungen	Fügen Sie Bedingungen hinzu, um einen Filter zum Eingrenzen der Datensätze zu erstellen, die nach einem übereinstimmenden zugehörigen Element durchsucht werden.

7. **Wahlweise:** Konfigurieren Sie die Instanz so, dass CI-Attribute aus verschiedenen Datenquellen korrekt konsolidiert werden.
Siehe CI-Abgleichregeln erstellen oder bearbeiten .

Konfigurieren Sie Folgendes Service-Mapping Zugehörige Parameter korrekt:

Abgleichsdefinitions-Formular

Feld	Beschreibung
Datenquelle	Wählen Sie ServiceWatch.
Betrifft	Wählen Sie den entsprechenden CI-Typ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Optionale Bedingung	Legen Sie ggf. eine Bedingung fest.

Hinweis: Wenn Sie keine CI-Abgleichsregel erstellen, werden von Mustern erkannte Daten zum Aktualisieren von CI-Attributen verwendet.

8. Konfigurieren Sie die CI-Klassifizierung für Ihren CI-Typ:
   - Führen Sie für CI-Typen, die Anwendungen darstellen, die Konfiguration wie in Discovery-Prozessklassifizierung erstellen beschrieben aus.
   - Führen Sie für CI-Typen, die SNMP-Geräte darstellen, die Konfiguration gemäß der Beschreibung in Discovery-CI-Klassifizierung erstellen durch.

   Hinweis: CI-Klassifizierungen für Hosts müssen nicht erstellt werden, da diese Klassifizierungen im Basissystem enthalten sind.

9. Definieren Sie für CI-Typen, die Einschlüsse darstellen, die Hierarchie für den neuen CI-Typ.

   Deaktivieren Sie während dieser Konfiguration das Kontrollkästchen **Beziehungsrichtung umkehren**.

   Siehe Abhängige Beziehungen erstellen .

10. Passen Sie bei Bedarf die Symbole an, die CIs in Zuordnungen darstellen.
    Siehe Kartensymbole erstellen oder ändern .

Einstiegspunkttypen für Service-Mapping erstellen

Ein Einstiegspunkt ist ein Punkt, an dem Clients auf eine Serviceinstanz zugreifen. Service-Mapping startet den Zuordnungsprozess für jeden Anwendungsservice ab dem Einstiegspunkt, den Sie dafür definieren. Service-Mapping beinhaltet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die die am häufigsten verwendeten Anwendungen abdecken. Wenn Ihre Organisation eine weniger bekannte oder eine proprietäre Anwendung verwendet, die über keinen entsprechenden Einstiegspunkt in Service-Mapping verfügt, müssen Sie ihn erstellen.

Vorbereitungen

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Erforderliche Rolle: Service_Mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Darüber hinaus verwenden Service-Mapping-Muster Einstiegspunkte, um ausgehende CI-Verbindungen zu erkennen und so den Zuordnungsprozess für Einstiegspunkte zu starten.

Einstiegspunkte werden in ServiceNow CMDB als CIs des Endpunkttyps modelliert. Einstiegspunkte werden als Datensätze in den Endpunkttabellen [cmdb_ci_endpoint] gespeichert.

Wie auch andere CI-Typen enthält ein Einstiegspunkt mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CI-Attribute werden den CMDB-Tabellen als Felder hinzugefügt.
- Bezeichner helfen Service-Mapping und Discovery bei der Unterscheidung zwischen neuen und vorhandenen CIs. Beispiel: Wenn in der CMDB mit mehreren Quellen ein Endpunkt-CI-Typ für die Active Directory-Gesamtstruktur definiert ist und Service-Mapping ein Active Directory-Gesamtstruktur-CI erkennt, verarbeitet Service-Mapping dieses CI mit Bezeichnern und erkennt es als aktualisierte Version des vorhandenen Active Directory-Gesamtstruktur-CI im System und nicht als neues Active Directory-Gesamtstruktur-CI.
- CI-Typhierarchie CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet. Erstellen Sie Standardeinstiegspunkte als untergeordnete CIs für den Endpunkt-CI-Typ, wodurch eine Erweiterung für die Tabelle cmdb_ci_endpoint erstellt wird. Erstellen Sie für Einstiegspunkte des Integrationstyps untergeordnete CIs für den CI-Typ des Integrationsendpunkts, der die Tabelle cmdb_ci_endpoint_inclusion erweitert. Bei einer Inklusion hostet ein Server Anwendungen, die als unabhängige Objekte behandelt werden.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**an.
2. Wählen Sie **Offene Hierarchie**.
3. Klicken Sie zum Erstellen eines Standardeinstiegpunkts mit der rechten Maustaste im Fenster **Klassenhierarchie** auf **Endpunkt** und wählen Sie **Untergeordnete Klasse hinzufügen** aus.
4. Klicken Sie zum Erstellen eines Einstiegspunkts des Integrationstyps mit der rechten Maustaste im Fenster **Klassenhierarchie** auf **Inclusion Endpoint** und wählen Sie **Nachfolgeklasse hinzufügen** aus.
5. Definieren Sie die Parameter für den neuen Einstiegspunkttyp wie in beschrieben Erstellen Sie eine CI-Klasse .

Zugehörige Informationen

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

CI-Typen für Service-Mapping und Discovery erstellen

Muster erstellen oder anpassen

Erstellen oder ändern Sie ein Erkennungsmuster, und definieren Sie seine Standardattribute.

Vorbereitungen

Stellen Sie sicher, dass die Anwendung, für die Sie ein Muster erstellen möchten, über einen entsprechenden CI-Typ (Configuration Item) und eine CI-Klassifizierung verfügt. Wenn sich der erforderliche CI-Typ nicht in der Liste befindet, erstellen Sie ihn wie unter CI-Typen für Service-Mapping und Discovery erstellen beschrieben.

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Erforderliche Rolle: pd_admin

Grundkenntnisse in der Programmierung sind wünschenswert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf **Neu**, oder wählen Sie das entsprechende Muster aus der Liste aus.
3. Definieren Sie die Standardmusterattribute auf der Registerkarte **Standard**.

Feld	Beschreibung
Mustertyp	○ Wählen Sie **Anwendung** für ein Anwendungsmuster aus. Es kann sowohl für die Erkennung von oben nach unten von Service-Mapping als auch für die horizontale Erkennung von Discovery verwendet werden. ○ Wählen Sie **Infrastruktur** aus, um ein Infrastrukturmuster für die horizontale Host-Erkennung von Discovery zu verwenden.
Name	Geben Sie den Musternamen ein. Dieser Name muss für dieses Muster eindeutig sein. Verwenden Sie selbsterklärende Namen wie Apache auf Unix-Muster.
CI-Typ	Wählen Sie den CI-Typ aus, den dieses Muster erkennen soll. **Hinweis:** Die Erkennung kann mehrere CIs finden, die zum gleichen CI-Typ gehören.
Betriebssystem [nur für Anwendungsmuster]	Wählen Sie das Betriebssystem aus, das das ausgewählte CI ausführt: ○ Klicken Sie auf **Alle**, wenn das CI auf mehr als einem Betriebssystem ausgeführt wird. Oder ○ Wählen Sie das relevante Betriebssystem aus der Liste aus.
Ausführungsreihenfolge [nur für Anwendungsmuster]	Definieren Sie für ein Anwendungsmuster, das von Service-Mapping verwendet wird, wann das Muster ausgeführt wird. **a.** Wählen Sie die Reihenfolge aus, in der dieses Muster immer ausgeführt wird: ▪ **Vor** ▪ **Nach** **b.** Wählen Sie dann das andere zutreffende Muster aus. Dieses Feld ist nur relevant, wenn ein bestimmtes Muster mit einem anderen Muster verwechselt werden kann. Beispielsweise verfügen IIS- und MS Exchange-Anwendungen über einen HTTP-Einstiegspunkt. MS Exchange verwendet jedoch einige der Komponenten von IIS. Daher kann die Erkennung MS Exchange fälschlicherweise als IIS identifizieren, wenn das IIS-Muster zuerst ausgeführt wurde. Klicken Sie im Feld **Ausführungsreihenfolge** in der MS Exchange-Musterdefinition auf **Vor** und **IIS**, um diesen Fehler zu vermeiden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für dieses Muster an.

4. **Wahlweise:** Wenn Sie ein Anwendungsmuster erstellen, darf dieses Muster vom MID-Server nur ausgeführt werden, wenn der auf einem CI erkannte Prozess mit den Klassifizierungskriterien für dieses Muster übereinstimmt. Wählen Sie dazu **Prozessklassifizierung erzwingen** aus.
   Bei allen vereinfachten Mustern, die aus generischen Anwendungen erstellt werden, ist dieses Attribut aktiviert. Weitere Informationen zum Erstellen der Prozessklassifizierung finden Sie unter Discovery-Klassifizierer.
5. Definieren Sie eine Reihe von Identifizierungsschritten für jede eingehende Verbindung eines Konfigurationselements (Configuration Item, CI), wie in beschrieben KB1698521: Muster erstellen oder anpassen .
6. Erstellen Sie bei Bedarf weitere Identifizierungsabschnitte.
7. Speichern Sie das Muster.
8. **Wahlweise:** Um das Muster zu testen, wählen Sie aus **Debug-Modus** Und geben Sie die IP-Adresse des Hosts ein.
9. Laden Sie die aktualisierte Gruppe von Mustern auf den MID-Server hoch:
   a. Navigieren zu **Discovery** > **MID-Server**an.
   b. Alternativ navigieren Sie zu **Service-Mapping** > **MID-Server**an.
   c. Klicken Sie auf **Mustersynchronisierung mit MID**.

Nächste Maßnahme

Fahren Sie für Anwendungstypmuster mit dem Erstellen eines Verbindungsabschnitts fort, wie im KB-artikel beschrieben KB1698521: Muster erstellen oder anpassen .

Zugehörige Informationen

Cloud-Discovery erkunden

KB0747679: Pre/Post Processing Scripts for patterns (Vor-/Nachverarbeitungsskripts für Muster)

KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung

Zugehörige Elemente zusammen mit dem Haupt-CI erkennen

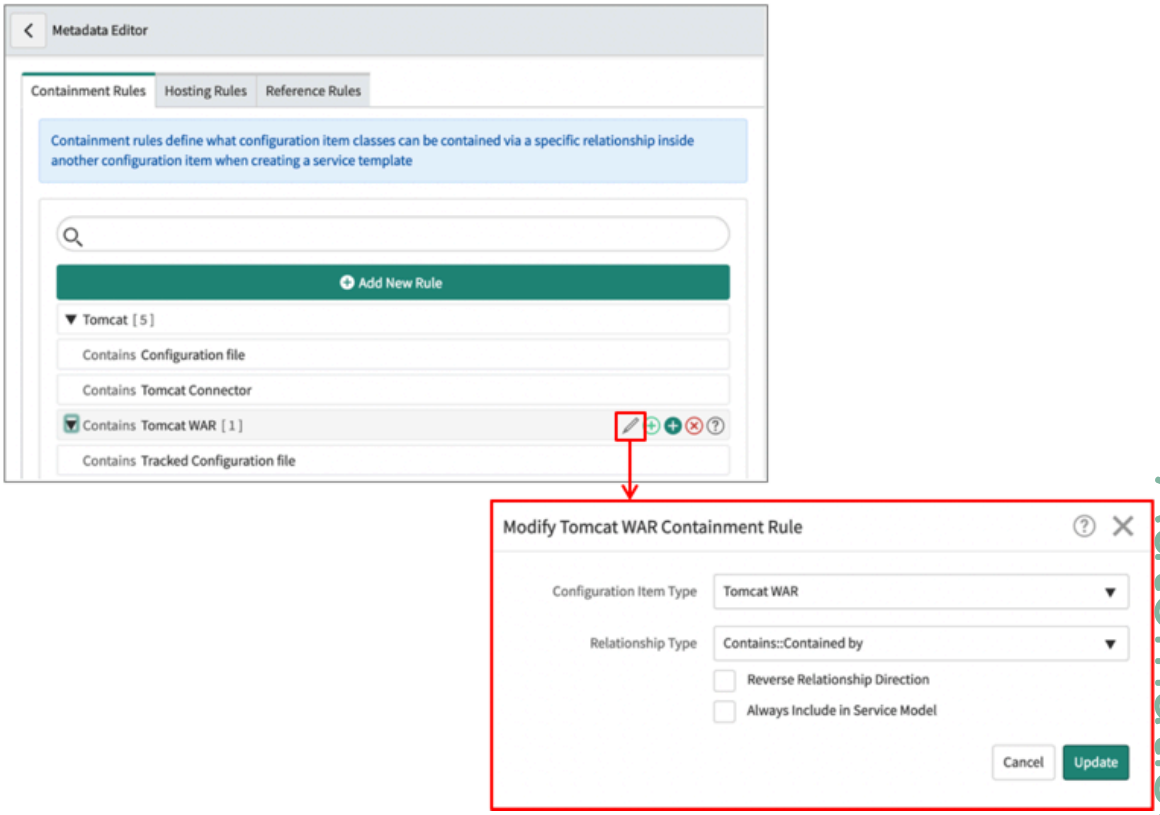
Fügen Sie den Mustern zugehörige Elemente hinzu, um eine horizontale Erkennung von Konfigurationselementen mit allen zugehörigen Elementen durchzuführen: CIs oder Nicht-CIs wie Ports oder Seriennummern.

Vorbereitungen

1. (Optional) Überprüfen Sie, ob das CI abhängig ist: Das System verwendet die Identifizierungsregeln, um das CI unabhängig von anderen CIs zu identifizieren. Siehe Erstellen oder bearbeiten Sie eine CI-Identifizierungsregel .
2. (Optional) Um das Modell besser zu verstehen, überprüfen Sie abhängige Beziehungsregeln, die die Abhängigkeitsstruktur der CI-Typen und die Beziehungstypen in diesen Servicedefinitionen definieren. Beispielsweise können Sie einen Tomcat-Server erkennen, zu dem Tomcat-WARs gehören. Weitere Informationen finden Sie unter Abhängige Beziehungsregeln .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für die Containment-Regel für Tomcat-WAR



3. Um dem Muster ein Nicht-CI hinzuzufügen, fügen Sie es als zugehöriges Element für den CI-Typ hinzu, zu dem das Haupt-CI gehört. Weitere Informationen zum Hinzufügen zugehöriger Elemente für den CI-Typ finden Sie unter Referenzen auf andere CIs oder Nicht-CIs als zugehörige Elemente für den CI-Typ konfigurieren.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Zugehörige Elemente, sowohl CIs als auch Nicht-CIs, dienen als Referenz und liefern zusätzliche Informationen zum CI. Beispielsweise können Sie eine Seriennummer, einen Port und eine Netzwerk-APR-Tabelle als zugehörige Elemente für einen Hardwareserver definieren. Diese Elemente werden vom System nicht zur Identifizierung verwendet. Nachdem Sie zugehörige Elemente für den CI-Typ konfiguriert haben, können Sie die Horizontal-Discovery für CIs dieses Typs zusammen mit den zugehörigen Elementen verwenden.

Hinweis: Nicht-CIs sind Elemente, die die Konfigurationselement-Tabelle [cmdb_ci] nicht erweitern. Beispiele für Nicht-CIs sind Ports, Seriennummern oder Netzwerk-ARP-Tabellen.

Der Musterdesigner zeigt Attribute zugehöriger CI-Typen an, die Sie dem Muster im CI-Attributbereich hinzugefügt haben. Sie können diese Attribute anzeigen und verwenden, während Sie das Haupt-CI-Muster erstellen oder ändern.

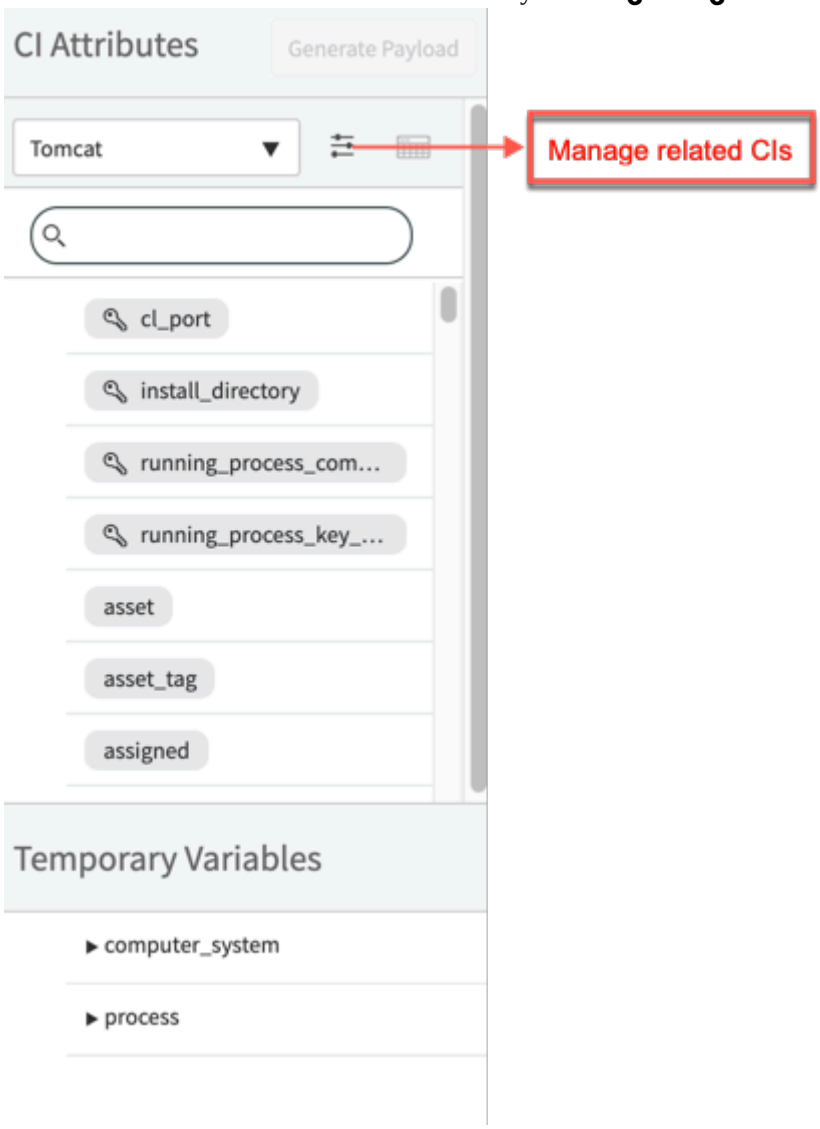
Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Wählen Sie das entsprechende Muster aus.
3. Wählen Sie im Musterformular den entsprechenden Identifikationsteil aus.
4. Stellen Sie sicher, dass Sie sich nicht im Debug-Modus befinden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

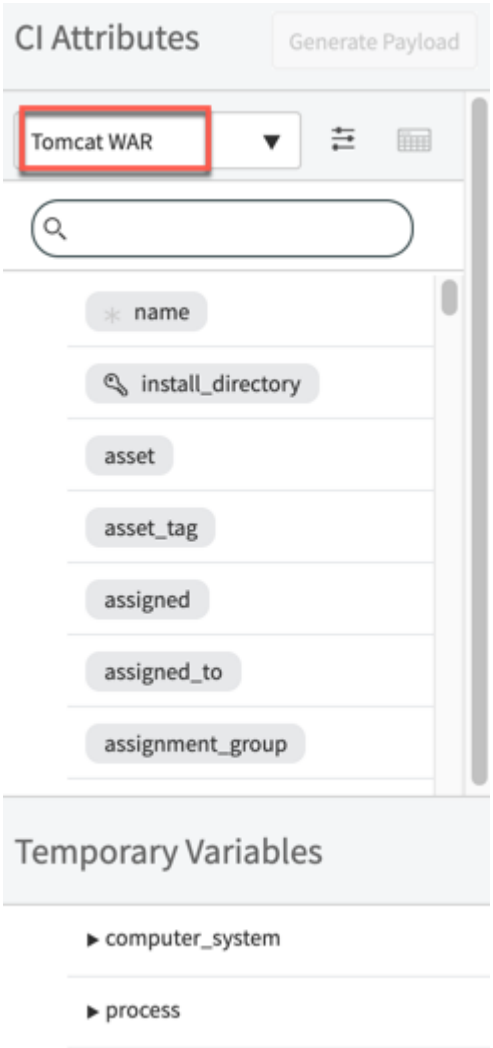
5. Klicken Sie im Bereich **CI-Attribute** auf das Symbol **Zugehörige CIs verwalten**.



6. Wählen Sie den entsprechenden CI-Typ aus.
   Sie können das Suchfeld verwenden, um nach einem bestimmten CI-Typ zu suchen.
7. Klicken Sie auf das Plussymbol.
   Das neue zugehörige Element „CI-Typ“ wird zur Liste hinzugefügt.
8. **Wahlweise:** Fügen Sie andere zugehörige CI-Typen hinzu.
9. Klicken Sie auf **OK**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Registerkarten für zugehörige CI-Typen, die Sie hinzugefügt haben, werden unter der Registerkarte für das Haupt-CI angezeigt:



Nächste Maßnahme
Setzen Sie die Bearbeitung des Musters fort, indem Sie nach Bedarf weitere Schritte hinzufügen. Zum Anzeigen oder Verwenden von Attributen eines zugehörigen CI-Typs klicken Sie im Bereich **CI-Attribute** auf die entsprechende Registerkarte.

Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern

Ermöglichen Sie Mustern die Suche nach zusätzlichen Attributen und ändern Sie die in Identifizierungsabschnitten definierte Mustererkennungslogik mithilfe von Erweiterungsabschnitten. Jeder Erweiterungsabschnitt enthält einen vorkonfigurierten Satz von Erkennungsschritten, die als gemeinsam genutzte Bibliothek bezeichnet werden.

Vorbereitungen
Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Grundkenntnisse in der Programmierung sind wünschenswert.

Erforderliche Rolle: pd_admin

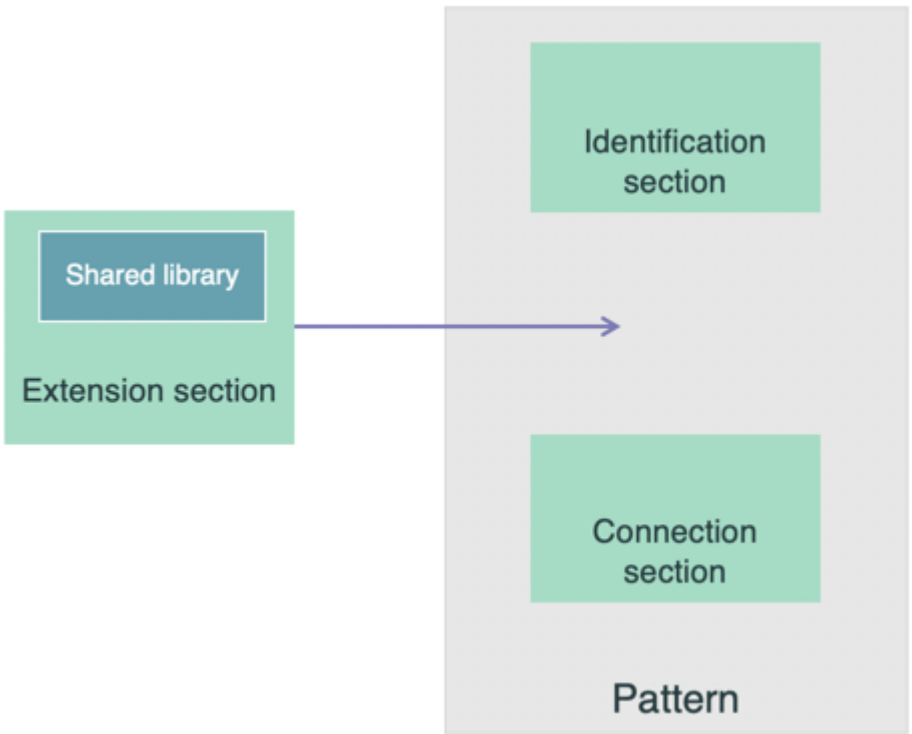
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden. Jedes Muster, einschließlich seiner Identifizierungs- und Verbindungsabschnitte, ist eine einzelne Datei. Es gibt auch wiederverwendbare Sequenzen von Erkennungsschritten, die als gemeinsam genutzte Bibliotheken bezeichnet werden. Jede gemeinsam genutzte Bibliothek ist eine einzelne Datei, sie ist jedoch immer Teil der Infrastruktur oder des Anwendungsmusters und wird nicht als eigenständiges Muster verwendet. Datensätze für Muster und gemeinsam genutzte Bibliotheken befinden sich in der Tabelle „Erkennungsmuster“ [sa_pattern].

Um die Erkennungslogik in Identifizierungsabschnitten zu ändern, ohne die Identifizierungsabschnitte selbst zu ändern, können Sie dem Muster Erweiterungsabschnitte hinzufügen. Jeder Erweiterungsabschnitt besteht aus einer gemeinsamen Bibliothek, entweder neu oder vorhanden.

Erweiterungsabschnitt zu einem Muster hinzufügen



Wenn Sie im Erweiterungsabschnitt eine gemeinsam genutzte Bibliothek erstellen oder ändern, speichern Sie Änderungen nur in der gemeinsam genutzten Bibliothek, nicht am Muster, das diesen Erweiterungsabschnitt enthält.

Warnung: Die Änderungen an der freigegebenen Bibliothek wirken sich auf alle Muster aus, die diese gemeinsam genutzte Bibliothek verwenden.

Der MID-Server führt Erweiterungsabschnitte nach Identifizierungsabschnitten aus und nur, wenn mindestens ein Identifizierungsabschnitt erfolgreich abgeschlossen wurde.

Wenn diesem Muster mehrere Erweiterungsabschnitte zugeordnet sind, definieren Sie die Reihenfolge, in der MID-Server diese Erweiterungsabschnitte ausführt.

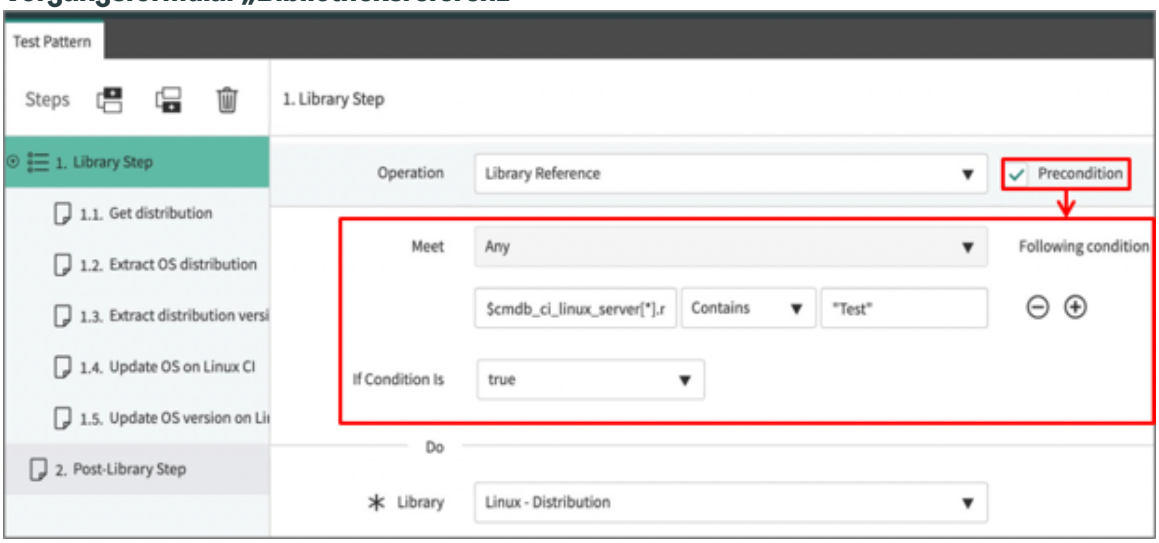
Sie können gemeinsam genutzte Bibliotheken deaktivieren, sodass die verwendeten Muster Schritte in deaktivierten gemeinsam genutzten Bibliotheken überspringen. Weitere Informationen finden Sie unter Discovery Konfigurationskonsole. Wenn eine für einen Schritt der gemeinsamen Bibliothek definierte Vorbedingung nicht erfüllt ist, werden alle Schritte, die zu dieser gemeinsamen Bibliothek gehören, vom Muster

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übersprungen. Beispiel: Wenn die Datei, auf die von der Variable verwiesen wird, nicht „test“ enthält, werden die Schritte 1-1 bis 1-5 der freigegebenen Bibliothek nicht ausgeführt. Die Voraussetzung ist nur für das Muster vorhanden, in dem Sie sie erstellt haben. Die Vorbedingung hat keine Auswirkungen auf andere Muster, von denen diese gemeinsam genutzte Bibliothek genutzt wird.

Vorgangsformular „Bibliotheksreferenz“



Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster** Und öffnen Sie das erforderliche Muster aus der Musterliste.

   Das Muster kann vom Infrastruktur- oder Anwendungstyp sein.

2. So erstellen Sie einen Erweiterungsabschnitt und definieren Erkennungsschritte für die gemeinsam genutzte Bibliothek.

   a. Klicken Sie im **Erweiterungsabschnitt** auf **Neu**.

   b. Geben Sie den Namen dieses Erweiterungsabschnitts ein.

   c. Klicken Sie auf **Erledigt**.
   Das Musterformular zeigt den neuen Abschnitt unter **Erweiterungsabschnitt** an.

   d. Klicken Sie auf den Namen des neuen Erweiterungsabschnitts.

   Der Musterdesigner wird geöffnet und zeigt die Schritte-Struktur auf der linken Seite an.

   Wenn für dieses Muster keine Erkennungsschritte identifiziert wurden, wird der **Schritt ohne Titel** in der Schritte-Struktur im linken Fensterbereich angezeigt.

   e. Definieren Sie Discovery-Schritte.

   f. Klicken Sie auf **Speichern**, um den Erweiterungsabschnitt zu speichern und damit Service-Mapping und Discovery diesen verwenden.
   Sie veröffentlichen keine Erweiterungsabschnitte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. So verwenden Sie eine vorhandene gemeinsam genutzte Bibliothek für den neuen Erweiterungsabschnitt:
   a. Klicken Sie im **Erweiterungsabschnitt** auf **Hinzufügen**.
   b. Wählen Sie die erforderliche gemeinsam genutzte Bibliothek aus der Namensliste aus.
4. Wenn mehrere Erweiterungsabschnitte vorhanden sind, definieren Sie die Reihenfolge, in der MID-Server diese Erweiterungsabschnitte ausführt.
   a. Aktivieren Sie das Kontrollkästchen neben dem Erweiterungsabschnitt.
   b. Klicken Sie im **Erweiterungsabschnitt** auf **Bearbeiten**.
   c. Geben Sie eine neue Ordnungszahl in das Feld **Reihenfolge** ein.
      Wenn nur ein Erweiterungsabschnitt vorhanden ist, ist die Reihenfolge standardmäßig **1**.

      Die Aktion mit der niedrigsten Nummer wird zuerst ausgeführt.
   d. Klicken Sie auf **Erledigt**.

Nächste Maßnahme
Klicken Sie Auf **Debuggen** Zum Ausführen des neu erstellten Erweiterungsabschnitts. Der Musterdesigner führt Erweiterungsabschnitte aus, nachdem Identifizierungsabschnitte ausgeführt wurden.

Muster mithilfe der datenverkehrsbasierten Erkennung optimieren

Als Alternative zum Anpassen des Musters auf der Seite des Musterdesigners verbessern Sie die vorhandenen Muster, damit Service-Mapping sie verwenden kann, um Konfigurationselement-Verbindungen (CIs) zu finden, die zuvor mithilfe der datenverkehrsbasierten Erkennung gefunden wurden.

Vorbereitungen
Erforderliche Rolle: pd_admin

Grundkenntnisse in der Programmierung sind wünschenswert.

Warum und wann dieser Vorgang ausgeführt wird
Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als Traffic-basierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung.

Mithilfe der datenverkehrsbasierten Erkennung erkennt Service-Mapping möglicherweise eine wichtige CI-Verbindung. In diesem Fall können Sie sicherstellen, dass diese Verbindung immer für alle CIs gefunden wird, die zum gleichen CI-Typ gehören. Dazu ändern Sie das Muster, das zum Erkennen von CIs dieses CI-Typs verwendet wird. Ein Muster ist eine Sequenz von Befehlen, die dazu dienen, Attribute eines CI und seiner ausgehenden Verbindungen zu erkennen.

Sie können CI-Konfigurationsdateien durchsuchen, um Daten zu finden, die mithilfe der datenverkehrsbasierten Erkennung ermittelt wurden, z. B. IP-Adresse und Port. Wenn Konfigurationsdateien diese Daten enthalten, erstellen Sie einen Musterschritt, um diese Datei zu analysieren. Wenn Service-Mapping das CI das nächste Mal mit dem geänderten Muster erkennt, extrahiert es die Informationen zu dieser Verbindung direkt aus der Konfigurationsdatei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**an.
2. Klicken Sie Auf **Karte Anzeigen** Neben der relevanten Serviceinstanz.
3. Klicken Sie mit der rechten Maustaste auf das entsprechende CI.
4. Wählen Sie **Traffic-basierte Verbindungen anzeigen**.
   Die Liste der datenverkehrsbasierten Verbindungen wird mit folgenden Informationen angezeigt:

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	○ **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. ○ **Nein** – Wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie Entfernen.

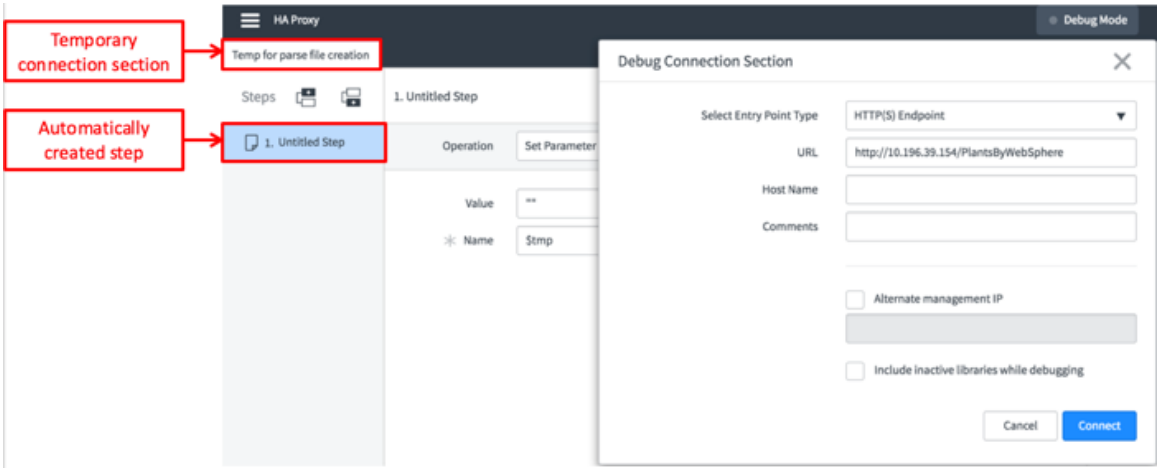
Hinweis: Es kann vorkommen, dass in der Zuordnung datenverkehrsbasierte Verbindungen angezeigt werden, nicht jedoch in der Liste der datenverkehrsbasierten Verbindungen. Dies geschieht für die Verbindungen, die vor weniger als drei Tagen aus der Tabelle TCP Connection [cmdb_tcp] entfernt wurden.

5. Doppelklicken Sie auf die Verbindung, die Sie zum Erstellen eines Musterschritts verwenden möchten.
6. Wenn zur Erkennung dieses CI mehrere Muster verwendet werden, wählen Sie das Muster aus, für das Sie den Schritt erstellen möchten, und klicken Sie auf **OK**.

   Der Musterdesigner erstellt einen vorübergehenden Verbindungsabschnitt für dieses Muster mit einem neuen Schritt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Fenster „Verbindungsabschnitt debuggen“ wird mit teilweise automatisch ausgefüllten Feldern angezeigt.

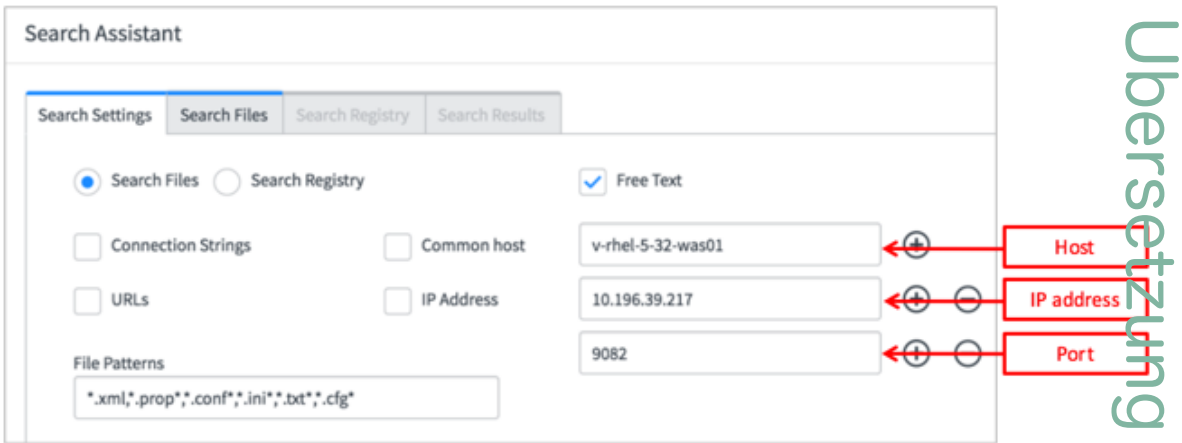
7. Klicken Sie auf **Verbinden**.

Der Debug-Modus ist aktiviert.

Das Fenster „Suchassistent“ wird geöffnet.

8. Durchsuchen Sie CI-Konfigurationsdateien nach Daten, die mithilfe der datenverkehrsbasierten Erkennung empfangen wurden:

   a. Überprüfen Sie unter **Freitext** Daten, die automatisch mit der Liste der datenverkehrsbasierten Verbindungen ausgefüllt werden.



Das Feld „Dateimuster“ zeigt Dateitypen an, in denen der Musterdesigner die Suche durchführt.

   b. Klicken Sie auf die Registerkarte **Dateien durchsuchen**, und überprüfen Sie die Dateien. Bei Bedarf können Sie irrelevante Dateien aus der Suche entfernen, indem Sie auf das Minuszeichen klicken.

   c. Klicken Sie auf **Suche**.

Nach Abschluss der Suche wird die Registerkarte **Suchergebnis** mit der Liste der Dateien geöffnet, in denen eines der Suchkriterien gefunden wurde.

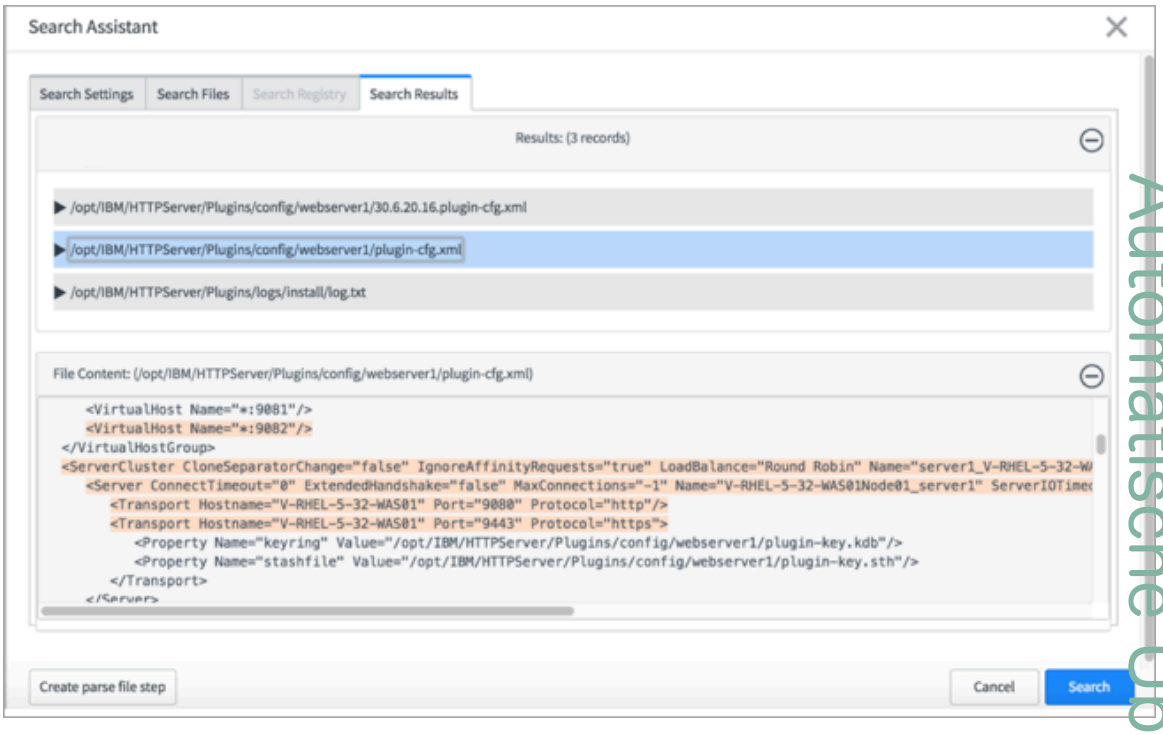
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Erstellen Sie einen Musterschritt für die Analyse der Konfigurationsdatei, die Informationen zur Verbindung enthält:

   a. Klicken Sie auf der Registerkarte Suchergebnis auf eine der Dateien, und überprüfen Sie die Verbindungsdaten in dieser Datei.

   b. Warten Sie, bis der Dateiinhalt geladen ist, und wählen Sie den entsprechenden Eintrag unter dem Dateinamen aus:



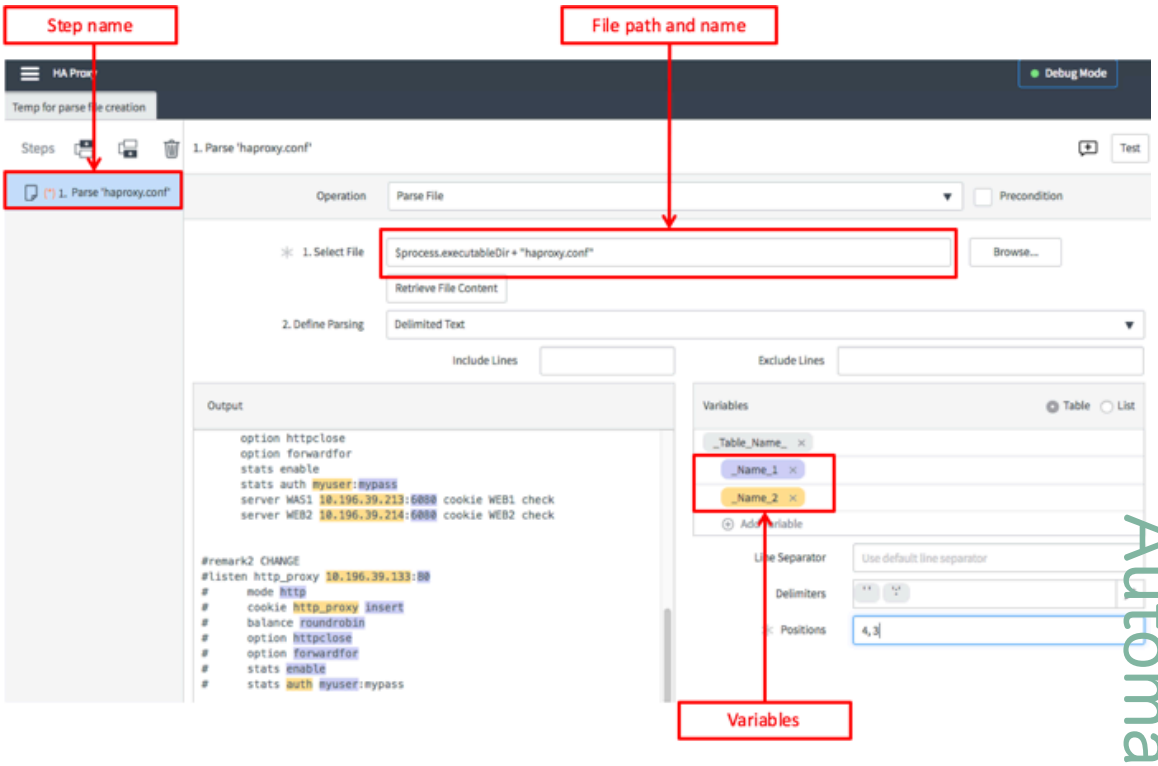
   c. Klicken Sie auf **Analysedateischritt erstellen**, um diese Daten zum Erstellen des Musterschritts zu verwenden.

      Der Musterdesigner zeigt den neuen Schritt mit dem Vorgang „Datei analysieren“ an. Er weist diesem Schritt automatisch den Namen im folgenden Format zu: Analyse <Dateiname>.

      Der Musterdesigner legt automatisch den Dateinamen, den Dateipfad und die Analysestrategie für den Schritt fest. Außerdem werden Variablen erstellt, die Daten enthalten, nach denen Sie gesucht haben. Wenn eine Variable vorhanden ist, die den Dateipfad enthält, gibt der Musterdesigner diese Variable für den Pfad ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Wahlweise: Bei Bedarf können Sie die Analysestrategie ändern.

e. Benennen Sie den Abschnitt um, um einen aussagekräftigen Namen anzugeben, z. B. „HA-Proxy-Clientverbindung erkennen“.
Oder

Kopieren Sie den Schritt und fügen Sie ihn in den entsprechenden Verbindungsabschnitt ein.

10. Schließen Sie die Bearbeitung des Musters wie in Muster abschließen beschrieben ab.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung in Service-Mapping

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Von ITOM-Transparenz verwendete Erkennungsmuster

Muster abschließen

Nachdem Sie Ihr Muster definiert haben, machen Sie es für die Verwendung von Service-Mapping und Discovery bereit.

Vorbereitungen

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Es gibt mehrere Möglichkeiten, ein Muster nach der Erstellung oder Änderung abzuschließen:

Automatische Übersetzung

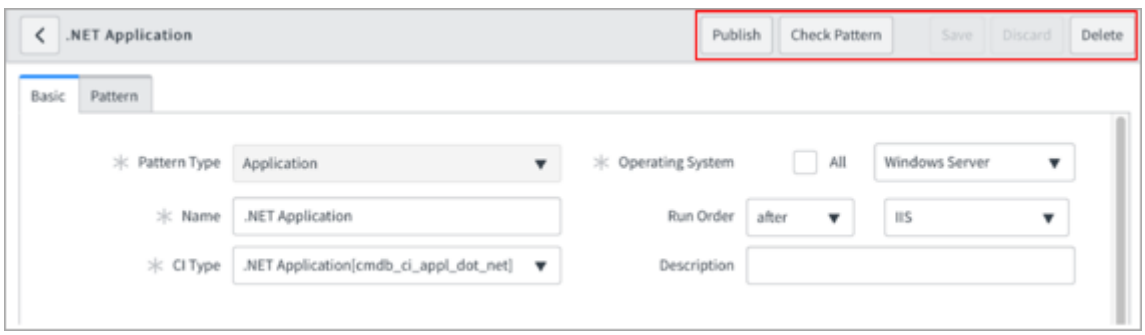
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Speichern – Speichern Sie alle Informationen, die Sie für das Muster definiert haben, das einen Entwurf erstellt. Sie können den Musterentwurf jederzeit weiter bearbeiten. Service-Mapping und Discovery verwenden den Musterentwurf nicht für Erkennung und Zuordnung.
- Änderung verwerfen – Wenn Sie festgestellt haben, dass die Änderungen, die Sie an einem Muster vorgenommen haben, falsch sind, können Sie sie verwerfen.
- Überprüfen – Führen Sie das Muster für das relevante Konfigurationselement (CI) aus, um zu überprüfen, ob die dafür definierten Vorgänge korrekt sind. Überprüfen Sie Ihr Muster, bevor Sie es aktivieren. Diese Option ist nur für Anwendungsmuster verfügbar, die von Service-Mapping verwendet werden.
- Veröffentlichen – Service-Mapping und Discovery verwenden dieses Muster für Erkennung und Zuordnung. Eine neue Version dieses Musters wird erstellt. Der Status der zuvor verwendeten Musterversion ändert sich in Verlauf.

Prozedur

1. Vervollständigen Sie im Musterdefinitionsformular Ihre Musterdefinition, indem Sie eine oder mehrere der folgenden Aktionen ausführen.

Durchzuführende Aufgabe	Aktion
Muster speichern	Klicken Sie auf **Speichern**.
Unerwünschte Änderungen verwerfen	Klicken Sie auf **Verwerfen**.
Muster prüfen (nur für Anwendungsmuster verfügbar, die von **Service-Mapping** verwendet werden)	**a.** Klicken Sie auf **Muster prüfen**. **b.** Geben Sie Parameter für die Verbindung mit diesem CI ein. **c.** Klicken Sie auf **Verbinden**. **d.** Warten Sie, bis der Musterdesigner das Muster ausgeführt hat, und überprüfen Sie, ob keine Fehler vorhanden sind. **e.** Beheben Sie Fehler. Wenn keine Fehler auftreten, können Sie Ihr Muster veröf–fentlichen oder speichern.
Muster veröffentlichen	Klicken Sie auf **Veröffentlichen**.



2. Schließen Sie die Registerkarte „Musterdesigner“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster aus einer Instanz in eine andere kopieren

Wenn Sie Muster von einer Instanz in eine andere kopieren möchten, erstellen Sie ein Update Set mit neuen oder geänderten Mustern mit zugehörigen Elementen in Ihrer Entwicklungsinstanz. Importieren Sie dann das Update Set in Ihre Produktionsinstanz.

Vorbereitungen

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: für die Produktion und für die Entwicklung. Erstellen oder ändern Sie Muster, testen Sie sie und überprüfen Sie die Ergebnisse in der Entwicklungsinstanz. Wenn Sie mit den Discovery-Ergebnissen zufrieden sind, exportieren Sie relevante Muster aus der Entwicklungsinstanz, um einen Update-Satz zu erstellen.

Update Sets ist eine Funktion von ServiceNow zum Übertragen von Anpassungen von einer Instanz zur anderen. Jedes Update Set wird in der Update Set-Tabelle [sys_update_set] gespeichert. Spezifische dem Update Set zugeordnete Anpassungen sind die Einträge in der Tabelle „Kundenupdate“ [sys_update_xml]. Diese erscheinen als zugehörige Liste im Datensatz des Update Sets. Die Methode zum Erstellen von Update Sets für Muster unterscheidet sich von der Erstellung von Update Sets für andere Anpassungstypen.

Warnung: Befolgen Sie immer dieses Verfahren, um Update Sets für Muster zu erstellen. Verwenden Sie nicht das standardmäßige Plattformverfahren zum Erstellen von Update Sets.

Je nach Umfang der Änderungen können Sie die folgenden Musterexportmethoden verwenden:

Muster exportieren

Mit dieser Option wird eine neue, anwenderdefinierte Version des Musters und der zugehörigen Elemente erstellt, die für die ordnungsgemäße Funktion der Muster erforderlich sind. Dann werden sie mit dem Update-Satz verknüpft. Zu den zugehörigen Elementen gehören:

- Erweiterungsabschnitte
- Nachverfolgte Dateien
- Zugehörige CI-Typen
- Klassifizierungsdatensätze
- Zugeordnete Skripts

Hinweis: Update Sets enthalten keine Änderungen an Skripteinbindungen in Mustern.

Muster mit CMDB-Elementen exportieren

Diese Option erstellt eine neue, anwenderdefinierte Version des Musters und seiner zugehörigen Elemente aus der vorherigen Option, einschließlich aller zugeordneten Elemente CMDB Elemente. Anschließend werden alle mit dem Update-Satz verknüpft. Die CMDB Zu den Elementen gehören:

- Haupt-CI-Typ
- Einstiegspunkttypen
- Nachschlagetabellen
- Kennungen
- Regeln für das Hosting und den Abgleich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Update Set ist eine XML-Datei mit der folgenden Namenskonvention: sys_remote_update_set <alphanumerische Zufallszeichenfolge>.xml.

Prozedur

1. Führen Sie in der Entwicklungsinstanz die folgenden Schritte aus, um Muster zu exportieren:
   a. Navigieren zu **Musterdesigner** > **Discovery-Muster**an.
   b. Wählen Sie Anwendungs- oder Infrastrukturmuster aus, die Sie exportieren möchten.
      Hinweis: Gemeinsame Bibliotheken können nicht exportiert werden.
   c. Klicken Sie am unteren Bildschirmrand auf **Aktionen für ausgewählten Zeilen**.
      Hinweis: Sie können nicht mehr als 20 Muster gleichzeitig für die Methode **Muster mit CMDB-Elementen exportieren** verwenden.
   d. Klicken Sie auf **Muster exportieren** oder **Muster mit CMDB-Elementen exportieren**.
   e. Wenn das System den Musterexport abgeschlossen hat, wird das Update Set erstellt.
   f. Klicken Sie zum Anzeigen der Liste der im Update Set enthaltenen Elemente in der Erfolgsmeldung auf **Protokolle anzeigen**.
   g. Klicken Sie auf **Schließen**.
      Die Update Set-Datei im XML-Format wird automatisch auf den Computer heruntergeladen.
   h. Speichern Sie die Update Set-Datei lokal zur zukünftigen Verwendung.
2. Führen Sie in der Produktionsinstanz die folgenden Schritte aus, um die angepassten Muster zu importieren:
   a. Erhöhen Sie die Berechtigungen auf die Rolle security_admin.
   b. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
   c. Wählen Sie den Link aus **Update-Satz aus XML importieren** .
   d. Wählen Sie Aus **Wählen Sie Datei** Und wählen Sie eine XML-Datei aus.
   e. Wählen Sie **Hochladen** aus.
      Die Anpassung ist jetzt als abgerufener Aktualisierungssatz mit Status *Geladen* verfügbar.
3. Vorschau des importierten Update-Satzes anzeigen .
   Das System scannt und validiert das Update Set und zeigt seinen Inhalt auf der Registerkarte **Kunden-Updates** an.
4. Update-Satz bestätigen .
5. Klicken Sie in der Erfolgsmeldung auf **Schließen**.
   Die Produktionsinstanz enthält alle neuen oder geänderten Muster mit zugehörigen Elementen aus dem Update Set.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Laden Sie die aktualisierte Gruppe von Mustern und zugehörigen Elementen auf den MID-Server hoch:
   a. Navigieren zu **Discovery** > **MID-Server**an.
   b. Alternativ navigieren Sie zu **Service-Mapping** > **MID-Server**an.
   c. Klicken Sie auf **Mustersynchronisierung mit MID**.
7. Wenn die Erkennung fehlschlägt oder das Ergebnis nicht den Erwartungen entspricht, starten Sie MID-Server erneut , um sicherzustellen, dass MID-Server den neuesten Mustersatz ausführt.

Zugehörige Informationen

System-Update Sets

Musterversion auswählen

Jedes Mal, wenn Sie ein Muster ändern und speichern, erstellen Sie eine Version dieses Musters. Wählen Sie aus, welche Musterversion Service-Mapping und Discovery für die Erkennung verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

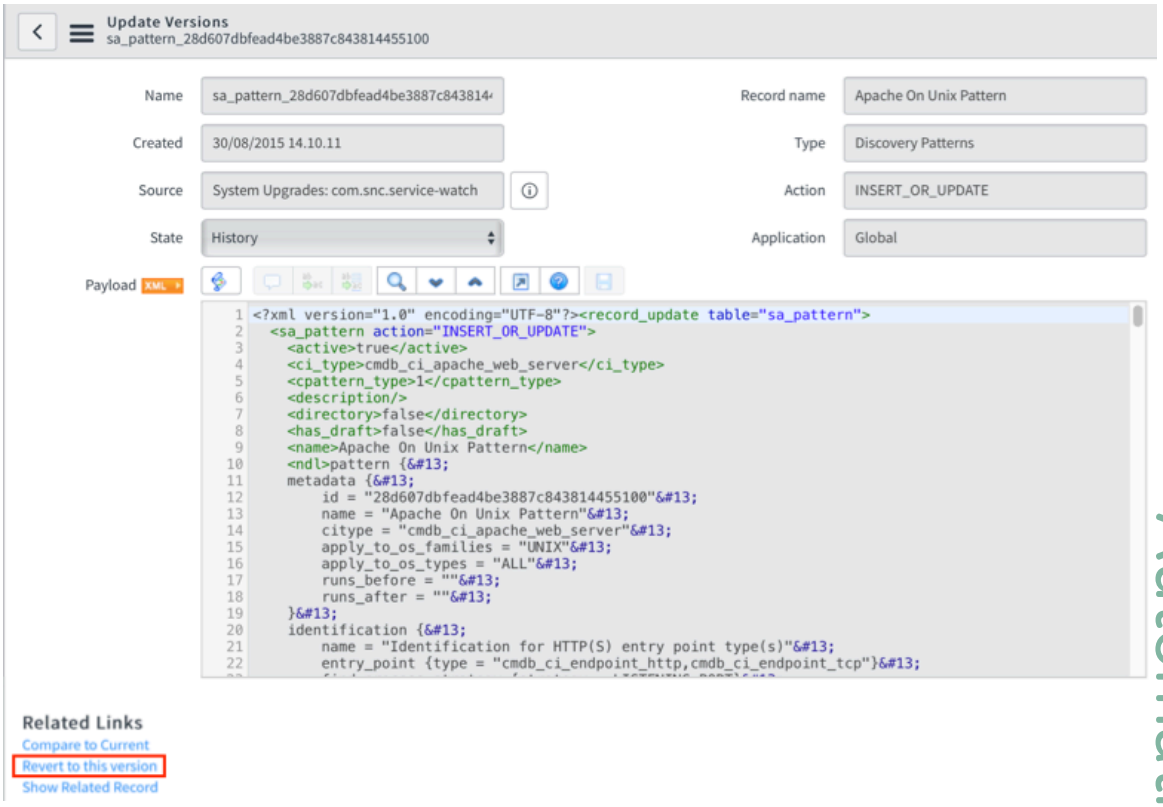
Standardmäßig wird die neueste Version für die Erkennung verwendet, Sie können jedoch eine beliebige andere Version auswählen.

Bei Bedarf können Sie Musterversionen vergleichen.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf das erforderliche Muster.
   Das Formular für dieses Muster wird geöffnet.
3. Klicken Sie auf die Registerkarte **Muster**.
4. Scrollen Sie nach unten zum Abschnitt **Versionen**.
   Der Status der aktiven Musterversion, die Service-Mapping und Discovery verwenden, ist **Aktuell**.
5. Klicken Sie auf die Version, die Sie verwenden möchten.
6. Klicken Sie unter **Zugehörige Links** auf **Diese Version wiederherstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Musterversion wird zur aktiven Version, die Service-Mapping und Discovery verwenden. Ihr Status wird zu „Aktuell“ geändert.

Musterversionen vergleichen

Wenn Sie mehrere Versionen desselben Musters haben, können Sie sie vergleichen, um zu entscheiden, welche Musterversion für die Erkennung verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

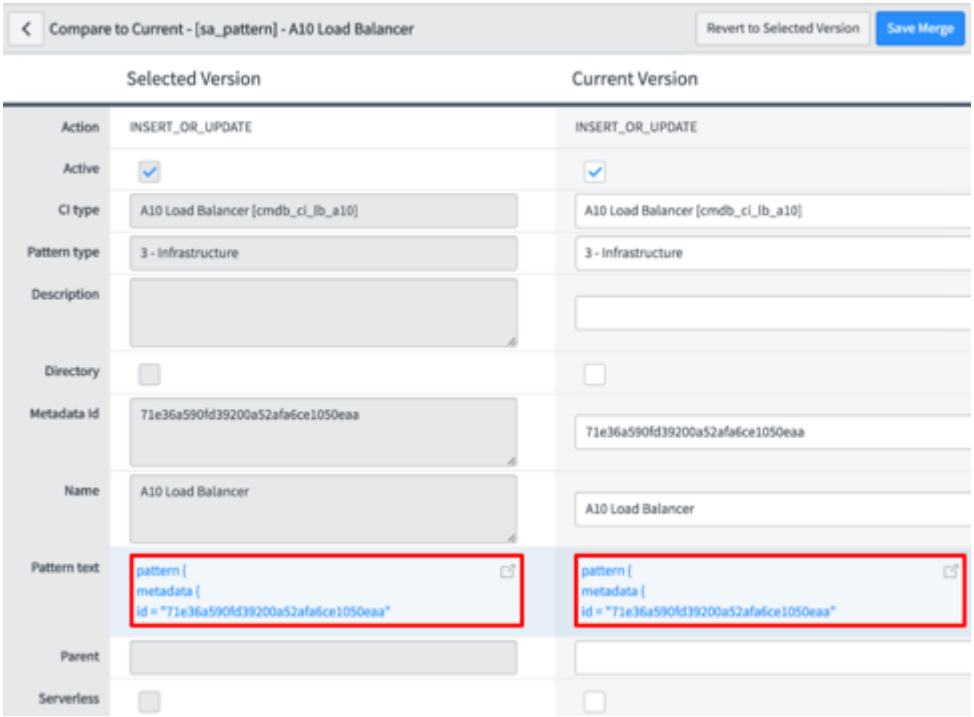
Service-Mapping und Discovery verwenden Muster in ihrem Erkennungsprozess. Jedes Mal, wenn Sie ein Muster ändern und speichern, erstellen Sie eine Version dieses Musters.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. Klicken Sie auf das erforderliche Muster.
   Das Formular für dieses Muster wird geöffnet.
3. Klicken Sie auf die Registerkarte **Muster**.
4. Scrollen Sie nach unten zum Abschnitt **Versionen**.
   Der Status der aktiven Musterversion, die Service-Mapping und Discovery verwenden, ist **Aktuell**.
5. Klicken Sie auf die vorherige Musterversion, die Sie mit der aktuellen Version vergleichen möchten.
6. Klicken Sie unter **Zugehörige Links** auf **Mit Aktuellem vergleichen**.
7. Klicken Sie im Fenster „Mit Aktuellem vergleichen“ auf den Bereich **Mustertext** unter **Ausgewählte Version** oder **Aktuelle Version**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

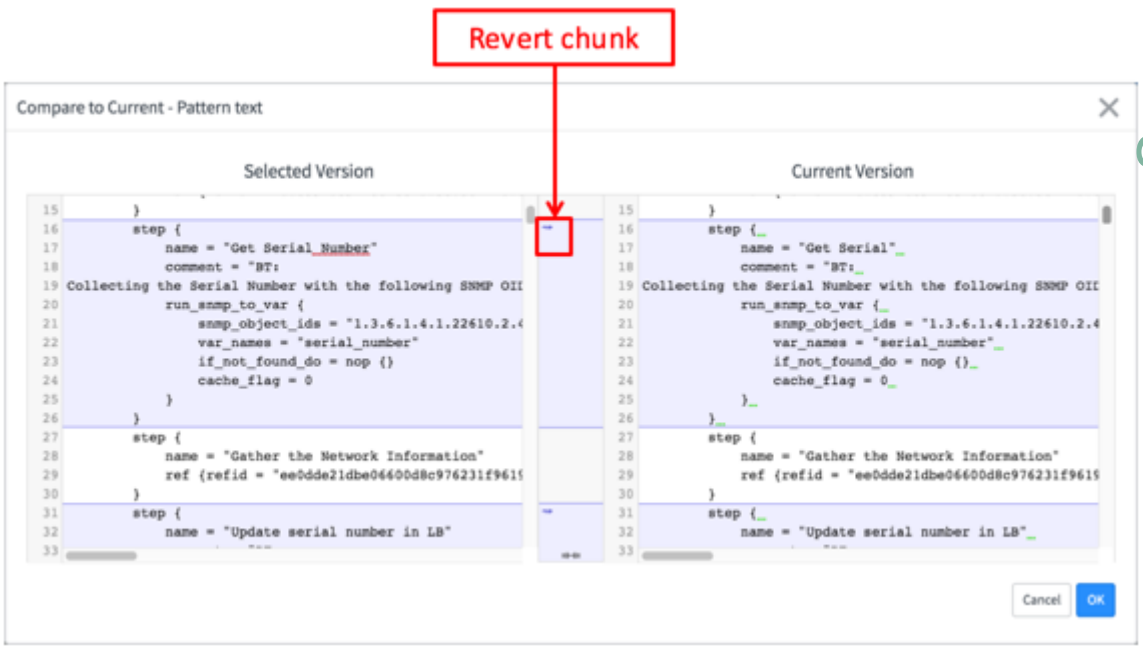


Die Textvergleichsansicht wird geöffnet und zeigt nebeneinander den Text der ausgewählten Musterversion und der aktuellen Musterversion an. Der Schritt, der den Unterschied enthält, wird hervorgehoben.

Hervorhebungsfarben geben die Art der Änderung an:

- Aktualisierter Schritt – violett
- Neue Zeile oder Zeichen – grün
- Zeile oder Zeichen gelöscht – rot

8. Überprüfen Sie die Unterschiede in den Musterversionen.
9. Klicken Sie ggf. auf **Block zurücksetzen**, um den Schritt in der aktuellen Version durch den Schritt aus der vorherigen Version zu ersetzen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **OK**, wenn Sie fertig sind.
11. Wenn Sie Schritte aus der vorherigen Version kopiert haben und die Änderung speichern möchten, klicken Sie auf **Zusammenführung speichern**.

Aktivieren Sie ein deaktiviertes Muster

Wenn Sie ein standardmäßig deaktiviertes Muster für die Discovery verwenden möchten, aktivieren Sie es manuell.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Beginnend mit Visibility Content In Version 6.28.0 wird das Aktivieren oder Deaktivieren eines Musters nicht als Anpassung betrachtet, und es erhält weiterhin Updates. Muster, die zuvor aktiviert oder deaktiviert wurden, werden nach dem Upgrade auf die neueste vordefinierte Version zurückgesetzt, wobei der letzte aktive Feldwert beibehalten wird.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**an.
2. In **Name** Feld, suchen Sie nach dem relevanten Muster.
3. Wählen Sie das Muster aus.
4. Aktivieren Sie die Checkbox **Aktiv**.
5. Wählen Sie **Aktualisieren**.

Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren

Aktivieren Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_Cloud_Hardware_type], um die vordefinierten Hardwaretyp-Datensätze für virtuelle Computer (VM) zu speichern Amazon AWS Cloud Microsoft Azure Cloud Und Google Cloud Platform (GCP). Diese Klassenerweiterung hilft, die Duplizierung der VM-Hardwaretypdatensätze in der Tabelle „Hardwaretyp“ [cmdb_ci_Compute_template] zu verhindern, was die Leistung für verbessert DiscoveryUnd zugehörige Flows.

Vorbereitungen

- Stellen Sie sicher, dass die neuesten Versionen der folgenden Anwendungen installiert sind:
  - CMDB CI-Klassenmodelle
  - Muster für Discovery und Service-Mapping

    Wenn die Version von Muster für Discovery und Service-Mapping Ist älter als 1,6.0, siehe Knowledge Base Artikel KB0955939 .
- Stellen Sie sicher, dass der Anwendungsbereich der ist Muster für Discovery und Service-Mapping Anwendung.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Jeder Cloud-Service Provider bietet mehrere vordefinierte VM-Hardwaretypen an, z. B. t1.micro (AWS) Und so weiter. Sie können auch eigene erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Diese Tabelle ist ein „untergeordnetes“ der Klasse „cmdb_ci_logical_Datacenter“, daher enthalten die Attribute in der Tabelle „Hardwaretyp“ die Attribute in der Klasse „cmdb_ci_logical_Datacenter“.

Dieses Modell kann doppelte Datensätze für jeden erkannten VM-Hardwaretyp erstellen:

Die Anzahl der Datensätze für jeden erkannten VM-Hardwaretyp wird durch die Anzahl der Service-Accounts multipliziert mit der Anzahl der logischen Rechenzentren bestimmt.

Nehmen wir beispielsweise an, dass eine Organisation einen hat AWS Account von t1.micro VM. Die Organisation verfügt über 3000 Service-Accounts und 10 logische Rechenzentren (LDCs), z. B. West US. Ihre nächste Discovery kann den VM-Hardwaretyp erkennen und 30.000 Datensätze in der Tabelle „Hardwaretyp“ [cmdb_ci_Compute_template] erstellen.

Dieser Ansatz könnte Ihre Discovery und die zugehörigen Flows verlangsamen.

Vermeiden Sie diese Probleme, indem Sie vordefinierte speichern AWS Und GCP VM-Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_Cloud_Hardware_type].

Diese Tabelle erweitert die Tabelle „Hardwaretyp“ [cmdb_ci_Compute_template]. Da es nicht an einen LDC oder einen Service-Account gebunden ist, Discovery Vermeidet das Hinzufügen vieler VM-Hardwaretypdatensätze zur Tabelle „Hardwaretyp“ [cmdb_ci_Compute_template].

Die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_Cloud_Hardware_type] verwendet die Felder „object_ID“ und „Provider“ in der Identifizierungsregel.

Hinweis: In AWS Umgebungen erkennt das Discovery-Muster Hardwaretypen nur für das Rechenzentrum des Master-Accounts. Anschließend werden Beziehungen der erkannten Hardwaretypen zu den entsprechenden Regionen in Mitgliedsaccounts erstellt.

- Wenn ein Discovery-Zeitplan sowohl für einen Master-Account als auch für Mitgliedsaccounts ausgeführt wird, erkennt das Muster nur den Hardwaretyp des Master-Accounts.
- Wenn ein Discovery-Zeitplan für einen eigenständigen Mitgliedsaccount ausgeführt wird, erkennt das Muster das Rechenzentrum dieses Mitgliedsaccounts und seinen Hardwaretyp.
- Wenn ein Discovery-Zeitplan für einen Master-Account ausgeführt wird, nachdem ein eigenständiger Mitgliedsaccount bereits erkannt wurde, erkennt das Muster den Hardwaretyp für den Mitgliedsaccount nicht erneut. Stattdessen erkennt er den Hardwaretyp für den Master-Account und ordnet die Beziehungen zwischen den Master- und Mitgliedsaccounts zu.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. In **Name** Feld, suchen Sie nach sn_itom_pattern.use ein einzelner Hardwaretyp für Cloud-Rechenzentren .
3. Wählen Sie die Eigenschaft *sn_itom_pattern.use a single hardware type for cloud data centers* aus.
4. Im Feld **Wert** geben Sie wahr ein.
5. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

1. Bereinigen Sie die Hardwaretyp-Datensätze. Weitere Informationen finden Sie unter Knowledge Base Artikel KB1285337 .

   Wichtig: Durch die Bereinigung werden alle vorhandenen Rechenprofile aus entfernt CMDB. Wenn Sie der Tabelle „Hardwaretyp“ [cmdb_ci_Compute_template] eine Hardwarevorlage manuell hinzugefügt haben, müssen Sie sie der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_Cloud_Hardware_type] manuell hinzufügen.

2. Führen Sie Cloud-Discovery erneut aus.

Zugehörige Informationen

AWS Discovery mithilfe von Mustern

Google Cloud Platform (GCP) Cloud-Discovery mithilfe von Mustern

Microsoft Azure Cloud-Discovery mithilfe von Mustern

Aktivieren Sie die Cloud-BS-Image-Discovery

Aktivieren Sie die Tabelle „Cloud-BS-Image“ [cmdb_ci_Cloud_os_image], um die Cloud-BS-Image-Datensätze für zu speichern Amazon AWS Cloud, Microsoft Azure Cloud, Google Cloud Platform (GCP), Oracle Cloud-Infrastruktur (OCI), und IBM Cloud.

Vorbereitungen

- Stellen Sie sicher, dass die neuesten Versionen der folgenden Anwendungen installiert sind:
  - Muster für Discovery und Service-Mapping
  - CMDB CI-Klassenmodelle
- Stellen Sie sicher, dass der Anwendungsbereich der ist CMDB CI-Klassenmodelle Anwendung.

Hinweis: Cloud Provisioning and Governance (CPG) unterstützt die Tabelle „Neues Cloud-Image“ (cmdb_ci_Cloud_os_image) nicht. Wenn Sie derzeit CPG-Bereitstellungs-Flows verwenden oder beabsichtigen, dies zu tun, migrieren Sie nicht zum neuen Image-Modell.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Jeder Cloud-Service Provider bietet BS-Images zum Starten einer Compute-/VM-Instanz an. Cloud-Discovery Speichert die Tabelle „erkanntes Image“ [cmdb_ci_os_template]. Diese Tabelle ist eine abhängige Klasse von [cmdb_ci_logical_Datacenter] oder [cmdb_ci_Cloud_Service_Account]. Das neue Image-Modell erstellt einen Datensatz für jedes öffentliche Image (Objekt-ID), unabhängig vom Service-Account und Wird ausgefüllt Sie in der Tabelle „Cloud-Image“ [cmdb_ci_Cloud_os_image]. Dort für reduziert das neue Modell die Anzahl der Datensätze in CMDB

Hinweis: Wenn Sie haben Muster für Discovery und Service-Mapping Version 1.10.0: November 2023. Fahren Sie mit dem folgenden Verfahren fort. Wenn Sie eine frühere Version haben, finden Sie unter Knowledge Base Artikel KB1000183 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. In **Name** Feld, suchen Sie nach sn_cmdb_ci_class.use_single_cloud_os_image .
3. Wählen Sie die Eigenschaft *sn_cmdb_ci_class.use_single_cloud_os_image* aus.
4. Im Feld **Wert** geben Sie wahr ein.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

1. Bereinigen Sie die Image-Datensätze. Weitere Informationen finden Sie unter Knowledge Base Artikel KB1537376 .
2. Führen Sie Cloud-Discovery erneut aus.

ITOM Content Service

ServiceNow® ITOM Content Service Bietet umfassende Transparenz von Produkten in Ihrer Infrastruktur. Die Klassifizierung der von identifizierten Prozesse Predictive Intelligence Aktiviert eine breitere Discovery und wöchentliche Updates neuer Konfigurationselemente in CMDB. Verwenden Sie Discovery-Administratorarbeitsbereich Zum Überprüfen und Verwalten ITOM Content Service Vorschläge.

ITOM Content Service Modell

Über ITOM Inhaltsservice

ITOM-Transparenz Bietet mehrere Methoden zur Erkennung von Produkten in Ihrer Infrastruktur. Beim Ausführen von Discovery mit Muster für Discovery und Service-Mapping Beispielsweise sucht jedes Muster nach einer Version eines Produkts und kann eine detaillierte Transparenz der Produktinformationen bieten.

Während Ihre Infrastruktur wächst und neue IT-Produkte schnell auf den Markt gebracht werden, müssen Sie über eine breitere, schnell aktualisierte Transparenz verfügen. Jede Woche, ITOM Content Service Identifiziert Produkte, die Sie derzeit verwenden, und stellt neue Konfigurationselemente (Configuration Items, CI) für Ihre Nutzung bereit. Die neueste Version von Discovery-Administratorarbeitsbereich Ermöglicht Ihnen, die Inhaltsservicevorschläge manuell zu aktualisieren, bevor Sie sie überprüfen.

ITOM Content Service bietet die folgenden Vorteile:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüft die Produkte, die Sie derzeit jede Woche verwenden, und stellt neue Konfigurationselemente (Configuration Items, CIs) bereit.
- Basierend auf KI hilft es Ihnen, Fingerabdrücke von laufenden Prozessen und SNMP-System-OIDs zu identifizieren und die CIs zu erstellen, die Sie für die Überwachung Ihrer Infrastruktur benötigen.
- Identifiziert irrelevante Prozesse, die keine geeigneten Kandidaten für CIs sind.
- Erkennt eine höhere Anzahl von Produkten mithilfe von KI-Fähigkeiten, die laufende Anwendungsprozesse gruppieren und klassifizieren.

Vorteile von Software Asset Management Integration mit ITOM Content Service

ITAM Software Asset Management(SAM) Anwender profitieren von der Integration mit ITOM Content Service Auf mehrere Arten.

- Verschaffen Sie sich Einblick in die Prozesse, die derzeit für die installierte Software ausgeführt werden. Auf diese Weise können Sie auch herausfinden, welche installierte Software keine laufenden Prozesse hat und möglicherweise redundant ist.
- ITOM Content ServiceKomplimente Software Asset Management In Fällen von Services, für die keine Installation erforderlich ist, z. B. eine Oracle Datenbank, die als Service ausgeführt und nicht installiert ist. In Fällen wie diesem ITOM Content Service Erstellt den Datensatz der installierten Software basierend auf der Kombination der Prozessfingerabdruckdaten mit den von SAM erkannten Daten. Ohne ITOM Content Service, Sie können diese Art von Transparenz nicht erhalten.
- Verwendung dateibasierter Discovery-Funktionen ITOM Content Service Kann eine laufende Systemdatei erkennen, die mit einer App identifiziert wurde. Beispiel: ITOM Content Service Kann einen Datensatz der installierten Software mit einem abgleichen Apache Kafka Wird ausgeführt Exe Datei. Weitere Informationen finden Sie unter File-based Discovery.

Weitere Informationen zu Software Asset Management finden Sie unter Software Asset Management Content Service .

Vorteile der Verwendung von Service-Mapping mit ITOM Content Service

Mit der neuesten Version von ITOM Content Service, Service-Mapping Anwender können nutzen Service-Fingerabdrücke Vorschläge zum Identifizieren und Auswählen von Anwendungsservices basierend auf klassifizierten Komponenten. Indem Sie Komponentendetails wie Produkt, Produktkategorie, Herausgeber und Beschreibung anzeigen, können Sie fundierte Entscheidungen darüber treffen, welche Kandidaten in Anwendungsservices konvertiert werden sollen. Sie können auch sehen, welche zusätzlichen Prozesse in den Service integriert werden können, da bestimmte Prozesse gemeinsam einen umfassenden Service erstellen, wenn sie kombiniert werden.

Beides ITOM Content Service Vorschläge und Service-Fingerabdrücke Bieten Sie automatisierte, wöchentliche Vorschläge für Kandidaten an, die sich jedoch in einigen Punkten unterscheiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich zwischen ITOM Content Service Vorschläge und Service-Fingerabdrücke

Name	Typ	Identifiziert	Fokus	Details zum Herausgeber	Standort
ITOM Content Service Vorschläge	Fingerabdrücke verarbeiten	Einzelne Prozesse, die Komponenten eines Service oder eigenständige Prozesse sein können.	Bestimmte Aktionen eines Prozesses, die eine höhere Granularität bieten.	Herausgeber des Prozesses. Wenn ein Prozess Teil eines Service ist, aber einen anderen Herausgeber hat, stellt der Prozess nur Details zu seinem eigenen Herausgeber bereit.	**Inhaltsservicevorschläge** Registerkarte in Discovery-Administratorarbeitsbereich Inhalt 360
Service-Fingerabdrücke	Service-Fingerabdrücke	Services, die auf klassifizierten Komponenten basieren.	Der Service als Ganzes und bietet eine breitere Perspektive.	Herausgeber des Service. Wenn ein Prozess Teil eines Service ist, aber einen anderen Herausgeber hat, enthält der Service-Fingerabdruck nur Details zum Herausgeber des Service.	**Service-Fingerabdrücke** Registerkarte in Service-Mapping Arbeitsbereich

Automatische Übersetzung

Weitere Informationen zur Verwendung von Service-Fingerabdrücke In Service-Mapping, Siehe Ordnen Sie Anwendungsservices basierend auf zu Empfehlungen für automatisierte Services.

Weitere Informationen zu finden Service-Fingerabdrücke Kandidaten, Siehe KB1706310 .

Verwalten ITOM Content Service Mit Discovery-Administratorarbeitsbereich

Überprüfen Sie empfohlene Aktionen und Anwendungsvorschläge, und konfigurieren Sie Discovery über Discovery-Administratorarbeitsbereich.

Beachten Sie, dass Discovery-Administratorarbeitsbereich Wird ab unterstützt Vancouver Release.

Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich Inhalt 360.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Freigabe von Daten im CDS

Das Continuance Delivery System (CDS) ist ein ServiceNow® Technologie, die Daten zwischen der Instanz „Datenservices“ synchronisiert Das Daten speichert und verteilt Und die Kundeninstanzen.

Aktivieren Sie die Freigabe von Anwendungsfingerabdruck-Prozessdaten für ITOM Content ServiceÜber das CDS können sie von KI-Bibliothekaren gekennzeichnet und klassifiziert werden. ITOM Content Service Stellt dann jede Woche neue CIs bereit. Ihre Daten werden für freigegeben ServiceNow® Instanz in einer sicheren Umgebung. Sie können den Zugriff auf Ihre Daten steuern, indem Sie Berechtigungen in festlegen Discovery-Administratorarbeitsbereich.

Die beiden Optionen für die Freigabe Ihrer Daten sind:

- Freigabe der Fingerabdruckdaten laufender Prozesse, wodurch der Zugriff auf die Tabelle „Prozessgruppen“ [cmdb_Process_groups] ermöglicht wird.
- Freigabe der SNMP-System-OIDs-Daten, wodurch der Zugriff auf die Tabelle „SNMP-OID“ [Discovery_snmp_oid] ermöglicht wird.

Weitere Informationen zum Festlegen der Berechtigungen finden Sie unter Geben Sie Daten für frei ITOM Content Service

ITOM Content Service – Anwendungsfall

Dies ITOM Content Service Der Anwendungsfall demonstriert, wie Unternehmen eine verbesserte Transparenz ihrer Umgebung erreichen können.

Anwendungsfallübersicht

Die Klasse „Anwendungskonfigurationselemente“ (Application Configuration Items, CIs) ist eine Schlüsselkomponente der Datenplattform einer Organisation innerhalb von Gemeinsames Servicedatenmodell(CSDM). Anwendungs-CIs helfen, Softwareaktivitäten zu protokollieren und kritische IT-Vorgänge zu unterstützen.

Viele Produkte und Anwendungen sind für wichtige Aufgaben auf Anwendungs-CIs angewiesen. Einige Schlüsselbeispiele sind:

- Service-Mapping: Verwendet Anwendungs-CIs zum Erstellen von Servicezuordnungen
- ITOM-Integrität: Überwacht die Integrität der Anwendung und löst Incidents mithilfe von Anwendungs-CIs
- IT Asset Management(ITAM): Verfolgt und verwaltet Softwareanwendungen und ihre zugehörigen Lizenzen mit Anwendungs-CIs
- IT Service Management(ITSM): Analysiert die Serviceauswirkung und berechnet den Explosionsradius mit Anwendungs-CIs
- Enterprise-Architektur(EA): Nutzt Anwendungs-CIs, um Geschäftsergebnisse zu generieren

Herausforderung

Eine große Organisation mit zahlreichen Anwendungen erfordert eine genaue Discovery. Die Verwaltung von Anwendungs-CIs ist wichtig, aber das IT-Team sieht es als schwierig, die Transparenz über die wachsende Infrastruktur zu erhalten.

ITOM-Transparenz Bietet mehrere Methoden zum Erkennen von Produkten in der Infrastruktur einer Organisation, z. B. Muster für Discovery und Service-Mapping. Diese Methode bietet detaillierte Transparenz in die Informationen eines Produkts. Wenn eine Vielzahl von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen verwendet wird, können nicht alle über ein dediziertes Muster verfügen. Wenn eine Anwendung kein dediziertes Muster hat, füllt die Discovery nur die Tabelle „laufender Prozess“ [cmdb_running_Process] aus, ohne das Produkt zu identifizieren oder ein CI dafür zu erstellen.

Ohne ein Anwendungs-CI fehlt der Organisation ein genauer Einblick in ihre Infrastruktur und könnte Schwierigkeiten haben, die folgenden wichtigen Aktionen zu optimieren:

- Binden Sie CIs mit Überwachungswarnungen und offenen Incidents in Bezug auf die CIs
- Planen Sie automatisierte Software-Upgrades
- Automatisieren Sie Skripts, um das Produkt zu optimieren oder Probleme zu beheben
- Führen Sie Auswirkungsbewertungen und Change-Auswirkungsanalysen durch
- Erstellen Sie Sicherheits-Workflows

Lösung

ITOM Content Service Verbessert den Discovery-Prozess durch Tagging und Klassifizierung von Prozessfingerabdrücken. Dieser Service bietet Details zum Herausgeber, zum Produkt und zur wesentlichen Komponente des CI. Im Gegensatz zur musterbasierten Discovery ITOM Content Service Identifiziert Anwendungen direkt in der Umgebung der Organisation, ohne dass veröffentlichte Musterklassifizierer erforderlich sind. Dieser Ansatz ermöglicht die kontinuierliche Bereitstellung von Inhalten, ohne durch einen geplanten Releasezyklus eingeschränkt zu werden.

Beispiel: Discovery Identifiziert den Elipse Software E3 Database Engine-Prozess (E3DBEngine.exe) und listet ihn in der Tabelle „laufender Prozess“ [cmdb_running_Process] auf. Wenn die Prozessklassifizierungsbedingung E3DBEngine.exe nicht so festgelegt ist, dass ein Muster ausgelöst wird, wird kein Muster gestartet, und es wird kein CI erstellt. Jedoch mit ITOM Content Service, Der Prozess E3DBEngine.exe ist gekennzeichnet und klassifiziert, wodurch aktiviert wird Discovery Dient zum Umwandeln des Prozesses in ein CI während des nächsten Scans.

Ergebnis

Discovery Verwenden ITOM Content Service Erstellt einen CI-Datensatz durch Tagging und Klassifizierung des Herausgebers, des Produkts und der wesentlichen Komponente für alle Anwendungen in der Umgebung der Organisation. Diese Methode bietet einen verbesserten und kontinuierlichen Einblick in die Anwendungslandschaft und ermöglicht eine effektive Überwachung, proaktive Aktionen und laufende Optimierung.

ITOM Content Service installieren

Installieren Sie ITOM Content Service Anwendung (sn_Smart_content) zur Verwaltung und Überwachung der Erstellung von Konfigurationselementen basierend auf Anwendungsfingerabdrücken.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie ITOM-Inhaltsservice Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Plugins werden mit aktiviert ITOM Content Service:

- Discovery (com.snc.discovery)
- Normalisierungsdaten-Services-Client (com.Glide.Data_Services_Canonicalization.Client)
- Dateibasierte Discovery (com.snc.Discovery.file_based_Discovery) – beginnend mit ITOM Content Service Version 1.5.1

Hinweis: Das Plugin „ITOM Smart Content“ (com.snc.itom.smart.content) ist ab XP5 verfügbar. Dieses Plugin ist optional und kann über angefordert werden ServiceNow Personal. Weitere Informationen finden Sie unter Plugins anfordern .

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach ITOM Content Service Anwendung (sn_Smart_content) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der App anhand ihres Namens oder ihrer ID suchen.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Nächste Maßnahme

Geben Sie Daten für frei ITOM Content Service

Zugehörige Informationen

ITOM Content Service

Discovery-Administratorarbeitsbereich

Geben Sie Daten für frei ITOM Content Service

Steuern Sie die Datenfreigabe, indem Sie diese aktivieren oder deaktivieren ITOM Content Service Freigabeoptionen mit Discovery-Administratorarbeitsbereich.

Vorbereitungen

Stellen Sie sicher, dass die folgende Anwendung und das folgende Plugin installiert sind:

- ITOM Content Service (sn_Smart_content)
- Discovery-Administratorarbeitsbereich (com.snc.itom.daw)

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**an.
2. Geben Sie an, ob und welche Daten Sie für KI-Bibliothekare freigeben möchten.

Option	Aktionen
Aktivieren Sie, um Ihre Daten freizugeben	**a.** In **Setup des Inhaltsservice** Kachel aus–wählen **Aktivieren** . **b.** Lesen Sie die Vereinbarung, und wählen Sie aus **Ja, ich habe die Aktivierungsver einbarung gelesen und stimme ihr zu** . **c.** Wählen Sie **Weiter**. **d.** Wählen Sie Ihr Setup aus. ▪ Erweitert: Aktiviert einen umfassenden Satz von Klassifizierern für erweiterte Sichtbarkeit ▪ Standard: Aktiviert die gängigsten Klassifizierer. ▪ Anwenderdefiniert: Sie wählen aus, welche Klassifizierer aktiviert werden sollen. **e.** Aktivieren Sie die Datenfreigabeoptionen, die Sie verwenden möchten. ▪ Fingerabdruckdaten des laufenden Prozesses: Gibt Metadaten und einige Beispiele von Prozessen aus der Ta–belle „Prozessgruppen“ frei. ▪ SNMP-System-OIDs: Gibt Metadaten und einige Beispiele von Prozessen aus der SNMP-OID-Tabelle frei. **f.** Wählen Sie **Speichern**. **g.** Wenn die Aktivierung abgeschlossen ist, wählen Sie aus **Startseite** Um zum Ar–beitsbereich zurückzukehren. Die **Inhaltsservicevorschläge** Kachel er–setzt **Setup des Inhaltsservice** Kachel. In der neuen **Setup des Inhaltsservice** Ab–schnitt wird ein grünes Häkchen ange–zeigt, das anzeigt, dass Sie sich für akti–viert haben ITOM Content Service.
Legen Sie die Berechtigungen für die Datenfrei-gabe ab	**a.** In **Setup des Inhaltsservice** Abschnitt auswählen **Konfigurieren Sie das Setup** . **b.** Deaktivieren Sie eine Option oder beide Optionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktionen
	c. Wählen Sie **Speichern**. **d.** Wenn die Einstellung abgeschlossen ist, wählen Sie aus **Startseite** Um zum Ar–beitsbereich zurückzukehren.
Opt Keine Freigabe Ihrer Daten	**a.** In **Setup des Inhaltsservice** Abschnitt auswählen **Deaktivieren** . **b.** Wählen Sie Aus **Deaktivieren** . **c.** Lesen Sie **Deaktivieren von** *`ITOM Content Service`*Systemnachricht und wählen Sie aus **Deaktivieren** . **d.** Wenn der Abwählvorgang abgeschlos–sen ist, wählen Sie aus **Startseite** Um zum Arbeitsbereich zurückzukehren. ITOM Content Service Die Verwendung Ihrer Daten wird beendet, und Ihr Arbeitsbe–reich enthält nur von Ihnen definierte CIs. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich.

Zugehörige Informationen

ITOM Content Service

Aktivieren Sie Discovery mit ITOM Content Service

Überprüfen Sie ITOM Content Service Vorschläge für die Anwendungs-Discovery und aktivieren Sie die Discovery-Klassifizierer, um die Erstellung von Konfigurationselementen zu ermöglichen.

Vorbereitungen

Stellen Sie sicher, dass die folgende Anwendung und das folgende Plugin installiert sind:

- ITOM Content Service (sn_Smart_content)
- Discovery-Administratorarbeitsbereich (com.snc.itom.daw)

Stellen Sie sicher ITOM Content Service Ist aktiv. Weitere Informationen finden Sie unter Geben Sie Daten für frei ITOM Content Service.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Content 360**an.
2. Wählen Sie aus **Inhaltsservicevorschläge** Kachel.
3. Synchronisieren Sie manuell mit Vorschlägen aus Ihrem System, indem Sie auswählen **Kandidaten synchronisieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn eine Meldung zum Anwendungsbereich angezeigt wird, wählen Sie aus **OK** Zum Beenden der Nachricht. Ändern Sie dann den Umfang, indem Sie das Symbol für den Anwendungsbereich ( ) Und auswählen **Global** .

4. Wählen Sie im Bestätigungsfenster für Synchronisierungskandidaten die Option aus **Ja** .
5. Überprüfen Sie die Inhaltsservicevorschläge für Discovery nach Produkt.
   - Um die Liste zu filtern, wählen Sie die Produkte aus der aus **Inhaltsservicevorschläge** Registerkarte.
   - Um die Beschreibung und Details eines Produkts zu überprüfen, wählen Sie den Link aus **Name** Spalte.
6. Wählen Sie das Produkt aus, für das Sie die Discovery aktivieren möchten.
7. Aktivieren Sie Discovery-Klassifizierer nach Produktkategorien.

   Hinweis: Die Anzahl der Klassifizierer, die aktiviert werden, wird in angegeben **Aktivieren** Schaltfläche.

   - Um die Discovery nach Produktkategorien zu aktivieren, aktivieren Sie die Kontrollkästchen Produktkategorien, und aktivieren Sie das Kontrollkästchen neben **Name** Spalte, und wählen Sie aus **Aktivieren** .
   - Um die Discovery nach einzelnen Produkten zu aktivieren, wählen Sie das Produkt aus der aus **Name** Spalte und wählen Sie aus **Aktivieren** .

Ergebnis

Die neuen Konfigurationselemente werden zu hinzugefügt CMDB Beim nächsten Mal Discovery Führt einen Zeitplan aus. Die Discovery Admin-Arbeitsbereich listet dann die hinzugefügten CIs auf und entfernt sie aus der Liste der vorgeschlagenen Anwendungen.

Zugehörige Informationen

ITOM Content Service

Discovery-Administratorarbeitsbereich

Erkennen Sie mit installierte Softwaredaten ITOM Content Service

Verwenden ITOM Content Service Und ITSM Software Asset Management Um installierte Software zu erkennen, die nicht automatisch mit erkannt wird Software Asset Management Kern oder Software Asset Management Professional Oder dateibasiert Discovery.

Vorbereitungen

Stellen Sie sicher, dass die folgende Anwendung und die folgenden Plugins installiert sind:

- ITOM Content Service (sn_Smart_content)
- Software Asset Management Core (com.snc.sam.Core) oder Software Asset Management Professional(Com.snc.samp)
- Dateibasierte Discovery (com.snc.Discovery.file_based_Discovery)

Stellen Sie sicher ITOM Content Service Ist aktiv. Weitere Informationen finden Sie unter Geben Sie Daten für frei ITOM Content Service.

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Intelligenter Inhalt** > **Intelligente Inhaltskategorien**an.
2. Aktivieren Sie die Kategorie installierter Software.
   a. Doppelklicken Sie auf **Installierte Software Erstellen** Feld.
   b. Wählen Sie in der Liste aus **Wahr** .
   c. Überprüfen Sie den Wert, indem Sie das grüne Häkchen auswählen Markieren.

Ergebnis

Der neu installierte Software-Datensatz wird erstellt und der Liste „CI-Softwareinstallationen“ hinzugefügt.

Zugehörige Informationen

ITOM Content Service

ITOM Content Service – Referenz

Verwenden ITOM Content Service Ermöglicht Ihnen, über zu verfügen CMDB Wird jede Woche mit neuen Daten ausgefüllt. Verwenden Sie die Knowledge Base-Artikel, um mehr über die Konfigurationselementkandidaten zu erfahren, die veröffentlicht wurden.

Informationen zu den CI-Kandidaten der Anwendung finden Sie unter KB1584650 .

Informationen zu den SNMP-OID-CI-Kandidaten finden Sie unter KB1702434 .

Um mehr über zu erfahren Service-Fingerabdrücke Kandidaten, Siehe KB1706310 .

Tag-Governance

Ein effektives Tag-Management verbessert die Effizienz der Berichterstellung und des gesamten Betriebsmanagements. Verwenden Sie ServiceNow® Tag-Governance App zur Identifizierung und Korrektur von lokalen oder Cloud-Ressourcen, die inkonsistent sind und nicht den Tag-Richtlinien Ihrer Organisation entsprechen.

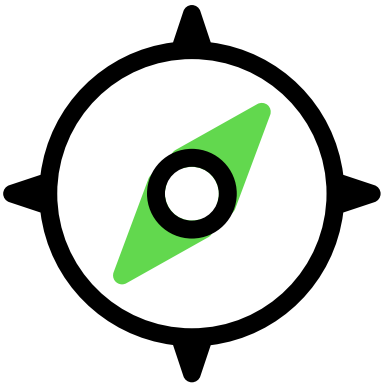
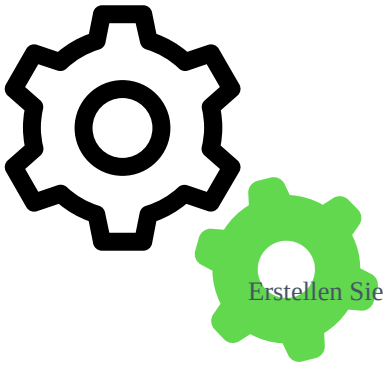
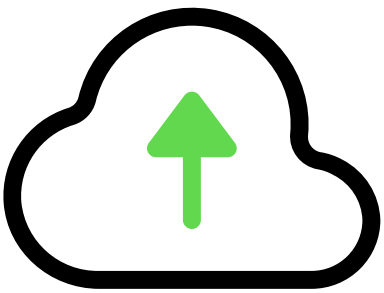
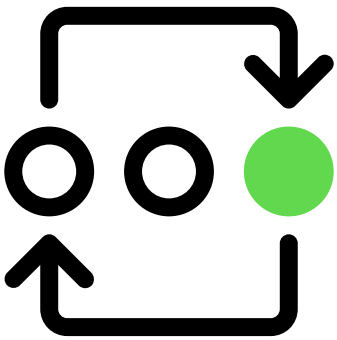
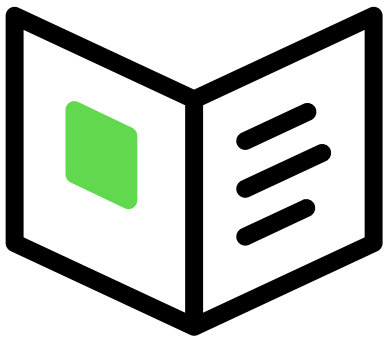
Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Erste Schritte

A *Tag* Ist ein Schlüssel-Wert-Paar, das einem CI oder einer Cloud-Ressource zugewiesen ist. Ihre Organisation kann Tags verwenden, um Assets zu kategorisieren, um den Einblick in Cloud-Nutzung und -Kosten zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen	Konfigurieren	
		
Erfahren Sie mehr über Tag-Governance	Installieren Sie die App.	Erstellen Sie Tag-Richtlinien Definieren Sie Tag-Standards, die geprüft werden.
Cloud-Tags werden aktualisiert	**Beheben**	**Referenz**
		
Echtzeit-Updates von Tags für Cloud-Ressourcen.	Beheben Sie Tag-Probleme	Zusätzliche Informationen zu Formularen und Einstellungen.

Automatische Übersetzung

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für Tag-Governance In ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Tag-Governance erkunden

Erfahren Sie mehr über Tag-Governance Berichte und Discovery.

Tag-Governance – Übersicht

Ein effektives Tag-Management verbessert die Effizienz der Berichterstellung und des gesamten Betriebsmanagements. Verwenden Sie ServiceNow® Tag-Governance App zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizierung und Korrektur von lokalen oder Cloud-Ressourcen, die inkonsistent sind und nicht den Tag-Richtlinien Ihrer Organisation entsprechen.

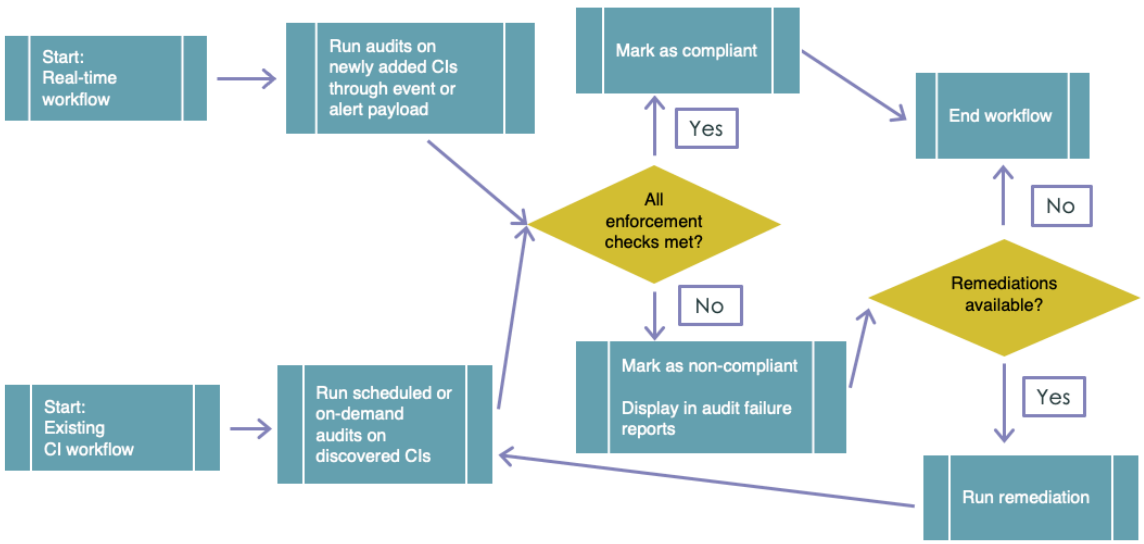
Tag-Governance Anwender

Anwender

Anwender	Beschreibung
Tag-Governance-Administrator	Verantwortlich für die Aufrechterhaltung einheitlicher Tag-Management-Richtlinien und die Sicherstellung, dass Ressourcen für Transparenz, Compliance und Kostenmanagement ordnungsgemäß getaggt werden.
Berichtsbetrachter	Schreibgeschützte Berechtigungen: • Überwachen Sie Berichte aus Audit-Ausführungen • Analysieren Sie die Daten, um Einblicke für Aktionen abzuleiten

Tag-Governance – Workflow

Tag-Governance – Workflow



Tag-Governance – Vorteile

Tag-Governance – Vorteile

Vorteil	Funktion	Anwender
Implementieren Sie die Cloud-Ereignisverarbeitung, und konfigurieren Sie eine Tag-Richtlinie, um Cloud-Ressourcen-Tags automatisch in Echtzeit zu aktualisieren.	Echtzeit-Updates von Tags für Cloud-Ressourcen werden durchgeführt	Cloud-Administratoren
Tag Governance unterstützt die Domänentrennung, sodass Sie Daten, Prozesse und administrative Aufgaben logisch in unterschiedliche Domänen gruppieren und trennen können. Dies ermöglicht eine	Domain Separation und Tag-Governance	Cloud-Administratoren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Governance – Vorteile (Fortsetzung)

Vorteil	Funktion	Anwender
präzise Kontrolle über Aspekte wie Anwenderzugriff und Datensichtbarkeit.		
Überprüfen Sie nicht konforme CIs, die durch Tag-Audits gekennzeichnet wurden, und lösen Sie sie, indem Sie die erforderlichen Tags hinzufügen.	Tag-Auditfehler in der Vorschau anzeigen und korrigieren	Tag-Administratoren

Erkunden

Discovery-Beitrag zu Tag-Governance

Die Discovery Und Cloud-Discovery Funktionen erkennen alle Ressourcen in CMDB Sowie Cloud-Ressourcen von Cloud-Anbietern wie Amazon AWS Cloud, Microsoft Azure Cloud, Und Google Cloud Platform (GCP).

Tag-Governance Dashboard: Registerkarte „Übersicht“

Die **Übersicht** Die Registerkarte verfolgt die Integrität und Compliance von CIs basierend auf Tag-Audits. Interaktive Widgets bieten Informationen, mit denen Sie den Tag-Compliance-Status und die am häufigsten verwendeten und am wenigsten verwendeten Tags anzeigen und analysieren können.

Tag-Governance Dashboard: Registerkarte „Richtlinienansicht“

Verwenden Sie die Registerkarte Richtlinienansicht, um die Tag-Compliance anzuzeigen und zu analysieren, gefiltert nach Cloud-Service-Account, Tag-Richtlinie und Rechenzentrum. Mit Filtern können Sie sich auf die Verbesserung der Tag-Compliance konzentrieren.

Tag-Governance Dashboard: Registerkarte „Effizienz“

Auf der Registerkarte „Wirksamkeit“ werden die Ergebnisse von Tag-Audits als Tag-Integritätsbewertungen und Compliance-Abdeckung von CIs angezeigt. Interaktive Widgets zeigen den Status der Tag-Abdeckung und Tagging-Trends im Zeitverlauf an.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Tag-Governance finden Sie unter:

- Tag-Governance konfigurieren
- Tag-Governance verwenden
- Tag-Governance – Referenz

Discovery-Beitrag zu Tag-Governance

Die Discovery Und Cloud-Discovery Funktionen erkennen alle Ressourcen in CMDB Sowie Cloud-Ressourcen von Cloud-Anbietern wie Amazon AWS Cloud, Microsoft Azure Cloud, Und Google Cloud Platform (GCP).

Die Rolle der Discovery

Mit Discovery und Cloud Provisioning and Governance können die von allen wichtigen Cloud Providern und Container-Ökosystemen verwendeten Tags anhand von Service-Mapping-Mustern erkannt werden. Sobald die Tags erkannt wurden, Service-Mapping Kann Anwendungsservices erstellen, die auf den Tags basieren. In der Regel verwenden Unternehmen Tags in virtualisierten, hyperkonvergenten oder Multi-Cloud-Infrastrukturen. Beispiele für die dafür verwendeten Infrastrukturtypen und Tags finden Sie unter Tag-basierte Discovery in Service-Mapping .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery erfasst auch Cloud-Tags, die für jede virtuelle Maschine (VM) spezifisch sind, und speichert sie in der Tabelle „Schlüsselwert“ [cmdb_key_value].

Der Discovery-Prozess erkennt auch Tags, die CIs zugeordnet sind. Wenn Ihre Organisation jedoch keine konsistenten Tagging-Standards oder -Begriffe (Schlüssel-Wert-Paare) verwendet, wird die Verwaltung von CIs mit Tags schwierig.

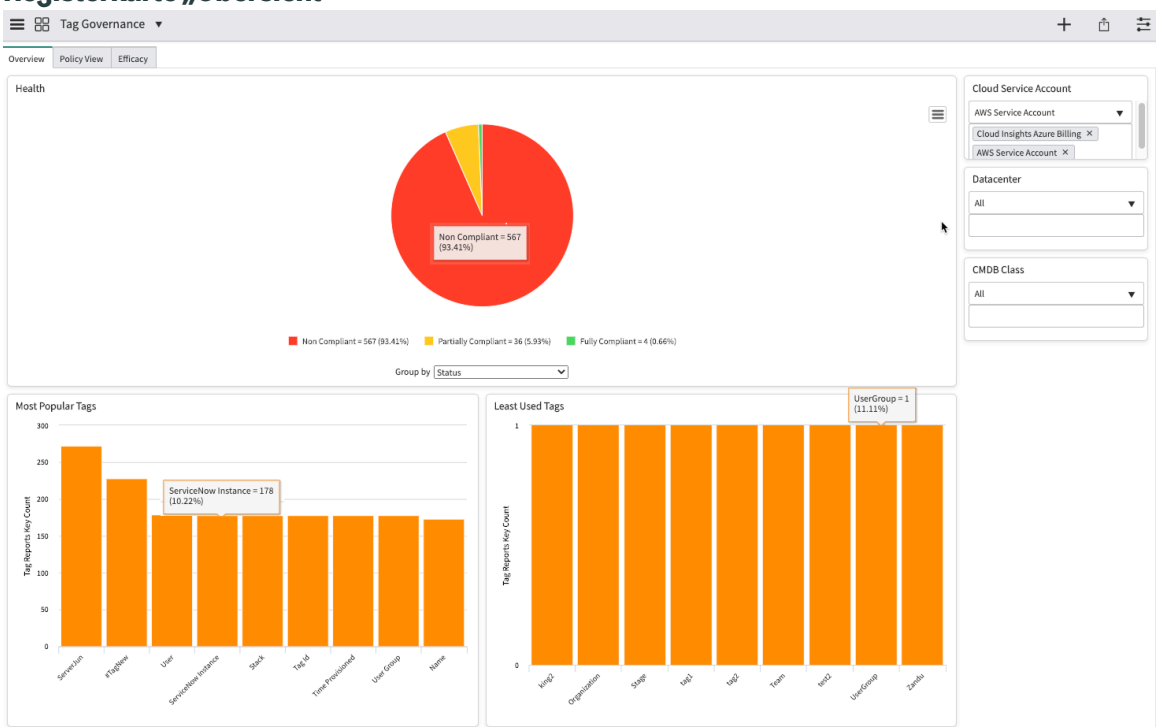
Tag-Governance Dashboard: Registerkarte „Übersicht“

Die **Übersicht** Die Registerkarte verfolgt die Integrität und Compliance von CIs basierend auf Tag-Audits. Interaktive Widgets bieten Informationen, mit denen Sie den Tag-Compliance-Status und die am häufigsten verwendeten und am wenigsten verwendeten Tags anzeigen und analysieren können.

Zugriff auf das Dashboard

Melden Sie sich als an Tag-Governance Administrator (sn_itom_Tag.Tag_Governance_admin) zum Konfigurieren von Berichten und Tag Governance Viewer (sn_itom_Tag.Tag_Reports_Viewer) zum Anzeigen der Berichte. Um auf das Dashboard zuzugreifen, navigieren Sie zu **Tag-Governance** > **Dashboard**an.

Registerkarte „Übersicht“



Filter werden angewendet

Auf der Registerkarte Integrität wird der kumulative Status der Tag-Integrität aller CIs angezeigt, für die die Tag-Audits ausgeführt wurden. Für jede Kategorie werden der prozentuale Anteil und die Anzahl der CIs mit Status „Übereinstimmung“ angezeigt.

Standardmäßig werden Daten nach Status gruppiert. Sie können die Ergebnisse auch mit den Filtern in der Liste **Group By** (Gruppieren nach) gruppieren.

Verwenden Sie die folgenden interaktiven Filter, um Berichte zu verfeinern:

- **Cloud Service Account (Cloud-Servicekonto)**
- **Logisches Rechenzentrum**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **CMDB Class** (CMDB-Klasse)

  Hinweis: Der Filter **CMDB Class** (CMDB-Klasse) gilt nur für den Bericht zur **Tag Health** (Tag-Integrität). Die Verwendung dieses Filters wirkt sich nicht auf die Ergebnisse der Berichte **Most Popular Tags** (Beliebteste Tags) und **Least Used Tags** (Am wenigsten verwendete Tags) aus.

Sie können beispielsweise eine Kombination der Filter **Cloud Service Account** (Cloud-Servicekonto), **CMDB Class** (CMDB-Klasse) und **Logical Datacenter** (Logisches Rechenzentrum) verwenden. Dann können Sie die Tag-Auditergebnisse für die VM-Instanzen anzeigen, die einem bestimmten Cloud-Servicekonto zugeordnet sind und sich in einem bestimmten logischen Rechenzentrum befinden.

Berichte

Tag-Audits werden für alle erkannten Ressourcen in ausgeführt CMDB CI [*cmdb_ci*] Tabelle. Auf der Registerkarte werden Integritäts- und Compliance-Ergebnisse für erkannte CIs angezeigt.

Widget	Beschreibung	Beschreibung
Gesundheitswesen	Kreisdiagramm	Prozentsatz und Anzahl aller CIs in den folgenden Kategorien: • Nicht konform: CIs, die keine der Tag-Richtlinienanforderungen erfüllen. • Teilweise konform: CIs, die einige Tag-Richtlinienanforderungen erfüllen. • Vollständig konform: CIs, die alle Tag-Richtlinienanforderungen erfüllen. Wählen Sie ein beliebiges zugehöriges Segment oder eine zugehörige Kategorie aus, um einen detaillierteren Bericht anzuzeigen.
Most Popular Tags (Beliebteste Tags)	Balkendiagramm	Die zehn am häufigsten verwendeten Tags für alle erkannten CIs, die Tag-Audits bewerten. • Zeigen Sie auf einen Balken, um den entsprechenden Prozentsatz der Gesamtzahl und die Anzahl des Vorkommens des Tags anzuzeigen. • Wählen Sie einen Balken aus, um die Liste der CIs mit diesem Tag anzuzeigen.
Least Used Tags (Am wenigsten verwendete Tags)	Balkendiagramm	Die zehn am wenigsten verwendeten Tags für alle erkannten CIs, die von Tag-Audits bewertet werden.

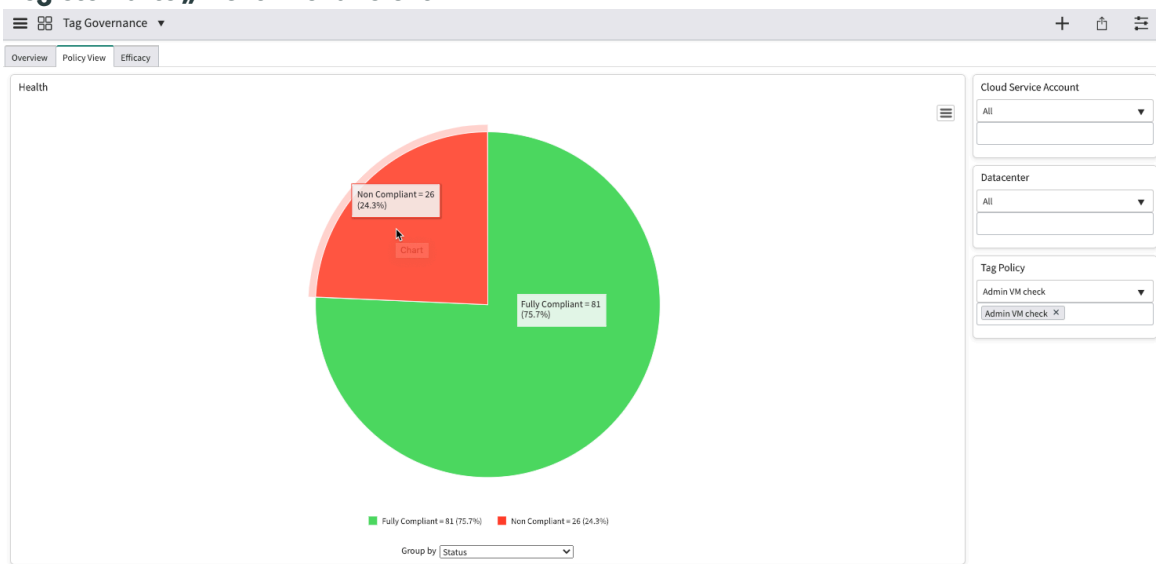
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget	Beschreibung	Beschreibung
		• Zeigen Sie auf einen Balken, um den entsprechenden Prozentsatz der Gesamtzahl und die Anzahl des Vorkommens des Tags anzuzeigen. • Wählen Sie einen Balken aus, um die Liste der CIs mit diesem Tag anzuzeigen.

Tag-Governance Dashboard: Registerkarte „Richtlinienansicht“

Verwenden Sie die Registerkarte Richtlinienansicht, um die Tag-Compliance anzuzeigen und zu analysieren, gefiltert nach Cloud-Service-Account, Tag-Richtlinie und Rechenzentrum. Mit Filtern können Sie sich auf die Verbesserung der Tag-Compliance konzentrieren.

Registerkarte „Richtlinienansicht“



Auf der Registerkarte Richtlinienansicht wird die kumulative Tag-Integrität aller auditierten CIs angezeigt. Das Richtlinien-Dashboard rendert die Compliance von Tag-Richtlinien für erkannte CIs in einem interaktiven Kreisdiagramm. Die Ergebnisse werden in den folgenden Kategorien aufgelistet.

- Vollständig konform: CIs, die alle Tag-Richtlinienanforderungen erfüllen.
- Nicht konform: CIs, die die Anforderungen der Tag-Richtlinie nicht erfüllen.

Verwenden Sie die folgenden interaktiven Filter, um Berichte zu verfeinern:

- **Cloud Service Account (Cloud-Servicekonto)**
- **Rechenzentrum**
- **Tag-Richtlinie**

Sie können beispielsweise eine Kombination aus verwenden **Cloud-Service-Accounts** , **Tag-Richtlinie** , Und **Rechenzentrum** Filter zum Anzeigen von Tag-Audit-Ergebnissen für CIs, die den von Ihnen konfigurierten Filtern entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Wird Erstellt Tag-Governance Richtlinien

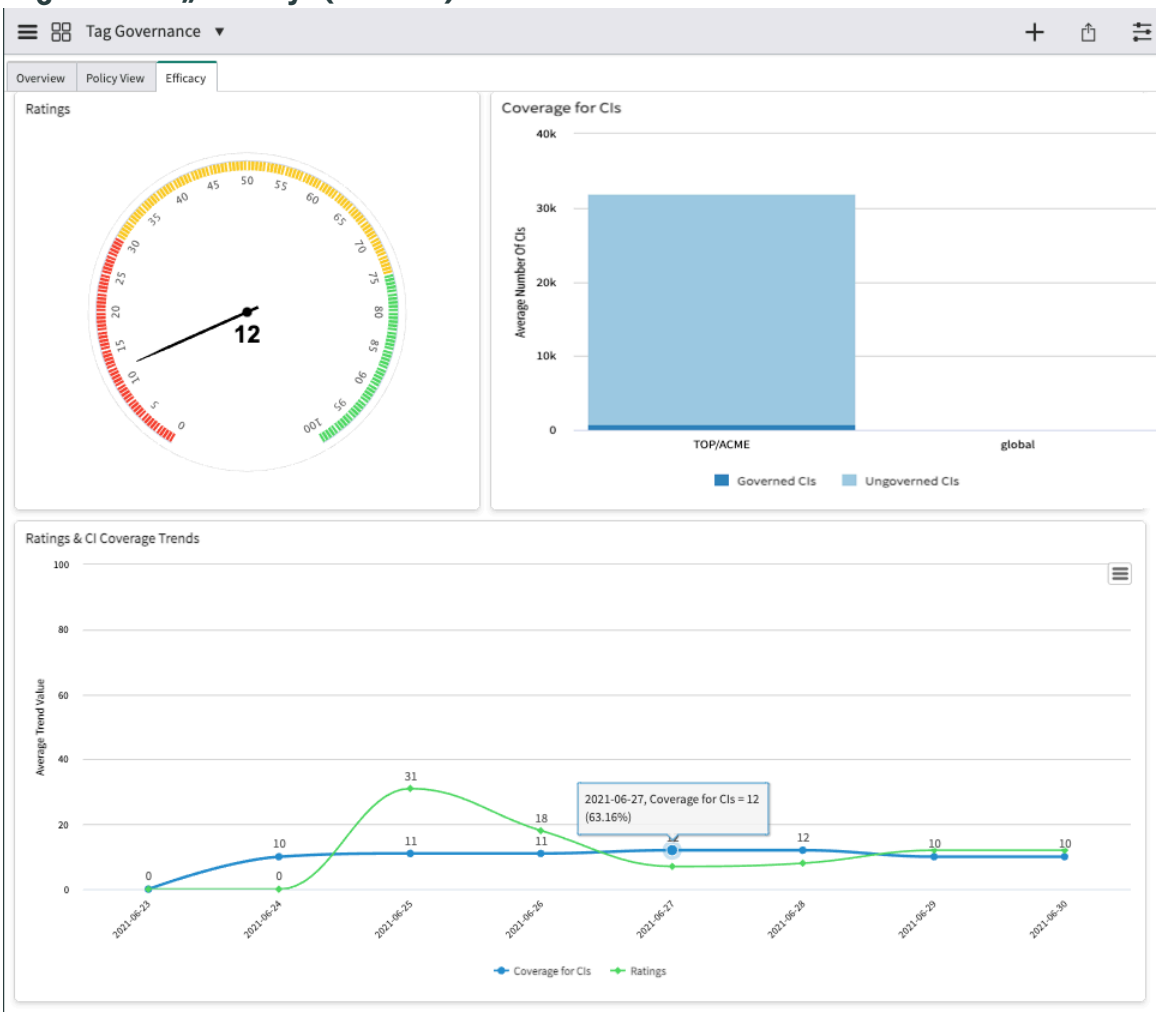
Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

Tag-Governance Dashboard: Registerkarte „Effizienz“

Auf der Registerkarte „Wirksamkeit“ werden die Ergebnisse von Tag-Audits als Tag-Integritätsbewertungen und Compliance-Abdeckung von CIs angezeigt. Interaktive Widgets zeigen den Status der Tag-Abdeckung und Tagging-Trends im Zeitverlauf an.

Registerkarte „Efficacy“ (Effizienz)



Bewertungen

Im Bericht Bewertungen finden Sie Informationen zur Überprüfung der Qualität der CI-Tag-Integrität. Die Punktzahl basiert auf einem Algorithmus, der die folgenden Informationen und die aus Tag-Audit-Ausführungen gesammelten Daten berücksichtigt:

- Compliance der Tag-Richtlinie
- Allgemeine Compliance der CI-Tags

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abdeckung für CIs

Der Bericht „Abdeckung für CIs“ zeigt die Anzahl der CIs in an CMDB Diese Tag-Richtlinien steuern und den Prozentsatz aller CIs, die verwaltet werden. Sie können diese Informationen verwenden, um die Abdeckung von Tag-Richtlinien zu verbessern.

Ratings and CI Coverage Trends (Bewertungen und Trends der CI-Abdeckung)

Die **Trends** Der Bericht zeigt den durchschnittlichen Trendwert im Zeitverlauf der Tag-Governance-Bewertung und der Abdeckung von CIs an. Der Bericht bietet Einblicke in die Entwicklung der Tag-Qualität und der Tag-Abdeckung im Laufe der Zeit.

Berichte

Titel	Typ	Beschreibung
Ratings (Bewertungen)	Messbericht	Punktzahl, die die allgemeine Tagging-Qualitätsbewertung aller CIs angibt. Dieser Wert basiert auf einem Algorithmus, der die Anzahl der CIs, die die Tag-Richtlinie abdeckt, und die Gesamtzahl der CIs verwendet, die die Tag-Richtlinie zertifiziert.
Abdeckung für CIs	Gestapelter Balkenbericht	Prozentsatz und Anzahl aller CIs, die von Tag-Richtlinien gesteuert werden, im Vergleich zu allen CIs in CMDB. Der Wert basiert auf der Gesamtzahl der CIs, die Tag-Richtlinien steuern, geteilt durch die Gesamtzahl der CIs in CMDB. Ein einzelner Balken stellt die CI-Abdeckungsdaten jeder Domäne dar.
Trends	Linientrendbericht	Leistungstrends der Tag-Qualität und der Tag-Abdeckung im Zeitverlauf.

Tag-Kategorisierung in Tag-Governance

Indem getaggte Konfigurationselemente (Configuration Items, CIs) und Cloud-Ressourcen automatisch in eine von fünf sofort einsatzbereiten Kategorien gruppiert werden, Tag-Kategorisierung Optimiert das Ressourcenmanagement. Beispielsweise trägt die automatische Gruppierung zugehöriger Tag-Schlüssel wie „dev“, „Test“ und „Prod“ in der Kategorie „Umgebung“ dazu bei, klare und konsistente Tagging-Praktiken zu fördern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Kategorisierungsanforderungen

Hinweis:

Die Tag-Kategorisierung Funktion in Tag-Governance Nutzt die Tabellen „CI-Tag-Kategorie“ [svc_Tag_Categories] und „CI-Tag-Schlüssel“ [svc_Tag_names] in Service-Mapping. Vollständiger Zugriff auf diese Tabellen erfordert die Installation von Version 1.16.3 oder höher von Service-Mapping Plus. Andernfalls ist der Zugriff auf diese Tabellen möglicherweise eingeschränkt, was Ihre Fähigkeit beeinträchtigt, Tags neu zu kategorisieren, Tag-Definitionen zu ändern oder die Funktion vollständig zu nutzen. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Tag-Kategorisierung – Übersicht

Tag-Kategorisierung Automatisiert den Prozess der Gruppierung getaggter CIs und Cloud-Ressourcen in eine von fünf vordefinierten Kategorien: Anwendungs-ID, Zuweisungsgruppe, Kostenstelle, Umgebung und Besitzer. Diese Kategorien helfen, das Ressourcenmanagement zu optimieren, indem sie sicherstellen, dass Tags einheitlich angewendet und einfach kategorisiert werden. Eine tägliche geplante Aufgabe kategorisiert neu hinzugefügte Tags und ordnet alle nicht erkannten Tag-Schlüssel der entsprechenden Kategorie zu. Weitere Informationen zu den vordefinierten Tag-Kategorien finden Sie unter Mit Tag-Governance installierte Komponenten.

Sie können die Tag-Kategoriedefinitionen ändern, eigene Kategorien erstellen oder nach Bedarf zusätzliche Tag-Schlüssel hinzufügen. Weitere Informationen finden Sie unter Ändern Sie die Tag-Kategorieinformationen für Tag-Kategorisierung.

Die Tag-Kategorierichtlinie bestätigt, dass alle Kategorien ordnungsgemäß zugeordnet und aktuell sind. Es ruft Datensätze ab und überprüft nach Kategoriezuordnungen, um fehlende Kategorien zu identifizieren. CIs, für die eine Kategorie fehlt, werden als nicht konform markiert, sodass Sie Probleme mit Tag-Kategorien beheben und beheben können.

Das System verwendet *`sn_itom_tag.recategorization_required`*Eigenschaft, um zu bestimmen, ob eine Neukategorisierung erforderlich ist. Standardmäßig ist diese Eigenschaft auf „falsch“ festgelegt. Wenn jedoch eine Änderung an einer Kategorie auftritt, legt eine Business-Regel die Eigenschaft auf „wahr“ fest, was darauf hinweist, dass eine Neukategorisierung erforderlich ist. Eine tägliche geplante Aufgabe überprüft diese Eigenschaft dann. Wenn sie auf „wahr“ festgelegt ist, beginnt der Rekategorisierungsprozess. Dieser Prozess aktualisiert die Tag-Zuordnungen automatisch innerhalb von 24 Stunden nach dem Change. Sie können jedoch auch eine Neukategorisierung initiieren, um die Änderungen sofort anzuwenden. Alle Changes und Updates werden in der CI-Tag-Kategorietabelle gespeichert.

Tag-Kategorisierung Und Domänentrennung

Tag-Kategorisierung Unterstützt domänenspezifische Verwaltung. . Bei domänengetrennten Instanzen werden jeder Blattdomäne die Kategorien hinzugefügt. Wenn Sie auf Tags zugreifen oder diese verwalten, ruft das System Domäneninformationen vom CI ab und fügt Tag-Zuordnungen der übereinstimmenden Kategorie in der entsprechenden Domäne hinzu. Für allgemeine Informationen zur Domänentrennung mit Tag-Governance, Siehe Domain Separation und Tag-Governance.

Tag-Governance konfigurieren

Installieren Sie Tag-Governance App, um Tag-Audits auszuführen, das Tag Data Governance-Dashboard anzuzeigen und Tag-Korrektur durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration – Übersicht

- Domain Separation und Tag-Governance

  Die Domänentrennung wird in Tag-Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

- Tag-Governance installieren

  Installieren Sie Tag-Governance App, um Tag-Audits auszuführen, das Tag Data Governance-Dashboard anzuzeigen und Tag-Korrektur durchzuführen.

Tag-Governance installieren

Installieren Sie Tag-Governance App, um Tag-Audits auszuführen, das Tag Data Governance-Dashboard anzuzeigen und Tag-Korrektur durchzuführen.

Vorbereitungen

- Stellen Sie sicher, dass Sie Muster für Discovery und Service-Mapping für tagbasierte Erkennung verwenden.
- Installieren Sie ServiceNow Cloud Access Interface-App für Cloud-Korrektur.

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **ServiceNow Store**an.
2. Verwenden Sie das Suchfeld, um nach zu suchen Tag-Governance Anwendung und wählen Sie aus **Installieren** .

Nächste Maßnahme

Konfigurieren Tag-Governance Richtlinien, die für erkannte Ressourcen ausgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance.

Tag-Governance verwenden

Verwenden Sie ServiceNow® Tag-Governance App zur Identifizierung und Korrektur von lokalen oder Cloud-Ressourcen, die inkonsistent sind und nicht den Tag-Richtlinien Ihrer Organisation entsprechen.

Tag-Governance-Aufgaben

- Wird Erstellt Tag-Governance Richtlinien

  Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an. Sie legen Tag-Richtlinien fest, die die Skalierung und die Anforderungen der verschiedenen Gruppen in Ihrer Organisation unterstützen, damit alle Anwender profitieren können.

- Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

  Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

  Konfigurieren Sie Korrekturoptionen, und zeigen Sie eine Vorschau an, generieren Sie Schlüssel, und führen Sie Aktionen zur Behebung von Nichteinhaltung oder Fehlern aus, die auf Tag-Audit-Berichten basieren.

- Tag-Auditfehler in der Vorschau anzeigen und korrigieren

  Basierend auf den Tag-Richtlinien, die Sie erstellen, können Sie eine Vorschau der Korrektur-Flows anzeigen und fehlende Tags für nicht konforme CIs automatisch generieren.

- Echtzeit-Updates von Tags für Cloud-Ressourcen werden durchgeführt

  Sie können die Verarbeitung von Cloud-Ereignissen einrichten und eine Tag-Richtlinie zuordnen, um Tags für Cloud-Ressourcen in Echtzeit zu aktualisieren.

Wird Erstellt Tag-Governance Richtlinien

Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an. Sie legen Tag-Richtlinien fest, die die Skalierung und die Anforderungen der verschiedenen Gruppen in Ihrer Organisation unterstützen, damit alle Anwender profitieren können.

Überlegungen

Befolgen Sie bei der Definition von Tagging-Standards einen methodischen Ansatz, um die Anzahl der Tags niedrig zu halten. Standardisierte Tag-Richtlinien verbessern die Leistung von Tag-Governance App zum Überwachen und Verwalten von Tags über CIs in Ihrer Organisation.

Möglicherweise benötigen Sie ausführliche Diskussionen und Recherchen, um die Anforderungen aller verschiedenen Teams in Ihrer Organisation zu verstehen. Beispielsweise möchten Finanzteams möglicherweise, dass CIs basierend auf Kostenstellenzuteilungen, Anwendungszuweisungen und Geschäftszweck getaggt werden. Im Gegensatz dazu möchten IT-Sicherheitsteams möglicherweise CIs nach Betriebssystem und Sicherheitspatchebene als Teil ihres Schwachstellenmanagementplans kategorisiert.

Bevor Sie Ihren Tagging-Ansatz abschließen, stellen Sie sicher, dass Sie die folgenden Probleme berücksichtigt haben:

- Tag-Filter, die verschiedene Teams verwenden.
- Die Zugriffsebene, die verschiedene Anwender benötigen.
- Ob Sie Echtzeitprüfungen benötigen.
- Gibt an, ob Sie Tags mit Cloud-Ressourcen synchronisieren müssen.

Zugehörige Informationen

Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an.

Vorbereitungen

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Filter angeben, die den Umfang eines Audits einschränken, z. B. um nur Service-Accounts und Rechenzentren zu auditieren.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Richtlinien**an.
2. Wählen Sie Aus **Neu** Und füllen Sie dann das Formular Tag-Richtlinien aus.
   Die Formularfelder werden in beschrieben Formular „Tag-Richtlinien“.
3. Wählen Sie **Absenden**.
   - Die zugehörige Liste „Tag-Richtlinienausführungen“ zeigt die Liste der Tag-Audit-Ausführungen mit den entsprechenden Status-, erstellt- und aktualisierten Zeitstempeln an.
   - In der zugehörigen Liste aktuelle Richtlinienausführungsergebnisse werden die Ergebnisse der Tag-Audit-Ausführung angezeigt.

Nächste Maßnahme

- Wählen Sie aus **Audit-Ergebnisse Anzeigen** Zugehöriger Link zum Anzeigen aller Audit-Ergebnisse.
- Wählen Sie aus **Punktscan Ausführen** Zugehöriger Link zum Ausführen aller anwendbaren Prüfungen für den Datensatz.
- Weitere Informationen finden Sie unter . Flows Und Subflows .

Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

Konfigurieren Sie Korrekturoptionen, und zeigen Sie eine Vorschau an, generieren Sie Schlüssel, und führen Sie Aktionen zur Behebung von Nichteinhaltung oder Fehlern aus, die auf Tag-Audit-Berichten basieren.

Vorbereitungen

Stellen Sie sicher, dass Tag-Richtlinien konfiguriert sind und sich im Status „aktiv“ befinden.

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Korrektur automatisch ausführen, wenn Sie einer Tag-Richtlinie eine Korrekturrichtlinie zuordnen. Sie können auch die Tags nicht konformer CIs am Ende des Cloud-Providers in Echtzeit aktualisieren.

Konfigurieren Sie Korrekturrichtlinien und -Logik, und aktivieren Sie auch die Aktualisierung von Tags für Cloud-Ressourcen, die folgenden zugeordnet sind CMDB Klassen:

- Virtuelle Maschinen
- Compute-Sicherheitsgruppen
- Speicher-Laufwerke
- Cloud-Netzwerke
- Cloud-Subnetz
- Netzwerkschnittstellen
- Lastenausgleichsmodule
- Verfügbarkeitszonen
- Öffentliche IP-Adressen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Speicherkonten
- Ressourcengruppen

Die Liste von CMDB Klassen, für die Sie Tags für CIs in aktualisieren können CMDB Sowie Cloud-Ressourcen werden auch im Formular „Tag-Korrektur“ angezeigt. Wenn Sie auswählen **Aktualisieren Sie Tags in der Cloud** Kontrollkästchen im Korrekturformular zeigt die Korrektur nur eine Vorschau auf CI-Fehler an, die zu gehören CMDB Klassen aufgelistet.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Korrektur**an.
2. Wählen Sie Aus **Neu** Zum Erstellen eines neuen Datensatzes.
3. Geben Sie im Feld **Name** einen eindeutigen beschreibenden Namen ein.
4. In **Richtlinie** Wählen Sie das Feld aus Suchsymbol.

   Hinweis: Die **Richtlinientyp** Das Feld wird automatisch ausgefüllt, nachdem Sie eine Richtlinie aus der Suchliste ausgewählt haben.

5. Konfigurieren Sie in der Liste Tag-Richtlinien eine Korrekturrichtlinie auf eine der folgenden Arten:
   - Wählen Sie aus der Nachschlageliste eine vorhandene Tag-Richtlinie aus.
   - Wählen Sie **Neu**. Füllen Sie Felder im Formular „Tag-Richtlinien“ aus (die Felder werden in beschrieben Formular „Tag-Richtlinien“.

     Hinweis: Wenn Sie eine neue Tag-Richtlinie erstellen, müssen Sie ein Audit ausführen, bevor Sie Korrektur-Flows ausführen können.

   Sie haben eine Richtlinie für den Fehlerkorrektur-Datensatz erstellt oder ausgewählt.
6. **Wahlweise:** Wählen Sie aus **Automatische Korrektur** Kontrollkästchen zum automatischen Ausführen der Korrektur für nicht konforme CIs.
   Wenn eine Audit-Ausführung abgeschlossen ist, wird die Korrektur für alle CIs mit Richtlinienfehlern ausgeführt.
7. **Wahlweise:** Wählen Sie aus **Aktualisieren Sie Tags in der Cloud** Kontrollkästchen zum Anwenden der Korrektur und Aktualisieren der Tags in der relevanten Cloud-Provider-Umgebung für unterstützt CMDB CI-Klassen.

   Wichtig: Die **Aktualisieren Sie Tags in der Cloud** Funktion funktioniert nur für AWS Und Microsoft Azure Cloud Ressourcen für CMDB Klassen, die im Formular „Tag-Korrektur“ aufgeführt sind. Weitere Informationen finden Sie unter Echtzeit-Updates von Tags für Cloud-Ressourcen werden durchgeführt.

8. Wählen Sie im Formular „Tag-Korrektur“ die Option aus **Übermitteln** .
   Die Korrekturrichtlinie ist konfiguriert. Die Liste Tag-Korrekturen wird geöffnet.

Tag-Auditfehler in der Vorschau anzeigen und korrigieren

Vorschau der Audit-Berichte für Ressourcen anzeigen, die Tag-Richtlinien als nicht konform identifizieren. Beheben Sie Fehler, indem Sie Tags hinzufügen oder aktualisieren.

Vorbereitungen

Konfigurieren Sie Tag-Richtlinien und Korrekturrichtlinien. Siehe Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance und Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das Update auf die Cloud funktioniert nur für AWS Und Microsoft Azure Cloud Ressourcen für CMDB Klassen, die im Formular „Tag-Korrektur“ aufgeführt sind.

Erforderliche Rolle: sn_itom_tag.tag_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Basierend auf den Tag-Richtlinien, die Sie erstellen, können Sie eine Vorschau der Korrektur-Flows anzeigen und fehlende Tags für nicht konforme CIs automatisch generieren. Diese Informationen werden in der zugehörigen Liste „Tag Remediation Preview“ (Vorschau der Tag-Fehlerkorrektur) angezeigt. Siehe Flows Und Subflows .

Hinweis:

- Wenn Sie bei der Konfiguration der Fehlerkorrektur das Kontrollkästchen **Update Tags in Cloud** (Tags in Cloud aktualisieren) aktivieren, werden in der Vorschau Auditfehler herausgefiltert, die zu den aufgeführten CI-Klassen gehören.
- Wenn Sie beide ausgewählt haben **Automatische Korrektur** Und **Aktualisieren Sie Tags in der Cloud** Einstellungen beim Konfigurieren der Korrektur werden Tags in beiden aktualisiert CMDB Und in Cloud-Ressourcen (nur für unterstützt CMDB CI-Klassen).
- Wenn Sie nur auswählen **Automatische Korrektur** , Die Korrektur wird ausgeführt und aktualisiert Tags in CMDB Allein.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Korrektur**an.
2. Wählen Sie in der Liste der Tag-Fehlerkorrekturen den Datensatz aus, den Sie anzeigen möchten.
3. Wählen Sie aus **Vorschau Der Korrektur Anzeigen** Zugehöriger Link.
   In der zugehörigen Liste „Tag Remediation Previews“ (Vorschau der Tag-Fehlerkorrektur) werden die nicht konformen CIs angezeigt.
4. Wählen Sie die zugehörige Liste Vorschauen der Tag-Korrektur aus, um die fehlenden Tags und ihre Werte zu identifizieren.
5. Wählen Sie in der zugehörigen Liste „Tag-Korrekturschlüssel“ die Option aus **Neu** Dient zum Erstellen eines Tags-Korrekturschlüssels.
   Die Felder im Formular „Tag-Korrekturschlüssel“ werden in beschrieben Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur).
6. Wählen Sie **Absenden**.
   Sie haben die Schlüssel zur Tag-Korrektur erstellt, die der Richtlinie zugeordnet sind.
7. **Wahlweise:** Wählen Sie aus **Schlüssel Generieren** Zugehöriger Link, wenn Sie ausgeführt haben **Tag-Schlüsselrichtlinie** .
   Der zugehörige Link **Generate Keys** (Schlüssel generieren) wird nur für den Richtlinientyp `Tag Key Policy` angezeigt. Da die Richtlinie die erwarteten Tags angibt, können Sie auswählen **Schlüssel Generieren** Zugehöriger Link zum Generieren der Schlüssel, die Sie für die Korrektur benötigen, anstatt sie manuell in der zugehörigen Liste „Tag-Korrekturschlüssel“ hinzuzufügen.
8. **Wahlweise:** Wählen Sie aus **Generieren Sie Schlüsselwerte** Zugehöriger Link, wenn Sie ausgeführt haben **Tag-Schlüssel- Und Wertrichtlinie** .
   Der zugehörige Link **Generate Key Values** (Schlüsselwerte generieren) wird nur für den Richtlinientyp `Tag Key and Value Policy` angezeigt. Da Sie die Werte, nach denen Sie in der Tag-Richtlinie suchen, bereits angegeben haben, können Sie auswählen **Generieren Sie Schlüsselwerte** Zugehöriger Link zum Hinzufügen der erwarteten Schlüsselwerte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie aus **Tags Nachbessern** Zugehöriger Link.
   Der Fehlerkorrektur-Flow zum Hinzufügen fehlender Tags wird initiiert. Eine entsprechende Informationsmeldung wird im Formular angezeigt, wenn die Fehlerkorrektur aktiv ist. Wählen Sie aus **Weitere Informationen** Link in der Nachricht, um zum Standard-Flow-Kontext zu navigieren.

Ergebnis

Basierend auf den Tag-Auditergebnissen und den von Ihnen erstellten Schlüsseln der Tag-Fehlerkorrektur fügt der Fehlerkorrektur-Flow den nicht konformen CIs fehlende Tags hinzu, um die Richtlinienkonformität herzustellen.

Echtzeit-Updates von Tags für Cloud-Ressourcen werden durchgeführt

Sie können die Verarbeitung von Cloud-Ereignissen einrichten und eine Tag-Richtlinie zuordnen, um Tags für Cloud-Ressourcen in Echtzeit zu aktualisieren.

Voraussetzungen

- Die Tabelle „Cloud-Ereignisse“ [sn_CMP_Cloud_Events] enthält keine Datensätze in *processed*status.
- CIs, die von Tag-Change-Events betroffen sind, werden entweder durch CAPI oder Discovery and Service Mapping Patterns identifiziert.
- Mindestens eine Tag-Richtlinie konfiguriert.
- Wählen Sie aus **Für Cloud-Ereignisse ausführen** Kontrollkästchen in der Tag-Richtlinie, die Sie erstellen.

Anweisungen hängen vom Cloud-Provider ab

Die folgenden Setup-Anweisungen für die Cloud-Ereignisverarbeitung finden Sie:

- Konfigurieren Sie den Amazon AWS Config-Service, um die CMDB automatisch zu aktualisieren
- Konfigurieren Sie den Microsoft Azure-Warnungsservice, um die CMDB automatisch zu aktualisieren
- Konfigurieren Sie den Logging-Service der Google Cloud Operations Suite, um die CMDB automatisch zu aktualisieren

Verarbeiten Sie Cloud-Ereignisse im Zusammenhang mit Änderungen an Tags, und führen Sie Tag-Audits für die Ereignisse in Echtzeit aus.

Im Gegensatz zu regulären Tag-Audits, bei denen das Audit für alle CIs in durchgeführt wird CMDB Für die die Tag-Richtlinie gilt, werden Tag-Ereignisse pro CI verarbeitet. Basierend auf den Voraussetzungen erfolgt die Tag-Event-Verarbeitung für Events, die mit einem Tag-Change identifiziert werden. Das betroffene CI wird identifiziert, und wenn die zugeordnete Richtlinie für das CI gilt, wird die Tag-Richtlinie für das identifizierte CI ausgeführt.

Wenn **Für Cloud-Ereignisse ausführen** Das Kontrollkästchen ist während der Richtlinienerstellung aktiviert. Die Richtlinie wird ausgewählt, um ein Audit für Tag-Change-Ereignisse auszuführen. Wenn das Kontrollkästchen deaktiviert ist, wird das Audit für das CI nicht ausgeführt, auch wenn Cloud-Ereignisse für Tag-Change vorliegen.

Zeigen Sie den Change-Typ an, der für das Tag gilt (der Change, der das Audit ausgelöst hat), in der Tabelle „Tag-Change-Protokoll“ [sn_itom_Tag_Change_log]. Die Datensätze in der Tabelle werden standardmäßig 90 Tage lang gespeichert. Die Change-Protokolldatensätze werden angezeigt, ob eine Korrekturausführung oder ein Ereignis den Change für das CI ausgelöst hat. Sie können auch Tags anzeigen, die als Teil des Change hinzugefügt oder aktualisiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Leistung wird optimiert

Ein hoher Ereigniseinfluss oder eine große Anzahl von Tag-Richtlinien kann die Leistung verringern. Sie können die folgenden Systemeigenschaften ändern, um eine akzeptable Leistung sicherzustellen:

- [sn_itom_tag.azure_window_size] – Diese Systemeigenschaft ist konfigurierbar (in Minuten).
- [sn_itom_Tag.max_Audit_lag_ratio] – Geben Sie die Verzögerung zwischen Tag-Audits an, die bereits ausgeführt werden, bevor das Audit für die Datensätze ausgelöst wird, die für das Audit bereit sind.
- [sn_itom_Tag.Policy_Batch_size]: Batch-Größe, für die das Tag-Audit ausgeführt wird.
- [sn_itom_Tag.event_Batch_size]: Zu verarbeitende Ereignisbatgröße.

Ändern Sie die Tag-Kategorieinformationen für Tag-Kategorisierung

Ändern Sie Tag-Kategoriedefinitionen, um zu unterstützen Tag-Kategorisierung Und stellen Sie sicher, dass Tag-Kategorien Ihren Anforderungen für Datenverwaltung und -Klassifizierung entsprechen.

Vorbereitungen

Stellen Sie sicher, dass Sie Version 1.16.3 von installiert haben Service-Mapping Plus Für den Zugriff auf die Tabellen „CI-Tag-Kategorie“ und „CI-Tag-Schlüssel“. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Erforderliche Rolle: Tag_Governance_admin

Prozedur

1. Navigieren zu **Alle** > *Tag-Governance* > **Tag-Kategorien**an.
2. Stellen Sie sicher, dass Sie sich in der Blattdomäne befinden.
   a. Wählen Sie im Header der Seite das Globus-Symbol aus .
   b. Wählen Sie Aus **Domänenbereich** , Und wählen Sie die entsprechende Blattdomäne aus.
3. Wählen Sie die Kategoriedefinition für die Tag-Kategorie aus, die Sie ändern möchten.
4. In **Regulärer Ausdruck** Feld ändern Sie die Definition.
   Sie können einen vorhandenen Wert (regulärer Ausdruck) löschen oder einen neuen Wert (regulärer Ausdruck) in diesem Feld hinzufügen.
5. **Wahlweise:** Geben Sie einen Wert in ein **Priorität** Feld zum Festlegen einer Priorität für diese Tag-Kategorie.
   Da ein Tag-Schlüssel zu mehreren Kategorien gehören kann. Durch Festlegen der Priorität wird dies sichergestellt Tag-Kategorisierung Ordnet CIs der richtigen Kategorie zu.
6. Wählen Sie Aus **Aktualisieren** Um die Änderungen zu speichern.
7. Wenn Sie Ihre Änderungen sofort anwenden möchten, anstatt innerhalb von 24 Stunden auf die automatische Aktualisierung zu warten, wählen Sie aus **Tags Neu Kategorisieren** Schaltfläche.

Fügen Sie eine Tag-Kategorie für hinzu, oder löschen Sie sie Tag-Kategorisierung

Fügen Sie eine Tag-Kategorie hinzu, oder löschen Sie sie, um das Tagging der Konfigurationselemente (CIs) und Cloud-Assets Ihrer Organisation zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Sie Version 1.16.3 von installiert haben Service-Mapping Plus Für den Zugriff auf die Tabellen „CI-Tag-Kategorie“ und „CI-Tag-Schlüssel“. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Erforderliche Rolle: Tag_Governance_admin

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Tag-Kategorien**an.
2. Stellen Sie sicher, dass Sie sich in der Blattdomäne befinden.
   a. Wählen Sie im Header der Seite das Globus-Symbol aus .
   b. Wählen Sie Aus **Domänenbereich** , Und wählen Sie die entsprechende Blattdomäne aus.
3. Fügen Sie eine Tag-Kategorie hinzu, oder löschen Sie sie.

Aktion	Beschreibung
Fügen Sie eine Tag-Kategorie hinzu	a. Wählen Sie **Neu**. b. Geben Sie den Kategorienamen in ein **Tag-Kategoriename** Feld. c. Wählen Sie das Symbol mit Liste suchen . d. Wählen Sie Aus **Neu** Im Fenster „Tag-Kategoriedefinitionen“. e. Geben Sie den Wert für die Kategoriedefinition in ein **Regulärer Ausdruck** Feld. **Hinweis:** Der reguläre Ausdruck identifiziert die Tag-Werte, die in der Kategorie enthalten sind. Trennen Sie mehrere Werte durch einen vertikalen Schrägstrich (|). f. Aktualisieren Sie den Prioritätswert. g. Wählen Sie **Absenden**. h. Wählen Sie Aus **Übermitteln** Auf der Seite „CI-Tag-Kategorie – neuer Datensatz“.
Löschen Sie eine Tag-Kategorie	a. Aktivieren Sie das Kontrollkästchen neben der Tag-Kategorie. b. In **Aktionen für ausgewählte Zeilen** Menü auswählen **Löschen** .

4. Wenn Sie Ihre Änderungen sofort anwenden möchten, anstatt innerhalb von 24 Stunden auf die automatische Aktualisierung zu warten, wählen Sie aus **Tags Neu Kategorisieren** Schaltfläche.

Legen Sie die Priorität für Tag-Kategoriedefinitionen für fest Tag-Kategorisierung

Legen Sie die Priorität für Tag-Kategoriedefinitionen fest, um sicherzustellen, dass Tag-Schlüssel, die zu mehreren Kategorien gehören, ordnungsgemäß kategorisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Sie Version 1.16.3 von installiert haben Service-Mapping Plus Für den Zugriff auf die Tabellen „CI-Tag-Kategorie“ und „CI-Tag-Schlüssel“. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Ein Tag-Schlüssel kann mehreren Kategorien angehören. Durch Festlegen der Priorität wird dies sichergestellt Tag-Kategorisierung Ordnet Konfigurationselemente (Configuration Items, CIs) und Cloud-Ressourcen der richtigen Kategorie zu.

Beispielsweise kann der Tag-Schlüssel „Anwendung“ sowohl zu den Tag-Kategorien „Anwendung“ als auch „Kostenstelle“ gehören. Legen Sie die Prioritäten für die Tag-Kategorien „Kostenstelle“ und „Anwendung“ auf 100 bzw. 101 fest, um die Zuordnung zur Kategorie „Anwendung“ zu priorisieren. Wenn ein Konflikt auftritt, stellt diese Einstellung sicher, dass die Kategorie „Anwendung“ eine höhere Priorität hat, und ordnet ihr automatisch den Tag-Schlüssel zu.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Tag-Kategorien**an.
2. Stellen Sie sicher, dass Sie sich in der Blattdomäne befinden.
   a. Wählen Sie im Header der Seite das Globus-Symbol aus .
   b. Wählen Sie Aus **Domänenbereich** , Und wählen Sie die entsprechende Blattdomäne aus.
3. Wählen Sie die Kategoriedefinition für die Tag-Kategorie aus, deren Priorität Sie festlegen möchten.
4. Legen Sie im Feld Priorität den Wert fest.
5. Wählen Sie Aus **Aktualisieren** Um die Änderung zu speichern.
6. Wenn Sie Ihre Änderungen sofort anwenden möchten, anstatt innerhalb von 24 Stunden auf die automatische Aktualisierung zu warten, wählen Sie aus **Tags Neu Kategorisieren** Schaltfläche.

Fügen Sie Tag-Schlüssel für hinzu, oder löschen Sie sie Tag-Kategorisierung

Fügen Sie Tag-Schlüssel hinzu, oder löschen Sie sie, um sicherzustellen, dass sie Ihren Anforderungen für Datenverwaltung und -Klassifizierung entsprechen.

Vorbereitungen

Stellen Sie sicher, dass Sie Version 1.16.3 von installiert haben Service-Mapping Plus Für den Zugriff auf die Tabellen „CI-Tag-Kategorie“ und „CI-Tag-Schlüssel“. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Erforderliche Rolle: Tag_Governance_admin

Prozedur

1. Navigieren zu **Alle** > *Tag-Governance* > **Tag-Kategorien**an.
2. Stellen Sie sicher, dass Sie sich in der Blattdomäne befinden.
   a. Wählen Sie im Header der Seite das Globus-Symbol aus .
   b. Wählen Sie Aus **Domänenbereich** , Und wählen Sie die entsprechende Blattdomäne aus.
3. Wählen Sie die Tag-Kategorie aus, der Sie Tag-Schlüssel hinzufügen oder löschen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Unter **CI-Tag-Schlüssel** , Fügen Sie entweder einen neuen Tag-Schlüssel hinzu, oder löschen Sie einen vorhandenen Tag-Schlüssel.

Aktion	Schritte
Fügen Sie einen Tag-Schlüssel hinzu	**a.** Doppelklicken Sie unter auf die leere Zeile **Tag-Schlüssel** , Wo Sie sehen **Fügen Sie eine neue Zeile ein** . **b.** Fügen Sie im Feld einen Schlüsselnamen hinzu. **c.** Wählen Sie das Symbol Speichern . **d.** Wiederholen Sie die vorherigen Schritte, um weitere Tag-Schlüssel hinzuzufügen. **e.** Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
Löschen Sie einen Tag-Schlüssel	**a.** Unter **Tag-Schlüssel** , Wählen Sie das Symbol zum Löschen markieren Neben dem Tag-Schlüssel, den Sie entfernen möchten. **b.** Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

5. Wenn Sie Ihre Änderungen sofort anwenden möchten, anstatt innerhalb von 24 Stunden auf die automatische Aktualisierung zu warten, wählen Sie aus **Tags Neu Kategorisieren** Schaltfläche.

Tag-Governance – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Tag-Governance Formulare und andere Ressourcen.

Domain Separation und Tag-Governance

Die Domänentrennung wird in Tag-Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domänentrennung

Sie können CIs oder Cloud-Ressourcen identifizieren, die inkonsistent sind und nicht den Richtlinien entsprechen, die Sie für die Steuerung von Tag-Daten konfigurieren. In Tag-Governance, Domänentrennung zielt auf Anwendungsfälle der anfordernden Mandantendomäne in einer Anwendung ab. Die Anwendung wurde entwickelt, um Aktivitäten der anfordernden Person in Mandantendomänen zu unterstützen. Es wurde Logik zum Weiterleiten von Daten an Mandantendomänen abhängig von den jeweiligen Anwendungsfällen implementiert. Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend normal funktioniert. Die Anwendung verarbeitet die Datenweiterleitung an Domänen.

Alle Tabellen in Tag-Governance unterstützen nur Datentrennung, delegierte Domänentrennung wird dagegen nicht unterstützt.

Um sicherzustellen, dass domänensensible Informationen in einer globalen Domäne nicht verfügbar sind, stellen Sie sicher, dass Sie Richtlinien auf Domänenebene und nicht auf globaler Ebene erstellen. Erstellen Sie beim Verwalten von Service Providern Richtlinien auf Service Provider-Ebene. Wenn Sie stattdessen Richtlinien auf globaler Ebene erstellen, werden beim Ausführen des Audits die Ergebnisse „Ausführen“ in der globalen Domäne anstelle der jeweiligen Domänen erstellt.

Zugehörige Informationen

Domänentrennung für Service Provider

Tag-Richtlinien und -Korrektur für AWS

Tag-Audits wenden Richtlinien auf erkannte CIs an, um die Tag-Compliance zu bestimmen, das Vorhandensein von Tags, die entsprechende Anzahl von Tags und das Vorhandensein angegebener Schlüssel-Wert-Paare.

Tag-Richtlinien

Führen Sie ein Tag-Audit aus, um erkannte CIs für die folgenden Tag-Richtlinientypen zu auditieren:

- Tag-Anzahl: Überprüft CIs auf die von Ihnen angegebene Tag-Schlüsselanzahl
- Tag-Anwesenheit: Überprüft CIs auf das Vorhandensein der von Ihnen angegebenen Tag-Schlüsselwerte
- Tag-Schlüssel und -Wert: Überprüft CIs auf das Vorhandensein von Schlüssel-Wert-Paaren, die Sie angeben.

Geben Sie den Zeichenfolgewert oder die Tag-Schlüssel, nach denen Sie suchen, in einem kommagetrennten Format im Richtlinientyp „Tag Presence“ (Tag-Vorhandensein) an. Sie können auch eine Zahl im Richtlinientyp „Tag Count“ (Tag-Anzahl) angeben, um CIs mit einem oder mehreren Tags zu identifizieren. Nachdem Sie die Tag-Audits ausgeführt haben, können Sie Audit-Ergebnisse anzeigen und Korrekturmaßnahmen konfigurieren, die auf der Compliance-Indexqualität basieren. Optional können Sie auch Benutzergruppen und Benutzern Folgeaufgaben für Korrekturaufgaben für nicht konforme CIs zuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die automatische Korrektur funktioniert mit der Rolle „Übernehmen“ auf AWS Um das Tagging von Cloud-Ressourcen zu automatisieren, führen Sie die Schritte in aus Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.

Die Übernahmerolle muss über die folgenden Berechtigungen (Richtlinie) verfügen, damit die Korrektur funktioniert:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "tag:TagResources",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:ec2:*:*:vpc/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
        "arn:aws:ec2:*:*:availability-zone/*",
        "arn:aws:ec2:*:*:public-ip/*",
        "arn:aws:storagegateway:*:*:gateway/*",
        "arn:aws:resource-groups:*:*:group/*"
      ]
    }
  ]
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn bei der Tag-Korrektur festgestellt wird, dass Discovery keine Anmeldeinformationen hat, MID-Server Mit Tag-Management-Fähigkeit wird ausgewählt. Fügen Sie daher die Funktion „Tag-Management“ zur richtigen hinzu MID-Server Mit angehängter IAM-Rolle des Service-Accounts. Diese Aktion ist wichtig, da mehrere Accounts mit der IAM-Rolle vorhanden sein können MID Servers Muss auswählen.

Weitere Informationen finden Sie unter Kontakt Kundenservice und Support an.

Formular „Tag-Richtlinien“

Sie verwenden das Formular „Tag-Richtlinie“, um Tag-Compliance- und Integritätsrichtlinien zu konfigurieren, die in Tag-Audits für erkannte Cloud-Ressourcen oder CIs verwendet werden.

Formular „Tag-Richtlinien“

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für die Richtlinie.
Kurzbeschreibung	Eine kurze Zusammenfassung, die die Richtlinie beschreibt.
Richtlinientyp	Auswahl des Richtlinientyps für das Audit der Tag-Compliance und -Integrität. • Richtlinie für Tag-Anzahl: Überprüfen Sie auf eine bestimmte Anzahl von Tags für CIs. • Tag-Schlüsselrichtlinie: Nach Tags mit bestimmten Werten (Zeichenfolgenausdrücke) suchen. • Tag-Schlüssel- und Wertrichtlinie: Überprüfen Sie auf Schlüssel-Wert-Paare und Wertzeichenfolgen. • Tag-Kategorierichtlinie: Nach Tags mit einer bestimmten Kategorie suchen. **Wichtig:** Sie müssen in einer Blattdomäne arbeiten, um die Tag-Kategorierichtlinie zu verwenden. Basierend auf Ihrer Auswahl geben Sie zusätzliche Werte an.
Erwartete Tag-Anzahl	Dieses Feld wird nur angezeigt, wenn **Richtlinie Für Tag-Anzahl** Richtlinientyp ist ausgewählt. CIs mit weniger Tags als die angegebene Zahl werden als fehlgeschlagen oder nicht konform betrachtet. CIs, die den Wert erfüllen, gelten als für diese Richtlinie zertifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“ (Fortsetzung)

Feld	Beschreibung
	Beispiel: Wenn Sie angeben `4` , Überprüft die Richtlinie, ob für die CIs mindestens vier Tags angegeben sind.
Erwartete Tag-Schlüssel	Dieses Feld wird nur angezeigt, wenn **Tag-Schlüsselrichtlinie** Richtlinientyp ist ausgewählt. Richtlinie, die erkannte CIs auf die in angegebenen Tags überprüft **Erwartete Tag-Schlüssel** Feld. Geben Sie mehrere Tags oder Zeichenfolgenausdrücke in einer kommagetrennten Liste an. Beispiel: Wenn Sie angeben `prod, Finanzen, Kostenstelle` Die Richtlinie überprüft, ob die CIs alle angegebenen Tags haben. CIs, die alle angegebenen Tags aufweisen, gelten als zertifiziert oder vollständig konform. Wenn CIs eines der aufgelisteten Tags fehlen, gelten sie als fehlgeschlagen oder nicht konform.
Prüfungen von Tag-Schlüsseln und -Werten	Führen Sie diese Richtlinie aus, um erkannte CIs für den in angegebenen Tag-Schlüssel und die in angegebenen Werte zu überprüfen **Tag-Schlüssel-Und Wertprüfungen** Feld. Sie können mehrere Tag-Schlüssel-Wert-Paare oder ein Skript angeben, um nach einer Sammlung von Werten zu suchen. Sie können beispielsweise angeben `Anwender` In **Schlüssel** Feld, und `Administrator` In **Wert** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“ (Fortsetzung)

Feld	Beschreibung

	Hinweis:
	Die **Skript** Feld wird nur angezeigt, wenn **Tag-Schlüssel- Und Wertrichtlinie** Ist in ausgewählt **Richtlinientyp** Feld. Verwenden Sie **Skript** Feld zum Angeben mehrerer Werte, um einen Zeichenfolgensatz zurückzugeben.
	Beispielcode
	`// The script should return a string set to tagValues variable.`
	`// the code sets the tagValues array with name of the CI`
	`// by this the check will be done for the tag to match the CI's name`
	`tagValues = [ci.name.toString()];`

Aktiv	Option zum Aktivieren oder Deaktivieren des Ausführungszeitplans.
Für Cloud-Ereignisse ausführen	Option zum Aktivieren von Echtzeit-Audit-Ausführungen, wenn Cloud-Ereignisse auftreten. **Hinweis:** Stellen Sie sicher, dass Sie die automatische Aktualisierung von konfiguriert haben CMDB Mit Cloud-Ereignissen für den relevanten Cloud-Provider.
Speichern Sie das Audit-Ergebnis des Zertifikats	Option zum Speichern der Zertifizierungs-Audit-Ergebnisse und zum Einbeziehen von Tag-Audit-Ergebnissen in die Integritätsberechnungen eines CI. **Hinweis:** Diese Option kann aktiviert werden, wenn es geschäftlich erforderlich ist, Tag-Audit-Ergebnisse in CI-Integritätsberechnungen zu integrieren.
Ausführen	Häufigkeit, mit der das Tag-Audit ausgeführt wird. • **Täglich** • **Monatlich** • **Wöchentlich** • **In regelmäßigen Abständen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“ (Fortsetzung)

Feld	Beschreibung
	• **Einmal** • **Bei Bedarf** **Hinweis:** Um ein Audit sofort nach der Konfiguration der Richtlinie auszuführen, wählen Sie aus **Bei Bedarf** Option. • **Business Calendar: Entry Start (Geschäftskalender: Eintragsbeginn)** • **Business Calendar: Entry End (Geschäftskalender: Eintragsende)**
Nächstes geplantes Ausführungsdatum	Datum und Uhrzeit der nächsten geplanten Ausführung des Tag-Audits. Dieses Feld wird nur für geplante Ausführungen und nicht für Ausführungen bei Bedarf angezeigt.
Filter	Bedingungsanweisungen mit einer Reihe von kontextabhängig generierten Feldern. Verwenden Sie Nachschlagelisten, um Bedingungen zu erstellen und die für das Audit geeigneten CIs zu filtern. Dynamische Bedingungen und Filter, die Sie angeben, um die gewünschten Tags basierend auf Servicekonten und zugehörigen Rechenzentren abzurufen.
Tabelle	Zeigt an `Configuration Item [cmdb_ci]`Tabelle, auf die Filter angewendet werden.
Richtlinienkriterien	Andere Richtlinienkriterien, die Sie mit dynamisch gefüllten Referenznachschlaglisten konfigurieren können. Die Tabelle „Konfigurationselement“ [cmdb_ci] füllt die Daten für diese Suchliste aus. Weitere Informationen finden Sie unter Referenzsuche .
Tag-Filter	Filtern Sie CIs weiter basierend auf Ihren Angaben für **Schlüssel**, **Stichwörter** und **Wert**. Verwenden Sie den Bedingungsgenerator, um einen Filter anzupassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“ (Fortsetzung)

Feld	Beschreibung
Aufgabenzuweisung	Option zum Zuweisen von Folgeaufgaben zu Benutzern oder Benutzergruppen.
Aufgaben erstellen	Option zum Erstellen von Folgeaufgaben. **Hinweis:** Wenn einer CI- und Tag-Richtlinie eine Aufgabe zugeordnet ist, wird die verwendet `sn_itom_tag.allow_new_cert_follow_on_task`Die Systemeigenschaft bestimmt, ob bei einem Compliance-Fehler eine neue Aufgabe erstellt oder eine vorhandene aktualisiert werden soll: • Um die vorhandene Aufgabe mit den Compliance-Fehlerdetails zu aktualisieren, aber keine neue Aufgabe zu erstellen, legen Sie die Eigenschaft auf „falsch“ fest (Standard). • Um eine neue Aufgabe zu erstellen, legen Sie die Eigenschaft auf „wahr“ fest.
Gruppe	Dieses Feld wird nur angezeigt, wenn Sie auswählen **Erstellen Sie Aufgaben** Kontrollkästchen. Zuweisungsgruppe, der die Aufgabe zugewiesen werden soll. Verwenden Sie Suchlisten, um eine Gruppe auszuwählen.
Anwender	Ein bestimmter Benutzer der Zuweisungsgruppe, dem Sie die Aufgabe zuweisen möchten. Verwenden Sie Nachschlagelisten, um einen Benutzer auszuwählen. Dieses Feld wird nur angezeigt, wenn Sie auswählen **Erstellen Sie Aufgaben** Kontrollkästchen.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur)

Sie verwenden das Formular „Tag-Korrekturschlüssel“, um einen Tag-Korrekturschlüssel zu erstellen.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur)

Feld	Beschreibung
Schlüssel	Tag-Schlüsselwert, der zur Fehlerkorrektur nicht konformer CIs verwendet wird. Wenn in der Fehlerkorrekturvorschau als Wert beispielsweise Kostenstelle angezeigt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur) (Fortsetzung)

Feld	Beschreibung
	wird, können Sie die Kostenstelle als neuen Fehlerkorrekturschlüssel angeben, sofern dieser noch nicht vorhanden ist.
Reihenfolge	Reihenfolge der Ausführung, die das System berücksichtigt, wenn Sie die Korrektur initiieren. Sie können beispielsweise eine Tag-Anzahlrichtlinie für vier Tags ausführen und CIs identifizieren, denen zwei Tag-Schlüssel fehlen. Wenn Sie mehrere Fehlerkorrekturschlüssel konfiguriert haben, berücksichtigt das System die beiden Schlüssel mit den niedrigsten Werten im Reihenfolgefeld.
Fehlerkorrektur	Name der Fehlerkorrektur und Datensatzvorschau.
Werttyp	Typ des Werts, den Sie in angeben **Wert** Feld – **Statisch** Oder **Zeichenfolge** . Je nach Auswahl müssen Sie ein Skript oder einen Wert für den Tag-Schlüssel angeben.
Wert	Zeichenfolgenwert für den Schlüssel, den Sie erstellen. Dieses Feld wird nur angezeigt, wenn **Zeichenfolge** Ist in ausgewählt **Werttyp** Feld.
Skript	Skriptcode zum Generieren von Werten für den Schlüssel. Dieses Feld wird nur angezeigt, wenn **Skript** Ist in ausgewählt **Werttyp** Feld.

Mit Tag-Governance installierte Komponenten

Mehrere wichtige Komponenten werden mit installiert oder mit verknüpft Tag-Governance Plugin zur Standardisierung und Verwaltung der Tags Ihrer Organisation.

Installierte Rollen

Rollentitel	Beschreibung	Enthält Rollen
[Tag_Governance_admin]	Richtet die Tag-Governance-Anwendung ein und verwaltet sie. Definiert und erzwingt Tag-Richtlinien, verwaltet Tag-Kategorien und -Werte und fördert die Compliance mit Organisationsstandards. Führt eine erweiterte Konfiguration	• [itil] • [Certification_admin] • [discovery_admin] • [flow_operator]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel	Beschreibung	Enthält Rollen
	und Anpassung von Tag-Governance-Funktionen durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.	
[Tag_Reports_Viewer]	Zeigt Tag-Berichte im Zusammenhang mit Tag-Nutzung und Compliance an und analysiert sie. Weisen Sie diese Rolle Anwendern zu, die Tag-Daten überwachen und analysieren.	[cmdb_read]

Tag-Kategorien installiert

Ab Version 1,7 werden die in der Tabelle aufgeführten vordefinierten Kategorien mit installiert Tag-Governance Und erfordern die Installation von mindestens Service-Mapping Plus Version 1.16.3. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.

Tag-Kategorie	Definition (Regulärer Ausdruck)
Anwendungs-ID	applicationid|Anwendungs-ID|App-ID|appID|Anwendungs-ID| App-ID
Zuweisungsgruppe	Zuweisungsgruppe|Zuweisungsgruppe_Gruppe| Zuweisungsgruppe|Zuweisungsgruppe| Zuweisungsgruppe
Kostenstelle	kostenstelle|Kostenstelle|Cost_Center|Kostenstelle| Kostenstelle|Kostenstelle
Umgebung	umgebung|envt|environ|Umgebung
Besitzer	Besitzen|Besitzer|Besitzer|Besitz|im Besitz

Installierte Eigenschaften

Eigenschaft	Beschreibung
sn_itom_Tag.Glide.script.Block.Client.globals	Steuert den Zugriff clientseitiger Skripts auf globale Variablen zur Erhöhung der Sicherheit. Bei „wahr“ können diese Skripts nicht auf globale Variablen zugreifen. • **Typ:** boolescher wert • **Wert:** Wahr/falsch • **Standardwert:** false
sn_itom_Tag.allow_New_cert_follow_on_Task	Ermöglicht die Erstellung neuer Zertifizierungsnachverfolgungsaufgaben für jedes Audit in Tag-Governance.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ:** boolescher wert • **Wert:** Wahr/falsch • **Standardwert:** false
sn_itom_Tag.Azure_window_size_in_min	Zeitfenstergröße in Minuten, um nach Änderungen in Azure-Ressourcen zu suchen. Dieser Wert hilft bei der Bestimmung der Start- und Endzeiten für die Prüfung: **Startzeit:** Die Zeit, zu der das Ereignis aufgetreten ist, minus der Zeitfenstergröße. **Endzeit:** Die Zeit, zu der das Ereignis aufgetreten ist, plus die Zeitfenstergröße. • **Typ:** Ganzzahl • **Standardwert:** 10
sn_itom_Tag.Performance.config.bulksize	Legt die Anzahl der App-Datenelemente fest, die gleichzeitig verarbeitet werden sollen. • **Typ:** Ganzzahl • **Standardwert:** 5000
sn_itom_Tag.Last_event_processed	Gibt an, dass das letzte Tag-Ereignis erfolgreich verarbeitet wurde, um sicherzustellen, dass das System mit den neuesten Änderungen auf dem neuesten Stand ist. • **Typ:** Zeichenfolge • **Standardwert:**
sn_itom_Tag.max_Audit_lag_ratio	Legt das maximal zulässige Verzögerungsverhältnis für Tag-Audits fest, um zu bestätigen, dass Tag-Richtlinien-Audits innerhalb eines angegebenen Zeitrahmens durchgeführt werden. • **Typ:** Ganzzahl • **Standardwert:** 2
sn_itom_Tag.Tag_Event_Batch_size	Legt die Anzahl der Tag-Ereignisse fest, z. B. die Erstellung, Aktualisierung oder Löschung von Tags, die zusammen in einem einzigen Batch verarbeitet werden. • **Typ:** Ganzzahl • **Standardwert:** 500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
sn_itom_Tag.Policy_Batch_size	Legt die Anzahl der Elemente fest, die zusammen in einem einzelnen Batch verarbeitet werden, wenn ein Tag-Richtlinienaudit ausgeführt wird. • **Typ:** Ganzzahl • **Standardwert:** 1000

Cloud Operations Workspace

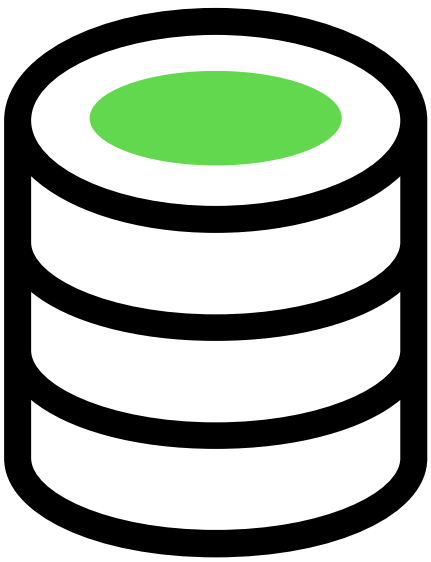
Cloud Operations Workspace bietet eine umfassende Lösung zum Verwalten der Cloud-Vorgänge Ihres Unternehmens.

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

Erste Schritte

Klicken Sie auf eine dieser Kacheln, um zu beginnen.

Installieren



Cloud Operations Workspace

installieren

Verwenden

Cloud Operations Workspace

verwenden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Fragen stellen oder beantworten im Cloud Operations Workspace-Forum der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Cloud Operations Workspace installieren

Sie können die Anwendung Cloud Operations Workspace (com.cloud_operations_workspace) installieren, wenn Sie über die Administratorrolle verfügen.

Vorbereitungen

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

Wenn Cloud Operations Workspace Ist installiert, werden auch mehrere Plugins und Anwendungen installiert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Cloud Operations Workspace erfordert das folgenden Plugin. Stellen Sie sicher, dass das folgende Plugin aktiviert ist, bevor Sie Cloud Operations Workspace installieren.

  Benötigte ServiceNow-Plugins

  Discovery (com.snc.discovery)

  ServiceNow Cloud-Discovery erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit mehreren Quellen mit den gefundenen Informationen.Weitere Informationen zum Aktivieren von Discovery finden Sie unter Discovery Anfordern .

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Anwendung Cloud Operations Workspace installieren, wird automatisch die folgende Rolle installiert:

Cloud Operations Workspace-Rolle

Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
sn_cloud_ops_ws.cloud_ops_admin	Der Cloud Operations Workspace-Administrator kann die folgenden Aktionen ausführen: • Cloud Operations Workspace-Dashboards anzeigen • Cloud-Discovery-Zeitpläne erstellen	• sn_itom_ui_comp.itom_component_user • discovery_admin • cloud_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Operations Workspace-Rolle (Fortsetzung)

Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
	• Cloud-Discovery-Vorgänge überwachen • Cloud-Discovery-Berichte anzeigen	

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Cloud Operations Workspace (com.cloud_operations_workspace).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .
3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation” die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von Plugins oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Cloud Operations Workspace installieren können.
4. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind die Beispieldatensätze, die Anwendungsfunktionen für allgemeine Anwendungsfälle beschreiben. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.
5. Wählen Sie **Installieren** aus.

Cloud Operations Workspace-Dashboard

Das ServiceNow® Cloud Operations Workspace-Dashboard bietet eine Zusammenfassung der Cloud-Vorgänge Ihrer Organisation und zeigt die ServiceNow-Anwendungen, mit denen Sie sie verwalten können.

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

Erforderliche ServiceNow AI Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriff auf das Dashboard von Cloud Operations Workspace

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cloud-Discovery-Arbeitsbereich**an.

Anwendungsfälle

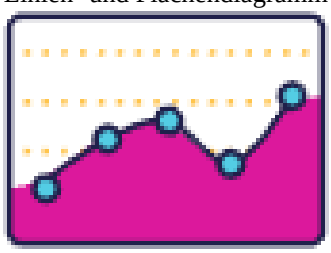
Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Gewinnen Sie Einblick in den Trend der CI-Erkennung, den Trend von Cloud-Discovery-Ereignissen und Cloud-Discovery-Fehlern. • Wählen Sie den Cloud-Provider Ihrer Organisation aus. • Greifen Sie auf die Anwendungen zu, mit denen Sie die Cloud-Vorgänge Ihrer Organisation verwalten können.

Indikatoren

Heutige Discovery-Fehler: Anzahl aller Cloud-Discovery-Fehler, die während der geplanten Erkennungen in den letzten 24 Stunden aufgetreten sind.

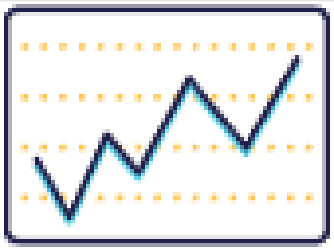
Berichte

Die folgenden Berichte sind in verfügbar Cloud Operations Workspace Dashboard:

Titel	Typ	Quelltabelle	Beschreibung
Total configuration items (Gesamte Konfigurationselemente)	Linien- und Flächendiagramm 	cmdb_ci	In diesem Bericht wird die Anzahl der im Laufe der Zeit erkannten CIs angezeigt. Wählen Sie den Bericht aus, um die Liste aller bisher erkannten Konfigurationselemente anzuzeigen. Sie können einen beliebigen CI-Datensatz auswählen, um weitere Informationen zum CI und den zugehörigen Daten aus mehreren Quellen anzuzeigen, falls verfügbar.
Ereignisse nach Anbieter: Letzte 24 Stunden	Liniendiagramm	sn_cmp_cloud_event_list	Dieser Bericht zeigt den Trend der in den letzten 24 Stunden empfangenen Cloud-Ereignisse an. Der Bericht enthält eine separate Trendlinie für jeden Cloud-Provider.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			

Zusätzlich werden auf den Dashboard-Karten die Anwendungen angezeigt, mit denen Sie die Cloud-Vorgänge Ihrer Organisation verwalten können. Verwenden Sie die Auswahlseite für Cloud-Anbieter, um den Cloud-Anbieter für Ihre Organisation auszuwählen. Die Auswahl hilft, die Menüs der Cloud Operations Workspace-Anwendungen anzupassen und nur die Cloud-Anbieter anzuzeigen, die für Ihre Organisation relevant sind.

Zugehörige Informationen

Liste der Arbeitsbereiche

Öffnen Sie Ihre konfigurierbare Arbeitsbereich-Experience in UI Builder für Cloud Operations Workspace

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen

Erforderliche Rolle: ui_builder_admin oder admin

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**an.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnis

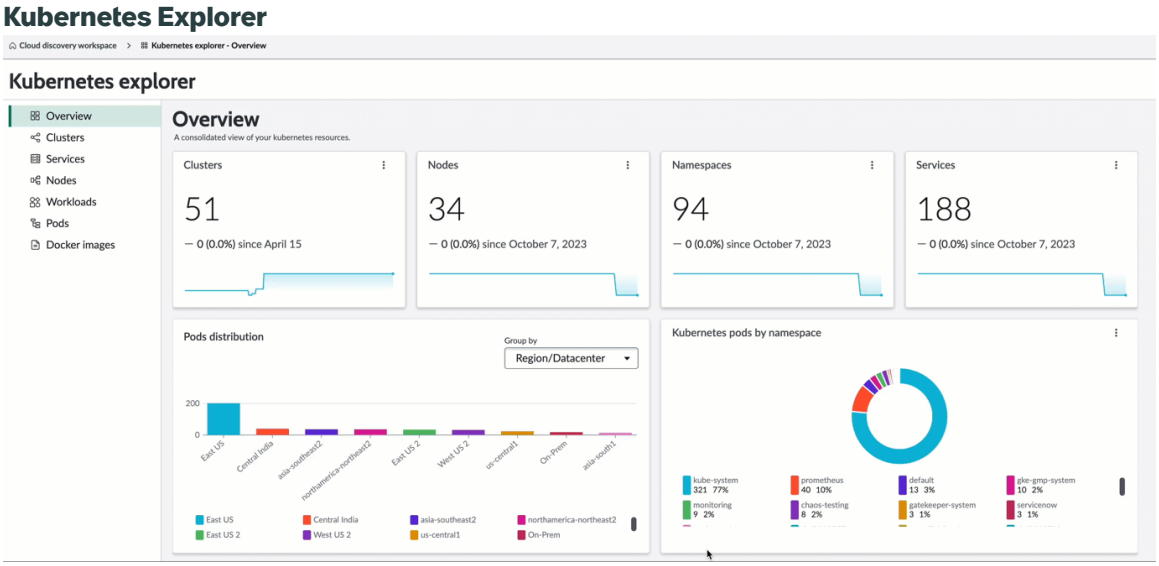
Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Kubernetes Explorer

Verwenden Sie den ServiceNow® Kubernetes Explorer, um die Kubernetes-Umgebungen und -Ressourcen Ihres Unternehmens anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Kubernetes Explorer bietet Unterstützung für folgende Cloud-Anbieter:

- Amazon Web Services (AWS): Amazon Elastic Kubernetes Service (EKS)
- Microsoft Azure Cloud: Azure Kubernetes-Service
- Google Cloud Platform (GCP): Google Kubernetes Engine (GKE)
- OpenShift

Wichtig: Im Kubernetes Explorer gilt jede unter OpenShift gehostete Kubernetes-Ressource als lokal. Dagegen gilt jede unter Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) gehostete Kubernetes-Ressource als in der Cloud gehostet.

Erforderliche ServiceNow AI Platform-Rollen

Die Rolle sn_Cloud_OPS_WS.Cloud_OPS_admin ist erforderlich, um den Kubernetes-Explorer anzuzeigen.

Auf Kubernetes Explorer zugreifen

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cloud-Discovery-Arbeitsbereich** > **Kubernetes-Explorer**an.

Wichtig: Ab dem Zurich-Release Cloud Operations Workspace Wird auf zukünftige Einstellung vorbereitet. Sie wird ausgeblendet und nicht mehr in neuen Instanzen aktiviert, wird jedoch weiterhin unterstützt. Discovery-Administratorarbeitsbereich Bietet die neueste Experience für diese Funktionalität. Weitere Informationen finden Sie unter Prozess zur Außerbetriebnahme von Anwendungen/Plugins [KB0867184] artikel in Now Support Knowledge Base.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer	Dashboard-Verwendung
Anwendungsbesitzer	Überprüfen Sie die Statistiken der in den Kubernetes-Clustern ausgeführten Anwendungen und Arbeitsauslastungen.
IT-Administrator, Cloud-Administrator	• Überprüfen Sie die Statistiken der Kubernetes-Infrastruktur: Cluster, Knoten, Namespaces, Services, Pods und Arbeitsauslastungen. • Überprüfen Sie die Verteilung der Pods über Dimensionen wie Region/Rechenzentrum, geografischer Standort oder Land. • Überprüfen Sie die Verteilung der Pods über Namespaces. • Überprüfen Sie die Liste der in Ihrer Organisation verwendeten Kubernetes-Docker-Images.

Indikatoren

Cluster

Ein Kubernetes-Cluster ist ein Satz von Knoten, auf denen containerisierte Anwendungen ausgeführt werden. Der Indikator „Cluster“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Cluster an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Cluster“ [sn_cow_k8s_cluster_analytics], um den Indikator „Cluster“ zu berechnen.

Knoten

Ein Knoten ist ein Worker-Computer in Kubernetes und kann je nach Cluster entweder ein virtueller oder ein physischer Computer sein. Der Indikator „Knoten“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Knoten an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Knoten“ [sn_cow_k8s_node_analytics], um den Indikator „Knoten“ zu berechnen.

Namespaces

Kubernetes-Namespaces bieten einen Mechanismus zum Isolieren von Ressourcengruppen innerhalb des Clusters. Der Indikator „Namespaces“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Namespaces an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Namespace“ [sn_cow_k8s_namespace_analytics], um den Indikator „Namespaces“ zu berechnen.

Services

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Kubernetes-Service ist eine Abstraktion, die einen logischen Satz von Pods und eine Richtlinie für den Zugriff auf diese definiert (manchmal wird dieses Muster auch als Mikroservice bezeichnet). Der Indikator „Services“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Services an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Service“ [sn_cow_k8s_service_analytics], um den Indikator „Services“ zu berechnen.

Der Indikator „Services“ ist auch auf der Registerkarte „Services“ von Kubernetes Explorer verfügbar.

Aufgliederungen

- Pod-Verteilung: Diese Aufgliederung zeigt die Verteilung der Kubernetes-Pods an, die in der lokalen Infrastruktur und der Cloud-Infrastruktur gehostet werden.

  Sie können die Aufgliederung nach folgenden Dimensionen filtern:

  - Region/Rechenzentrum
  - Geo-Standort
  - Land

  Die Pod-Verteilungsaufgliederung ist auf der Registerkarte „Übersicht“ von Kubernetes Explorer verfügbar.

- Kubernetes-Services nach Plattform oder Kubernetes-Services nach Typ: Diese Aufgliederung zeigt die Verteilung von Kubernetes-Services über Dimensionen wie Plattform und Typ an.
- Knoten nach Region: Diese Aufgliederung zeigt die Verteilung der Kubernetes-Knoten über Hosting-Regionen an.

Filter

Sie können die Liste filtern, indem Sie mit Datenvisualisierungen wie Ring und einzelne Punktzahlkarte interagieren.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
Kubernetes-Pods nach Namespace	Ring	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Verteilung der Kubernetes-Pods über die erkannten Namespaces angezeigt. Dieser Bericht ist auf der Registerkarte „Übersicht“ verfügbar.
Cluster insgesamt	Liste	Analytics für Kubernetes-Cluster [sn_cow_k8s_cluster_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Cluster aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Cluster“ verfügbar. Wenn Sie auf den Clusternamen klicken, wird Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Services insgesamt	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_service_analytics]	Dieser Bericht zeigt die Gesamtzahl der Kubernetes-Services an. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar.
Kubernetes-Services nach Plattform/Typ	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_service_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Services über die Anbieter an. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar.
Kubernetes-Services	Liste	Analytics für Kubernetes-Namespace [sn_cow_k8s_service_analytics]	Dieser Bericht listet die erkannten Kubernetes-Services auf. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar. Wenn Sie auf den Servicenamen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Knoten nach Cluster	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Knoten über die erkannten Cluster an. Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar.
Knoten nach Region	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Knoten über die erkannten Cluster an. Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar.
Knoten insgesamt	Liste	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Knoten aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar. Wenn Sie auf den Knotennamen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Gesamtanzahl der Arbeitsauslastungen	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	Dieser Bericht zeigt die Gesamtanzahl der Kubernetes-Arbeitsauslastungen an, die für die Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden. Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar.
Gewünschte/ Verfügbare Replikate stimmen nicht überein	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	In diesem Bericht wird die Anzahl der Nichtübereinstimmungen zwischen den gewünschten und verfügbaren Replikaten angezeigt. Wenn eine Nichtübereinstimmung vorliegt, ergreifen Sie geeignete Maßnahmen, um das Problem zu beheben.
Arbeitsauslastungen nach Klasse	Ring	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	Dieser Bericht zeigt die Arbeitsauslastungen nach Arbeitsauslastungsklasse an. Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar.
Gesamtanzahl der Arbeitsauslastungen	Liste	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Arbeitsauslastungen aufgelistet. Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar. Wenn Sie auf den Namen der Arbeitsauslastung klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Pods insgesamt	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	Dieser Bericht zeigt die Gesamtanzahl der Kubernetes-Pods an, die für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
	42		Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Ausgeführte Pods	Einzelne Punktzahl 42	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Ausgeführt“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Ausstehende Pods	Einzelne Punktzahl 42	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Ausstehend“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Erstellende Pods	Einzelne Punktzahl 42	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Erstellung“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Crashloop-Backoff-Pods	Einzelne Punktzahl 42	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Crashloop-Backoff“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Pods insgesamt	Liste	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Pods aufgelistet. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar. Wenn Sie auf den Pod-Namen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Docker-Images	Liste	Analytics für Kubernetes-Image [sn_cow_k8s_img_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Docker-Images aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte für Docker-Images verfügbar. Wenn Sie auf den Namen des Docker-Image klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt. Sie können die SBOM herunterladen. Weitere Informationen zum Generieren der SBOM finden Sie unter Laden Sie eine Software-Stückliste herunter (SBOM).

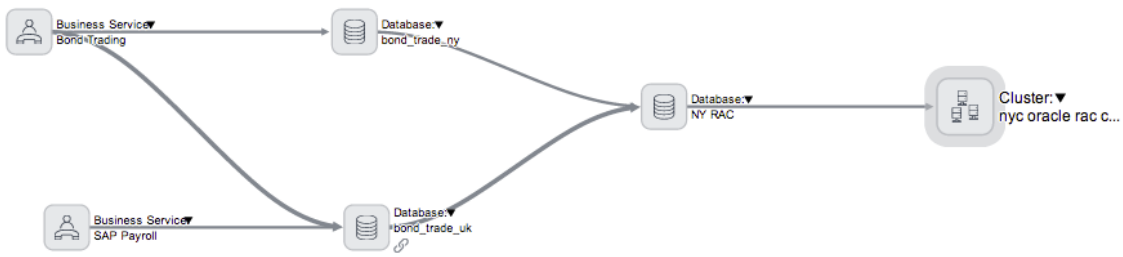
Abhängigkeitsansichten-Karte

ServiceNow® Die Zuordnung „Abhängigkeitsansichten“ zeigt eine allgemeine Top Down-Kubernetes-Perspektive , Von einem Cluster der obersten Ebene bis zum Container und innerhalb des Containers.

Eine Abhängigkeitsansichtszuordnung hat einen Ausgangspunkt, das als Stamm-CI oder Stammknoten der Zuordnung bezeichnet wird. Das Root-CI ist von einem dunkleren Frame umgeben, der sich mit einem pulsierenden Effekt neu zeichnet, um die Aufmerksamkeit auf das Root-CI zu lenken. Die Karten können sowohl vorgelagerte als auch nachgelagerte Abhängigkeiten für das Stamm-CI anzeigen. Standardmäßig zeigt die Zuordnung „Abhängigkeitsansichten“ drei Ebenen an, sowohl vorgelagerte als auch nachgelagerte Beziehungen. Administratoren können die Anzahl der angezeigten Ebenen konfigurieren. Die Karte reduziert und vergrößert Cluster, um sie besser anzeigen zu können. Standardmäßig werden Cluster reduziert.

Das Modul Abhängigkeitsansichten ist in allen Instanzen aktiv und enthält Demodaten.

Dependency Views-Beispielzuordnung



In einer Abhängigkeitsansichtszuordnung zeigen Zuordnungsindikatoren an, ob ein CI aktive, ausstehende Probleme hat. Sie können die mit einem CI verbundenen Aufgaben untersuchen, um weitere Details zu erhalten. Wenn Sie aus einem anderen Formular zur Karte zurückkehren, stellt das System die zuletzt angezeigte Karte wieder her, wobei die Standardfilter- und Layouteinstellungen verwendet werden.

Viele der Beziehungen in der Zuordnung werden durch den Discovery-Prozess erstellt. Sie können auch CI-Beziehungen in der Karte erstellen, definieren und löschen. Sie können die Karte aus verschiedenen Perspektiven anzeigen und bestimmte Datensätze öffnen, die sich auf Configuration Items beziehen. Das System aktualisiert die Zuordnung automatisch, um Änderungen an der CMDB widerzuspiegeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

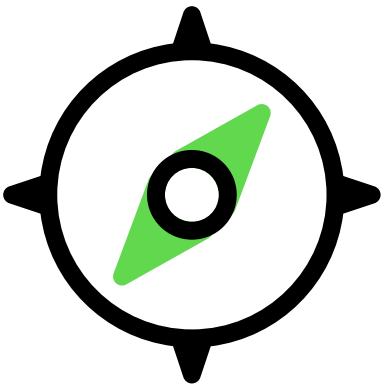
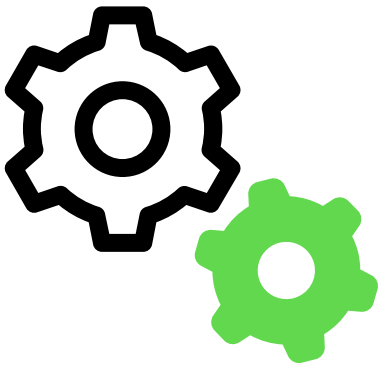
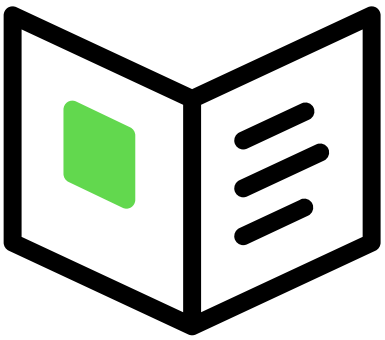
Hinweis: CIs, die nicht aus der Tabelle „Konfigurationselement“ [cmdb_ci] erweitert wurden, werden in Zuordnungen von Abhängigkeitsansichten und in CI-Beziehungsformatierern nicht angezeigt.

Rollen

Benutzer mit den Rollen itil und ecmdb_admin können Karten anzeigen und alle Aktionen in der Karte ausführen. Zu den Aktionen gehört der Zugriff auf die Kartenansichten und gespeicherten Filter, sowohl von den Listen in der Karte als auch von dem Modul **Gespeicherte Filter** aus.

Cloud-Lizenzrechner

Mit dem Cloud-Lizenzrechner können Sie die geschätzte Ressourcenanzahl für alle Cloud-Ressourcen abrufen, die für die Lizenzierung in Frage kommen.

Untersuchen	Konfigurieren	Berichte generieren
		
Erfahren Sie mehr über Cloud-Lizenzrechner.	Richten Sie Anmeldeinformationen ein, und konfigurieren Sie Accounts.	Generieren Sie Berichte mit dem Cloud-Lizenzrechner.

Cloud-Lizenzrechner Erkunden

Erfahren Sie mehr über die Funktionen der Cloud-Lizenzberechnung.

Die **Cloud-Lizenzrechner** Ermöglicht das Abrufen der geschätzten Ressourcenanzahl für alle Cloud-Ressourcen, die gemäß ITOM- und CCM-Lizenzierungsregeln für die Lizenzierung in Frage kommen. #Validiert die##vom Anwender bereitgestellten Cloud-Account-Details und schätzt die Ressourcenanzahl##basierend auf den geltenden Lizenzierungsregeln.

Mit dem Cloud-Lizenzrechner können Anwender die Anzahl der Cloud-Ressourcen zusammen mit den erforderlichen Lizenzschätzungen einfach abrufen. CLE unterstützt AWS- und Azure-Cloud-Umgebungen, jedoch keine Cloud-Services für Behörden. Ein Anwender kann eine Konfiguration erstellen, indem er die erforderlichen Details bereitstellt, und dann den Lizenzschätzer ausführen, um den Bericht abzurufen. CLE bietet Ihnen auch die Möglichkeit, den Bericht im PDF-Format herunterzuladen.

Konfigurieren Sie Den Cloud-Lizenzrechner

Richten Sie die Accounts und Anmeldeinformationen ein, die für den Cloud-Lizenzrechner erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Azure-Anmeldeinformationen für den Cloud-Lizenzrechner

Um dieses Tool zu verwenden, konfigurieren Sie die Anmeldeinformationen des Azure-Service-Prinzipalkontos. Wenn Sie bereits Anmeldeinformationen in der ServiceNow-Instanz konfiguriert haben, können diese Anmeldeinformationen verwendet werden.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Filternavigation** > **Alle** > **ITOM-Cloud-Lizenzrechner** > **Startseite**an.
2. Wählen Sie auf der Homepage die Option aus **Wechseln Sie zu Anmeldeinformationen** Um zu öffnen **Anmeldeinformationen (Discovery_credentials)** Seite.
3. Auswahlvorgang **Neu** > **Azure-Service-Prinzipal** Und geben Sie die Details des Azure-Service-Prinzipalkontos ein.

Ergebnis
A **Anmeldeinformations-ID** Wird generiert, was beim Erstellen von Konfigurationen erforderlich ist.

Erstellen Sie eine Azure-Account-Konfiguration, und generieren Sie CLE-Berichte

Das Tool unterstützt Verwaltungskonten und einzelne Abonnements. Verwaltungsaccounts enthalten alle Abonnements unter diesem Account.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Filternavigation** > **Alle** > **ITOM-Cloud-Lizenzrechner** > **Startseite**an.
2. Wählen Sie auf der Homepage die Option aus **Konfiguration Erstellen** Um das Popup-Fenster Konfiguration erstellen zu öffnen.
3. Geben Sie die folgenden Details ein:
   - **Name** : Geben Sie einen Namen für die Konfiguration ein.
   - **Cloud-Anbieter** : Wählen Sie **Azure** Aus der Liste. Füllen Sie die zusätzlichen Felder aus, die angezeigt werden.
   - **Account-ID** : Geben Sie die Verwaltungs-Account-ID oder Abonnement-ID ein.
   - **Verwaltungsgruppe** : Aktivieren Sie dieses Kontrollkästchen, wenn die Account-ID ein Verwaltungsaccount ist.
   - **Anmeldeinformationen** : Wählen Sie die in konfigurierten Azure-Serviceprinzip-Anmeldeinformationen aus Konfigurieren Sie Azure-Anmeldeinformationen für den Cloud-Lizenzrechner.
   - **Aktivieren** : Aktivieren Sie diese Option.
4. Wählen Sie Aus **Speichern Sie die Lizenzschätzung, und führen Sie sie aus** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Konfiguration wird gespeichert, und das Tool generiert den Bericht. Sie werden zu weitergeleitet **Bericht** Seite, auf der der Status der Berichtgenerierung nachverfolgt werden kann.

5. Von **Bericht** Seite auswählen **Ressourcenbericht herunterladen** Zum Herunterladen einer PDF-Datei des Berichts.

Zugehörige Informationen

Generieren Sie Cloud-Lizenzrechner-Berichte

Konfigurieren Sie Amazon Web Service-Anmeldeinformationen für den Cloud-Lizenzrechner

Diese Aufgabe führt Sie bei der Konfiguration der permanenten Anmeldeinformationen des IAM-Anwenders für den angegebenen Account.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sie können IAM-Rollen konfigurieren, um temporäre Anmeldeinformationen mithilfe der STS-API für einen angegebenen Account zu generieren. Bei Verwendung von IAM-Rollen für temporäre Anmeldeinformationen ist die Anmeldeinformations-ID im Konfigurationsformular optional. AWS-Service-Accounts erfordern jedoch die Konfiguration einer IAM-Rolle in Service-Accounts. Stellen Sie sicher, dass mindestens ein Service-Account über Anmeldeinformationen verfügt, um temporäre Anmeldeinformationen zu generieren.

Prozedur

1. Navigieren zu **Filternavigator** > **Alle** > **ITOM-Cloud-Lizenzrechner** > **Startseite**an.
2. Wählen Sie auf der Homepage die Option aus **Wechseln Sie zu Anmeldeinformationen** Um zu öffnen **Anmeldeinformationen (Discovery_credentials)** Seite.
3. Auswahlvorgang **Neu** > **AWS-Anmeldeinformationen** Und geben Sie die erforderlichen Informationen ein.
   A **Anmeldeinformations-ID** Wird generiert, was beim Erstellen von Konfigurationen verwendet wird.

Konfigurieren Sie AWS-Service-Accounts für CLE

Je nach Anmeldeinformationen und Master-Accounts gibt es verschiedene Möglichkeiten, AWS-Service-Accounts zu konfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Service-Accounts können mit den folgenden Optionen konfiguriert werden:

- Konfigurieren Sie einen Service-Account mit permanenten Anmeldeinformationen. Wenn ein Account mit permanenten Anmeldeinformationen konfiguriert ist, wird er als Zugriffsberechtigter-Account bezeichnet. Dieser Account kann entweder ein Verwaltungs-Account oder ein Mitgliedsaccount sein.

- Konfigurieren Sie einen Verwaltungsaccount mit der IAM-Rolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren Sie einen Mitgliedsaccount mit einer anwenderdefinierten IAM-Rolle. Wenn der Mitgliedsaccount die standardmäßige IAM-Rolle (OrganizationAccountAccessRole) zum Generieren temporärer Anmeldeinformationen verwendet, ist die Konfiguration eines Service-Accounts für den Mitgliedsaccount nicht erforderlich.

Prozedur

1. Navigieren zu **Filternavigation** > **Alle** > **ITOM-Cloud-Lizenzrechner** > **Startseite**an.
2. Wählen Sie aus **Service-Account-Liste** Symbol.
3. Auf der **Service-Account** Seite auswählen **Neu Erstellen** .
4. **Wahlweise:** Um einen Service-Account mit permanenten Anmeldeinformationen zu konfigurieren, geben Sie die folgenden Informationen ein:
   - (Optional) **Name:** Geben Sie den AWS-Account-Namen ein.
   - (Optional) **Cloud-Anbieter:** Wählen Sie AWS aus.
   - (Optional) **Account-ID:** Geben Sie die AWS-Account-ID ein.
   - (Optional) **Master-Account:** Wählen Sie aus, ob es sich um einen Verwaltungsaccount handelt.
   - (Optional) **Anmeldeinformationen:** Wählen Sie die für dauerhafte Anmeldeinformationen erstellte AWS-Anmeldeinformations-ID aus.
   - (Optional) **Master-Account:** Lassen Sie das Feld leer, falls nicht zutreffend.
   - (Optional) **ARN des Zugriffsberechtigungs-Accounts und der Zugriffsberechtigungsrolle:** Gilt nicht für dauerhafte Anmeldeinformationen.
5. **Wahlweise:** Geben Sie die folgenden Informationen ein, um einen Verwaltungsaccount mit der IAM-Rolle zu konfigurieren:
   - (Optional) **Name:** Geben Sie den AWS-Account-Namen ein.
   - (Optional) **Cloud-Anbieter:** Wählen Sie AWS aus.
   - (Optional) **Account-ID:** Geben Sie die AWS-Account-ID ein.
   - (Optional) **Master-Account:** Wählen Sie aus, ob es sich um einen Verwaltungsaccount handelt.
   - (Optional) **Anmeldeinformationen:** Lassen Sie das Feld leer. Für diesen Account sind keine Anmeldeinformationen erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Optional) **Master-Account:** Lassen Sie das Feld leer.
- (Optional) **Zugriffsberechtigter-Account:** Wählen Sie den Account aus, der eine Vertrauensbeziehung mit der IAM-Rolle dieses Verwaltungs-Accounts hat.
- **ARN der Zugriffsberechtigungsrolle:** Geben Sie den vollständigen ARN der IAM-Rolle ein.

6. **Wahlweise:** Um einen Mitgliedsaccount mit einer anwenderdefinierten IAM-Rolle zu konfigurieren, geben Sie die folgenden Informationen ein:
   - (Optional) **Name:** Geben Sie den AWS-Account-Namen ein.
   - (Optional) **Cloud-Anbieter:** Wählen Sie AWS aus.
   - (Optional) **Account-ID:** Geben Sie die AWS-Account-ID ein.
   - (Optional) **Master-Account:** Wählen Sie diese Option nicht aus, da dies ein Mitgliedsaccount ist.
   - (Optional) **Anmeldeinformationen:** Lassen Sie das Feld leer. Für diesen Account sind keine Anmeldeinformationen erforderlich.
   - (Optional) **Master-Account:** Wählen Sie den Verwaltungsaccount aus der Liste aus.
   - (Optional) **Zugriffsberechtigter-Account:** Wählen Sie den Account aus, der eine Vertrauensbeziehung mit der IAM-Rolle dieses Mitglieds-Accounts hat. Dies kann entweder der Verwaltungsaccount oder ein anderer Mitgliedsaccount sein.
   - **ARN der Zugriffsberechtigungsrolle:** Geben Sie den vollständigen ARN der IAM-Rolle ein.
7. Wählen Sie aus, nachdem Sie die relevanten Informationen für Ihren Account-Typ angegeben haben **Speichern** .

Erstellen Sie eine AWS-Account-Konfiguration, und generieren Sie CLE-Berichte

Das Tool unterstützt Verwaltungskonten und einzelne Abonnements. Verwaltungsaccounts enthalten alle Abonnements unter diesem Account.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Filternavigation** > **Alle** > **ITOM-Cloud-Lizenzrechner** > **Startseite**an.
2. Wählen Sie auf der Homepage die Option aus **Konfiguration Erstellen** Um das Popup-Fenster Konfiguration erstellen zu öffnen.
3. Geben Sie die folgenden Details ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Name** : Geben Sie einen Namen für die Konfiguration ein.
- **Cloud-Anbieter** : Wählen Sie **AWS** Aus der Liste. Wenn Sie die Option „Anmeldeinformationsbasiert“ auswählen, werden zusätzliche Felder angezeigt.
- **Account-ID** : Geben Sie die AWS-Account-ID ein.
- **Verwaltungsgruppe** : Aktivieren Sie dieses Kontrollkästchen, wenn die Account-ID ein Verwaltungsaccount ist.
- **Anmeldeinformationen** : Wählen Sie die für diesen Account konfigurierten AWS-Anmeldeinformationen aus.
  - **Konfigurations-Aggregator-Account** : Geben Sie die Account-ID ein, in der der Aggregator erstellt wird.
  - **Name des Konfigurations-Aggregators** : Geben Sie den Namen des AWS Config Aggregators ein.
  - **Konfigurationsaggregator-Region** : Geben Sie die AWS-Region ein, in der der Aggregator erstellt wird.
- **Aktivieren** : Aktivieren Sie diese Option.

4. Wählen Sie Aus **Speichern Sie die Lizenzschätzung, und führen Sie sie aus** .

   Die Konfiguration wird gespeichert, und das Tool generiert den Bericht. Sie werden zu weitergeleitet **Bericht** Seite, auf der der Status der Berichtgenerierung nachverfolgt werden kann.

5. Von **Bericht** Seite auswählen **Ressourcenbericht herunterladen** Zum Herunterladen einer PDF-Datei des Berichts.

Zugehörige Informationen

Generieren Sie Cloud-Lizenzrechner-Berichte

Generieren Sie Cloud-Lizenzrechner-Berichte

Cloud-Lizenzrechner-Berichte bieten einen Überblick über Account-Informationen.

Die heruntergeladene PDF des Ressourcenberichts enthält eine Übersicht über die Informationen des Accounts, z. B. den Cloud-Provider, den Account-Konfigurationsnamen und die Gesamtanzahl der Ressourcen.

Der Bericht unterscheidet zwischen lizenzierbaren CCM-Ressourcen und ITOM-lizenzierbaren Ressourcen. Auf den folgenden Seiten enthält der Bericht Tabellen der CCM- und ITOM-Ressourcen.

ITOM-Transparenz-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von ITOM-Transparenz-Listen und -Formularen.

Durch ITOM-Transparenz erfasste Daten

ITOM-Transparenz erfasst spezifische Daten für jeden Gerätetyp und speichert sie in dedizierten Tabellen, Feldern und Beziehungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystem

Betriebssystem

Erkennen Sie Server und Computer abhängig vom Betriebssystem des Computers:

- Windows
- Solaris
- Linux
- Mac-Discovery (OS/X)
- HP-UX
- AIX

Virtualisierung

Virtualisierung

Erfassen Sie Informationen über Bereitstellungen, die Virtualisierung beinhalten:

- Erkennung von Hyper-V
- Virtualisierung mit IBM
- Virtualisierung mit Red Hat
- Nutanix Acropolis
- VMware vCenter
- OpenStack-Virtualisierung

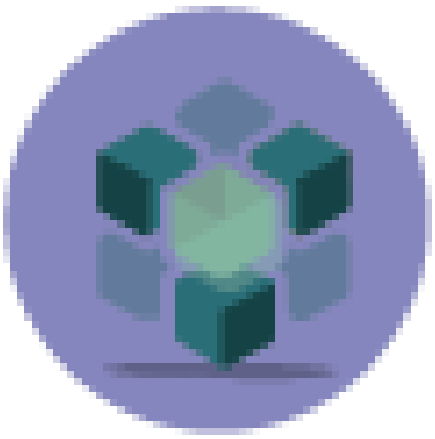
Cloud

Cloud

- AWS
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM-Cloud
- VMware Cloud

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container



Container

- Kubernetes und OpenShift
- Amazon ECS-Ressourcen-Discovery mit Mustern
- Erkennung von Pivotal Cloud Foundry

Software

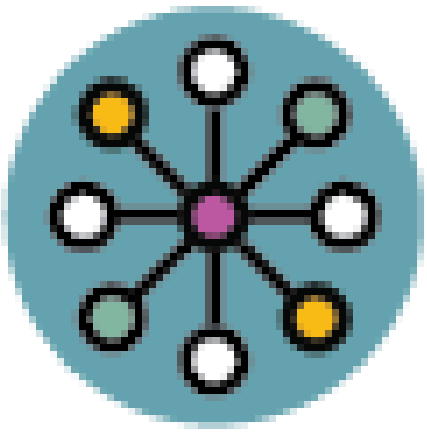
Software

Erkennen Sie zahlreiche Softwareanwendungen, einschließlich:

- Apigee Edge
- ColdFusion
- HP Operations Manager
- IBM Websphere DataPower
- JBOSS unter Windows und Linux
- Web- und E-Mail-Server, einschließlich Microsoft IIS, Apache, Tomcat, Exchange-Postfach
- Puppet-Automatisierungssoftware
- Red Hat JBoss Fuse
- SAP-Anwendungen
- WebLogic- und WebSphere-Server
- Allgemeine Software

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geclusterte Anwendungen



Geclusterte Anwendungen

- IBM PowerHA-Cluster (HACMP)
- Linux Red Hat-Cluster
- Erkennung von Veritas Cluster Server
- Windows-Servercluster

Datenbanken

Datenbanken

Erkennen Sie Datenbanken, einschließlich:

- Oracle
- MySQL
- Microsoft SQL
- MongoDB
- SAP HANA
- PostgreSQL
- Sybase
- Amazon DynamoDB
- Oracle-Datenbank 12c

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkgeräte

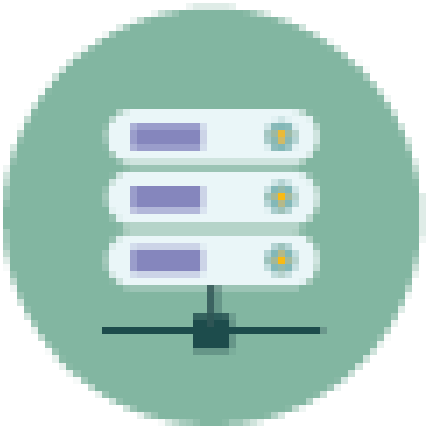
Netzwerkgeräte

- Router und Switches
- Lastenausgleichsmodule:
  - A10
  - F5 BIG-IP
  - Cisco GSS
  - Cisco CSS
  - Citrix NetScaler
  - HAProxy
  - NGINX
  - Alteon
  - ACE
  - Radware-appDirector
  - AWS Anwendungs-ELB-Service-Discovery mit Mustern
- Firewalls
  - Cisco-Firewall
  - Fortinet-Firewall
  - Juniper-Firewall
  - Palo Alto-Firewall
- IP-Netzwerke und bestimmte IP-Adressen
- Cisco UCS-Geräte
- Cisco Switch Wireless Access Point (WAP)
- Drucker und Netzgeräte
- IP-Services und -Daemons

Sie können Geräte auch basierend auf TCP-Verbindungen und mithilfe der Layer 2-Erkennung auf SNMP-Ebene finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicher



Speicher

Erkennen Sie die folgenden Typen von Speichergeräten:

- Pure Storage FlashBlade
- NetApp-Server
- Erkennung von Storage Area Networks (SAN)
- Direct Attached Storage (DAS)
- Network Attached Storage (NAS)
- Hostbusadapter (HBA)
- EMC Isilon

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Discovery und Service-Mapping können eine Vielzahl von Betriebssystemen und Anwendungen erkennen.

Discovery Sucht nach Computern, Servern, Druckern, einer Vielzahl von IP-fähigen Geräten und den darauf ausgeführten Anwendungen. Es kann dann die CIs in Ihrer CMDB mit den gesammelten Daten aktualisieren. Diese Erkennungsmethode wird als horizontale Erkennung bezeichnet. Service-Mapping Ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Die Top-Down-Zuordnung hilft Ihnen, die Auswirkungen eines problematischen Objekts auf den Rest des Serviceinstanzvorgangs sofort zu erkennen.

Zusätzlich zu den standardmäßig unterstützten Hosts und Anwendungen können Sie zusätzliche Hosts und Anwendungen ermitteln, indem Sie im Store verfügbare Muster bereitstellen.Referenzinformationen zu Mustern, die im Store veröffentlicht wurden, finden Sie unter Verfügbare lokale Discovery-Muster.

Wenn Ihr Unternehmen Geräte oder Anwendungen verwendet, die nicht standardmäßig unterstützt werden oder Muster verwenden, die im ServiceNow Store verfügbar sind, können Sie Discovery und Service-Mapping so konfigurieren, dass die Erkennung wie unter Von ITOM-Transparenz verwendete Erkennungsmuster beschrieben erfolgt.

Cloud-Discovery Muster suchen die Cloud-Ressourcen von AWS, Azure, Google Cloud Platform (GCP), IBM, Und Oracle.

Wenn Sie die erforderlichen Musterbefehle vor der Ausführung der Discovery validieren möchten, verwenden Sie das Tool zur Befehlsvalidierung. Weitere Informationen finden Sie unter Validiert Befehle, die in der musterbasierten Discovery verwendet werden.

ITOM Content Service Bietet Transparenz für Ihre Anwendungen, indem KI-Fähigkeiten verwendet werden, die laufende Anwendungsprozesse gruppieren und klassifizieren. Weitere Informationen finden Sie unter ITOM Content Service.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
.Net Framework	Windows	1.x.x, 2.x.x, 3.x.x, 4.x.x	WMI WinRM	Von oben nach unten	.NET-Applikation
A10 (Lastenausgleichsmodul)	A10	N/V	REST	Horizontal	A10 Lastenausgleich
Adobe JRun	Windows UNIX	4.x	WMI WinRM SSH	Horizontal und von oben nach unten	JRun
Radware Alteon RadWare ADC	Alteon	v31, v29.5	SNMP	Horizontal und von oben nach unten	Alteon Load Balancer
Amazon Relativer Datenbankservice	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS Relational Database Service
Amazon Route53-Service	AWS	N/V	REST	Horizontal	Amazon AWS Route53 HD
Amazon ECS in AWS Fargate	AWS	N/V	REST	Horizontal	AWS ECS/ Fargate
Amazon Application Load Balancer Service	AWS	N/V	REST	Von oben nach unten	Amazon AWS Application ELB Service - TD
Amazon Einfacher Speicherservice (AWS S3)	AWS	N/V	REST	Horizontal und von oben nach unten	AWS S3
Amazon DynamoDB	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS – DynamoDB (Muster)
AWS Automatische Skalierung der Gruppen-	AWS	N/V	REST	Horizontal	AWS Auto Scaling-Gruppen (LP) (Muster)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Discovery mit Mustern					
AWS Lambda-Discovery mit Mustern	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS Lambda
AWS MemoryDB für Redis-Discovery mit Mustern	AWS	N/V	REST	Horizontal	AWS MemoryDB (Muster)
AWS Ressourcenbestands-Discovery mit Mustern	AWS	N/V	REST	Horizontal	AWS-Ressourcenbestand
AWS DB-Cluster-Discovery mit Mustern	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS DB-Cluster
Amazon Elastischer Lastenausgleichsmodul-Service	AWS	N/V	REST	Von oben nach unten	Amazon AWS Classic ELB Service - TD
Erkennung von Amazon Kinesis	AWS	N/V	REST	Horizontal	Muster: • Amazon AWS – Kinesis Video Stream Services (LP) • Amazon AWS – Kinesis Data Stream Services (LP) • Amazon AWS – Kinesis Firehose Stream Services (LP) • Amazon AWS – Kinesis Data

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Analytics Stream Services (LP)
AWS Services-Discovery mithilfe von Mustern	AWS	N/V	REST	Horizontal	Siehe Link
Apache Cassandra-Datenbank und DataStax	UNIX	N/V	SSH	Horizontal und von oben nach unten	Cassandra
Apache HBase	UNIX	N/V	SSH	Horizontal	Sonden: • HBase - Version • HBase - Hauptklasse • HBase - Konfiguration
Apache HTTP Server	Windows UNIX	2.x	WMI WinRM SSH	Horizontal und von oben nach unten	Apache
Apache Kafka und Zookeeper	Apache Kafka	N/V	SSH	Horizontal	Kafka und Zookeeper
Apache HTTP-Webserver des Tomcat-Servlet-Containers	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tomcat
Apigee Edge Enterprise Edition	Linux	4.xx	SSH HTTP	Horizontal und von oben nach unten	APIGee
Lastenausgleichsmodul Avi Vantage einschließlich Avi Controller und GSLB	VMware AWS Avi Networks	N/V	REST	Horizontal und von oben nach unten	AVI LB – Lastenausgleichsmodul Avi Vantage

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					AVI LB – AVI von oben nach unten AVI Session – Avi Controller AVI-GSLB-Unterstützung
Azure-App-Konfigurationsspeicher	Microsoft Azure	N/V	REST	Horizontal	Azure – App-Konfigurationsspeicher – Erweiterter Bestand (LP)
Azure App Service – App-Serviceplan	Microsoft Azure	N/V	REST	Horizontal	Azure – App-Service-App-Serviceplan – Erweiterter Bestand (LP)
Azure Application Insight-Komponente	Microsoft Azure	N/V	REST	Horizontal	Azure – Anwendungseinblickkomponente – Erweiterter Bestand (LP)
Azure Application Security Group	Microsoft Azure	N/V	REST	Horizontal	Azure – Anwendungssicherheitsgruppe – Erweiterter Bestand (LP)
Azure-Automatisierungsaccount	Microsoft Azure	N/V	REST	Horizontal	Azure – Automatisierungs-Account – Erweiterter Bestand (LP)
Azure-Verfügbarkeitssätze	Microsoft Azure	N/V	REST	Horizontal	Azure – Verfügbarkeitssatz (LP)
Azure-Verfügbarkeitszonen	Microsoft Azure	N/V	REST	Horizontal	Azure – Verfügbarkeitszonen (LP)
Azure Compute Gallery – Image-Definition	Microsoft Azure	N/V	REST	Horizontal	Azure – Computergalerie-Image-Definition – Erweiterter Bestand (LP)
Azure Compute-Snapshot	Microsoft Azure	N/V	REST	Horizontal	Azure – Snapshot berechnen – Erweiterter Bestand (LP)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Azure Container-Registrierung	Microsoft Azure	N/V	REST	Horizontal	Azure – Containerregistrierung – Erweiterter Bestand (LP)
Azure Data Factory	Microsoft Azure	N/V	REST	Horizontal	Azure – Data Factory – Erweiterter Bestand (LP)
Azure Data Protection – Sicherungstresor	Microsoft Azure	N/V	REST	Horizontal	Azure – Datenschutz-Sicherungsresor – Erweitertes Inventar (LP)
Azure-Datenbankservice	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Azure DataBase (Muster)
Azure Databricks – Arbeitsbereich	Microsoft Azure	N/V	REST	Horizontal	Azure – Arbeitsbereich „Databricks“ – Erweiterter Bestand (LP)
Azure-Datenträgerverschlüsselungssatz	Microsoft Azure	N/V	REST	Horizontal	Azure – Datenträgerverschlüsselungssatz – Erweiterter Bestand (LP)
Azure DNS Zonen- und Datensatzsätze Discovery anhand von Mustern	Microsoft Azure	N/V	REST	Horizontal	Muster: Azure DNS Zones HD oder Azure DNS Zones (LP) Azure DNS Zone Recordsets (LP)
Azure Event Grid – Systemthema	Microsoft Azure	N/V	REST	Horizontal	Azure – Thema „Ereignisrastersystem“ – Erweiterter Bestand (LP)
Azure Event Hub – Namespace	Microsoft Azure	N/V	REST	Horizontal	Azure – Ereignis-Hub-Namespace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					– Erweiterter Bestand (LP)
Azure Functions	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Muster: Azure Functions TD oder Azure Functions (LP)
Azure-Bestandsressourcen	Microsoft Azure	N/V	REST	Horizontal	Azure Inventory und Tags
Azure Schlüsseltresor	Microsoft Azure	N/V	REST	Horizontal	Azure – Key Vault – Erweiterter Bestand (LP)
Microsoft Azure LoadBalancer-Service	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Azure LoadBalancer TD
Azure Logic-App	Microsoft Azure	N/V	REST	Horizontal	Azure – Logik-App – Erweiterter Bestand (LP)
Azure – Verwaltete Identität – Vom Anwender Zugewiesene Identität	Microsoft Azure	N/V	REST	Horizontal	Azure – verwaltete Identität – vom Anwender zugewiesene Identität – Erweitertes Inventar (LP)
Azure Networks – IP-Gruppe	Microsoft Azure	N/V	REST	Horizontal	Azure – Netzwerk-IP-Gruppe – Erweiterter Bestand (LP)
Privater Azure-Link – Privater Endpunkt	Microsoft Azure	N/V	REST	Horizontal	Azure – privater Link – privater Endpunkt – Erweiterter Bestand (LP)
Azure Service Bus – Namespace	Microsoft Azure	N/V	REST	Horizontal	Azure – Service-Bus-Namespace – Erweitertes Inventar (LP)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Azure Service Bus – Warteschlange	Microsoft Azure	N/V	REST	Horizontal	Azure – Servicebus-Warteschlange – Erweiterter Bestand (LP)
Azure SQL-Datenbank	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Cloud-Datenbankinstanz
Azure Service Bus-Thema	Microsoft Azure	N/V	REST	Horizontal	Azure – Service-Bus-Thema – Erweiterter Bestand (LP)
Azure Virtual Machine Scale Sets (VMSS) Instanz-Discovery	Microsoft Azure	N/V	REST	Horizontal	Azure VM Scale Set Instance
Azure-Website-Service und -Datenbank	Microsoft Azure	N/V	REST	Horizontal	Muster: Azure WebSite Azure WebSite (LP) Erfassen Sie Azure-Datenbank-Tags und WebSite-Tags.
BMC Control-M	UNIX Windows	6.x	WMI WinRM SSH	Horizontal	Cntl-M Enterprise Manager
Verwendung der eigenen Lizenz (Bring Your Own License, BYOL)	Amazon AWS Cloud Microsoft Azure Cloud Google Cloud Platform (GCP)	N/V	REST Azure Resource Graph	Horizontal	Die gemeinsame Bibliothek „Image License“ ist eine Erweiterung der Muster:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					• Amazon AWS – Executable Template (LP) • Amazon AWS – Owned Template (LP) Die gemeinsame Bibliothek „Azure Virtual Machine License“ ist eine Erweiterung des Musters „Azure – Virtual Machine (LP)“. Die gemeinsame Bibliothek „Google Cloud Platform (GCP) – VM-Lizenz“ ist eine Erweiterung des Musters „Google Cloud Platform (GCP) – Virtual Server“.
CA eTrust-Verzeichnisserver	Windows	7.x, 8.x	WMI WinRM	Von oben nach unten	CA eTrust-Verzeichnisserver
CA Identity Manager-Bereitstellungsserver	Windows	11.x, 12.x	WMI WinRM	Von oben nach unten	CA Identity Manager-Bereitstellungsserver für Windows

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
CA Introscope Enterprise Manager	Windows Unix	8.x, 9.x	WMI WinRM SSH	Von oben nach unten	CA Introscope Enterprise Manager
CA Policy-Server	Windows Unix	11.x	WMI WinRM SSH	Von oben nach unten	CA Policy-Server
CA Site Minder Agent	Windows Unix	11.x	WMI WinRM SSH	Horizontal und von oben nach unten	CA Site Minder Agent
Cisco Lastenausgleichsmodul für Content Services-Switch	ACE	6.x	SNMP SSH	Horizontal und von oben nach unten	Cisco CSS SNMP
Cisco ACE-Anwendungssteuerungs-Engine	ACE	2.x	SSH	Horizontal und von oben nach unten	ACE Load Balancer
Cisco Call Manager	Cisco	3.x, 4.x	SNMP SSH	Von oben nach unten	Cisco CallManager
Cisco Fiber Connect	Cisco	Keine Daten	SNMP SSH	Von oben nach unten	Cisco Fibre Connect
Cisco Lastenausgleichsmodul Für Globale Standortauswahl	ACE	3.x	SNMP SSH	Horizontal und von oben nach unten	Cisco GSS
Cisco Einheitliches Computersystem	UCS	3.x	REST	Horizontal	UCS - HD
Citrix Delivery Controller	Windows	7.x> 7,5, 8.x	WMI WinRM	Von oben nach unten	Delivery Controller

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Citrix Netscaler Global Server Load Balancing (GSLB)	Netscaler	10.x	SNMP SSH NS.conf	Horizontal und von oben nach unten	Netscaler GLB
Citrix Netscaler Load Balancer	Netscaler	9.x, 10.x	SNMP SSH NS.conf	Horizontal und von oben nach unten	Citrix Netscaler
Citrix Netscaler SDX	Citrix NetScaler SDX	13	SSH	Horizontal	Citrix NetScaler SDX
Citrix Lizenzserver	Windows	7.x	WMI	Horizontal	Lizenzserver
Citrix Xen Hyper-V	Xen Server	7.6	SSH	Horizontal	Citrix Xen Hyper-V
Cloudian-Speicher	Linux	7.x	SSH	Horizontal	Cloudian-Speicher-Discovery
APK verbinden	Windows	1.xx	WMI WinRM	Von oben nach unten	Connect-It Service
Container-Image-Scan für Softwareaufgliederung	Linux		REST HTTP	Horizontal	Container-Image-Scan
Software-Stückliste (Software Bill of Material, SBOM)	Linux	N/V	REST HTTP	Horizontal	SBOM ist ein Erweiterungsabschnitt des Container-Image-Scan-Musters
Docker-Virtualisierung	Linux	N/V	N/V	Horizontal	Docker (Muster)
Epic Systems Corporation	UNIX	2014.xx, 2015.xx	SSH	Von oben nach unten	EPIC Cache
Discovery des Berichts „Datenbankadministrator“ (DBA)	N/V	N/V	N/V	Horizontal	DBA ist ein Erweiterungsabschnitt der Muster:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					• Cassandra-DB • MSSQL-DB • MySQL-DB • Oracle-DB
Dell Powermax-Speicher-Discovery mit Mustern	Dell EMC	9 und 10	N/V	Horizontal	EMC PMAX Phase 1 (Muster) EMC PMAX Phase 2 (Muster)
Dell Datendomänenspeicher-Discovery anhand von Mustern	DD OS	DD OS 7.3 oder höher	REST	Horizontal	DELL EMC Data Domain (Muster)
Dell EMC XtremIO-Speicher-Array Discovery	Linux	6.3.0 und 6.3.1	REST	Horizontal	EMC XtremIO (Muster)
EMC Isilon	OneFS	8.0	SNMP REST	Horizontal	EMC Isilon
F5 BIG-IP Device Service Clustering	F5	11.x, 12.x	SNMP SSH REST	Horizontal	F5-Cluster
F5 BIG-IP	F5	11.x, 12.x	REST	Horizontal und von oben nach unten	F5-Lastenausgleichsmodul, F5-Lastenausgleichsmodul SSH
Fortinet Firewalls	Fortinet Firewall-Gerät	FortiOS 5,2.x, FortiOS 5,4.x, FortiOS 5,6.x, FortiOS 6,2.x, FortiOS 6,4.x, FortiOS 7,2.x	SNMP	Horizontal	Fortinet-Netzwerk-Firewall Der Nächsten Generation
Fortinet Firewalls und FortiGate-VDOMs	Fortinet Firewall-Gerät	FortiOS 6,2.x, FortiOS 6,4.x, FortiOS 7.x	REST	Horizontal	Fortinet-Netzwerk-Firewall der nächsten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Generation – REST
Google Cloud Apigee API-Plattform	Linux	4.xx	SSH	Horizontal und von oben nach unten	Apigee-Service
Google Cloud Platform (GCP) AlloyDB für PostgreSQL	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP): AlloyDB für PostgreSQL
Google Cloud-Firebase	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Firebase Realtime DB
Google Cloud-FireStore	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Firestore DB
Google Cloud-SQL	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Cloud SQL DB
Google Cloud BigQuery	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – BigQuery DB
Google Cloud-Bigtable	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Bigtable DB
Google Cloud Platform	GCP	N/V	REST	Horizontal	Google Cloud Platform-(GCP-)Ressource
Google Cloud Platform (GCP) Asset-Bestand	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Ressourcenbestand
Google Cloud Platform (GCP) Cloud-Funktionen	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP): Cloud-Funktionen
Google Cloud Platform (GCP)-Speicherspeicher	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Memorystore DB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Google Cloud Platform (GCP) Organisation	GCP	N/V	REST	Horizontal	GCP-Organisation
Google Cloud-Spanner	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Spanner DB
HAProxy Lastenausgleichsmodul der Community-Edition	UNIX	1,5, 1,6, 1,7	SSH	Horizontal und von oben nach unten	HA-Proxy
HP Vorgangsmanager	Windows Unix	9.x	WMI WinRM SSH	Horizontal und von oben nach unten	HP Operations Manager
HP Quality Center	Windows	10.x	WMI WinRM	Von oben nach unten	HP Quality Center on Windows
HP Servicemanager	Windows Unix	9.x	WMI WinRM SSH	Horizontal und von oben nach unten	HP Service Manager-Anwendungsserver
HP UCMDB	Windows	N/V	WMI WinRM	Horizontal und von oben nach unten	HP uCMDB on Windows
HP-UX UNIX Server	HP-UX	11i	SSH	Horizontal	HP-UX Server
IBM AIX	UNIX	6.x, 7.x	SSH	Von oben nach unten	AIX-Server
IBM CICS Transaction Gateway	Windows UNIX	5.x	WMI WinRM SSH	Von oben nach unten	CTG
IBM Cloud Platform	IBM Cloud Platform	N/V	REST	Horizontal	IBM Cloud – Lastenausgleichsmodul, IBM Cloud – Standortgruppen, IBM Cloud –

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Netzwerk, IBM Cloud – Organisationen und Bereiche, IBM Cloud – Ressourcengruppen, IBM Cloud – SSH-Schlüssel, IBM Cloud – Speicher, IBM Cloud – Virtual Server
IBM Customer Information Control System	Windows UNIX	4.x, 5.x	WMI WinRM	Von oben nach unten	CICS
IBM DB2 unter Unix	UNIX	8.x, 9.x, 10.x, 11.x	WMI WinRM SSH	Horizontal	DB2
IBM DB2 unter Windows	Windows	8.x, 9.x, 10.x, 11.x	WMI WinRM SSH	Horizontal	DB2
IBM-Virtualisierung und Hardware Management Console (HMC) – Komponenten	UNIX	N/V	SSH	Horizontal	IBM HMC-Server
IBM PowerHA-Cluster (HACMP)	IBM	N/V	REST	Horizontal	IBM PowerHA-Cluster (HACMP)
IBM Security Access Manager	ISAM	8.0.1	SNMP REST	Horizontal und von oben nach unten	ISAM-Server
IBM WebSEAL Discovery	ISAM	9.*,10.*.	REST	Horizontal und von oben nach unten	IBM WebSEAL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
IBM Tivoli Access Manager	Windows UNIX	6.x	WMI WinRM SSH	Von oben nach unten	ITAM - Asset Center
IBM Tivoli WebSEAL	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Von oben nach unten	Webseal (Muster)
IBM WebSphere Application Server	Windows UNIX	5.x, 6.x, 7.x, 8.x, 9.x	WMI WinRM SSH	Horizontal und von oben nach unten	Websphere
IBM WebSphere DataPower SOA-Appliance	DataPower	I40, I50	SNMP REST	Horizontal und von oben nach unten	DataPower
IBM WebSphere Message Queue	Windows UNIX	6.x, 7.x, 8.x, 9.x	WMI WinRM SSH	Horizontal und von oben nach unten	Die folgenden Muster: • WMQ unter Unix • WMQ unter Windows • WMQ-Warteschlange Unix • WMQ-Warteschlange Windows
IBM App Connect Enterprise- und HTTP-Listener-Discovery	UNIX	6, 7, 8, 9, 10, 11, 12.	N/V	Horizontal und von oben nach unten	WMB unter UNIX (Muster)
IBM WebSphere Portal	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	Websphere Portal On Windows

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
IBM Z-Mainframe	Z/OS	OS/390	SSH	Horizontal	IBM zOS Server
Infini-Box		5.0.x	REST HTTP	Horizontal	InfiniBox
Interconnect Web Service	Windows	2014	WMI WinRM	Von oben nach unten	Inter Connect
Istio Service Mesh	Kubernetes	1.15 und höher	HTTP	Horizontal	ISTIO Service Mesh
Kubernetes	Kubernetes	1.21 – 1.30	REST HTTP	Horizontal	Kubernetes
Linux-Server	UNIX	Ubuntu 16, RHEL 5.x, CentOS 7.x	SSH	Horizontal	Linux-Server
Linux Pacemaker-Cluster	Linux	N/V	SSH	Horizontal	Pacemaker Linux-Cluster
Microsoft BizTalk Orchestration-Server	Windows	2004, 2006, 2007, 2009, 2010	WMI WinRM	Von oben nach unten	BizTalk-Server
Microsoft Zertifizierungsstelle	Microsoft	N/V	WMI	Horizontal	Microsoft-Zertifizierungsstelle
Microsoft Dynamics CRM	Windows	2003, 2005, 2007, 2010	WMI WinRM	Von oben nach unten	Dynamic CRM-Komponente
Microsoft Schnellsuche	Windows	2005	WMI WinRM	Horizontal und von oben nach unten	Schnellsuche
Microsoft Hyper-V-Server	Windows	2008, 2012, 2016	WMI WinRM	Horizontal	Hyper-V-Server
Microsoft Identity Integration Server	Windows	2003	WMI WinRM	Von oben nach unten	IIFP On Windows Pattern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Microsoft Internet Information Services	Windows	6.0, 7.x, 8.x	WMI WinRM	Horizontal und von oben nach unten	IIS
Microsoft Message Queuing	Windows	3.x, 4.x, 5.x	WMI WinRM	Von oben nach unten	MSMQ (Muster)
Microsoft SharePoint	Windows	2003, 2007, 2010, 2013	WMI WinRM	Horizontal und von oben nach unten	Microsoft SharePoint
Microsoft SQL Server- und Cluster-Discovery	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Horizontal und von oben nach unten	MSSQL-DB unter Windows (Muster)
Microsoft SQL Server Analysis Services (SSAS)	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Horizontal und von oben nach unten	SSAS (Muster)
Microsoft Discovery von SQL Server Integration Services (SSIS)	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Von oben nach unten	SSIS (Muster)
Microsoft SQL Server Reporting Services	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Von oben nach unten	SSRS (Muster)
Microsoft Windows-Desktops	Windows	2003, 2008, 2012,	WMI WinRM	Horizontal	Windows OS - Desktops
Microsoft Windows-Server	Windows	2003, 2008, 2012, 2016, 2022	WMI WinRM	Horizontal	Windows OS - Server
MongoDB	Windows UNIX	3.x.x	WMI WinRM SSH	Horizontal und von oben nach unten	Mongos-Server
NetApp Server und Cluster Discovery	NetApp	7.x,8.x	SNMP	Horizontal	Muster:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					NetApp Storage 7-Modus NetApp Cluster SNMP
NetApp Server und Cluster Discovery	NetApp	7.x,8.x,9.x	HTTP	Horizontal	NetApp Cluster HTTP (Muster)
NetApp SolidFire-Speichersystem	NetApp SolidFire	N/V	HTTP	Horizontal	NetApp SolidFire-Speichersystem
Netzwerkrouter	Windows UNIX	N/V	SNMP	Horizontal	Network Router
Netzwerk-Switch	Windows UNIX	N/V	SNMP	Horizontal	Network Switch
NGINX-Webserver	Windows UNIX	1.10, 1.10.1	WMI WinRM SSH	Von oben nach unten	Nginx-Muster
Nutanix Acropolis (AOS)	UNIX	N/V	REST	Horizontal	Nutanix-Komponenten
Nutanix Prism Central	UNIX	N/V	REST	Horizontal	Nutanix-Komponenten
OpenText Documentum	Windows UNIX	6.x, 7.x	WMI WinRM SSH	Von oben nach unten	Muster für Lizenzserver
OpenStack-Ressourcen	OpenStack	N/V	REST	Horizontal	OpenStack (Muster)
Oracle Applikationsserver	Windows UNIX	9.x, 10.x	WMI WinRM	Von oben nach unten	Oracle iAS

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
			SSH		
Oracle Concurrent Server	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Von oben nach unten	Concurrent Server
Oracle Cloud-Infrastruktur	Oracle	N/V	REST	Horizontal	Oracle Cloud-Infrastruktur
Oracle Clusterware	Linux	10.x, 11.x, 12.x	SSH	Horizontal	Oracle CRS
Oracle Datenbank	Windows UNIX	8.x.x, 9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Horizontal und von oben nach unten	Oracle-DB
Oracle Database Advanced Queuing	Windows UNIX	9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Von oben nach unten	Advanced Queue Queue
Oracle Datenbank 12c	Windows UNIX	N/V	WMI WinRM SSH	Horizontal	PDB/CDB
Oracle Discover Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Discoverer Engine
Oracle E-Business Suite	Windows UNIX	10.x, 11.x	WMI WinRM SSH	Von oben nach unten	E-Business Suite
Oracle Formulare	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Formulare-Engine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle Fulfillment Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Fulfillment Server
Oracle GoldenGate	Windows UNIX	N/V	WMI SSH	Horizontal und von oben nach unten	Oracle GG
Oracle Linux Virtualization Manager (OLVM) und Red hat Virtualization (RHV)	OLVM und RHV	N/V	REST	Horizontal	Muster: • OVirt-Cluster und -Hosts • OVirt – logische Rechenzentren erkennen • OVirt Discover Manager-Instanz • Virtuelle oVirt-Maschinen
Oracle Global License Advisory Services (GLAS)	N/V	N/V	SSH	Horizontal	Oracle GLAS-Datenerfassung (Muster)
Oracle Java-Prozesse	JDK	Alle	N/V	Horizontal	Java-Installationsmuster ACC-basierte Discovery
Oracle Solaris LDOM	Solaris	10, 11	SSH	Horizontal	Solaris Logical Domain (LDOM)-Infrastruktur
Oracle HTTP Server	Windows UNIX	N/V	WMI WinRM SSH	Von oben nach unten	HTTP Server

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle iPlanet Webserver	Solaris	4.x, 6.x, 7.x	SSH	Horizontal und von oben nach unten	Sun iPlanet Webserver
Oracle Java Enterprise System (JES)	Solaris	7.x	SSH	Von oben nach unten	Sun JES-Muster
Oracle-Listener	Linux	12.2.x.x	SSH	Horizontal	Oracle Listener HD
Oracle Metric Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Metric Server
Oracle MySQL Server	Windows UNIX	4.x, 5.x	WMI WinRM SSH	Horizontal und von oben nach unten	My SQL Server unter Windows und Linux (Muster)
Oracle Notification Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Oracle Benachrichtigungs-Server
Oracle Peoplesoft	Windows Unix	8.x	WMI WinRM SSH	Von oben nach unten	PeopleSoft-Applikationsserver
Oracle Prozessmanager	Windows Unix	9.x.x, 10.x.x	WMI WinRM SSH	Von oben nach unten	Prozessmanager
Oracle RAC	Windows UNIX	9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Von oben nach unten	App TNS-Dienst
Oracle Berichtsserver	Windows	9.x.x, 10.x.x	WMI WinRM	Von oben nach unten	Berichtsserver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
	UNIX		SSH		
Oracle Solaris Server	Solaris	9, 10, 11, SPARC	SSH	Horizontal	Solaris-Server
Oracle Solaris Infrastruktur der logischen Domäne	Solaris	N/V	SSH	Horizontal	Solaris LDOM
Oracle WebLogic Application Server	Windows UNIX	8.x, 9.x, 10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	WebLogic
Pivotal Cloud Foundry	PCF	N/V	REST	Horizontal und von oben nach unten	Muster: Pivotal Cloud Foundry Bosh
Pivotal RabbitMQ	Windows UNIX	3.x.x	WMI WinRM SSH	Von oben nach unten	RabbitMQ Cluster Unix - Muster
PostgreSQL-DB	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	PostgreSQL-DB
Puppet	UNIX	N/V	SSH	Horizontal	Sonden: • Puppet – Master-Info • Puppet – Zertifikatsanfragen • Puppet – Manifest • Puppet - Modules
Reiner Speicher FlashArray Discovery	Pure Storage	N/V	REST	Horizontal	Pure Flash Array Storage (Muster)
Pure Storage FlashBlade	Pure Storage	4.10.7	REST	Horizontal	Pure Storage

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
			SSH		
RadWare AppDirector (Lastenausgleichsmodul)	Radware	N/V	SNMP	Horizontal und von oben nach unten	AppDirector Load Balancer
Red Hat Cluster Suite	Linux	RH 5.x, 6.x, 7.x	SSH	Horizontal	RH Cluster
Red Hat JBoss-Anwendungsserver	Windows UNIX	6.x, 7.x	WMI WinRM SSH	Horizontal und von oben nach unten	Jboss (Muster)
Red Hat JBoss Fuse-Erkennung	Windows UNIX	N/V	SSH	Horizontal und von oben nach unten	Jboss Fuse (Muster)
Red Hat OpenShift-Komponenten von Kubernetes	RHEL	API 1.x	REST	Horizontal	OpenShift-Infobibliothek sammeln, die als Erweiterungsabschnitt des Kubernetes-Musters verwendet wird
Rubrik-Cluster		N/V	HTTP HTTPS	Horizontal	Mehrere Muster
SAP Business Object XI Scheduler	Windows	2004, 2005, 2008	WMI WinRM	Horizontal und von oben nach unten	SAP BO BOXIScheduleRouter on Windows - Muster
SAP Crystal Management Server	Windows	2004, 2005, 2008	WinRM	Horizontal und von oben nach unten	SAP Business Objects CMS Server on Windows
SAP HANA	Windows UNIX	2015, 2016, 2017	WMI WinRM SSH	Horizontal und von oben nach unten	SAP HANA DB (Muster)
SAP HANA-Katalog	UNIX	N/V	N/V	Horizontal	SAP Hana 2.0 DB-Katalog (Muster)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
SAP Sybase-ASE-Discovery	Windows UNIX	16	WMI WinRM SSH	Horizontal und von oben nach unten	Sybase (Muster)
SAP Sybase-ASE-Discovery-Katalog	UNIX	16	SSH	Horizontal	Sybase (Mustererweiterung)
Cisco Wireless Access Point (WAP) wechseln	Cisco Network Switch	N/V	SNMP	Horizontal	WAP
Sun Directory Proxy Server	Solaris	4.0.8	SSH	Von oben nach unten	Sun Directory-Proxy-Server
Sun Java System Directory Server	Solaris	6.3	SSH	Von oben nach unten	Sun Directory Server
Thunder ADC	A10	2.x, 4.x	SNMP/SSH	Horizontal und von oben nach unten	A10 Lastenausgleich
Tibco ActiveMatrix Adapter	UNIX	7.1.0	SSH	Von oben nach unten	Tibco-Adapter
Tibco BusinessWorks	Windows UNIX	5.7.2	WMI WinRM SSH	Horizontal	ActiveMatrix BusinessWorks
Tibco Enterprise Message Service (EMS)	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Horizontal und von oben nach unten	Enterprise Message Service
Tibco Enterprise Message Service (EMS)-Warteschlange	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Horizontal und von oben nach unten	Enterprise Message Service
Tibco Hawk	UNIX	5.2.0	SSH	Von oben nach unten	TibcoHawk

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Veritas Enterprise Vault	Windows	14.1	WMI WinRM	Von oben nach unten	Enterprise Vault
Veritas-Clusterserver	UNIX	6.xx	SSH	Horizontal und von oben nach unten	Veritas-Cluster
VMware NSX Advanced Load Balancer	VMware	1	REST-API	Horizontal und von oben nach unten	NSX

Referenzen zur Discovery von Cloud-Ressourcen

ITOM-Transparenz erkennt Ressourcen auf Cloud-Plattformen.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Für Amazon erfasste Daten AWS Cloud-Discovery

Discovery erfasst Informationen über Cloud-Ressourcen in AWS-Rechenzentren. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Hinweis: Sie können testen AWS REST APIs mit Postman API-Plattform. Weitere Informationen finden Sie unter So testen Sie die AWS-REST-API mit POSTMAN [KB0782183] artikel in Now Support Knowledge Base.

Bei der Erkennung von AWS Cloud erfasste Daten

AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Bezeichnung	Feldname
Name	Name
Region	region
Objekt-ID	object_id

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Bezeichnung	Feldname
Name	Name

VM-Instanz [cmdb_ci_vm_instance]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
CPUs	CPUs
Datenträger	disks
Arbeitsspeicher	memory
Netzwerkadapter	nics
ID der VM-Instanz	vm_inst_id

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Images [cmdb_ci_os_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Gast-BS	guest_os
Stammgerätetyp	root_device_type
Image-Quelle	image_source
Bildtyp	image_type

Hardwaretyp [cmdb_ci_compute_template]

Bezeichnung	Feldname
Name	Name
vCPUs	vcpus
Arbeitsspeicher – MB	memory_mb
Lokaler Speicher – GB	local_storage_gb

Speichervolume [cmdb_ci_storage_volume]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
Speichertyp	storage_type
Größe	size

Cloud-Netzwerke [cmdb_ci_network] und VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Bezeichnung	Feldname
Name	Name
Status*	Status
CIDR*	cidr

*In VMware vCenter-Netzwerken nicht erkannt

Cloud-Subnetze [cmdb_ci_cloud_subnet]

Bezeichnung	Feldname
Name	Name
Status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Subnetze [cmdb_ci_cloud_subnet] (Fortsetzung)

Bezeichnung	Feldname
CIDR	cidr

Cloud Management-Netzwerkschnittstellen [cmdb_ci_nic]

Bezeichnung	Feldname
Name	Name
Netzmaske	netmask
MAC-Hersteller	mac_manufacturer
Status	install_status

Cloud-Lastenausgleichsmodule [cmdb_ci_cloud_load_balancer]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Ressourcengruppen [cmdb_ci_resource_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Öffentliche IP-Adresse	public_ip_address
Öffentlicher DNS	public_dns

Speicherkonten [cmdb_ci_cloud_storage_account]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
SKU-Name	sku_name
Status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DNS-Alias [cmdb_ci_dns_alias] und DNS-Name [cmdb_ci_dns_name]

Bezeichnung	Feldname
DNS-Alias [cmdb_ci_dns_alias]	
Name	Name
Kategorie	Kategorie
Status	Status
DNS-Name [cmdb_ci_dns_name]	
Name	Name
IP-Adresse	ip_address

Cloud-Datenbanken [cmdb_ci_cloud_database]

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name der Datenbank, die Sie in AWS erstellt haben
Objekt-ID	object_id	Dies ist auch der Name der Datenbank.
Typ	Typ	Der Typ der von Ihnen erstellten Datenbank.
Vollqualifizierter Domänenname	fqdn	Der FQDN, den AWS Ihrer Datenbank zugewiesen hat. Ein Beispielformat für AWS lautet wie folgt: `database-name.{random-number}.{datacenter}.rds.amazonaws.com`
Status	Status	Der Status der Datenbank: Verfügbar oder Beendet.
TCP-Port(s)	tcp_port	Der TCP-Port, über den die Datenbank kommuniziert.
Kategorie	Kategorie	Die Instanzklasse der Datenbank, zum Beispiel: db.t2.micro.

Cloud-Webserver [cmdb_ci_cloud_webserver]

Bezeichnung	Feldname
Name	Name
Installationsstatus	install_status
Lieferant	Lieferant
Vollqualifizierter Domänenname	fqdn
Betriebsstatus	operational_status
Status	state

Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name des kube-Controller-Manager-Leader

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kubernetes-Cluster [cmdb_ci_kubernetes_cluster] (Fortsetzung)

Bezeichnung	Feldname	Beschreibung
Port	port	Der Bezeichner für den Kubernetes-Apiserver-Port.
Kubernetes-UID	k8s_uid	Eindeutiger Bezeichner für den Kubernetes-Cluster.
Lieferant	Lieferant	Anbieter des Kubernetes-Clusters.
Vollqualifizierter Domänenname	fqdn	Vollständig qualifizierter Domänenname des Kubernetes-API-Servers.

Für Microsoft Azure Cloud-Discovery erfasste Daten

Von Discovery werden Informationen über Cloud-Ressourcen in Microsoft Azure-Rechenzentren erfasst. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Erstellen Azure Cloud-Anmeldeinformationen

Erstellen Sie Microsoft Azure-Anmeldeinformationen für den Zugriff auf das Microsoft Azure-Konto. Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Vorgehensweise von Discovery zur Erkennung von Microsoft Azure-Ressourcen

Discovery Verwendet Cloud Provisioning and Governance API und Muster für Discovery und Service-Mapping Um Cloud-Ressourcen zu finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmuster

Muster	Beschreibung
Azure Datenbank (LP)	Erkennt Datenbanktypen von: • Microsoft.sql/Server • microsoft.sql/managedInstances • microsoft.dbformysql • microsoft.documentdb/databaseAccounts • microsoft.cache/redis • microsoft.dbforpostgresql/Servers • microsoft.dbformysql/Server • microsoft.dbformysql/flexibleservers • microsoft.dbforpostgresql/flexibleservers Füllt die Tabelle [cmdb_ci_Cloud_database] aus.
Azure LoadBalancer TD	Ruft Microsoft Azure-Lastenausgleichsmodule ab und füllt die Tabelle cmdb_ci_lb_service. Dieses Muster wird nicht von Discovery für die horizontale Erkennung verwendet, sondern nur von Service-Mapping für die Erkennung von oben nach unten.
Azure Website (LP)	Ruft Microsoft Azure-Webserver ab und füllt die Tabellen „Cloud-Webserver“ [cmdb_ci_cloud_webserver] und „IP-Adresse“ [cmdb_ci_ip_address].

Von Discovery während der horizontalen Erkennung erfasste Daten

Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Bezeichnung	Feldname
Name	Name
Region	region
Objekt-ID	object_id

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Bezeichnung	Feldname
Name	Name

VM-Instanz [cmdb_ci_vm_instance]

Bezeichnung	Feldname
Name	Name
Status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VM-Instanz [cmdb_ci_vm_instance] (Fortsetzung)

Bezeichnung	Feldname
Objekt-ID	object_id
CPUs	CPUs
Datenträger	disks
Datenträgergröße (GB)	disks_size
Arbeitsspeicher	memory
Netzwerkadapter	nics
ID der VM-Instanz	vm_inst_id

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Images [cmdb_ci_os_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Gast-BS	guest_os
Image-Quelle	image_source

Speichervolume [cmdb_ci_storage_volume]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
Speichertyp	storage_type
Größe	size

Cloud-Netzwerke [cmdb_ci_network] und VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Bezeichnung	Feldname
Name	Name
Status*	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Netzwerke [cmdb_ci_network] und VMware vCenter-Netzwerk [cmdb_ci_vcenter_network] (Fortsetzung)

Bezeichnung	Feldname
CIDR*	cidr

*In VMware vCenter-Netzwerken nicht erkannt.

Cloud-Subnetze [cmdb_ci_cloud_subnet]

Bezeichnung	Feldname
Name	Name
Status	Status
CIDR	cidr

Cloud Provisioning and Governance Netzwerkschnittstellen [cmdb_ci_nic]

Bezeichnung	Feldname
Name	Name
Netzmaske	netmask
MAC-Adresse	mac_address
MAC-Hersteller	mac_manufacturer
Status	install_status

Cloud-Lastenausgleichsmodule [cmdb_ci_cloud_load_balancer]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	state

Azure-Bereitstellungen [cmdb_ci_azure_deployment]

Bezeichnung	Feldname
Name	Name
Bereitstellungsstatus	provisioning_state

Hinweis: Diese Tabelle ist nur für verfügbar Discovery Wenn Cloud Provisioning and Governance Plugin ist aktiviert.

Ressourcengruppen [cmdb_ci_resource_group]

Bezeichnung	Feldname
Name	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcengruppen [cmdb_ci_resource_group] (Fortsetzung)

Bezeichnung	Feldname
Objekt-ID	object_id
Status	Status
Betriebsstatus	operational_status
Installationsstatus	install_status

Hinweis:

- Wenn eine Ressourcengruppe zum ersten Mal erkannt wird, wird **Status** Feld ist auf festgelegt **Verfügbar** , **Operational_Status=operativ** , Und **Status=Installiert** ; Basierend auf der Antwortzuordnung.
- Wenn eine Ressourcengruppe am beendet wird Microsoft Azure, Die CMPReconciler-Skripts legen fest **Status** Feld bis **Beendet** , Und **Operational_Status=nicht funktionsfähig** Und **Status=Abwesend** .

Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Öffentliche IP-Adresse	public_ip_address
Öffentlicher DNS	public_dns

Speicherkonten [cmdb_ci_cloud_storage_account]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
SKU-Name	sku_name
Status	Status

Cloud-Datenbanken [cmdb_ci_cloud_database]

Bezeichnung	Feldname
Vollqualifizierter Domänenname	fqdn
Name	Name
Objekt-ID	object_id
Betriebsstatus	operational_status
Typ	type
Status	Status
Lieferant	Lieferant

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Datenbanken [cmdb_ci_cloud_database] (Fortsetzung)

Bezeichnung	Feldname
Version	Version **Hinweis:** Für NoSQL- und MSSQL-verwaltete Instanzen geben die API-Antworten für diese Datenbanken keine Versionsdaten zurück.
Kategorie	Kategorie

Cloud-Webserver [cmdb_ci_cloud_webserver]

Bezeichnung	Feldname
Name	Name
Installationsstatus	install_status
Lieferant	Lieferant
Vollqualifizierter Domänenname	fqdn
Betriebsstatus	operational_status
Status	Status

IP-Adresse [cmdb_ci_ip_address]

Bezeichnung	Feldname
Vollqualifizierter Domänenname	fqdn
Installationsstatus	install_status
IP-Adresse	ip_address
Name	Name
Netzmaske	netmask
Betriebsstatus	operational_status
Lieferant	Lieferant

Datenbank [cmdb_ci_database]

Bezeichnung	Feldname
Status der Lebenszyklusphase	life_cycle_stage_status
Name	Name
Status	status
Seriennummer	serial_number
Typ	type

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechnungsvorlage [cmdb_ci_compute_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
VCPUS	vcpus

Hardwaretyp [cmdb_ci_Hardware_type]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Anbieter	Anbieter
vCPUs	vcpus

Zugehörige Informationen

Microsoft Azure Cloud-Discovery mithilfe von Mustern

Für GCP Cloud-Discovery erfasste Daten

Discovery Sammelt Informationen zu Cloud-Ressourcen in Google Cloud Platform (GCP). Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP Daten erfasst

Tabelle	ServiceNow-Feld	GCP-Feld
Region [cmdb_ci_google_datacenter]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	region	items.name
Virtueller Server [cmdb_ci_vm_instance]	object_id	id
	Name	Name
	Status	Status
	CPUs	Nicht zugeordnet
	memory	Nicht zugeordnet
	disks	Datenträger (Array-Größe)
	disks_size	Nicht zugeordnet
	nics	networkInterfaces (Array-Größe)
	termination_protection	deletionProtection
	Nicht zugeordnet	canIpForward
	Nicht zugeordnet	selfLink
	sys_created_on	creationTimestamp
Speichervolume (cmdb_ci_storage_volume)	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	status	Status
	size	sizeGb
	storage_type	storage_type
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	object_id	items.id
	Name	Name
	public_ip_address	address
	Status	Status
Verfügbarkeitszone [cmdb_ci_availability_zone]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	status	Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	ServiceNow-Feld	GCP-Feld
Hardwarevorlage [cmdb_ci_compute_template]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	vcpus	guestCpus
	memory_mb	memoryMb
	local_storage_gb	imageSpaceGb
Instanzvorlage [cmdb_ci_instance_template]	object_id	items.id
	Name	Name
	short_description	Beschreibung
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	object_id	items.id
	Name	Name
	Status	Status
	volume_name	sourceDisk
	Kapazität	storageBytes
	Keine Zuordnung	storageBytesStatus
	Keine Zuordnung	selfLink
	Keine Zuordnung	labelFingerprint
	Keine Zuordnung	diskSizeGb
Datenträgertyp [cmdb_ci_disk_type]	object_id	zone:name
	Name	name@zone
	short_description	Beschreibung
	valid_disk_size	validDiskSize
	default_disk_size_gb	defaultDiskSizeGb
Subnetz [cmdb_ci_cloud_subnet]	object_id	id
	Name	Name
	cidr	ipCidrRange
	gateway	gatewayAddress
Image [cmdb_ci_os_template]	object_id	items.id
	Name	Name
	image_type	sourceType
	Keine Zuordnung	Status
	Keine Zuordnung	archiveSizeBytes
	Keine Zuordnung	diskSizeGb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	ServiceNow-Feld	GCP-Feld
	image_source	• sourceDisk • sourceDiskId
Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]	object_id	id
	Name	Name
	Keine Zuordnung	defaultService
Lastenausgleichsservice (cmdb_ci_lb_service)	object_id	id
	Name	Name
	Pool	backends
	port	port
	listener_protocol	protocol
	Keine Zuordnung	portName
	Keine Zuordnung	loadBalancingScheme
	Keine Zuordnung	sessionAffinity
	Keine Zuordnung	enableCDN
	service_type	Back-End/Front-End
Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_health_service]	object_id	id
	Name	Name
	monitor_type	type (tcp/http/https)
	request_path	requestPath
	port	port
	unhealthy_threshold	unhealthyThreshold
	healthy_threshold	healthyThreshold
	timeout_sec	timeoutSec
	check_interval_sec	checkIntervalSec
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	object_id	Instanz-ID von GCP
	Name	instance.substring nach dem letzten „/“
	Betriebsstatus	Status
Load Balancer-Pool [cmdb_ci_lb_pool]	object_id	id
	Name	Name
Netzwerk [cmdb_ci_network]	Status	Keine Zuordnung
	cidr	IPv4Range
	is_external	Keine Zuordnung
	Name	Name
	object_id	items_id

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	ServiceNow-Feld	GCP-Feld
	Beschreibung	Beschreibung
Netzwerk-ACL [cmdb_ci_network_acl]	object_id	id
	Name	Name
	short_description	Beschreibung
Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule]	is_outbound (True/False)	ac
	dest_from_port	Keine Zuordnung
	dest_to_port	Keine Zuordnung
	src_from_port	Keine Zuordnung
	src_to_port	Keine Zuordnung
	source_ranges	sourceRanges
	destination_ranges	destinationRanges
	target_tags	targetTags
	allowed_traffic	allowed
Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]	IP-Adresse	ip_address
	Name	Name
	Port	port
	Kubernetes-UID	k8s_uid
	Lieferant	Lieferant

Für IBM Cloud-Discovery erfasste Daten

Discovery Sammelt Informationen zu Cloud-Ressourcen in IBM Cloud Platform Und erstellt Beziehungen zwischen den gefundenen CIs. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Lastenausgleichsmodule

Für Lastenausgleichsmodule erfasste Daten

Tabelle	Feldname/-beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	**object_id**: Eindeutiger Bezeichner des Lastenausgleichsmoduls
	name: Name des Lastenausgleichsmoduls
	fqdn: Adresse (Hostname) des Lastenausgleichsmoduls. Das ist der *vollqualifizierte Domänenname* des Lastenausgleichsmoduls.
	dns_name: Adresse (Hostname) des Lastenausgleichsmoduls
	short_description: Beschreibung des Lastenausgleichsmoduls
	operational_status: Betriebsstatus des Lastenausgleichsmoduls, entweder **ONLINE** oder **OFFLINE**
	location: Verweist auf den Standort des Lastenausgleichsmoduls mit dem Typ
	state: Bereitstellungsstatus des Lastenausgleichsmoduls, entweder **Verfügbar** oder **Beendet**
Load Balancer-Service [cmdb_ci_lb_service]	**object_id**: Eindeutiger Bezeichner des Lastenausgleichsservice
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Port • Ressourcentyp: **-listener**
	Port: Portnummer des Listener-Protokolls
	front_end_port: Portnummer des Listener-Protokolls
	listener_protokoll: Listener-Protokoll, entweder **TCP**, **HTTP** oder **HTTPS**
	operational_status: Bereitstellungsstatus des Listener.
Load Balancer-Pool [cmdb_ci_lb_pool]	**object_id**: Eindeutiger Bezeichner des Pools von Lastenausgleichsmodulen
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Lastenausgleichsmodule erfasste Daten (Fortsetzung)

Tabelle	Feldname/-beschreibung
	• Name des Lastenausgleichmoduls • Protokoll • Port • Ressourcentyp: **-pool**
	port: Protokollport am Back-End
	pool_status: Bereitstellungsstatus eines Lastenausgleichsmodul-Pools
	load_balancing_method: Methode, die für den Lastenausgleich des Pools verwendet wird
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	**object-id**: Eindeutiger Bezeichner des Poolmitglieds, zusammengesetzt aus der ID des Mitglieds und der Listener-ID
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Port • Ressourcentyp: **-member** • IP-Adresse des Poolmitglieds
	ip_address: IP-Adresse eines Lastenausgleichsmodulmitglieds
	server_id: ID des Mitglieds in der IBM-Cloud
	load_balancer: Name des zugehörigen Lastenausgleichsmoduls
Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_health_service]	**object_id**: Eindeutiger Bezeichner der Integritätsserviceprüfung
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Ressourcentyp: **Integritätsprüfung** • Ressourcen-ID
	monitor_type: Typ der Integritätsprüfung. Gültige Werte: **TCP**, **HTTP** und **HTTPS**
	timeout_sec: Dauer in Sekunden, die auf die Antwort der Integritätsprüfung gewartet wird, bis eine Zeitüberschreitung auftritt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Lastenausgleichsmodule erfasste Daten (Fortsetzung)

Tabelle	Feldname/-beschreibung
	check_interval_sec: Intervall in Sekunden zur Durchführung der Integritätsprüfung

Für Lastenausgleichsmodule erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_health_service
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_lb_service
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Enthält::Enthalten in	cmdb_ci_lb_pool
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member

Organisationen und Bereiche

Für Organisationen und Bereiche erfasste Daten

Tabelle	Felder
IBM Cloud-Organisationen [cmdb_ci_cloud_org]	• **guid**: Der eindeutige Bezeichner der Organisation • **URL**: Die eindeutige URL der Organisation • **billing_enabled**: Gibt an, ob die Abrechnungsmethode der Organisation aktiviert oder deaktiviert ist • **name**: Eindeutiger Name der Cloud-Organisation • **quota_definition_url**: Ressourcen, die für die Organisation verfügbar sind • **spaces_url**: Eindeutige URL des Bereichs, der der Organisation zugewiesen ist • **operational_status**: Betriebsstatus der Organisation
IBM-Cloudbereich [cmdb_ci_cloud_space]	• **object_id**: Eindeutiger Bezeichner (GUID) des Bereichs • **name**: Eindeutiger Name des Bereichs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Organisationen und Bereiche erfasste Daten (Fortsetzung)

Tabelle	Felder
	• **url**: Eindeutige URL des Bereichs • **allow_ssh**: Die IP-Adresse einer Speicherressource

Für Organisationen und Bereiche erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_org	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_space	Gehostet auf::Hostet	cmdb_ci_cloud_org
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_cloud_space

SSH-Schlüssel

Für SSH-Schlüssel erfasste Daten

Tabelle	Felder
Cloud-Schlüsselpaare [cmdb_ci_cloud_key_pair]	• **object_id**: ID des SSH-Schlüsseldatensatzes • **Name**: Beschreibender Name, der zur Identifizierung des SSH-Schlüssels verwendet wird • **key**: SSH-Schlüssel • **finger_print**: Kurze Bytefolge, die zur Authentifizierung oder Suche nach einem längeren SSH-Schlüssel verwendet wird. Diese wird beim Hinzufügen oder Ändern des SSH-Schlüssels automatisch generiert. Diese Eigenschaft ist schreibgeschützt. Vorgenommene Änderungen werden ignoriert. • **created_date**: Datum, an dem der SSH-Schlüssel hinzugefügt wurde. Diese Eigenschaft ist schreibgeschützt. Vorgenommene Änderungen werden ignoriert. • **modify_date**: Datum, an dem der SSH-Schlüssel zuletzt geändert wurde. Diese Eigenschaft ist schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für SSH-Schlüssel erfasste Daten (Fortsetzung)

Tabelle	Felder
	Vorgenommene Änderungen werden ignoriert. • **short_description**: Kurze Notiz zum SSH-Schlüssel.

Für SSH-Schlüssel erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

IBM Cloud-Speicher

Daten erfasst für IBM Cloud-Speicher

Tabelle	Felder
Speichervolume [cmdb_ci_storage_volume]	• **object_id**: Eindeutiger Bezeichner des Speicherkontos • **size**: Kapazität des Speicherkontos in Gigabyte • **size_bytes**: Kapazität des Speicherkontos in Byte • **name**: Benutzername, der für den Zugriff auf ein Nicht-EVault-Speichervolume verwendet wird. Dieser Benutzername wird verwendet, um den EVault-Server-Agent beim Vault-Sicherungssystem zu registrieren. • **label**: Name der Netzwerkressource für den Speicher • **storage_type**: Beschreibung des Speicherobjekts • **fqdn**: IP-Adresse einer Speicherressource • **device**: Eindeutige Identifikationsnummer des Gasts, der dem Speichervolume zugeordnet ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erfasst für IBM Cloud-Speicher (Fortsetzung)

Tabelle	Felder
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	• **object_id**: Eindeutiger Bezeichner des Speicherkontos • **name**: Name der Netzwerkressource des Speichers • **capacity**: Konfigurierte Snapshot-Speichergröße des Volume • **fqdn**: IP-Adresse einer Speicherressource • **location**: Eindeutige Verfügbarkeitszone, in der sich das Speichervolume befindet

Beziehungen für erstellt IBM Cloud-Speicher

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_storage_volume	Bereitgestellt::Bereitgestellt von	cmdb_ci_storage_vol_snapshot
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_vol_snapshot	Positioniert in Zone::Zone beinhaltet	cmdb_ci_availability_zone
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_storage_volume

IBM Virtuelle Cloud-Server

Daten erfasst für IBM Virtuelle Cloud-Server

Tabelle	Felder
VM-Instanz [cmdb_ci_vm_instance]	• **name**: Name des virtuellen Computers • **object_id**: ID des virtuellen Computers • **dns_domain**: Domäne des virtuellen Computers • **fqdn**: IP-Adresse des virtuellen Computers • **short_description**: Hinweise, die dem virtuellen Computer auf der IBM-Konsole hinzugefügt sind • **cpus**: Anzahl der CPUs des virtuellen Computers • **memory**: Größe des Arbeitsspeichers des virtuellen Computers • **disks**: Anzahl der vom virtuellen Computer verwendeten Datenträger

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erfasst für IBM Virtuelle Cloud-Server (Fortsetzung)

Tabelle	Felder

	• **state**: Ausführungsstatus des virtuellen Computers Die Auswahlmöglichkeiten sind:
	  ○ **Wird ausgeführt**
	  ○ **Angehalten**
	• **placement_group_id**: Name der IBM-Platzierungsgruppe, die den virtuellen Computer enthält
	• **nics**: Anzahl der Netzwerkschnittstellen auf dem virtuellen Computer

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	• **name**: Name und Port der NIC im Format ***<Name><Port>*** • **ip_address**: Auf der NIC konfigurierte IP-Adresse • **mac_address**: MAC-Adresse der NIC • **netmask**: Netzmaske der NIC • **object_id**: ID der NIC • **status**: Status der NIC – VERFÜGBAR
Image [cmdb_ci_os_template]	• **name**: Lange Beschreibung der Vorlage. Beispiel: **CentOS 7.0-64 Minimal für VSI**. • **version**: Version des Betriebssystems. Beispiel: **7.0-64 Minimal für VSI** • **object_id**: ID des Image • **guest_os**: Betriebssystem des virtuellen Computers, zum Beispiel Windows, Ubuntu und CentOS
Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]	• **name**: Schlüsselbezeichnung • **object_id**: ID des Schlüssels
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	• **name**: Name der Sicherheitsgruppe • **object_id**: ID der Sicherheitsgruppe • **short_description**: Hinweise zur Sicherheitsgruppe
Speichervolume [cmdb_ci_storage_volume]	**object_id**: ID des Speichervolume

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen für erstellt IBM Virtuelle Cloud-Server

CI	Beziehung	CI
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_vm_instance	Positioniert in::Anordnen	cmdb_ci_availability_zone
cmdb_ci_nic	Enthalten in::Enthält	cmdb_ci_vm_instance
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_os_template	Bereitgestellt von::Stellt bereit	cmdb_ci_vm_instance
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_key_pair	Verwendet von::Verwendet	cmdb_ci_vm_instance
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_compute_security_group	Endpunkt implementieren von::Endpunkt implementieren in	cmdb_ci_vm_instance
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Endpunkt implementieren von::Endpunkt implementieren in	cmdb_ci_vm_instance

IBM Cloud-Service-Account

Daten erfasst für IBM Cloud-Service-Account

Tabelle	Feld
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	• **name**: Anzeigename des Cloud-Servicekontos • **account_id**: Servicekonto-ID • **object_id**: Cloud-ID des Servicekontos. Diese ist mit der account_id identisch. • **datacenter_type**: Dies ist **cmdb_ci_ibm_datacenter**. • **discovery_credentials**: Die sys_id der Anmeldeinformationen
IBM-Rechenzentrum [cmdb_ci_ibm_datacenter]	• **name**: Anzeigename des Cloud-Servicekontos • **account_id**: Servicekonto-ID • **object_id**: Cloud-ID des Servicekontos. Diese ist mit der account_id identisch. • **datacenter_type**: Dies ist **cmdb_ci_ibm_datacenter**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen für erstellt IBM Cloud-Service-Accounts

CI	Beziehung	CI
cmdb_ci_cloud_service_account	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_cloud_service_account	Enthalten in::Enthält	cmdb_ci_ibm_datacenter
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_cloud_key_pair
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_vm_instance
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_lb_service
cmdb_ci_ibm_datacenter	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Hostet::Gehostet auf	cmdb_ci_network

Daten erfasst für VMware Cloud Discovery

Discovery sammelt Informationen zu VMware Ressourcen in Ihren Cloud-Service-Accounts.

Erkennung von Distributed Resource Scheduler (DRS)

VMware Discovery erfasst diese DRS-Einstellungen und speichert sie in der Tabelle „DRS-VM-Konfig.“ [cmdb_ci_drs_vm_config]:

- DRS-Einstellungen von vCenter-Clustern
- DRS-Einstellungen von VMs, die so konfiguriert sind, dass sie das Clusterverhalten überschreiben

DRS-VM-Konfiguration [cmdb_ci_drs_vm_config]

Feldbezeichnung	Spaltenname
Cluster	Cluster
DRS-Verhalten	drs_behavior
DRS-fähig	drs_enabled
Virtueller Computer	virtual_machine

VMware-Tags

VMware Cloud-Discovery erfasst VMware-Tags aus vCenter und speichert sie in der Tabelle „Schlüsselwert“ [cmdb_key_value].

Schlüsselwerte [cmdb_key_value]

Feldbezeichnung und -name	Beschreibung
Konfigurationselement [configuration_item]	Referenzierte VM mit angehängtem Tag in vCenter
Schlüssel [key]	Kategoriename des Tag, das auf die Ressource in vCenter angewendet wird
Tag [tag]	Quelle in vCenter, aus der Tags abgerufen werden. In diesem Fall lautet der Wert immer **Tags**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwerte [cmdb_key_value] (Fortsetzung)

Feldbezeichnung und -name	Beschreibung
Wert [value]	Name des Tag, das in vCenter auf die Ressource angewendet wird

Erkennung von Betriebssystemen

Discovery identifiziert die folgenden Computer, Cluster und virtuellen Computer.

Erkennung von AIX-Servern

Discovery identifiziert und klassifiziert Informationen über AIX-Server.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Verwenden Sie für AIX-Computer OpenSSH Version 7.5.102 und höher, da sich frühere Versionen von OpenSSH darauf auswirken können, welche Geräte von Discovery erkannt werden.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
AIX (UNIX-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • AIX - Installed Software^ • AIX - ADM^ • AIX - Identity* • AIX - CPU* • AIX - Hardware Model* • AIX - Memory* • AIX - OS Patches* • AIX - OS Release* • AIX - OS Revision* • UNIX - Find FQDN	AIX-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierung	Probes	Muster
	• UNIX - OS Filesystems • UNIX - OS Uptime	

*Diese Probes sind in der Klassifizierung als nicht aktiv Discovery Verwendet standardmäßig Muster für diese Erkennungen.

^diese Probes bleiben standardmäßig aktiv, auch wenn Discovery Verwendet Muster-Discovery.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
BS-Version	cmdb_ci_computer	os_version	oslevel
BS-Service Pack	cmdb_ci_computer	os_service_pack	oslevel
Kurzbeschreibung	cmdb_ci_aix_server	short_description	uname
Name	cmdb_ci_aix_server	Name	DNS, NBT
Hostname	cmdb_ci_aix_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_aix_server	dns_domain	DNS
Startdatum	cmdb_ci_aix_server	start_date	uptime
CPU-Typ	cmdb_ci_computer	cpu_type	lsdev, lsattr
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	lsdev, lsattr
CPU-Anzahl	cmdb_ci_computer	cpu_count	lsdev, lsattr
Hersteller	cmdb_ci_aix_server	manufacturer	lsattr
Modell-ID	cmdb_ci_aix_server	model_id	lsattr
RAM (MB)	cmdb_ci_computer	ram	lsdev, lsattr
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	instfix
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Verbunden mit	cmdb_running_process	connects_to	lsof
Lauschen auf	cmdb_running_process	listening_on	lsof
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	ifconfig, netstat
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig, netstat
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig, netstat
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig, netstat

Die LPAR-Discovery der AIX-Servermustererweiterung schlägt aufgrund eines Fehlers von „MISSING_DEPENDENCY“ fehl

Wenn das Gebietsschema des AIX-Servers ja_JP.UTF-8 ist, schlägt die LPAR-Discovery der AIX-Servermustererweiterung aufgrund eines Fehlers „MISSING_DEPENDENCY“ fehl und gibt die Suche auf Japanisch zurück. Um dieses Problem zu beheben, führen Sie die Schritte im aus LPAR-Discovery im AIX-Servermuster schlägt fehl mit MISSING_DEPENDENCY in Nutzlast, keine Beziehungen definiert für abhängige Klasse [cmdb_ci_lpar_instance], die allen Containment-/Hosting-Regeln entspricht: [cmdb_ci_lpar_instance >> virtualisiert von >> cmdb_ci_ibm_Frame] [KB0963418] artikel in Now Support Knowledge Base.

Apache-Erkennung von HBase-Instanzen

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von HBase auf einem UNIX-Server erkannt wird.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

In der folgenden Tabelle HBase-Instanz@ `Hostname` Die Quelle kann Informationen darüber enthalten, ob die Instanz eine primäre oder eine sekundäre Instanz ist. Der Name enthält `Hmaster` Wenn die Instanz eine primäre Instanz ist. Der Name einer Sekundärinstanz enthält `HRegionServer`.

Erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_db_hbase_instance	Name	HBase-Instanz@`Hostname`
Stammverzeichnis	cmdb_ci_db_hbase_instance	root_dir	hbase-site.xml
TCP-Port	cmdb_ci_db_hbase_instance	tcp_port	Laufender Prozess
Standort-XML	cmdb_ci_db_hbase_instance	site_xml	hbase-site.xml
Version	cmdb_ci_db_hbase_instance	Version	HBase-Shell
HBase-Homepage	cmdb_ci_db_hbase_instance	hbase_home	Laufender Prozess
ZooKeeper Quorum	cmdb_ci_db_hbase_instance	zookeeper	hbase-site.xml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von HP-UX

Discovery Identifiziert und klassifiziert Informationen zu HP-UX Computer.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
HP-UX (Unix-Klassifizierer)	• Probe „Horizontal Discovery“: Startet Muster • HP-UX - Installed Software^ • HP-UX - ADM^ • HP-UX - OS Patches* • HP-UX - CPU Speed* • HP-UX - Total Memory* • HP-UX - Hardware Model* • HP-UX - CPU Info* • HP-UX - Identity* • UNIX - Find FQDN* • UNIX - OS Filesystems* • UNIX - OS Uptime*	HP-UX Server

*Diese Probes sind in der Klassifizierung als nicht aktiv Discovery Verwendet standardmäßig Muster für diese Erkennungen.

^diese Probes bleiben standardmäßig aktiv, auch wenn Discovery Verwendet Muster-Discovery.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_hpux_server	os	uname
Kurzbeschreibung	cmdb_ci_hpux_server	short_description	uname
Name	cmdb_ci_hpux_server	Name	DNS, NBT
Hostname	cmdb_ci_hpux_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_hpux_server	dns_domain	DNS
Startdatum	cmdb_ci_hpux_server	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	dmidecode
Seriennummer	cmdb_ci_hpux_server	serial_number	uname
CPU-Typ	cmdb_ci_hpux_server	cpu_type	cpuinfo
CPU-Geschwindigkeit (MHz)	cmdb_ci_hpux_server	cpu_speed	adb
CPU-Anzahl	cmdb_ci_hpux_server	cpu_count	cpuinfo
Modell-ID	cmdb_ci_hpux_server	model_id	Modell
RAM (MB)	cmdb_ci_hpux_server	ram	adb
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	swlist
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	hifconfig
IP-Adresse	cmdb_ci_network_adapter	ip_address	hifconfig
MAC-Adresse	cmdb_ci_network_adapter	mac_address	hifconfig
Netzmaske	cmdb_ci_network_adapter	netmask	hifconfig

Erkennung von Hyper-V

Die ServiceNow Discovery Anwendungsfunde Microsoft Hyper-V-Hypervisoren in Ihrer Umgebung.

Hyper-V ist ein von entwickelter Hypervisor Microsoft Damit können Sie virtuelle Computer (VMs) auf einem physischen Server oder Computer erstellen und verwalten. Sie ermöglicht die Hardwarevirtualisierung, sodass mehrere virtuelle Computer auf einem einzigen physischen Computer ausgeführt werden können und gleichzeitig die zugrunde liegenden Hardwareressourcen wie CPU, Arbeitsspeicher, Speicher und Netzwerk gemeinsam genutzt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Hyper-V unterstützt die folgende Funktionalität:

- Failoverclustering: Failover wird mit dem Failovercluster-Manager verwaltet.
- Live-Migration: Virtuelle Computer können zwischen Failovercluster-Knoten verschoben werden, ohne den virtuellen Computer herunterzufahren.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Unterstützte Versionen

Discovery wird für folgende Versionen von Hyper-V Server unterstützt:

- 2008
- 2012
- 2012 R2
- 2016
- 2019

Wichtig: Discovery von Hyper-V, die auf ausgeführt wird Windows2016 wird für Muster unterstützt *Nur* . Wenn Sie ein Upgrade durchgeführt haben und noch Probes und Sensoren für Discovery verwenden, finden Sie unter KB0694773 Anweisungen zum Konfigurieren von Hyper-V-Probes.

Hyper-V-Datenmodelle

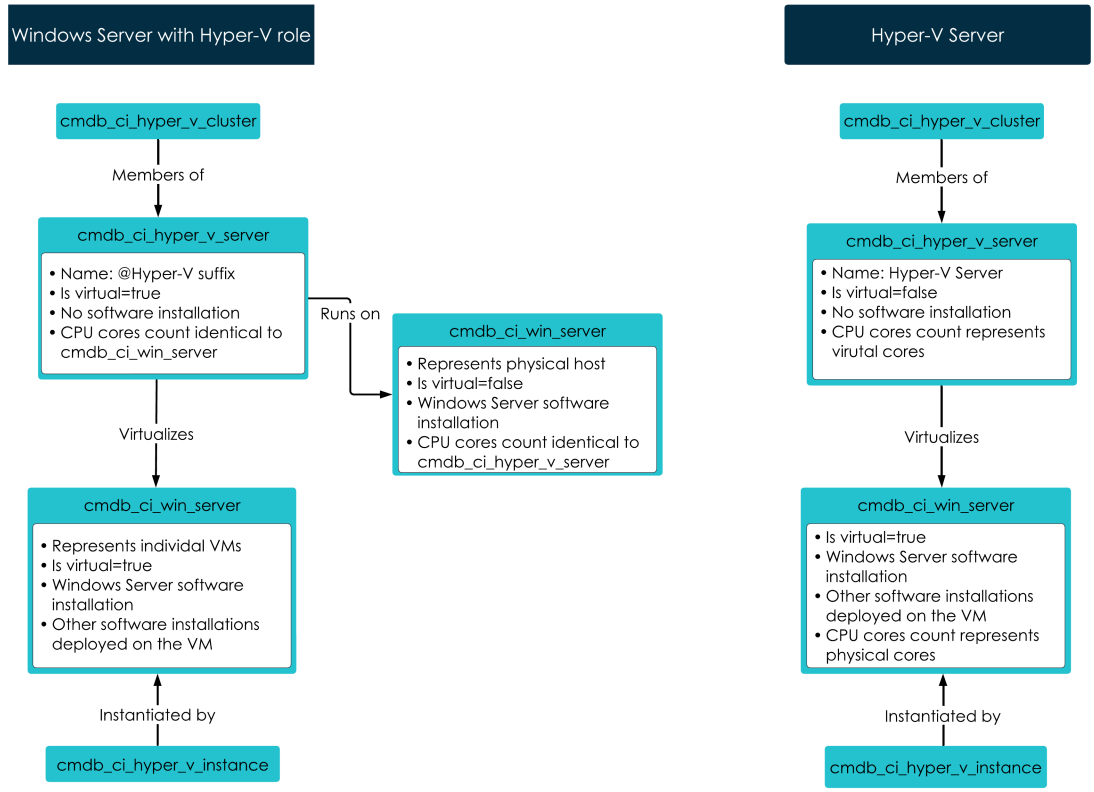
Es gibt 2 Arten von Hyper-V:

- Hyper-V ein Windows Server: Dieses Modell, das als Serverrolle auf installiert ist Windows Server ist für Unternehmen konzipiert, die sowohl Virtualisierungs- als auch andere Serverrollen (z. B. Dateiserver, Active Directory, Webserver) auf demselben Computer benötigen.
- Hyper-V-Server (Standalone): Eine kostenlose, schlanke Version von Windows Server speziell für Virtualisierung entwickelt. Es enthält nur den Hyper-V-Hypervisor und keine grafische Anwenderoberfläche (GUI) oder zusätzliche Serverrollen.

Discovery Unterstützt die Identifizierung und Zuordnung beider Typen von Hyper-V-Umgebungen. Jedoch ist CMDB Datenmodelle unterscheiden sich zwischen den beiden Bereitstellungstypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Windows Server mit Hyper-V-Rolle vs.. Hyper-V-Server (VM mit angezeigt Windows BETRIEBSSYSTEM)



Vergleich zwischen Windows Server mit Hyper-V-Rolle und Hyper-V-Server

Wichtige Aspekte	Windows Server mit Hyper-V-Rolle	Hyper-V-Server
Hyper-V-Server-CI	• Der Name des CI enthält **@Hyper-V-Server** Suffix. Beispiel: Hyperv1@Hyper-V Server. • Die **Windows-Host** Feld verweist auf die übergeordnete Windows-Servertabelle, die den physischen Host des Hyper-V-Servers darstellt.	Der Name des CI ist Hyper-V-Server.
Hyper-V-Cluster hat **Mitglieder::Mitglied von** Beziehung zum Hyper-V-Server	Ja Die Hyper-V-Servertabelle: • Hat **Ist virtuell** Feld auf „wahr“ festgelegt • Hat keine Softwareinstallation	Ja Die Hyper-V-Servertabelle: • Hat **Ist virtuell** Feld auf „falsch“ festgelegt • Hat keine Softwareinstallation
Hyper-V-Server hat **Wird ausgeführt am::Runs**	Ja Die Windows Server-Tabelle:	Nein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich zwischen Windows Server mit Hyper-V-Rolle und Hyper-V-Server (Fortsetzung)

Wichtige Aspekte	Windows Server mit Hyper-V-Rolle	Hyper-V-Server
Beziehung zu Windows Server	• Stellt den physischen Host dar • Hat **Ist virtuell** Feld auf „falsch“ festgelegt • Hat Windows Serversoftwareinstallation	
Das auf der VM installierte Betriebssystem (OS) hat **Virtualisiert von::virtualisiert** Beziehung zum Hyper-V-Server	Ja Die BS-Tabelle (z. B. Windows Server/Linux Server): • Stellt die einzelnen virtuellen Computer (VMs) dar • Hat **Ist virtuell** Feld auf „wahr“ festgelegt • Hat eine Installation der BS-Software, z. B. Windows Oder Linux Server • Hat andere Softwareinstallationen auf der VM bereitgestellt	Ja Die BS-Tabelle (z. B. Windows Server/Linux Server): • Hat **Ist virtuell** Feld auf „wahr“ festgelegt • Hat eine Installation der BS-Software, z. B. Windows Oder Linux Server • Hat andere Softwareinstallationen auf der VM bereitgestellt
Das auf der VM installierte Betriebssystem hat **Instanziiert::instanziiert von** Beziehung zur Hyper-V-VM-Instanz	Ja	Ja
Anzahl der CPU-Kerne	Ist zwischen den physischen identisch Windows Serverhost und Hyper-V-Server	Die Tabelle „übergeordnete Windows-Server“ spiegelt die physischen Kerne wider, während die Tabelle „Hyper-V-Server“ die virtuellen Kerne anzeigt

Anmeldeinformationen

Konfigurieren Windows-Anmeldeinformationen Mit Domänenadministratorrechten. Sie sollten auch Aktivieren Sie PowerShell Für MID-Server Wird verwendet, um Hyper-V-Server und -Instanzen zu erkennen.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Hyper-V-Server Die Klassifizierung gilt nur für eigenständige Hyper-V-Server (Server, die NICHT	• Probe „Horizontal Discovery“: Startet Muster • Windows - ADM^ • Windows - Installed Software^	Hyper-V-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierung	Probes	Muster
unter Windows 2008 ausgeführt werden).	• Hyper-V - Cluster* • Hyper-V - Resource Pools* • Hyper-V - Virtual Machines* • Hyper-V - Virtual Networks* • Mehrere andere Windows-Probes werden ebenfalls ausgeführt, zum Beispiel „Windows - Identity“ und „Windows - Software“.*	

*Diese Probes sind in der Klassifizierung als nicht aktiv Discovery Verwendet standardmäßig Muster für diese Erkennungen.

^diese Probes bleiben standardmäßig aktiv, auch wenn Discovery Verwendet Muster-Discovery.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Virtuelle Instanzen

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Objekt-ID ^	object_id	ID	cmdb_ci_hyper_v_instance
Name^	Name	Name	cmdb_ci_hyper_v_instance
Status	state	• An • Aus	cmdb_ci_Hyper_V_instance*
CPUs	CPUs	Anzahl	cmdb_ci_Hyper_V_instance*
Arbeitsspeicher	memory	Menge in MB	cmdb_ci_Hyper_V_instance*
Netzwerkadapter	nics	Anzahl	cmdb_ci_Hyper_V_instance*
Datenträger	disks	Anzahl+	cmdb_ci_Hyper_V_instance*
Datenträgergröße	disks_size	Kapazität in GB+	cmdb_ci_Hyper_V_instance*
Seriennummer virtuelle Hauptplatine	baseboard_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuelle Instanzen (Fortsetzung)

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
BIOS-Seriennummer	bios_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance
Gehäuse-Seriennummer	chassis_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance
BIOS-GUID	bios_guid	Global eindeutiger Bezeichner (GUID)	cmdb_ci_hyper_v_instance

*Attribute, die der Tabelle cmdb_ci_hyper_v_instance hinzugefügt werden, wenn das Muster „Hyper-V Server“ verwendet wird. Für Upgrades fügen Probes und Sensoren diese Attribute weiterhin der Tabelle cmdb_ci_vm_instance hinzu.

^Neu erkanntes Attribut bei Verwendung des Musters Hyper-V Server.

+Discovery kann diese Informationen nur zurückgeben, wenn die virtuelle Maschine ausgeführt wird.

Virtuelle Server

Bezeichnung	Feld	Gespeichert in Tabelle
Name	Name	cmdb_ci_hyper_v_server
Gehäusetyp	chassis_type	cmdb_ci_hyper_v_server
Beschreibung	short_description	cmdb_ci_hyper_v_server
OS-Adressbreite (Bit)	os_address_width	cmdb_ci_hyper_v_server
Betriebssystem	BS	cmdb_ci_hyper_v_server
Host-Name	hostname	cmdb_ci_hyper_v_server
IP-Adresse	ip_address	cmdb_ci_hyper_v_server
BS-Version	os_version	cmdb_ci_hyper_v_server
BS-Service Pack	os_service_pack	cmdb_ci_hyper_v_server
Ist virtuell	virtual	cmdb_ci_hyper_v_server

Virtuelle Netzwerke

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Name	Name	Name des virtuellen Netzwerks	cmdb_ci_Hyper_V_Network *
ID	object_id	Global eindeutiger Bezeichner (GUID)	cmdb_ci_Hyper_V_Network *

*Attribute, die zur Tabelle cmdb_ci_hyper_v_network hinzugefügt werden, wenn das Muster „Hyper-V Server“ verwendet wird. Für Upgrades fügen Probes und Sensoren diese Attribute weiterhin den Tabellen cmdb_ci (name) und cmdb_ci_vm_object (object_id) hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenpools

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Name^	Name	Name des Ressourcenpools	cmdb_ci_hyper_v_resource_pool
ID	object_id	Global eindeutiger Bezeichner (GUID)	cmdb_ci_hyper_v_rpool_comp
Kapazität	Kapazität	Maximaler Betrag der entsprechenden Zuteilungseinheit	cmdb_ci_hyper_v_rpool_comp
Zuordnungseinheiten	allocation_units	Verwendete Maßeinheiten (zum Beispiel MB oder GB)	cmdb_ci_hyper_v_rpool_comp
Ressourcentyp	resource_type	Typ der erkannten Ressource (zum Beispiel Arbeitsspeicher oder Festplattenspeicher)	cmdb_ci_hyper_v_rpool_comp

Cluster

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle	Referenztabelle
Windows-Cluster	Name	Referenzfeld, in dem das Windows-Cluster angezeigt wird, in dem sich das Hyper-V-Cluster befindet	cmdb_ci_hyper_v_cluster	cmdb_ci_win_cluster

Beziehungen

Discovery Erstellt Datensätze in CMDB Für den Hostcomputer die übergeordnete Partition, die Windows Server 2008 ausführt, und alle virtuellen Computer, die auf dem Hyper-V-Server ausgeführt werden. Discovery Sucht die gespeicherten Vorlagen und ordnet alle Beziehungen zwischen Komponenten zu.

Die Instanz ändert die folgenden Tabellen, damit sie für mehrere Virtualisierungsprodukte verwendet werden können:

Tabelle	Zweck
Virtualisierungsserver [cmdb_ci_virtualization_server]	Enthält Daten über alle erkannte Virtualisierungsserver
VM-Instanz [cmdb_ci_vm_instance]	Enthält Daten über alle erkannte Instanzen virtueller Computer
VM-Objekt [cmdb_ci_vm_object]	Enthält Daten über verschiedene Objekte, die einem Hyper-V-Server zugeordnet sind, zum Beispiel Partitionen, Netzwerke, Ressourcenpools und Cluster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnete Tabelle	Beziehung	Untergeordnete Tabelle
Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]	Registriert auf::Hat sich registriert	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]	Verbunden von::Verbindet	Hyper-V-Netzwerk [cmdb_ci_hyper_v_network]
Hyper-V-Netzwerk [cmdb_ci_hyper_v_network]	Bereitgestellt::Stellt bereit	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]	Definiert Ressourcen für:Erhält Ressourcen von	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Ressourcenpoolkomponenten [cmdb_ci_hyper_v_resource_pool]	Enthalten in::Enthält	Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]
Hyper-V-Cluster [cmdb_ci_hyper_v_cluster]	Mitglieder::Mitglied von	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Server [cmdb_ci_hyper_v_server]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]
Windows-Server [cmdb_ci_win_server]	Instanziiert::Instanziiert von	Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]
Windows-Server [cmdb_ci_win_server]	Virtualisiert von::Virtualisiert	Hyper-V-Server [cmdb_ci_hyper_v_server]

Virtuelle Hyper-V-Computer klonen

Stellen Sie beim Importieren (Klonen) von virtuellen Hyper-V-Computern sicher, dass jeder virtuelle Computer eine eindeutige ID aufweist. Discovery identifiziert virtuelle Computer mit identischen IDs als denselben Computer.

1. Exportieren Sie den virtuellen Computer vom Hyper-V-Server.
2. Importieren Sie den virtuellen Computer auf einen anderen Server, und wählen Sie eine der folgenden Optionen aus:
   - Move or restore the virtual machine (Virtuellen Computer verschieben oder wiederherstellen): Bei Auswahl dieser Option wird das Image mit derselben ID geklont und auf einen anderen Server verschoben. Das Original-Image bleibt auf dem Hyper-V-Server.
   - Copy the virtual machine (Virtuellen Computer kopieren): Bei Auswahl dieser Option wird der virtuelle Computer mit einer anderen ID kopiert und vom Hyper-V-Server verschoben. Das ist die beste Auswahl. Sie erfordert vor Ausführung von Discovery keine weitere Aktion.
3. Wenn Sie den Hyper-V-Klon mit der Option zum **Verschieben oder Wiederherstellen** importieren, müssen Sie das Original-Image vom Hyper-V-Server löschen.

   Wenn Discovery auf zwei virtuelle Computer mit denselben äquivalenten Seriennummern trifft, wird nur ein Konfigurationselement (CI) erstellt.

Erkennung von Red Hat JBoss-Servern

Discovery kann JBoss-Anwendungsserver erkennen, die unter Linux und Windows ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anforderungen

Für JBoss-Anwendungsserver, die unter Linux ausgeführt werden:

- Legen Sie Probe-Berechtigungen zur Verwendung der folgenden Befehle der Bourne-Shell fest: *find*, *cat* und *dirname*.
- Aktivieren Sie SSH auf dem JBoss-Anwendungsserver. Die SSH-Anmeldeinformationen müssen auch Leseberechtigungen für die Dateien web.xml und jboss-service.xml beinhalten.

Aktivieren Sie für JBoss-Anwendungsserver, die unter Windows ausgeführt werden, PowerShell auf dem MID Server.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
JBoss-Server	• Horizontal Pattern: Startet Muster • Windows - JBoss Find web.xml List* • Windows - JBoss Get jboss-service.xml* • JBoss - Find web.xml List* • JBoss - Get jboss-service.xml*	JBoss

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Daten

Discovery füllt in der JBoss-Tabelle [cmdb_ci_app_server_jboss] die folgenden Felder:

Bezeichnung	Feldname
Name	Name
Kategorie	Kategorie
Version	Version
TCP-Port(s)	tcp_port

Discovery füllt in den Servertabellen für Webservices [cmdb_ci_web_service] und Webanwendungen [cmdb_ci_web_application] die folgenden Felder:

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_web_service	Name	jboss-service.xml
App-Server	cmdb_ci_web_service	app_server	Interne Referenz
Beschreibung	cmdb_ci_web_application	short_description	web.xml
Name	cmdb_ci_web_application	Name	web.xml
Dokumentenbasis	cmdb_ci_web_application	document_base	web.xml
App-Server	cmdb_ci_web_application	app_server	web.xml
Servlet-Name*	cmdb_ci_web_application	servlet_name	web.xml
Servlet-Klasse*	cmdb_ci_web_application	servlet_class	web.xml

*Nur Windows-Server

Beziehungen

Erstellte Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_web_service	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server
cmdb_ci_app_server_jboss	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_app_server_jboss	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_web_application
cmdb_ci_app_server_jboss	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_web_service

Veraltet: JBoss-Probes und -Sensoren

Discovery identifiziert einen Linux JBoss-Anwendungsserver mithilfe von Probes und Sensoren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Muster JBoss.

1. Die Probe „UNIX - Active Processes“ erkennt einen laufenden Prozess, der dem Einstiegspunktparameter *org.jboss.main* entspricht.
2. Bei einer Übereinstimmung wird in der Tabelle „JBoss-Anwendungsserver“ [cmdb_ci_App_Server_jboss] ein Datensatz erstellt. Die folgenden Sonden werden ebenfalls aktiviert:
   - JBoss - Find web.xml list: Der Sensor dieses Tests füllt gegebenenfalls Informationen in die Tabelle der Webanwendung [cmdb_ci_web_application].
   - JBoss - jboss-service.xml abrufen: Der Sensor dieses Tests füllt die Informationen in der Tabelle "Web Service [cmdb_ci_web_service]" auf.
3. Der JBoss - Find web.xml Listentest sucht nach dem web.xml-Dateien des JBoss-Anwendungsservers. Von der Probe wird der Parameter *classpath* im ausgeführten Prozess verwendet. Dann wird im zugehörigen Verzeichnis server\default\deploy nach der JBoss-Installation gesucht.
4. Wenn sich zugehörige Webanwendungen im Verzeichnis server\default\deploy befinden, wird die Sonde JBoss - Get web.xml für jede Anwendung ausgelöst. Diese Sonde liest die web.xml-Datei für jede Webanwendung und der Sensor füllt zusätzliche Informationen in die Tabelle Web Service [cmdb_ci_web_service].
5. Von der Probe „Boss - Get jboss-service.xml“ wird der Parameter *classpath* im ausgeführten Prozess zum Suchen nach der jboss-service.xml -Datei im zugehörigen Verzeichnis server\default\conf\ für die JBoss-Installation verwendet.
6. Wenn die Sonde die Datei jboss-service.xml im Verzeichnis server\default\conf\ gefunden hat, liest der Sensor den Inhalt der XML-Datei. Anschließend erstellt er bei Bedarf zusätzliche Datensätze in der Tabelle Web Service [cmdb_ci_web_service].

Windows

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Muster JBoss.

1. Die Probe „Windows - Active Processes“ erkennt einen laufenden Prozess, der dem Einstiegspunktparameter *org.jboss.main* entspricht.
2. Bei einer Übereinstimmung wird in der Tabelle „JBoss-Anwendungsserver“ [cmdb_ci_App_Server_jboss] ein Datensatz erstellt. Die folgenden Sonden werden ebenfalls aktiviert:
   - JBoss - Find web.xml list: Der Sensor dieses Tests füllt gegebenenfalls Informationen in die Tabelle der Webanwendung [cmdb_ci_web_application].
   - JBoss - jboss-service.xml abrufen: Der Sensor dieses Tests füllt die Informationen in der Tabelle "Web Service [cmdb_ci_web_service]" auf.
3. Der JBoss - Find web.xml Listentest sucht nach dem web.xml-Dateien des JBoss-Anwendungsservers. Von der Probe wird der Parameter *classpath* im ausgeführten Prozess verwendet. Dann wird im zugehörigen Verzeichnis server\default\deploy nach der JBoss-Installation gesucht.
4. Wenn sich zugehörige Webanwendungen im Verzeichnis server\default\deploy befinden, wird die Sonde JBoss - Get web.xml für jede Anwendung ausgelöst. Diese Sonde liest die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

web.xml-Datei für jede Webanwendung und der Sensor füllt zusätzliche Informationen in die Tabelle Web Service [cmdb_ci_web_service].

5. Von der Probe „Boss - Get jboss-service.xml“ wird der Parameter `classpath` im ausgeführten Prozess zum Suchen nach der jboss-service.xml -Datei im zugehörigen Verzeichnis server\default\conf\ für die JBoss-Installation verwendet.
6. Wenn die Sonde die Datei jboss-service.xml im Verzeichnis server\default\conf\ gefunden hat, liest der Sensor den Inhalt der XML-Datei. Anschließend erstellt er bei Bedarf zusätzliche Datensätze in der Tabelle Web Service [cmdb_ci_web_service].

Linux Discovery

Discovery Und Service-Mapping Anwendungen verwenden Probes und Muster, um Informationen zu erkennen und zuzuordnen Linux Computer und Server. Die Informationen werden in ausgefüllt CMDB. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Supportability-Details

Die Linux Das Servermuster kann nur auf Englisch erkennen Linux.

Unterstützt Linux Betriebssysteme

Für IPv4-Erkennung:

- Red Hat
- Oracle
- Fedora
- Debian
- SUSE
- CentOS
- Ubuntu

Für IPv6-Erkennung:

- CentOS 7
- Ubuntu 20

Die folgenden Betriebssysteme oder Geräte wurden nicht für die IPv6-Discovery verifiziert:

- Red Hat-Cluster
- Oracle Clusterware
- Linux Pacemaker-Cluster
- Netzwerkspeicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Linux (UNIX-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • Linux - Installed Software^ • Unix - ADM^ • Linux - Identity* • Linux - CPU* • Linux - Distribution* • Linux - Find FQDN* • Linux - Memory* • Linux - Memory Modules* • Linux - Network ARP Tables* • Linux - Storage* • Linux - Amazon EC2* • Unix - OS Uptime* • UNIX - OS Filesystems* • UNIX - Find FQDN* • Unix - ADM Enhanced*	Linux Server

*Diese Probes sind in der Klassifizierung als nicht aktiv Discovery Verwendet standardmäßig Muster für diese Erkennungen.

^diese Probes bleiben standardmäßig aktiv, auch wenn Discovery Verwendet Muster-Discovery.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Anforderungen für Linux Discovery

Bevor Sie eine Discovery ausführen, müssen Sie sicherstellen, dass alle erforderlichen Konfigurationen abgeschlossen sind.

Überprüfen Sie die Installation und Aktivierung der Plugins

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Muster für Discovery und Service-Mapping installieren
- Visibility Content installieren

Überprüfen Sie die Konfiguration der erforderlichen Anmeldeinformationen

Konfigurieren Sie die Anmeldeinformationen anhand der erforderlichen SSH-Berechtigungen. Erkennung von sensiblen Elementen Linux Für Daten ist möglicherweise ein Anwender mit entsprechenden sudo-Berechtigungen erforderlich, um die sudu-Befehle auszuführen. Weitere Informationen zu den Befehlen, die einen Anwender mit erhöhten Rechten erfordern, finden Sie in den folgenden Dokumenten.

- Befehle, die Stammberechtigungen für Discovery, Orchestration und Integration Hub erfordern .
- Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.
- Zeigen Sie Befehle an, die in der musterbasierten Discovery verwendet werden
- Validiert Befehle, die in der musterbasierten Discovery verwendet werden

Anmeldeinformationen für privaten SSH-Schlüssel sind aus Sicherheitsgründen den Anmeldeinformationen für SSH-Passwörter vorzuziehen.

Verifizieren Sie MID-Server Konfiguration

Detaillierte Informationen finden Sie unter:

- Testen Sie die MID-Server-Konnektivität
- MID Server-Eigenschaften

Überprüfen Sie die Konfiguration des Discovery-Zeitplans

Informationen zum Erstellen eines Discovery-Zeitplans finden Sie unter Horizontale Erkennung planen.

Durch das Definieren von IP-Bereichen wird sichergestellt, dass während nur die angegebenen Netzwerkadapter und ihre primären IP-Adressen verwendet werden Linux Discovery. Sie können konfigurieren **Schnellbereiche** Durch Eingabe von kommagetrennten IPv4-Adressbereichen oder einer einzelnen IPv6-Adresse.

Alternativ können Sie verwenden *network_adapter_exclusion_list*Zu begrenzende Eigenschaft Linux Discovery für bestimmte Netzwerkadapter und ihre primären IP-Adressen. Weitere Informationen finden Sie unter Sekundäre IP-Adressen des Netzwerkadapters in auslassen Linux Discovery.

Erfasste Daten

Die LinuxDer Klassifizierer löst Probes aus, die die Discovery durchführen. Während der Discovery werden mehrere Probes gestartet. Eine Liste der ausgelösten Probes finden Sie unter dem Klassifizierer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_linux_server	os	uname -a
BS-Version	cmdb_ci_computer	os_version	uname -a or cat /etc/*release
Kurzbeschreibung	cmdb_ci_linux_server	short_description	uname -a
Name	cmdb_ci_linux_server	Name	DNS, NBT
Hostname	cmdb_ci_linux_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_linux_server	dns_domain	DNS
Startdatum	cmdb_ci_linux_server	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	dmidecode
Seriennummer	cmdb_ci_computer	serial_number	dmidecode
CPU-Typ	cmdb_ci_linux_server	cpu_type	/proc/cpuinfo
CPU-Geschwindigkeit (MHz)	cmdb_ci_linux_server	cpu_speed	/proc/cpuinfo
CPU-Anzahl	cmdb_ci_linux_server	cpu_count	/proc/cpuinfo
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count	/proc/cpuinfo
CPU-Kern-Thread	cmdb_ci_computer	cpu_core_thread	/proc/cpuinfo
CPU-Hersteller	cmdb_ci_linux_server	cpu_manufacturer	/proc/cpuinfo
Modellnummer	cmdb_ci_computer	model_number	dmidecode
Modell-ID	cmdb_ci_computer	model_id	dmidecode
RAM (MB)	cmdb_ci_linux_server	ram	meminfo
Festplattenspeicher (GB)*	cmdb_ci_linux_server	disk_space	/proc/ide, /proc/scsi, /var/log/dmesg
Typ	cmdb_ci_disk	Typ	/proc/ide, /proc/scsi, /var/log/dmesg
Modell-ID	cmdb_ci_disk	model_id	/proc/ide, /proc/scsi, /var/log/dmesg
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	/proc/ide, /proc/scsi, /var/log/dmesg
Name	cmdb_ci_disk	Name	/proc/ide, /proc/scsi, /var/log/dmesg
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Freier Speicherplatz in Byte (MB)	cmdb_ci_file_system	free_space_bytes	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	ifconfig oder ip address show
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig oder ip address show
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig oder ip address show
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig oder ip address show
Standard-Gateway	cmdb_ci_hardware	default_gateway	route

* Der Wert im Feld **disk_space** ist eine Zusammenfassung der Gesamtkapazität (einschließlich belegtem Platz) für alle nicht entnehmbaren Festplatten, einschließlich Direct Attached Storage und SAN-Speicher.

Hinweis: Stellen Sie sicher, dass Sie eindeutige Seriennummern für die RAMs im definieren Linux Server.

Discovery Identifiziert und klassifiziert auch Informationen zu Linux KVM. Discovery Identifiziert Linux Kernel-basierte virtuelle Maschinen (KVM), wenn der Prozessklassifizierer erkennt `Libvirtd` Wird auf ausgeführt Linux Server. Die Klassifizierung löst die Erstellung eines cmdb_ci_kvm-Datensatzes aus und startet die SSH-Befehlsprobes, um zu erkunden Linux Server mit `Virsh` , `Lbvert` Dienstprogramm und Konfigurationsdaten der virtuellen Maschine.

Discovery Erstellt einen [cmdb_ci_kvm_instance]-Datensatz für jede virtuelle Maschine auf dem Server und gleicht dann den [cmdb_ci_kvm_instance]-Datensatz mit einem entsprechenden [cmdb_ci_Computer]-Datensatz ab, wobei die MAC-Adressen der installierten Netzwerkadapter verwendet werden.

Von verwendete Tabellen Discovery Ein Linux KVM

Tabellenname	Erweitert	Beschreibung	Quelle
cmdb_ci_kvm	cmdb_ci_vm	Ein Hypervisor, der Kernel-basierte virtuelle Computer (KVMs) verwaltet	Prozessklassifizierer erkennt libvirtd, das auf Linux-Servern ausgeführt wird
cmdb_ci_kvm_vm_instance	cmdb_ci_vm_instance	Eine VM-Instanz für diesen Hypervisor	Virsh list-all- und dumpxml-Befehl
cmdb_ci_kvm_object	cmdb_ci_vm_object	Ein Objekt, das mit einer VM-Instanz verbunden ist	Elemente <network> , <storage pool> und <storage volume> des dumpxml-Befehls
cmdb_kvm_device	Nicht zutreffend	Ein Gerät, das mit einer VM-Instanz verbunden ist	Element <devices> des dumpxml-Befehls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erfasst von Discovery Ein Linux KVM

Bezeichnung	Tabellenname	Feldname	Quelle
Linux-Host	cmdb_ci_kvm	linux_host	Verweis auf den cmdb_ci_linux_server, auf dem diese VM ausgeführt wird
Details	cmdb_ci_kvm	details_xml	dumpxml
Objekt-ID	cmdb_ci_kvm_vm_instance	object_id	virsh dumpxml
Status	cmdb_ci_kvm_vm_instance	Status	Virsh-Liste – alle
CPUs	cmdb_ci_kvm_vm_instance	CPUs	virsh dumpxml
Arbeitsspeicher	cmdb_ci_kvm_vm_instance	memory	virsh dumpxml
Datenträger	cmdb_ci_kvm_vm_instance	disks	virsh dumpxml
Datenträgergröße	cmdb_ci_kvm_vm_instance	disks_size	virsh domblkinfo
Netzwerkadapter	cmdb_ci_kvm_vm_instance	nics	virsh dumpxml
Name	cmdb_ci_kvm_vm_instance	Name	virsh dumpxml
Kurzbeschreibung	cmdb_ci_kvm_vm_instance	short_description	virsh desc
Details	cmdb_ci_kvm_object	details_xml	XML-Element aus dumpxml
KVM-Instanz	cmdb_kvm_device	kvm_instance	Verweis auf cmdb_ci_kvm_instance
Gerät	cmdb_kvm_device	Gerät	Datenträger, Controller, Schnittstelle usw.
Typ	cmdb_kvm_device	type	Abhängig vom Gerät
Details	cmdb_kvm_device	details_xml	XML-Element aus dumpxml

Von Discovery über die KVM-Beziehung erfasste Daten

Beziehung	Übergeordnete Tabelle	Untergeordnete Tabelle
Registriert auf::Hat sich registriert	KVM [cmdb_ci_kvm]	KVM-VM-Instanz [cmdb_ci_kvm_vm_instance]
Bereitgestellt von::Stellt bereit	KVM [cmdb_ci_kvm]	Netzwerk [cmdb_ci_kvm_network]
Definiert Ressourcen für:Erhält Ressourcen von	KVM [cmdb_ci_kvm]	Speicherpool [cmdb_ci_kvm_storage_pool]
Verbunden von::Verbindet	KVM-VM-Instanz [cmdb_ci_kvm_vm_instance]	Netzwerk [cmdb_ci_kvm_network]
Instanziiert von::Instanziiert	KVM-VM-Instanz [cmdb_ci_kvm_vm_instance]	Computer [cmdb_ci_computer]
Virtualisiert von::Virtualisiert	Computer [cmdb_ci_computer]	KVM [cmdb_ci_kvm]
Stellt Speicher bereit für::Gespeichert auf	Speicherpool [cmdb_ci_kvm_storage_pool]	KVM-VM-Instanz [cmdb_ci_kvm_vm_instance]

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support

- https://support.servicenow.com/now
- Known Error-Portal
- KB1425502Linux-Discovery schlägt fehl mit „Verbindung kann nicht hergestellt werden, Status ist SSH_CONNECTION_FAILURE. Signaturalgorithmus-Client (KB1425502) konnte nicht vereinbart werden
- Grundlegende Details werden nicht in CMDB für Linux Server Discovery (KB1199574) ausgefüllt.
- Linux-Discovery schlägt in Unix-Klassifizierung mit dem Fehler fehl – Name des nicht klassifizierten CI ist „Servername“ (KB0860486)
- Linux-Discovery-Fehler „rbash: PFAD: Schreibgeschützte Variable Exit-Status: 1“ (KB0866860)

Linux Red hat-Cluster-Discovery

Discovery kann finden Linux Red hat-Cluster, die Hochverfügbarkeit und Lastenausgleich bieten.

Erforderliche Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Zusätzliche Anforderungen

Sie benötigen außerdem Berechtigungen zum Lesen des Verzeichnisses `/etc/hosts/` und der Datei `/etc/cluster/cluster.conf`, die Hostnamen mit IP-Adressen verknüpft.

Die folgenden Befehle werden für Oracle-Clusterware ausgeführt:

Befehl
`ps -ef | grep korosync | grep -V grep`
`clustat -x`
`ifconfig | grep 'inet addr:' |awk '{print $1, $2 }'`
`hostname -s`
`hostname -s`

Sudo-Berechtigung zur Ausführung: `sudo /u01/app/12.1.0.2/grid/bin/ocrcheck \| egrep -v 'error\|return code'`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Linux (UNIX-Klassifizierung)	Probe „Horizontal Discovery“: Startet Muster	Die folgenden Muster stellen eine Erweiterung des Musters Linux Server dar: • UNIX-Cluster – Linux Red Hat-Cluster • Linux – Red Hat-Cluster Das Muster verwendet den Befehl `clustat -x` und untersucht die folgende Clusterkonfigurationsdatei: `/etc/cluster/cluster.conf`

Erfasste Daten

Tabelle	Bezeichnungen und Feldnamen
Unix-Cluster [cmdb_ci_unix_cluster]	Name [name] Clusterstatus [cluster_status] Clustertyp [cluster_type] IP-Adresse [ip_address] Cluster-ID [cluster_id] Clusterversion [cluster_version]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Name [name] Knotenzustand [node_state] IP-Adresse [ip_address] Knotenstatus [node_status]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Name [name] Ressourcentyp [resource_type] Ressourcenstatus [resource_status] Eigenschaften [properties]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Name [name] IP-Adresse [ip_address]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Bezeichnungen und Feldnamen
	Cluster-ID [cluster_id]

Beziehungen

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Virtualisiert::Virtualisiert von	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet::Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet::Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Linux-Server [cmdb_ci_linux_server]

Sekundäre IP-Adressen des Netzwerkadapters in auslassen Linux Discovery

Grenzwert Linux Discovery für bestimmte Netzwerkadapter und ihre primären IP-Adressen, um die Leistung zu verbessern, indem sekundäre IP-Adressen ignoriert werden.

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren von *network_adapter_exclusion_list*Die Systemeigenschaft stellt sicher, dass während nur angegebene Netzwerkadapter und ihre primären IP-Adressen verwendet werden Linux Discovery. Sekundäre IP-Adressen, die nicht benannt sind, werden automatisch ausgelassen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. In **Name** Feld, suchen Sie nach Network_Adapter_Exclusion_list .
3. Wählen Sie die Eigenschaft *network_adapter_exclusion_list* aus.
4. In **Wert** Feld den Netzwerkadapter eingeben, der der NIC-IP-Adresse zugeordnet ist, um sie vom Löschen auszuschließen.

   Der Netzwerkadapter muss in einem der in der folgenden Tabelle aufgeführten Formate eingegeben werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Format	Beschreibung
Einzelner Name	Name des einzelnen Adapters. Beispiel: `Bond0` .
Regulärer Ausdruck, der mehreren Adapternamen entspricht	Regulärer Ausdruck, der mehreren Adapternamen entspricht, die mit einer oder mehreren Ziffern enden. Beispiel: `Bond\d+` .
Mehrere Adapternamen	Mehrere Adapternamen, getrennt durch Kommas, einschließlich regulärer Ausdrücke. Beispiel: `nic1,Bond\d+` .

5. Wählen Sie **Aktualisieren**.

Ergebnis

Wenn der vordefinierte Zeitplan auslöst Linux Server-Discovery oder eine geplante horizontale Discovery wird ausgeführt. Nur die spezifischen Netzwerkadapter und ihre primären IP-Adressen werden in den Discovery-Prozess einbezogen.

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Zugehörige Informationen

Linux Discovery

Netware-Erkennung

Discovery identifiziert und klassifiziert Informationen über Netware.

Erfasste Daten

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_netware_server	Name	snmp
Seriennummer	cmdb_ci_netware_server	serial_number	snmp
BS-Version	cmdb_ci_netware_server	os_version	snmp
RAM	cmdb_ci_netware_server	ram	snmp
CPU-Anzahl	cmdb_ci_netware_server	cpu_count	snmp

Mac-Discovery (OS/X)

Discovery identifiziert und klassifiziert Informationen über Mac (OS/X)-Computer.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Erfasste Daten

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
BS-Version	cmdb_ci_computer	os_version	system_profiler
BS-Service Pack	cmdb_ci_computer	os_service_pack	system_profiler
Kurzbeschreibung	cmdb_ci_computer	short_description	uname
Name	cmdb_ci_computer	Name	DNS, NBT
Hostname	cmdb_ci_computer	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_computer	dns_domain	DNS
Startdatum	cmdb_ci_computer	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	Vermutlich Apple
Seriennummer	cmdb_ci_computer	serial_number	system_profiler
CPU-Typ	cmdb_ci_computer	cpu_type	system_profiler
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	system_profiler
CPU-Anzahl	cmdb_ci_computer	cpu_count	system_profiler
Modell-ID	cmdb_ci_computer	model_id	system_profiler
RAM (MB)	cmdb_ci_computer	ram	system_profiler
Festplattenspeicher (GB)	cmdb_ci_computer	disk_space	system_profiler
Volume-Name	cmdb_ci_disk	volume_name	system_profiler
Volume-Seriennummer	cmdb_ci_disk	volume_serial_number	system_profiler
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	system_profiler
Name	cmdb_ci_disk	Name	system_profiler
Geräte-ID	cmdb_ci_disk	device_id	system_profiler
Freier Speicherplatz (GB)	cmdb_ci_disk	free_space	system_profiler
Dateisystem	cmdb_ci_disk	file_system	system_profiler
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Verbunden mit	cmdb_running_process	connects_to	lsof
Lauschen auf	cmdb_running_process	listening_on	lsof
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	system_profiler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
IP-Adresse	cmdb_ci_network_adapter	ip_address	system_profiler
MAC-Adresse	cmdb_ci_network_adapter	mac_address	system_profiler
Netzmaske	cmdb_ci_network_adapter	netmask	system_profiler
MAC-Hersteller	cmdb_ci_network_adapter	mac_mfr	Vermutlich Apple
DHCP-fähig	cmdb_ci_network_adapter	dhcp_enabled	system_profiler

Solaris-Erkennung

Discovery identifiziert und klassifiziert Informationen über Solaris-Computer.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Unterstützte Betriebssysteme

- Oracle Solaris 10
- Oracle Solaris 11

Voraussetzungen

Discovery speichert Daten in der Tabelle [cmdb_running_process] mit Befehlszeilenparametern, die auf maximal 80 Zeichen beschnitten sind. Das kann dazu führen, dass mehrere Anwendungen in einem CI zusammengeführt werden. Um die vollständige Befehlszeile zu erhalten und dieses Problem zu vermeiden, führen Sie `pargs -a` aus, und analysieren Sie das Ergebnis.

Damit Discovery Muster für die Suche nach Solaris-Computern verwendet, müssen Sie SNEEP installieren. Andernfalls kann Discovery die Seriennummer nicht finden.

Bei Verwendung von Solaris-Zonen muss jede Zone so konfiguriert werden, dass sie einen eindeutigen Wert für die Seriennummer zurückgibt. Andernfalls gibt jede Zone dieselbe Nummer zurück, wodurch Probleme bei der CI-Identifizierung entstehen.

Hinweis: Solaris-Discovery unterstützt nur lokale Zonen, die auf demselben Host wie die globale Zone installiert sind. Wenn die lokale Zone auf einem anderen Host als der globalen Zone installiert ist, wird `Zoneadm -Liste: cip` Befehl ruft die UUID für die lokale Zone nicht ab.

Die Probe „Solaris - ADM“ erfordert die Installation des LSQF-Befehls.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Anmeldeinformationen

Konfigurieren SSH-Anmeldeinformationen Für die Systeme, die Sie erkennen möchten.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Solaris (UNIX-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • Solaris - Installed Software^ • Solaris - Identity* • Solaris - CPU* • Solaris - Hardware Model* • Solaris - Memory* • Solaris - Network ARP Tables* • Solaris - OS Patches* • Solaris - Storage* • Solaris - Zones* • Solaris - Disks* • DNS*	Solaris-Server

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

^Diese Probe bleibt standardmäßig aktiv, selbst wenn Discovery die Mustererkennung verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
Kurzbeschreibung	cmdb_ci_solaris_server	short_description	uname
Name	cmdb_ci_solaris_server	Name	DNS, NBT
Hostname	cmdb_ci_solaris_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_solaris_server	dns_domain	DNS
Startdatum	cmdb_ci_solaris_server	start_date	uptime
CPU-Typ	cmdb_ci_computer	cpu_type	kstat
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	kstat
CPU-Anzahl	cmdb_ci_computer	cpu_count	kstat

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count	kstat
CPU-Kern-Thread	cmdb_ci_computer	cpu_core_thread	kstat
Modellnummer	cmdb_ci_solaris_server	model_number	suntype
Modell-ID	cmdb_ci_solaris_server	model_id	suntype
RAM (MB)	cmdb_ci_computer	ram	prtconf
Festplattenspeicher (GB)	cmdb_ci_solaris_server	disk_space	iostat
Seriennummer	cmdb_ci_solaris_server	serial_number	sneep *
Hersteller	cmdb_ci_disk	manufacturer	iostat
Modell-ID	cmdb_ci_disk	model_id	iostat
Volume-Seriennummer	cmdb_ci_disk	volume_serial_number	iostat
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	iostat
Name	cmdb_ci_disk	Name	iostat
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	showrev
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Verbunden mit	cmdb_running_process	connects_to	lsof
Lauschen auf	cmdb_running_process	listening_on	lsof
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	ifconfig
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig
Standard-Gateway	cmdb_ci_hardware	default_gateway	netstat

* Zum Erkennen von Fujitsu PRIMEPOWER-Geräten müssen Sie Oracle SNEEP installieren und die Solaris-Erkennung mit Root-Anmeldeinformationen ausführen.

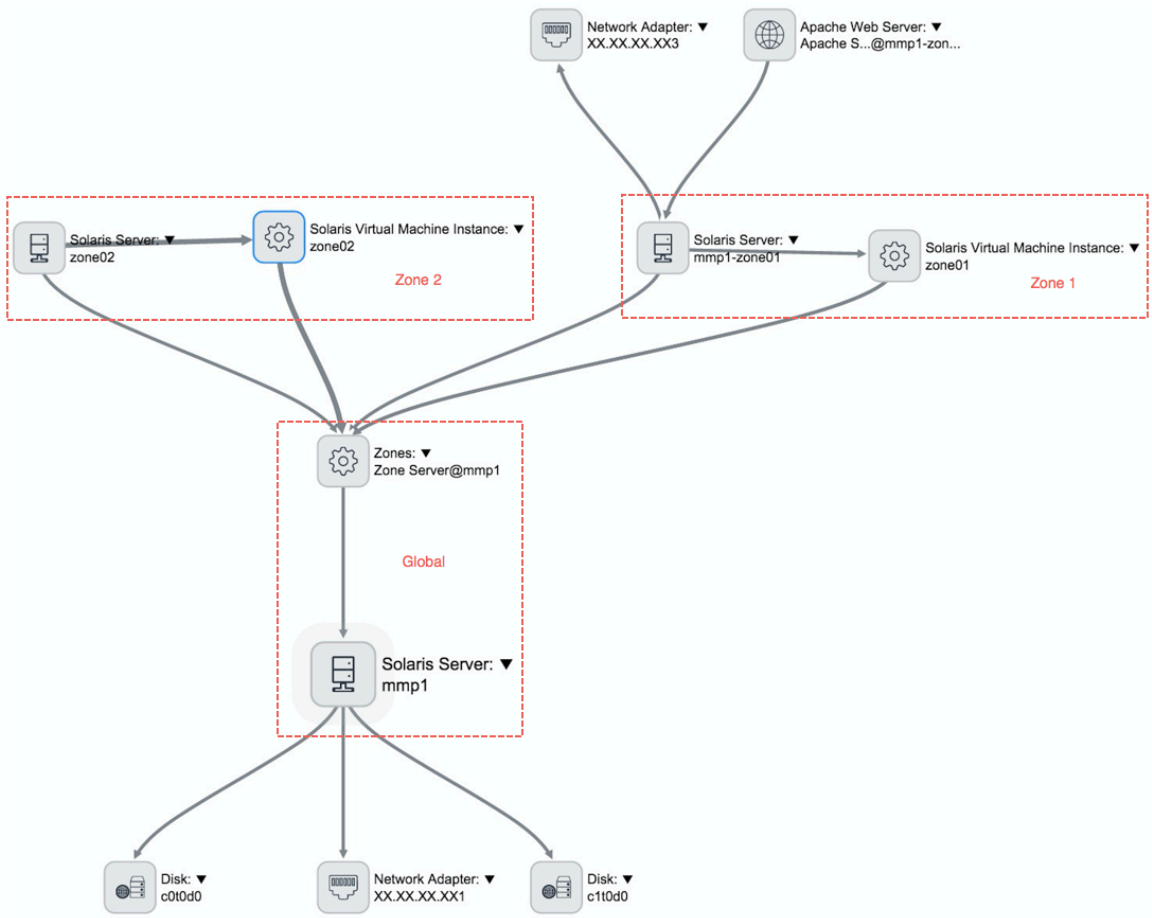
Erkennung von Solaris-Zonen

Bei der Erkennung ordnet Discovery die Beziehungen zwischen globalen und lokalen Solaris-Zonen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im folgenden Beispiel enthält eine globale Solaris-Zone zwei lokale Zonen: zone01 und zone02. Jede lokale Zone wird durch einen physischen Solaris-CI-Datensatz und einen VM-Instanzdatensatz dargestellt. Jede der lokalen Zonen ist an einen Zonenserver gebunden, wodurch die Beziehung zwischen Virtualisierung und globaler Zone (mmp1) verdeutlicht wird.

Zuordnung der Solaris-Zonenbeziehungen



Die TCP-Verbindungs- und -Prozessinformationen für lokale Zonenserver müssen durch Ausführung von Befehlen in ihrer übergeordneten globalen Zone erfasst werden. Der Beziehungspfad zwischen den physischen Computern der lokalen und globalen Zone muss festgelegt werden, bevor TCP-Verbindungs- und -Prozessinformationen für lokale Zonenserver erfasst werden können.

Fall 1: Die globale Zone wird zuerst erkannt.

- Das System erstellt das CI für den Solaris-Server für die globale Zone.
- Discovery erkennt die lokalen Zonen und erstellt für jedes Solaris-Gerät in der lokalen Zone je einen Datensatz für den Hypervisor-Zonenserver und die VM-Instanz.
- Discovery erstellt die Beziehung zwischen dem Hypervisor-Datensatz und dem VM-Instanzdatensatz.

Fall 2: Die lokale Zone wird zuerst erkannt.

- Das System erstellt das CI für den Solaris-Server für die lokale Zone.
- Discovery legt die Korrelations-ID fest, damit sie bei späteren globalen Zonenerkennungen abgeglichen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall 3: Die globale Zone wird nach der Erstellung von CIs für Solaris-Server der lokalen Zone erkannt.

- Die globale Zonenerkennung erkennt lokale Zonen.
- Discovery erstellt für jedes Solaris-Gerät in der lokalen Zone je einen Datensatz für den Hypervisor-Zonenserver und die VM-Instanz.
- Discovery erstellt die Beziehung zwischen dem Hypervisor-Datensatz und dem VM-Instanzdatensatz. Darüber hinaus wird die Beziehung zwischen dem virtuellen Computer der physischen lokalen Zone und dem entsprechenden Datensatz für die VM-Instanz hergestellt.
- Die globale Zone führt die Probe „Solaris - ADM“ für sich selbst aus, filtert nach der lokalen Zone und aktualisiert die physischen VMs der lokalen Zone mit diesen Daten.

Fall 4: Der Beziehungspfad zwischen physischen lokalen und globalen Zonencomputern wird eingerichtet.

Nachfolgende Erkennungen der globalen Zone aktualisieren die TCP-Verbindungs- und -Prozessinformationen für die enthaltenen lokalen Zonen.

Wenn das System eine globale Zone erkennt, löst die Probe „Solaris - Zones & ADM Launcher“ die Probe „Solaris - ADM“ aus, um die globale Zone und alle gefundenen lokalen Zonen zu untersuchen. Da die Probe „Solaris - ADM“ in der globalen Zone ausgeführt werden muss, um Informationen über TCP-Verbindungen und Prozesse aus ihren lokalen Zonen zu erkennen, werden möglicherweise mehrere ECC-Warteschlangen-Datensätze angezeigt, die identisch aussehen.

ECC-Warteschlangeneinträge zur Zonenerkennung

☐	2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31
☐	2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31
☐	2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31

Bei der Überprüfung der Nutzlast werden Sie jedoch feststellen, dass jede Probe tatsächlich auf ein anderes Zonen-CI abzielt, nach dem gefiltert und aktualisiert werden soll.

Nutzlast der lokalen Zone

```
<parameter name="sequence" value="1523a01c947000001
<parameter name="from_host" value=""/>
<parameter name="zone" value="zone01"/>
<parameter name="sys_created_on" value="2016-01-13 (
<parameter name="used_by_discovery" value="true"/>
```

In Solaris-Zonen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Version	cmdb_ci_vm_zones	Version	zoneadm, zonename
Zuordnungs-ID	cmdb_ci_vm_zones	correlation_id	zoneadm, zonename
Name	cmdb_ci_solaris_instance	Name	zoneadm, zonename
Übergeordnet	cmdb_ci_solaris_instance	parent	Intern
CMDB CI	cmdb_ci_solaris_instance	cmdb_ci	Intern
Zuordnungs-ID	cmdb_ci_solaris_instance	correlation_id	zoneadm, zonename

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: cmdb_ci_solaris_instance erweitert cmdb_ci_vm_instance.

Discovery der virtuellen Maschine (VM)

Muster für Discovery und Service-Mapping Identifizieren und klassifizieren Sie Informationen zu virtuellen Computern.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (August 2024 Store), können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Und verwenden Sie das erweiterte Dashboard.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Erfasste Daten

Bezeichnung	Tabellenname	Feldname
CPUs	cmdb_ci_vm_instance	CPUs
Datenträger	cmdb_ci_vm_instance	disks
Datenträgergröße	cmdb_ci_vm_instance	disks_size
Bildpfad	cmdb_ci_vmware_instance	image_path
Arbeitsspeicher	cmdb_ci_vm_instance	memory
Netzwerkadapter	cmdb_ci_vm_instance	nics
Status	cmdb_ci_vm_instance	Status
Vorlage	cmdb_ci_vmware_instance	Vorlage
vCenter-Referenz	cmdb_ci_vmware_instance	vcenter_ref
vCenter-Referenz-UUID	cmdb_ci_vmware_instance	vcenter_uuid

Erkennung von VMware

Ein Discovery-Zeitplan kann erkennen VMware VCenter- und ESX-Hosts sowie einzelne ESXi-Hosts, die VMs und zugehörige Komponenten ohne vCenter verwalten.

Die folgenden Optionen sind zum Abrufen von VMware vCenter-Daten verfügbar:

- Discovery führt die Probe VMware - vCenter Datacenters aus und identifiziert einen VMware vCenter-Prozess, der auf einem Windows-Computer ausgeführt wird, oder erkennt Aktivität mit der Probe „vmapp port“.
- Klassische Orchestration kann alle vCenter-Probes aus einem Workflow ausführen.

Um VMware-Daten ohne vCenter zu erkennen, verwenden Sie die eigenständige ESXi-Discovery.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery für VMware VCenter

Discovery kann den VMware vCenter-Prozess untersuchen, der auf einem Windows- oder Linux-Host ausgeführt wird. IPv6 wird für vCenter unterstützt.

Hinweis:

Wenn auf einem Windows- oder Linux-Server die Anwendung vCenter ausgeführt wird, wird nach dem Erstellen des vCenter-CI eine Beziehung vom Typ „Wird ausgeführt auf“ mit dem Windows- oder Linux-Serverhost erstellt.

Wenn eine vCenter-Anwendung auf einer dedizierten vCenter-Appliance ausgeführt wird, wird keine Beziehung „wird ausgeführt auf“ zum vCenter-CI erstellt.

Getestete vCenter-Versionen

Die ServiceNow® Platform unterstützt die vCenter-API Version 4.0 und höher. Die folgenden Versionen wurden mit Release Zurich getestet:

- vCenter Version 7.0 und früher
- vCenter-Appliance Version 6.7 und früher

Für Installationen, die auf der vCenter-Appliance basieren, wird ein Server-CI für die vCenter-Appliance erstellt, und die folgenden Felder werden ausgefüllt:

- NameIP
- AddressMAC
- AddressDiscovery
- Quelle

Hinweis: Wenn Sie SUSE Linux-Hosts für vCenter-Appliances Version 6,0 und früher erkennen, beachten Sie diese SSH-Einschränkungen .

Unter Für VMware vCenter-Server erfasste Daten finden Sie eine Beschreibung der VMware-Architektur und der Komponentenbeziehungen.

Erkennungsprozess für vCenter

Nach der Klassifizierung von vCenter startet Discovery die Probe „VMware - vCenter Datacenters“, der wiederum spezifische Probes startet, die Informationen über ESX-Computer, virtuelle Computer und andere vCenter-Objekte zurückgeben. Die Probe „vmapp port“ ist auch zum Starten des Probe „VMware - vCenter Datacenters“ konfiguriert.

Hinweis: Für eine genaue Beziehungszuordnung zwischen Server-CIs und vCenter-Ressourcen (z. B. ESX-Hosts und Datenspeicher) sollten Sie die Discovery der vCenter-Umgebung initiieren, bevor Sie Server-CIs erkennen. Dieser Ansatz hilft Discovery Ordnen Sie Server der entsprechenden von vCenter verwalteten Infrastruktur effektiver zu.

VMware-Anmeldeinformationen

Wenn Sie eine Domänenkonto für den Zugriff auf vCenter verwenden, geben Sie die Domäne mit dem Benutzernamen im Datensatz für die Anmeldeinformationen in einem der unterstützten Formate an, zum Beispiel **Domäne\Benutzername**. Die VMware-Anmeldeinformationen müssen in vCenter über eine schreibgeschützte Rolle und die Lizenzadministratorberechtigung verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Windows-Anmeldeinformationen sind für vCenter Discovery nicht erforderlich, wenn gültig VMware-Anmeldeinformationen Werden verwendet.

CMDB mit vCenter-Ereignissammlung aktualisieren

Neben der Suche nach vCenter-Daten über den Standard-Discovery-Prozess kann Discovery auch die CMDB aktualisieren, indem vCenter-Ereignisse über eine MID-Server-Erweiterung namens erkannt werden VCenter-Ereignissammler .

Mit dem Ereignissammler kann die CMDB zusätzlich zu den von Discovery erkannten Aktualisierungen mit Änderungen an virtuellen Maschinen (VMs) aktualisiert werden. Eine Änderung an einer VM wird vom vCenter-Server als Ereignis an den vCenter-Ereignissammler gesendet. Wenn ein Ereignis empfangen wird, wird die CMDB entsprechend aktualisiert. Full vCenter Discovery muss nicht erneut ausgeführt werden. Bei einigen Ereignissen, z. B. eingeschalteten und ausgeschalteten Ereignissen, muss Discovery nicht erneut ausgeführt werden. Bei den meisten Ereignissen wird Discovery nur auf der erforderlichen vCenter-Ressource ausgeführt.

Anweisungen zum Konfigurieren von vCenter-Ereignissen finden Sie unter Konfigurieren Sie die vCenter-Ereignissammlererweiterung, und führen Sie sie aus .

VM aus vCenter gelöscht

Beim Löschen der VM aus vCenter wird der Status von „cmdb_ci_vm_instance“ in „Beendet“ und der Wert des Statusfelds in „Deaktiviert“ geändert.

CIs aus vCenter entfernt

Wenn ein vCenter-CI wie ein virtueller Computer entfernt wird, wird es von der ServiceNow-Instanz in der CMDB mit einem der folgenden Verfahren als „veraltet“ markiert:

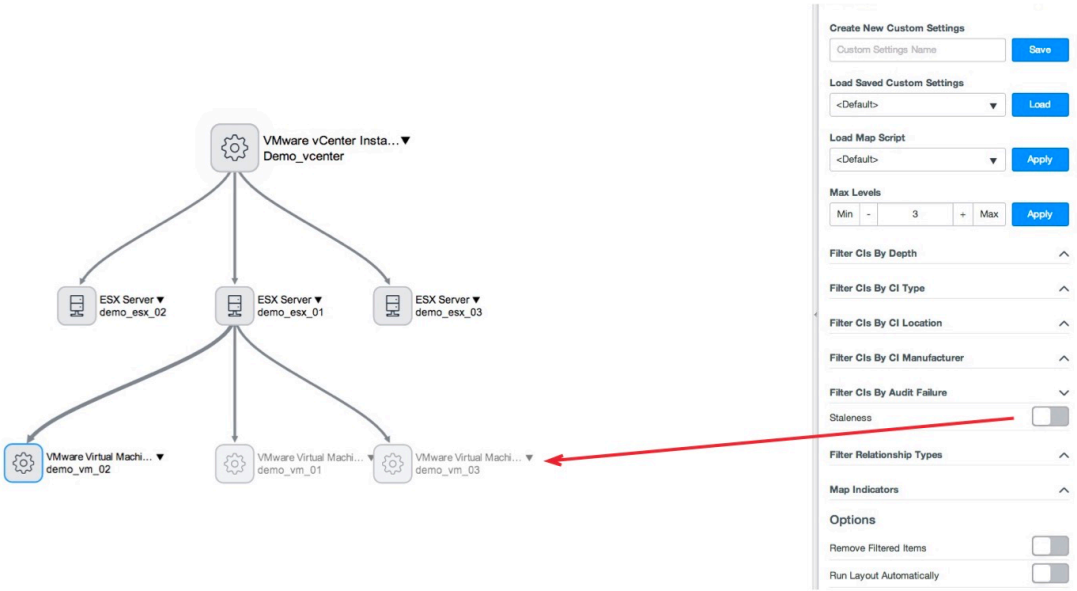
- Wenn Discovery Wird ausgeführt, wird ein Audit-Datensatz in erstellt Mit CMDB-Integrität installierte Komponenten Tabelle für das fehlende CI und markiert das CI als veraltet.
- Wenn die Instanz zum Erfassen von vCenter-Ereignissen konfiguriert ist, kann das System auch auf Basis des Ereignisses VmRemovedEvent einen „Veraltet“-Audit-Datensatz für das CI in der Tabelle „CMDB-Integritätsergebnis“ [cmdb_health_result] erstellen, ohne Discovery ausführen zu müssen.

Hinweis: Wenn die Einstellung **Veraltung** konfiguriert ist, werden in der Abhängigkeitsansicht (BSM-Zuordnung) veraltete CIs im Beziehungsdiagramm grau dargestellt, um anzugeben, dass sie aus vCenter entfernt wurden.

Um zu vermeiden, dass veraltete CI-Integritätsindikatoren während der VMware-Discovery generiert werden, legen Sie die Systemeigenschaft fest `glide.cmdb.health.src.cmdb_health_audit_only`Bis **Wahr** . Dadurch wird das Reporting veralteter CI aus der VMware-Discovery-Quelle deaktiviert, sodass Sie den CI-Lebenszyklus auf andere Weise verwalten können. Weitere Informationen finden Sie unter CMDB-Integrität – Systemeigenschaften .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als „veraltet“ markiertes vCenter-CI



Sie haben die Möglichkeit, einen zu erstellen CMDB-Korrekturregel Dient zum automatischen Ausführen eines Korrektur-Workflows, der z. B. veraltete CIs löschen kann. Weitere Informationen zu veralteten CIs finden Sie unter CMDB-Integritätsmetriken .

Erkennung von vCenter auf Windows-Host

Windows-Anmeldeinformationen sind für vCenter Discovery nicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

Alternativen Port für vCenter konfigurieren

Für die Probe „VMWare - vCenter Datacenters“ können Sie einen alternativen Port angeben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird die vCenter-Discovery für diese Ports initiiert:

- **vmapp6_https**: 9443
- **vmapp_https**: 5480

Wenn diese Ports erkannt werden, wird die VMware – vCenter Datacenters-Probe ausgelöst.

Prozedur

1. Hartcodieren Sie die Portinformationen.

a. Navigieren zu **Alle** > **Konfiguration** > **VMware** > **vCenter**an.

b. Wählen Sie aus der Liste der Instanzen die gewünschte Instanz aus.

c. Bearbeiten Sie das Feld **URL** so, dass der Port einbezogen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: `https://10.0.0.1:444`

d. Wählen Sie **Aktualisieren**.

2. Geben Sie für die Probe „VMWare - vCenter Datacenters“ einen alternativen Port für vCenter an.

a. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**an.

b. Öffnen Sie den Probe-Datensatz **VMware - vCenter Datacenters**.

c. In **Probe-Parameter** Zugehörige Liste, wählen Sie aus **Neu** .

d. Geben Sie in das Feld **Name** des Probe-Parameterdatensatzes den Namen `vcenter_port` ein.

e. Geben Sie in das Feld **Wert** die alternative Portnummer ein.

f. Wählen Sie **Absenden**.

3. Aktivieren Sie die VMware – vCenter-Klassifizierungsprobe.

Wichtig: Diese Konfiguration ist nur erforderlich, wenn sich vCenter auf Port 443 befindet.

a. Navigieren zu **Alle** > **Discovery-Definition** > **Anschlussprobes**an.

b. Öffnen Sie **http** Port-Probe-Datensatz.

c. In **Auslöserprobes** Zugehörige Liste wählen Sie aus **Falsch** Link für **VMware – vCenter-Klassifizierung** Klassifizierungsprobe.

d. Aktivieren Sie die Checkbox **Aktiv**.

e. Wählen Sie **Aktualisieren**.
VMware – vCenter – Klassifizierung von Probe versucht, eine Verbindung zwischen herzustellen MID-Server Und die vCenter-Instanz. Wenn die Verbindung erfolgreich ist, wird die VMware-vCenter-Datencenter-Probe ausgelöst.

Für VMware vCenter-Server erfasste Daten

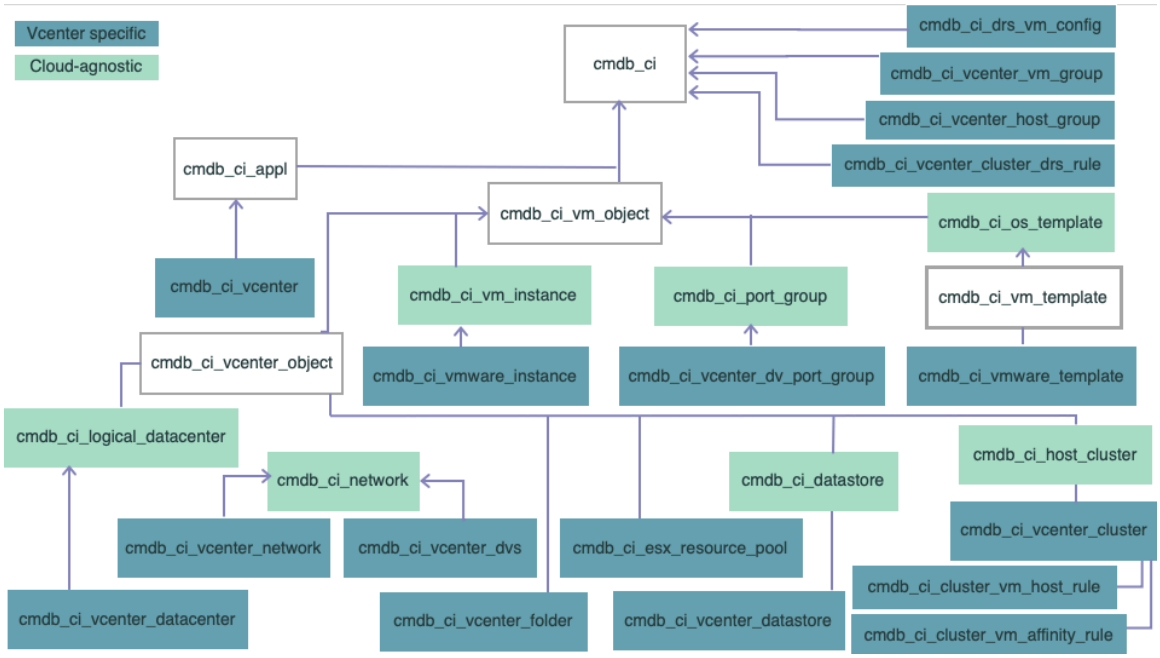
Discovery identifiziert und klassifiziert Informationen über VMware vCenter-Server.

vCenter-Tabellenschema

Im folgenden Diagramm wird das vCenter-Tabellenschema dargestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Tabellenschema



Bei mehreren Tabellen handelt es sich um Cloudagnostische Tabellen. Das heißt, dass sie für jede Cloud-Ressource gefüllt werden können, nicht nur für vCenter-Ressourcen. Suchen Sie in den untergeordneten Tabellen, die Erweiterungen der Cloudagnostischen Tabellen sind, nach erkannten CIs.

Cloudagnostische Tabelle	Entsprechende vCenter-spezifische Tabelle
VM-Instanz [cmdb_ci_vm_instance]	VMware-VM-Instanz [cmdb_ci_vmware_instance]
Betriebssystemvorlage [cmdb_ci_os_template]	Vorlage für virtuellen VMware-Computer [cmdb_ci_vmware_template]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Cloud-Netzwerke [cmdb_ci_network]	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
Datenspeicher [cmdb_ci_datastore]	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
Hostcluster [cmdb_ci_host_cluster]	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]

vCenter-Daten

Mithilfe von mehreren vCenter-Probes erfasst Discovery Daten aus vCenter. Die Daten werden in Tabellen gespeichert, die Erweiterungen der Tabelle der Konfigurationselemente [cmdb_ci] darstellen.

VMware vCenter-Instanz [cmdb_ci_vcenter]

Feldbezeichnung	Spaltenname
Name	Name
IP-Adresse	ip_address
API-Version	api_version

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VMware vCenter-Instanz [cmdb_ci_vcenter] (Fortsetzung)

Feldbezeichnung	Spaltenname
Vollständiger Name	fullname
Instanz-UUID	instance_uuid
URL	URL
Vollqualifizierter Domänenname	fqdn

Die Kombination der vCenter-Instanz in der Tabelle cmdb_ci_vcenter und der Objekt-ID in der Tabelle cmdb_ci_vm_object identifiziert ein bestimmtes vCenter.

Die Tabellen erweitern die Tabelle „VM-Objekte“ [cmdb_ci_vm_object], die Objekt-IDs für alle cloudbasierten Ressourcen mit Ausnahme von Virtualisierungsservern enthält.

DRS-VM-Konfiguration [cmdb_ci_drs_vm_config]

Feldbezeichnung	Spaltenname
Cluster	Cluster
DRS-Verhalten	drs_behavior
DRS-fähig	drs_enabled
Virtueller Computer	virtual_machine

In dieser Tabelle wird das DRS-Verhalten für die VMs gespeichert, das das Clusterverhalten überschreibt. Weitere Informationen zu DRS finden Sie in der VMware-Dokumentation zum verteilten Ressourcenplaner .

VMware vCenter-VM-Gruppe [cmdb_ci_vcenter_vm_group]

Feldbezeichnung	Spaltenname
Cluster	Cluster

Die Tabelle „VMware vCenter-VM-Gruppe“ [cmdb_ci_vcenter_vm_group] weist gegenüber „cmdb_ci_vmware_instance“ eine Beziehung vom Typ „Enthält::Enthalten in“ auf. Diese Gruppe verfügt über eine Reihe von VMs.

VMware vCenter-Hostgruppe [cmdb_ci_vcenter_vm_group]

Feldbezeichnung	Spaltenname
Cluster	Cluster

Die Tabelle „VMware vCenter-Hostgruppe“ [cmdb_ci_vcenter_host_group] weist gegenüber „cmdb_ci_vmware_instance“ eine Beziehung vom Typ „Enthält::Enthalten in“ auf. Diese Gruppe besitzt mehrere Hosts.

DRS-Regel für VMware vCenter-Cluster [cmdb_ci_vcenter_cluster_drs_rule]

Feldbezeichnung	Spaltenname
Regel-UUID	rule_uuid

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DRS-Regel für VMware vCenter-Cluster [cmdb_ci_vcenter_cluster_drs_rule] (Fortsetzung)

Feldbezeichnung	Spaltenname
Aktiv	active
Cluster	Cluster

VMware-VM-Instanz [cmdb_ci_vmware_instance]

Feldbezeichnung	Spaltenname
Name	Name
Vorlage	Vorlage
CPUs	CPUs
Datenträger	disks
Datenträgergröße (GB)	disks_size
Arbeitsspeicher (MB)	memory
Netzwerkadapter	nics
Bildpfad	image_path
Status	state
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Basisname	base_name
BIOS-UUID	bios_uuid
VM-Instanz-UUID	vm_instance_uuid
IP-Adresse	ip_address

Verteilte virtuelle VMware-Portgruppen [cmdb_ci_vcenter_dv_port_group]

Feldbezeichnung	Spaltenname
Name	Name
vCenter-Instanz-UUID	vcenter_uuid
Verweis auf verteilten virtuellen Switch	dvs_ref

Vorlage für virtuellen VMware-Computer [cmdb_ci_vmware_template]

Feldbezeichnung	Spaltenname
Name	Der Vorlagenname aus VMware
CPUs	CPUs
Datenträgergröße (GB)	disks_size
Gast-ID	guest_id
Arbeitsspeicher (MB)	memory

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlage für virtuellen VMware-Computer [cmdb_ci_vmware_template] (Fortsetzung)

Feldbezeichnung	Spaltenname
Bildpfad	image_path
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Netzwerkadapter	nics
Basisname	base_name
VM-Namensgeber	vm_namer
BIOS-UUID	bios_uuid
VM-Instanz-UUID	vm_instance_uuid

VMware vCenter-Objekt [cmdb_ci_vcenter_object]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref

VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]*

Feldbezeichnung	Spaltenname
Region	region
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Ordner der obersten Ebene für VMs	folder_moreid
Ordner der obersten Ebene für Hosts	host_morid

*Die Tabelle „VMware vCenter-Rechenzentrum“ [cmdb_ci_vcenter_datacenter] ist eine Erweiterung der Tabelle [cmdb_ci_logical_datacenter].

VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]*

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Netzwerk, auf das von Hosts oder VM zugegriffen werden kann	accessible

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

*Die Tabelle „VMware vCenter-Netzwerk“ [cmdb_ci_vcenter_network] ist eine Erweiterung der Tabelle [cmdb_ci_network].

Verteilter virtueller VMware-Switch [cmdb_ci_vcenter_dvs]

Feldbezeichnung	Spaltenname
VMCount	vm_count
Hostanzahl	host_count

VMware vCenter-Ordner [cmdb_ci_vcenter_folder]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Vollständiger Pfad	fullpath

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter
vCenter-Referenz	vcenter_ref
Besitzer	Eigentümer
Eigentümer verwaltetes Objekt Referenz-ID	owner_morid
CPU erweiterbar	cpu_expandable
CPU limitiert (MHz)	cpu_limit_mhz
CPU reserviert (MHz)	cpu_reserved_mhz
CPU Anteile	cpu_shares
Vollständiger Pfad	fullpath
Arbeitsspeicher erweiterbar	mem_expandable
Arbeitsspeicher limitiert (MB)	mem_limit_mb
Arbeitsspeicher reserviert (MB)	mem_reserved_mb
Speicheranteile	mem_shares

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
Zugänglich	accessible

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore] (Fortsetzung)

Feldbezeichnung	Spaltenname
vCenter-Referenz	vcenter_ref
Typ	Typ
Kapazität (GB)	Kapazität
Freier Speicherplatz (GB)	freespace
URL	url
Geclustert	clustered

*Die Tabelle „VMware vCenter-Datenspeicher“ [cmdb_ci_vcenter_datastore] ist eine Erweiterung der Tabelle [cmdb_ci_datastore].

VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]*

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
Effektive Hosts	effectivehosts
vCenter-Referenz	vcenter_ref
Tatsächliche CPU	effectivecpu
Tatsächlicher Speicher	effectivememory
Anzahl tatsächlicher Hosts	effectivehosts
Anzahl Hosts	numhosts
CPU gesamt	totalcpu
Speicher gesamt	totalmemory
Anzahl der CPU-Kerne	numcpucores
Anzahl der CPU-Kerne	numcputhreads
DRS-Verhalten	drs_behavior
DRS aktiviert	drs_enabled
DRS-VMotion-Rate	drs_vmotion_rate

*Die Tabelle „VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]“ ist eine Erweiterung der Tabelle [cmdb_ci_host_cluster].

Informationen zur Clusterhostregel der VM [cmdb_ci_cluster_vm_host_rule]

Feldbezeichnung	Spaltenname
VM-Gruppe	vm_group
Hostgruppe	host_group
Obligatorisch	Obligatorisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zur Clusterhostregel der VM [cmdb_ci_cluster_vm_host_rule] (Fortsetzung)

Feldbezeichnung	Spaltenname
Affinität	affinity

Informationen zur Clusteraffinitätsregel der VM [cmdb_ci_cluster_vm_affinity_rule]

Feldbezeichnung	Spaltenname
Affinität	affinity

Die Tabelle „Informationen zur Clusteraffinitätsregel der VM“ [cmdb_ci_cluster_vm_affinity_rule] weist gegenüber „cmdb_ci_vmware_instance“ die Beziehung „Enthält::Enthalten in“ auf. Diese Gruppe besitzt mehrere VMs, auf die diese Affinität angewendet wird.

Verteilter virtueller VMware-Switch [cmdb_ci_vcenter_dvs]

Feldbezeichnung	Spaltenname
Name	Name
VMCount	vm_count
Hostanzahl	host_count

Discovery ordnet die Beziehungen auch VMs und verteilten virtuellen Portgruppen zu.

Verteilte virtuelle VMware-Portgruppe [cmdb_ci_vcenter_dv_port_group]

Feldbezeichnung	Spaltenname
Name	Name
vCenter-Instanz-UUID	vcenter_uuid
Verweis auf verteilten virtuellen Switch	dvs_ref

Discovery ordnet die Beziehungen auch dem verteilten virtuellen Switch zu.

Sie können die folgenden zugehörigen Listen hinzufügen, um zusätzliche erkannte Daten anzuzeigen:

- **Speicher-Laufwerke**

  Die virtuellen Datenträger für diesen virtuellen Computer. Diese Daten werden in der Tabelle „Speichervolume“ [cmdb_ci_storage_volume] mit dem Wert `type=v Disk` gespeichert.

Speichervolume [cmdb_ci_storage_volume]

Feldbezeichnung	Spaltenname
Name	Name
Größe	size

- **Netzwerkadapter**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die virtuellen Netzwerkadapter für die virtuellen Datenträger. Diese Daten werden in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] gespeichert.

Netzwerkadapter [cmdb_ci_network_adapter]

Feldbezeichnung	Spaltenname
Name	Name
IP-Adresse	ip_address
MAC-Adresse	mac_address
Netzmaske	netmask

vCenter-Erkennung mit Software Asset Management

Wenn Software Asset Management aktiv ist, füllt Discovery diese vCenter-Tabellen mithilfe der Probe „VMware - vCenter ESX Hosts License“.

VMware-Lizenzschlüssel [samp_vmware_license_key]

Feldbezeichnung	Spaltenname
vCenter-Referenz	vcenter_ref
Kosteneinheit	cost_unit
Edition	Edition
Funktionen	features
Lizenzschlüssel	license_key
Produktname	product_name
Produktversion	product_version
Rechte im Besitz	rights_owned
Verwendete Rechte	rights_used

VMware-Lizenzschlüsselnutzung [samp_vmware_license_key_usage]

Feldbezeichnung	Spaltenname
Verwendete Rechte	rights_used
Ablaufdatum	expiration_date
Verwendete Funktionen	used_features
Lizenzschlüssel	license_key
Softwareinstallation	software_install
Verwendet von	used_by

vCenter-Beziehungen

Discovery erstellt mithilfe von Daten aus einer Schlüsselklasse automatisch Beziehungen für vCenter-Komponenten. Nachfolgende Erkennungen verwenden dieselbe Schlüsselklasse, um Beziehungen, die nicht mehr gültig sind, automatisch zu validieren und zu entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

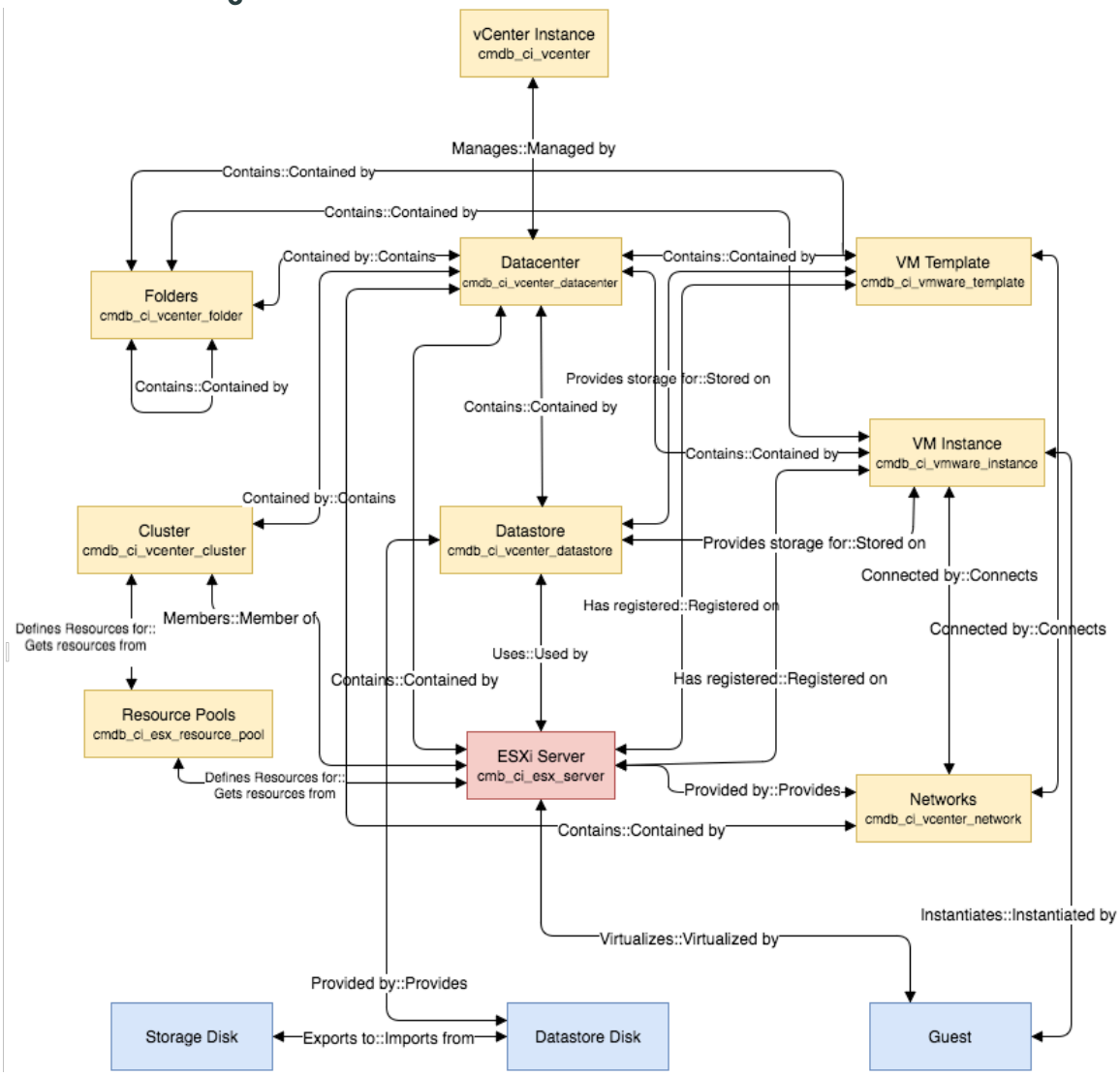
vCenter-CIs können Mitglieder von Ordnern oder Clustern sein, was sich darauf auswirkt, wie Discovery deren Beziehungen erstellt.

- Wenn sich ein CI in einem Ordner befindet, erstellt Discovery eine Beziehung zwischen diesem CI und dem Ordner. Befindet sich das CI nicht in einem Ordner, erzeugt Discovery die Beziehung zwischen dem CI und dem Rechenzentrum. Die folgenden vCenter-CIs können sich in einem Ordner befinden:
  - VM-Instanz
  - VM-Template
  - vCenter-Netzwerk
  - Datenspeicher
  - vCenter-Ordner
  - vCenter-Cluster
- Wenn sich ein ESX-Server in einem Cluster befindet, erstellt Discovery eine Beziehung zwischen dem ESX-Server und dem Cluster. Ist ein ESX-Server kein Mitglied eines Clusters, erzeugt Discovery eine Beziehung zum Rechenzentrum.
- Wenn sich ein Ressourcenpool in einem Cluster befindet, erstellt Discovery eine Beziehung zwischen dem Ressourcenpool und dem Cluster. Ist der Ressourcenpool kein Mitglied eines Clusters, erstellt Discovery eine Beziehung zum ESX-Server.

Das folgende Diagramm veranschaulicht vCenter-Beziehungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Beziehungen



Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Computer [cmdb_ci_computer]	Virtualisiert von::Virtualisiert	ESX-Server [cmdb_ci_esx_server] **Hinweis:** Die vom ESX-Server und der VM-Instanz erstellte Beziehung zum Gast wird durch die Business-Regel „Überprüfung virtueller Computer“ erstellt. Der Gastcomputer muss erkannt werden, nachdem das vCenter erkannt wurde, um die Business-Regel auszulösen und solche Beziehungen zu erstellen.
Computer [cmdb_ci_computer]	Instanziiert::Instanziiert von	VM-Instanz [cmdb_ci_vmware_instance]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
		Hinweis: Die vom ESX-Server und der VM-Instanz erstellte Beziehung zum Gast wird durch die Business-Regel „Überprüfung virtueller Computer“ erstellt. Der Gastcomputer muss erkannt werden, nachdem das vCenter erkannt wurde, um die Business-Regel auszulösen und solche Beziehungen zu erstellen.
VMware-VM-Instanz [cmdb_ci_vmware_instance]	Registriert auf::Hat sich registriert	ESX-Server [cmdb_ci_esx_server]
VMware-VM-Instanz [cmdb_ci_vmware_instance]	Verbunden von::Verbindet	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
Vorlage für virtuellen Computer [cmdb_ci_vmware_template]	Verbunden von::Verbindet	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]	Bereitgestellt von::Stellt bereit	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Stellt Speicher bereit für::Gespeichert auf	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Verwendet von::Verwendet	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Stellt Speicher bereit für::Gespeichert auf	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]
VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]	Mitglieder::Mitglied von	ESX-Server [cmdb_ci_esx_server]
ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für::Erhält Ressourcen von	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]
ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für::Erhält Ressourcen von	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

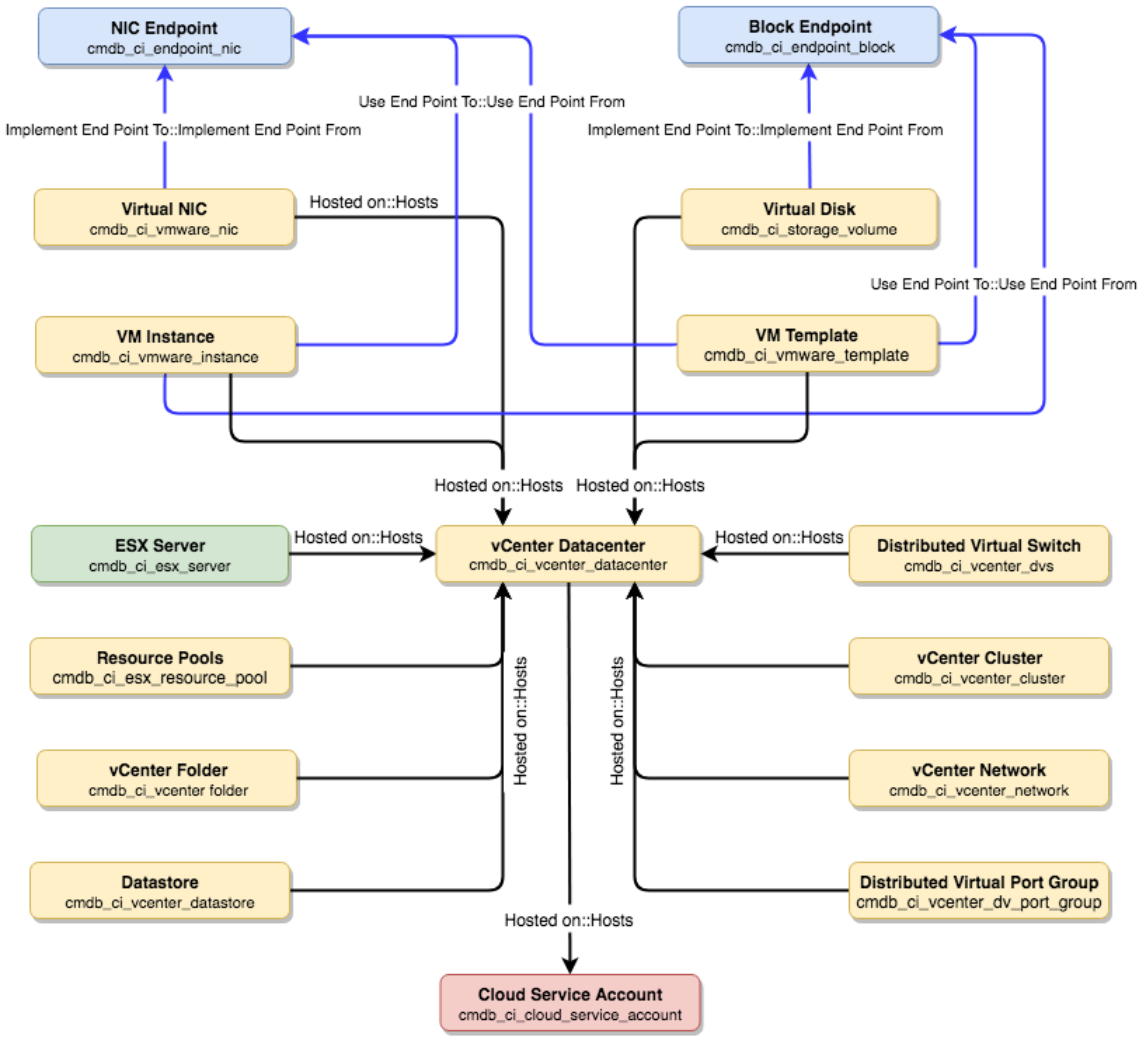
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]

Cloud Management-Beziehungen

Die folgenden zusätzlichen Beziehungen werden erstellt, wenn Cloud Management (CMP) aktiv ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
ESX-Server [cmdb_ci_esx_server]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Ordner [cmdb_ci_vcenter folder]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
vCenter-Cluster [cmdb_ci_vcenter_cluster]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Ressourcenpools [cmdb_ci_esx_resource_pool]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Instanz [cmdb_ci_vmware_instance]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Vorlage [cmdb_ci_vmware_template]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Netzwerk [cmdb_ci_vcenter_network]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Verteilter virtueller Switch [cmdb_ci_vcenter_dvs]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Verteilte virtuelle Portgruppe [cmdb_ci_vcenter_dv_port_group]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Datenspeicher [cmdb_ci_vcenter_datastore]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Virtueller Datenträger [cmdb_ci_storage_volume]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Virtuelle NIC [cmdb_ci_vmware_nic]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Vorlage [cmdb_ci_vmware_template]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
VM-Instanz [cmdb_ci_vmware_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
Virtueller Datenträger [cmdb_ci_storage_volume]	Endpunkt implementieren in::Endpunkt implementieren von	Block-Endpunkt [cmdb_ci_endpoint_block]
Virtuelle NIC [cmdb_ci_vmware_nic]	Endpunkt implementieren in::Endpunkt implementieren von	NIC-Endpunkt [cmdb_ci_endpoint_nic]
VM-Vorlage [cmdb_ci_vmware_template]	Endpunkt verwenden an::Endpunkt verwenden von	NIC-Endpunkt [cmdb_ci_endpoint_nic]
VM-Instanz [cmdb_ci_vmware_instance]	Endpunkt verwenden an::Endpunkt verwenden von	NIC-Endpunkt [cmdb_ci_endpoint_nic]

VMware-Tags

Über die vSphere-Schnittstelle können Sie Tags an vSphere-Objekte (zum Beispiel virtuelle Computer) anhängen. Die Tags können dann in Kategorien gruppiert werden. Objekte mit Tags können basierend auf den Parametern, die Sie den Tags und Kategorien zuweisen, sortiert und durchsucht werden. Die Probe VMWare - vCenter VM Tags erkennt diese Tags. Die erkannten Tags können Sie anzeigen, indem Sie den VM-Datensatz in **cmdb_ci_vmware_instance** öffnen. Wechseln Sie dann zur Registerkarte **Schlüsselwerte**.

Schlüsselwerte [cmdb_key_value]

Feldbezeichnung und -name	Beschreibung
Konfigurationselement [configuration_item]	Referenzierte VM mit angehängtem Tag in vCenter
Schlüssel [key]	Kategoriename des Tag, das auf die Ressource in vCenter angewendet wird
Tag [tag]	Quelle in vCenter, aus der Tags abgerufen werden. In diesem Fall lautet der Wert immer **Tags**.
Wert [value]	Name des Tag, das in vCenter auf die Ressource angewendet wird

Von Discovery erfasste Datenspeicherdaten

Discovery identifiziert jeden Datenspeicher im System und erstellt die Beziehungen zu den virtuellen Computern und den ESX-Servern, die diese Datenspeicher verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenspeicher

Discovery verwendet die Probe „VMware - vCenter Datastores“, um diese Daten aus Datenspeichern zu erfassen.

Feldbezeichnung	Tabellenname	Spaltenname	Beschreibung
Zugänglich	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	accessible	Angabe, ob der Datenspeicher erfasst wurde oder nicht
Kapazität (GB)	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Kapazität	Vom Datenspeicher bereitgestellter Speicherplatz
Geclustert	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	clustered	Angabe, ob der Datenspeicher geclustert ist (zu einem Speicher-Pod gehört)
Freier Speicherplatz (GB)	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	freespace	Im Datenspeicher noch verfügbarer Speicherplatz
Typ	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Typ	Typ des Dateisystemvolume, zum Beispiel WFS oder NFS
URL	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	url	Der eindeutige URL-Locator für den Datenspeicher

Host-Mounts

Discovery verwendet die Probes „VMWare - vCenter ESX Hosts“ und „VMWare - vCenter Datastores“, um Daten des Host-Mount für den Datenspeicher zu erfassen.

Feldbezeichnung	Tabelle	Spalte
Zugänglich	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	accessible
Zugriffsmodus	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	access_mode
VMware vCenter-Datenspeicher	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	datastore
ESX-Server	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	esx_server
vCenter-Referenz	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	vcenter_ref

Erkennung von ESXi-Servern

Informationen über ESXi-Server und ESXi-Ressourcenpools identifiziert und klassifiziert Discovery nicht durch die direkte Erkennung von ESXi-Servern, sondern durch die Erkennung von vCenter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Die Erkennung von ESXi-Servern erfolgt über vCenter. Geben Sie die IP-Adresse des ESXi-Servers nicht in einem Discovery-Zeitplan an. Führen Sie anhand des Erkennungszeitplans stattdessen eine Erkennung von vCenter durch.

Unter Für VMware vCenter-Server erfasste Daten finden Sie eine Beschreibung der VMware-Architektur und der Komponentenbeziehungen.

Eine Beschreibung, wie Discovery Informationen über Datenspeicher erfasst und die Beziehungen zwischen den ESXi-Hosts und den an die Datenspeicher angehängten Speicherdatenträgern herstellt, finden Sie unter Erkennung von Datenspeicher.

Erforderliche Rollen

Benutzer mit den Rollen `itil` und `asset` haben Zugriff auf Datensätze von ESXii- und ESXi-Konfigurationselementen (CIs). Zum Ausführen der Erkennung auf vCenter-Servern müssen Benutzer über die Rolle `discovery_admin` verfügen.

Berechtigungen

Zum Ausführen einer vollständigen Erkennung von vCenter-/ESXi-Servern benötigen Sie vCenter-Anmeldeinformationen. Wenn die Probe „vmapp port“ deaktiviert ist, müssen Sie mit Windows-Anmeldeinformationen auf den Windows-Host zugreifen, auf dem der vCenter-Server ausgeführt wird.

Hinweis: Stellen Sie sicher, dass Sie Anmeldeinformationen mit *VMware* als *Typ* auswählen.

Komponenten bei der Erkennung von ESXi-Servern

Discovery identifiziert ESXi-Server basierend auf der Korrelations-ID (BIOS-UUID), wenn sich der Hardwarehersteller auf einer zertifizierten Aufnahmeliste befindet. Befindet sich der Hersteller also in der Liste der kompatiblen Hersteller, muss die Korrelations-ID eindeutig sein. Wenn der Hersteller nicht auf der zertifizierten Aufnahmeliste steht, werden auch die verwaltete Objektreferenz-ID (MORID) und die Seriennummer überprüft. Nach der Ausführung der vCenter-Klassifizierung startet Discovery die Probe „VMware - vCenter Datacenters“, die die Probes startet, die den ESXi-Server untersuchen. Die vollständige Liste der vCenter-Probes finden Sie unter Liste der Discovery-Probes.

Komponente	Name	Beschreibung
Klassifizierung	vCenter	Klassifiziert eigenständige vCenter-Server
Probe	VMWare - vCenter ESX Hosts	Erstellt Datensätze für ESXi-Server und Host-Mounts. Erstellt Beziehungen zwischen ESXi-Servern und vCenter-Komponenten. Löst Probes zur Speichererkennung aus
Probe	VMWare - vCenter ESX Hosts Storage	Erstellt Datensätze für ESXi-Hosthardware: Netzwerkadapter, Datenträger, HBAs, FC-Ports, iSCSI und FC-Datenträger. Erstellt Beziehungen zwischen DAS/iSCSI/FC-Datenträgern und Datenspeicher-Datenträgern

Erfasste Daten

Grundlegende Serverdaten von ESXi-Hosts werden mit der Probe „VMware - vCenter ESX-Hosts“ erfasst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery auf ESXi-Hosts erfasste Daten

Bezeichnung	Tabellenname	Feldname
Betriebssystem	cmdb_ci_esx_server	os
BS-Version	cmdb_ci_computer	os_version
Name	cmdb_ci_esx_server	Name
DNS-Domäne	cmdb_ci_esx_server	dns_domain
Hersteller	cmdb_ci_computer	manufacturer
Seriennummer	cmdb_ci_computer	serial_number
CPU-Typ	cmdb_ci_esx_server	cpu_type
CPU-Geschwindigkeit (MHz)	cmdb_ci_esx_server	cpu_speed
CPU-Anzahl	cmdb_ci_esx_server	cpu_count
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count
CPU-Hersteller	cmdb_ci_esx_server	cpu_manufacturer
Modell-ID	cmdb_ci_computer	model_id
RAM (MB)	cmdb_ci_esx_server	ram
Festplattenspeicher (GB)	cmdb_ci_esx_server	disk_space
Typ	cmdb_ci_disk	Typ
Modell-ID	cmdb_ci_disk	model_id
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space
Name	cmdb_ci_disk	Name
Name	cmdb_ci_network_adapter	Name
IP-Adresse	cmdb_ci_network_adapter	ip_address
MAC-Adresse	cmdb_ci_network_adapter	mac_address
Netzmaske	cmdb_ci_network_adapter	netmask
Verwaltetes Objekt Referenz-ID	Virtualisierungsserver [cmdb_ci_virtualization_server]	morid
Seriennummer	Seriennummer [cmdb_serial_number]	serial_number

Beziehungen

Discovery erfasst die folgenden Beziehungsdaten für ESXi-Server.

Basisklasse	Beziehung	Abhängige Klasse
ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für:Erhält Ressourcen von	ESXi-Server [cmdb_ci_esx_server]
VM-Instanz [cmdb_ci_vmware_instance]	Registriert auf::Hat sich registriert	ESXi-Server [cmdb_ci_esx_server]
ESXi-Server [cmdb_ci_esx_server]	Stellt Speicher bereit für::Gespeichert auf	VM-Vorlage [cmdb_ci_vmware_template]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basisklasse	Beziehung	Abhängige Klasse
ESXi-Server [cmdb_ci_esx_server]	Bereitgestellt von::Stellt bereit	Netzwerke [cmdb_ci_vcenter_network]
ESXi-Server [cmdb_ci_esx_server]	Mitglieder von::Mitglieder	Cluster [cmdb_ci_vcenter_Cluster]
ESXi-Server [cmdb_ci_esx_server]	Enthält::Enthalten in	Rechenzentrum [cmdb_ci_vcenter_datacenter]

ESXi-Ressourcenpools

Ressourcenpools werden in vCenter konfiguriert. Sie definieren die maximale Menge an Ressourcen, die von virtuellen Computern in diesem Pool verwendet werden können. Eine ESXi-Servereigenschaft ermöglicht, dass Ressourcenpools bei Bedarf erweitert werden, wenn der ESXi-Server über zusätzliche Ressourcen verfügt. Die Felder **Name** und **Besitzer** jedes Ressourcenpools auf dem ESXi-Server müssen auf der ServiceNow AI Platform

in der Tabelle „ESXi-Ressourcenpool“ [cmdb_ci_esx_resource_pool] konfiguriert werden. Wenn Orchestration für VMware manuelle Bereitstellungsaufgaben ausführt, muss der Bereitsteller den richtigen Ressourcenpool für den angeforderten virtuellen Server auswählen. Discovery erkennt Ressourcenpools auf ESXi-Computern und füllt automatisch die Felder im Formular „ESXi-Ressourcenpool“. Weitere Informationen finden Sie unter ESXi-Ressourcenpools konfigurieren.

ESXi-Ressourcenpools erfordern das Plugin „Orchestration - VMware Support“.

Hinweis: Stellen Sie sicher, dass vCenter und der ESXi-Server vollständig konfiguriert wurden. Dies schließt die Erstellung der Vorlagen und Ressourcenpools ein.

Erfasste Daten

Bezeichnung	Tabelle	Feldname	Quelle
CPU erweiterbar	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_expendable	Probe „VMWare - vCenter Clusters“
CPU limitiert (MHz)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_limit_mhz	Probe „VMWare - vCenter Clusters“
CPU reserviert (MHz)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_reserved_mhz	Probe „VMWare - vCenter Clusters“
CPU Anteile	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_shares	Probe „VMWare - vCenter Clusters“
Vollständiger Pfad	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	fullpath	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher erweiterbar	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_expandable	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher limitiert (MB)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_limit_mb	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher reserviert (MB)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_reserved_mb	Probe „VMWare - vCenter Clusters“
Speicheranteile	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_shares	Probe „VMWare - vCenter Clusters“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Daten (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
Besitzer	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	Eigentümer	Probe „VMWare - vCenter Clusters“
Eigentümer verwaltetes Objekt Referenz-ID	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	owner_morid	Probe „VMWare - vCenter Clusters“

ESXi-Ressourcenpools konfigurieren

Der ESXi-Server besitzt einen standardmäßigen Ressourcenpool namens „Ressourcen“, in dem normale Ressourcen für virtuelle Computer definiert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Ressourcenebenen werden dynamisch aus *Freigaben* der gesamten Ressourcen generiert, die virtuellen Computern auf dem ESXi-Server zugewiesen sind. Ausführliche Informationen zur Berechnung dieser Ressourcen finden Sie in der VMware Knowledge Base https://www.vmware.com/ . ServiceNow Discovery erkennt diesen Standardressourcenpool und fügt dem Modul „ESXi-Ressourcenpools“ automatisch einen Datensatz hinzu. Wenn Discovery nicht auf der ServiceNow-Instanz ausgeführt wird , erstellen Sie einen Datensatz für den Pool **Ressourcen**. Stellen Sie sicher, dass das Feld **Besitzer** korrekt ist, und lassen Sie die Ressourcenfelder leer. Wenn ein Bereitsteller bei der Bereitstellung eines virtuellen Servers den Pool **Ressourcen** auswählt, erstellt der ESXi-Server einen virtuellen Computer zur Verwendung unter normaler Last.

Prozedur

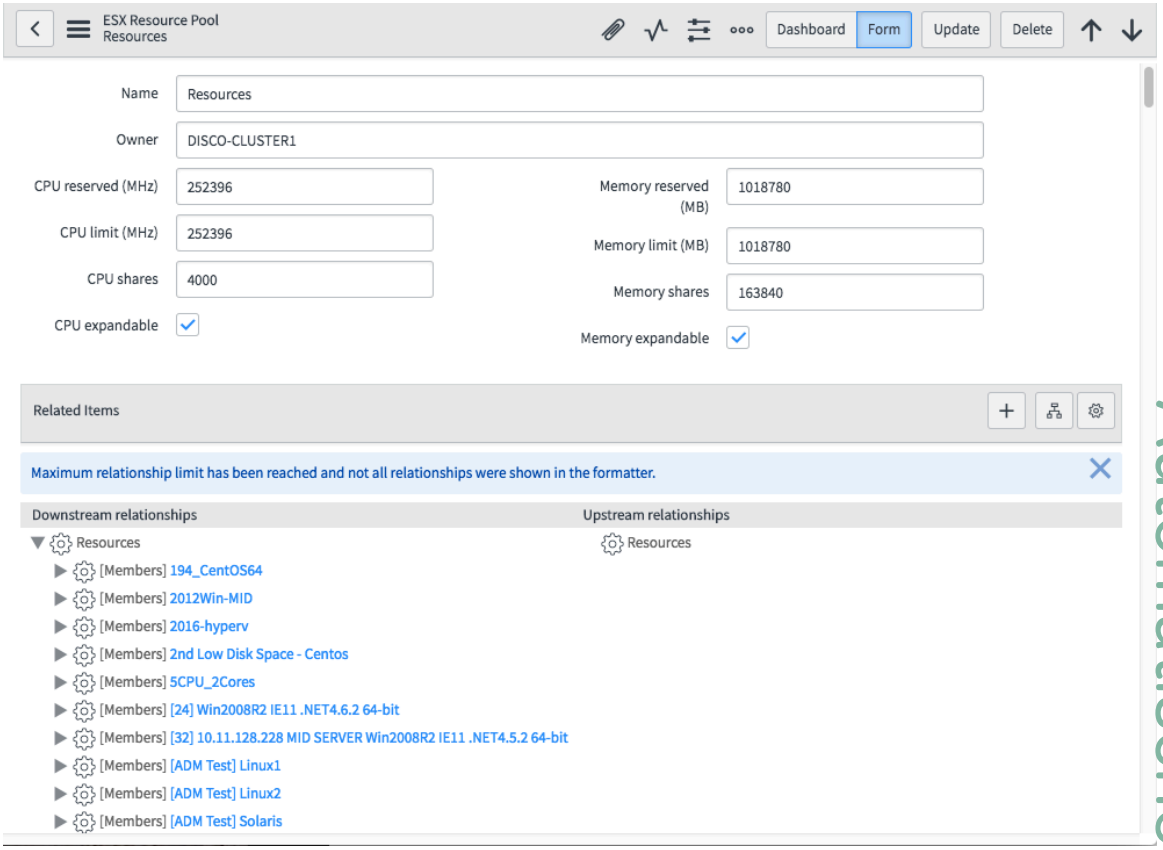
1. Navigieren zu **Alle** > **VMware-Cloud** > **Konfiguration** > **ESX-Ressourcenpools**an.
2. Klicken Sie in der Liste auf **Neu**.
3. Erstellen Sie einen neuen Datensatz für jeden Ressourcenpool auf dem ESXi-Server, und vergewissern Sie sich, dass die Felder **Name** und **Besitzer** korrekt ausgefüllt sind.
4. Aktivieren Sie die Kontrollkästchen **CPU erweiterbar** und **Arbeitsspeicher erweiterbar**, um bei Bedarf eine Erhöhung der CPU- und der Arbeitsspeicherlimits zu ermöglichen, wenn diese Ressourcen auf dem ESXi-Server verfügbar sind.

   Nach der Gewährung können diese zusätzlichen Ressourcen bei Bedarf widerrufen werden, um andere virtuelle Computer bereitzustellen. Die zusätzlichen Felder im Formular dienen nur zu Anzeigezwecken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.

Formular „ESX-Ressourcenpool“



Erkennung eigenständiger ESXi-Server

Mit der Erkennung eigenständiger ESXi-Server wird die Erkennung einzelner ESXi-Server unterstützt, auf denen virtuelle Computer (Virtual Machines, VMs) und zugehörige Komponenten ohne vCenter gehostet werden. Verschiedene CIs und Beziehungen werden im Rahmen eines Discovery-Zeitplans erkannt.

Erforderliche Rollen

Anwender mit `itil`Und `asset`Rollen können auf ESXi-Konfigurationselement-Datensätze (CI) zugreifen. Um eine eigenständige ESXi-Discovery auszuführen, müssen Anwender über verfügen `discovery_admin`Rolle.

VMware-Anmeldeinformationen

Zum Ausführen einer Erkennung eigenständiger ESXi-Server benötigen Sie VMware-Anmeldeinformationen. Erstellen Sie die Anmeldeinformationen, indem Sie zu navigieren **Discovery** > **Anmeldeinformationen** > **VMware-Anmeldeinformationen.**

Wenn Sie ein Domänenkonto für den Zugriff auf den ESXi-Host verwenden, geben Sie die Domäne mit dem Benutzernamen im Datensatz für die Anmeldeinformationen in einem der unterstützten Formate an, zum Beispiel **Domäne\Benutzername**.

Hinweis: Die VMware-Anmeldeinformationen müssen auf dem ESXi-Host über eine Rolle mit Lesezugriff verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen

- Stellen Sie sicher, dass das Plugin „Discovery“ (com.snc.discovery) installiert und aktiviert ist und dass Sie auf Release Zurich oder höher aktualisiert haben.
- Aktivieren Sie die ESXi-Auslöser-Probe. Navigieren Sie zur Tabelle „Auslöser-Probe“ [trigger_probe_m2m]. Der esxi-Datensatz ist standardmäßig inaktiv. Markieren Sie „Aktiv“ als „true“, um die Erkennung eigenständiger ESXi-Server zu aktivieren.
- Erstellen Sie einen neuen Discovery-Zeitplan für den Host mit der entsprechenden IP-Adresse des ESXi-Hosts.

Hinweis: Wenn sowohl SSH als auch ESXi ausgelöst werden, wird zuerst SSH gestartet und kann dazu führen, dass Discovery mit der Meldung „ESX Discovery wird nur über vCenter unterstützt“ abgeschlossen wird. Öffnen Sie in diesem Fall die Probe Unix – Classify, und legen Sie ESX – OS inaktiv fest.

Komponenten bei der Erkennung von ESXi-Servern

Discovery identifiziert ESXi-Server basierend auf der Korrelations-ID (BIOS-UUID), wenn sich der Hardwarehersteller auf einer zertifizierten Aufnahmeliste befindet. Wenn der Hersteller in der Liste aufgeführt ist, muss die Korrelations-ID eindeutig sein. Wenn der Hersteller nicht auf der zertifizierten Aufnahmeliste steht, werden auch die verwaltete Objektreferenz-ID (MORID) und die Seriennummer überprüft.

Nach der Ausführung von Shazzam findet eine Suche nach der Port-Probe esxi statt. Anschließend startet Discovery die Probe „VMware - Standalone ESXi Server“, von der dann wiederum die Probes gestartet werden, mit denen der ESXi-Server untersucht wird. Andere vorhandene Discovery-Probes werden ebenfalls gestartet. Die vollständige Liste der Probes finden Sie unter Liste der Discovery-Probes.

Komponenten bei der Erkennung von ESXi-Servern

Komponente	Name	Beschreibung
IP-Service	ESXi	IP-Service ESXi - Die VMware VM-Konsole ist für Port 902 definiert.
Port-Probe	esxi	Webbenutzeroberfläche der ESXi-Server-Appliance. Wird von IP Service ESXi ausgelöst und löst die Probe „VMware - Standalone ESXi Server“ aus.
Probe	VMware - Standalone ESXi Server	Probe, mit der Informationen zu einem ESXi-Server abgerufen werden
Probe	VMWare - vCenter ESX Hosts	Erstellt Datensätze für ESXi-Server und Host-Mounts. Löst andere Probes aus: • VMware - vCenter ESX Hosts Storage • VMware - vCenter Datastores

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten bei der Erkennung von ESXi-Servern (Fortsetzung)

Komponente	Name	Beschreibung
		• VMware - vCenter Networks • VMware - vCenter VMs
Probe	VMWare - vCenter ESX Hosts Storage	Erstellt Datensätze für ESXi-Hosthardware: Netzwerkadapter, Datenträger, HBAs, FC-Ports, iSCSI und FC-Datenträger. Erstellt Beziehungen zwischen DAS/ iSCSI/FC-Datenträgern und Datenspeicher-Datenträgern

Grundlegende Serverdaten von ESXi-Hosts werden mit der Probe „VMware - vCenter ESX-Hosts“ erfasst.

Daten zu eigenständigen ESXi-Servern

Discovery nutzt mehrere vorhandene Probes, um diese Daten von ESXi zu erfassen. Die Daten werden in verschiedenen Tabellen gespeichert. Einige der CIs, die über das Feld „Server“ verfügen, beinhalten einen Verweis auf den ESXi-Host (z. B. cmdb_ci_esx_server).

VMware-VM-Instanz [cmdb_ci_vmware_instance]

Feldbezeichnung	Spaltenname
Name	Name
Arbeitsspeicher (MB)	memory
CPUs	CPUs
Datenträger	disks
Netzwerkadapter	nics
Objekt-ID	object_id
Server	Server
Status	state
Zuordnungs-ID	correlation_id
VM-Instanz-UUID	vm_instance_uuid
Status	install_status

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]

Feldbezeichnung	Spaltenname
Name	Name
Kapazität (GB)	Kapazität
Freier Speicherplatz (GB)	freespace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore] (Fortsetzung)

Feldbezeichnung	Spaltenname
Zugänglich	accessible
Typ	Typ
Objekt-ID	object_id
Server	Server
URL	url
Status	install_status

VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Feldbezeichnung	Spaltenname
Name	Name
Objekt-ID	object_id
Server	Server
Status	install_status

VMware-Netzwerkadapter [cmdb_ci_vmware_nic]

Feldbezeichnung	Spaltenname
Name	Name
MAC-Adresse	mac_address
IP-Adresse	ip_address
Netzmaske	netmask
Configuration Item	cmdb_ci
Objekt-ID	object_id
MAC-Hersteller	mac_manufacturer
DHCP aktiviert	dhcp_enabled
Status	install_status

Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]

Feldbezeichnung	Spaltenname
VMware vCenter-Datenspeicher	datastore
ESX-Server	esx_server
Zugänglich	accessible
Zugriffsmodus	access_mode

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenspeicher-Datenträger [cmdb_ci_vcenter_datastore_disk]

Feldbezeichnung	Spaltenname
Name	Name
Hersteller	manufacturer
Standort	location
Beschreibung	short_description
Klasse	sys_class_name
Aktualisiert	sys_updated_on
Wartungsplan	maintenance_schedule
Zuordnungs-ID	correlation_id
Datenspeicher	datastore
Status	install_status

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]

Feldbezeichnung	Spaltenname
Name	Name
CPU reserviert (MHz)	cpu_reserved_mhz
CPU limitiert (MHz)	cpu_limit_mhz
CPU Anteile	cpu_shares
Arbeitsspeicher reserviert (MB)	mem_reserved_mb
Arbeitsspeicher limitiert (MB)	mem_limit_mb
Speicheranteile	mem_shares
Objekt-ID	object_id
Server	Server
Verwaltetes Objekt Referenz-ID	morid
Status	install_status

ESX-Server [cmdb_ci_esx_server]

Feldbezeichnung	Spaltenname
Name	Name
Hersteller	manufacturer
Modell-ID	model_id
Betriebssystem	os
BS-Version	os_version
Beschreibung	short_description
Klasse	sys_class_name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ESX-Server [cmdb_ci_esx_server] (Fortsetzung)

Feldbezeichnung	Spaltenname
Status	install_status

Netzwerkadapter [cmdb_ci_network_adapter]

Feldbezeichnung	Spaltenname
Name	Name
Mac-Adresse	mac_address
Netzmaske	netmask
Configuration Item	cmdb_ci
MAC-Hersteller	mac_manufacturer
DHCP aktiviert	dhcp_enabled
Status	install_status

Datenträger [cmdb_ci_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Hersteller	manufacturer
Modell-ID	model_id
Status	install_status

Speicher-HBA [cmdb_ci_storage_hba]

Feldbezeichnung	Spaltenname
Name	Name
Modell-ID	model_id
Computer	Computer
WWNN	wwnn
Status	install_status

Fibre-Channel-Port [cmdb_ci_fc_port]

Feldbezeichnung	Spaltenname
Name	Name
WWNN	wwnn
WWPN	wwpn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre-Channel-Port [cmdb_ci_fc_port] (Fortsetzung)

Feldbezeichnung	Spaltenname
Geschwindigkeit	speed
Controller	controller
Computer	Computer
Status	install_status

iSCSI-Datenträger [cmdb_ci_iscsi_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Bereitgestellt von	provided_by
IQN	iqn
Geräte-LUN	device_lun
Speichertyp	storage_type
Status	install_status

Fibre Channel-Datenträger [cmdb_ci_fc_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Bereitgestellt von	provided_by
Geräte-LUN	device_lun
WWN	wwn
Status	install_status

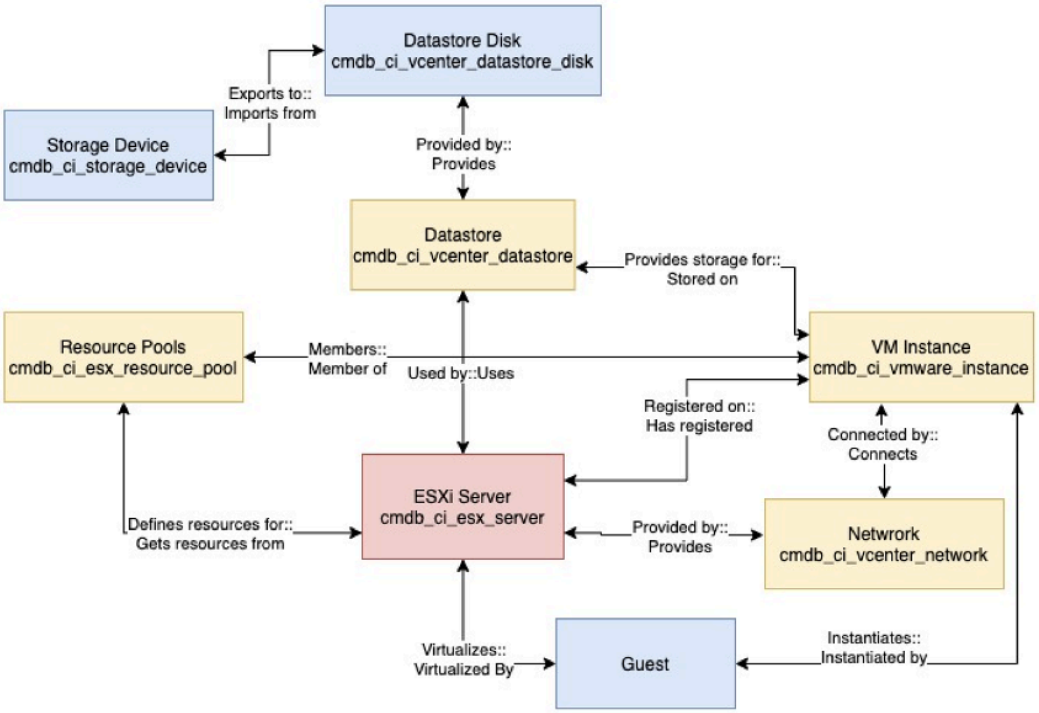
IP-Adresse [cmdb_ci_ip_address]

Feldbezeichnung	Spaltenname
IP-Adresse	ip_address
IP-Version	ip_version
Netzmaske	netmask
Nic	nic
Status	install_status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen

Beziehungen bei der Erkennung eigenständiger ESXi-Server



Ressourcenpools

Bei der Erkennung eigenständiger ESXi-Server werden auch die Ressourcenpools auf dem Host abgerufen, einschließlich des Stammressourcenpools. Dieser Stammressourcenpool ist für jeden ESXi-Host immer ausgeblendet. Der Stammressourcenpool ist im vSphere-Webclient für den ESXi-Host möglicherweise nicht sichtbar, Sie können ihn jedoch mit dem MOB-Browser anzeigen.

Navigieren Sie zu dieser URL: **<domain name/or ip_address>/mob/?moid=ha-root-pool**.

Im Stammressourcenpool werden die Ressourcen des betreffenden Hosts gruppiert. Andere untergeordnete Ressourcenpools können auch aus dem Stammressourcenpool erstellt werden. Der Stamm wird auf dem ESXi-Host anhand der ID des verwalteten Objekts (ha-root-pool) identifiziert.

Zukunftssichere Migration

Wenn Sie die Erkennung eigenständiger ESXi-Server verwendet haben und derselbe ESXi-Server nun mit vCenter verwaltet wird, können Sie stattdessen die vCenter-Erkennung verwenden. Erstellen Sie einen vCenter-Discovery-Zeitplan, und lösen Sie diesen aus. Durch das Auslösen einer vCenter-Erkennung werden doppelte CIs in den folgenden Tabellen erstellt, da für eigenständige ESXi-Server und mit vCenter verwaltete ESXi-Server jeweils unterschiedliche Bezeichner für die betreffenden CIs verwendet werden:

- VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
- ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
- Datenspeicher-Datenträger [cmdb_ci_vcenter_datastore_disk]

Um Duplikate zu vermeiden, müssen Sie die von der Erkennung eigenständiger ESXi-Server erstellten CIs in den obigen vier Tabellen als „Deaktiviert“ markieren. Wenn die vCenter-Erkennung ausgelöst wird, prüft die Skripteinbindung vCenterESXHostsSensor für alle ESXi-Server, ob sie zuvor als eigenständige ESXi-Server erkannt wurden. Wenn ja, wird automatisch das Skript ESXMigrationUtil ausgelöst, sodass alle zuvor erkannten doppelten CIs als deaktiviert markiert werden.

Hinweis: Wenn Sie die Migration manuell auslösen möchten, führen Sie das folgende Skript aus dem Hintergrundskript aus: // @params esx_sys_ids – Array von sys-IDs aller ESXi-Server, die migriert werden müssen.

```
ESXMigrationUtil. retireCIsForESXForwardMigration(esx_sys_ids)
```

Sobald ein ESXi-Server zu vCenter migriert wurde, führt das Auslösen eines Discovery-Zeitplans für die Erkennung eigenständiger ESXi-Server auf demselben ESXi-Host zu einem Fehler. Die Erkennung wird mit einer Fehlermeldung abgebrochen, die besagt, dass dieser ESXi-Server Teil des Discovery-Zeitplans von vCenter <IP-Adresse von vCenter> ist und dass die Erkennung abgebrochen wird.

Virtuelle VMware-Computer

Discovery erfasst Informationen über virtuelle Computer, die von vCenter verwaltet werden.

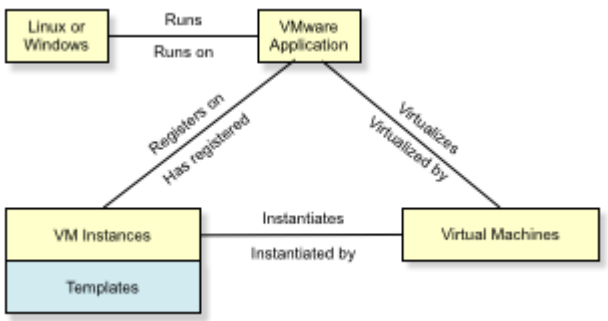
Das Produkt Discovery kann Informationen aus VMware-Konfigurationselements (CIs) extrahieren, einschließlich ihrer Beziehungen. Discovery ist für den gemeinsamen Einsatz mit dem Plugin „Orchestration VMware Support“ konfiguriert, das das automatische Klonen von virtuellen Computern durch einen von vCenter verwalteten ESX-Server ermöglicht. Informationen zu Daten, die von Discovery in vCenter erfasst werden, finden Sie unter Für VMware vCenter-Server erfasste Daten.

VMware-Workstation – Veraltet

Im VMware-Basissystem wird die VMware-Workstation auf einem Windows- oder Linux-Hostcomputer ausgeführt.

Dieses System kann Instanzen aus Vorlagen klonen, lässt sich jedoch nicht automatisieren. Die Beziehungen zwischen VMware-Komponenten für diesen Installationstyp sind im folgenden Diagramm dargestellt:

Beziehungen der VMware-Workstation



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen von Komponenten der VMware-Workstation

Komponente	Beziehungen
Windows- oder Linux-Server	Führt die VMware-Anwendung aus
VMware-Anwendung	• Wird auf einem Windows- oder Linux-Hostcomputer ausgeführt • Besitzt registrierte VM-Instanzen • Virtualisiert virtuelle Computer
VM-Instanzen (einschließlich Images und Vorlagen)	• Wird bei der VMware-Anwendung registriert • Wird von einzelnen virtuellen Computern instanziiert
Virtuelle Computer	• Instanziiert VM-Instanzen • Wird durch die VMware-Anwendung virtualisiert

VM-Instanzstatus- und Statusfelder

Diese Tabellen stellen den Status und den Status von cmdb_ci_vm_instance in verschiedenen Flows wie vCenter dar Discovery Und vCenter-Ereignisse und die Business-Regeln, die ausgelöst werden.

VCenter Discovery Die verschiedene status- und Statusfelder im Zusammenhang mit der VM-Instanz ändern

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
VCenter Discovery	VCenterVMsSensor	Installationsstatus	Deaktiviert	Installiert
VCenter Discovery	VCenterDatacentersSensor	Installationsstatus Status Betriebsstatus	Installiert	Deaktiviert Beendet Nicht funktionsfähig

VCenter-Ereignisse, die verschiedene status- und Statusfelder im Zusammenhang mit der VM-Instanz ändern

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
VCenter-Ereignisse	VCenterVmStateUpdates PowerOnEvtsToUse = [„VmPoweredOffEvent“,	Status „installiert“ Status	Installiert Beliebig	Installiert EIN

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VCenter-Ereignisse, die verschiedene status- und Statusfelder im Zusammenhang mit der VM-Instanz ändern (Fortsetzung)

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
	„VmPowerOffOnIsolationEvent“, „VmShutdownOnIsolationEvent“, „VmSuspendedEvent“],			
VCenter-Ereignisse	PowerOffEvtsToUse = [„VmPoweredOnEvent“, „DrsVmPoweredOnEvent“, „VmRestartedOnAlternateHostEvent“, „VmSuspendedEvent“],	Status = installiert“ Status	Installiert Beliebig	Installiert AUS
VCenter-Ereignisse	SuspendEvtsToUse = [„VmPoweredOnEvent“, „DrsVmPoweredOnEvent“, „VmRestartedOnAlternateHostEvent“, „VmPoweredOffEvent“, „VmPowerOffOnIsolationEvent“]	Status = installiert“ Status	Installiert Beliebig	Installiert Angehalten
VCenter-Ereignisse	VmRemovedEvent	Status „installiert“ Status	Installiert Beliebig	Deaktiviert Beendet

Geschäftsregeln, die verschiedene status- und Statusfelder im Zusammenhang mit der VM-Instanz und dem zugehörigen Server ändern

Business-Regel	Feldname	Plugin-Name
Betriebsstatus an Server kaskadieren	Betriebsstatus	Musterdesigner
Kaskadieren Sie den Betriebsstatus an die VM-Instanz	Betriebsstatus	Musterdesigner
Status der Synchronisierungsvorgänge für CMDB-CI	Betriebsstatus Hardwarestatus Installationsstatus	CMDB

Erkennung von Datenspeicher

Ein Datenspeicher ist ein Speicherobjekt für virtuelle Computer, die auf einem ESXi-Server gehostet werden.

Ein Datenspeicher ist eine Sammlung von mindestens einem physischen Datenträger, zum Beispiel einem iSCSI-Datenträger, die von mehr als einem ESXi-Host verwendet werden kann. Ein physischer Datenträger kann jedoch nur eine Verbindung zu maximal einem Datenspeicher herstellen. Da Datenspeicher von ESXi-Hosts gemeinsam genutzt werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können, lässt sich der virtuelle Computer problemlos zwischen Hosts mit gemeinsamem Datenspeicher verschieben.

Hinweis: Aus der Perspektive eines virtuellen Computers, der an einen Datenspeicher angehängt ist, wird Speicher von einem einzelnen Datenträger bereitgestellt.

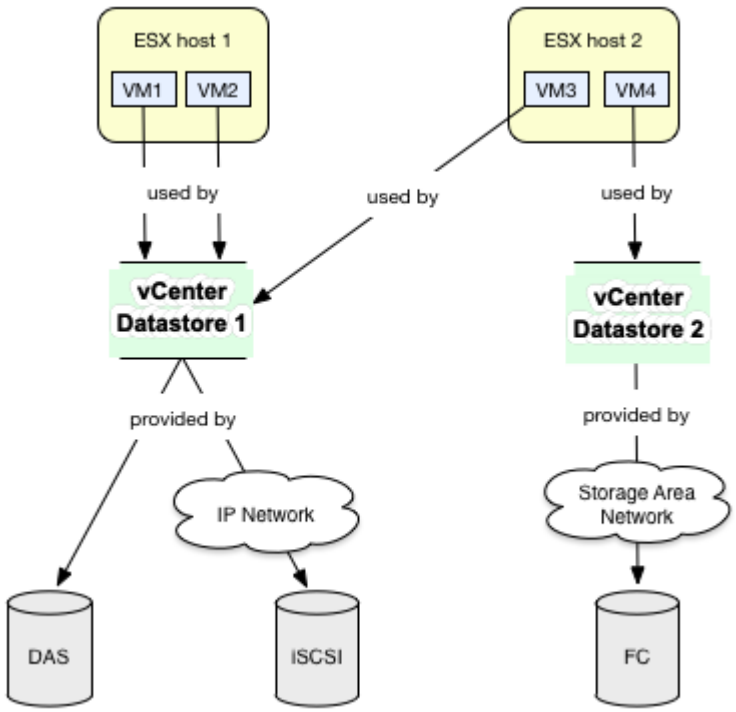
Die Verbindung eines Datenspeichers mit mehreren Datenträgern bietet folgende Vorteile:

- Die Möglichkeit, die Datenträger zum Failover-Schutz zu spiegeln
- Das einfache Hinzufügen von Speicher zum Datenspeicher

Informationen über die Tabellen, die in Discovery zum Speichern der Daten für physische Datenträger und ihrer Beziehung zu Datenspeichern und ESXi-Hosts verwendet werden, finden Sie unter Erkennung von ESXi-Servern.

In dieser Beispielkonfiguration nutzen zwei ESXi-Hosts einen gemeinsamen Datenspeicher, der verschiedene Speichertypen verwendet.

Erkennung von Datenspeicher mit unterschiedlichen Speichertypen



Beziehungen

ServiceNow stellt Tabellen bereit, die die Beziehungen zwischen einem ESXi-Host und seinem Datenspeicher und den spezifischen Datenträgern enthalten, mit denen der Datenspeicher verbunden ist.

ServiceNow Discovery erkennt die Beziehungen zwischen einem Datenspeicher, den mit dem Datenspeicher verbundenen Datenträgern und dem ESXi-Server, auf dem die virtuellen Computer gehostet werden, die diesen Datenspeicher nutzen. Aus der Perspektive des ESXi-Hosts werden iSCSI- und Fibre Channel-Datenträger, die mit dem Datenspeicher verbunden sind, als physische Datenträger behandelt. Discovery zeigt nicht die direkte Beziehung der Speicherdatenträger zum ESX-Host an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Speicher kann auf Computern gehostet werden, die nicht von Discovery erkannt werden. ESXi-Hosts werden über vCenter erkannt, und Speicher wird über CIM separat erkannt. Die Beziehung zwischen beiden kann nur hergestellt werden, wenn der Speicher vor dem ESXi-Host erkannt wird.

Datenspeichertabellen

Tabelle	Beschreibung
cmdb_ci_vcenter_datastore_disk	Speichert die Beziehung des physischen Datenträgers zum Datenspeicher
vcenter_datastore_hostmount	Speichert die Beziehung zwischen dem Datenspeicher und dem ESXi-Server, mit dem er verbunden ist
cmdb_ci_disk	Enthält die physischen Datenträger, die direkt mit dem Datenspeicher verbunden sind Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.
cmdb_ci_fc_disk	Enthält die Fibre Channel-Datenträger in einem Storage Area Network (SAN), das mit dem Datenspeicher verbunden ist Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.
cmdb_ci_iscsi_disk	Enthält die iSCSI-Datenträger in einem IP-Netzwerk, das mit dem Datenspeicher verbunden ist Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.

Erkennung von Windows

Discovery identifiziert und klassifiziert Informationen zu Windows Computer, die IPv4-Adressen, IPv6-Adressen oder beides verwenden.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Hinweis: admin$ Freigabezugriff ist für erforderlich Windows Discovery von Madrid P3 und höher. Eine Remote-Zugriffsrolle muss im Ziel konfiguriert werden Windows Server, um Konnektivität mit ServiceNow Discovery zuzulassen.

Unterstützt Windows Versionen

Für IPv4-Erkennung:

- Windows Workstation 7, 8, 10
- Windows Serverversionen:
  - 2008
  - 2008R2
  - 2012R2
  - 2016
  - 2019
  - 2022
  - 2025

Für IPv6-Erkennung:

- Windows 2019 (10,0,17763)
- Windows Server 2016

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Windows Desktop 10
- Windows 2019 Rechenzentrum

Hinweis: Für Fibre-Channel-Discovery auf einem Windows2008-Host, das Microsoft Fibre Channel-Informationstool (fcinfo.exe) Muss auf diesem Computer installiert sein. Die ausführbare Datei fcinfo muss im Umgebungspfad verfügbar sein. Das Microsoft-Informationstool für Fibre Channel kann unter http://www.microsoft.com heruntergeladen werden.

Einschränkungen der IPv6-Unterstützung

Die folgenden Gerätetypen wurden nicht für die IPv6-Erkennung überprüft:

- Drucker
- Netzwerkspeicher (NFS, CIFS, NAS, FC, ISCSI)
- Virtuelle Azure-Computer (Der native IPv6-Modus wird von Microsoft nicht unterstützt.)

PowerShell-Anforderungen

ServiceNow bietet jetzt Unterstützung für PowerShell 3.0 bis 5.1.

Anmeldeinformationen

Konfigurieren Windows-Anmeldeinformationen . Der in den -Anmeldeinformationen konfigurierte Anwender muss über lokalen Administratorzugriff auf den verfügen Windows Computer.

Die von Ihnen konfigurierten Anmeldeinformationen benötigen:

- Zugriff auf den WMI-Service für den aktuellen Namespace und die untergeordneten Namespaces
- Zugriff auf den Powershell-Service
- Mitgliedschaft in der lokalen Sicherheitsgruppe „Distributed COM-Benutzer“

Klassifizierer, Probes und Muster

Klassifizierungen	Probes	Muster
• Windows • Windows 2008-Server • Windows 2012-Server • Windows 2016-Server • Windows 2025-Server	• Probe „Horizontal Discovery“: Startet Muster • WMIRunner-Windows - Installed Software^ • Multi-Probe-Windows - ADM^ • Windows - Identity* • Windows - Network ARP Table* • Windows - Network NDP Table* • Windows - OS Information*	• Windows OS - Server • Windows OS - Desktops

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierungen	Probes	Muster
	• Windows - Cluster* • Windows - CPU/Memory* • Windows - Installed Software* • Windows - Printers* • Windows - Storage 2008* • Windows - Storage 2012* • Windows - Amazon EC2* • Windows - Azure* • DNS* • SNMP - Routing*	
Windows 2019-Server	N/V	Windows OS - Server

*Diese Probes sind in der Klassifizierung als nicht aktiv Discovery Verwendet standardmäßig Muster für diese Erkennungen.

^diese Probes bleiben standardmäßig aktiv, auch wenn Discovery Verwendet Muster-Discovery.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Bezeichnung	Tabellenname	Feldname	Quelle
Zugewiesen an	cmdb_ci_win_server	assigned_to	wmi
Gehäusetyp	cmdb_ci_win_server	chassis_type	wmi
Befehl	cmdb_running_process	command	wmi
Verbunden mit	cmdb_running_process	connects_to	wmi
Anzahl CPU-Kerne*	cmdb_ci_computer	cpu_core_count	wmi
CPU-Kern-Thread*	cmdb_ci_computer	cpu_core_thread	wmi
CPU-Anzahl*	cmdb_ci_computer	cpu_count	wmi
CPU-Hersteller	cmdb_ci_computer	cpu_manufacturer	wmi
CPU-Name	cmdb_ci_computer	CPU-Name	wmi
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	wmi
Standard-Gateway	cmdb_ci_win_server	default_gateway	wmi
Beschreibung	cmdb_ci_disk	short_description	wmi

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Festplattenspeicher (GB)	cmdb_ci_computer	disk_space	wmi
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	wmi
DHCP-fähig	cmdb_ci_network_adapter	dhcp_enabled	wmi
DNS-Domäne	cmdb_ci_win_server	dns_domain	DNS
Freier Speicherplatz (GB)	cmdb_ci_file_system	free_space	wmi
Hostname	cmdb_ci_win_server	host_name	DNS, NBT
IP-Adresse	cmdb_ci_network_adapter	ip_address	wmi
Lauschen auf	cmdb_running_process	listening_on	wmi
MAC-Adresse	cmdb_ci_network_adapter	mac_address	wmi
Hersteller	cmdb_ci_win_server	manufacturer	wmi
Modell-ID	cmdb_ci	model_id	wmi
Name	cmdb_ci_win_server	Name	DNS, NBT
Name	cmdb_ci_disk	Name	wmi
Name	cmdb_running_process	Name	wmi
Name	cmdb_ci_network_adapter	Name	wmi
Netzmaske	cmdb_ci_network_adapter	netmask	wmi
Betriebssystem	cmdb_ci_computer	os	wmi
BS-Domäne	cmdb_ci_computer	os_domain	NBT
BS-Service Pack	cmdb_ci_computer	os_service_pack	wmi
BS-Version	cmdb_ci_computer	os_version	wmi
Parameter	cmdb_running_process	parameters	wmi
PID	cmdb_running_process	pid	wmi
RAM (MB)	cmdb_ci_computer	ram	wmi
Seriennummer	cmdb_ci_win_server	serial_number	wmi
Kurzbeschreibung	cmdb_ci_win_server	short_description	wmi
Typ	cmdb_ci_disk	Typ	wmi

* Die Angaben für Anzahl der Kerne und Threads pro Kern sind aufgrund von Problemen mit der Microsoft-Berichterstellung möglicherweise nicht genau.

** Der Wert im Feld **disk_space** ist eine Zusammenfassung der Gesamtkapazität (einschließlich belegtem Platz) für alle nicht entnehmbaren Festplatten, einschließlich Direct Attached Storage und SAN-Speicher.

Windows-Registrierung

Discovery Kann Software finden, die auf einem Windows-Computer installiert wurde, indem Sie sich die Windows-Registrierung ansehen. Discovery Kann die folgenden Attribute der erkannten Software finden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Produktname**: Kombination aus Name und Version, zum Beispiel Windows Imaging Component 3.0
- **Name**: Name des Produkts ohne Version
- **Version**: Version des Produkts
- **Deinstallationszeichenfolge**: Pfad zum Deinstallationsprogramm, zum Beispiel C:\Programme\Notepad ++\uninstall.exe.
- **Teil von**: Update, von dem dies ein Teil ist, zum Beispiel Windows Internet Explorer 8 - Software Update
- **Installationsdatum**: Datum, an dem die Software installiert wurde Der Sensor „Windows - Installierte Software“ wendet einen Zeitstempel von 00:00:00 auf den in der Registrierung abgerufenen Wert „install_date“ ab. Die Installationszeit aller Windows Software ist unabhängig von der Zeitzone und wird auf Mitternacht des Tages festgelegt, an dem sie installiert wurde. Zum Beispiel ein Installationsdatum von **2.19.2017** In Windows Registrierung wird als angezeigt **2.19.2017 00:00:00** In CMDB.
- **Installiert auf**: Name des Asset, auf dem die Software installiert ist

Zugehörige Informationen

Windows Probes und Berechtigungen

Windows Server-Cluster-Discovery

Discovery Stellt die Beziehungen zwischen her Windows Servercluster und seine Knoten.

Wenn ein Windows Server gefunden, und Discovery Erkennt, dass es Teil eines Clusters ist, startet das System die Windows-Cluster-Probe. Navigieren zu **Discovery-Definition** > **Probes** Und öffnen Sie den Datensatz für die Windows – Cluster-Probe, um die spezifischen Daten anzuzeigen, die Discovery erfasst.

Hinweis: Discovery Sammelt Clusterressourcen basierend auf der WMI-Klasse MSCluster_ResourceType. Eine Liste der standardmäßigen Clusterressourcen finden Sie unter Ressourcentypen . Informationen zum Zusammenhang von Clusterressourcen mit Prozessklassifizierern finden Sie unter Prozessklassifizierer mit Windows-Clusterressourcen verknüpfen.

Clusterdatentabellen

Discovery Erstellt CIs für Cluster in diesen Tabellen:

- Windows Cluster [cmdb_ci_WIN_Cluster]
- Windows Clusterressource(n) [cmdb_ci_win_Cluster_resource]
- Windows Clusterknoten [cmdb_ci_win_Cluster_node]
- Clusterknotenressourcen [cmdb_ci_cluster_node_resource]
- Virtuelle IPs des Clusters [cmdb_ci_cluster_vip]

Clusterbeziehungen

Discovery erstellt für jeden Knoten einen CI-Beziehungsdatensatz [cmdb_rel_ci] mit den folgenden Beziehungen:

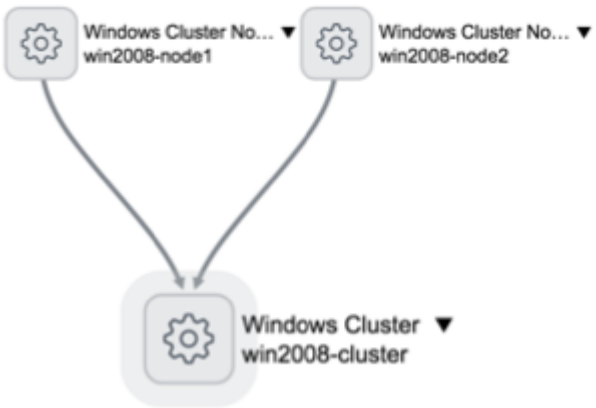
- **Cluster von::Cluster**: Beziehung zwischen den Clusterknoten und dem Cluster. Service Mapping verwendet diese Beziehung, um das Windows-Cluster und seine Knoten zuzuordnen.
- **Mitglieder::Mitglied von**: Beziehung zwischen dem Cluster und dem Clusterknoten

Automatische Übersetzung

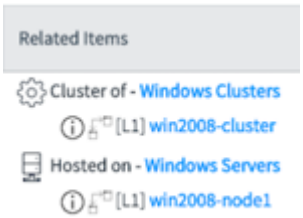
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Gehostet auf::Hostet**: Beziehung zwischen den Clusterknoten und dem Windows-Server
- **Verwendet::verwendet von** : VirtualIP-Cluster und Windows-Clusterknoten.
- **Definiert Ressourcen für::ruft Ressourcen ab** : Windows Clusterressourcen und Windows Cluster.
- **Definiert Ressourcen für::ruft Ressourcen ab** : Windows Clusterressourcen und Windows Clusterknoten.

Windows Clusterzuordnung



Windows Clusterknoten-Beziehungen



Clusterreferenzen

Discovery erstellt die folgenden Clusterreferenzen:

- Von Windows Clusterknoten, die dem zugeordnet sind Windows Cluster.
- Von Windows Clusterressourcen, die dem zugeordnet sind Windows Cluster.
- Von virtuellen Cluster-IPs zu zugehörigem Windows Cluster.
- Von Clusterknotenressourcen zu zugehörigem Windows Clusterknoten.
- Von virtuellen Cluster-IPs zu zugehörigem Windows Clusterknoten.

Hinweis: Referenzen werden in verwaltet Discovery Um Abwärtskompatibilität für Systeme bereitzustellen, die sie verwenden.

z/OS-Erkennung

Discovery sucht nach Computern, auf denen das Betriebssystem z/OS ausgeführt wird.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen

Unter z/OS muss an Port 22 der USS-Service ausgeführt werden.

Die folgenden Befehle können auf dem Hostcomputer ausgeführt werden:

- uname
- hostname
- sysvar SYSNAME
- netstat
- df
- ls
- cat
- grep
- ps
- cut

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Anmeldeinformationen

Erstellen SSH-Anmeldeinformationen .Der Anwender muss über Schreibberechtigung für verfügen `/Tmp` , Haben Lesezugriff auf alle Anwenderprozesse und können REXX-Skripts ausführen.

Klassifizierer, Probe und Muster

Klassifizierung	Auslöser-Probe	Muster
IBM z/OS	Horizontal Pattern: Startet Muster	IBM zOS Server

Erfasste Daten

Discovery füllt die Tabelle „IBM zOS-Server“ [cmdb_ci_ibm_zos_server] mit folgenden Informationen:

Bezeichnung	Feldname
Name	Name
BS-Version	os_version
Betriebssystem	os
Hersteller	manufacturer
Seriennummer	serial_number

Virtualisierungs-Discovery auf Betriebssystemebene

Discovery Kann Image- und Containerinformationen aus Virtualisierungs-Engines auf Betriebssystemebene (Virtualisierung auf Betriebssystemebene) erfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery kann Containerstatus und -größe bestimmen sowie Images und deren Tags identifizieren, die durch Virtualisierung auf Betriebssystemebene bereitgestellt werden.

Hinweis: Derzeit unterstützt die ServiceNow® Platform nur die Erkennung von Docker-Virtualisierungscontainern.

Tabellenschema

Tabelle	Beschreibung
cmdb_ci_oslv_engine	Basistabelle für alle OSLV-Engines
cmdb_ci_oslv_image	Basistabelle für global eindeutige OSLV-Images
cmdb_ci_oslv_local_image	Basistabelle für lokale Instanzen von OSLV-Images
cmdb_ci_oslv_image_tag	Basistabelle für Tags in OSLV-Images
cmdb_ci_oslv_container	Basistabelle zum Speichern von auf dem Host gefundenen Containern

Erfasste Daten

Tabelle	Felder
Virtualisierungs-Engine auf Betriebssystemebene [cmdb_ci_oslv_engine]	Server [Server]
Virtualisierungs-Image auf Betriebssystemebene [cmdb_ci_oslv_image]	• Image-ID [image_id] • Image-Auszug [image_digest] • Image erstellt [image_created_at] • Größe (Byte) [size_bytes]
Lokales Image der Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_image]	Image-ID [image_id]
Image-Tag für Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_image_tag]	• Image-ID [image_id] • Repository [repository] • Tag [tag]
Container der Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_container]	• Container-ID [container_id] • Status [status] • Größe (Byte) [size_bytes] • Image-ID [image_id]

Docker-Virtualisierung

Discovery verwendet das *Docker Pattern*, um Daten über bestimmte Objekte in einer Docker-Engine zu erfassen, die auf einem Linux-Host ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ServiceNow® Platform unterstützt die Erkennung von Docker Release 1.11.0 oder höher.

Discovery führt den Prozessklassifizierer „Docker Engine“ im Netzwerk aus. Wenn der Klassifizierer den Prozess **dockerd** oder **docker daemon** identifiziert, löst der Klassifizierer die Probe „Horizontal Pattern“ (HorizontalDiscoveryProbe) aus, die das Muster „Docker“ startet und mit dem Erfassen von Daten aus Docker-Komponenten beginnt.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Voraussetzungen

Benutzerrechte

Der Benutzer, dessen Anmeldeinformationen zum Ausführen der Docker Discovery verwendet werden, muss über Berechtigungen verfügen, die mit einer der folgenden Methoden definiert wurden:

- Erteilen Sie einem Benutzer erweiterte Rechte für die Ausführung von Befehlen, da der Docker-Daemon als Root-Benutzer ausgeführt wird. Das Docker-Muster unterstützt die Verwendung von Privilegierte Befehle , Z. B. *sudo*Oder *pbrun*, Um als Stammanwender auszuführen.
- Zuweisung zu einer Gruppe mit dem Namen **docker**, die über besondere Berechtigungen zum Ausführen von Docker-Befehlen verfügt. Anweisungen zum Einrichten einer Gruppe finden Sie in der Dokumentation zu Docker .

Neueste Muster

Stellen Sie die aktuelle Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store bereit.

Einschränkungen und Überlegungen für Docker

Beachten Sie bei Verwendung der Docker-Virtualisierung Folgendes:

- Der erste Prozess-Scan von Discovery kann eine Anwendung in einem Container identifizieren und korrekt klassifizieren. Nachfolgende Probes, die gestartet werden, um die Anwendung zu untersuchen, können jedoch nicht in den Container sehen und keine Details zur Anwendung zurückgeben.
- Discovery durchsucht alle gefundenen Container, einschließlich inaktiver Container. Dadurch kann Discovery verlangsamt werden. Daher sollten Sie nicht ausgeführte Container löschen.
- Vor der Einstellung *sn_itom_pattern.manifest_digest_image_ID* Eigenschaft bis **Wahr** Und Discovery wird ausgeführt: Duplikate verhindern Docker Datensätze, die durch Löschen aller erstellt werden Docker Bilddatensätze.
- Pro (physischem oder virtuellem) Computer ist nur eine Docker-Engine zulässig.

Von Discovery während der horizontalen Erkennung erfasste Daten

Zusätzlich zu den aus den übergeordneten OSLV-Tabellen abgeleiteten Attributen werden die folgenden Attribute erkannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Felder	Beschreibung
Docker-Engine [cmdb_ci_docker_engine]	
Name [name]	Speichert Informationen zu Instanzen der Docker-Engine.
BS-Arch [os_Arch]	
GIT-Commit [git_commit]	
Build-Datum [Build_date]	
Version [version]	
API-Version [api_Version]	
Go-Version [Go_Version]	
Ist geclustert [is_clustered]	
Prozess wird ausgeführt [running_Process]	
Prozessbefehl wird ausgeführt [running_Process_command]	
Schlüsselparameter für laufenden Prozess [running_Process_key_Parameters]	
Docker-Image [cmdb_ci_docker_image]	
Name [name]	Speichert Informationen zur global eindeutigen Darstellung von Docker-Images.
Image-ID [image_id]	
Image-Auszug [image_digest]	
Größe (Byte) [size_byte]	
Bild erstellt [Image_created_at]	
Lokales Docker-Image [cmdb_ci_docker_image]	
Name [name]	Speichert lokale Instanzen von Docker-Images
Image-ID [image_id]	
Docker-Image-Tag [cmdb_ci_docker_image_tag]	
Name [name]	Speichert Tags aus lokalen Docker-Images
Image-ID [image_id]	
Repository [repository]	
Tag [tag]	
Docker-Container [cmdb_ci_docker_container]	
Name [name]	Speichert Docker-Container, die auf dem Host gefunden wurden In Fällen, in denen doppelte Datensätze erstellt werden, werden Deduplizierungsaufgaben angezeigt, sobald die Discovery ausgeführt wird. Informationen zur Lösung dieser Aufgaben finden Sie unter Docker-Container-Bezeichner
Image-ID [image_id]	
Container-ID [container_id]	
Größe (Byte) [size_bytes]	
Befehl [command]	
Container erstellt [container_created_at]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Felder	Beschreibung
Status [status]	unabhängig machen [KB1443042] artikel in ServiceNow® Knowledge Base.

Diese Informationen werden vom Erweiterungsabschnitt *`Collect Container Repository`* erkannt.

Tabelle und Feld	Beschreibung
Container-Repository [cmdb_ci_container_repository]	
Name [name]	Der Name des Container-Repositorys.
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	
Name [name]	Der Name des Container-Repository-Eintrags.
Kategorie [category]	Die Kategorie des Container-Repository-Eintrags.

CI-Beziehungen

Die folgenden Beziehungen zwischen erkannten CIs werden vom Docker-Muster identifiziert.

CI	Beziehung	CI
cmdb_ci_server	Runs::Runs On	cmdb_ci_docker_engine
cmdb_ci_docker_engine	Manages::Managed By	cmdb_ci_docker_container
cmdb_ci_docker_engine	Verwaltet::Verwaltet Bis	cmdb_ci_docker_local_image
cmdb_ci_docker_image	Instanziiert::Instanziiert Bis	cmdb_ci_docker_container
cmdb_ci_docker_local_image **Hinweis:** Die Richtung dieser Beziehung ist für alle Store-Versionen vor 1,0.99, Februar 2023 umgekehrt.	Instanziiert::Instanziiert Bis	cmdb_ci_docker_container
cmdb_ci_docker_image_tag	Registriert Am::Hat Registriert	cmdb_ci_docker_local_image
cmdb_ci_docker_local_image	Instantiates::Instantiated By	cmdb_ci_docker_image

Der Erweiterungsabschnitt *`Collect Container Repository`* des Docker-Musters identifiziert diese Beziehungen.

CI	Beziehung	CI
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizierungs-, Containment- und Hosting-Regeln

Discovery verwendet für die Suche nach der Docker-Engine einen Bezeichner für Anwendungsregeln und wendet dann andere Regeln an, um bestimmte Docker-Objekte zu identifizieren.

Bezeichner für Anwendungsregeln

Das System erstellt während der Prozessklassifizierung das Konfigurationselement (CI) cmdb_ci_docker_engine. Darauf aufbauend, verwendet Discovery den Bezeichner der Anwendungsregel in der Anwendungstabelle [cmdb_ci_appl], um die spezifische Docker-Engine zu identifizieren. Nach der Herstellung dieser Identität verwendet Discovery die Beziehungen, die in den Containment- und Hosting-Regeln definiert sind, um die einzelnen CIs der Docker-Komponente, die zu dieser Engine gehören, genau zu erstellen und zu aktualisieren.

Kennungen

Name	Tabelle	Attribute
Docker-Container	Docker-Container [cmdb_ci_docker_container]	container_id
Globales Docker-Image	Docker-Image [cmdb_ci_docker_image]	image_id
Lokales Docker-Bild	Lokales Docker-Image [cmdb_ci_docker_image]	image_id
Docker-Bild-Tag	Docker-Image-Tag [cmdb_ci_docker_image_tag]	Repository, Tag

Containment- und Hosting-Regeln

Docker-Discovery verwendet diese Erstellen oder bearbeiten Sie eine Sammlung von Containment-Regeln Und Erstellen oder bearbeiten Sie eine Sammlung von Hosting-Regeln Regeln zum Erstellen von Konfigurationselementen (CI) aus der Datenretur n ed nach dem Docker-Muster. Nachdem Discovery die Docker-Engine anhand ihrer Beziehung zur Anwendungstabelle [cmdb_ci_appl] identifiziert hat, werden diese Regeln angewendet, um die spezifischen CIs, die mit dieser Engine verbunden sind, anhand ihrer Beziehungen zueinander zu identifizieren. Indem die Komponenten auf diese Weise (von der Anwendung nach unten, ausgehend von der Engine) verbunden werden, verhindert Discovery, dass doppelte CIs für Komponenten aus anderen Docker-Engines erstellt werden, die denselben Namen oder dieselbe image_id aufweisen.

Containment-Regel

Übergeordnet	Untergeordnetes Element	Beziehung
Lokales Docker-Bild	Docker-Bild-Tag	Hat sich registriert

Hosting-Regeln

Übergeordnet	Untergeordnetes Element	Beziehung
Docker-Container	Docker-Engine	Verwaltet von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hosting-Regeln (Fortsetzung)

Übergeordnet	Untergeordnetes Element	Beziehung
Lokales Docker-Bild	Docker-Engine	Verwaltet von

Erkennung von Software

Discovery identifiziert mehrere Arten von Software.

Erkennung des Active Directory-Domänencontrollers

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet den Active Directory-Domänencontroller im Windows-Muster, um Active Directory-Domänencontroller zu finden, die auf einem ausgeführt werden Windows Server. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Active Directory-Domänencontrollers auf Windows-Muster.

Active Directory-Domänencontroller [cmdb_ci_ad_controller]

Bezeichnung	Feldname
Name	name
Domänenname	domain_name
Domänencontrollername	Domain_Controller_Name
Forest-Name	Forest_Name
Klasse	sys_class_name
TCP-Port(s)	tcp_port

Adobe JRun-Discovery

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von erkannt wird Adobe JRun.

Standardmäßig verwendet Discovery das Muster `Jrun`, um Discovery auszuführen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Privilegierte Befehle

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Adobe JRun erfasste Daten

In der JRun-Tabelle [cmdb_ci_app_server_jrun] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Installationsverzeichnis	install_directory
Konfigurationsverzeichnis	config_directory
Konfigurationsdatei	config_file

Apache Webserver-Discovery

Discovery Identifiziert und klassifiziert Informationen zu Apache Webserver auf beiden Windows Und Linux Computer.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Apache-Server	• Probe „Horizontal Discovery“: Startet Muster • Apache - Version* • Apache - Get Configuration* • Apache - Get JK ModuleApache - Get Proxy Module*	• Apache On Windows • Apache On Unix

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Mit Probes erfasste Daten

Für Unix und Windows erfasst Discovery in der Apache-Tabelle [cmdb_ci_apache_web_server] die folgenden Daten:

Bezeichnung	Feldname
Name	Name
Version	Version
Beschreibung	Beschreibung
TCP-Port(s)	tcp_port

Verbindungen, die von Service-Mapping während der Erkennung von oben nach unten gefunden werden

Service-Mapping verwendet Erkennungsmuster, um die folgenden Verbindungen zu erkennen:

- Alle Anwendungen, die Java verwenden
- Alle Anwendungen, die den LDAP-Port verwenden
- Oracle WebLogic-Modul und Oracle WebLogic Server (Version 10.3)
- (Nur unter Windows) Jiva-Anwendungen
- (Nur unter Windows) Tomcat-Server
- (Nur unter UNIX) Mit dem mod_jk-Prozess erkannte Anwendungen
- (Nur unter UNIX) Hosts, zu denen der Apache-Webserver eine Verbindung im Lastenausgleichsmodus herstellt
- (Nur unter UNIX) Anwendung Epic

Apache mod_JK- und mod_Proxy-Discovery

Discovery Verwendet SSH, um zu finden Apache Connectors mod_jk und mod_Proxy.

Discovery Verwendet **Unix: Aktive Prozesse** Probe zum Identifizieren von Apache Webserverprozess durch Übereinstimmung mit einem der folgenden Kriterien **Name** Des Prozesses ist:

- `httpd` oder
- `apache` oder
- `httpd2` oder
- `httpd2-prefork`
- `httpd.worker`

Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Tabelle „Webserver“ [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Webserver-Probes

Probe	Beschreibung	Befehle
Apache – Version	Der Sensor dieser Probe füllt den aus Apache Versionsinformationen im Webserver-Datensatz.	httpd
Apache – Get Configuration	Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad von bestimmt Apache Konfigurationsdatei. Der Sensor dieser Probe fügt dem Webserver-Datensatz einige zusätzliche Informationen hinzu.	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Die Sensorverarbeitung der Probe **Apache - Get Configuration** gibt an, ob die Module mod_jk und mod_proxy vorhanden sind, und löst die entsprechende Probe aus.

Apache Modul-Probes

Probe	Beschreibung	Befehle
Apache – Get JK Module	Wenn das Modul mod_jk als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Get Proxy Module	Wenn das Modul mod_proxy als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.	grep, egrep (im Bourne-Shell-Skript)

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden vom Datensatz der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool_member sind Mitglieder der Tabelle cmdb_ci_lb_pool.

Veraltet: Sudo-Zugriff für die Probe „Unix - Active Processes“ hinzufügen

Für einen Apache-Webserver erfordert die Probe „Unix - Active Processes“ Sudo-Berechtigungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Probe „Unix - Active Processes“ zum Erweitern von Berechtigungen konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Probes**an.
2. Suchen Sie im Feld **Suche** nach „Unix - Active Processes“.
3. Klicken Sie in das Feld, und suchen Sie nach „Unix - Active Processes“.
4. In **Probe-Parameter** Zugehörige Liste, klicken Sie auf **Neu** .
5. Klicken Sie auf **Neu**.
6. Verwenden Sie die folgenden Informationen, um das Formular auszufüllen:

Probe	Befehle
Name	must_sudo
Wert	Wahr

7. Klicken Sie auf **Absenden**.

Vom Modul mod_jk erfasste Daten

Das Apache-Modul mod_jk leitet Anforderungen vom Apache-Webserver an einen Servlet-Container wie Tomcat weiter.

Zusätzliche mod_jk-Direktiven können auch den Lastenausgleich verwalten. Discovery füllt die CMDB, wenn ein Apache-Server erkannt wird. Wenn der Prozess des Apache-Webservers erkannt wird und das Modul mod_jk auf dem Webserver als Lastenausgleichsmodul ausgeführt wird, werden die zugehörigen Informationen in die CMDB eingetragen.

- Das MID Server-Benutzerkonto zum Untersuchen des Zielservers muss Zugriff auf die Konfigurationsdatei httpd.conf im Ordner /etc/httpd/conf/ haben.
- Discovery verwendet SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - Apache Get Configuration
  - Apache Version
  - Apache Get JK Module
- Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Probes, die Ausführungsberechtigungen erfordern

Probe	Befehl
Apache – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Version	httpd
Apache – Get JK Module	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Sonden und Sensoren

Discovery verwendet die Probe „Unix - Active Processes“, um einen Apache-Server zu identifizieren, der das Modul mod_jk enthält:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Die Probe „Unix – Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet httpd.
   - Der Name des Prozesses lautet apache.
2. Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Webserver-Tabelle [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist. Die folgenden Sonden werden ebenfalls aktiviert:
   - Apache – Version: Der Sensor dieser Probe fügt dem Webserver-Datensatz die Apache-Versionsinformationen hinzu.
   - Apache – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der Apache-Konfigurationsdatei bestimmt. Der Sensor dieser Probe fügt dem Webserver-Datensatz einige zusätzliche Informationen hinzu.
3. Die Sensorverarbeitung der Probe „Apache - Get Configuration“ löst die folgenden Probes aus, wenn das Modul mod_jk auf dem Webserver ausgeführt wird:

   Apache – JK Module: Wenn das Modul mod_jk als Lastenausgleichsmodul auf dem Server ausgeführt wird, füllt der Sensor dieser Probe die Informationen in den Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member].

Erfasste Daten

Für das Modul mod_jk ohne Lastenausgleichsmodul werden standardmäßig die folgenden Daten erfasst:

Von Discovery standardmäßig erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_web_server	Name [name]	Apache – Get Configuration
cmdb_ci_web_server	Version [version]	Apache – Version
cmdb_ci_web_server	Beschreibung [short_description]	Apache – Version

Wenn das Modul mod_jk für den Lastenausgleich aktiviert ist, verknüpft Discovery die folgenden Daten:

Von Discovery erfasste Daten, wenn das Modul mod_jk als Lastenausgleichsmodul identifiziert wird

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_appl	Name [name]	Apache – Apache - Get JK Module
cmdb_ci_lb_appl	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_appl	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Name [name]	Apache – Apache - Get JK Module

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery erfasste Daten, wenn das Modul mod_jk als Lastenausgleichsmodul identifiziert wird (Fortsetzung)

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_pool_member	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Port [port]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Eingabe-URL [Input_url]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Name [name]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Port [port]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Lastenausgleichsmethode [load_balancing_method]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Name [name]	Apache – Apache - Get JK Module

Beziehungen

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden vom Datensatz der Tabelle cmdb_ci_service verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool.

Vom Modul mod_proxy erfasste Daten

Das Apache-Modul mod_proxy implementiert einen Proxy, ein Gateway oder einen Cache für den Apache-Webserver.

Ein zusätzlicher mod_proxy_balancer kann den Lastenausgleich ebenfalls verwalten. Discovery füllt die CMDB, wenn ein Apache-Server erkannt wird. Wenn der Prozess des Apache-Webservers erkannt wird und das Modul mod_proxy auf dem Webserver als Lastenausgleichsmodul ausgeführt wird, werden die zugehörigen Informationen in die CMDB eingetragen.

Beachten Sie die folgenden Anforderungen für die Erkennung eines Apache-Servers, der das Modul mod_proxy enthält:

- Das MID Server-Benutzerkonto zum Untersuchen des Zielservers muss Zugriff auf die Konfigurationsdatei [httpd.conf] im Ordner /etc/httpd/conf/ haben.
- Discovery verwendet SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - Apache Get Configuration
  - Apache Version
  - Apache Get Proxy Module
- Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Vom Modul mod_jk erfasste Daten

Probe	Befehle
Apache – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Get Proxy Module	grep, egrep (im Bourne-Shell-Skript)
Apache – Version	httpd

Sonden und Sensoren

Discovery verwendet die Probe „Unix - Active Processes“, um einen Apache-Server zu identifizieren, der das Modul mod_proxy enthält: Die Probes und Sensoren funktionieren wie folgt:

1. Die Probe „Unix – Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet httpd.
   - Der Name des Prozesses lautet apache2.
2. Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Webserver-Tabelle [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist. Die folgenden Sonden werden ebenfalls aktiviert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Apache – Version: Der Sensor dieser Probe fügt dem Webserver-Datensatz [cmdb_ci_web_server] die Apache-Versionsinformationen hinzu.
- Apache – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der Apache-Konfigurationsdatei bestimmt. Der Sensor dieser Probe fügt dem Webserver-Datensatz [cmdb_ci_web_server] einige zusätzliche Informationen hinzu.

3. Die Sensorverarbeitung der Probe „Apache - Get Configuration“ löst die folgenden Probes aus, wenn das Modul mod_proxy auf dem Webserver ausgeführt wird:

   Apache - Get Proxy Module: Wenn das Modul mod_proxy als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.

Erfasste Daten

Für das Modul mod_proxy ohne Lastenausgleichsmodul werden standardmäßig die folgenden Daten erfasst:

Von Discovery standardmäßig erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_web_server	Name [name]	Apache – Get Configuration
cmdb_ci_web_server	Version [version]	Apache – Version
cmdb_ci_web_server	Beschreibung [short_description]	Apache – Version

Wenn das Modul mod_proxy für den Lastenausgleich aktiviert ist, verknüpft Discovery die folgenden Daten:

Von Discovery erfasste Daten, wenn das Modul mod_proxy als Lastenausgleichsmodul identifiziert wird

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_appl	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_appl	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Name [name]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Port [port]	Apache - Get Proxy Module

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery erfasste Daten, wenn das Modul mod_proxy als Lastenausgleichsmodul identifiziert wird (Fortsetzung)

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_service	Eingabe-URL [Input_url]	Apache - Get Proxy Module
cmdb_ci_lb_service	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_service	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_service	Name [name]	Apache - Get Proxy Module
cmdb_ci_lb_service	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_service	Port [port]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Lastenausgleichsmethode [load_balancing_method]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Name [name]	Apache - Get Proxy Module

Beziehungen

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Datensätze der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool_member sind Mitglieder der Datensätze der Tabelle cmdb_ci_lb_pool.

Anwendungszuordnung für UNIX Discovery

Für die Zuordnung, mit der die Anwendungsbeziehungen hergestellt werden, muss Discovery in der Lage sein, TCP-Verbindungen zu erkennen.

Dies lässt sich am besten erreichen, indem auf Zielcomputern der Befehl lsof ausgeführt wird. Für AIX-Computer ist Discovery so konfiguriert, dass die Probe für aktive Verbindungen für AIX-Ziele verwendet wird. Der Benutzer, der das Shell-Skript auf AIX-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Computern ausführt, benötigt jedoch möglicherweise zusätzliche Berechtigungen, um im Skript verwendete Befehle wie kdb auszuführen.

Auf Linux-Computern verwendet Discovery zum Erkennen von TCP-Verbindungen den (unter Linux standardmäßig installierten) Befehl lsof. Die Linux-Klassifizierungs-Probe löst die Probe „Linux - Active Connections“ aus, der lsof zum Erkennen von Anwendungsbeziehungen verwendet und keine Unterbrechungen verursacht. Der Befehl lsof stellt die empfohlene Methode zur Rückgabe aktiver TCP-Verbindungen dar. Er kann auf Solaris- und AIX-Zielcomputern installiert werden, um alle durch das Shell-Skript verursachten Probleme zu beheben.

Hinweis: Discovery aktiver Verbindungen auf HP-UX Wird nicht unterstützt.

lsof-Befehl verwenden

Verwenden Sie den lsof-Befehl, um aktive TCP-Verbindungen zurückzugeben. Er kann auf Solaris- und AIX-Zielcomputern installiert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

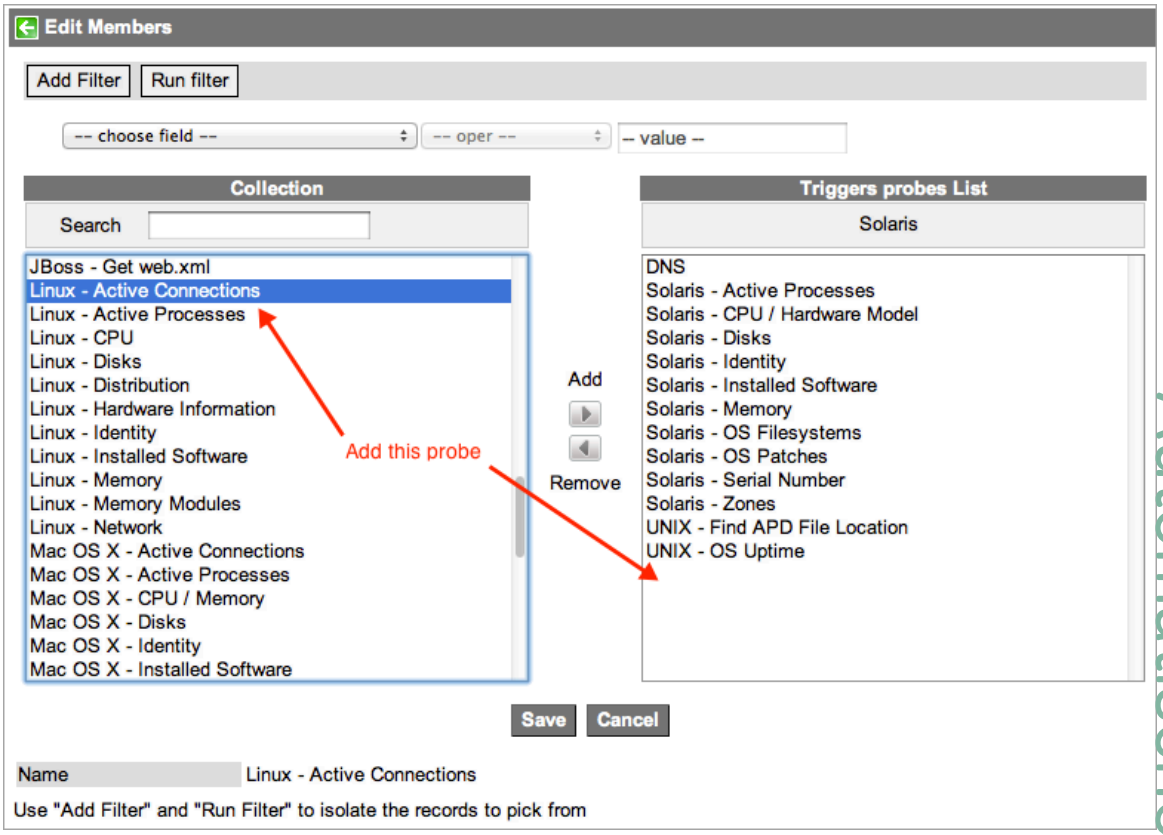
Prozedur

1. Installieren Sie lsof auf den Solaris- und AIX-Computern, auf denen Sie Daten über Anwendungsbeziehungen erfassen möchten.
2. Navigieren Sie in der -Instanz zu **Discovery-Definition** > **CI-Klassifizierung** > **UNIX**an.
3. Wählen Sie aus der Liste **Solaris** aus.
4. Wählen Sie im Formular „UNIX-Klassifizierung“ für Solaris die zugehörige Liste **Auslösertests** aus, und klicken Sie dann auf **Bearbeiten**.
5. Verschieben Sie **Linux - Active Connections** aus der Liste „Sammlungen“ in die Liste „Löst Probe aus“. Diese Probe ist für die Verwendung von lsof konfiguriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example

Solaris Active Connections lsof



6. Klicken Sie auf **Speichern**.
7. Wiederholen Sie dieses Verfahren für die AIX-Klassifizierung-Probe.

Citrix Discovery von Lizenzserver und Delivery Controller

Discovery kann finden Citrix Lizenzserverinstanzen und Delivery Controller-Komponenten, die auf ausgeführt werden Windows Computer.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anforderungen

- Konfigurieren Sie die Windows-Anmeldeinformationen , um auf den Hostcomputer zuzugreifen.
- Stellen Sie sicher, dass PowerShell für Discovery auf Ihren MID Servern installiert ist. Für die für die Citrix-Discovery verwendeten Muster müssen PowerShell-Befehle ausgeführt werden können.
- Für Betriebssystembenutzer müssen Sie „Get-XDSite“ ausführen. Der Citrix Studio-Administrator muss Berechtigungen erteilen.
- (Optional) Für die Top Down-Discovery mit Service-Mapping installieren Sie auf dem Citrix Delivery Controller das Modul Citrix.Broker.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Optional) Für die Top Down-Discovery mit Service-Mapping, erstellen Sie einen Benutzer mit Berechtigung zum Ausführen von PowerShell-Befehlen.
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Muster

Zur Ausführung einer horizontalen Erkennung verwendet Discovery die folgenden Muster:

Muster	Erkannter Prozess
Citrix Lizenzserver	lmadmin.exe
Delivery Controller	BrokerService

Erfasste Daten und Beziehungen

Tabelle	Felder
Citrix-Lizenzserver [cmdb_ci_appl_license_server]	Name [name] TCP-Ports [tcp_port] Betriebsstatus [operational_status]
Citrix Delivery Controller [cmdb_ci_appl_delivery_controler]	Name [name] Version [version] TCP-Ports [tcp_port] Betriebsstatus [operational_status]

CI	Beziehung	CI
Citrix-Lizenzserver [cmdb_ci_appl_license_server]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]
Citrix Delivery Controller [cmdb_ci_appl_delivery_controler]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]

Discovery der geclusterten Anwendung auf Windows

Ein Prozess und die entsprechenden Ressourceninformationen können verwendet werden, um zu bestimmen, ob es sich bei einem Prozess um einen geclusterten Prozess handelt.

Der Prozessklassifizierer **Microsoft SQL Server** im Lieferumfang Ihrer Instanz identifiziert geclusterte SQL-Server. Mit demselben Verfahren können Sie mithilfe von Discovery unter Windows auch andere geclusterte Anwendungen erkennen.

Um zu erkennen Windows Geclusterte Anwendungen mit Discovery, Erstellen Sie eine Prozessklassifizierung, die erkennt, ob ein Prozess ein gruppierter Prozess ist. Führen Sie die nachfolgenden Schritte durch:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer für geclusterte Prozesse erzeugen

Erstellen Sie zum Erkennen von geclusterten Windows-Anwendungen einen Prozessklassifizierer für diesen CI-Typ.

Vorbereitungen

Erforderliche Rolle: discovery_admin

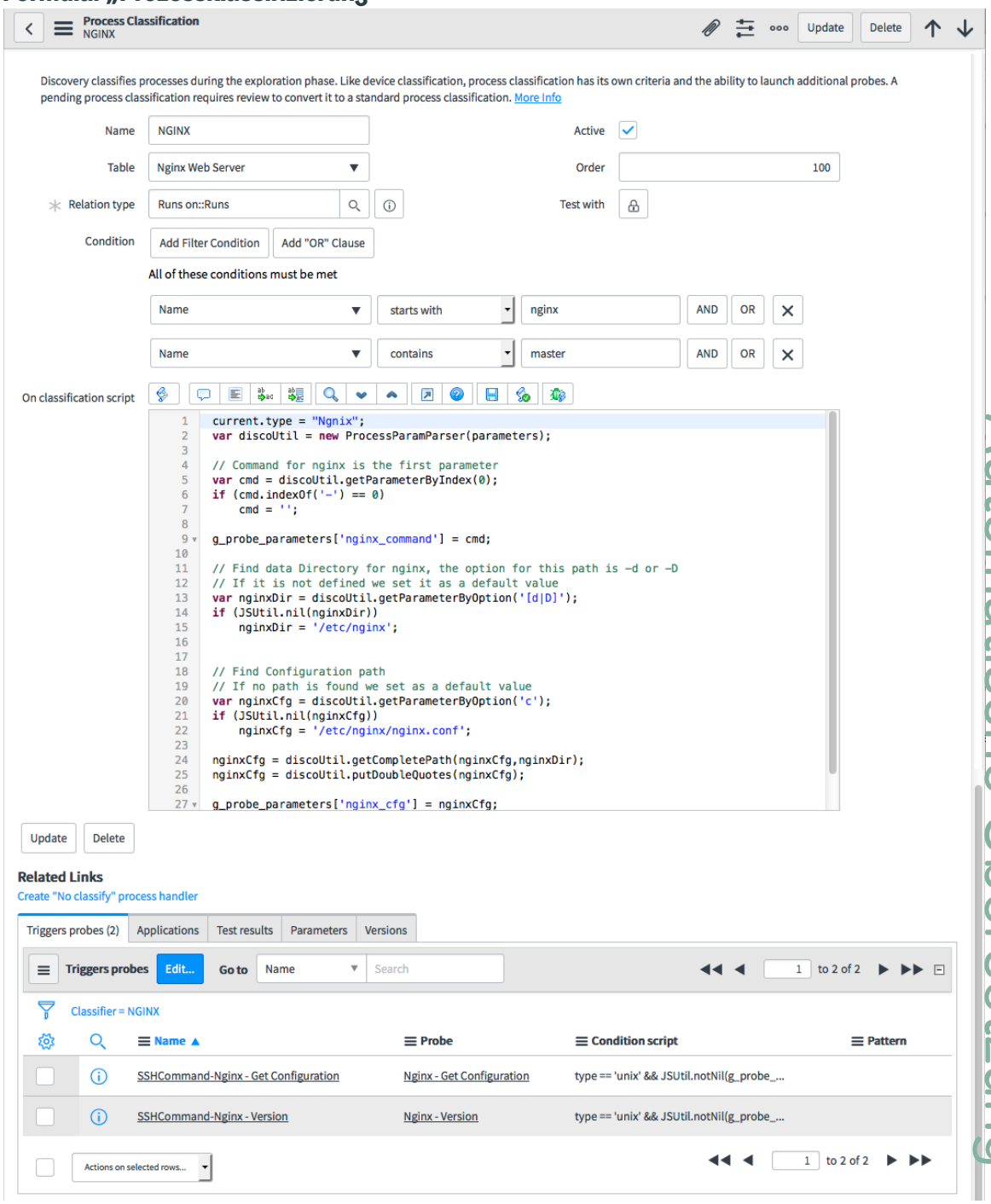
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mithilfe der Felder aus der Tabelle.
4. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Prozessklassifizierung“



Automatische Übersetzung

Formular „Prozessklassifizierung“

Feld	Beschreibung
Name	Ein eindeutiger Name für den Prozessklassifizierer
Tabelle	Wählen Sie **Anwendung** aus.
Beziehungstyp	Wählen Sie den CI-Beziehungstyp für diese Klassifizierung aus. Das Beziehungsfeld ist nur für Prozess- und Scan-Anwendungsklassifizierungen verfügbar. Für Erkennungsprozessklassifizierungen wird normalerweise einer der folgenden Beziehungstypen verwendet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Wird ausgeführt auf::Wird ausgeführt**: Definiert die Beziehung einer Anwendung mit dem Host, auf dem sie ausgeführt wird. Diese Beziehung wird aus der Perspektive des Hosts und der Anwendung ausgedrückt. Beispiel: Meine Datenbankanwendung wird auf server001 ausgeführt::server001 führt meine Datenbankanwendung aus. ○ **Abhängig von::Verwendet von**: Definiert die Beziehung einer Anwendung, die mit einer anderen Anwendung kommuniziert. Diese Beziehung wird aus der Perspektive der jeweiligen Anwendung ausgedrückt. Beispiel: Die Anwendung Tomcat ist von der Datenbank MySQL abhängig::Die Datenbank MySQL wird von Tomcat verwendet. ○ **Virtualisiert von::Virtualisiert**: Definiert die Beziehung eines virtuellen Computers mit ihrem Host. Diese Beziehung wird aus der Perspektive des virtuellen Computers und des Hosts ausgedrückt. Beispiel: server001 wird virtualisiert von ServerESX::ServerESX virtualisiert server001. ○ **Cluster von::Cluster**: Definiert die Beziehung eines Clusterknotens mit dem Cluster, dem er angehört. Diese Beziehung wird aus der Perspektive des Clusterknotens und des Clusters ausgedrückt. ○ **Gehostet auf::Hostet**: Definiert die Beziehung eines Clusterknotens und des Windows-Hosts. Diese Beziehung wird aus der Perspektive des Clusterknotens und des Windows-Hosts ausgedrückt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Prozessklassifizierung zu aktivieren. Deaktivieren Sie es, um sie zu deaktivieren.
Reihenfolge	Geben Sie die Reihenfolge ein, in der Discovery diese Prozessklassifizierung ausführen soll, wenn für eine Tabelle mehrere Klassifizierungen verfügbar sind. Discovery führt Prozessklassifizierungen von der niedrigsten zur höchsten Ordnungszahl aus.
Testen mit	Listet das Host-CI auf, bei dem die Bedingungen einer automatisch generierten Prozessklassifizierung erfüllt wurden. Verwenden Sie dieses Feld, um Änderungen an der Prozessklassifizierung zu testen. Auf diese Weise können Sie sicherstellen, dass sich die aktualisierte Klassifizierung wie erwartet verhält.
Bedingung	Konfigurieren Sie die gewünschte Bedingung. Im Beispiel-Screenshot wird diese Prozessklassifizierung ausgelöst, wenn der Prozessbefehl die Zeichenfolge `MSFT SQL Server 2000` enthält.

Prozessklassifizierer mit Windows-Clusterressourcen verknüpfen

Verknüpfen Sie im zweiten Schritt den Prozessklassifizierer mit den Informationen in der Tabelle „Windows-Clusterressourcen“.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Name der Tabelle Windows-Clusterressourcen lautet cmdb_ci_win_cluster_resource. Diese Beziehung wird über JavaScript erstellt.

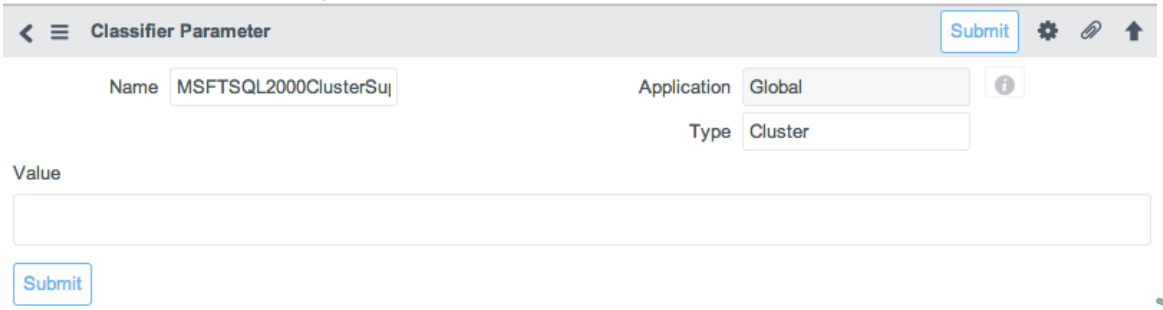
Prozedur

1. Navigieren Sie zurück zur gerade erstellten Prozessklassifizierung.
2. Klicken Sie auf die Registerkarte **Parameter**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder im Formular in geeigneter Weise aus (siehe Tabelle).
5. Klicken Sie auf **Absenden**.

Formular „Klassifizierungsparameter“



Formular „Klassifizierungsparameter“

Feld	Beschreibung
Name	Wählen Sie einen eindeutigen Namen aus.
Applikation	Wählen Sie **Global** aus.
Typ	Geben Sie **Cluster** ein.
Wert	Dieses Feld definiert die beiden JavaScript-Objekte `resourceType` und `isMatch`. Weitere Informationen finden Sie unter Feld „Wert“ im Formular „Klassifizierungsparameter“ füllen.

Feld „Wert“ im Formular „Klassifizierungsparameter“ füllen

Dieses Feld definiert die beiden JavaScript-Objekte `resourceType` und `isMatch`.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Wert von `resourceType` verweist auf die Spalte „Ressourcentyp“ in der Tabelle „Windows-Clusterressourcen“ [cmdb_ci_win_cluster_resource]. Der Wert `resourceType` darf nicht leer oder NULL sein.

Prozedur

1. Navigieren Sie zu einer Windows-Clusterseite, um auf die Tabelle „Windows-Clusterressourcen“ zuzugreifen.
2. Klicken Sie auf die Registerkarte **Windows-Clusterressourcen**.

Example:

Mit dem Wert **isMatch** wird ausgewertet, ob es sich bei dem Prozess um einen geclusterten Prozess handelt.

- Wenn die Auswertung **true** ergibt, handelt es sich bei dem Prozess um eine geclusterte Anwendung, und der Prozess wird im Cluster als geclusterte Anwendung klassifiziert.
- Ergibt die Auswertung hingegen **false**, wird der Prozess als normale Anwendung klassifiziert, die auf dem Clusterknoten ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Wert **isMatch** ist eine Funktion, die die beiden Eingabevariablen „process“ und „resource“ enthält:

- process: Der Prozess ist der GlideRecord der Prozessanwendung. Diese Variable wird durch das Feld **Tabelle** im Klassifizierer bestimmt. In diesem Beispiel wird für den Prozess, der klassifiziert wird, der GlideRecord-Eintrag der Anwendungstabelle (cmdb_ci_app) verwendet. Sie haben Zugriff auf alle Feldwerte für den CI-Typ, zum Beispiel Name oder Version.
- resource: Die Ressource ist der GlideRecord-Eintrag in der Tabelle „Windows-Clusterressourcen“, nachdem die resourceType-Bedingung angewendet wurde. Im Beispiel ist es der GlideRecord-Eintrag der sechsten Zeile.

JavaScript-Beispiele für das Feld „Wert“.

Im folgenden Beispielcode (resourceType: "SQL Server") filtert die Abfrage den Eintrag der Tabelle „Windows-Clusterressourcen“ für das Feld „Ressourcentyp“, das den Wert „SQL Server“ enthält. In der folgenden Beispieltabelle würde der sechste Datensatz zurückgegeben.

Das folgende Skript gibt an, dass der Prozess als geclusterte Anwendung klassifiziert ist, wenn eine Ressource vom Typ „SQL Server“ vorhanden ist.

```
resourceType: "SQL Server"
isMatch: function(process, resource) {
   return true;
}
```

Das folgende Skript gibt an, dass der Prozess als geclusterte Anwendung klassifiziert ist, wenn eine Ressource vom Typ „SQL Server“ vorhanden ist und der Anwendungsname dem Ressourcennamen entspricht.

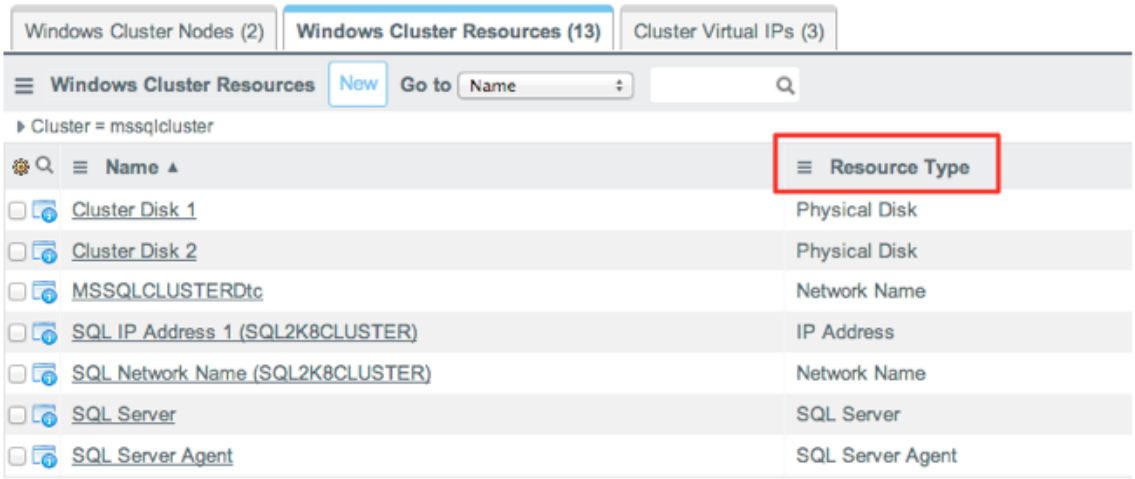
```
resourceType: "SQL Server"
isMatch: function(process, resource) {
   if (process.name == resource.name)
      return true;
}
```

Wenn mehrere Übereinstimmungen mit der resourceType-Bedingung vorhanden sind, wird die Abgleichfunktion mehrmals aufgerufen. Im folgenden Beispiel für resourceType wird die Abgleichfunktion zweimal aufgerufen, da in der Beispieltabelle „Windows-Clusterressourcen“ zwei Einträge vorhanden sind, die in der Spalte **Ressourcentyp** den Eintrag **Physical Disk** haben.

```
resourceType: "Physical Disk"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Windows-Clusterressourcen“



Erkennung mit Software Asset Management

Die Tabellenstruktur zur Verwaltung von Softwareinstallationen verhält sich anders, wenn die Anwendung Software Asset Management (SAM) aktiviert ist.

Das Vorhandensein dieser Anwendung hat Einfluss darauf, wie Discovery die von einem Scan zurückgegebenen Softwareinstallationsdaten speichert. Dafür ist eine zusätzliche Konfiguration der Datensätze von Konfigurationselementen (CIs) erforderlich.

Die folgenden Tabellen werden erstellt, wenn das Plugin „Software Asset Management“ aktiviert ist:

- Software-Discovery-Modell [cmdb_sam_sw_discovery_model]
- Softwaremodell [cmdb_software_product_model]
- Softwareinstallation [cmdb_sam_sw_install]

> **Hinweis:** Das von vorherigen Versionen verwendete ursprüngliche Schema ist nicht betroffen, wenn das Plugin „Software Asset Management“ nicht aktiviert ist.

Wenn es ausgeführt wird, füllt Discovery die Tabelle „Softwareinstallation“ [cmdb_sam_sw_install]. Das entsprechende Konfigurationselement (CI) verweist auf die Softwaredaten. Eine Geschäftsregel in dieser Tabelle wird ausgeführt und sucht nach einem übereinstimmenden Datensatz in der Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model]. Wenn in der Tabelle „Software-Discovery-Modell“ ein Datensatz vorhanden ist, wird dieser anhand der Tabelle „Softwareinstallation“ aktualisiert. Wenn in der Tabelle „Software-Discovery-Modell“ kein Datensatz vorhanden ist, wird ein Datensatz erstellt.

Diese Tabellen werden *nicht* von Discovery mit Software Asset Management verwendet:

- Software [cmdb_ci_spkg]
- Softwaremodell [cmdb_software_product_model]

> **Wichtig:** Wenn SAM installiert ist, stellt die Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] die richtige Quelle für alle aktuellen Softwaredaten dar. Das bedeutet, dass Sie alle zugehörigen Listen und benutzerdefinierten Referenzfelder aktualisieren müssen, die Sie CI-Datensätzen hinzugefügt haben.

Ab der Kingston-Version füllt die Discovery die Tabellen mit dem VMWare-Lizenzschlüssel [samp_vmware_license_key] und dem VMWare-Lizenzschlüssel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[samp_vmware_license_key_usage] aus. Siehe Für VMware vCenter-Server erfasste Daten, für weitere Informationen dazu, wo Discovery vCenter-Daten speichert.

CI zur Anzeige von Software Asset Management-Daten konfigurieren

Nachdem Sie das Plugin „Software Asset Management“ aktiviert haben, konfigurieren Sie das Formular für alle Computer-CIs, die erkannt werden sollen, um ihre Daten aus der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie einen beliebigen Computer-CI-Datensatz.
2. Konfigurieren Sie das Formular so, dass die zugehörige Liste **Softwareinstallation** hinzugefügt wird, und entfernen Sie die zugehörige Liste **Software installiert**.

Microsoft Exchange Client-Zugriffsserver-Discovery

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von erkannt wird Microsoft Exchange Client-Zugriffsserver (Microsoft Exchange CAS).

Standardmäßig verwendet Discovery das Muster *`CAS On Windows`*, um den Exchange-Clientzugriffsserver zu erkennen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery auf dem Exchange-Clientzugriffsserver erfasste Daten

In der Tabelle „Exchange-Clientzugriffsserver“ [cmdb_ci_exchange_cas] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	Typ

Erkennung von Exchange-Hub-Transport-Servern

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von Exchange Hub erkannt wird.

Standardmäßig Discovery Verwendet das Muster Hub-Transportserver unter Windows, um Exchange Hub-Transportserver zu erkennen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Hub-Transportservers unter Windows-Muster.

ExchangeHub [cmdb_ci_exchange_hub]

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	type

CI-Beziehungen

Der Hub-Transportserver unter Windows erkennt keine Beziehungen.

Erkennung von Exchange-Postfächern

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz des Exchange-Postfachs erkannt wird.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Voraussetzungen

Auf dem Server, der erkannt werden soll, muss das Modul Microsoft.Exchange.Management.PowerShell installiert sein.

Auf dem Hostcomputer muss der Service winRM ausgeführt werden. Führen Sie im Powershell-Fenster den folgenden Befehl zur Überprüfung aus: New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri "http://$hostname/PowerShell/" -Authentication Kerberos

Muster

Standardmäßig verwendet Discovery das Muster *MailBox On Windows*, um das Exchange-Postfach zu erkennen.

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

Anmeldeinformationstyp	Zusätzliche Hinweise
Applicative-Anmeldeinformationen	Der Benutzer muss in der Lage sein, PowerShell-Befehle für die Exchange-Hosts auszuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationstyp	Zusätzliche Hinweise
	Verwenden Sie **Exchange-Postfach** als CI-Typ für die Applicative-Anmeldeinformationen. **Wichtig:** Verwenden Sie nicht den CI-Typ **Exchange-Postfachserver**.
Windows-Anmeldeinformationen	Der BS-Benutzer darf kein lokaler Benutzer für den Server, sondern muss ein Domänenbenutzer sein.

Erfasste Daten

In der Tabelle „Exchange-Postfächer“ [cmdb_ci_exchange_mailbox] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	Typ

Erkennung von allgemeinen Softwarepaketen

Allgemeine Softwarepakete sind Sammlungen von Programmen, die zusammenarbeiten, häufig mit ähnlichen Anwenderoberflächen. Beispiele Microsoft Office 365(Word, Excel, PowerPoint) und Apple iWork (Seiten, Zahlen, Keynote). Discovery Identifiziert und klassifiziert Informationen zu allgemeinen Softwarepaketen. Zu den erfassten Daten gehören Name, Version, Installationsanzahl, Lizenzanzahl, Installationsdatum, Software und mehr.

Von Discovery für allgemeine Softwarepakete erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_spkg	Name	Verschiedene
Version	cmdb_ci_spkg	Version	Verschiedene
Anzahl Installationen	cmdb_ci_spkg	install_count	Verschiedene
Lizenzanzahl	cmdb_ci_spkg	license_count	Verschiedene
Microsoft SMS-ID	cmdb_ci_spkg	msft_sms_id	Verschiedene
Installiert auf	cmdb_software_instance	installed_on	Verschiedene
Software	cmdb_software_instance	Software	Verschiedene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von GlassFish-Servern

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von GlassFish Server erkannt wird.

Standardmäßig verwendet Discovery zur Erkennung die folgenden Muster: *`GlassFish Server`* und *`GlassFish WAR`*.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery für GlassFish erfasste Daten

Die folgenden Daten werden in den Tabellen „GlassFish“ [cmdb_ci_appl_glassfish] und „GlassFish Wars“ [cmdb_ci_appl_glassfish_war] erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
TCP-Port(s)	tcp_port
Konfigurationsverzeichnis	config_directory
Konfigurationsdatei	config_file

HP Vorgangsmanager-Discovery

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von erkannt wird HP Vorgangsmanager.

Standardmäßig verwendet Discovery das Muster *`HP Operations Manager for Windows`*, um HP Operations Manager zu erkennen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery für HP Operations Manager erfasste Daten

In der Tabelle „HP Operations Manager“ [cmdb_ci_appl_hp_operations] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	name

HP Servicemanager-Discovery

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von erkannt wird HP Servicemanager.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig verwendet Discovery das Muster *HP Service Manager Application Server*, um HP Service Manager zu erkennen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery für HP Service Manager erfasste Daten

In der Tabelle „HP Service Manager“ [cmdb_ci_appl_hp_service] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Lieferant	Lieferant

IBM App Connect Enterprise- und HTTP-Listener-Discovery

Muster für Discovery und Service-Mapping Die Anwendung verwendet die WMB-Muster, um Integrationsbus (früher WebSphere Message Broker und) zu erkennen IBM Integrationsbus) und HTTP-Listener, die auf beiden ausgeführt werden Linux Und Windows. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Standardmäßig Discovery Verwendet die folgenden Muster, um die Discovery durchzuführen:

- WMB ein UNIX
- WMB ein Windows
- WMB-HTTP-Listener auf UNIX
- WMB-HTTP-Listener auf Windows

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Um mehr über zu erfahren IBM WebSphere Message Broker (WMB) und WMB HTTP Listener-Komponenten und -Versionen, die Sie erkennen können, siehe Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen auf dem neuesten Stand sind

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster für Discovery und Service-Mapping
- Visibility Content

Von Discovery während der horizontalen Erkennung erfasste Daten

Vom WMB auf UNIX-Muster erkannte Ressourcen

IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]

Feld	Beschreibung
Name [name]	Name des Nachrichten-Brokers
Installationsverzeichnis [install_directory]	Installationsverzeichnis des Nachrichten-Brokers
Version [version]	Version des Nachrichten-Brokers

Vom WMB auf Windows-Muster erkannte Ressourcen

IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]

Feld	Beschreibung
Name [name]	Name des Nachrichten-Brokers
Installationsverzeichnis [install_directory]	Installationsverzeichnis des Nachrichten-Brokers
Version [version]	Version des Nachrichten-Brokers

Vom WMB-HTTP-Listener erkannte Ressourcen im UNIX-Muster

IBM WMB HTTP-Listener [cmdb_ci_appl_ibm_wmb_Listener]

Feld	Beschreibung
Name [name]	Name des HTTP-Listeners
Installationsverzeichnis [install_directory]	Installationsverzeichnis des HTTP-Listeners

Vom WMB-HTTP-Listener im Windows-Muster erkannte Ressourcen

IBM WMB HTTP-Listener [cmdb_ci_appl_ibm_wmb_Listener]

Feld	Beschreibung
Name [name]	Name des HTTP-Listeners
Installationsverzeichnis [install_directory]	Installationsverzeichnis des HTTP-Listeners

IBM MQ-Discovery

Die ServiceNow Discovery Die Anwendung verwendet WMQ in Unix und WMQ in Windows-Mustern, um zu finden IBM MQ (früher IBM WebSphere MQ) Ressourcen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Discovery Verwendet die folgenden Muster, um eine horizontale Discovery durchzuführen:

- *WMQ On Unix*
- *WMQ On Windows*

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Daten erfasst von Discovery Für IBM MQ

Discovery Füllt die Daten in aus CMDB Beim Ausführen der WMQ-Muster.

IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]

Bezeichnung	Feldname
Name	Name
Version	Version
Installationsverzeichnis	install_directory
Klasse	sys_class_name

Microsoft IIS-Server-Discovery

Discovery Identifiziert und klassifiziert Informationen zu Microsoft IIS-Server.

Voraussetzungen

Installieren Sie IIS-Verwaltungsskripts und -Tools auf einem Microsoft IIS-Server.

Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen

Klassifizierer, Muster und Probe

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Zur Erkennung von IIS verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierung	Auslöser-Probes	Muster
Microsoft IIS Server	• Probe „Horizontal Discovery“: Startet Muster • Windows - Get IIS Information*	IIS

*Probes bei neuen Instanzen inaktiv

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Von Discovery für IIS-Webserver erfasste Daten

In der Tabelle „IIS-Webserver“ [cmdb_ci_microsoft_iis_web_server] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Typ*	Typ
Prozessbefehl wird ausgeführt	running_process_command
Zentrale Parameter des ausführenden Prozesses	running_process_key_parameters

*Der Typ lautet immer IIS.

In der Tabelle „Website“ [cmdb_ci_web_site] werden die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Name	Name	wmi
TCP-Port	tcp_port	wmi

Erkennung von Microsoft SharePoint

Discovery Erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine laufende Instanz von erkannt wird Microsoft SharePoint.

Standardmäßig Discovery Verwendet *SharePoint*Zu erkennendes Muster Microsoft SharePoint. Für Informationen zu unterstützt Microsoft SharePoint Versionen, siehe Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Daten erfasst von Discovery Für Microsoft SharePoint

In der Tabelle „SharePoints“ [cmdb_ci_appl_sharepoint] werden die folgenden Daten erfasst:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname
Name	Name
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Version	Version

Erkennung von NGINX-Webservern

NGINX ist ein Open Source-Webserver mit einem Lastenausgleichsmodul. Discovery erkennt den Webserver und Informationen über das Lastenausgleichsmodul.

Discovery identifiziert die Serversoftware NGINX mit dem folgenden Prozess:

1. Der NGINX-Prozessklassifizierer erkennt einen laufenden Prozess, der die folgenden Kriterien bei der Untersuchung von erfüllt Linux Server:
   - Name beginnt mit „nginx“
   - Name enthält „master“
2. Wenn es eine Übereinstimmung gibt:
   - In der Tabelle „NGINX-Webserver“ [cmdb_ci_nginx_web_server] wird ein Datensatz erstellt.
   - In der Tabelle „CI-Beziehung“ [cmdb_rel_ci] für wird eine Beziehung ausgeführt Linux Server (Linux-Server [cmdb_ci_linux_Server]) und für einen NGINX-Webserver (NGINX-Webserver [cmdb_ci_nginx_Web_Server]).

     Die folgenden beiden Probes werden ausgelöst:

     - NGINX – Version: Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „NGINX-Webserver“ [cmdb_ci_nginx_web_server].
     - NGINX – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei bestimmt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.

     Der -Sensor auf der ServiceNow Die Instanz analysiert das Nutzlastergebnis und füllt den aus CMDB.

Zur Erkennung eines NGINX-Webservers müssen die folgenden Voraussetzungen erfüllt sein:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- Die MID-Server Hat Zugriff auf die NGINX-Konfigurationsdatei, die / lautet `Etc/nginx/nginx.conf` Standardmäßig.

Anforderungen

Für NGINIX-Server:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- Gewähren Sie MID-Server Hat Zugriff auf die NGINX-Konfigurationsdatei, die ist `/Etc/nginx/nginx.conf` Standardmäßig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - NGINX - Version
  - NGINX - Get Configuration

Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Befehle

Probe	Befehle
Nginx – Version	nginx
Nginx – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Hinweis: Das Nginx-Muster führt für beide eine Top Down-Discovery durch Windows Und Linux Server. Informationen zu den Voraussetzungen für die Top Down-Discovery für NGINX-Webserver finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Probes und Sensoren

Discovery identifiziert die Serversoftware NGINX mit dem folgenden Prozess:

1. Der Prozessklassifizierer „Nginx“ erkennt einen laufenden Prozess, der während der Erkundung eines UNIX-Servers die folgenden Kriterien erfüllt:
   - Der Name des Prozesses beginnt mit nginx.
   - Der Name des Prozesses enthält master.
2. Wenn es eine Übereinstimmung gibt:
   - In der Tabelle „Webserver“ [cmdb_ci_web_server] wird ein Datensatz erstellt.
   - In der Tabelle „CI-Beziehung“ [cmdb_rel_ci] wird für den Linux-Server (Linux-Server [cmdb_ci_linux_server]) und für den Webserver (Webserver [cmdb_ci_web_server]) eine Beziehung vom Typ Wird ausgeführt auf erstellt.
3. Die folgenden beiden Probes werden ausgelöst:
   - **Nginx – Version**: Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „Webserver“ [cmdb_ci_web_server].
   - **Nginx – Get Configuration**: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei bestimmt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.
4. Der -Sensor auf der ServiceNow Die Instanz verarbeitet die Nutzlast und füllt die aus CMDB.

Erfasste Daten

Discovery Erstellt oder aktualisiert CMDB Zeichnet auf, wenn ein laufender NGINX-Prozess erkannt wird. Die folgenden Daten werden erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery für NGINX erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
Name	cmdb_ci_lb_appl [name]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_appl [ip_address]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_appl [last_discovered]	Nginx– Get Configuration
Version	cmdb_ci_lb_appl [version]	Nginx– Version
Name	cmdb_ci_lb_pool_member [name]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_pool_member [last_discovered]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_pool_member [ip_address]	Nginx– Get Configuration
Lastenausgleich	cmdb_ci_lb_pool_member [load_balancer]	Nginx– Get Configuration
Vollqualifizierter Domänenname	cmdb_ci_lb_pool_member [fqdn]	Nginx– Get Configuration
Port	cmdb_ci_lb_pool_member [port]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_service [last_discovered]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_service [ip_address]	Nginx– Get Configuration
Name	cmdb_ci_lb_service [name]	Nginx– Get Configuration
Lastenausgleich	cmdb_ci_lb_service [load_balancer]	Nginx– Get Configuration
Eingabe-URL	cmdb_ci_lb_service [input_url]	NGINX - Get Configuration

Beziehungen

In die Tabelle [cmdb_rel_ci] werden die folgenden Beziehungen eingefügt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Tabelle cmdb_ci_pool.

Oracle Tuxedo-Discovery

Die ServiceNow Discovery Anwendung verwendet das Tuxedo-Muster, um zu finden Oracle Tuxedo-Ressourcen. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Verwendet **Tuxedo** Muster zum Ausführen der horizontalen Discovery.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Daten erfasst von Discovery Für Oracle Tuxedo

Discovery Füllt die Daten in aus CMDB Beim Ausführen des Tuxedo-Musters.

Tuxedo [cmdb_ci_appl_tuxedo]

Name	Beschreibung
Port [port]	Der von verwendete Netzwerkkommunikationsport Oracle Tuxedo-Services und -Prozesse für die Netzwerkkommunikation.
Domäne [domain]	Die logische Gruppierung von Oracle Tuxedo-Komponenten und -Services, die in einer definierten Umgebung ausgeführt werden.
Installationsverzeichnis [install_directory]	Der Speicherort, der alle Binärdateien und Konfigurationsdateien enthält, die für die Ausführung erforderlich sind Oracle Tuxedo.
Protokollverzeichnis [log_dir]	Das Verzeichnis, in dem alle von generierten Protokolldateien gespeichert sind Oracle Tuxedo für Überwachung und Fehlerbehebung.
Version [version]	Das spezifische Release von Oracle Tuxedo, das installiert ist und derzeit verwendet wird.
Modus [Modus]	Die Definition des Interaktionsprotokolls zwischen Oracle Tuxedo und verschiedene Clients oder andere Domänen, z. B. Jolt, Workstation oder Domain Gateway, je nach Betriebskonfiguration.

Erkennung der Automatisierungssoftware Puppet

Discovery Identifiziert Puppet-Master, die auf ausgeführt werden UNIX Server.

Discovery verwendet SSH-Befehle (Secure Shell) zur Erfassung von Informationen.

Um auf Puppet-Master-Datensätze zuzugreifen, navigieren Sie zu **Alle** > **Konfiguration** > **Automatisierungsserver** > **Master-Puppets**an. Sie können die Ressourcen in der zugehörigen Liste des Puppet Master-Datensatzes anzeigen.

Funktionsweise der Probe „Puppet Master“

Discovery identifiziert Puppet Master mit dem folgenden Prozess:

1. Die Probe **UNIX - Active Processes** erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet `pe-httpd`.
   - Der Name des Prozesses lautet `ruby`, und die Parameter des Prozesses enthalten *`puppet master`*.
2. Wenn eine Übereinstimmung mit einem der folgenden Kriterien vorliegt:
   - Ein Datensatz wird in der Puppet Master-Tabelle [cmdb_ci_puppet_master] erstellt, wenn für den ausgeführten Prozess noch kein Datensatz vorhanden ist.
   - Die Probe **Puppet - Master Info** wird ausgelöst. Der Sensor dieser Probe fügt dem Puppet Master-Datensatz [cmdb_ci_puppet_master] einige zusätzliche Informationen hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen zum Erkennen eines Puppet-Masters

Standardmäßig erkennt Discovery auf UNIX-Servern ausgeführte Puppet-Master. Discovery verwendet SSH-Befehle (Secure Shell) zur Erfassung von Informationen.

Die zum Erkennen des UNIX-Servers verwendeten Anmeldeinformationen müssen über Berechtigungen zum Ausführen der folgenden Befehle verfügen. Die Verwendung von sudo wird unterstützt, Sie müssen der Probe jedoch den Parameter *must_sudo* hinzufügen.

Probe	Befehle
Puppet - Master Info	puppet, echo, hostname (im Bourne-Shell-Skript)
Puppet - Certificate Requests	puppet
Puppet - Manifests	echo, sed, find (im Bourne-Shell-Skript)
Puppet - Modules	puppet

Erfasste Daten

Daten, die Discovery standardmäßig für die Automatisierungssoftware Puppet erfasst

Name	Puppet-Master [cmdb_ci_puppet_master]	Name	Puppet - Master Info
Konfigurationsverzeichnis	Puppet-Master [cmdb_ci_puppet_master]	config_directory	Puppet - Master Info
Manifestverzeichnis	Puppet-Master [cmdb_ci_puppet_master]	manifestdir	Puppet - Master Info
Modulpfad	Puppet-Master [cmdb_ci_puppet_master]	modulepath	Puppet - Master Info
Vollqualifizierter Domänenname	Puppet-Master [cmdb_ci_puppet_master]	fqdn	Puppet - Master Info
IP-Adresse	Puppet-Master [cmdb_ci_puppet_master]	ip_address	Puppet - Master Info
Version	Puppet-Master [cmdb_ci_puppet_master]	Version	Puppet - Master Info

Puppet-Probes den Parameter must_sudo hinzufügen

Um Puppet-Probes mit sudo zu verwenden, müssen Sie jeder Probe, für die das erforderlich ist, den Parameter *must_sudo* hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie allen Puppet-Probes den Parameter must_sudo hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Probes**an.
2. Suchen Sie im Feld **Suchen** nach dem Namen **Puppet**.
3. Klicken Sie auf den Namen der Probe.
   Beispiel: **Puppet Master - Info**.
4. Wählen Sie im Bereich **Zugehörige Links** die Registerkarte **Probe Parameter** aus.
5. Klicken Sie auf **Neu**.
6. Geben Sie in das Feld **Name** den Namen `must_sudo` ein.
7. Im Feld **Wert** geben Sie `wahr` ein.
8. Klicken Sie auf **Absenden**.

Erkennung von SAP-Produkten

ITOM-Transparenz Kann erkennen SAP Anwendungen, SAP HANA-Datenbank, und SAP HANA DB-KATALOG . Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Um mehr über zu erfahren SAP Komponenten und ihre Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

Visibility Content

CMDB CI-Klassenmodelle

Überprüfen Sie die Konfiguration der Anmeldeinformationen

- (Beim Hosting auf UNIX-Server) Konfigurieren Sie auf der ServiceNow AI Platform die Applicative-Anmeldeinformationen und SSH-Anmeldeinformationen . Die SSH-Anmeldeinformationen werden dazu verwendet, Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. Geben Sie dem Anwender zusätzlich erhöhte Rechte an, um Befehle ausführen zu können, die einen privilegierten Anwender erfordern: Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.
- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der ServiceNow AI Platform die Windows-Anmeldeinformationen , um Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen.
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Optional für Discovery von oben nach unten durch Service-Mapping) Erteilen Sie einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion.
- (Optional für Top Down-Discovery durch Service-Mapping) Wenn Ihre Organisation digitale SAP-Business-Services mithilfe von Webservices implementiert und Sie alle verbundenen Services zuordnen möchten, führen Sie die folgenden Aktionen aus:
  - Konfigurieren Sie Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: CVERS, DBCONS und RFCONS.
  - Stellen Sie sicher, dass Sie über die Webservice-URL verfügen. Informationen zum Erstellen von Webservices finden Sie unter https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ .

SAP HANA 2,0 DB-Katalog auf UNIX

Überprüfen Sie, ob die anwendbaren Anmeldeinformationen für **SAP HANA DB-App-Creds** Sind mit konfiguriert **SAP hana-DB [cmdb_ci_appl_sap_hana_DB]** Als CI-Typ.

Überprüfen Sie die auszuführenden Berechtigungen Service-Mapping Befehle

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Stellen Sie sicher, dass der Anwender über die Berechtigungen zum Ausführen der Musterabfragen verfügt

Die folgenden Befehle werden ausgeführt, wenn die Muster SAP HANA DB und SAP HANA DB-Katalog ausgeführt werden.

- * Aus Schemas auswählen;
- Wählen Sie * aus M_HOST_INFORMATION aus, wobei Upper(KEY) wie „%TIMEZONE%“;
- Wählen Sie SCHEMA_NAME aus, runden Sie (Summe(TABLE_SIZE) /1024/1024) aus der M_TABLES-GRUPPE NACH SCHEMA_NAME

Der Abfragetyp	Fallback-Befehle werden in der Reihenfolge ausgeführt
Schemainformationen	**1.** $hdbsql_path + " -n " + $entry_Point.ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$$password$' \"Select * from Schemas;\"" **2.** $hdbsql_path + " -n " + $ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$$password$' \"Select * from Schemas;\"" **3.** $hdbsql_path + " -n " + $Server_Name + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username $' -p '$$password$' \"Select * from Schemas;\""

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abfragetyp	Fallback-Befehle werden in der Reihenfolge ausgeführt
	4. $hdbsql_path + " -n localhost -i " + $Ziffern + " -u '$$username$' -p '$ $password$' \"select * from Schemas; \""
Zeitzone:	**1.** $hdbsql_path + " -n " + $entry_Point.ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$ $password$' \"Select * from M_HOST_INFORMATION, wobei Upper(KEY) like '%TIMEZONE%';\"" **2.** $hdbsql_path + " -n " + $ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$$password$' \"Select * from M_HOST_INFORMATION, wobei Upper(KEY) like '%TIMEZONE%';\"" **3.** $hdbsql_path + " -n " + $Server_Name + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username $' -p '$$password$' \"Select * from M_HOST_INFORMATION, wobei Upper(KEY) like '%TIMEZONE%';\"" **4.** $hdbsql_path + " -n localhost -i " + $Ziffern + " -u '$$username$' -p '$$password$' \"select * from M_HOST_INFORMATION where upper(KEY) like '%TIMEZONE%';\""
Datenträgergröße	**1.** $hdbsql_path + " -n " + $entry_Point.ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$$password $' \"SCHEMA_NAME auswählen, runden(Summe(TABLE_SIZE) /1024/ 1024) aus M_TABLES GRUPPIEREN NACH SCHEMA_NAME;\" **2.** $hdbsql_path + " -n " + $ip_address + ":" + $query_Port + " -i " + $Ziffern + " -u '$$username$' -p '$$password $' \"SCHEMA_NAME auswählen, runden(Summe(TABLE_SIZE) /1024/ 1024) aus M_TABLES-GRUPPE NACH SCHEMA_NAME;\" **3.** $hdbsql_path + " -n " + $Server_Name + ":" + $query_Port + " -i " + $Ziffern + " -u '$ $username$' -p '$$password$'

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abfragetyp	Fallback-Befehle werden in der Reihenfolge ausgeführt
	\"SCHEMA_NAME auswählen, runden(Summe(TABLE_SIZE) /1024/ 1024) aus M_TABLES-GRUPPE NACH SCHEMA_NAME;\" 4. $hdbsql_path + " -n localhost -i " + $Ziffern + " -u '$ $username$' -p '$$password$' \"SCHEMA_NAME auswählen, runden(sum(TABLE_SIZE) /1024/ 1024) aus M_TABLES-GRUPPE NACH SCHEMA_NAME;\"

Überprüfen Sie die Konfiguration von Discovery Zeitplan

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
SAP ASCS [cmdb_ci_appl_sap_ascs]	
Name [name]	Für SAP Advanced Business Application Programming (ABAP) SAP Central Services (ASCS) gesammelte Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [confi_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP Business Objects CMS-Server [cmdb_ci_appl_sap_bo]	
Name [name]	Für SAP Business Objects CMS-Server erfasste Daten
Servername [server_name]	
Version [version]	
Installationsverzeichnis [install_directory]	
SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]	
Name [name]	Für SAP Central Services (SCS) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP CI-Anwendung [cmdb_ci_appl_sap_ci]	
Name [name]	Für SAP Convergent Invoicing (CI) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP DI-Anwendungen [cmdb_ci_appl_sap_di]	
Name [name]	Für SAP NetWeaver Development Infrastructure (DI) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]	
Name [name]	Für SAP Evaluated Receipt Settlement (ERS) erfasste Daten
Version [version]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
HANA-Datenbank [cmdb_ci_appl_sap_hana_db]	
Name [name]	Für SAP HANA-Datenbank erfasste Daten
IP-Adresse [id_address]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
Version [version]	
Installationsverzeichnis [install_directory]	
SAP-SID [cmdb_ci_sap_sid]	
Name [name]	Für SAP System Identification (SID) gesammelte Daten. Eine SID ist ein eindeutiger Identifizierungscode für eine SAP R/3-Installation. Eine SID ist ein dreistelliger Code wie D10, PRD oder E56. Eine R/3-Installation besteht aus einem Datenbankserver und mehreren Anwendungsservern. ITOM-Transparenz Verwendet SAP Muster der gemeinsamen SID-Bibliothek, für die SIDs erkannt werden sollen SAP Anwendungen.
Version [version]	
Informationen zur Patch-Ebene [sap_Patch_info]	

Von erfasste Daten SAP HANA-DB-Katalog auf UNIX Muster während der horizontalen Discovery

SAP HANA-Katalog [cmdb_ci_DB_hana_catalog]

Feld	Beschreibung
Katalogbesitzer [catalog_owner]	Die Anwender-ID des Schemabesitzers.
Katalogerstellungszeit [catalog_create_time]	Die Katalogerstellungszeit.
Zugeteilte Datenträgergröße (MB) [Disk_allocated_size_mb]	Die Größe des zugeteilten Datenträgers in MB.
Datenbankreferenz [database_ Instanz]	Der Verweis auf die SAP HANA DB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Die SAP Das Muster der gemeinsamen SID-Bibliothek erstellt CI-Beziehungen zwischen allen wichtigen CI-Anwendungen und SAP System-ID.

CI	Beziehung	CI
SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP DI-Anwendungen [cmdb_ci_appl_sap_di]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP ASCS [cmdb_ci_appl_sap_ascs]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP CI-Anwendung [cmdb_ci_appl_sap_ci]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP JC-Anwendung [cmdb_ci_appl_sap_jc]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]

SAP HANA-DB-Katalog auf UNIX CI-Beziehungen

CI	Beziehung	CI
SAP HANA-DB [cmdb_ci_appl_sap_hana_DB]	Enthält::Enthalten in	SAP HANA DB-Katalog [cmdb_ci_DB_hana_catalog]

Einschränkungen

Service-Mapping kann pro Bereitstellung nur eine ASCS-Instanz zuordnen.

Die SAP HANA DB-Katalogmuster kann nur auf ausgeführt werden UNIX.

Ordnen Sie Anwendungsservices zu, die SAP-Anwendungen enthalten

Ordnen Sie einen Serviceinstanz zu, der eine SAP-Anwendung enthält, und vergewissern Sie sich, dass Service-Mapping alle SAP-Komponenten richtig erkannt hat.

Vorbereitungen

Erforderliche Rolle: Service_Mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.

   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**an.

   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

   c. In **Name** Geben Sie einen beschreibenden Namen für die Serviceinstanz ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:

   a. Wählen Sie die Kachel **SAP-Anwendung**.
   Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.

   b. Definieren Sie den Einstiegspunkt wie folgt:

   - Eine URL zu einem beliebigen SAP-Modul
   - Eine TCP-Verbindung zu einem beliebigen SAP-Modul
   - Zum Erkennen von Umgebungen mit verbundenen Services geben Sie die URL für den Webservice im folgenden Format an: .

     ```
     http://<hostname>:<port>/sap/bc/srt/scs/sap/z_servicenow_read?sap-client=003
     ```

   c. Klicken Sie auf **Hinzufügen**.

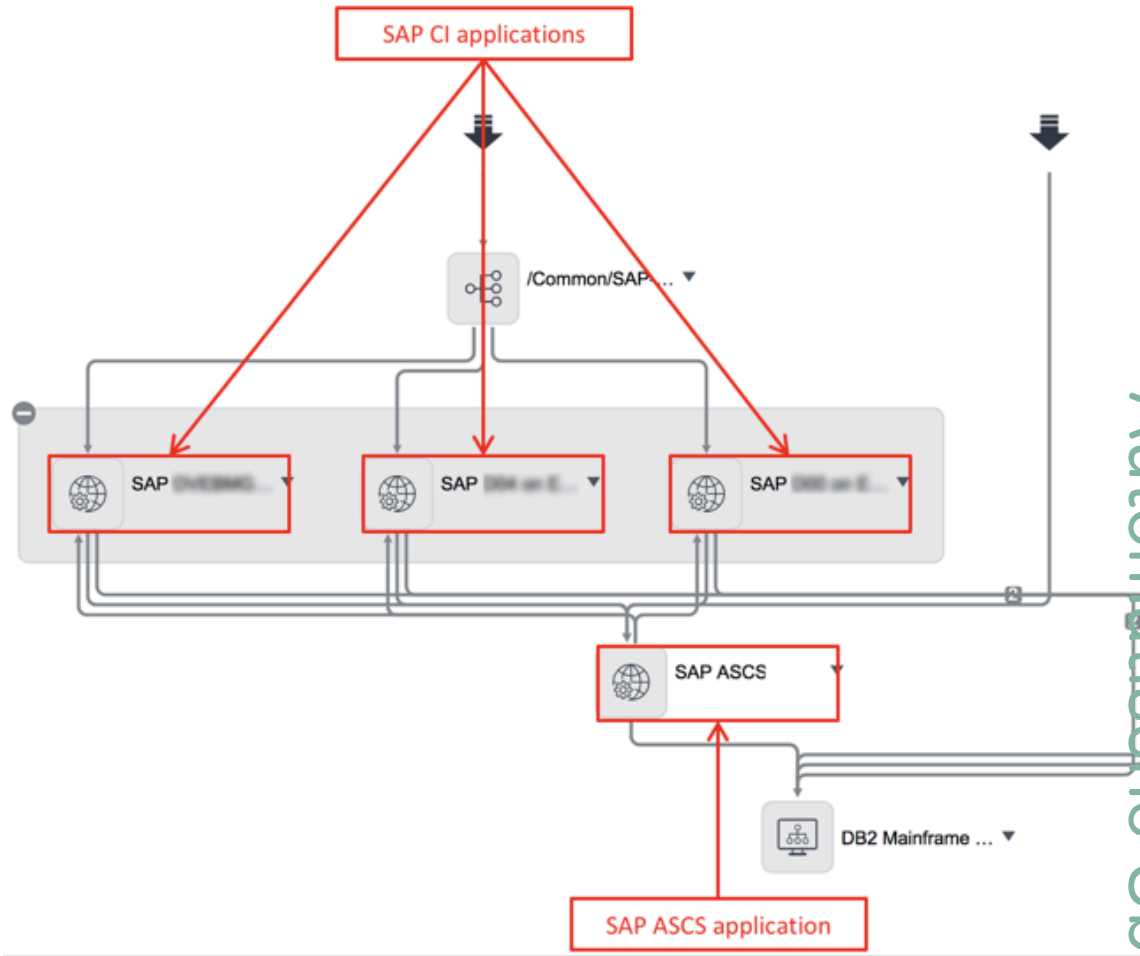
   d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist.
   Es kann einige Minuten dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

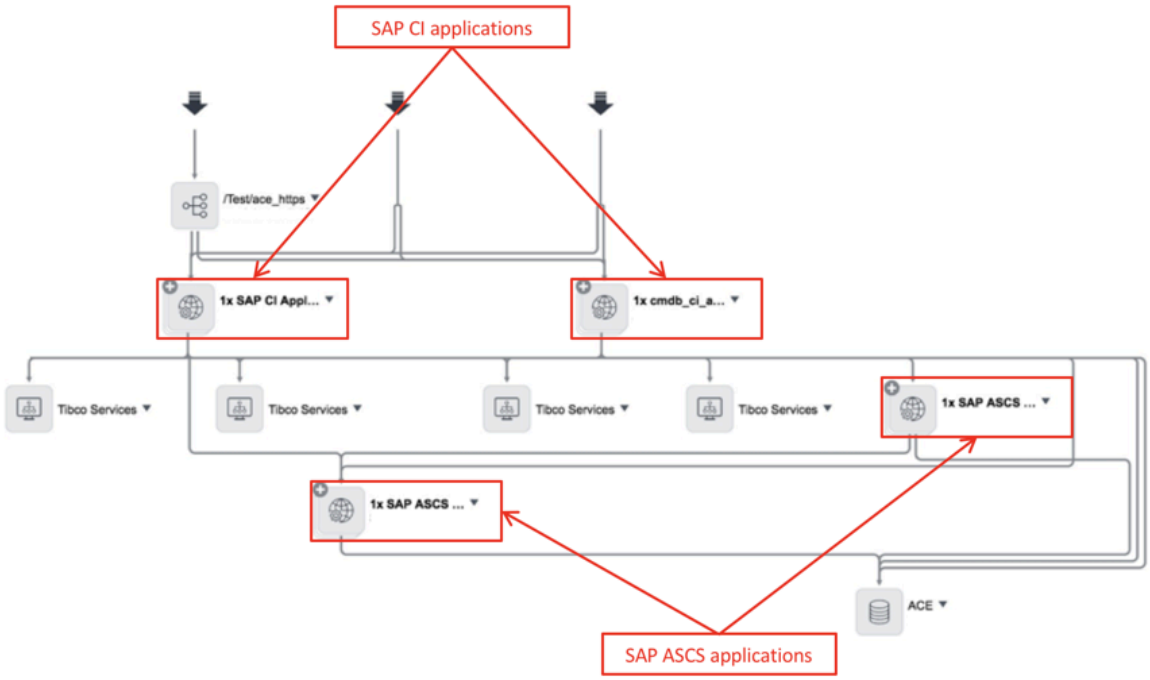
b. Überprüfen Sie die Zuordnung des Anwendungsservice, und stellen Sie sicher, dass das Servicelayout wie in den folgenden Beispielen aussieht.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die SAP-Umgebung SAP-Komponenten mit Tibco-Services integriert, können Sie dieses Zuordnungsergebnis erwarten:



Problembehebung bei Anwendungsservices, die SAP-Anwendungen enthalten

Beheben Sie grundlegende Erkennungsprobleme basierend auf den Symptomen und Erkennungsmeldungen.

Symptom

In der Zuordnung des Anwendungsservice in Service-Mapping wird die folgende Meldung angezeigt: Fehler beim Erkennen von <Name der SAP-Komponente>.

Ursache

Das CI konnte nicht identifiziert werden, und die Prozesserkennung ruft die Prozessattribute ab.

Lösung

Führen Sie die nachfolgenden Schritte durch:

1. Öffnen Sie den fehlgeschlagenen Musterschritt im Debug-Modus:
   a. Klicken Sie in der Zuordnung des Business-Service oder der Serviceinstanz mit der rechten Maustaste auf die Fehlermeldung, und wählen Sie aus **Discovery-Protokoll anzeigen** .

      Das Fenster „Discovery-Protokoll“ wird geöffnet.

   b. Suchen Sie im rechten Bereich den fehlerhaften Identifikationsbereich und den fehlgeschlagenen Schritt innerhalb dieses Bereichs.
   c. Wählen Sie diesen fehlerhaften Identifikationsbereich aus und klicken Sie auf **Debuggen**.

Automatische Übersetzung

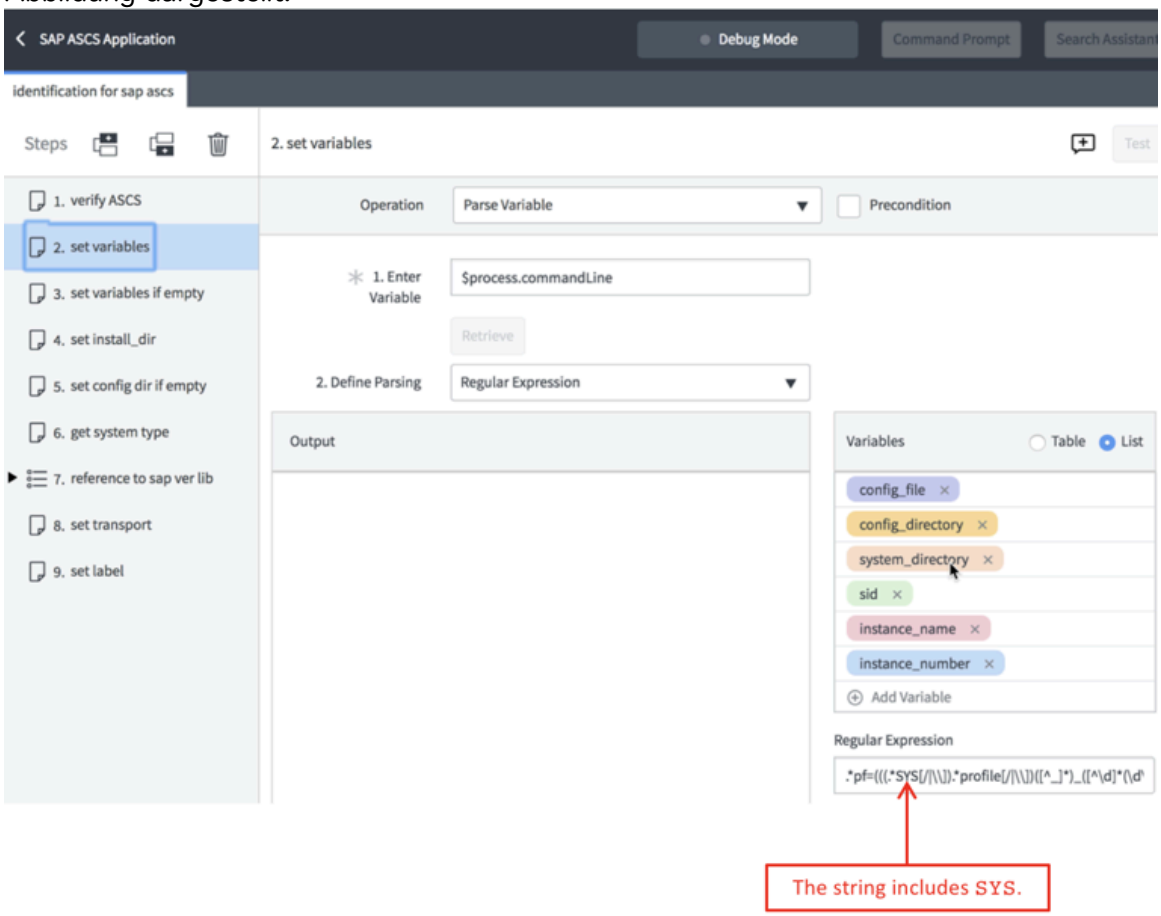
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fenster „Identifikationsbereich debuggen“ wird geöffnet.

d. Füllen Sie ggf. die erforderlichen Angaben aus und klicken Sie auf **Verbinden**.

2. Klicken Sie unter **Schritte** auf den Schritt **Variablen festlegen**.

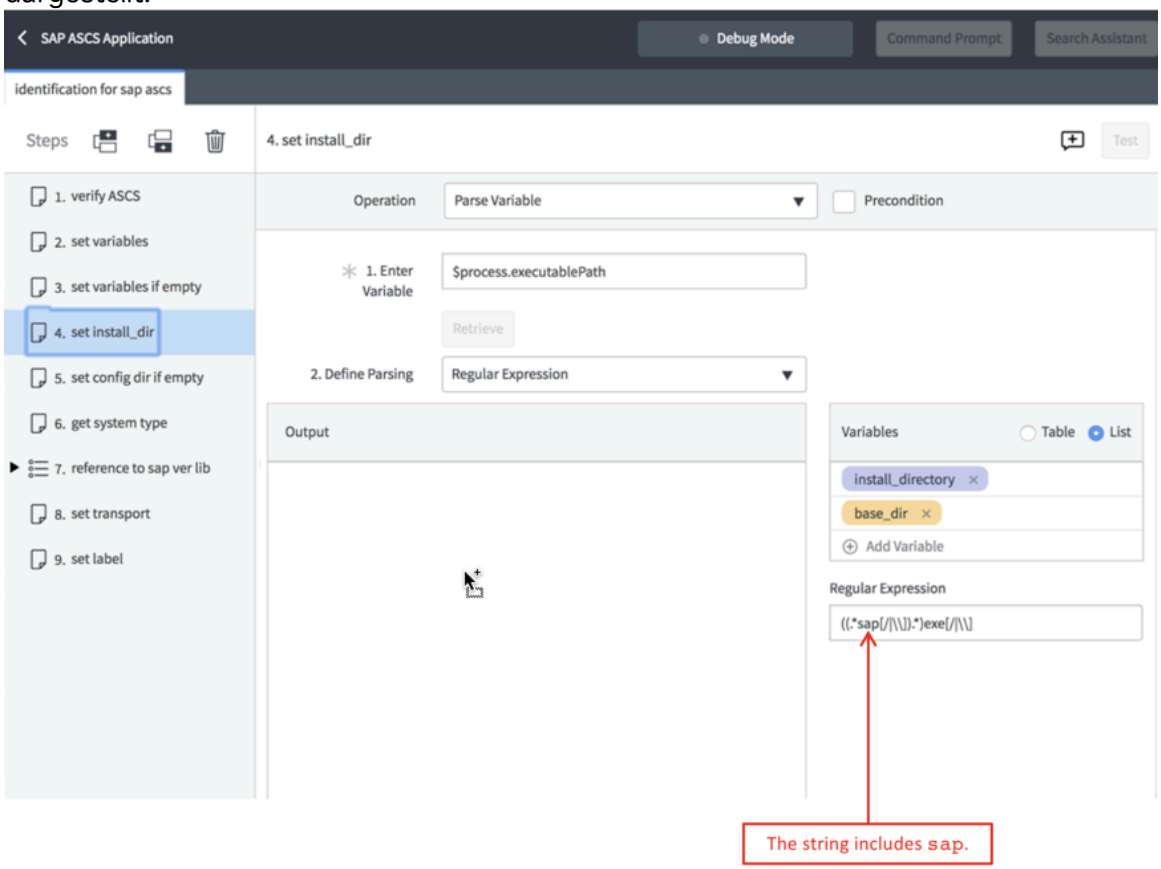
3. Stellen Sie sicher, dass der reguläre Ausdruck SYS enthält, wie in der folgenden Abbildung dargestellt.



4. Klicken Sie unter **Schritte** auf den Schritt **install_dir festlegen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Stellen Sie sicher, dass der reguläre Ausdruck `sap` enthält, wie in der folgenden Abbildung dargestellt.



Symptom

Service-Mapping erkennt den Webservice nicht, den Ihre Organisation für die Bereitstellung von SAP Digital Business Services verwendet.

Ursache 1

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl.

Lösung 1

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Überprüfen Sie, ob das Erkennungsprotokoll die folgende Nachricht enthält: GROOVE_CODE_FAILURE: Keine solche Eigenschaft: com für Klasse: Script1.
4. Öffnen Sie den fehlgeschlagenen Musterschritt im Debug-Modus:
   a. Klicken Sie in der Zuordnung des Business-Service oder der Serviceinstanz mit der rechten Maustaste auf die Fehlermeldung, und wählen Sie aus **Discovery-Protokoll anzeigen** .

      Das Fenster „Discovery-Protokoll“ wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Suchen Sie im rechten Bereich den fehlerhaften Identifikationsbereich und den fehlgeschlagenen Schritt innerhalb dieses Bereichs.

c. Wählen Sie diesen fehlerhaften Identifikationsbereich aus und klicken Sie auf **Debuggen**.

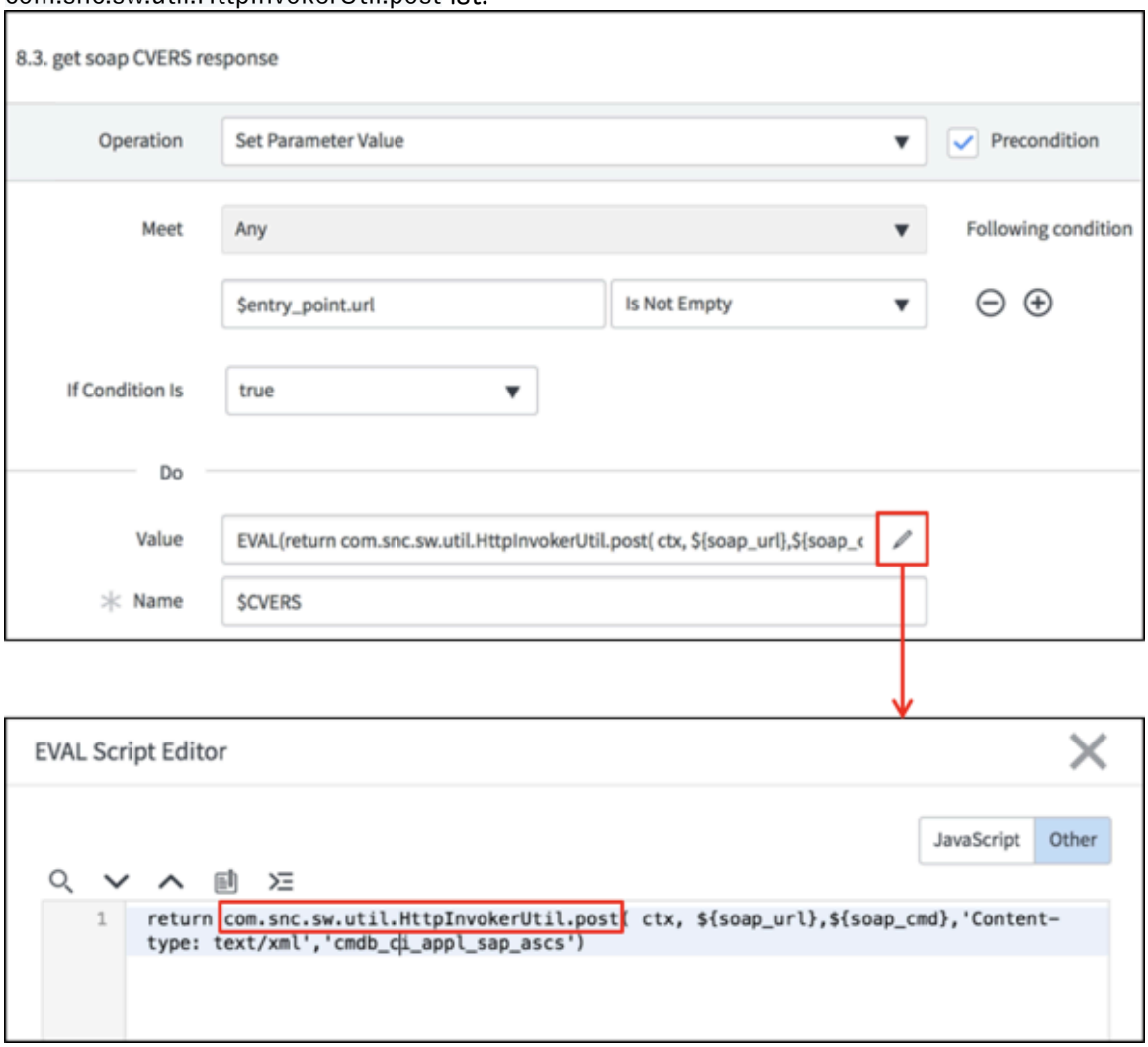
Das Fenster „Identifikationsbereich debuggen“ wird geöffnet.

d. Füllen Sie ggf. die erforderlichen Angaben aus und klicken Sie auf **Verbinden**.

5. Der Musterdesigner wird mit dem ausgewählten Identifizierungsabschnitt geöffnet.

6. Wählen Sie rechts den fehlgeschlagenen Schritt aus.

7. Stellen Sie sicher, dass die auf EVAL ausgeführte Funktion com.snc.sw.util.HttpInvokerUtil.post ist.



8. Versuchen Sie, den Anwendungsservice erneut zuzuordnen, und überprüfen Sie das Ergebnis.

Ursache 2

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl, weil der Webservice falsch konfiguriert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösung 2

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Erstellen Sie den Webservice neu, wie in https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ beschrieben.
5. Versuchen Sie, den Anwendungsservice erneut zuzuordnen, und überprüfen Sie das Ergebnis.

Ursache 3

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl, da die im Einstiegspunkt konfigurierte URL nicht korrekt ist oder weil der MID-Server nicht auf diese URL zugreifen kann.

Lösung 3

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Stellen Sie sicher, dass Sie die richtige URL für den Serviceeinstiegspunkt verwendet haben:
   a. Navigieren Sie im TCode SOAMANAGER zu **Vereinfachte Webservice-Konfiguration**.
   b. Suchen Sie auf der Registerkarte **Konfiguration** des Fensters „Vereinfachte Servicekonfiguration“ nach dem Webservice, der Teil des Serviceinstanz s ist.
   c. Klicken Sie auf das Kontrollkästchen unter **Benutzername/Passwort (Standard)** für diesen Webservice.
   d. Klicken Sie auf **Details anzeigen**.
   e. Überprüfen Sie im Fenster „Details“ der Servicedefinition die tatsächliche URL des Webservices unter WSDL-URLs.
   f. Korrigieren Sie ggf. die für den Einstiegspunkt konfigurierte URL, und versuchen Sie erneut, den Serviceinstanz zuzuordnen.

Ursache 4

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des Serviceinstanz konfiguriert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösung 4

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Vergewissern Sie sich, dass Sie den MID-Server für den Zugriff auf die URL verwendet haben, die Sie im Serviceeinstiegspunkt konfiguriert haben:
   a. Melden Sie sich remote beim MID-Server-Host an.
   b. Öffnen Sie einen Browser.
   c. Fügen Sie die URL in die Adresszeile des Browsers ein, und drücken Sie die Eingabetaste.
   d. Wenn die Seite nicht geöffnet wird, liegt ein Netzwerkproblem vor, z. B. ist eine Firewall vorhanden, die verhindert, dass der MID-Server auf diese URL zugreift.
5. Beheben Sie das Netzwerkproblem, und stellen Sie sicher, dass der MID-Server wie in Schritt 4 beschrieben auf die URL zugreifen kann.

Ursache 5

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des Serviceinstanz konfiguriert wurde.

Lösung 5

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Überprüfen Sie, ob die Applicative-Anmeldeinformationen, die Sie auf der ServiceNow AI Platform für den Webservice konfiguriert haben, gültig sind:
   a. Melden Sie sich remote beim MID-Server-Host an.
   b. Öffnen Sie einen Browser.
   c. Fügen Sie die URL in die Adresszeile des Browsers ein, und drücken Sie die Eingabetaste.
   d. Die Browserseite zeigt das Popup-Fenster für die Anmeldeinformationen an.
   e. Geben Sie die Anmeldeinformationen ein, und überprüfen Sie, ob die Seite geöffnet wird.

      Die Seite wird nicht geöffnet, was bedeutet, dass die konfigurierten Applicative-Anmeldeinformationen falsch sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Ermitteln Sie die richtigen Anmeldeinformationen.
6. Überprüfen Sie die neuen Anmeldeinformationen wie in Schritt 4 beschrieben.
7. Wenn die Seite geöffnet wird, nachdem Sie die neuen Anmeldeinformationen verwendet haben, konfigurieren Sie diese Anmeldeinformationen als Applicative-Anmeldeinformationen auf der ServiceNow AI Platform.

Ursache 6

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des Serviceinstanz konfiguriert wurde.

Lösung 6

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Fehlende gültige Applicative-Anmeldeinformationen für den CI-Typ <Name des CI-Typs>.“
3. Vergewissern Sie sich, dass Sie wie in Ordnen Sie Anwendungsservices zu, die SAP-Anwendungen enthalten beschrieben Applicative-Anmeldeinformationen für das relevante CI definiert haben.

Erkennung von SQL Server Analysis Services (SSAS)

Die Discovery Und Service-Mapping Die Anwendung verwendet das SSAS-Muster, um SQL Server Analysis Services (SSAS) in Ihrer Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store. .

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen auf dem neuesten Stand sind.

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Auf der ServiceNow AI Platform®, Verifizieren Sie die Konfiguration von Windows Anmeldeinformationen. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen

Während der horizontalen Erkennung erfasste Daten

Discovery Füllt die folgenden Daten aus, wenn das SSAS-Muster ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server Analysis Services [cmdb_ci_db_mssql_analysis]		
Bezeichnung	**Feld**	**Beschreibung**
Name	name	Die SSAS auf der Windows Servername
IP-Adresse	ip_address	Die SSAS-IP-Adresse
Version	Version	Die SSAS-Version
Edition	Edition	Die SSAS-Edition
Installationsverzeichnis	install_directory	Das SSAS-Installationsverzeichnis
Instanzname	Instanz	Der Name der SSAS-Instanz
TCP-Port(s)	tcp_port	Der SSAS-TCP-Port

Microsoft Discovery von SQL Server Integration Services (SSIS)

Die Discovery Und Service-Mapping Die Anwendung verwendet das SSIS-Muster, um SQL Server Integration Services (SSIS) in Ihrer Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie das Setup der Plugins

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Auf der ServiceNow AI Platform®, Verifizieren Sie die Konfiguration von Windows Anmeldeinformationen. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen

Daten, die während erfasst wurden Horizontal Discovery

Discovery Füllt die folgenden Daten aus, wenn das SSIS-Muster ausgeführt wird.

SQL Server-Integrationsservices [cmdb_ci_DB_mssql_Integration_list]		
Bezeichnung	**Feld**	**Beschreibung**
Name	name	Die SSIS auf der Windows Servername
IP-Adresse	ip_address	Die SSIS-IP-Adresse
Version	Version	Die SSIS-Version

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server-Integrationsservices [cmdb_ci_DB_mssql_Integration_list]		
Bezeichnung	**Feld**	**Beschreibung**
Edition	Edition	Die SSIS-Edition
Installationsverzeichnis	install_directory	Das SSIS-Installationsverzeichnis
Instanzname	Instanz	Der SSIS-Instanzname

Erkennung von Sun Java Enterprise System (JES)

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von Sun Java Enterprise System (JES) erkannt wird.

Standardmäßig verwendet Discovery das Muster *`Sun JES pattern`*, um Sun Java Enterprise System zu erkennen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Von Discovery für Sun Java Enterprise System erfasste Daten

In der JES-Tabelle [cmdb_ci_email_server_jes] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn

Erkennung von Tomcat-Servern

Discovery Identifiziert und klassifiziert Informationen zu Tomcat-Server-Webanwendungen, auf denen ausgeführt wird UNIX Computer.

Discovery kann Webanwendungen im Verzeichnis CATALINA_BASE oder im Verzeichnis CATALINA_HOME identifizieren und klassifizieren.

Der Klassifizierer verwendet für die Suche nach Tomcat-Serverprozessen die folgende Bedingung: [Parameter] [enthält] [org.apache.catalina.startup.Bootstrap].

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Applicative-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Tomcat	• Horizontal Pattern: Startet Muster • SSHCommand-Tomcat - Find web.xml List* • SSHCommand-Tomcat - Get server.xml* • SSHCommand-Tomcat - Get Version*	Tomcat

*Probes bei neuen Instanzen inaktiv

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Für Unix und Windows erfasst Discovery in der Tomcat-Tabelle [cmdb_ci_app_server_tomcat] die folgenden Daten:

Bezeichnung	Feldname	Quelle
Name	Name	server.info
Installationsverzeichnis	install_directory	server.xml
Version	Version	server.info
Serverport	server_port	server.xml
Attribute	attributes	server.xml

In der Tabelle „Tomcat Connector“ [cmdb_ci_tomcat_connector] werden für Unix und Windows die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Tomcat	tomcat	server.xml
Port	port	server.xml

In der Webanwendungs-Tabelle [cmdb_ci_web_application] werden für Unix und Windows die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Beschreibung	Beschreibung	web.xml
Dokumentenbasis	document_base	web.xml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname	Quelle
App-Server	app_server	web.xml

Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_app_server_tomcat	Enthält::Enthalten in	cmdb_ci_web_application

Erkennung von WebLogic-Anwendungsservern

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine Instanz von erkannt wird Oracle Oder BEA WebLogic-Anwendungsserver, der auf einem ausgeführt wird Windows Oder Linux System.

Anforderungen

Für Windows

- PowerShell muss auf dem MID Server aktiviert sein.
- Für die WebLogic-Administrationsserverinstanzen, die über WebLogic NodeManager starten, muss der Parameter *-Dweblogic.RootDirectory=<path>* beim Start des Servers definiert sein. Die Windows-Anmeldeinformationen müssen auch Leseberechtigungen für die Datei config.xml besitzen.

Für Linux

- Discovery erfordert die Verwendung der folgenden Bourne-Shell-Befehle:
  - `find`
  - `cat`
  - `dirname`
- Für WebLogic-Administrationsserverinstanzen, die über NodeManager gestartet wurden, muss der Parameter *-Dweblogic.RootDirectory=<path>* definiert und über den Linux-Befehl *ps process stat* (für jeden Administrationsserver) sichtbar gemacht werden, damit die CMDB mit den übrigen Informationen der Linux WebLogic-Anwendungsserver und -Webanwendungen gefüllt wird.
- Die folgende Konfiguration muss in der Datei sudorers festgelegt werden:

  `User ALL=(root) NOPASSWD: /bin/sh *`

  `User` entspricht dem Benutzernamen in den SSH-Anmeldeinformationen, die Sie für diese Erkennung erstellen.
- Der folgende Befehl muss ausgeführt werden können:

  `/bin/sh /tmp/snc-*-findcat.sh * *"`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nehmen Sie keine Änderungen an `findcat.sh` vor.

- Wenn Sie für die Weblogic-Erkennung Probes und keine Muster verwenden, müssen Sie in der Probe *`Linux - Weblogic - Find config.xml`* den folgenden Parameter und Wert angeben: *`must_sudo = true`*

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Weblogic-Server	• Horizontal Pattern: Startet Muster • Windows - Weblogic - Get web.xml* • Windows - Weblogic - Find config.xml* • Linux - Weblogic - Find config.xml*	WebLogic

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Unter Windows erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_app_server_weblogic	Name	Laufender Prozess
Version	cmdb_ci_app_server_weblogic	Version	config.xml
WebLogic-Domäne	cmdb_ci_app_server_weblogic	weblogic_domain	config.xml
TCP-Port(s)	cmdb_ci_app_server_weblogic	tcp_port	web.xml und laufender Prozess
Name	cmdb_ci_web_application	Name	config.xml
Dokumentenbasis	cmdb_ci_web_application	document_base	config.xml
Beschreibung	cmdb_ci_web_application	Beschreibung	web.xml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Quelle
Servlet-Klasse	cmdb_ci_web_application	servlet_class	web.xml
Servlet-Name	cmdb_ci_web_application	servlet_name	web.xml
App-Server	cmdb_ci_web_application	app_server	config.xml
TCP-Port(s)	cmdb_ci_web_application	tcp_port	web.xml

Unter Linux erfasste Daten

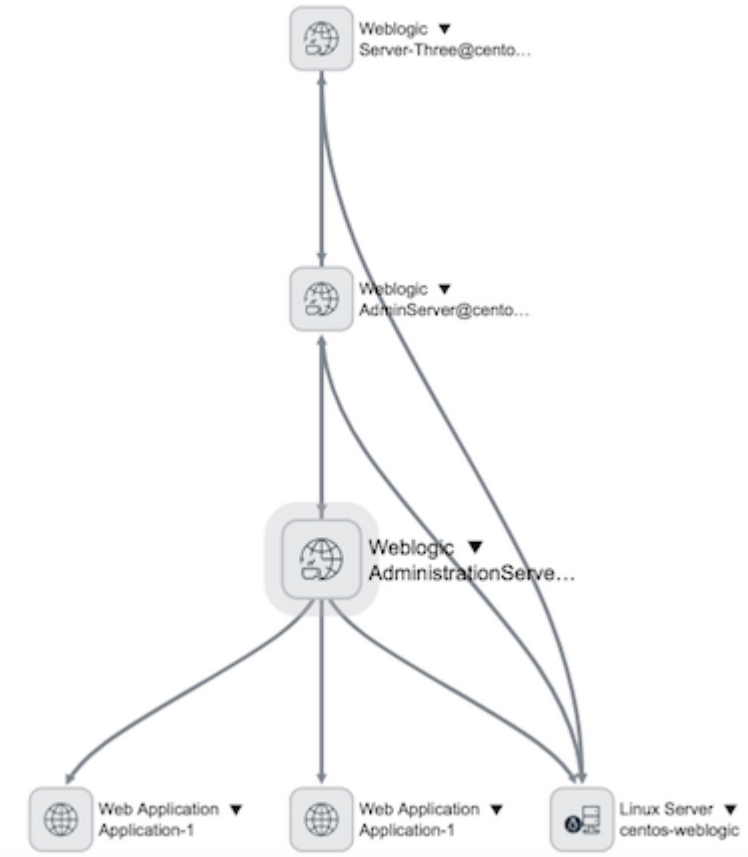
Tabelle	Feld	Quelle
cmdb_ci_app_server_weblogic	Name (name)	Laufender Prozess
cmdb_ci_app_server_weblogic	TCP-Port [tcp_port]	Laufender Prozess
cmdb_ci_app_server_weblogic	Version (version)	config.xml
cmdb_ci_app_server_weblogic	Weblogic-Domäne (weblogic_domain)	config.xml
cmdb_ci_web_application	Name (name)	config.xml
cmdb_ci_web_application	Kontextpfad (context_path)	config.xml
cmdb_ci_web_application	App-Server (app_server)	config.xml

Beziehung

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
cmdb_ci_app_server_weblogic	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server oder cmdb_ci_linux_server
cmdb_ci_app_server_weblogic	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_app_server_weblogic	Abhängig von::Verwendet von	cmdb_ci_app_server_weblogic Diese Beziehung wird zwischen einem Administrationsserver und allen von ihm gekapselten verwalteten Servern hergestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Weblogic-Beziehungen



sudo-Zugriff für die Probe „Weblogic - Find config.xml“ hinzufügen

Wenn Sie das Weblogic-Muster nicht verwenden, können Sie unter Linux der Probe „Weblogic - Find config.xml“ sudo-Berechtigungen hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**an.
2. Suchen Sie nach der Probe **Linux - Weblogic - Find config.xml**, und wählen Sie sie aus.
3. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf **Neu**.
4. Füllen Sie das Formular mit den folgenden Informationen aus:

Probe	Befehle
Name	must_sudo
Wert	Wahr

5. Klicken Sie auf **Absenden**.

Windows WebLogic-Anwendungsserver identifizieren

Falls Sie das Weblogic-Muster nicht verwenden, folgt Discovery diesem Prozess, wenn die Probes „Windows - Active Processes“ und „Linux - Active Processes“ verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Weblogic-Muster.

1. Die Probe „Windows - Active Processes“ oder „Linux - Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Die Parameter des Prozesses enthalten *`weblogic.Server`*.
   - Die Parameter des Prozesses enthalten *`-Dweblogic.name`*.
2. Wenn eine Übereinstimmung mit einem der folgenden Kriterien vorliegt:
   - Ein Datensatz wird in der BEA Weblogic-Tabelle [cmdb_ci_app_server_weblogic] erstellt. Der Datensatz wird mit dem Servernamen und dem TCP-Port gefüllt, die aus dem laufenden Prozess erfasst werden.
   - Die Probe „Windows - Weblogic - Find config.xml“ oder „Linux - Weblogic - Find config.xml“ wird ausgelöst. Der Sensor dieser Probe fügt dem BEA Weblogic-Datensatz [cmdb_ci_app_server_weblogic] und gegebenenfalls dem Webanwendungsdatensatz [cmdb_ci_web_application] zusätzliche Informationen hinzu.
3. Die Probe „Windows - Weblogic - Find config.xml“ oder „Linux - Weblogic - Find config.xml“ versucht wie folgt, die zugehörige Datei config.xml für den Server zu finden:
   - Mit dem im laufenden Prozess definierten Parameter *`-Dweblogic.RootDirectory=<path>`*.
   - [Windows] Durch Suche nach den config.xml-Dateien unter dem im laufenden Prozess definierten Parameter *`-Dplatform.home=<path>`* (nicht so effizient wie die Verwendung der Prozessparameter).
   - [Linux] Durch Suche nach dem übergeordneten Prozess, der den WebLogic-Server gestartet hat (nur möglich, wenn die WebLogic-JVM über *`startWeblogic.sh`* oder ein zugehöriges benutzerdefiniertes Skript und nicht über den init-Prozess gestartet wurde).
4. Wenn in der WebLogic-Datei config.xml zugehörige Webanwendungen gefunden werden, wird die Probe „Windows - Weblogic Find web.xml“ für jede Anwendung ausgelöst. Diese Probe liest die WebLogic-Datei web.xml für jede Webanwendung und den Sensor und fügt zusätzliche Informationen hinzu.

IBM WebSphere-Server-Discovery mithilfe von Probes

Die IBM WebSphere-Anwendungsserver ist ein Software-Framework mit Middleware, das Java-basierte Webanwendungen hostet. Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine Instanz eines WebSphere-Anwendungsservers erkannt wird, der auf einem ausgeführt wird Windows Oder Linux System.

Hinweis: Beginnend mit Visibility Content Version 6,1.0, musterbasierte Discovery ist die Standardmethode für die Erkennung IBM WebSphere-Anwendungsserver. Die WebSphere-Probes sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter IBM WebSphere-Anwendungsserver-Discovery mithilfe von Mustern.

Websphere-Erkennung unter Windows

Anforderungen für die Erkennung:

Aktivieren Sie für WebSphere-Anwendungsserver, die unter Windows ausgeführt werden, PowerShell auf dem MID Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Websphere-Erkennung unter Linux

Anforderungen für die Erkennung:

- Aktivieren Sie SSH auf dem WebSphere-Anwendungsserver.
- Legen Sie Ausführungsrechte fest, damit die folgenden Probes Befehle ausführen können:
  - WebSphere - Get serverindex.xml: cat/read-Berechtigungen für die Datei serverindex.xml
  - WebSphere - Get cell.xml: cat/read-Berechtigungen für die Datei cell.xml
  - WebSphere - Get server.xml: cat/read-Berechtigungen für die Datei server.xml

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Sonden und Sensoren

Discovery verwendet den folgenden Prozess, um Linux WebSphere-Anwendungsserver zu identifizieren:

1. Die Probe „Unix - Active Processes“ erkennt einen laufenden Prozess, der *`com.ibm.ws.runtime.WsServer`* entspricht. Beispielsweise enthält die Ausgabe des Prozesses *`...com.ibm.ws.bootstrap.WSLauncher com.ibm.ws.runtime.WsServer`* den Parameter */opt/IBM/WPS/profiles/ccmdb/config localhostNode01Cell ccmdb01 server1*. Die Werte sind:
   - letzter Parameter = Servername = Server1
   - letzter Parameter - 1 = Knotenname = ccmdb01
   - letzter Parameter - 2 = cell_name = localhostNode01Cell
   - letzter Parameter - 3 = config_path = ‘/opt/IBM/WPS/profiles/ccmdb/config’
2. Bei Übereinstimmung wird ein Datensatz in der IBM Websphere-Tabelle [cmdb_ci_app_server_websphere] erstellt. Die folgenden Probes werden ausgelöst:
   - WebSphere - Cell
   - WebSphere - Web Applications
   - WebSphere –Web Services
3. Von der Probe „WebSphere - Cell“ wird nach der cell.xml-Datei für die Instanz gesucht, indem die Parameter im ausgeführten Prozess verwendet werden und dann im zugehörigen Verzeichnis <config_path>\cells\<cell_name>\ gesucht wird.
4. Wenn die cell.xml-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen. Die zusätzlichen Tabellendatensätze der Tabelle [cmdb_ci_websphere_cell] werden nach Bedarf ausgefüllt.
5. Wenn die serverindex.xml -Datei von der Probe gefunden wurde, wird der Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webanwendungstabelle [cmdb_ci_web_application] werden nach Bedarf ausgefüllt.
6. Wenn die server.xml-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webservicetabelle [cmdb_ci_web_service] werden nach Bedarf ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery verwendet den folgenden Prozess, um Windows WebSphere-Anwendungsserver zu identifizieren:

1. Die Probe „Windows - Active Processes“ erkennt einen laufenden Prozess, der *com.ibm.ws.runtime.WsServer* entspricht. Beispielsweise enthält die Ausgabe des Prozesses *...com.ibm.ws.bootstrap.WSLauncher com.ibm.ws.runtime.WsServer* den Parameter */opt/IBM/WPS/profiles/ccmdb/config localhostNode01Cell ccmdb01 server1*. Die Werte sind:
   - letzter Parameter = Servername = Server1
   - letzter Parameter - 1 = Knotenname = ccmdb01
   - letzter Parameter - 2 = cell_name = localhostNode01Cell
   - letzter Parameter - 3 = config_path = ‘/opt/IBM/WPS/profiles/ccmdb/config’
2. Bei Übereinstimmung wird ein Datensatz in der IBM Websphere-Tabelle [cmdb_ci_app_server_websphere] erstellt. Die folgenden Probes werden ausgelöst:
   - Windows - WebSphere - Cell
   - Windows - WebSphere - Web Applications
   - Windows - WebSphere –Web Services
3. Die Probe „Windows - WebSphere - Cell“ sucht nach der Datei cell.xml für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis <config_path>\cells\<cell_name>\ gesucht wird.
4. Wenn die cell.xml-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen. Die zusätzlichen Tabellendatensätze der Tabelle [cmdb_ci_websphere_cell] werden nach Bedarf ausgefüllt.
5. Die Probe „Windows - WebSphere - Web Applications“ sucht nach der Datei serverindex.xml für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis <config_path>\cells\<cell_name>\nodes\<node_name> gesucht wird.
6. Wenn die serverindex.xml -Datei von der Probe gefunden wurde, wird der Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webanwendungstabelle [cmdb_ci_web_application] werden nach Bedarf ausgefüllt.
7. Die Probe „Windows WebSphere - Web Services“ sucht nach der Datei server.xml für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis <config_path>\cells\<cell_name>\nodes\<node_name>\servers\<server_name> gesucht wird.
8. Wenn die server.xml-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webservicetabelle [cmdb_ci_web_service] werden nach Bedarf ausgefüllt.

Erfasste Daten

Auf Websphere-Servern unter Windows erfasste Daten

Tabelle	Feld	Quelle
cmdb_ci_app_server_websphere	Name (name)	Laufender Prozess
cmdb_ci_websphere_cell	Name (name)	cell.xml
cmdb_ci_websphere_cell	Zellen-ID (cell_id)	cell.xml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf Websphere-Servern unter Windows erfasste Daten (Fortsetzung)

Tabelle	Feld	Quelle
cmdb_ci_websphere_cell	Zellentyp (cell_type)	cell.xml
cmdb_ci_websphere_cell	Zellenerkennungsprotokoll (cell_discovery_protocol)	cell.xml
cmdb_ci_web_service	Name (name)	server.xml
cmdb_ci_web_service	Service-ID (service_id)	server.xml
cmdb_ci_web_application	Name (name)	serverindex.xml

Auf Websphere-Servern unter Linux erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_websphere_cell	Name	server.xml
App-Server	cmdb_ci_web_service	app_server	Interne Referenz
Name	cmdb_ci_web_service	Name	server.xml
Name	cmdb_ci_web_application	Name	serverindex.xml
App-Server	cmdb_ci_web_application	app_server	serverindex.xml

Beziehungen

In der Tabelle „CI-Beziehungen“ [cmdb_rel_ci] werden die folgenden Beziehungen erstellt.

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
cmdb_ci_app_server_websphere	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_linux_server
cmdb_ci_win_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_win_server
cmdb_ci_app_server_websphere	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_web_service	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_app_server_websphere
cmdb_ci_websphere_cell	Enthält::Enthalten in	cmdb_ci_app_server_websphere

Erkennung von Datenbanken

Discovery kann nach Datenbankanwendungen wie MySQL, Oracle und MongoDB suchen. Außerdem kann Discovery auch nach Software zur Datenbankverwaltung wie MSSQL Server suchen.

Erkennung von Datenbankkatalogen

Der Datenbankkatalog listet alle Katalogobjekte oder Datenbanken auf, die für eine Instanz einer Datenbank erkannt wurden.

Datenbanken und Kataloge im Vergleich

Die meisten Datenbankhersteller verwenden den Begriff *Katalog* Bis Mittelwert *Datenbank* , Während Microsoft SQL verwendet den Begriff *Datenbank* . Datenbankkataloge können über das Erkennungstool eines Drittanbieters in Ihre Instanz importiert, manuell in die Plattform eingegeben oder von Discovery erkannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Discovery unterstützt keine MySQL-Datenbankkatalog-Discovery im Basissystem. Die Muster Oracle DB unter Unix und Oracle DB unter Windows erkennen Oracle-Katalogobjekte über die Mustererweiterung Get Catalog info (Kataloginformationen abrufen). Die Muster MSSQL DB unter Windows und MSSQL 2000 DB erkennen sowohl Datenbankinstanzen als auch Kataloge und speichern sie in den Datensätzen der Datenbankinstanz.

Weitere Informationen zu finden Oracle Katalog-Discovery, siehe Oracle Katalog-Discovery.

Weitere Informationen zu finden Microsoft SQL-Datenbankinstanzen, siehe Microsoft SQL Server- und Cluster-Discovery.

Wenn Sie Datenbankkataloge mit Probes erkannt haben, bevor Sie zu Mustern migrieren, können Sie die probenbasierten Datenbankkataloge anzeigen, indem Sie zu navigieren **Alle** > **Konfiguration** > **Datenbankkataloge** Und Auswahl einer Datenbank.

Discovery des Berichts „Datenbankadministrator" (DBA)

Discovery Und Service-Mapping Verwendet Muster Erweiterungsabschnitte zur Bereitstellung eines Datenbankadministratorberichts (DBA-Bericht) für Apache Cassandra, Microsoft SQL, MySQL, MongoDB und Oracle Datenbanken. Die Erweiterungsabschnitte für jedes DB-Muster füllen die zugehörigen Eintragstabellen aus. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie das Setup der Plugins

- CMDB CI-Klassenmodelle 1.49.0 (September 2023)
- Muster für Discovery und Service-Mapping 1.8.0 (September 2023)

Überprüfen Sie, ob die Systemeigenschaften aktiviert sind

Standardmäßig sind die Systemeigenschaften für DBA-Berichte auf festgelegt **Falsch** . Um die Berichtssammlung zu aktivieren, überprüfen Sie, ob der Wert der Systemeigenschaften für jedes Muster auf festgelegt ist **Wahr** .

Muster	Systemeigenschaft
Cassandra	cassandra_DBA_Report_enabled
MongoDB	mongo_DBA_Report_enabled
MSSQL-DB unter Windows	mssql_DBA_Report_enabled
Mein SQL-Server unter Windows und Linux	mysql_DBA_Report_enabled
Oracle-DB	oracle_DBA_Report_enabled

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Weitere Informationen finden Sie unter Applicative-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Ausführungsbefehl	Anwendbare Anmeldeinformationen müssen Lesezugriff haben, um ausgeführt zu werden „GetSiblingDB (databaseName)“
Apache Cassandra Befehl ausführen	Discovery-Anmeldeinformationen müssen Lesezugriff auf haben „Nodetool“
MySQL-Tabellen und Ausführungsbefehle	Discovery-Anmeldeinformationen müssen Lesezugriff auf haben: • „Information_Schema.Tabellen“ Tabelle • Ausführen „Datenbanken anzeigen“ Befehl
Microsoft SQL-Tabellen	Discovery-Anmeldeinformationen müssen Lesezugriff auf die folgenden Tabellen haben: • *master.sys.databases* • *sys.sysprocesses* • *sys.dm_os_sys_info* • *sys.dm_os_ring_buffers* • *msdb.dbo.backupset* • *master.dbo.sysdatabases* • *master..sysprocesses* • *msdb..sysjobactivity* • *sys.master_files* • *sys.dm_tran_session_transactions* • *sys.dm_os_sys_memory* • *sys.database_files*
Oracle DB-Tabellen und Ausführungsbefehle	Discovery Anmeldeinformationen müssen Lesezugriff auf haben: • Ausführen „Lsnrctl-Services“ Und „Sqlplus“ Befehle • *dba_data_files* Tabelle • *dba_segments* Tabelle • *v$database* Tabelle • *gv$instance* Tabelle • *dba_hist_osstat* Tabelle • *dba_hist_snapshot* Tabelle • *v$asm_disk* Tabelle • *v$asm_diskgroup* Tabelle • *dba_audit_session* Tabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	• *gv$session_longops* Tabelle • *gv$session* Tabelle • *gv$sqlarea* Tabelle • *gv$process* Tabelle

Überprüfen Sie, ob ein Discovery Zeitplan ist konfiguriert

Weitere Informationen finden Sie unter Erstellen Sie einen Discovery-Zeitplan

Daten, die vom Erweiterungsabschnitt von erfasst werden Apache Cassandra Muster

Discovery Füllt die folgenden Daten aus, wenn ausgeführt wird Apache Cassandra Muster.

Hinweis: Wichtige Informationen zum Aktivieren der Systemeigenschaft finden Sie im Abschnitt Voraussetzungen.

Tabellenname	Tabellenbezeichnung	Felder
cassandra_Health_Report	Cassandra-Integritätsbericht	• Database_Host • LOCAL_write_Latency • Read_Latency • Snapshot_used_space • Space_used • table • Keyspace • CI

Daten, die vom Erweiterungsabschnitt des MongoDB-Musters erfasst werden

Discovery Füllt die folgenden Daten aus, wenn das MongoDB-Muster ausgeführt wird.

Hinweis: Wichtige Informationen zum Aktivieren der Systemeigenschaft finden Sie im Abschnitt Voraussetzungen.

Tabellenname	Tabellenbezeichnung	Felder
mongo_DB_statistics	Mongo DB-Statistiken	• Database_Host • Database_Name • fs_total_size • fs_used_size • Scale_factor • Index_size

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
		• Index_count • Extents_count • Storage_size • Data_size • Average_object_size • Objects_count • Collection_count • view_count • CI

Daten, die vom Erweiterungsabschnitt des MSSQL-Musters erfasst werden

Discovery Füllt die folgenden Daten aus, wenn MSSQL ausgeführt wird Muster .

Hinweis: Wichtige Informationen zum Aktivieren der Systemeigenschaft finden Sie im Abschnitt Voraussetzungen.

Tabellenname	Tabellenbezeichnung	Felder
ms_sql_DB_Blocking_info	MSSQL DB – Blockierungsinformation	• Database_Host • database_instance • Definition • object_name • Blocking_spid • spid • CI
ms_sql_DB_cpu_util	MS SQL DB CPU-UTIL	• Database_Host • database_instance • Load_date • Other_Process_cpu_util • Other_Process • System_Idle_Process • sql_Server_cpu_util • Event_time • server_name • CI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
ms_sql_DB_not_Backup	MSSQL-DB nicht gesichert	• Database_Host • database_instance • Last_Backup_date • database_name • CI
ms_sql_DB_running_Job	MSSQL DB – ausgeführter Auftrag	• Database_Host • database_instance • Login_Name • nt_Domain • cmd • hostname • name • status • Open_tran • Spid • Last_wait_type • Login_time • CI
ms_sql_Disk_info	MSSQL DB – Datenträgerinformation	• Database_Host • database_instance • Percentage_free_space • Volume_free_space • Volume_Capacity • Volume_label • volume_name • CI
ms_sql_files_space	MSSQL DB – Dateibereich	• Database_Host • database_instance • database_name • Free_space_mb • File_size_mb • file_type

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
		• Datei_Logik_Name • CI
ms_sql_Fregment_info	MSSQL DB – Fragmentierungsinformation	• Database_Host • database_instance • index_status • page_count • durchschn._frag • index_name • object_name • Schema_Name • CI
ms_sql_Last_restart	MSSQL DB – letzter Neustart	• Database_Host • database_instance • Betriebszeit_in_Tagen • Current_date • Last_Recycle • CI
ms_sql_Long_trans	Ms SQL DB – lange Transaktionen	• Database_Host • database_instance • Blockiert • sql • cmd • Program_Name • hostname • Login_Name • status • Last_Batch • Dauer • Login_time • database_name • User_tran • Trans_ID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
		• spid • CI
ms_sql_Memory_info	MSSQ DB – Datenträgerinformation	• Database_Host • database_instance • System_Memory_State_desc • percentage_used • Available_page_file_mb • Total_page_file_mb • Available_physical_Memory_mb • Total_physical_Memory_mb • CI
ms_sql_Temp_files_space	Speicherplatz für temporäre MSSQL DB-Dateien	• Database_Host • database_instance • Percent_Full • Available_space_mb • Datei_physischer_Name • Datei_Logik_Name • database_name • CI

Daten, die vom Erweiterungsabschnitt des MySQL-Musters erfasst werden

Discovery Füllt die folgenden Daten aus, wenn das MySQL-Muster ausgeführt wird.

Hinweis: Wichtige Informationen zum Aktivieren der Systemeigenschaft finden Sie im Abschnitt Voraussetzungen.

Tabellenname	Tabellenbezeichnung	Felder
mysql_table_Schemas	MySql-Tabellenschemata	• Database_Host • database_instance • Data_index_lengh • Table_Schema • CI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten, die vom Erweiterungsabschnitt von erfasst werden Oracle DB-Muster

Discovery Füllt die folgenden Daten aus, wenn ausgeführt wird Oracle DB-Muster.

Hinweis: Wichtige Informationen zum Aktivieren der Systemeigenschaft finden Sie im Abschnitt Voraussetzungen.

Tabellenname	Tabellenbezeichnung	Felder
oracle_Active_Session	Oracle Aktive Sitzung	• Database_Host • database_instance • Schlüssel • sql_ID • Programm • Modul • Aktion • status • Last_call_et_Std • sid • spid • Inst • CI
oracle_asm_info	Oracle, ASM-Datenträgerinformationen	• Database_Host • database_instance • Used_gb • Free_gb • Total_gb • Status • Block_size • ASM • CI
oracle_asm_nodes_info	Oracle Informationen zum ASM-Knoten-Datenträger	• Database_Host • database_instance • Redundanz • Free_gb • Total_gb • Status

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
		• asm_node • CI
oracle_cpu_usage	Oracle CPU-Auslastung	• Database_Host • database_instance • Inaktiv • e/A • sys • Schön • Anwender • Snapshot-ID • Inst • end_time • BEGIN_time • CI
oracle_inactive_Sessions	Oracle Inaktive Sitzungen	• Database_Host • database_instance • key • status • spid • sid • Programm • Modul • Last_call_et_Std • Inst • CI
oracle_instance_info	Oracle Instanzinformationen	• Database_Host • database_instance • Plattformname • Current_scn • dbid • db_unique_name • Log_Mode • db_name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Tabellenbezeichnung	Felder
		• Open_Mode • CI
oracle_nodes_info	Oracle Knoteninformationen	• Database_Host • database_instance • Instance_Mode • Instance_State • Instance_role • Instance_Status • Instance_Version • hostname • instance_name • CI
oracle_table_space	Oracle Tabellenbereich	• Database_Host • database_instance • Used_mb • Free_percent • Free_mb • Tabellenbereich • Total_mb • CI
oracle_Top_10_Abfragen	Oracle Top-10-Abfragen	• Database_Host • database_instance • Eindeutig • status • sql_ID • spid • sid • Programm • Modul • Last_call_et_Std • CI

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft SQL Server- und Cluster-Discovery

Die Muster für Discovery und Service-Mapping Die Anwendung verwendet die MSSQL DB auf Windows-Muster, um zu finden Microsoft SQL DB-Server und -Cluster in Ihrer Infrastruktur. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Detaillierte Informationen zu unterstützten SQL Server-Versionen finden Sie unter: Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Voraussetzungen

Überprüfen Sie, ob die folgenden Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping Ab Version 1.7.0 (August 2023)
- Visibility Content Ab Version 6.12.1 (August 2023)

Erstellen Windows Anmeldeinformationen

Nachdem überprüft wurde, dass MID-Server Ist mit dem Ziel verbunden Windows Server, erstellen Windows Anmeldeinformationen für ServiceNow AI Platform. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen .

Erstellen Sie bei Verwendung der SQL-Authentifizierung anwendbare Anmeldeinformationen

Weitere Informationen finden Sie unter Anwendbare Anmeldeinformationen .

Überprüfen Sie die Konfiguration von MID-Server

Überprüfen Sie, ob MID-Server Verfügt über die erforderlichen Berechtigungen zum Lesen von Windows Registrierung in einem Remote-Modus. Die MSSQL-DB unter Windows-Muster verwendet Registrierungswerte, um SQL-Clusterdetails zu erkennen.

Überprüfen Sie, ob der SQL Server-Discovery-Bericht aktiv ist

Überprüfen Sie, ob der SQL Server-Discovery-Bericht auf Ihrem Server aktiv ist. Discovery Verwendet den SQL Server-Discovery-Bericht, um Microsoft SQL Server-Komponenten zu erkennen.

Überprüfen Sie die Berechtigungen zum Ausführen von WMI-Abfragen

Überprüfen Sie den schreibgeschützten Remote-Zugriff auf die folgenden WMI-Namespaces:

- `Stamm\CIMv2`
- `Stamm\Microsoft\SQLServer\Computermanagement*`

Überprüfen Sie die Berechtigungen der SQL Server-Tabelle

Die MSSQL-DB unter Windows-Muster erfordert schreibgeschützte Berechtigungen zum Lesen der folgenden Tabellen:

- `@@Version`
- `sys.Konfigurationen`
- `sys.dm_exec_sessions`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys.dm_os_Schedulers
- SERVICE

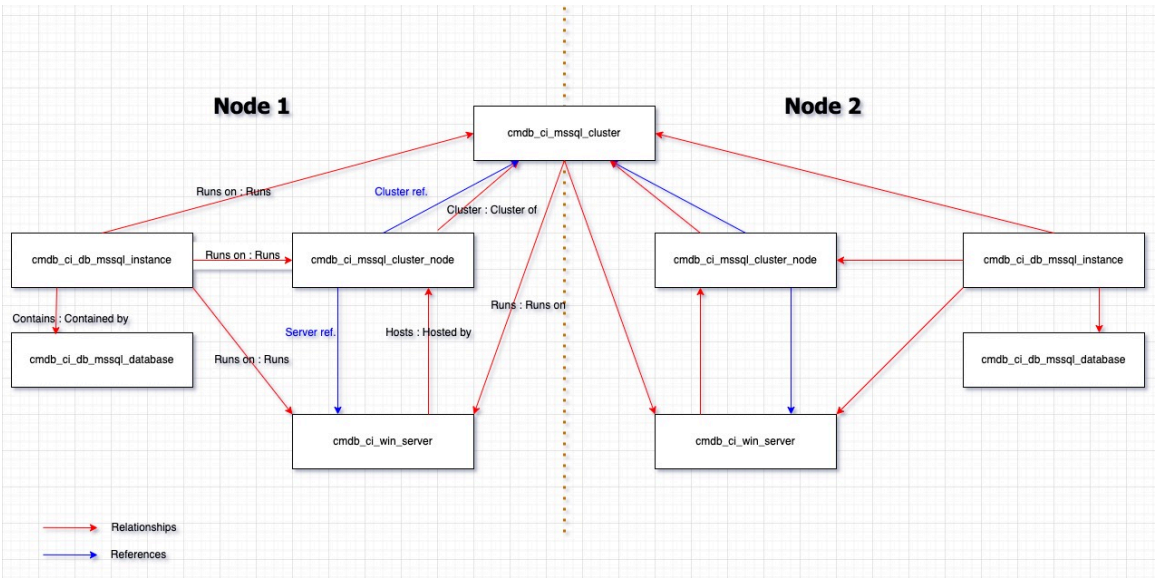
Überprüfen Sie die Berechtigungen der Verfügbarkeitsgruppentabelle

Überprüfen Sie die folgenden Tabellenberechtigungen, um zu erkennen Microsoft SQL Server immer in Verfügbarkeitsgruppen:

- **ZEIGEN SIE DEN SERVERSTATUS AN** Zugriff auf sys.dm_hadr_Availability_Group_states Tabelle
- Lesezugriffsberechtigung für die folgenden Tabellen:
  - sys.Availability_groups
  - sys.Availability_Group_listeners
  - sys.Availability_Group_listener_ip_address

SQL-Failover-Clusterinstanz (FCI)

Der Satz von Mustern der Version 1.6.1 wird aktualisiert, die in verfügbar sind ServiceNow® Store Ab August 2023 wird eine entsprechende Discovery der Details der Verfügbarkeitsgruppe „Always on“ und der SQL Failover-Cluster aktiviert. Wenn das Failover-Szenario auftritt, erkennt das Muster MSSQL DB unter Windows den Failover-Cluster (Knoten 2). Dann werden eine neue MSFT SQL-Instanz und Datenbanken erstellt.



Das folgende Verfahren ermöglicht eine angemessene Sichtbarkeit der SQL-Cluster.

1. Legen Sie fest *sn_itom_pattern.discover_mssql_cluster.load_cluster_name_from_registry=true* MID-Server Eigenschaft bis **Wahr** Zum Aktivieren von **MSSQL-Clusterinformationen erfassen: MSSQL-Cluster** Erweiterungsabschnitt.
2. Stellen Sie sicher, dass ein Sqlservr.exe Prozess zum Auslösen der MSSQL DB unter Windows-Muster wird auf dem Server ausgeführt.
3. Führen Sie eine CI-Discovery aus.

   Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.
4. Behalten Sie doppelte Instanzen und Datenbanken bei, oder löschen Sie sie.

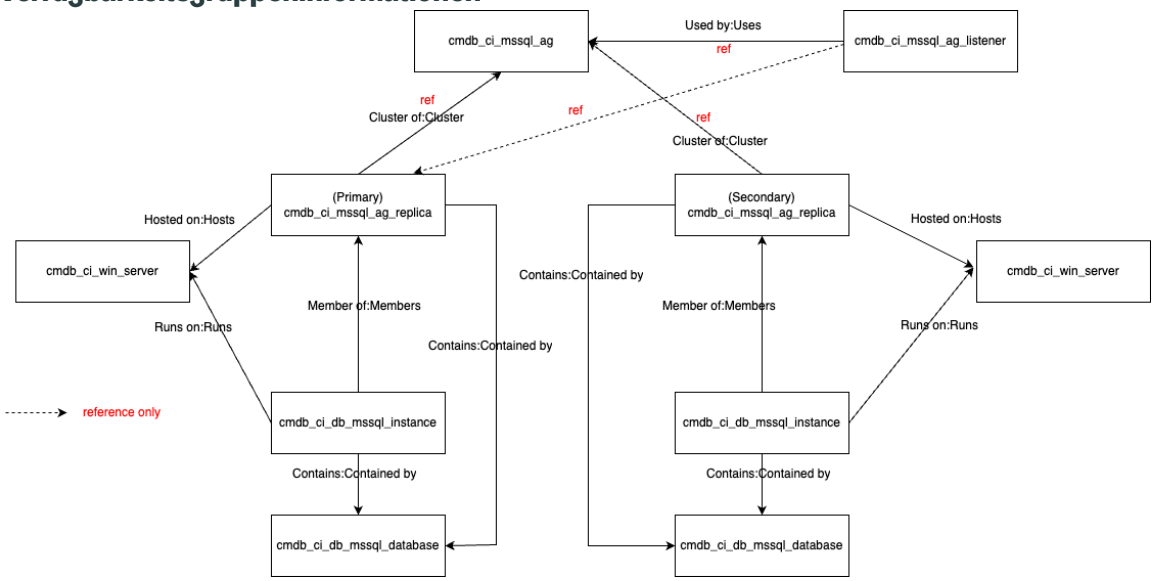
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die doppelten Instanzen und Datenbanken beizubehalten, behalten Sie die Standardkonfiguration bei.
  - Der Installationsstatus der Knoten des passiven Clusters ändert sich in **Abwesend** .
  - Der Installationsstatus der Knoten des aktiven Clusters ändert sich in **Installiert** .
- Um die passiven Instanzen und Datenbanken zu löschen, legen Sie fest `discovery.mssql.cluster.instance.postsensor.delete`Systemeigenschaft zu **Wahr** .

Microsoft SQL Server-Unterstützung für Verfügbarkeitsgruppen immer

Beginnt ab Muster für Discovery und Service-Mapping Version 1.27.0, die MSSQL DB auf Windows-Mustererweiterung **Sammeln Sie MSSQL HADR – Verfügbarkeitsgruppeninformationen** Unterstützt die Discovery von Microsoft SQL Server immer in Verfügbarkeitsgruppen.

Datenmodell von „MSSQL-HADR erfassen – Verfügbarkeitsgruppeninformationen“



Voraussetzungen

Überprüfen Sie die Berechtigungen der Verfügbarkeitsgruppentabelle

Erkannte Ressourcen

Von der Mustererweiterung erkannte Ressourcen: MSSQL HADR sammeln – Verfügbarkeitsgruppeninformationen

Erkannte Beziehungen

Von der Mustererweiterung erkannte Beziehungen: MSSQL HADR sammeln – Verfügbarkeitsgruppeninformationen

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery Füllt die Daten in aus CMDB Beim Ausführen der MSSQL-DB auf Windows-Muster.

MSFT SQL-Instanz [cmdb_ci_DB_mssql_instance]

Die für die laufenden Prozesse der Datenbank (der tatsächliche SQL-Server) erfassten Daten werden als bezeichnet *Datenbankinstanz*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name [name]	Der Feldname. Beispiel: MSSQLSERVER@Windows_Server_Name
Instanzname [instance_Name]	Der Name der SQL Server-Instanz. Beispiel: MSSQLSERVER
Ist geclustert [is_clustered]	Gibt den Typ der Installation an: • Wenn dieser Wert auf festgelegt ist **Wahr** , Der SQL-Server ist Teil eines Clusters, und der Failover-Mechanismus ist aktiviert. • Wenn dieser Wert auf festgelegt ist **Falsch** , Der SQL-Server ist eine eigenständige Bereitstellung, und der Failover-Mechanismus ist deaktiviert.
Kommentare [comments]	Der Typ der Instanz: • Standalone_instance • Failover_Cluster • Always_on
Version [version]	Die SQL Server-Versionsnummer. Beispiel: 16.0.1000.6
Versionsname [Version_Name]	Die SQL Server-Version nach Releasedaten. Beispiel: Der Wert **2022** Stellt Version dar **16.0.1000.6**
Service Pack [Service_Pack]	Die Service Pack-Version. Beispiel: SP2.
Edition [edition]	Der Typ der Edition. Beispiel: Enterprise-Edition.
TCP-Port [tcp_port]	Der TCP-Port, den die MSSQL-Instanz zum Akzeptieren von Verbindungen verwendet.
Installationsstatus [install_status]	Der Installationsstatus der Instanz: **Installiert** – Die Instanz wird derzeit ausgeführt. **Abwesend** – Die Instanz wird nicht ausgeführt, und sie ist die Sicherungsinstanz für ein Failover-Szenario.

MSSQL-Datenbank [cmdb_ci_db_mssql_database]

Feld	Beschreibung
Name [name]	Name der Datenbank Beispiel: Msdb.
Installationsstatus [install_status]	Der Installationsstatus der Datenbank.
Instanzname [instance_Name]	Der Name der Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSSQL-Clusterknoten [cmdb_ci_mssql_cluster]

Feld	Beschreibung
Name [name]	Der Serverhostname
IP-Adresse [ip_address]	Das Hosting Windows IP-Adresse des Servers
Cluster [cluster]	Verweis auf den SQL-Cluster-Datensatz.
Server [Server]	Verweis auf das Hosting Windows Serverdatensatz.

MSSQL-Cluster [cmdb_ci_mssql_cluster]

Feld	Beschreibung
Name [name]	Der SQL-Cluster-Netzwerkname
IP-Adresse [ip_address]	Die virtuelle IP-Adresse des SQL-Clusters.

MSSQL-Serviceinformation [mssql_sqlservice_info]

Feld	Beschreibung
Beschreibung [description]	Beschreibt den MSSQL-Service. Beispiel: „Bietet Speicherung, Verarbeitung und kontrollierten Zugriff auf Daten und schnelle Transaktionsverarbeitung.“
Servicename [service_name]	Der MSSQL-Servicename, wie auf dem Server angezeigt. Beispiel: MSSQL$NAMEDMSSQL2016
Binärpfad [binary_path]	Der Dateipfad des Service. Beispiel: C:\Programme\Microsoft SQL Server\MSSQL13.NAMEDMSSQL2016\MSSQL\Binn\sqlservr.exe
CI [ci]	Verweis auf MSFT SQL-Instanzdatensatz [cmdb_ci_DB_mssql_instance]
Installiert auf [installed_on]	Verweis auf Windows Serverdatensatz [cmdb_ci_WIN_Server] **Hinweis:** Dieses Feld ist für eigenständige Bereitstellungen nicht ausgefüllt.

Informationen zu MSSQL-Komponenten [mssql_components_info]

Feld	Beschreibung
Installationspfad [install_path]	Der Installationspfad des Komponentenservice. Feindbeispiel: C:\Programme\Microsoft SQL Server\MSSQL16.SQLEXPRESS\MSSQL
Servicename [service_name]	Der Komponentenservicetyp des Servers. Beispiel: **Datenbank-Engine-Services**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
SKU-Name [sku_name]	Die MSSQL-Version des Komponentenservice. Beispiel: **Express-Edition (64-Bit)**
Version [version]	Die MSSQL-Versionsnummer des Komponentenservice
CI [ci]	Verweis auf den MSFT SQL-Instanzdatensatz.
Installiert auf [installed_on]	Verweis auf Windows Serverdatensatz [cmdb_ci_WIN_Server]. **Hinweis:** Dieses Feld wird nur für SQL-Cluster und nicht für eigenständige Bereitstellungen ausgefüllt.

MSSQL DB in Windows-Mustererweiterung: MSSQL HADR – Verfügbarkeitsgruppeninformationen erfassen

MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]

Feld	Beschreibung
Cluster-ID [cluster_id]	Global Unique Bezeichner (GUID) der Verfügbarkeitsgruppe.
Name [name]	Clustername
IP-Adresse [ip_address]	IP-Adresse des Clusters.

Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]

Feld	Beschreibung
Replikat-ID [Replica_ID]	Eindeutige ID des Replikats.
Rolle [Rolle]	Rolle des Replikats. Mögliche Werte: • Primär • Sekundär • Auflösen
Verfügbarkeitsmodus [Availability_Mode]	Verfügbarkeitsmodus des Replikats. Mögliche Werte: • Asynchroner Commit • Synchroner Commit • Nur Konfiguration
Failover-Modus [Failover_Mode]	Failover-Modus des Verfügbarkeits-Replikats. Mögliche Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica] (Fortsetzung)

Feld	Beschreibung
	• Automatisch • Manuell
Lesbar sekundär [lesbar_sekundär]	Gibt an, ob ein Verfügbarkeitsreplikat, das die sekundäre Rolle ausführt, Verbindungen von Clients akzeptieren kann. Mögliche Werte: • wahr • falsch
Verfügbarkeitsgruppe [Availability_Group]	Verweist auf die Tabelle „MSSQL-Verfügbarkeitsgruppe“ [cmdb_ci_mssql_ag].
Name [name]	Name des Replikatservers.
Seriennummer [serial_number]	Eindeutige ID des Replikats.
Status [state]	Failover-Status. Mögliche Werte: • Ausstehend • Online • Offline • Fehlgeschlagen • Fehlgeschlagen – kein Quorum

MSSQL-Verfügbarkeitsgruppen-Listener [cmdb_ci_mssql_ag_Listener]

Feld	Beschreibung
Name [name]	Name des Verfügbarkeitsgruppen-Listeners.
Listener-ID [listener_ID]	Global Unique Bezeichner (GUID) der Ressource von Windows WSFC-Cluster (Server Failover Clustering).
IP-Subnetzmaske [ip_Subnet_mask]	IP-Subnetzmarke für die IPv4-Adresse, falls vorhanden, die für den Verfügbarkeitsgruppen-Listener konfiguriert ist.
Verfügbarkeitsgruppe [Availability_Group]	Verweist auf die Tabelle „MSSQL-Verfügbarkeitsgruppe“ [cmdb_ci_mssql_ag].
Primäres Replikat [primary_replica]	Verweist auf die Tabelle „Replikat der MSSQL-Verfügbarkeitsgruppe“ [cmdb_ci_mssql_ag_Replica].

CI-Beziehungen

Die MSSQL-DB unter Windows erstellt CI-Beziehungen mithilfe von **Sammeln Sie Informationen zu MSSQL-Komponenten** Mustererweiterung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Windows-Server [cmdb_ci_WIN_Server]	Wird ausgeführt:Wird ausgeführt auf	MSSQL-Cluster [cmdb_ci_mssql_Cluster]
MSFT SQL-Instanz [cmdb_ci_DB_mssql_instance]	Wird ausgeführt:Wird ausgeführt auf	MSSQL-Cluster [cmdb_ci_mssql_Cluster]
MSSQL-Clusterknoten [cmdb_ci_mssql_Cluster_node]	Cluster::Cluster von Referenz [Cluster]	MSSQL-Cluster [cmdb_ci_mssql_Cluster]
Windows-Server [cmdb_ci_WIN_Server]	Hosts::gehostet von Referenz [Server]	MSSQL-Clusterknoten [cmdb_ci_mssql_Cluster_node]
MSFT SQL-Instanz [cmdb_ci_DB_mssql_instance]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_WIN_Server]
MSFT SQL-Instanz [cmdb_ci_DB_mssql_instance]	Enthält::enthalten in	Ms SQL-Datenbank [cmdb_ci_DB_mssql_database]
MSSQL-Serviceinformation [mssql_sqlservice_info] **Hinweis:** Diese Beziehung wird nur erstellt, wenn das Muster die WMI-Abfragen verwendet.	Referenz	MSFT SQL-Instanz☒ [cmdb_ci_DB_mssql_instance]

Die MSSQL-DB unter Windows erstellt CI-Beziehungen mithilfe von **Sammeln Sie MSSQL HADR – Verfügbarkeitsgruppeninformationen** Mustererweiterung.

CI	Beziehung	CI
MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]	Erstreckt sich von	Cluster [cmdb_ci_cluster]
MSFT SQL-Instanz [cmdb_ci_DB_mssql_instance]	Mitglied von::Mitglieder	Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]
MSSQL-Verfügbarkeitsgruppen-Listener [cmdb_ci_mssql_ag_Listener]	Erstreckt sich von	Endpunkt [cmdb_ci_Endpoint]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
MSSQL-Verfügbarkeitsgruppen-Listener [cmdb_ci_mssql_ag_Listener]	Referenzen	MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]
MSSQL-Verfügbarkeitsgruppen-Listener [cmdb_ci_mssql_ag_Listener]	Referenzen	Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]
MSSQL-Verfügbarkeitsgruppen-Listener [cmdb_ci_mssql_ag_Listener]	Verwendet von::Verwendet	MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]
Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]	Enthält::Enthalten in	Ms SQL-Datenbank [cmdb_ci_DB_mssql_database]
Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]	Cluster von::Cluster	MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]
Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]	Erstreckt sich von	MSSQL-Clusterknoten [cmdb_ci_mssql_Cluster_node]
Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]	Gehostet auf::Hostet	Windows-Server [cmdb_ci_WIN_Server]
Replikat der MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag_Replica]	Referenzen	MSSQL-Verfügbarkeitsgruppe [cmdb_ci_mssql_ag]

Zugehörige Informationen

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Probe „Horizontal Pattern“

Discovery des Berichts „Datenbankadministrator“ (DBA)

MySQL-Erkennung

Discovery Kann eine Instanz von MySQL identifizieren, die auf ausgeführt wird UNIX Oder Windows Betriebssysteme.

Anforderungen

Discovery sucht für die folgenden Bereiche nach dem Speicherort der MySQL-Konfigurationsdatei:

- UNIX: Discovery sucht nach dem Speicherort der MySQL-Konfigurationsdatei im Prozess mysqld oder an Port 3306.
- Windows: Discovery sucht nach dem Speicherort der MySQL-Konfigurationsdatei im Prozess mysqld.exe oder an Port 3306.

Für jeden Prozess werden die folgenden Prozessparameter in der folgenden Reihenfolge untersucht:

`--defaults-extra-file`

`--defaults-file`

Wenn der Speicherort der MYSQL-Konfigurationsdatei bei dieser Suche nicht gefunden wird, geschieht Folgendes:

- UNIX: Für den Speicherort der Konfigurationsdatei wird standardmäßig /etc/my.cnf übernommen.
- Windows: Es ist kein Standardspeicherort für Konfigurationsdateien vorhanden, und die Probe zum Lesen des Speicherorts für Konfigurationsdateien wird übersprungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen
- Anwendbare Anmeldeinformationen (Wenn Anwendungen zusätzlich zu den Anmeldeinformationen Anmeldeinformationen erfordern, benötigt der Host-Computer.)

Hinweis: Sie müssen keine anwendbaren Anmeldeinformationen konfigurieren, es sei denn, Ihre Discovery-Voraussetzungen enthalten sie.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Klassifizierer, Muster und Probes

Zur MySQL-Erkennung verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

Klassifizierung	Auslöser-Probes	Muster
MySQL-Server	• Horizontal Pattern: Startet Muster • Windows - MySQL Configuration* • Windows - MySQL Version* • MySQL - Configuration* • MySQL - Version*	My SQL server On Windows and Linux - Muster

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Discovery füllt die folgenden Felder in der Tabelle „MySQL-Instanz“ [cmdb_ci_db_mysql_instance]:

Bezeichnung	Feldname	Quelle
MySQL-Konfiguration	myconf	my.cnf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname	Quelle
TCP-Port(s)	tcp_port	running_process
Version	Version	mysqld

Zugehörige Informationen

Discovery des Berichts „Datenbankadministrator“ (DBA)

MongoDB-Erkennung

Discovery Erstellt oder aktualisiert einen CMDB Erfassen Sie, wenn eine laufende Instanz von MongoDB erkannt wird.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Die folgenden Daten werden erfasst:

Von Discovery für MongoDB-Instanzen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Version	cmdb_ci_db_mongodb_instance	Version	mongod (UNIX) oder mongod.exe (Windows)
Mongo-Konfiguration	cmdb_ci_db_mongodb_instance	mongodb_conf	mongod.conf
TCP-Port(s)	cmdb_ci_db_mongodb_instance	tcp_port	Prozessklassifizierung oder mongod.conf

PostgreSQL-Erkennung

Discovery kann ausgeführte Instanzen von PostgreSQL auf finden Windows Und Linux Systeme.

Anmeldeinformationen und andere Voraussetzungen

Die folgenden Anmeldeinformationen sind erforderlich:

- SSH-Anmeldeinformationen
- [Optional] Anwendbare Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Benutzer muss Root-Zugriff auf die Datenbank haben, um auf die Datei `postgresql.conf` zugreifen zu können.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
PostgreSQL-Instanz	• Horizontal Pattern: Startet Muster • PostgreSQL - Configuration* (diesem Probe Parameter *must_sudo* hinzufügen) • PostgreSQL - Version*	PostgreSQL-DB

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Mit dem folgenden Verfahren werden die angegebenen Informationen vom Ziel erfasst. Wenn die Quelle nicht konfiguriert ist, werden Standardinformationen zurückgegeben. Beispiel: Für PostgreSQL Instance@hostname (Standardname) muss die Quelle geändert werden. Andernfalls werden für die Tabelle [cmdb_ci_db_postgresql_instance] alle „PostgreSQL Instance@hostname“-Namen der Quelle hinzugefügt.

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_db_postgresql_instance	Name	PostgreSQL Instance@*Hostname*
Datenverzeichnis	cmdb_ci_db_postgresql_instance	data_dir	Laufender Prozess
TCP-Port	cmdb_ci_db_postgresql_instance	tcp_port	Laufender Prozess
SQL-Konfiguration	cmdb_ci_db_postgresql_instance	postgres_conf	*Datenverzeichnis*/postgresql.conf
Version	cmdb_ci_db_postgresql_instance	Version	postmaster/postgres

Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_db_postgresql_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server oder cmdb_ci_linux_server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Datenbank-Discovery

Discovery Kann identifizieren Oracle Datenbankinstanz, die auf ausgeführt wird UNIX Oder Windows Betriebssysteme. Von Discovery kann auch Oracle-Clusterware erkannt werden, von der Real Application Clusters (RAC) ausgeführt werden.

Muster führen die Discovery von durch Oracle Installationen. Diese Muster ersetzen mehrere Probes für neue Instanzen. Wenn Sie weiterhin Probes verwenden möchten, können Sie die Probe „Horizontal Discovery“ deaktivieren, die das Muster startet, und dann die erforderlichen Probes aktivieren.

Hinweis: Oracle DB unter Unix und Oracle DB unter Windows unterstützen die RAC-Discovery mit einem Knoten nicht.

Oracle DB unter Unix und Oracle DB unter Windows-Muster erkennen Oracle Katalotobjekte über die Mustererweiterung erhalten Kataloginformationen. Weitere Informationen finden Sie unter Oracle Katalog-Discovery. Allgemeine Informationen zur Datenbankkatalog-Discovery finden Sie unter Datenbankkataloge .

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

Anmeldeinformationstyp	Zusätzliche Information
Applicative-Anmeldeinformationen	Anwendbare Anmeldeinformationen sind für zwei Anwendungsfälle obligatorisch: • SQL-Abfragen für die Remote-Oracle DB-Instanz werden ausgeführt • Verbindungen zu Datenbanklinks erstellen • Software Asset Management aktiviert Sie müssen den Datenbankanwender hinzufügen, den Sie während konfiguriert haben Oracle Datenbankinstallation. Geben Sie als CI-Typ Oracle-Instanz [cmdb_ci_db_ora_instance] an. Der Benutzer muss auch über Zugriff auf die Parameterdatei *tnsnames.ora* verfügen. Stellen Sie sicher, dass „tnsnames.ora“ korrekt konfiguriert ist und in vorhanden ist Oracle Pfad auf dem Ziel-Windows-Host. Überprüfen Sie außerdem, ob die verwendeten Discovery-Anmeldeinformationen die Datei „tnsnames.ora“ lesen können. Der Anwender benötigt Berechtigungen für das SQL*Plus-Befehlszeilentool und Berechtigungen zum Ausführen von AUSWAHLABFRAGEN für die folgenden Tabellen: • PRODUCT_COMPONENT_VERSION • V$VERSION

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationstyp	Zusätzliche Information
	• V$DATABASE • V$PARAMETER
Windows-Anmeldeinformationen SSH-Anmeldeinformationen	Neben Applicative-Anmeldeinformationen können Sie auch Windows- und SSH-Anmeldeinformationen verwenden. Für Windows-Anmeldeinformationen muss der Benutzer über Leseberechtigungen für die Datei `tnsnames.ora` verfügen. SSH-Anmeldeinformationen müssen Leseberechtigung für die Datei `oratab` und Leseberechtigung für das Serverparameterfile aufweisen. Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Zusätzliche Anforderungen

Discovery Identifiziert eine ausgeführte Instanz von Oracle Datenbank auf UNIX Aus dem Prozess, der mit beginnt `Ora_pmon_` . Stellen Sie sicher, dass dieser Prozess im IP-Bereich ausgeführt wird, den Sie für festgelegt haben Discovery. Discovery Identifiziert eine ausgeführte Instanz von Oracle Datenbank auf Windows Von `oracle.exe` Prozess. Stellen Sie sicher, dass dieser Prozess in dem von Ihnen festgelegten IP-Bereich ausgeführt wird.

Für Oracle clusterware benötigen Sie auch Leseberechtigungen Die `/Etc/Hosts/` Datei , Der Hostnamen IP-Adressen zuordnet.

Die folgenden Befehle werden für ausgeführt Oracle clusterware:

Befehl	Beschreibung
`ps -ef | grep 'crsd.bin' |grep -v grep`	Überprüft, ob Oracle CRS-Prozess wird ausgeführt.
`ps -ef |grep-LISTENER | grep -V $$ | Head -1 | awk „{print $8}“`	Ruft Ab Oracle Startseite.
`/U01/App/12.1,0.2/Grid/bin/olsnodes -c | egrep -V „Fehler| Rückgabecode“`	Ruft Ab Oracle CRS-Clustername.
`/U01/App/12.1,0.2/Grid/bin/crsctl query CRS Softwareversion| egrep -V „error|Return Code“`	Ruft Ab Oracle CRS-Cluster-ID.
`/U01/App/12.1,0.2/Grid/bin/crsctl query CRS Softwareversion| egrep -V „error|Return Code“`	Ruft Ab Oracle CRS-Version.
`/U01/App/12.1,0.2/Grid/bin/olsnodes | egrep -V „error|Return Code“`	Ruft Ab Oracle CRS-Knoten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
/U01/App/12.1,0.2/Grid/bin/crsctl Statusserver | egrep -V „error|Return Code“	Ruft Ab Oracle CRS-Knotenstatus.
/U01/App/12.1,0.2/Grid/bin/crsctl stat res -f | tr „\n“ „#“	Ruft Ab Oracle CRS-Ressourcen.
/u01/app/12.1.0.2/grid/bin/crsctl stat res -p | grep -v CHECK_R |grep -v error |grep -v failed	Ruft Ab Oracle CRS VIP-Ressourcen.
/u01/app/12.1.0.2/grid/bin/srvctl config scan | tr '\n' ‘ '	Ruft Ab Oracle RAC-SCAN-VIP-KONFIGURATIONEN.
/U01/App/12.1,0.2/Grid/bin/srvctl config vip -node ol7-121-rac1| egrep „ Name“ | awk „{print $3}“	Ruft Ab Oracle CRS-VIPs-Name.
/U01/App/12.1,0.2/Grid/bin/srvctl config vip -node ol7-121-rac1| grep „ IPv4-Adresse:“ | awk „{print $4}“	Abrufen Oracle CRS-VIPs ip_address.

Sudo-Berechtigung zur Ausführung: `sudo /u01/app/12.1.0.2/grid/bin/ocrcheck | egrep -v 'error|return code'`

Klassifizierer, Muster und Probes

Discovery Verwendet diese Klassifizierer, Probes und Muster für Oracle Datenbank-Discovery:

Klassifizierer	Auslöser-Probes	Muster
Oracle-Instanz	• Probe „Horizontal Discovery“: Startet Muster • Powershell-Oracle - Instance PFile (für Windows)* • Powershell-Oracle - Instance Version (für Windows)* • SSHCommand-Oracle - Instance Details (für Linux)*	Anwendungsmuster: • Oracle DB On Windows • Oracle DB on UNIX Das folgende Muster für gemeinsam genutzte Bibliotheken, das vom Muster Linux Server verwendet wird: UNIX Cluster - ORACLE Clusterware **Hinweis:** Dieses Muster der gemeinsamen Bibliothek wird ausgelöst, wenn `crsd.bin` Prozess wird auf ausgeführt Oracle Datenbankserver.
Oracle-Listener	SSHCommand-Oracle - Listener Details	keine

*Probes inaktiv für neue Instanzen

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Daten

Die folgenden Daten werden in der Tabelle „Oracle-Instanzen“ [cmdb_ci_DB_ora_instance] für beide erfasst UNIX Und Windows:

Daten erfasst am UNIX Computer

Bezeichnung	Feldname	Zusätzliche Informationen
SID	sid	Abgeleitet aus dem Namen des Prozesses, der mit `ora_pmon_`beginnt
Installationsverzeichnis	install_directory	Abgeleitet aus dem Pfad von ORA_HOME
Version	Version	In der folgenden Reihenfolge abgerufen: • Aus der Ausgabe des Befehls ORA_HOME/bin/sqlplus/NOLOG • Aus der Ausgabe des Statusbefehls ORA_HOME/bin/lsnrctl • Aus dem Pfad von ORA_HOME
Parameterdatei	pfile	Die folgenden Speicherorte werden für den Speicherort des Systemparameterfile untersucht. Wenn diese Datei an keinem der untersuchten Speicherorte vorhanden ist, findet Discovery die Datei nicht, und es wird ein Fehler gemeldet. • *oracle_home*/dbs/spfile*SID*.ora • *oracle_home*/dbs/spfile.ora • *oracle_home*/dbs/init*SID*.ora
Oracle Home	oracle_home	Aus der Datei *ORATAB* abgerufen
Edition	Edition	Abgerufen aus der Datei context.xml
Name	Name	Kombination aus SID-Name und Hostname im Format *SID@HOST_NAME*
TCP-Port(s)	tcp_port	Abgerufen aus der Datei tnsnames.ora oder mit dem Statusbefehl *lsnrctl*. Wenn keine gültigen Informationen abgerufen werden, wird der Standardport 1521 zugewiesen.

Hinweis: Unter Oracle Optionen finden Sie Informationen über Mustererweiterungen und zusätzlich erfasste Informationen.

Daten erfasst am Windows Computer

Bezeichnung	Feldname	Zusätzliche Informationen
SID	sid	Abgeleitet aus dem Prozessparameter, der an den Prozess *oracle.exe* übergeben wird
Installationsverzeichnis	install_directory	
Version	Version	Abgerufen aus der Ausgabe des Befehls *ORA_HOME/bin/sqlplus.exe -V*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erfasst am Windows Computer (Fortsetzung)

Bezeichnung	Feldname	Zusätzliche Informationen
Parameterdatei	pfile	Die folgenden Speicherorte werden für den Speicherort des Systemparameterfile untersucht. Wenn diese Datei an keinem der untersuchten Speicherorte vorhanden ist, findet Discovery die Datei nicht, und es wird ein Fehler gemeldet. • *oracle_home*\database\spfile*SID*.ora • *oracle_home*\database\spfile.ora • *oracle_home*\database\init*SID*.ora
Oracle Home	oracle_home	Analysiert aus dem Pfad von *oracle.exe*
Edition	Edition	

Hinweis: Unter Oracle Optionen finden Sie Informationen über Mustererweiterungen und zusätzlich erfasste Informationen.

Oracle Optionen

Für allgemeine Informationen zu Oracle Optionen, siehe https://docs.oracle.com/en/ .

Discovery kann auch finden Oracle Optionen, die Sie in der Instanz mit der Legacy-Mustererweiterung, Oracle-Optionserweiterung für Windows/Unix aktivieren. Beachten Sie, dass erkannt werden soll Oracle Optionen ist das Plugin „Software Asset Management Professional for Oracle“ (com.snc.samp.oracle) erforderlich.

Oracle-Optionen [samp_oracle_options]

Bezeichnung	Feldname
Instanz	instance
Option	option
Lizenzierbar	lizenzierbar
Derzeit verwendet	currently_used
Datum der ersten Verwendung	first_usage
Datum der letzten Verwendung	last_usage
Datum des letzten Beispiels	last_sample
Erkannte Verwendung	detected_usage
Beispielintervall	sample_interval

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
Auf die folgenden Tabellen wird als Teil der Oracle-Optionserweiterung für UNIX und Windows zugegriffen:	Die folgenden Mustererweiterungen verwenden Oracle Skript: Options_Packs_usage_statistics.sql. Dieses SQL-Skript kann für DB Server Version 11.2 und höher verwendet werden. Um das Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
• DBA_FEATURE_USAGE_STATISTICS • CDB_FEATURE_USAGE_STATISTICS • V$DATABASE • V$VERSION • GV$PARAMETER • V$CONTAINERS • V$INSTANCE	auszuführen, benötigen Sie die Berechtigung zur **Auswahl eines beliebigen Wörterbuchs**. Weitere Informationen zu Usage-Skripts finden Sie im Supportdokument ID13172651.1 auf https://support.oracle.com/portal/ . • Oracle-Optionserweiterungen für UNIX • Oracle-Optionserweiterungen für Windows

Auf Clusterware erfasste Daten

Tabelle	Bezeichnungen und Feldnamen
Unix-Cluster [cmdb_ci_unix_cluster]	Name [name] Clusterstatus [cluster_status] Clustertyp [cluster_type] IP-Adresse [ip_address] Kurzbeschreibung [short_description] Cluster-ID [cluster_id] Clusterversion [cluster_version]
cmdb_ci_unix_cluster_node	Name [name] Knotenzustand [node_state] IP-Adresse [ip_address] Knotenstatus [node_status]
cmdb_ci_unix_cluster_resource	Name [name] Ressourcentyp [resource_type] Ressourcenstatus [resource_status] Eigenschaften [properties]
cmdb_ci_cluster_vip	Name [name] IP-Adresse [ip_address] Clustername [cluster_name] Cluster-ID [cluster_id]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Abhängigkeitsansicht A **+1** Auf einem Oracle Der Datenbankserver gibt an, dass er Teil eines Clusters ist.

Erweiterung „Extend Oracle instance“

Hinweis: Discovery Kann mithilfe der Erweiterung „Oracle-Instanz erweitern“ auch zusätzliche Attribute für die Instanz finden. Siehe Oracle Website für weitere Informationen zu Optionen https://docs.oracle.com/en/ . Discovery speichert diese Attribute in der Tabelle „Oracle-Instanzen“ [cmdb_ci_db_ora_instance].

Bezeichnung	Feldname
Instanz	instance
Host-Name	host_name
IS_CDB	cdb_yn
DB – Eindeutiger Name	db_unique_name
DB-Name	database_name
Replikation aktiviert	replication_enabled

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
Als Teil der Erweiterung „Extend Oracle Instance“ für UNIX und Windows wird auf die folgenden Tabellen zugegriffen: • V$DATABASE • V$INSTANCE	Die Erweiterung „Extend Oracle Instance“ muss installiert sein. Diese Erweiterung ist in der Anwendung Discovery and Service Mapping Patterns, Version 1.0.72 oder höher, enthalten, die aus dem ServiceNow Store heruntergeladen werden kann.

Oracle Instanzen auf virtuellen Computern

Wenn Oracle Instanzen werden auf virtuellen Computern gehostet, das System erstellt Beziehungen zwischen CIs.

CI	Beziehung	CI
Oracle-Instanz	Gehostet auf	Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.
Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.	Virtualisiert von	Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist kein virtueller Computer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Instanzen auf virtuellen Computern, die auf gehostet werden AWS Oder Azure Clouds

Basisklasse	Beziehung	Abhängige Klasse
Oracle-Instanz	Gehostet auf	Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.
Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.	Virtualisiert von	Computer [cmdb_ci_computer] **Hinweis:** Das ist kein virtueller Computer.
Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.	Virtualisiert von	VM-Instanz [cmdb_ci_vm_instance] **Hinweis:** Die vCPU-Anzahl wird in diese Tabelle gefüllt.
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_datacenter] oder Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Beziehungen für Clusterware

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Virtualisiert::Virtualisiert von	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet::Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet::Gehostet auf	Linux-Server [cmdb_ci_linux_server]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Linux-Server [cmdb_ci_linux_server]

Zugehörige Informationen

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Probe „Horizontal Pattern“

Discovery des Berichts „Datenbankadministrator“ (DBA)

SAP Sybase-ASE-Discovery

Discovery Und Service-Mapping Verwendet das Sybase-Muster für die Suche SAP Sybase Adaptive Server Enterprise (ASE)-Datenbanken und -Kataloge in Ihrer Infrastruktur. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind.

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Details zum erkannten Produkt finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Hinweis: Discovery Sucht nach Sybase-Katalog, der auf ausgeführt wird Linux Nur.

Überprüfen Sie die Konfiguration der BS-Server-Anmeldeinformationen.

Überprüfen Sie die Konfiguration der anwendbaren Anmeldeinformationen

Stellen Sie beim Konfigurieren der anwendbaren Anmeldeinformationen sicher, dass Sie angeben Sybase Instanz [cmdb_ci_DB_syb_instance] Als CI-Typ.

Weitere Informationen zu anwendbaren Anmeldeinformationen finden Sie unter Anwendbare Anmeldeinformationen

Überprüfen Sie, ob der Anwender berechtigt ist, die folgenden Befehle auszuführen

Führen Sie aus `isql` Befehl.

Lassen Sie die Sybase-Umgebung einen der folgenden Befehle ausführen:

- „Echo -ne „Anzahl bei Auswahl des Namens aus sysdatabase\ngo\n festlegen“ | „ + $isql_path + " -U $$Anwendername$$ -P '$$password$' -S " + $Instanz + " -W 999 -b -y " + $Process.environmentVariables.SYBASE.value
- „SYBASE exportieren=“ + $Process.environmentVariables.SYBASE.value + „ &&“. „ + $Process.environmentVariables.SYBASE.value + "/SYBASE.sh && Echo

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
-ne 'Anzahl bei Auswahl des Namens aus sysdatabase\ngo\n' festlegen | " +
$isql_path + " -U $$username$$ -P '$$password$' -S " + $Instanz + " -W 999 -b
-y " + $Process.EnvironmentVariables.SYBASE.value
```

Überprüfen Sie die Konfiguration von Discovery Zeitplan

Detaillierte Informationen finden Sie unter . Siehe Erkennungen im Netzwerk ausführen

Während der horizontalen Discovery erfasste Daten

Discovery Füllt die folgenden Daten in aus CMDB Beim Ausführen des Sybase-Musters.

Sybase-Instanz [cmdb_ci_DB_syb_instance]	
Bezeichnung	**Feldname**
Name	Name
Version	Version
Installationsverzeichnis	install_directory
Instanzname	Instanz
Konfigurationsdatei	config_file

Sybase-Katalog [cmdb_ci_DB_syb_catalog]	
Bezeichnung	**Feldname**
Name	Name

CI-Beziehungen

Diese Beziehungen werden erstellt, um die Sybase ASE-Discovery zu unterstützen.

CI	Beziehung	CI
[cmdb_ci_DB_syb_instance]	Enthält::Enthalten in	[cmdb_ci_DB_syb_catalog]

Erkennung von Netzwerkgeräten

Discovery erkennt verschiedene Netzwerkgeräte. Dazu gehören Lastenausgleichsmodule, Router, TCP-Verbindungen und IP-Netzwerke. Geräte können mit herkömmlichen Port-Probes, Identifizierungs- und Erkundungs-Probes oder Mustern erkannt werden. Discovery unterstützt auch die Erkennung durch die Identifizierung von HTTP- und TCP-Verbindungen.

Hinweis: Siehe wissensartikel KB0687582 Für Informationen zur model_ID und zum Hersteller.

Lastenausgleicherkennung

Discovery Kann Daten zu Netzwerkroutern, Switches und Anwendungen erfassen.

Discovery unterstützt die Datenerfassung aus der folgenden Software und Hardware:

- A10
- Apache mod_jk und Apache mod_proxy
- Big-IP F5 Traffic Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cisco
- Citrix NetScaler
- HAProxy
- NGINX
- Alteon
- ACE
- RadWare

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Lastenausgleichsmuster

Ab dem Jakarta-Release verwendet Discovery vordefinierte Muster, um einige Typen von Lastenausgleichsmodulen für neue Instanzen zu erkennen (siehe Tabelle).

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Load Balancer	Musternamen und -beschreibung	Gefüllte CI-Haupttabelle
A10	A10 LoadBalancer	A10 Load Balancer [cmdb_ci_lb_a10]
ACE	ACE Load Balancer by SSH (früher ACE Load Balancer)	ACE [cmdb_ci_lb_ace]
Alteon	Alteon Load Balancer	Alteon [cmdb_ci_lb_alteon]
F5 BIG-IP	F5 - HD, F5 Load Balancer	F5 BIG-IPs [cmdb_ci_lb_bigip]
NetScaler	Netscaler Load Balancer	Citrix NetScaler [cmdb_ci_lb_netscaler]
Radware - AppDirector	AppDirector Load Balancer	Radware-Load Balancer [cmdb_ci_lb_radware]
HAProxy Lastenausgleichsmodul-Discovery mit Mustern	HA-Proxy	HAProxy Load Balancer [cmdb_ci_lb_haproxy]

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Lastenausgleicherkennung, Service Mapping und benutzerdefinierte CI-Felder

Discovery erfasst Informationen über den Installations- und Betriebsstatus von Lastenausgleichsmodulen. Wenn Sie Discovery mit Service Mapping verwenden, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

davon abgeraten, die Felder [operational_status] und [install_status] anzupassen. Standardmäßig ignoriert Service Mapping alle Host-CIs, für die der Wert des Felds `[operational_status]` ungleich `1` (Funktionsfähig) oder der Wert des Statusfelds `[install_status]` gleich `100` (Abwesend) ist. Weitere Informationen zu diesem Verhalten finden Sie unter Preparing customized ServiceNow deployments to work with Service Mapping (Vorbereitung benutzerdefinierter ServiceNow-Bereitstellungen zur Verwendung mit Service Mapping) [KB0647574] in der HI Knowledge Base.

A10-Lastenausgleicherkennung

Discovery und Service-Mapping verwenden Muster, um Informationen über A10-Lastenausgleichsmodule zu sammeln.

Hinweis: Die Probe-zu-Muster-Migration wird ab dem New York-Release unterstützt. Weitere Informationen finden Sie in Artikel KB0694477 der Wissensdatenbank.

Die folgenden Muster unterstützen die A10-Lastenausgleicherkennung:

- A10 Lastenausgleich
- A10 Load Balancer SSH
- A10

Der A10 IP Source NAT (Network Address Translator) ist eine Erweiterung des A10 Load Balancer-Musters. Die Erweiterung IP-Quell-NAT-Muster erkennt IP-Quell-NAT-Pools. Diese Erweiterung ist ab Release Februar 2023, Store-Version 1,0.98, im Store verfügbar.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anmeldeinformationen

Konfigurieren SNMP-Anmeldeinformationen Oder (optional) SSH-Anmeldeinformationen .

Discovery and Service Mapping Patterns

Um A10-Lastenausgleichsmodul-Partitionen zu erkennen, stellen Sie die Anwendung „Discovery and Service Mapping Patterns“ (1.0.98) aus dem bereit ServiceNow Store.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
A10 Load Balancer [cmdb_ci_lb_a10]	
Seriennummer [serial_number]	Seriennummer des Lastenausgleichsmoduls im folgenden Format: ##Object_ID=<LB_ARN>
Betriebsstatus [operational_status]	Betriebsstatus des Lastenausgleichsmoduls
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	
Name [name]	Name der Lastenausgleichs-Schnittstelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

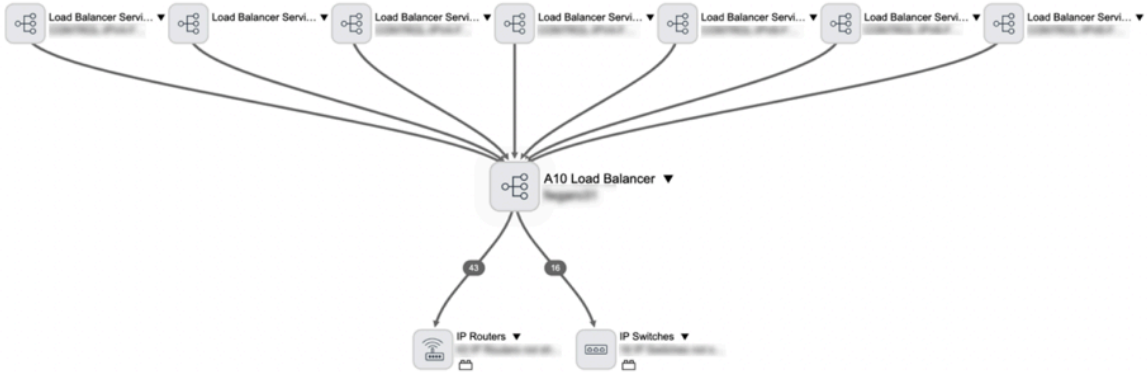
Tabelle und Feld	Beschreibung
MAC-Adresse [mac_address]	MAC-Adresse der Lastenausgleichs-Schnittstelle im folgenden Format: 55:0d:f9:98:3i:ae
Betriebsstatus [operational_status]	Betriebsstatus der Lastenausgleichs-Schnittstelle
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Name des Pools von Lastenausgleichsmodulen
Lastenausgleichsmethode [load_balancing_method]	Die vom Lastenausgleichsmodul verwendete Methode
Betriebsstatus [operational_status]	Betriebsstatus des Pools von Lastenausgleichsmodulen
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name des Poolmitglieds
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Serviceport [service_port]	Vom Poolmitglied verwendeter Port
Betriebsstatus [operational_status]	Betriebsstatus der Mitglieder des Pools von Lastenausgleichsmodulen
Pool [pool]	Poolmitglied
Load Balancer-Services [cmdb_ci_lb_service]	
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
IP-Adresse [ip_address]	IP-Adresse des FQDN
Port [port]	Port des Lastenausgleichsmoduls
Betriebsstatus [operational_status]	Betriebsstatus des Lastenausgleichsservice
Installationsstatus [install_status]	Installationsstatus des Lastenausgleichsservice
Pool [pool]	Poolmitglied des Lastenausgleichsservice
DNS [cmdb_ci_dns_name]	
Name [name]	DNS-Name
IP-Adresse [ip_address]	DNS-IP-Adresse
Partition des A10-Lastenausgleichsmoduls [cmdb_ci_lb_a10_partition]	
Name [name]	Name der Partition
Index [index]	Partitions-ID. Ein Administrator weist diese ID beim Erstellen einer Partition zu.
Max. Aflex [Max_aflex]	Maximale Anzahl von aFleX-Skripts, die zur Partition gehören können
Administratoranzahl [admin_count]	Anzahl der der Partition zugewiesenen Administratoren
L3V [lev]	Wert, der angibt, ob die Layer 2/3-Virtualisierung für die Partition aktiviert ist
Netzwerkadapter [cmdb_ci_network_adapter]	
Betriebsstatus [operational_status]	Betriebsstatus des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Alias [alias]	Aliasname des Netzwerkadapters
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Primäre IP [primaryIP]	Primäre IP-Adresse des Netzwerkadapters
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse
Netzmaske [netmask]	Netzmaske, zu der die IP-Adresse gehört
Version [version]	IP-Version
Betriebsstatus [operational_status]	Betriebsstatus der IP-Adresse
Seriennummer [cmdb_serial_number]	
Seriennummer [serial_number]	Attribute der Seriennummer des Lastenausgleichsmoduls
Seriennummerntyp [serial_number_type]	
Gültig [valid]	
Quell-NAT-IP-Pool [cmdb_ci_snat_ip_Pool]	
NAT-Pool fehlgeschlagen [nat_Pool_failed]	Die Gesamtzahl der Fehlschläge im Pool.
HA-Gruppe [ha_Group]	
NETZMASKE [net_mask]	
NAT-Pool insgesamt frei [nat_Pool_total_free]	Die Gesamtzahl der freien Adressen im Pool.
NAT-Pool-Gesamtnutzung [nat_Pool_total_usage]	Die Gesamtzahl der verwendeten Adressen im Pool.
NAT-Pool-Portnutzung [nat_Pool_Port_usage]	Die gesamte Portauslastung im Pool.
NAT-Pool-Endadresse [nat_Pool_end_address]	Die Endadresse des IP-NAT-Pools (IPv4 oder IPv6).
Startadresse des NAT-Pools [nat_Pool_Start_address]	Die Startadresse des IP-NAT-Pools (IPv4 oder IPv6).
Konfigurationselement [cmdb_ci]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeitsansichten, in denen A10-Lastenausgleichsmodule und verbundene Komponenten und Anwendungen angezeigt werden



CI-Beziehungen

Um die A10-Lastenausgleicherkennung zu unterstützen, werden die folgenden Beziehungen erstellt:

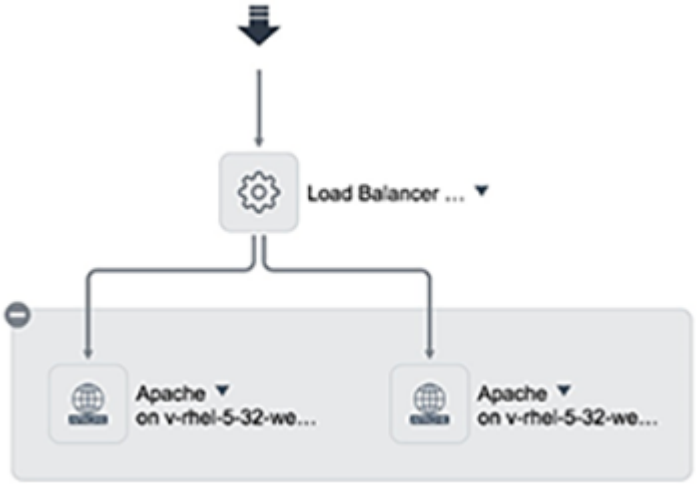
CI	Beziehung	CI
Routerschnittstelle [dscy_router_interface]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Services [cmdb_ci_lb_service]	Verwendet von::Verwendet	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Services [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
DNS-Name [cmdb_ci_dns_name]	Verwendet von::Verwendet	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Pool [cmdb_ci_lb_a10]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Lastenausgleichsmodul A10 [cmdb_ci_LB_a10]	Besitzt:im Besitz von	Quell-NAT-IP-Pool [cmdb_ci_snat_ip_Pool]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping erkennt die Verbindungen zwischen A10-Lastenausgleichsmodulen und Anwendungen in der Bereitstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicezuordnung für A10-Lastenausgleichsanwendung



Cisco ACE-Lastenausgleicherkennung

Discovery Identifiziert und klassifiziert Informationen zu ACE-Lastenausgleichsmotoren.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren SNMP-Anmeldeinformationen Und SSH-Anmeldeinformationen .

Klassifizierer, Muster und Probe

Klassifizierung	Auslöser-Probes	Muster
ACE Load Balancer	Probe „Horizontal Discovery“: Startet Muster	ACE Load Balancer by SSH (früher ACE Load Balancer)

Erfasste Daten

In der Tabelle „ACE-Lastenausgleichsmodule“ [cmdb_ci_lb_ace] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number
Betriebsstatus	operational_status

In der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname
Betriebsstatus	operational_status
Installationsstatus	install_status
Kurzbeschreibung	short_description

In der DNS-Tabelle [cmdb_ci_dns_name] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

In der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Kontext	context
Lastenausgleichsmethode	load_balancing_method

In der Tabelle „Mitglieder von Load Balancer-Pools“ [cmdb_ci_lb_pool_member] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Serviceport	service_port
Pool	Pool
Kontext	context

In der Seriennummertabelle [cmdb_serial_number] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number
Seriennummerntyp	serial_number_type
Gültig	valid

In der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	name
MAC-Adresse	mac_address

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname
Betriebsstatus	operational_status

Cisco GSS-Lastenausgleicherkennung

Discovery Von Cisco GSS-Lastenausgleichsmodule wird sowohl von SNMP als auch von SSH ausgeführt.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Klassifizierer

Um das Gerät zu klassifizieren, verwendet Discovery den Klassifizierer „Cisco GSS Load Balancer“, der die folgende Bedingung enthält: sysdescr enthält Global Site Selector.

Probes

Zur Identifizierung der Seriennummer des Geräts verwendet Discovery mehrere Probes, darunter eine SNMP-Probe zur Erkennung des spezifischen GSS-Geräts und eine Probe für die **Seriennummer**. In der Tabelle unten finden Sie eine Liste der zugehörigen Probes.

Warnung: Sie müssen SNMP und haben SSH-Anmeldeinformationen Richtig konfiguriert für die GSS-Lastenausgleichsmodule in Ihrem Netzwerk.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

Probe	Beschreibung	Typ
Cisco GSS - Identity	Eine Multi-Probe, die das GSS-Gerät und die Seriennummer identifiziert	Mehrfachprobe
Cisco GSS - Network	In der Probe „Cisco GSS - Identify“ enthalten	Java-SNMP
Cisco GSS - Serial Number	In der Probe „Cisco GSS - Identify“ enthalten	JavaScript
Cisco GSS - Get Domains	Eine Probe, die globale Domänennamen erkennt, die dem Gerät entsprechen	JavaScript

Tabellen

Discovery erstellt einen Datensatz für jedes GSS-Gerät in der Tabelle „Cisco GSS“ [cmdb_ci_lb_cisco_gss]. Domänen werden in der Tabelle „DNS-Namen“ [cmdb_ci_dns_name] angegeben. Hostnamen und IP-Adressen werden in der Tabelle „IP-Adresse zu DNS-Name“ [cmdb_ip_address_dns_name] gespeichert. Diese Informationen werden von Service Mapping verwendet. Sie können die Informationen über DNS-Namen in der zugehörigen Liste **DNS-Namen für CIs** im Formular „Lastenausgleich“ anzeigen.

Hinweis: Das Muster „Cisco GSS“ ist standardmäßig zur Verwendung im Musterdesigner verfügbar.

Cisco CSS-Lastenausgleichsmodul

Die Erkennung von Cisco CSS-Lastenausgleichsmodulen erfolgt mithilfe von SNMP.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierer

Discovery verwendet den Klassifizierer „Cisco CSS Load Balancer“, der die folgende OID-Klassifizierung enthält: 1.3.6.141.9.9.368.4.5.

Probes

Die folgenden Probes werden ausgelöst:

Probe	Beschreibung	Typ
SNMP - Load Balancer - Identity	Eine Multi-Probe, die Lastenausgleichsmodule erkennt	Java-SNMP
Cisco CSS - Get Services	Eine Java-Probe mit dem Cisco CSS-Sensor zum Erkennen von Services, die für das Lastenausgleichsmodul in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] definiert sind. Discovery wird für jeden Service ausgefüllt **Name** , **ip_address** , Und **Port** .	Java-SNMP

Tabellen

Discovery erstellt einen Datensatz für jedes CSS-Gerät in der Tabelle „Cisco CSS“ [cmdb_ci_lb_cisco_css], die **Name**, **Modell**, **Seriennummer**, **Hersteller** und **NIC** (ip_address) des Geräts enthält. Außerdem wird für jeden Service in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] ein Datensatz erstellt.

.

Citrix NetScaler-Lastenausgleicherkennung

Discovery und Service-Mapping erkennen Citrix NetScaler-Lastenausgleichsmodule einschließlich Server Load Balancing (GSLB).

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anforderungen und Support

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Virtuelle NetScaler-Lastenausgleichsmodule werden nicht vollständig unterstützt. Discovery unterstützt Lastenausgleichsmodule für lokale Server und GSLB.

Berechtigungen

- Konfigurieren Sie die SNMP-Anmeldeinformationen .

Hinweis: Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-Anmeldeinformationen angeben möchten.
- Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster

NetScaler Load Balancer	• Probe „Horizontal Discovery“: Startet Muster (siehe Spalte „Muster“)
	• NetScaler - Network Path Information (Multi-Probe)
	  ○ NetScaler - ARP Information
	  ○ NetScaler - Route Information
	• SNMP - NetScaler - Identity
	• SNMP - NetScaler - Identity - Serial
	• SNMP - NetScaler - Identity Info
	• SNMP - NetScaler - System
		• NetScaler Load Balancer
		• NetScaler Load Balancer NS.CONF
		• NetScaler Load Balancer SSH
		• NetScaler-Lastenausgleichsmodul-NITRO

Um Probes für die horizontale Erkennung zu verwenden, stellen Sie sicher, dass die Multi-Probe *NetScaler - Network Path Information* in der zugehörigen Liste **Auslösertests** für den Klassifizierer *NetScaler Load Balancer* aktiv ist. Deaktivieren Sie dann die Probe *Horizontal discovery*, oder entfernen Sie sie aus der zugehörigen Liste **Auslösertests**.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Hinweis: Wenn Probes und Sensoren verwendet werden und die Systemeigenschaften *glide.discovery.hostname.snmp_trusted* und/oder *glide.discovery.hostname.dns_nbt_trusted* auf „false“ festgelegt sind, verwendet das System *dns_name* als Namen für das Lastenausgleichsmodul. Bei Verwendung des Musters „Netscaler Load Balancer“ erkennt das System diese Systemeigenschaften nicht, wenn sie auf „false“ festgelegt sind.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping Führt die Top Down-Discovery des NetScaler Global Server Load Balancer im Kontext von Anwendungsservices durch. Dadurch werden konfigurierte URLs des Lastenausgleichsmoduls NetScaler Global Server erkannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
DNS-Name [cmdb_ci_dns_name]	
Name [name]	Der Name oder der DNS-Namensalias des Lastenausgleichsmoduls NetScaler Global Server (GSLB)
IP-Adresse [ip_address]	Management-IP-Adresse des NetScaler Global Server-Lastenausgleichsmoduls (GSLB)
Port [port]	Der DNS-Port, den das Global Server-Lastenausgleichsmodul abhört
Citrix NetScaler [cmdb_ci_lb_netscaler]	
Seriennummer [serial_number]	Die Seriennummer des NetScaler-Geräts und dessen aktueller Betriebsstatus
Betriebsstatus [operational_status]	
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Der Name des Pools und die Methode für den Lastenausgleich, die der Pool aktiviert
Lastenausgleichsmethode [load_balancing_method]	
Load Balancer Pool-Mitglied [cmdb_ci_l b_pool_member]	
Name [name]	Name, IP-Adresse und Serviceport, die von jedem Poolmitglied verwendet werden
IP-Adresse [ip_address]	
Serviceport [service_port]	
VLAN des Lastenausgleichsmoduls [cmdb_ci_lb_vlan]	
Name [name]	Der Name des VLAN und das Tag, das diesem VLAN zur Identifizierung zugeordnet ist
Tag [tag]	
Load Balancer-Services [cmdb_ci_lb_service]	
Name [name]	Details zu dem Service, der im Lastenausgleichsmodul ausgeführt wird, zum Beispiel:
IP-Adresse [ip_address]	
Port [port]	
Betriebsstatus [operational_status]	
Installationsstatus [install_status]	
Trefferanzahl [hit_count]	
Weiterleitungsregeln für Exit-Schnittstellen [dscy_route_interface]	
Routerschnittstelle [router_interface]	Details zu Weiterleitungsregeln für die Exit-Schnittstelle, einschließlich der Schnittstelle auf dem Router, ...
Konfigurationselement [cmdb_ci]	
Ziel-IP-Netzwerk [dest_ip_network]	
Weiterleitungsregeln für nächsten Hop [dscy_route_next_hop]	
IP-Adresse für nächsten Hop [router_interface]	Details zu den Weiterleitungsregeln im Lastenausgleichsmodul, einschließlich der IP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Routerschnittstelle [router_interface]	Adressen des nächsten Hop-Routers im Netzwerk. Das Feld „Konfigurationselement“ gibt den Router an, der das nächste Hop-Gerät ist.
Konfigurationselement [cmdb_ci]	
Ziel-IP-Netzwerk [dest_ip_network]	

cmdb_ci_lb_netscaler

Spaltenname	Typ	Referenz
ip_address	IP-Adresse (validierte IPV4, IPV6)	
name	Zeichenfolge	
operational_status	Ganzzahl	
serial_number	Zeichenfolge	

Daten, die während des Netscaler Loadbalancer-NITRO erfasst werden.

cmdb_serial_number

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Konfigurationselement	cmdb_ci	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Seriennummer	serial_number	Zeichenfolge	
Seriennummertyp	serial_number_type	Zeichenfolge	
Gültig	gültig	Wahr/falsch	

cmdb_ci_LB_vlan

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Name	name	Zeichenfolge	
Tag	Tag	Ganzzahl	

cmdb_ci_LB_Interface

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Name	name	Zeichenfolge	
Betriebsstatus	operational_status	Ganzzahl	
MAC-Adresse	mac_address	Zeichenfolge	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

cmdb_ci_lb_service

Spaltenbezeichnung	Spaltenname	Typ	Referenz
IP-Adresse	ip_address	IP-Adresse (validierte IPV4, IPV6)	
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Name	name	Zeichenfolge	
Port	port	Ganzzahl	

cmdb_ci_lb_pool

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Name	name	Zeichenfolge	

cmdb_ci_lb_pool_member

Spaltenbezeichnung	Spaltenname	Typ	Referenz
IP-Adresse	ip_address	IP-Adresse (validierte IPV4, IPV6)	
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Lastenausgleichsmodul)
Name	name	Zeichenfolge	
Pool	Pool	Referenz	Lastenausgleichsmodul-Pool
Serviceport	service_port	Ganzzahl	

Zum Anzeigen der DNS-Namen und -Aliasnamen für ein NetScaler-Lastenausgleichsmodul müssen Sie das Formular konfigurieren und die zugehörige Liste **DNS-Namen für CIs** hinzufügen. DNS-Namen beinhalten auch Aliasnamen.

Hinweis: Discovery fügt Informationen über die Lastenausgleichs-Schnittstelle ein, die zum Zuordnen des Netzwerkpfads in Service-Mapping erforderlich sind.

Beziehungen von Konfigurationselementen

Um die NetScaler Global Server-Lastenausgleicherkennung zu unterstützen, werden die folgenden Beziehungen erstellt:

CI	Beziehung	CI
DNS-Name [cmdb_ci_dns_name]	Verwendet::Verwendet von	IP-Adresse [cmdb_ci_ip_addresses]

Diese Beziehungen werden erstellt, um NetScaler Loadbalancer-NITRO ZU unterstützen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	Schnittstellen [cmdb_ci_LB_Interface]
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	vlan [cmdb_ci_LB_vlan]
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	Servicegruppen [cmdb_ci_LB_Pool]
Servicegruppen [cmdb_ci_LB_Pool]	Eigentümer von::Eigentum von	LbvServer [cmdb_ci_LB_Pool_member]
-Services [cmdb_ci_LB_Service]	Wird ausgeführt auf::Wird ausgeführt	Netscaler [cmdb_ci_lb_netscaler]

sysName des NetScaler-Geräts

Um den sysName des NetScaler-Geräts zu verifizieren, überprüfen Sie die SNMP-MIB, und verifizieren Sie den sysName-Wert, indem Sie den Befehl *`show snmp mib`* ausführen.

Um den Wert von sysName zu ändern, führen Sie den folgenden Befehl aus: *`set mib -name <DNS_NAME or NAME_OF_THE_NETSCALER_LB>`*, um den Namen der SNMP-MIB festzulegen.

F5 BIG-IP-Lastenausgleicherkennung

Discovery und Service-Mapping erkennen F5 BIG-IP-Lastenausgleichsmodule über SNMP, SSH und die REST API.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Sie können VMware-Images von BIG-IP mit einer kostenlosen 90-Tage-Testversion von herunterladen https://www.f5.com/trial .

Für BIG-IP-Lastenausgleichsmodule von F5 Global Traffic Manager (GTM), Discovery Kann den DNS-Namen der F5 GTM-Hardware sowie die DNS-Namen aller Server auflösen, die dem Lastenausgleichsmodul zugeordnet sind und verteilten Datenverkehr empfangen. Um diese Daten anzuzeigen, navigieren Sie zu **Alle** > **Konfiguration** > **Lastenausgleichsmodule** > **LB-Hardware** Und öffnen Sie den F5-Lastenausgleichsmodul-Datensatz, und wählen Sie dann aus **DNS-Namen für CIs** Zugehörige Liste. Service-Mapping Verwendet diese Informationen, um F5-Beziehungen zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Ihr F5 BIG-IP Das Gerät ist Teil eines Failover-Clusters und kann zwei Clusterknoten zugeordnet werden. In diesem Fall wird einer der Knoten in als funktionsfähig angezeigt **Betriebsstatus** Und das andere Feld wird als nicht funktionsfähig angezeigt.

Voraussetzungen

- Um die Mitglieder des Lastenausgleichsmodul-Pools erfolgreich zu erkennen, legen Sie fest **Servicenamen anzeigen** Option (`bigpipe.displayservicenames`) Des Lastenausgleichsmodul bis **Falsch** Auf dem F5-Lastenausgleichsmodul.
- Für F5-Lastenausgleichsmodul-Muster:
  - Konfigurieren SNMP-Anmeldeinformationen Auf der ServiceNow AI Platform.
  - (Optional) wenn iRules oder SNMP-Community-Anmeldeinformationen für die Erkennung ausgehender Verbindungen nicht ausreichen, konfigurieren Sie SSH-Anmeldeinformationen .

    Hinweis: Wenn Sie keine SSH-Anmeldeinformationen verwenden möchten, können Sie mit der REST API eine Verbindung zu F5-BIG-IP-Geräten herstellen.

    Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery.
- Für SSH-Muster des F5-Lastenausgleichsmoduls:
  - Konfigurieren Sie SSH-Anmeldeinformationen .
  - Überprüfen Sie die Berechtigungen für die folgenden SSH-Befehle:
    - Autorisierungspartition aller auflisten
    - Listen Sie globale SYS-Einstellungen auf
    - SYS-Hardware anzeigen
    - Listen Sie SYS-DB-Failover.State auf
    - Listen Sie das Eigenkapital einzeilig auf
    - SYS-mac-address | grep-Schnittstelle anzeigen
    - Netzschnittstellenfeld-fmt anzeigen
    - NET Self anzeigen | grep -e „Mac-Adresse“ „IP:“
    - ltm-Pool auflisten | grep -e „Pool“ „Modus“
    - ltm-Pool auflisten /<partition_name>/* | grep -e „Pool“ „Mode“
    - ltm-Pool anzeigen | grep -e „LTM::“ „Verbindungen insgesamt“
    - ltm-Pool /<partition_name>/* |grep -e 'LTM::' 'Verbindungen insgesamt' anzeigen
    - Listen Sie sys DB bigpipe.displayservicenames | grep-Wert auf
    - /Net vlan anzeigen | grep -e „Schnittstellenname“ „Mac“ „Tag“
    - Virtuelles ltm-Detail anzeigen | grep -e „Server:“ „Status“ „Pool:“ „Ziel“ „Verbindungen insgesamt“
    - Virtuelle ltm-Details anzeigen /<partition_name>/* | grep -e „Server:“ „Status“ „Pool:“ „Ziel“ „Verbindungen insgesamt“
    - gtm-Wideip anzeigen | grep -e „WideIp“ „Status“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Listenwideip a /<partition_name>/* | grep -e 'WideIp' 'Status'
- gtm-Wideip alle anzeigen | grep -e „WideIp“ „Status“
- gtm-Widget auflisten
- gtm-Wideip alle auflisten

- Für F5REST-Muster:
  - Für horizontale Discovery mit Discovery, Geben Sie schreibgeschützte Berechtigungen zum Ausführen der folgenden APIs an:
    - „https://“ + $ipAddress + „/mgmt/tm/ltm/Pool“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/global-settings“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/Hardware“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/Failover“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Self“
    - „https://“ + $ipAddress + „/mgmt/tm/ltm/Virtual?$select=destination,mask,vlans“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Interface“
    - „https://“ + $ipAddress + „/mgmt/tm/net/interface/stats“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Trunk“
    - „https://“ + $ipAddress + „/mgmt/tm/net/vlan“
    - „https://“ + $ipAddress + „/mgmt/tm/net/vlan/“+<vlan id>+“/interface“
    - „https://“ + $ipAddress + „/mgmt/tm/gtm/wideip“
    - „https://“ + $ipAddress + „/mgmt/tm/cm/Traffic-Group/“
    - „https://“ + $ipAddress + „/mgmt/tm/cm/device“
  - Erstellen Standardauthentifizierung Anmeldeinformationen.
- Für F5 REST OAuth 2,0-Authentifizierungsmuster:
  - Überprüfen Sie die schreibgeschützte Berechtigung für die folgenden APIs:
    - „https://“ + $ipAddress + „/mgmt/Shared/authn/login“
    - „https://“ + $ipAddress + „/mgmt/tm/ltm/Pool“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/global-settings“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/Hardware“
    - „https://“ + $ipAddress + „/mgmt/tm/sys/Failover“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Self“
    - „https://“ + $ipAddress + „/mgmt/tm/ltm/Virtual?$select=destination,mask,vlans“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Interface“
    - „https://“ + $ipAddress + „/mgmt/tm/net/interface/stats“
    - „https://“ + $ipAddress + „/mgmt/tm/net/Trunk“
    - „https://“ + $ip_address + „/mgmt/tm/net/vlan“
    - „https://“ + $ipAddress + „/mgmt/tm/net/vlan/“+<vlan id>+“/interface“
    - „https://“ + $ipAddress + „/mgmt/tm/gtm/wideip“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

    - „https://“ + $ipAddress + „/mgmt/tm/cm/Traffic-Group/“
    - „https://“ + $ipAddress + „/mgmt/tm/cm/device“
  - Erstellen Standardauthentifizierung Anmeldeinformationen.
  - Erstellen Ein Anmeldeinformationsalias Für die Anmeldeinformationen für die Standardauthentifizierung.
  - Erstellen Sie einen serverloser Discovery-Zeitplan .

- Geben Sie für die Top Down-Discovery mit Service-Mapping Berechtigungen zum Ausführen der folgenden APIs an:
  - https://" get_attr {"managementIP"}"/mgmt/tm/ltm/"get_attr {"irule"}
  - https://" get_attr {"managementIP"}"/mgmt/tm/ltm/Virtual/~Common~"get_attr {"vip_Name"}
  - https://" get_attr {"computer_system.managementIP"}"/mgmt/tm/ltm/pool/"get_attr {"pool_name"}"/members?
- (Optional) Für die Top Down-Discovery mit Service-Mapping, konfigurieren Sie Applicative-Anmeldeinformationen .
- (Optional) Für die Top Down-Discovery mit Service-Mapping, stellen Sie einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle bereit:
  - Bigpipe-Befehle (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 9)
  - Bigpipe- und Traffic Management Shell-Befehle (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10)
  - TMSH-Befehle (Traffic Management Shell) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 11)
  - Erweiterte Befehle für die Traffic Management Shell (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10, 11 und 12)
  - Der *`show cm traffic-group – get command`* für die Erkennung von F5 BIG-IP Device Service Clustering
- (Optional) Für die Top Down-Discovery mit Service-Mapping , geben Sie dem Benutzer erhöhte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.

Erkennung von F5-Clustern

Der horizontale Erkennungsprozess kann F5-Cluster ermitteln. Zum Erkennen von Clustern müssen die Anmeldeinformationen über Leseberechtigungen für Datenverkehrgruppen verfügen. Für SNMP ist dies die reguläre Leseberechtigung. Für SSH müssen Sie haben **Traffic-Management-Shell (TMSH-Shell)** Aktiviert und zugänglich.

Hinweis: Da F5-Cluster dieselben virtuellen IPs und Adressen für alle Geräte gemeinsam nutzen, kann der horizontale Erkennungsprozess keine spezifischen IP-Adressen für jedes Gerät finden.

Klassifizierer, Muster und Probes

Zur F5-Erkennung verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierungen	Auslöser-Probes	Muster
F5 BIG-IP-Lastenausgleichsmodul	Probe „Horizontal Discovery“: Startet Muster	Die folgenden Muster werden für die standardmäßige horizontale Erkennung verwendet, die die Erkennung von Clustern einschließt: • F5 Load Balancer • F5 Load Balancer SSH • F5REST • F5 REST OAuth 2,0-Authentifizierung **Hinweis:** Die Muster „F5 Load Balancer“ und „F5 Load Balancer SSH“ enthalten den Erweiterungsabschnitt, der F5-Zertifikate erkennt.
F5 HTTP	Der Klassifizierer „F5 HTTP“ verwendet keine Auslöser-Probe. Er löst das Muster „F5 Load Balancer REST“ aus, um die Datensammlung über REST durchzuführen.	Diese Muster verwenden iRules, um Informationen über REST abzurufen. Service-Mapping verwendet die folgenden Muster für die Erkennung von oben nach unten: • F5 Load Balancer REST • F5 BIG-IP GTM • F5 BIG-IP LTM

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping Führt die Top Down-Discovery des GTM BIG-IP-Lastenausgleichsmoduls im Kontext von Anwendungsservices durch. Erkennt konfigurierte URLs der GTM BIG-IP-Lastenausgleichsmodule.

Von Discovery während der horizontalen Erkennung erfasste Daten

In der Tabelle „F5 Big-IP“ [cmdb_ci_lb_bigip] werden die folgenden Daten erfasst.

Tabelle und Feld	Beschreibung
F5 Big-IP [cmdb_ci_lb_bigip]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Name [name]	Details zum Lastenausgleichsmodul. Zeigen Sie einen Datensatz in dieser Tabelle an, um die vor- und nachgelagerten Beziehungen mit dem Lastenausgleichsmodul anzuzeigen.
Seriennummer [serial_number]	
Betriebsstatus [operational_status]	
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	
Name [name]	Details zu jeder Schnittstelle für das Lastenausgleichsmodul
MAC-Adresse [mac_address]	
Betriebsstatus [operational_status]	
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Der Name des Pools und die Methode für den Lastenausgleich, die der Pool aktiviert
Lastenausgleichsmethode [load_balancing_method]	
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name, IP-Adresse und Serviceport, die von jedem Poolmitglied verwendet werden.
IP-Adresse [ip_address]	
Serviceport [service_port]	
Pool [pool]	
VLAN des Lastenausgleichsmoduls [cmdb_ci_lb_vlan]	
Name [name]	Der Name des VLAN und das Tag, das diesem VLAN zur Identifizierung zugeordnet ist
Tag [tag]	
MAC-Adresse [mac_address]	
Load Balancer-Services [cmdb_ci_lb_service]	
Name [name]	Details zum Lastenausgleichsservice, der die Arbeitslast auf andere Server (zum Beispiel Webserver) verteilt.
IP-Adresse [ip_address]	
Port [port]	
Betriebsstatus [operational_status]	
Trefferanzahl [hit_count]	
DNS [cmdb_ci_dns_name]	
Name [name]	Name und IP-Adresse des Domänennamenservers für die Netzwerkadapter
IP-Adresse [ip_address]	
Netzwerkadapter [cmdb_ci_network_adapter]	
Name [name]	Details über die Netzwerkadapter im Lastenausgleichsmodul

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
IP-Adresse [ip_address]	
Netzmaske [netmask]	
MAC-Adresse [mac_address]	
Cluster [cmdb_ci_cluster]	
Name [name]	Details über das Cluster von Lastenausgleichsmodulen
Clusterstatus [cluster_status]	
Cluster-ID [cluster_id]	
IP-Adresse [ip_address]	
Clusterknoten [cmdb_ci_cluster_node]	
Name [name]	Details über alle Knoten in einem Cluster
Cluster-ID [cluster_id]	
Clusterstatus [cluster_status]	

Beziehungen von Konfigurationselementen für Cluster

Für Cluster werden die folgenden Beziehungen erstellt:

CI	Beziehung	CI
cmdb_ci_cluster	Hostet::Gehostet auf	cmdb_ci_lb_bigip
cmdb_ci_cluster_node	Gehostet auf::Hostet	cmdb_ci_lb_bigip
cmdb_ci_cluster_node	Cluster von::Cluster	cmdb_ci_cluster

Erstellen Sie einen serverlosen Zeitplan für F5 BIG-IP Auf REST OAuth 2,0-Authentifizierung basierende Discovery

Erstellen Sie einen serverlosen Discovery-Zeitplan für die Erkennung F5 BIG-IP Lastenausgleichsmodule über REST OAuth 2,0-Authentifizierung (Token).

Vorbereitungen

- Stellen Sie sicher, dass Sie über die IP-Adresse für verfügen F5 BIG-IP Lastenausgleichsmodul.
- Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung. Weitere Informationen finden Sie unter Virtual Server Interface .
- Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung. Weitere Informationen finden Sie unter Anmeldeinformationsaliasse für Discovery .

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**an.
2. Erstellen Sie den Discovery-Zeitplandatensatz.
   a. Wählen Sie **Neu**.
   b. Füllen Sie im Formular die Felder aus.

Discovery-Zeitplan – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Erkannt	Scan-Typ, der serverlos sein muss.
MID-Server verwenden	Name des MID-Server Zur Verwendung für diesen Zeitplan.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

   c. Wählen Sie **Absenden**.
3. Erstellen Sie das Ausführungsmuster.
   a. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.
   b. In **Serverlose Ausführungsmuster** Wählen Sie die Registerkarte aus **Neu** .
   c. Füllen Sie im Formular die Felder aus.

Serverloses Ausführungsmuster – Formular „neuer Datensatz“

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll, wobei es sich um das F5 REST OAuth 2,0-Authentifizierungsmuster handeln muss.
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren, der global sein muss.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

   d. Wählen Sie **Absenden**.
4. Legen Sie die Parameter des Musterstartprogramms fest.
   a. In **Startprogramm-Parameter Für Discovery-Muster** Wählen Sie den von Ihnen erstellten Datensatz aus.
   b. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
ip_address	IP-Adresse des F5 BIG-IP Lastenausgleichsmodul.
credential_alias	Name des von Ihnen erstellten Anmeldeinformationsalias.

c. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem Sie auswählen **Entdecken Sie jetzt** Oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

HAProxy Lastenausgleichsmodul-Discovery mithilfe von Probes

Discovery von HAProxy Lastenausgleichsmodule der Community-Edition werden von SSH ausgeführt.

Hinweis: Beginnend mit Muster für Discovery und Service-Mapping Version 1.15.0, musterbasierte Discovery ist die Standardmethode für die Erkennung HAProxy Lastenausgleichsmodule.

- Informationen zum Aktivieren der probenbasierten Discovery finden Sie unter Aktivieren HAProxy Lastenausgleichsmodul-Discovery mit Probes.
- Informationen zum HA-Proxy-Muster finden Sie unter HAProxy Lastenausgleichsmodul-Discovery mit Mustern.
- Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

HAProxy ist ein Open Source-Lastenausgleichsmodul, das jeden TCP-Service verwalten kann. Sie eignet sich besonders für den HTTP-Lastenausgleich, da sie die Sitzungspersistenz und die Layer 7-Verarbeitung unterstützt. Discovery Unterstützt HAProxy Für HTTP-Lastenausgleich. Der TCP-Lastenausgleich wird nicht unterstützt.

Berücksichtigen Sie die folgenden Anforderungen für die Erkennung von HAProxy:

- Die HAProxy Software wird auf einem Linux-Server installiert und ausgeführt.
- Die MID-Server Wird bereitgestellt, um den Server und zu erkunden MID-Server Hat Zugriff auf den Server HAProxy Konfigurationsdatei.
- Die Konfigurations-Probe sucht mit einer der folgenden Methoden nach der Datei haproxy.cfg:
  - Mit *f*Parameter für HAProxy Prozessausgabe.
  - Im Standardpfad /etc/haproxy/haproxy.cfg
- Die HAProxy Probes erfordern Anmeldeinformationen und Ausführungsberechtigungen, um Befehle auszuführen.

Discovery Verwendet **Unix: Aktive Prozesse** Probe zum Identifizieren von HAProxy Lastenausgleichsmodul, wenn der Name des Prozesses lautet `haproxy` . Wenn dieses Kriterium erfüllt ist, wird ein Datensatz in der Tabelle „HAProxy-Load Balancer“ [cmdb_ci_lb_haproxy] erstellt, falls für den ausgeführten Prozess noch kein Datensatz vorhanden ist.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy-Probes

Probe	Beschreibung	Befehle
HAProxy - Version	Der Sensor dieser Probe füllt den aus HAProxy Version in der Tabelle „HAProxy-Lastenausgleichsmodule“ [cmdb_ci_lb_haproxy].	haproxy
HAProxy - Get Configuration	Der Sensor dieser Probe trägt zusätzliche Informationen in die Tabelle „HAProxy-Load Balancer“ [cmdb_ci_lb_haproxy] ein. Die Probe trägt auch Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool], „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member], „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] und „Load Balancer-Applikation“ [cmdb_ci_lb_appl] ein.	echo, sed, cut, grep, egrep (im Bourne-Shell-Skript)

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungsdatensätze erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool.

Aktivieren HAProxy Lastenausgleichsmodul-Discovery mit Probes

Wenn Sie nicht mit der Verwendung von beginnen möchten HAProxy Musterbasierte Discovery, aktivieren Sie probenbasierte HAProxy Discovery, um sie stattdessen weiterhin zu verwenden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**an.
2. In **Name** Feld, suchen Sie nach HAProxy .
3. Wählen Sie den HAProxy-Klassifizierer aus.
4. In **Löst Probe aus** Zugehörige Liste, wählen Sie aus **Bearbeiten** .
5. Entfernen **Horizontales Muster** Aus der Liste der Auslöser-Probes.
6. Fügen Sie in der Liste Sammlung hinzu **HAProxy: Konfiguration abrufen** Und **HAProxy: Version** Zur Liste Auslöser-Probe.
7. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Planen Sie eine horizontale Discovery, um den HAProxy-Lastenausgleichsmodul mit Probes zu erkennen. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Zugehörige Informationen

HAProxy Lastenausgleichsmodul-Discovery mithilfe von Probes

NGINX-Lastenausgleicherkennung

Die Erkennung von NGINX-Lastenausgleichsmodulen erfolgt mithilfe von SSH.

NGINX ist ein Open Source-Webserver mit einem Lastenausgleichsmodul. Discovery erkennt den Webserver und Informationen über das Lastenausgleichsmodul.

Beachten Sie die folgenden Anforderungen für die Erkennung von NGINX-Servern:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- Der MID Server hat Zugriff auf die NGINX-Konfigurationsdatei, die standardmäßig `/etc/nginx/nginx.conf` lautet.
- Aktivieren Sie SSH-Befehle (Secure Shell).
- Zur Ausführung von Befehlen benötigen die NGINX-Probes Anmeldeinformationen und Ausführungsrechte.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service-Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. Diese Liste enthält Befehle, die erhöhte Rechte erfordern, um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen.

Der Prozessklassifizierer „Nginx“ erkennt einen laufenden Prozess, der während der Erkundung eines UNIX-Servers die folgenden Kriterien erfüllt:

- Der Name des Prozesses beginnt mit *`nginx`*.
- Der Name des Prozesses enthält *`master`*.

Die beiden folgenden Bedingungen müssen erfüllt sein:

- In der Tabelle „Webserver“ [cmdb_ci_web_server] wird ein Datensatz erstellt.
- In der Tabelle „CI-Beziehung“ [cmdb_rel_ci] wird für den Linux-Server (Linux-Server [cmdb_ci_linux_server]) und für den Webserver (Webserver [cmdb_ci_web_server]) eine Beziehung vom Typ **Wird ausgeführt auf** erstellt.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

NGINX-Probes

Probe	Beschreibung	Befehle
Nginx – Version	Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „Webserver“ [cmdb_ci_web_server].	nginx
Nginx – Get Configuration	Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei festlegt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.	echo, sed, cut, grep, egrep (im Bourne-Shell-Skript)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungsdatensätze erstellt:

- Die Datensätze in der Tabelle „cmdb_ci_web_server“ werden für die Datensätze in der Tabelle „cmdb_ci_linux_server“ ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool.

Radware Alteon-Lastenausgleicherkennung

Discovery Identifiziert und klassifiziert Informationen zu Alteon-Lastenausgleichsmotoren.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen .

Klassifizierer, Muster und Probe

Klassifizierung	Auslöser-Probe	Muster
Alteon Load Balancer	Horizontal pattern	Alteon Load Balancer by SNMP (früher Alteon Load Balancer)

Erfasste Daten

In der Alteon-Tabelle [cmdb_ci_lb_alteon] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number
Betriebsstatus	operational_status

In der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	nam
MAC-Adresse	mac_address
Betriebsstatus	operational_status
Index	index

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Index	index
Lastenausgleichsmethode	load_balancing_method

In der Tabelle „Load Balancer Pool-Mitglied“ [cmdb_ci_pool_member] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
IP-Adresse	ip_address
Serviceport	service_port

In der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port
Betriebsstatus	operational_status
Installationsstatus	install_status
Trefferanzahl	hit_count

In der DNS-Tabelle [cmdb_ci_dns_name] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

Radware-appDirector-Lastenausgleicherkennung

Die Erkennung von Radware-Lastenausgleichsmodulen erfolgt mithilfe von SNMP.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen .

Klassifizierer, Muster und Probes

Klassifizierung	Probe	Muster
Radware - AppDirector - Load Balancer	Probe „Horizontal Discovery“: Startet Muster	AppDirector Load Balancer

Datenerkennung

In der Tabelle „Radware-Lastenausgleichsmodule“ [cmdb_ci_lb_radware] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number

In der Tabelle „DNS-Name“ [cmdb_ci_dns_name] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

In der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port
Betriebsstatus	operational_status
Installationsstatus	install_status

Felder und Probes von Lastenausgleichsmodulen

Discovery speichert die Informationen der Lastenausgleichsmodule in mehreren Tabellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Informationen in diesem Thema beziehen sich nur auf die Erkennung mit Probes und Sensoren. Wenn Sie Muster verwenden, um zum Beispiel F5 Big-IP-Lastenausgleichsmodule zu erkennen, lesen Sie das entsprechende Thema für diesen Typ von Lastenausgleichsmodul.

Hinweis: Standardmäßig verwendet das System für den CI-Datensatz die erkannte IP-Adresse eines Lastenausgleichsmoduls. Das kann die Verwaltungs-IP sein, die für das Gerät erstellt wurde und die im Erkennungszeitplan verwendet wird. Anweisungen dazu, wie Discovery dazu gezwungen werden kann, anstelle einer Management-IP die IP-Adresse der NIC des Lastenausgleichsmoduls zu verwenden, finden Sie unter Eigenschaften der IP-Adressauswahl.

Felder in der Tabelle „Citrix NetScaler" [cmdb_ci_lb_netscaler]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	SNMP - Netscaler - Identity - Serial
Asset-Tag [asset_tag]	SNMP - Netscaler - Identity
Modell-ID [model_id]	SNMP - Netscaler - Identity

Felder in der Tabelle „Cisco GSS" [cmdb_ci_lb_cisco_gss]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	Cisco GSS - Serial Number
Modell-ID [model_id]	Cisco GSS - Identity
IP-Adresse [ip_address]	Cisco GSS - Network
Hersteller [manufacturer]	Cisco GSS - Identity

Felder in der Tabelle „Cisco CSS" [cmdb_ci_lb_cisco_css]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	SNMP - Load Balancer – Identity
Modell-ID [model_id]	
IP-Adresse [ip_address]	
Hersteller [manufacturer]	

Felder in der Tabelle „F5 BIG-IP" [cmdb_ci_lb_bigip]

Feldbezeichnung und -name	Probes, die Daten erfassen
Aktive Module [active_modules]*	SNMP - F5 BIG-IP - System
Asset-Tag [asset_tag]	
Modell-ID [model_id]	
Failover-Modus [failover_mode]*	
Failover-Peer [failover_peer]*	
Seriennummer [serial_number]	Cisco GSS - Serial Number

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder in der Tabelle „Load Balancer“ [cmdb_ci_lb]

Feldbezeichnung und -name	Probes, die Daten erfassen
Betriebsstatus [operational_status]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System • SNMP - Load Balancer - Identity
Name [name]	

Felder in der Tabelle „Load Balancer-Applikation“ [cmdb_ci_lb_appl]

Feldbezeichnung und -name	Probes, die Daten erfassen
Konfigurationsdatei [config_file]*	Nginx - Get Configuration
Name [name]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx - Get Configuration
IP-Adresse [ip_address]*	
Letzter Discovery-Scan [last_discovered]*	
Version [version]	• Apache - Version • HAProxy - Version • Nginx - Version

Felder der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface]

Feldbezeichnung und -name	Probes, die Daten erfassen
Status [install_status]*	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Name [name]	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder in der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool]

Feldbezeichnung und -name	Probes, die Daten erfassen
Lastenausgleichsmethode [load_balancing_method]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Letzter Discovery-Scan [last_discovered]*	
Name [name]	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder der Tabelle „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member]

Feldbezeichnung und -name	Probes, die Daten erfassen
Vollqualifizierter Domänenname [fqdn]*	• HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
IP-Adresse [ip_address]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx- Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Letzte Erkennung [last_discovery]*	
Name [name]	
Pool [pool]*	
Serviceport [service_port]	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service]

Feldbezeichnung und -name	Probes, die Daten erfassen
Eingabe-URL [input_url]	• Apache - Get JK Module • Apache - Get Proxy Module • Nginx - Get Configuration
IP-Adresse [ip_address]	• Apache - Get JK Module • Apache - Get Proxy Module • Cisco GSS - Identity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] (Fortsetzung)

Feldbezeichnung und -name	Probes, die Daten erfassen
	• HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Letzter Port [last_port]*	HAProxy - Get Configuration
Load Balancer [load_balancer]	• Apache - Get JK Module • Apache - Get Proxy Module • Cisco GSS - Identity • HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Letzte Erkennung [last_discovery]*	
Serviceport [service_port]*	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer-VLAN“ [cmdb_ci_lb_vlan]

Feldbezeichnung und -name	Probes, die Daten erfassen
Load Balancer [load_balancer]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Name [name]	
Tag [tag]	• SNMP - F5 BIG-IP - System • SNMP - Netscaler - System

Apache-Webserverdaten

Discovery erfasst mithilfe von SSH auch Daten in Apache-Webserver-Lastenausgleichsmodulen. Unter Apache mod_JK- und mod_Proxy-Discovery finden Sie weitere Informationen zu Probes für Apache-Webserverdaten. Informationen zu den Tabellen, Feldern und Datenquellen, die Discovery für Apache-Webserver füllt, finden Sie unter Apache Webserver-Discovery.

Automatische Übersetzung

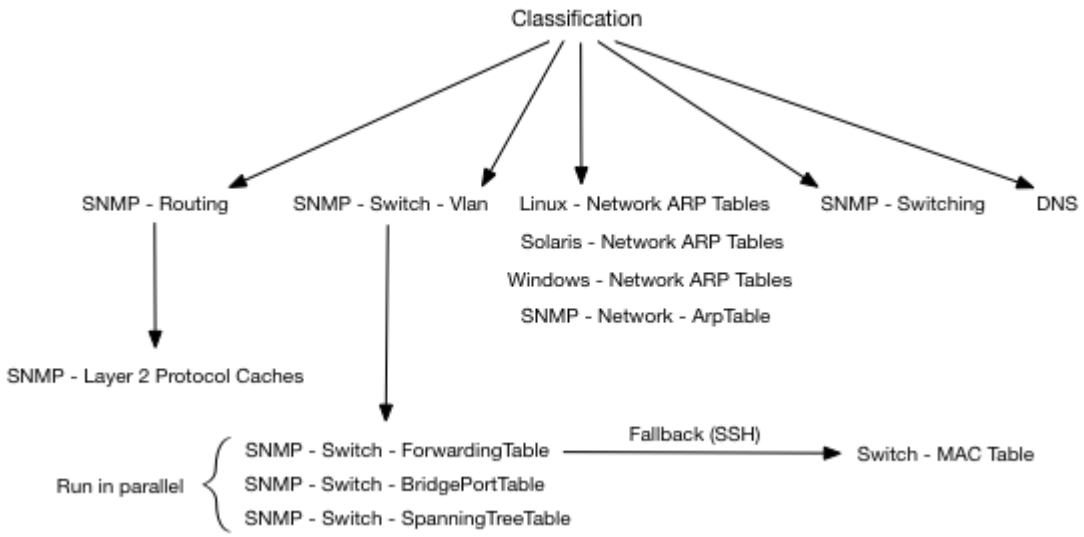
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Layer 2-Erkennung

Discovery kann die physischen Verbindungen (als Layer 2 bezeichnet) zwischen Netzwerkgeräten erkennen.

Layer 2-Erkennungsprozess

Discovery verwendet mehrere Probes, um Informationen über Netzwerkadapter und deren Layer 2-Verbindungen zu sammeln. Das folgende Diagramm zeigt die Probes, die Discovery für die Netzwerkerkennung startet, einschließlich der für die Layer 2-Erkennung verwendeten.



Wenn Discovery beispielsweise einen Switch in einem Netzwerk erkennt, werden die Probes *`SNMP - Switch - Vlan`* und *`SNMP - Network - ARPTable`* ausgelöst. Für jedes von Discovery erkannte VLAN werden verschiedene Switch-Probes ausgelöst. Wenn ein Switch über Weiterleitungsfunktionen verfügt, löst Discovery die Probe *`SNMP - Routing`* aus, um Informationen zu Netzwerkadaptern in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] zu erfassen. Wenn Discovery einen Server erkennt, wird die entsprechende ARP-Probe (Address Resolution Protocol) für dieses Betriebssystem ausgelöst. Discovery unterstützt auch die Verwendung von Mustern wie *`Network Switch`* und *`Network Router`*, die in Discovery standardmäßig verfügbar sind. Weitere Informationen finden Sie unter Netzwerk-Switch- und Router-Discovery.

Während der Erkennung eines Netzwerkgeräts erstellt Discovery Datensätze in den Tabellen „Routerschnittstelle“ [dscy_router_interface] und „Switchport“ [dscy_switchport]. Diese Informationen beinhalten Informationen über die Netzwerkadapter für dieses Gerät. Für SNMP-fähige Geräte erfasst Discovery die Informationen während der Erkundungsphase von einer Weiterleitungs-Probe. Als Nächstes wird die Probe „Layer 2 Protocol Cache“ ausgeführt, um Nachbardaten von dem Gerät zu erfassen.

Nachbardaten abrufen

Während Discovery Netzwerkinformationen von den Probes auf einem Gerät erfasst, identifiziert die Probe „SNMP - Layer 2 Protocol Caches“ Nachbargeräte über CDP und LLDP. Diese Probe aktualisiert die Tabelle „Nachbargeräte“ [discovery_device_neighbors], die die Layer 2-Verbindungen zwischen Switches enthält. Manchmal sind der Instanz die Nachbarn dieses Geräts noch nicht bekannt. Die Schnittstelle des Nachbarn kann erst dann in einen Datensatz aufgelöst werden, wenn Discovery die Seite des Nachbarn in der Beziehung ermittelt hat. Wenn Discovery auf dem Nachbargerät ausgeführt wird,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vervollständigt Discovery die Informationen für die Schnittstelle des Nachbarn für das ursprüngliche Meldegerät.

Aus den folgenden Caches kann Discovery Nachbardaten auf einem Netzwerkgerät abrufen:

- CDP (Cisco Discovery Protocol) : Cache auf Cisco-Geräten, der Informationen zu Nachbargeräten in Form einer protokollspezifischen Nachbar-ID enthält. CDP (Cisco Discovery Protocol).
- LLDP (Link Layer Discovery Protocol) : Generischer Cache, der Informationen zu Nachbargeräten in Form einer protokollspezifischen Nachbar-ID enthält
- ARP (Address Resolution Protocol) : Cache, der die IP- und MAC-Adressen aller verbundenen Geräte und Server enthält

Funktionsweise der Layer 2-Erkennung

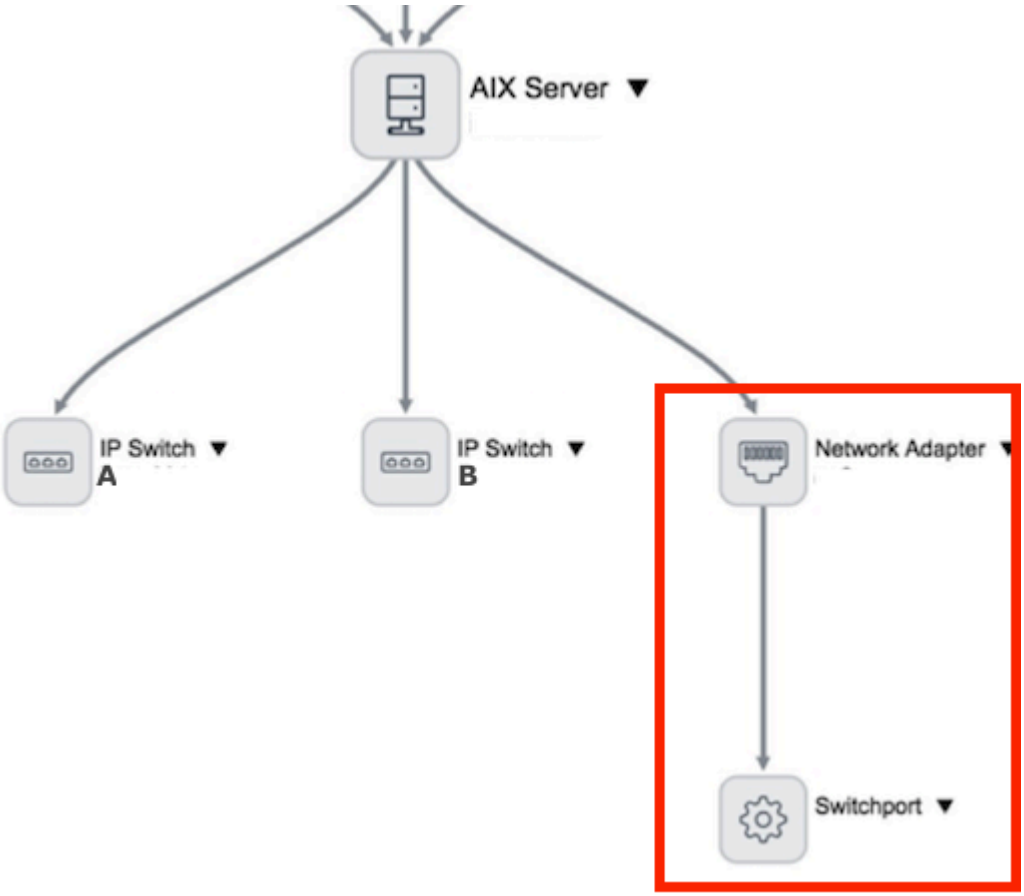
Nach der Geräteerkennung führt das System in der Gerätetabelle [discovery_device_history] die Geschäftsregel „Service Discovery - Device Complete (Service Discovery - Gerät abgeschlossen)“ aus. Diese Geschäftsregel verwendet mehrere Strategien zusammen mit Informationen aus verschiedenen Tabellen, um *`Connects to:Connected by`*-Beziehungen in der CMDB zu erstellen. Beziehungen können zwischen folgenden Komponenten erstellt werden:

- Einem Server und einem Switch
- Zwei Switches
- Einem Gerät und dem Port eines anderen Geräts
- Den Ports von zwei Geräten

Im folgenden Beispiel hat Discovery einen Server, auf dem AIX ausgeführt wird, und zwei IP-Switches im Netzwerk gefunden. Die folgenden Beziehungen wurden erstellt:

- Eine Beziehung vom Typ *`Connects to`* zwischen dem AIX-Server und den beiden IP-Switches A und B.
- Eine Referenz zwischen dem AIX-Server und seinem eigenen Netzwerkadapter.
- Eine Beziehung vom Typ *`Connects to`* zwischen den Adaptern auf den beiden IP-Switches (in der folgenden Abbildung nicht dargestellt).
- Eine Beziehung vom Typ *`Connects to`* zwischen dem Netzwerkadapter des AIX-Servers und dem Switchport von IP-Switch A (rot hervorgehoben). Diese Art von Beziehung wird standardmäßig erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um diese Beziehungen anzuzeigen, öffnen Sie die Abhängigkeitsansicht für den Server. Um die Beziehung zwischen den beiden IP-Switches anzuzeigen, öffnen Sie die Abhängigkeitsansicht von einem der Switches aus, und wählen Sie in den Zuordnungseinstellungen als **Abhängigkeitstyp** die Option **Physische Netzwerkverbindungen** aus.

Layer 2-Verbindungsstrategien

Bei der Layer 2-Erkennung werden die folgenden Strategien verwendet, um Beziehungen zwischen Geräten in einem Netzwerk zu erstellen:

PhysicalHostConnectionStrategy

Diese Strategie erstellt eine Verbindung zwischen einem erkannten Server, der kein Netzwerkgerät ist, und einem Netzwerkgerät. Durch diese Strategie können Layer 2-Verbindungen nur erstellt werden, wenn in der Weiterleitungstabelle des Switch eine einzelne MAC-Adresse für den Port vorhanden ist. Wenn der Port über mehrere MAC-Adressen verfügt, erstellt Discovery keine Verbindung zwischen Server und Switch.

Wenn der Port des Switches identifiziert wird, erstellt Discovery einen **Stellt eine Verbindung her mit::Connected by** Beziehung zwischen dem Serveradapter und dem Switch-Port. Andernfalls erstellt Discovery einen **Stellt eine Verbindung her mit::Connected by** Beziehung zwischen dem Serveradapter und dem Switch selbst.

VMLayer2ConnectionStrategy

Diese Strategie erstellt eine Verbindung zwischen einer VM und einem Netzwerkgerät. Wenn die Anzahl der außergewöhnlichen MAC-Adressen sehr gering ist (weniger als 3 und weniger als 15 % aller MAC-Adressen des ESX-Servers und der zugehörigen VMs), erstellt Discovery eine Layer 2-Verbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NetworkDeviceLayer2ConnnectionStrategy

Mit dieser Strategie wird eine Verbindung zwischen einem Netzwerkgerät und seinen Nachbarn erstellt. Discovery erstellt eine Layer 2-Verbindung, wenn ein einzelner Nachbar mit einer Nachbaradresse und/oder einer Nachbarschnittstelle ist. Wenn die Schnittstelle des Nachbarn vorhanden ist, erstellt Discovery eine Beziehung vom Typ **Verbunden mit::Verbunden von** zwischen der Ursprungsschnittstelle und der Schnittstelle des Nachbarn. Andernfalls erstellt Discovery eine Beziehung vom Typ **Verbunden mit::Verbunden von** zwischen der Ursprungsschnittstelle und dem Switch mit der Adresse des Nachbarn.

SpanningTreeLayer2ConnectionStrategy

Bei dieser Strategie wird eine Verbindung zwischen einem Netzwerkgerät und dem übergeordneten Element des Netzwerkgeräts in der Strukturansicht erstellt.

JavaScriptLayer2ConnectionStrategy

Diese Strategie ruft eine Javascript-Funktion mit leerer Implementierung auf. Dadurch wird die Erstellung einer zusätzlichen Strategie ermöglicht.

Address Resolution Protocol (ARP) bei der Layer 2-Erkennung

Die Probes für Address Resolution Protocol (ARP) ordnen die IP-Adresse eines Computers oder Netzwerkgeräts einer MAC-Adresse zu. Diese Probes rufen die IP-Adresse und MAC-Adresse für ein Konfigurationselement aus der Tabelle „Netzwerkinfrastrukturelement“ [dscy_net_base] ab. Geräte, die SNMP unterstützen, wie Linux-Computer und Netzwerkgeräte, speichern im Cache zwei Arten von Adressinformationen:

- **Statisch**: Manuell hinzugefügte Adressauflösungen
- **Dynamisch**: Paare aus Hardwarename und IP-Adresse, die dem Cache durch vorherige, erfolgreiche ARP-Auflösungen hinzugefügt wurden

Wenn Discovery mit der ARP-Tabelle fertig ist, erfasst das System alle statischen und dynamischen Tabelleneinträge von Geräten über SNMP. Wenn ein neuer ARP-Eintrag verfügbar ist, wird er der Netzwerk-ARP-Tabelle [discovery_net_arp_table] hinzugefügt. Wenn zuvor erkannte ARP-Einträge nicht mehr in der ARP-Tabelle des Geräts zwischengespeichert werden, löscht das System die entsprechenden Datensätze nach einem Abgleich aus der CMDB.

Hinweis: Wenn nach der Ausführung von Discovery neue ARP-Einträge erstellt werden, werden sie erst bei Ausführung des nächsten Discovery-Zeitplans erkannt. Wenn ARP-Einträge nach der Ausführung von Discovery vom Gerät gelöscht werden, wird die CMDB-ARP-Tabelle erst aktualisiert, wenn Discovery erneut ausgeführt wird.

Discovery stellt folgende Probes zum Extrahieren von Informationen zur Auflösung von IP- und MAC-Adressen bereit:

Probe	ECC-Warteschlangenthema	Befehl	Beschreibung
Linux - Network ARP Tables	SSHCommand	sh ${file:linux_arp.sh} Dadurch wird eine Skriptdatei ausgeführt, damit zuerst der Befehl net-tools (arp -n) ausgeführt wird. Wenn dies fehlschlägt, wird	Probe „SSH Command“, die Netzwerkinformationen aus der ARP-Tabelle auf einem Linux-Server abruft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	ECC-Warteschlangenthema	Befehl	Beschreibung
		der Befehl iproute2 (ip neighbor) ausgeführt.	
Solaris - Network ARP Tables	SSHCommand	arp -an	Probe „SSH Command“, die Netzwerkinformationen aus der ARP-Tabelle auf einem Solaris-Server abruft
Windows - Network ARP Table	PowerShell	arp -a	Powershell-Probe, die Netzwerkinformationen aus der ARP-Tabelle auf einem Windows-Server abruft
SNMP - Network - ArpTable	SNMP	Tabelle Die SNMP-Probe verwendet zunächst folgende OID: iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable ipNetToMediaPhysAddress,ipNetToMediaNetAddress. Wenn die Probe keine Ergebnisse zurückgibt, wird folgende OID verwendet: iso.org.dod.internet.mgmt.mib-2.ip.ipNetToPhysicalTable ipNetToPhysicalNetAddress,ipNetToPhysicalPhysAddress.	SNMP-Probe, die Informationen aus der ARP-Tabelle auf einem Switch oder Router sammelt

SNMP-Switch-Probes

Diese Probes geben Überbrückungsinformationen aus VLANs zurück, die über Netzwerk-Switches verbunden sind, einschließlich Portauswahl, Weiterleitungstabellen und die Nutzung des STP-Protokolls (Spanning Tree Protocol).

SNMP - Switch - BridgePortTable

Diese Probe gibt alle Ports eines Switch zurück, die zum Erstellen einer Bridge zwischen Netzwerksegmenten verwendet werden.

Zurückgegebene Überbrückungsdaten

Tabelle	Switch-Brückenporttabelle [discovery_switch_bridge_port_table] Diese Tabelle wird verwendet, um eine Portnummer in der Tabelle „discovery_switch_fwd_table“ einem Schnittstellenindex zuzuordnen.
OID	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBasePortTable dot1dBasePort,dot1dBasePortIfIndex

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zurückgegebene Überbrückungsdaten (Fortsetzung)

Gefüllte Felder	• cmdb_ci • port • interface_index

SNMP - Switch - SpanningTreeTable

Diese Probe gibt den aktiven Pfad zwischen zwei beliebigen Netzwerkknoten zurück, die von einem Switch überbrückt werden.

Zurückgegebene Bereichsstrukturdaten

Tabelle	Switch-Bereichsstrukturtabelle [discovery_switch_spanning_tree_table]. Diese Tabelle wird für die Suche nach Layer 2-Verbindungen zwischen Switches verwendet.
OID	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dStp.dot1dStpPortTable dot1dStpPort,dot1dStpPortState,dot1dStpPortEnable,dot1dStpPortDesignatedRoot,dot1dStpPortD
Gefüllte Felder	• cmdb_ci • port • port_state • port_enable • designated_root • designated_bridge_mac

SNMP - Switch - ForwardingTable

Diese Probe gibt Informationen aus der Weiterleitungstabelle eines Switch zurück.

Zurückgegebene Daten aus Weiterleitungstabellen

Tabelle	Switch-Weiterleitungstabelle [discovery_switch_fwd_table] Das ist die Weiterleitungstabelle für Switches.
OIDs	Diese OIDs werden nach Bedarf durch die Skripteinbindung `DiscoveryVlanSwitchProcessor` erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zurückgegebene Daten aus Weiterleitungstabellen (Fortsetzung)

	• **Non-Cisco**: ○ **Q-BRIDGE MIB**: oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot dot1qTpFdbAddress.' + vlanIndex + ',dot1qTpFdbPort.' + vlanIndex + ',dot1qTpFdbStatus.' + vlanIndex; ○ **BRIDGE MIB**: oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable dot1dTpFdbAddress,dot1dTpFdbPort,dot1dTpFdbStatus'; • **Cisco BRIDGE MIB**: oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable dot1dTpFdbAddress,dot1dTpFdbPort,dot1dTpFdbStatus';
Zusätzliche aufgerufene Probe	Die SSH-Probe Switch - MAC Table kann durch die Skripteinbindung *DiscoveryVlanSwitchProcessor* ausgelöst werden, um zusätzliche Layer 2-Daten bereitzustellen. Wenn Layer 2-Daten fehlen, nachdem Sie die Erkennung in mehreren VLANs ausgeführt haben, sollten Sie das Auslösen der Probe Switch - MAC Table aktivieren und die Erkennung erneut ausführen. Fügen Sie dazu der Tabelle „Systemeigenschaft“ [sys_properties] die folgende Eigenschaft hinzu: glide.discovery.sensors.forwardingtable.ssh. Legen Sie den Wert der Eigenschaft auf **true** fest. Standardmäßig ist diese Eigenschaft auf „false“ eingestellt.
Befehl	show mac address-table
Gefüllte Felder	• cmdb_ci • vlan_id • port • Status • mac_address (aus dem Feld **cmdb_ci** in der Tabelle „Netzwerkinfrastrukturelement“ [discovery_net_base])

SNMP - Switch - Vlan

Diese Probe gibt VLAN-IDs von einem Netzwerk-Switch und die folgenden OIDs zurück:

```
iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoVtpMIB.vtpMIBObjects.vlanInfo.vtpVlanTable vtpVlanState

iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoVlanMembershipMIB.ciscoVlanMembershipMIBObjects.vmMembership.vmMembershipSummaryTable
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
vmMembershipSummaryVlanIndex,vmMembershipSummaryMemberPorts,vmMembershipSummaryMember2kPorts

iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnxExMibRoot.jnxExSwitching.jnxExVlan.jnxVlanMIBObjects.jnxExVlanTable jnxExVlanTag

iso.org.dod.internet.mgmt.mib-2.system.sysDescr
```

Andere Switch-Typen werden nicht unterstützt.

Porttabellen

Die folgenden Porttabellen werden während der horizontalen Erkennung eines Geräts gefüllt:

- Netzwerkadapter [cmdb_ci_network_adapter]
- Switchport [dscy_switchport]
- Routerschnittstelle [dscy_router_interface]
- Load Balancer-Schnittstelle [cmdb_ci_lb_interface]

Erkennung von TCP-Verbindungen

Discovery identifiziert und klassifiziert Informationen zu TCP-Verbindungen mithilfe der ADM- und ADME-Probes.

Discovery füllt die Tabelle „TCP-Verbindungen“ [cmdb_tcp] mit folgenden Daten.

Bezeichnung	Tabellenname	Feldname	Beschreibung
Abwesend	cmdb_tcp	absent	Wenn der Prozess auf diesem Gerät nicht mehr ausgeführt wird. Wenn der Prozess zum ersten Mal erkannt wird, wird der Wert nicht ausgewählt (sprich: der Prozess fehlt nicht). Wenn Discovery erneut ausgeführt wird und den Prozess nicht erkennt, wird er ausgewählt.
Computer	cmdb_tcp	Computer	Das Gerät, das mit dem TCP-Port verbunden ist oder diesen abhört
IP	cmdb_tcp	ip	Die IP-Adresse, die von diesem Gerät oder Prozess abgehört wird oder mit der eine Verbindung besteht. Wenn die IP-Adresse 127.0.0.1 lautet, handelt es sich um den Hostcomputer selbst.
PID	cmdb_tcp	pid	Die ID des Prozesses, zu dem eine Verbindung hergestellt wird oder der von diesem Gerät (IP-Adresse) abgehört wird
Port	cmdb_tcp	port	Die Portnummer, über die der TCP-Datenverkehr erkannt wurde
Vorgang	cmdb_tcp	process	Der Prozess, zu dem eine Verbindung hergestellt wird oder der von dem Port abgehört wird
Typ	cmdb_tcp	Typ	• **Lauschen auf**: Der Prozess hört das Gerät über TCP ab. • **Verbindung wird hergestellt**: Wenn der Prozess über TCP mit diesem Gerät verbunden ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Tabellenname	Feldname	Beschreibung
count	cmdb_tcp	count	Die Häufigkeit, mit der Discovery eine bestimmte TCP-Verbindung erkennt. Dieses Feld wird von erweiterten ADM-Probes verwendet.

Discovery füllt die Tabelle „Laufender Prozess“ [cmdb_running_process] mit diesen Daten.

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name des laufenden Prozesses
Computer	Computer	Das Gerät, auf dem der Prozess ausgeführt wird
Übergeordnet	parent	Der übergeordnete Prozess dieses Prozesses, falls vorhanden
Lauschen auf	listening_on	Die Ports, die von den Prozessen abgehört werden
Verbunden mit	connected_to	Die Ports, mit denen die Prozesse verbunden sind
Befehl	command	Der Befehl für diesen Prozess, einschließlich Pfad
PID	pid	Die ID für den Prozess
PPID	ppid	Die ID für den übergeordneten Prozess
Abwesend	absent	Wenn der Prozess auf diesem Gerät nicht mehr ausgeführt wird. Wenn der Prozess zum ersten Mal erkannt wird, wird der Wert nicht ausgewählt (sprich: der Prozess fehlt nicht). Wenn Discovery erneut ausgeführt wird und den Prozess nicht erkennt, wird er ausgewählt.
Klassifizieren	classify	Gibt an, ob der laufende Prozess klassifiziert werden soll
Schlüsselparameter	key_parameters	Die Schlüsselparameter für den Befehl
Parameter	parameters	Die Parameter für den Befehl
Anzahl	count	Die Häufigkeit, mit der Discovery eine bestimmte TCP-Verbindung erkennt. Dieses Feld wird von erweiterten ADM-Probes verwendet.

Standardmäßige ADM-Probes

Mit der standardmäßigen ADM-Erkennung startet Discovery die folgenden Probes:

Name	Beschreibung	Eingeschlossene Sub-Probes
AIX - ADM	Fragt Informationen über aktive (laufende) AIX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• AIX - Active Connections • AIX - Active Processes
HP-UX - ADM	Fragt Informationen über aktive (laufende) HP-UX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich. Diese Probe erfordert die Installation von lsof und die Aktivierung der Probe „UNIX - Active Connections“, der standardmäßig inaktiv ist.	• UNIX - Active Connections • HP-UX - Active Processes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Eingeschlossene Sub-Probes
Solaris - ADM	Fragt Informationen über aktive (laufende) Solaris-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich. Diese Probe wird durch die Probe „Solaris Zones“ ausgelöst. Das System löst eine ADM-Probe für jede lokale Zone in einer globalen Zone aus. Diese Probe erfordert, dass lsof in der globalen Zone installiert wird.	• Solaris - Active Processes • Solaris - Active Connections
UNIX - ADM	Fragt Informationen über aktive (laufende) UNIX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• UNIX - Active Connections • UNIX - Active Processes
Windows - ADM	Fragt Informationen über aktive (laufende) Windows-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• Windows - Active Connections • Windows - Active Processes
UNIX - ADM netstat	Führt dieselben Funktionen wie die Probe „UNIX ADM“ aus, ist dabei zur Unterstützung der kontinuierlichen TCP-basierten Erkennung auf Netstat angewiesen. Service Mapping verwendet diese Probe für die auf Datenverkehr basierende Erkennung.	• UNIX - Active Connections with Netstat. Diese Probe ruft TCP-Verbindungen ab, um die Tabellen cmdb_tcp und cmdb_tcp_connection zu füllen. • UNIX - Active Processes. Diese Probe ruft TCP-Prozesse ab und füllt die Tabelle cmdb_running_process.

Erweiterte ADM-Probes

Wenn erweitertes ADM aktiviert ist, startet Discovery die folgenden Probes:

Probe	Beschreibung
Windows - ADM Enhanced	Führt dieselben Funktionen wie die Probe „Windows ADM“ aus, jedoch mit zusätzlichen Parametern, um die kontinuierliche TCP-basierte Erkennung zu steuern. Diese Probe ist sowohl mit von WinRM unterstützten als auch mit nicht von WinRM unterstützten MID Servern kompatibel. Konfigurieren Sie Ihren MID Server mit dem Parameter mid.windows.management_protocol. Siehe MID-Server-Parameter Für die Werte, die Sie für diesen Parameter verwenden können.
UNIX - ADM Enhanced	Führt dieselben Funktionen wie die Probe „UNIX ADM“ aus, jedoch mit zusätzlichen Parametern, um die kontinuierliche TCP-basierte Erkennung zu steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie mit den erweiterten ADM-Probes die folgenden Probe-Parameter:

Parameter	Beschreibung
mid.adme.max_result_size	Steuert die Größe der TCP-Nachverfolgungsdatei
max.adme_result_payload_size	Steuert die Größe des Ergebnisses, einschließlich der Nutzlast **Hinweis:** Wenn dieser Wert größer ist als MID-Server-Eigenschaften Mid.Discovery.max_Payload_size, ein Konfigurationsfehler kann auftreten.

Zugehörige Informationen

Application Dependency Mapping (ADM) für Discovery

Erkennung von IP-Adressen

Discovery identifiziert und klassifiziert Informationen über IP-Adressen.

Von Discovery über IP-Adressen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
IP-Adresse	cmdb_ci_ip_address	ip_address	Verschiedene interne
IP-Version	cmdb_ci_ip_address	ip_version	Verschiedene interne
Netzmaske	cmdb_ci_ip_address	netmask	Verschiedene interne
Nic	cmdb_ci_ip_address	nic	Verschiedene interne

Erkennung von IP-Netzwerken

Discovery identifiziert und klassifiziert Informationen über IP-Netzwerke.

Von Discovery über IP-Netzwerke erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Erkennen	cmdb_ci_ip_network	discover	Verschiedene interne
Subnetz	cmdb_ci_ip_network	subnet	Verschiedene interne
Netzwerk-Discovery	cmdb_ci_ip_network	network_discovery	Verschiedene interne
Zuletzt erkannt	cmdb_ci_ip_network	last_discovered	Verschiedene interne
MID-Server	cmdb_ci_ip_network	mid_server	Verschiedene interne
Router	cmdb_ci_ip_network	router	Verschiedene interne
Status	cmdb_ci_ip_network	state	Verschiedene interne

Erkennung von Netzwerkdruckern

Discovery identifiziert und klassifiziert Informationen über Netzwerkdrucker.

Discovery kann Netzwerkdrucker identifizieren und klassifizieren. Weitere Informationen finden Sie unter Netzwerk-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery über Netzwerkdrucker erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Seriennummer	cmdb_ci	serial_number	SNMP, verschiedene MIBs
Startdatum	cmdb_ci	start_date	SNMP, RFC1213 MIB
Hersteller	cmdb_ci	manufacturer	SNMP, RFC1213 MIB
Modell-ID	cmdb_ci	model_id	SNMP, RFC1213 MIB
IP-Adresse	cmdb_ci_network_adapter	ip_address	SNMP, IP MIB
MAC-Adresse	cmdb_ci_network_adapter	mac_address	SNMP, IF MIB
Druckertyp	cmdb_ci_printer	print_type	SNMP, PRINT MIB
Zähler verwenden	cmdb_ci_printer	use_count	SNMP, PRINT MIB
Einheiten für Nutzungszähler	cmdb_ci_printer	use_units	SNMP, PRINT MIB
Farben	cmdb_ci_printer	colors	SNMP, PRINT MIB
Horizontale Auflösung	cmdb_ci_printer	horizontal_resolution	SNMP, PRINT MIB
Vertikale Auflösung	cmdb_ci_printer	vertical_resolution	SNMP, PRINT MIB
Auflösungseinheiten	cmdb_ci_printer	resolution_units	SNMP, PRINT MIB
Beschreibung	discovery_printer_supplies	Beschreibung	SNMP, PRINT MIB
Versorgungstyp	discovery_printer_supplies	supply_type	SNMP, PRINT MIB
Versorgungsklasse	discovery_printer_supplies	supply_class	SNMP, PRINT MIB
Aktuelle Ebene	discovery_printer_supplies	current_level	SNMP, PRINT MIB
Max. Kapazität	discovery_printer_supplies	max_capacity	SNMP, PRINT MIB
Name	cmdb_ci	Name	Shazzam, SNMP, verschiedene MIBs

Netzwerk-Switch- und Router-Discovery

Discovery Identifiziert und klassifiziert Informationen zu Netzwerk-Switches und -Routern.

Netzwerk-Switches und -Router verfügen häufig über sehr ähnliche Fähigkeiten. Einige Switches, die als Layer 3-Switches bezeichnet werden, verfügen üblicherweise über IP-Weiterleitung. Größere Router mit optionalen Modulen können unter Umständen Switching-Module aufnehmen. Aufgrund dieser Überschneidungen und der sich daraus ergebenden Mehrdeutigkeit der Klassifizierung eines bestimmten Geräts erfasst Discovery für Router und Switches dieselben Daten, sofern diese auf einem bestimmten Gerät verfügbar sind. Weitere Informationen dazu, wie Discovery Daten über Verbindungen zwischen Netzwerkgeräten und anderen Komponenten erfasst, finden Sie unter Layer 2-Erkennung.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Voraussetzungen

- Der Router oder Switch muss über IP-Adressinformationen verfügen.
- Die Systemeigenschaft glide.discovery.L3_mapping wird auf „true“ festgelegt, damit Router und Switches erkannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Router oder Layer 3-Switch, der die IP-Adresse bereitstellt, muss erfolgreich mit den vorhandenen Weiterleitungsregeln für Exit-Schnittstellen erkannt werden.
- Wenn Sie die Tabelle [Discovery_device_neighbors] während der Erkennung der horizontalen Ebene 2 der bgp-fähigen Geräte ausfüllen müssen, legen Sie fest **BGP-Routererkundung deaktiviert** Eigenschaft bis **Nein** . Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen mit zu wenig Arbeitsspeicher auf dem MID-Server.

Systemeigenschaften

Sie können viele Aspekte von Discovery so konfigurieren, dass sie Ihren persönlichen Präferenzen entsprechen. Die folgenden Eigenschaften gelten für Netzwerkrouter und -Switches. Um die Eigenschaften anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Eigenschaften** Sofern nicht anders angegeben.

Eigenschaft	Beschreibung
glide.discovery.L3_mapping	Dadurch wird eine Beziehung vom Typ IP-Verbindung::IP-Verbindung zwischen Servern und Netzwerkgeräten erstellt. • **Typ:** Zeichenfolge • **Standardwert:** Wahr • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
glide.discovery.max_concurrent_invocations_per_schedule	Legt die maximale Anzahl geplanter Aufrufe desselben Erkennungszeitplans fest. Dadurch wird verhindert, dass die geplanten Ausführungen in Rückstand geraten, wenn die Erkennung nicht vor der geplanten Ausführung des nächsten Aufrufs abgeschlossen ist. Der Wert ist eine Ganzzahl, die der maximalen Anzahl automatisierter Aufrufe desselben Zeitplans entspricht, die gleichzeitig ablaufen können. Nach Erreichen des Limits werden nachfolgende geplante Aufrufe storniert. Diese Eigenschaft wird durch den Wert 0 oder eine negative Zahl deaktiviert. • **Typ:** Ganzzahl • **Standardwert:** 3 • **Standort: Discovery-Definition** > **Eigenschaften** **Hinweis:** Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „auch wenn abgebrochen“ festgelegt ist.

Eine Liste der in der Discovery allgemein verwendeten Eigenschaften finden Sie unter Discovery-Eigenschaften.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen

Discovery untersucht mit dem SNMP-Protokoll viele Arten von Geräten (Switches, Router, Drucker usw.). Anmeldeinformationen für SNMP-Communitys beinhalten keinen Benutzernamen, sondern nur ein Passwort, das als Community-Zeichenfolge bezeichnet wird. Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und Discovery testet diese automatisch. SNMPv3-Anmeldeinformationen erfordern je nach ausgewähltem Protokoll einen Benutzernamen und einen Schlüssel. Geben Sie den entsprechenden ein SNMP-Anmeldeinformationen Ob sie sich von der Zeichenfolge der öffentlichen Community unterscheiden.

Hinweis: SSH wird für Lastenausgleichsmodule unterstützt, für Router und Switches aber nicht.

Klassifizierer, Muster und Probes

Klassifizierungen	Auslöser-Probes	Muster
Standard Network Router Standard Network Switch	• Horizontal Pattern: Startet Muster • SNMP-Weiterleitung^ • DNS* • SNMP-Identität* • SNMP-Switch-VLAN* • SNMP-Switching* • SNMP - Network - ArpTable* (nur Standard Network Switch)	Network Router Network Switch

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

^Diese Probe bleibt für den Klassifizierer „Standard Network Router“ standardmäßig aktiv, selbst wenn Discovery die Mustererkennung verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Gestapelte Switches erkennen

Die gemeinsam genutzte Bibliothek „Network Switch“ bietet Unterstützung für gestapelte Cisco-Switches. Die CI-Tabelle hierfür ist „IP-Switch“ [cmdb_ci_ip_switch]. Mehrere Switches im Stapel werden anhand der primären IP-Adresse identifiziert. Jedes Mitglied des Stapels wird durch eine Kombination von Elementen identifiziert, darunter die primäre IP-Adresse, einen dem Switch zugeordneten Namen und den Stapelmodus. Die Beziehung wird zwischen einer primären und allen sekundären IP-Adressen erstellt. Der primäre Switch verfügt über alle in der folgenden Tabelle aufgeführten Felder. Der sekundäre Switch hat Name, Serial_number, model_ID, Manufacturer, Stack, und Stack_Mode.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn alle Ports auf einem Switch an Port 161 geöffnet sind, besitzt dieser Switch mehrere IP-Adressen (eine für jeden Port), während die Seriennummer für alle Ports identisch ist. Die CI-Identifizierung erfolgt basierend auf der Seriennummer. Daher wird jedes Mal derselbe Datensatz aktualisiert, anstatt einen neuen Datensatz zu erstellen.

Router- und Switch-Daten

Tabellenname	Bezeichnung/Feldname	Quelle
cmdb_ci	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci	Startdatum (nur, wenn das Ziel ein Host ist) start_date	SNMP, RFC1213 MIB
cmdb_ci	Hersteller manufacturer	SNMP, RFC1213 MIB
cmdb_ci	Modell-ID model id	SNMP, RFC1213 MIB
cmdb_ci_ip_router	Name Name	
cmdb_ci_ip_router	Modell-ID model ID	SNMP, RFC1213 MIB
cmdb_ci_ip_router	Hersteller manufacturer	SNMP, RFC1213 MIB
cmdb_ci_ip_router	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci_ip_router	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_ip_router	Beschreibung short_description	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
cmdb_ci_ip_router	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_ip_router	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB
cmdb_ci_ip_router	Port port	
cmdb_ci_ip_switch	Name Name	
cmdb_ci_ip_switch	Modell-ID model ID	SNMP, RFC1213 MIB
cmdb_ci_ip_switch	Hersteller manufacturer	SNMP, RFC1213 MIB
cmdb_ci_ip_switch	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci_ip_switch	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_ip_switch	Beschreibung short_description	
cmdb_ci_ip_switch	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_ip_switch	Ports Ports	SNMP, dot1dBridge MIB
cmdb_ci_ip_switch	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
cmdb_ci_ip_switch	Kann VLANs partitionieren can_partitionvlans	SNMP, dot1dBridge MIB
cmdb_ci_ip_switch	Stapel stack	SNMP, entPhysicalTable
cmdb_ci_ip_switch	Stapelmodus stack_mode	SNMP, entPhysicalTable
cmdb_ci_netgear	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_netgear	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB
cmdb_ci_netgear	Kann VLANs partitionieren cdscy_router_interface	SNMP, dot1dBridge MIB
cmdb_ci_netgear	Hub möglich can_hub	SNMP, IP MIB
cmdb_ci_network_adapter	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_network_adapter	MAC-Adresse mac_address	SNMP, IF MIB
discovery_device_neighbors	Nachbaradresse neighbor_address	CiscoCdpMIB
discovery_device_neighbors	Nachbar-ID neighbor_ID	ciscoCdpMIB, lldpMIB
discovery_device_neighbors	Nachbarschnittstelle neighbor_interface	ciscoCdpMIB, lldpMIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
discovery_device_neighbors	Nachbarquelle neighbor_source	ciscoCdpMIB, lldpMIB
discovery_device_neighbors	Ursprungsschnittstelle origin_interface	ciscoCdpMIB, lldpMIB
discovery_net_arp_table	IP-Adresse IP_address	SNMP, IP MIB
discovery_net_arp_table	MAC-Adresse mac_address	SNMP, IP MIB
discovery_switch_bridge_port_table	Schnittstellenindex interface_index	SNMP, dot1dBridge MIB
discovery_switch_bridge_port_table	Port port	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	Port port	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	Status Status	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	VLAN-ID vlan_id	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Festgelegter Brücken-MAC designated_bridge_mac	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Festgelegter Root designated_root	SNMP, dot1dBridge MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
discovery_switch_spanning_tree_table	Port port	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Portaktivierung port_enable	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Portstatus port_state	SNMP, dot1dBridge MIB
dscy_router_interface	Name Name	SNMP, IP MIB
dscy_router_interface	Typ Typ	SNMP, IP MIB
dscy_router_interface	Nummer Nummer	SNMP, IP MIB
dscy_router_interface	IP-Adresse ip_address	SNMP, IP MIB
dscy_router_interface	MAC-Adresse mac_address	SNMP, IP MIB
dscy_route_interface	Zielnetzwerk dest_ip_network	SNMP, IP MIB
dscy_route_interface	Typ Typ	SNMP, IP MIB
dscy_route_next_hop	Zielnetzwerk dest_ip_network	SNMP, IP MIB
dscy_route_next_hop	Typ Typ	SNMP, IP MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
dscy_route_next_hop	Nächster Hop next_hop_ip_address	SNMP, IP MIB
dscy_switchport	Typ Typ	SNMP, dot1dBridge MIB
dscy_switchport	Status Status	SNMP, dot1dBridge MIB
dscy_switchport	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
dscy_switchport	Portnummer port_number	SNMP, dot1dBridge MIB
dscy_switchport	Schnittstellenname interface_name	SNMP, dot1dBridge MIB
dscy_switchport	Schnittstellennummer interface_number	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	MAC-Hersteller mac_mfr	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	Status Status	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	IP-Adresse ip_address	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	Netzmaske netmask	SNMP, dot1dBridge MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenname	Bezeichnung/Feldname	Quelle
dscy_swtch_partition	Basis-IP-Adresse base_ip_address	SNMP, dot1dBridge MIB
dscy_swtch_partition	Basis-MAC-Adresse base_mac_address	SNMP, dot1dBridge MIB
dscy_swtch_partition	Basis-Netzmaske base_netmask	SNMP, dot1dBridge MIB
dscy_swtch_partition	Typ Typ	SNMP, dot1dBridge MIB
dscy_swtch_partition	Transparent transparent	SNMP, dot1dBridge MIB
dscy_swtch_partition	Quellroute sourceroute	SNMP, dot1dBridge MIB
dscy_swtch_partition	Name Name	SNMP, dot1dBridge MIB
dscy_swtch_partition	Status Status	SNMP, dot1dBridge MIB
dscy_swtch_partition	Schnittstellennummer interface_number	SNMP, dot1dBridge MIB

Erfassung von Portdaten für SNMP-Netzwerkgeräte deaktivieren

In einigen Umgebungen möchten Sie die Portdaten für SNMP-Netzwerkgeräte möglicherweise nicht erfassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Netzwerkgeräte eine sehr große Anzahl von Ports enthalten und die Informationen jedes einzelnen Ports für die Gesamtverwaltung der Geräte nicht kritisch sind, möchten Sie Portdaten für SNMP-Netzwerkgeräte möglicherweise nicht erfassen. Dies wirkt sich auf die Erstellung von Datensätzen in der Switchports-Tabelle (dscy_switchport) aus. Dieser Prozess wirkt sich nur auf die Probe-Erkennung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Discovery-Definition** > **Probes**an.
2. Wechseln Sie zur Probe **SNMP - Switching**.
3. In **SNMP-Felder** Registerkarte suchen Sie das Feld mit dem Namen **Ports** , Doppelklicken Sie auf den Wert in **Aktiv** Und ändern Sie den Wert in **Falsch** .
   Dadurch werden die Erfassung und Verarbeitung von Portinformationen für Switches deaktiviert. Das Feld **ports** für das Switch-CI muss die richtige Anzahl von Ports enthalten, auch wenn die zugehörige Liste **switchports** leer ist.
4. Klicken Sie auf das Häkchen, um die Änderung zu speichern.

Erkennung von IP-Services und Daemons

Discovery identifiziert und klassifiziert Informationen über Services und Daemons.

Von Discovery über Services und Daemons erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ip_service	Name	Verschiedene
Port	cmdb_ip_service	port	Verschiedene
Beschreibung	cmdb_ip_service_ci	Beschreibung	Verschiedene
CI	cmdb_ip_service_ci	ci	Interne Referenz
Service	cmdb_ip_service_ci	service	Interne Referenz

Erkennung unterbrechungsfreier Stromversorgungen (USV)

Discovery identifiziert und klassifiziert Informationen zu einer unterbrechungsfreien Stromversorgung (USV).

Discovery kann unterbrechungsfreie Stromversorgungen identifizieren und klassifizieren.

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Seriennummer	cmdb_ci	serial_number	SNMP, verschiedene MIBs
Startdatum	cmdb_ci	start_date	SNMP, RFC1213 MIB
Hersteller	cmdb_ci	manufacturer	SNMP, RFC1213 MIB
Modell-ID	cmdb_ci	model_id	SNMP, RFC1213 MIB
IP-Adresse	cmdb_ci_network_adapter	ip_address	SNMP, IP MIB
MAC-Adresse	cmdb_ci_network_adapter	mac_address	SNMP, IF MIB
Version der USV-Software	cmdb_ci_ups	ups_software_version	SNMP, UPS MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Version der Agent-Software	cmdb_ci_ups	agent_software_version	SNMP, UPS MIB
Angeschlossene Geräte	cmdb_ci_ups	attached_devices	SNMP, UPS MIB
Batteriestatus	cmdb_ci_ups	battery_status	SNMP, UPS MIB
Sekunden Restbatterieleistung	cmdb_ci_ups	seconds_on_battery	SNMP, UPS MIB
Geschätzte Minuten Restbatterieleistung	cmdb_ci_ups	est_mins_remaining	SNMP, UPS MIB
Geschätzte verbleibende Ladung (%)	cmdb_ci_ups	est_charge_remaining	SNMP, UPS MIB
Batteriespannung	cmdb_ci_ups	battery_voltage	SNMP, UPS MIB
Batteriestromstärke	cmdb_ci_ups	battery_current	SNMP, UPS MIB
Batterietemperatur (C)	cmdb_ci_ups	battery_temperature	SNMP, UPS MIB
Eingangsleitungsfehler	cmdb_ci_ups	input_line_bads	SNMP, UPS MIB
Ausgangsquelle	cmdb_ci_ups	output_source	SNMP, UPS MIB
Ausgangsfrequenz	cmdb_ci_ups	output_freq	SNMP, UPS MIB
Umgehungs-Frequenz	cmdb_ci_ups	bypass_freq	SNMP, UPS MIB
Nenn-Eingangsspannung	cmdb_ci_ups	nom_input_volt	SNMP, UPS MIB
Nenn-Eingangsfrequenz	cmdb_ci_ups	nom_input_freq	SNMP, UPS MIB
Nenn-Ausgangsspannung	cmdb_ci_ups	nom_output_volt	SNMP, UPS MIB
Nenn-Ausgangsfrequenz	cmdb_ci_ups	nom_output_freq	SNMP, UPS MIB
Nenn-Ausgangs-VA	cmdb_ci_ups	rated_output_va	SNMP, UPS MIB
Nenn-Ausgangsleistung	cmdb_ci_ups	rated_output_power	SNMP, UPS MIB
Schwellenwert niedriger Batteriestand (Minuten)	cmdb_ci_ups	low_battery_threshold_mins	SNMP, UPS MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Akustischer Alarmstatus	cmdb_ci_ups	audible_alarm_status	SNMP, UPS MIB
Niederstrom-Transferpunkt	cmdb_ci_ups	low_voltage_transfer_point	SNMP, UPS MIB
Starkstrom-Transferpunkt	cmdb_ci_ups	high_voltage_transfer_point	SNMP, UPS MIB
Eingabeverzeichnis	cmdb_ci_ups_input	input_index	SNMP, UPS MIB
Eingangsfrequenz (Hz)	cmdb_ci_ups_input	input_freq	SNMP, UPS MIB
Eingangsspannung (RMS VAC)	cmdb_ci_ups_input	input_volt	SNMP, UPS MIB
Eingangsstrom (RMS AAC)	cmdb_ci_ups_input	input_current	SNMP, UPS MIB
Eingangsleistung (Watt)	cmdb_ci_ups_input	input_power	SNMP, UPS MIB
Ausgangsverzeichnis	cmdb_ci_ups_output	output_index	SNMP, UPS MIB
Ausgangslast (%)	cmdb_ci_ups_output	output_load	SNMP, UPS MIB
Ausgangsspannung (RMS VAC)	cmdb_ci_ups_output	output_volt	SNMP, UPS MIB
Ausgangsstrom (RMS AAC)	cmdb_ci_ups_output	output_current	SNMP, UPS MIB
Ausgangsleistung (Watt)	cmdb_ci_ups_output	output_power	SNMP, UPS MIB
Verzeichnis umgehen	cmdb_ci_ups_bypass	bypass_index	SNMP, UPS MIB
Spannung umgehen (RMS VAC)	cmdb_ci_ups_bypass	bypass_volt	SNMP, UPS MIB
Stromstärke umgehen (RMS AAC)	cmdb_ci_ups_bypass	bypass_current	SNMP, UPS MIB
Leistung umgehen (Watt)	cmdb_ci_ups_bypass	bypass_power	SNMP, UPS MIB
Alarmverzeichnis	cmdb_ci_ups_alarm	alarm_index	SNMP, UPS MIB
Alarmtyp	cmdb_ci_ups_alarm	alarm_type	SNMP, UPS MIB
Alarmzeit	cmdb_ci_ups_alarm	alarm_time	SNMP, UPS MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere DataPower-Discovery

ITOM-Transparenz Erkennt IBMWebSphere DataPower. Discovery verwendet das Muster „DataPower Server“ für die horizontale Erkennung. Service-Mapping verwendet das Muster „DataPower“ für die Erkennung von oben nach unten.

Voraussetzungen

Konfigurieren Sie vor der Erkennung von IBM WebSphere DataPower-Geräten die folgenden Anmeldeinformationen:

SNMP-Anmeldeinformationen

SNMP-Anmeldeinformationen sind für die Verwendung der folgenden SNMP-Abfragen erforderlich:

- Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.2.1.4.20.1
  - 1.3.6.1.2.1.2.2.1
  - 1.3.6.1.4.1.14685.3.1.196.1
  - 1.3.6.1.4.1.14685.3.1.11.1
  - 1.3.6.1.4.1.14685.3.1.112.1
- Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.4.1.14685.3.1.11.1

Applicative-Anmeldeinformationen

Neben SNMP-Anmeldeinformationen sind zum Erkennen von DataPower-Anwendungsdomänen auch Applicative-Anmeldeinformationen erforderlich, auch als logische CIs bekannt.

Darüber hinaus werden SNMP- und Applicative-Anmeldeinformationen für die Top Down-Discovery von Anwendungsbeziehungen (entsprechende DataPower-Anwendungsdomäne) verwendet.

Benutzer mit Berechtigungen zum Ausführen von SOAP

Damit eine Top Down-Discovery für den DataPower-Webservice und die MQ-Verbindung ausgeführt werden kann, sind Berechtigungen zum Ausführen von SOAP-Abfragen erforderlich.

Von Discovery während der horizontalen Erkennung erfasste Daten

Standardmäßig verwendet Discovery zur Erkennung das Muster „DataPower Server“.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
DataPower-Hosting-Server [cmdb_ci_datapower_server]	
Modellnummer [model_number]	Das Modell des Servers, auf dem WebSphere DataPower gehostet wird
Hostname [host_name]	Der Hostname des Servers, auf dem WebSphere DataPower gehostet wird
Seriennummer [serial_number]	Die Seriennummer des Servers, auf dem WebSphere DataPower gehostet wird
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	Die IP-Adresse des Servers, auf dem WebSphere DataPower gehostet wird
Netzmaske [netmask]	Die Netzmaske des Servers, auf dem WebSphere DataPower gehostet wird
Netzwerkadapter [cmdb_ci_network_adapter]	
MAC-Adresse [mac_address]	Die MAC-Adresse des Netzwerkadapters
Name [name]	Der Name des Netzwerkadapters

CI-Beziehungen

CI	Beziehung/Referenz	CI
DataPower-Hosting-Server [cmdb_ci_datapower_server]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	DataPower-Hosting-Server [cmdb_ci_datapower_server]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Tabelle und Feld	Beschreibung
DataPower [cmdb_ci_app_server_datapower]	
Hostname [host_name]	Die Attribute der Anwendung DataPower
SOAP-URL [soap_url]	
Version [version]	
IP-Adresse [ip_address]	
Name [name]	
Domäne [domain]	

Cisco Unified Computing System (UCS) – HD-Geräte-Discovery

Discovery identifiziert und klassifiziert Informationen zu Cisco UCS-Geräte, einschließlich Gehäuse und Blades.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anmeldeinformationen

Konfigurieren Sie beide SNMP-Anmeldeinformationen Und Anwendbare Anmeldeinformationen .

Klassifizierer, Muster und OIDs

Der Klassifizierer UCS verwendet HorzontalDiscoveryProbe, um das Muster UCS - HD zu starten. Der Klassifizierer verwendet auch die folgenden SNMP-OIDs, die die Tabelle „Cisco-UCS-Zubehör“ [cmdb_ci_ucs_equipment] angeben:

OID	Hersteller	Modell	Tabelle
1.3.6.1.4.1.9.12.3.1.3.847	Unified Computing Cisco UCS 6120XP 20-Port Fabric Interconnect	1.4(3u)(NX-OS) 5.0 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.899	Unified Computing Cisco UCS 6140XP 40-Port Fabric Interconnect	1.4(3u)(NX-OS) 5.0 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.1062	Unified Computing Cisco UCS 6248UP 48-Port Fabric Interconnect	2.0(1t)(NX-OS) 5.0.2 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.1063	Unified Computing Cisco UCS 6296UP 96-Port Fabric Interconnect	2.0(1t)(NX-OS) 5.0.2 Aggregation Switch	Cisco-UCS-Zubehör

Erfasste Daten

Es werden nur Geräte der B-Serie erkannt. Mit dem Muster „UCS - HD“ werden keine Geräte der C-, S- oder E-Serie erkannt. In der Tabelle „Cisco-UCS-Zubehör“ [cmdb_ci_ucs_equipment] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Modell	model_id
Distinguished Name (DN)	dn
UCS-Manager-Version	Version

In der Tabelle „Cisco-UCS-Gehäuse“ [cmdb_ci_ucs_chassis] werden die folgenden Daten erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname
Name	Name
Modellnummer	model_number
Seriennummer	serial_number
Gehäuse-ID	chassis_id
Betriebsstatus	operational_status
Distinguished Name (DN)	dn

In der Tabelle „Cisco-UCS-Blade“ [cmdb_ci_ucs_blade] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Modellnummer	model_number
Seriennummer	serial_number
CPU-Anzahl	cpu_count
Anzahl CPU-Kerne	cpu_core_count
RAM	ram
Anzahl der Adapter	number_of_adapters
Gehäuse-ID	chassis_id
Steckplatz-ID	slot_id
Beschreibung	short_description
Distinguished Name (DN)	dn
Blatt-Seriennummer	Blade_Serial_number
Betriebsstatus	operational_status

In der Tabelle „Cisco-UCS-Rackmount-Einheiten“ [cmdb_ci_ucs_rack_unit] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Lieferant	Lieferant
Server-ID	server_id
Verfügbarkeitsdiagramm	availability
UUID	uuid
Rack-Seriennummer	rack_serial
Anzahl an CPUs	num_of_cpus
Anzahl der Kerne	num_of_cores
Modell-ID	model_id

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Feldname
Speicher gesamt	total_memory
Distinguished Name (DN)	dn
Status	state

Beziehungen

Diese Beziehungen werden erstellt, um UCS – HD-Discovery zu unterstützen:

CI	Beziehung	CI
cmdb_ci_ucs_chassis	Enthält::Enthalten in	cmdb_ci_ucs_blade
cmdb_ci_ucs_equipment	Enthält::Enthalten in	cmdb_ci_ucs_rack_unit
cmdb_ci_ucs_equipment	Enthält::Enthalten in	cmdb_ci_ucs_chassis
cmdb_ci_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_ucs_blade

Dell Remote-Assistent – Kartenerkennung

Die Dell ™Remote Assistant Card (DRAC) und Integrated Remote Assistance Card (iDRAC) bieten Anwendern Tools und Funktionen zur Überwachung, Problembehandlung und Reparatur von Servern. Sie können DNS-URLs für den Zugriff auf Out-of-Band-Geräte generieren, wenn der Zugriff von IP-Adressen aus Sicherheitsgründen verhindert wird.

Zur Identifizierung von DRACs verwendet Discovery die Probe **SNMP - DRAC**. Diese Probe verwendet SNMPv1 und SMNPv2c. Für Out-of-Band-Geräte gibt es einen dedizierten Verwaltungskanal zur Gerätewartung. Systemadministratoren können Geräte mit dem dedizierten Managementkanal remote überwachen und verwalten. Dies schließt die Überwachung von Hardwaresensoren, den Zugriff auf lokale Medienlaufwerke und die Anpassung der BIOS-Einstellungen ein. Für Out-of-Band-Geräte können DNS-URLs generiert werden, um auf die Seite des Out-of-Band-Geräts zuzugreifen, wenn das SSL-Zertifikat die Navigation zur IP-Adresse verbietet.

Erfasste Daten

Von Discovery über Dell DRAC erfasste Daten

Bezeichnung	Tabelle	Name	Befehl
Firmware-Version	cmdb_ci_outofband_device	firmware_version	SNMP-Walk: drsFirmwareVersion (racFirmwareVersion für iDRAC7)
Host *	cmdb_ci_outofband_device	host	SNMP-Walk: drsSystemServiceTag (systemServiceTag für iDRAC7)
IP-Adresse	cmdb_ci_outofband_device	ip_address	DNS probe
Name	cmdb_ci_outofband_device	Name	SNMP Identity probe
Produktversion	cmdb_ci_outofband_device	product_version	SNMP-Walk: drsProductVersion (racVersion für iDRAC7)
Typ	cmdb_ci_outofband_device	Typ	SNMP-Walk: drsProductType (racType für iDRAC7)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery über Dell DRAC erfasste Daten (Fortsetzung)

Bezeichnung	Tabelle	Name	Befehl
URL	cmdb_ci_outofband_device	url	SNMP-Walk: drsProductURL (racURL für iDRAC7)

* **Host** verweist über die Seriennummer auf die Tabelle cmdb_ci_computer. Damit das Feld cmdb_ci_outofband_device.host ordnungsgemäß gefüllt wird, muss der Hostcomputer erkennbar oder in der CMDB mit der entsprechenden Seriennummer vorhanden sein.

Out-of-Band-Geräte

Eine **DNS-URL** wird für Konfigurationselemente in der Liste **Out-Of-Band-Gerät** generiert, wenn das Konfigurationselement einen **Namen** und eine **DNS-Domäne** besitzt. **DNS-URLs** können für Out-of-Band-Geräte generiert werden, um auf die Out-of-Band-Geräteseite zuzugreifen, wenn das SSL-Zertifikat die Navigation zur **IP-URL** verbietet. Die **DNS-URL** weist das Format https://Name.DNS_Domain auf. Wenn das Feld **Name** oder **DNS-Domäne** leer ist, enthält die **DNS-URL** den Wert im Feld **URL**.

Erkennung von HTTP-Geräten

Discovery kann Geräte erkennen, die das HTTP-Protokoll verwenden.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Klassifizierer, Probes und Muster

Die HTTP-Erkennung basiert auf der Port-Probe *`HTTP`*, den Discovery nach dem Versuch ausführt, Probes für SSH- und SNMP-Ports auszuführen. Diese Port-Probe startet die Probe *`HTTP - Classify`*, der eine HTTP GET-Anforderung für jeden Eintrag in der HTTP-Klassifizierungstabelle ausführt. Sie sollten Ihre eigenen Klassifizierungen konfigurieren, auf die die Probe *`HTTP - Classify`* zugreifen kann.

Die Port-Probe „HTTP“ verwendet Zuordnungen zwischen einem Protokoll und einer Portnummer in der Tabelle „IP-Service“ [cmdb_ip_service]. In dieser Tabelle können Sie zusätzliche Port-zu-Protokoll-Definitionen hinzufügen oder das für einen bestimmten HTTP-Klassifizierer verwendete Protokoll überschreiben.

Klassifizierung	Probes	Muster
	HTTP (Port-Probe): Diese Probe startet die Probe „HTTP - Classify“, die eine HTTP GET-Anforderung für jeden Eintrag in der HTTP-Klassifizierungstabelle ausführt.	

Erkennung über einen HTTP- oder HTTPS REST-Aufruf ausführen

Discovery kann Geräte klassifizieren, die das HTTP(S)-Protokoll nutzen. Anstatt SNMP- oder SSH-Anmeldeinformationen zu verwenden, können Sie Ihren eigenen HTTP-Klassifizierer erstellen, um Geräte zu erkennen und mit Anmeldeinformationen der Standardauthentifizierung darauf zuzugreifen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

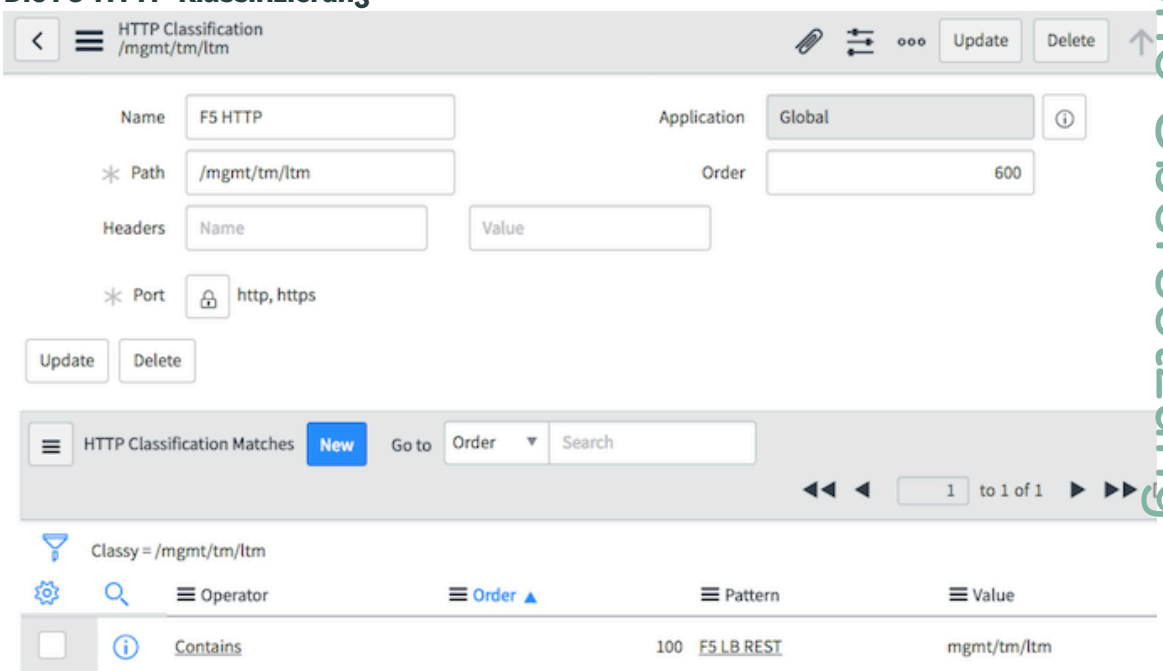
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Klicken Sie auf **Basisanmeldedaten**.
   In den meisten Fällen können Sie über einen HTTP- oder HTTPS REST-Aufruf mit Standardauthentifizierungsinformationen auf ein Gerät zugreifen.

> **Wichtig:** Die HTTP-Klassifizierungsprobe versucht standardmäßig nicht mehr Anmeldeinformationen über das HTTP-Protokoll. Um dieses Verhalten zu überschreiben, können Sie aktivieren `mid.http_classy.allow_credentials_over_http`. Das Aktivieren dieser Einstellung kann jedoch Anmeldeinformationen für MitM-Angriffe (man-in-the-Middle) verfügbar machen. Daher wird dringend empfohlen, diese Eigenschaft auf festzulegen **Falsch** Und verwenden Sie HTTPS, wann immer möglich.

4. Fügen Sie den Anwendernamen und das Passwort hinzu, die Sie für den Zugriff auf das Gerät benötigen.
5. Wählen Sie **Absenden**.
6. Richten Sie einen HTTP-Klassifizierer ein, indem Sie zu navigieren **Discovery-Definition** > **CI-Klassifizierung** > **HTTP**an.
7. Wählen Sie **Neu**.
8. Füllen Sie die Formularfelder aus (siehe Tabelle):

Die F5-HTTP-Klassifizierung



Feld	Beschreibung
Name	Geben Sie einen Namen für den Klassifizierer ein.
Pfad	Geben Sie den Pfad für die HTTP-GET-Anforderung ein.
Header	Fügen Sie einen Optionsheader mit einem Wert hinzu. Sie können eine Variable im Format `${variable}` anstatt eines statischen Wertes verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

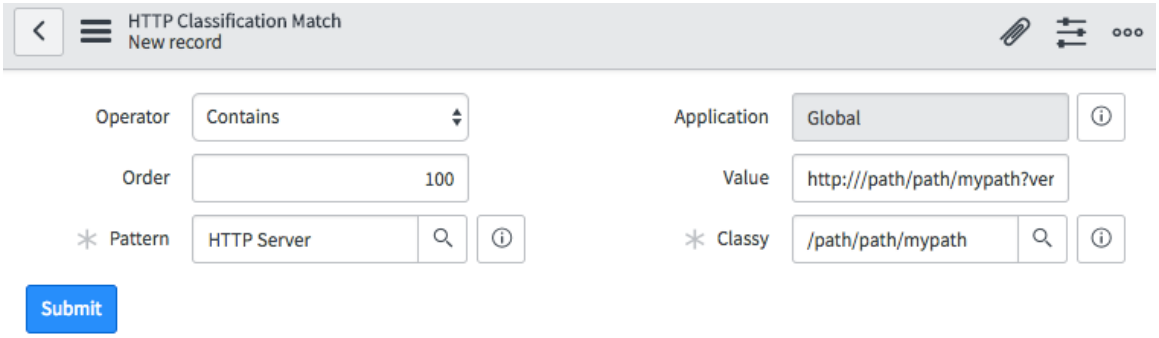
Feld	Beschreibung
	Unterstützte Header hängen vom REST-Webservice-Provider ab, mit dem Sie eine Verbindung herstellen möchten. In der Dokumentation Ihres Web Service Providers erfahren Sie, welche Header gültig oder erforderlich sind.
Port (IP-Dienst)	Wenn Sie möchten, dass dieser Klassifizierer einen benutzerdefinierten Port verwendet, der nicht bereits ein Standardwert in der Tabelle IP-Dienst [cmdb_ip_service] ist, führen Sie folgende Schritte aus: **a.** Wählen Sie das Suchsymbol, um die Liste der IP-Services anzuzeigen. **b.** Wählen Sie Aus **Neu** Und erstellen Sie eine Port-zu-Protokoll-Zuordnung. **c.** Wählen Sie diese Port-zu-Protokoll-Zuordnung dafür im Feld **Port**. Viele häufig verwendete Protokolle sind standardmäßig bereits Ports zugeordnet, z. B. http zu Port 80 und https zu Port 443. Wenn Sie eine dieser standardmäßigen Port-zu-Protokoll-Zuordnungen verwenden möchten, geben Sie keine Werte in ein **Port** Feld. Die HTTP-Port-Sonde verwendet standardmäßig den richtigen Port.
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieses Klassifizierers darstellt. Wenn Discovery mehr als einen zutreffenden Klassifizierer verwendet, wird der Klassifizierer mit niedriger **Rang-**Nummer verwendet.
Protokoll [optional] Dieses Feld ist standardmäßig nicht sichtbar. Sie müssen das Formular konfigurieren, um es hinzuzufügen.	Wenn Sie eine eindeutige Port-zu-Protokoll-Zuordnung für das Fel **Port** konfigurieren, geben Sie in das Feld eine optionale Protokollüberschreibung ein, die Discovery mit diesem Klassifizierer verwendet. Wenn Sie beispielsweise Port 5000 und das HTTP-Protokoll verwenden möchten, fügen Sie die 5000/HTTP-Port-zu-Protokoll-Zuordnung zum Feld **Port** hinzu, und wählen Sie dann **http** im Feld **Protokoll**.

9. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
   Die zugehörige Liste „Übereinstimmung der HTTP-Klassifizierung“ wird angezeigt. Diese zugehörige Liste enthält Kriterien, die Sie für den Abgleich mit dem Hauptteil der Antwort auf die von Discovery gesendete GET-Anforderung konfigurieren können.
10. Definieren Sie in der zugehörigen Liste „Übereinstimmung der HTTP-Klassifizierung“ die Abgleichskriterien, und geben Sie das für diesen Klassifizierer zu startende Muster an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder des Formulars „Übereinstimmung der HTTP-Klassifizierung“ aus (siehe Tabelle).



Feld	Beschreibung
Operator	Wählen Sie den Operator aus, mit dem das System die Bedingung bewertet: ▪ **Enthält** ▪ **Ist gleich** ▪ **Regulärer Ausdruck**
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieser Bedingung darstellt. Wenn Discovery mehr als eine zutreffende Bedingung findet, wird die Bedingung mit niedriger Rang-Nummer verwendet.
Muster	Geben Sie das Muster an, das nach einer korrekten Übereinstimmung gestartet werden soll. Dieses Muster muss HTTP verwenden, um das Gerät zu ermitteln.
Wert	Geben Sie den Wert ein, den der Rumpf der zurückgegebenen REST-Methode haben muss.

c. Wählen Sie **Absenden**.

d. Definieren Sie so viele Übereinstimmungen der HTTP-Klassifizierung wie erforderlich.
Sie können dies tun, wenn verschiedene Muster für verschiedene Versionen des Geräts vorhanden sind, das Sie erkennen möchten.

Example:
In diesem Beispiel ist die HTTP-Klassifizierung so konfiguriert, dass die F5-Lastenausgleichsmodul-API verwendet wird:

Nächste Maßnahme

Wenn Sie keine anderen Arten von Anmeldeinformationen haben, die Geräte finden können, z. B. Linux-Anmeldeinformationen oder SNMP-Anmeldeinformationen, können Sie sehen, wie die Discovery-Anwendung HTTP-Discovery verarbeitet:

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne** Und führen Sie eine Discovery aus.
2. Überprüfen Sie nach Abschluss des Discovery-Prozesses die ECC-Warteschlange, um die Ergebnisse der HTTP-Erkennung anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie sollten sehen, dass nach dem Starten der Shazzam-Probe und dass UNIX- und SNMP-Klassifizierungsprobes fehlgeschlagen sind. Es sollte sowohl die Probe „HTTP - Classify“ als auch das Muster gestartet werden, die Sie im HTTP-Klassifizierungsdatensatz angeben.

Topic	Name	Source	Queue
Multiprobe	Unix - Classify	10.196.39.128	input
Multiprobe	Unix - Classify	10.196.39.128	output
SNMP	SNMP - Classify	10.196.39.128	output
SNMP	SNMP - Classify 108 OIDs	10.196.39.128	input
HTTPClassyProbe	HTTPClassyProbe	10.196.39.128	input
HTTPClassyProbe	HTTPClassyProbe	10.196.39.128	output
Shazzam	wmi,snmp,ssh,wins,dns,slp,wbem,vmapp,win..	See Payload	input
Shazzam	wmi,snmp,ssh,wins,dns,slp,wbem,vmapp,win..	See Payload	output

Erkennung von Speicher

Discovery Sammelt Informationen zu Direct Attached Storage (das), Storage Area Networks (SAN) und Network Attached Storage (NAS).

Speicher kann sich auf speziellen Geräten wie Speicher-Arrays, Fibre Channel-Switches, iSCSI-Datenträger oder auf Host-Betriebssystemen befinden, einschließlich Windows, Linux, Und Solaris.

Discovery erkennt Abhängigkeiten für die folgenden Speichertypen und ordnet sie zu:

- Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Network (SAN)
- NAS- oder SAN-Speicher, der über Storage Management Initiative Specification (SMI-S) und ein Common Information Model (CIM) erkannt wird
- Virtueller Speicher für VMware ESX-Server und Linux Kernel-basierte virtuelle Maschinen (KVM). Discovery ordnet diesen Speicher dem zugrunde liegenden physischen Speicher zu.

Durch die Erkennung von Speicher über einen Host werden Daten abgeglichen und Beziehungen zwischen den Dateisystemen des Hosts und zugehörigen lokalen Speichergeräten erstellt. Die lokalen Speichergeräte stellen den für den Host verfügbaren Speicher dar, und zwar unabhängig davon, ob er direkt angeschlossen ist oder über Fibre Channel oder iSCSI bereitgestellt wird. Bei diesem Abgleich wird davon ausgegangen, dass der Speicherserver bereits erkannt wurde.

Hinweis: Treiber für Bandspeicher werden nicht erkannt.

Discovery Sammelt und erstellt CIs in CMDB Für die folgenden Informationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dateisysteme (lokal und NAS)
- Datenträger (sowohl SAN-Datenträger als auch DAS-Laufwerke)
- FC-HBAs und -Ports (Fibre Channel)
- Linux Volume Manager-Volumes (LVM). LVM-Volumedaten befinden sich in der Tabelle „Speicherpool“ [cmdb_ci_storage_pool].
- Veritas Volume Manager-Datenträger, -Teildatenträger, -Datenträgergruppen, -Plexe und -Volumes

Hinweis: Weitere Informationen zur Erkennung von auf einem Linux-Host bereitgestelltem Direct Attached Storage oder Multipath Block Storage finden Sie unter KB0622583 .

Probes, Sensoren und Muster

- KVM - Storage Pools: Identifiziert Speicher, der an virtuelle KVM-Computer angeschlossen ist
- Linux: Speicher: Identifiziert Speicher, der an Systeme angehängt ist, auf denen ausgeführt wird Linux Betriebssystem.
- Solaris: Speicher: Identifiziert Speicher, der an Systeme angeschlossen ist, auf denen ausgeführt wird Solaris Betriebssystem.
- Windows – Speicher 2008: Identifiziert Speicher, der an ausgeführte Systeme angehängt ist Windows2008.
  - Windows– Speicher 2008 – PS: Identifiziert Speicher, der an ausgeführte Systeme angehängt ist Windows2008, PowerShell verwenden.
  - Windows– Speicher 2008 – WMI: Identifiziert Speicher, der an ausgeführte Systeme angehängt ist Windows2008, mit WMI Runner.
- Windows– Speicher 2012: Identifiziert Speicher, der an ausgeführte Systeme angehängt ist Windows2012 und höher.
  - Windows– Speicher 2012 – PS: Gibt den an angehängten Speicher an Windows Systeme mit PowerShell.
  - Windows– Speicher 2012 – WMI: Identifiziert Speicher, der an angehängt ist Windows Systeme mit WMI Runner.
- VMWare - vCenter ESX Hosts Storage: Erfasst Informationen über ESX-Server und erstellt Beziehungen von Datenspeichern zu zugrunde liegenden Datenträgern
- Muster zur Erkennung von NetApp-Speicher:
  - NetApp7-Modus: Findet NetApp Server über REST mit zwei Knoten.
  - NetApp Clustermodus: Findet NetApp Server über REST, wenn mehr als zwei Knoten über einen Cluster-Interconnect-Switch verbunden sind.

Hinweis: Informationen zur Migration von Probe zu Muster finden Sie im wissensartikel KB0694477 .

Anforderungen

Windows

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unterstützt die folgenden Konfigurationen:
  - Windows Server 2012, das oder NAS mit Fibre Channel (FC) oder Internet Small Computer System Interface (iSCSI).
  - Windows Server 2008, das oder NAS mit FC oder iSCSI.
- Installieren Sie fcinfo.exe Tool auf Windows2008- und 2012-Server, die über FC an den Speicher angehängt werden.
- Installieren Sie Windows Management Instrumentation (WMI).
- Aktivieren Sie Powershell auf dem MID-Server Hostserver.
- Stellen Sie der Instanz die erforderlichen Anmeldeinformationen für den Hostserver bereit.
- Platzieren Sie MID-Server Und den Zielcomputer in derselben Domäne oder fügen Sie den Zielcomputer der Liste vertrauenswürdiger Hosts auf der hinzu MID-Server Computer.
- Installieren Sie auf dem Hostserver optional Windows Remote Management (WinRM) , um Fibre Channel-Informationen zu erkennen. WinRM ist standardmäßig für aktiviert Windows2012 und Windows2016 Computer, aber nicht für Windows2008.

Linux

- Unterstützt die folgenden Konfigurationen:
  - Solaris, Das, NAS oder SAN mit iSCSI
  - CentOS, DAS, NAS oder SAN mit FC oder iSCSI
  - Ubuntu Server, DAS, NAS oder SAN mit iSCSI
- Stellen Sie dem Gerät SSH-Anmeldeinformationen mit Root- oder Sudo-Zugriff bereit.
- Geben Sie an MID-Server Mit den erforderlichen Anmeldeinformationen für den Hostserver.

Beziehungen

Discovery erstellt für Speicher-CIs die folgenden Beziehungen:

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
Speicherexport [cmdb_ci_storage_export]	Exportieren nach::Importieren von	Speichergerät [cmdb_ci_storage_device]
Fibre Channel-Datenträger [cmdb_ci_fc_disk]	Stellt bereit::Bereitgestellt von	Dateisystem [cmdb_ci_file_system]
iSCSI-Datenträger [cmdb_ci_iscsi_disk]	Stellt bereit::Bereitgestellt von	Dateisystem [cmdb_ci_file_system]

Erkennung von Hosts mit angeschlossenem Speicher konfigurieren

Discovery kann Informationen über UNIX-, Linux- und Windows-Hosts mit angeschlossenem Speicher erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery für die Erkennung von UNIX- oder Linux-Hosts mit angeschlossenem Speicher konfigurieren

Discovery kann Informationen über einen UNIX- oder Linux-Host und angeschlossenen Speicher erkennen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. **Wahlweise:** Weisen Sie dem Konto, das von Discovery verwendet wird, auf dem Host erweiterte Berechtigungen zu.
2. Auf der ServiceNow Instanz, Anmeldeinformationen hinzufügen Zu Discovery Anmeldeinformationstabelle.
3. Erstellen Sie einen Discovery-Zeitplan für jede Host-IP-Adresse.
4. **Wahlweise:** Erstellen Sie ein Verhalten, das eine Funktionalitätsdefinition mit einer wbem-Port-Probe verwendet, um die anfängliche Port-Scanphase (Shazzam) effizienter zu gestalten.
5. Führen Sie eine Netzwerkerkennung aus.

Hinweis: Wenn der Host auch eine Verbindung zu einem NAS- oder SAN-Speicher-Array herstellt, richten Sie den ein SMI-S-Anbieter Und CIM-Anmeldeinformationen .

Konfigurieren Discovery Für Windows Hosts mit angehängtem Speicher

Discovery Kann Informationen zu finden Windows Host und angehängter Speicher.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Führen Sie die Schritte aus, wenn Sie verwenden Windows2008 Server, die an Speicher angehängt sind:
   a. Laden Sie herunter, und installieren Sie Microsoft Fibre Channel-Informationstool von http://www.microsoft.com , und durchsuchen Sie die Website nach Microsoft Fibre Channel-Informationstool.
   b. Legen Sie den Umgebungspfad für die ausführbare Datei fcinfo.exe fest, und führen Sie sie aus.

   Hinweis: Für Server, die neuere Betriebssysteme verwenden, ist ähnliche Funktionalität mit dem Betriebssystem vorhanden. Dieser Schritt ist nicht erforderlich.

2. Für alle Windows Hosts einschließlich Windows2008, Windows-Anmeldeinformationen hinzufügen Zu Discovery Anmeldeinformationstabelle.
3. Erstellen Sie in der ServiceNow-Instanz einen Discovery-Zeitplan für jede Host-IP-Adresse.
4. **Wahlweise:** Erstellen Sie ein Verhalten, das eine Funktionalitätsdefinition mit einer wbem-Port-Probe verwendet, um die anfängliche Port-Scanphase (Shazzam) effizienter zu gestalten.
5. Führen Sie eine Netzwerkerkennung aus.

Hinweis: Wenn der Host auch eine Verbindung zu einem NAS- oder SAN-Speicher-Array herstellt, richten Sie den ein SMI-S-Anbieter Und CIM-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Speicher über einen Host erfasste Erkennungsdaten

Discovery erfasst Informationen über Speichereinheiten, die über einen lokalen E/A-Port oder Hostbusadapter (HBA) mit Linux-, Solaris- und Windows-Hosts verbunden sind.

Probes, die zum Erkennen von Speicher von einem Host aus verwendet werden

Tabelle	Probes
Datenträger [cmdb_ci_disk]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Datenträgerpartition [cmdb_ci_disk_partition]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Fibre Channel-Datenträger [cmdb_ci_fc_disk]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Fibre-Channel-Port [cmdb_ci_fc_port]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Dateisystem [cmdb_ci_file_system]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
iSCSI-Datenträger [cmdb_ci_iscsi_disk]	• KVM • Linux - Storage • Solaris - Storage

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Probes
	• Windows - Storage 2008 • Windows - Storage 2012
NAS-Dateisystem [cmdb_ci_nas_file_system]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Speicher-HBA [cmdb_ci_storage_hba]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Speicherpool [cmdb_ci_storage_pool]	Linux - Storage
Speicherpoolmitglied [cmdb_ci_storage_pool_member]	Linux - Storage
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	VMware - vCenter Datastores

Erkannte Speicherreferenzen

Discovery ordnet diese Referenzen für Speichereinheiten zu, die über einen lokalen E/A-Port oder Hostbusadapter (HBA) mit einem Host verbunden sind.

Tabelle und Spalte	Referenz	Zieldatenelement
cmdb_ci_storage_device.computer	referenziert	cmdb_ci_computer
cmdb_ci_storage_device.provided_by	referenziert	cmdb_ci_fc_port (nur für FC)
cmdb_ci_disk_partition.disk	ist eine Partition von	cmdb_ci_disk
cmdb_ci_storage_hba.computer	ist	cmdb_ci_computer
cmdb_ci_fc_port.controller	enthält	cmdb_ci_storage_hba
cmdb_ci_fc_port.computer	ist identisch mit	cmdb_ci_computer wie cmdb_ci_storage_hba.computer
cmdb_ci_storage_volume.computer	ist	cmdb_ci_computer
cmdb_ci_storage_volume.provided_by	ist	cmdb_ci_storage_pool oder cmdb_ci_storage_pool oder cmdb_ci_storage_device (bereitstellender Speicher)
cmdb_ci_storage_pool.hosted_by	ist	cmdb_ci_computer
cmdb_ci_computer	Pool befindet sich in	cmdb_ci_storage_pool.container

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Spalte	Referenz	Zieldatenelement
cmdb_ci_storage_pool.container	ist	cmdb_ci_storage_pool oder cmdb_ci_storage_pool_member, die Pool enthalten (wenn Pool vorhanden)
cmdb_ci_storage_pool_member.pool	ist	cmdb_ci_storage_pool
cmdb_ci_storge_pool_member.storage	ist	cmdb_ci_storage_pool, cmdb_ci_disk_partition oder cmdb_ci_storage_device (bereitstellender Speicher)

Für HBAs auf Linux- und ESX-Servern erfasste Daten

Discovery erfasst Informationen über Hostbusadapter (HBA) für Fibre Channel-fähige Geräte, die mit Linux- und ESX-Servern verbunden sind.

HBA-Tabellen und -Felder

Bezeichnung	Tabelle	Feldname	Quelle
Name	Speicher-HBA [cmdb_ci_storage_hba]	Name	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
WWNN	Speicher-HBA [cmdb_ci_storage_hba]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Modell-ID	Speicher-HBA [cmdb_ci_storage_hba]	model_id	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Computer	Speicher-HBA [cmdb_ci_storage_hba]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage

Fibre Channel-Ports

Bezeichnung	Tabelle	Feldname	Quelle
WWPN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwpn	VMWare - vCenter ESX Hosts Storage • probe • Linux - Storage

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre Channel-Ports (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
WWNN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Porttyp	Fibre-Channel-Port [cmdb_ci_fc_port]	port_type	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Geschwindigkeit	Fibre-Channel-Port [cmdb_ci_fc_port]	speed	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Controller	Fibre-Channel-Port [cmdb_ci_fc_port]	controller	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Computer	Fibre-Channel-Port [cmdb_ci_fc_port]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage

Fibre Channel-Ziele

Bezeichnung	Tabelle	Feldname	Quelle
FC-Datenträger	Fibre Channel-Ziele [cmdb_fc_target]	fc_disk	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Erstellt von	Fibre Channel-Ziele [cmdb_fc_target]	sys_created_by	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Erstellt	Fibre Channel-Ziele [cmdb_fc_target]	sys_created_on	• Linux - Storage • Solaris - Storage

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre Channel-Ziele (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
			• Windows - Storage 2008 • Windows - Storage 2012
SysID	Fibre Channel-Ziele [cmdb_fc_target]	sys_id	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Updates	Fibre Channel-Ziele [cmdb_fc_target]	sys_mod_count	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Aktualisiert von	Fibre Channel-Ziele [cmdb_fc_target]	sys_updated_by	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Aktualisiert	Fibre Channel-Ziele [cmdb_fc_target]	sys_updated_on	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
WWNN	Fibre Channel-Ziele [cmdb_fc_target]	wwnn	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
WWPN	Fibre Channel-Ziele [cmdb_fc_target]	wwpn	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für HBAs auf Solaris-Servern erfasste Daten

Discovery unter Solaris unterstützt HBAs von:

- Emulex
- QLogic

In der Tabelle „Speicher-HBA“ [cmdb_ci_storage_hba] füllt Discovery mithilfe der Probe „Solaris - Storage“ und des zugehörigen Sensors die folgenden Felder.

Bezeichnung	Feldname
Name	Name
Computer	Computer
Geräte-ID	device_id
Hersteller	manufacturer
Modell-ID	model_id
Seriennummer	serial_number

In der Tabelle „Fibre Channel-Port“ [cmdb_ci_fc_port] füllt Discovery die folgenden Felder.

Bezeichnung	Feldname
Name	Name
Computer	Computer
Controller	controller
WWPN	wwpn
WWNN	wwnn
Porttyp	port_type
Geschwindigkeit	speed
Betriebsstatus	operational_status

In der Tabelle „Fibre Channel-Datenträger“ [cmdb_ci_fc_disk] füllt Discovery die folgenden Felder.

Bezeichnung	Name
Name	Name
Speichertyp	storage_type
Geräteschnittstelle	device_interface
Geräte-LUN	device_lun

In der Tabelle „Fibre Channel-Ziele“ [cmdb_ci_fc_port] füllt Discovery die folgenden Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Name
FC-Datenträger	fc_disk
WWNN	wwnn
WWPN	wwpn

Für HBAs auf Windows-Servern erfasste Daten

Unter Windows unterstützt Discovery unter beliebigen Betriebssystemen ausgeführte HBAs.

HBA-Tabellen und -Felder

Bezeichnung	Tabelle	Feldname	Quelle
Name	Speicher-HBA [cmdb_ci_storage_hba]	Name	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
WWNN	Speicher-HBA [cmdb_ci_storage_hba]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Modell-ID	Speicher-HBA [cmdb_ci_storage_hba]	model_id	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Computer	Speicher-HBA [cmdb_ci_storage_hba]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

Fibre Channel-Ports

Bezeichnung	Tabelle	Feldname	Quelle
WWPN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwpn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre Channel-Ports (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
WWNN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Porttyp	Fibre-Channel-Port [cmdb_ci_fc_port]	port_type	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Geschwindigkeit	Fibre-Channel-Port [cmdb_ci_fc_port]	speed	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Controller	Fibre-Channel-Port [cmdb_ci_fc_port]	controller	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Computer	Fibre-Channel-Port [cmdb_ci_fc_port]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

Speichererkennung über SMI-S und CIM

Discovery kann Speichergeräte untersuchen, die einen SMI-S Provider (Storage Management Initiative Specification), einen speziellen CIM-Server (Common Information Model), enthalten.

Die aktuelle Liste der Lieferanten und Produkte, die von SNIA auf SMI-S-Konformität getestet wurden, finden Sie auf der SNIA-Website .

Für andere Speichertypen, zum Beispiel über einen Host angeschlossenen Speicher, auf VMware ESX-Servern verfügbaren VM-Speicher und Speicher für Kernel-VM (KVM), werden separate Probes und Sensoren verwendet.

Discovery erfasst Informationen über SAN (Storage Area Network) und NAS (Network Attached Storage) von spezialisierten Geräten wie Speicher-Arrays und FC-Switches (Fibre Channel). Discovery erfasst und erstellt CIs in der CMDB für die folgenden Informationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Array-Datenträger, Pools und Volumes
- Fibre Channel-HBAs, -Ports und -Controller
- FC-Exporte
- Fabrics, einschließlich Endpunkte, Zoning und Switches
- Abhängigkeiten zwischen untergeordneten Speicherkomponenten

Hinweis: Weitere Informationen zur Speichererkennung und zur Verwendung des Abfragetools CIM zur Problembehandlung können Sie Wissensartikel KB0782305 entnehmen.

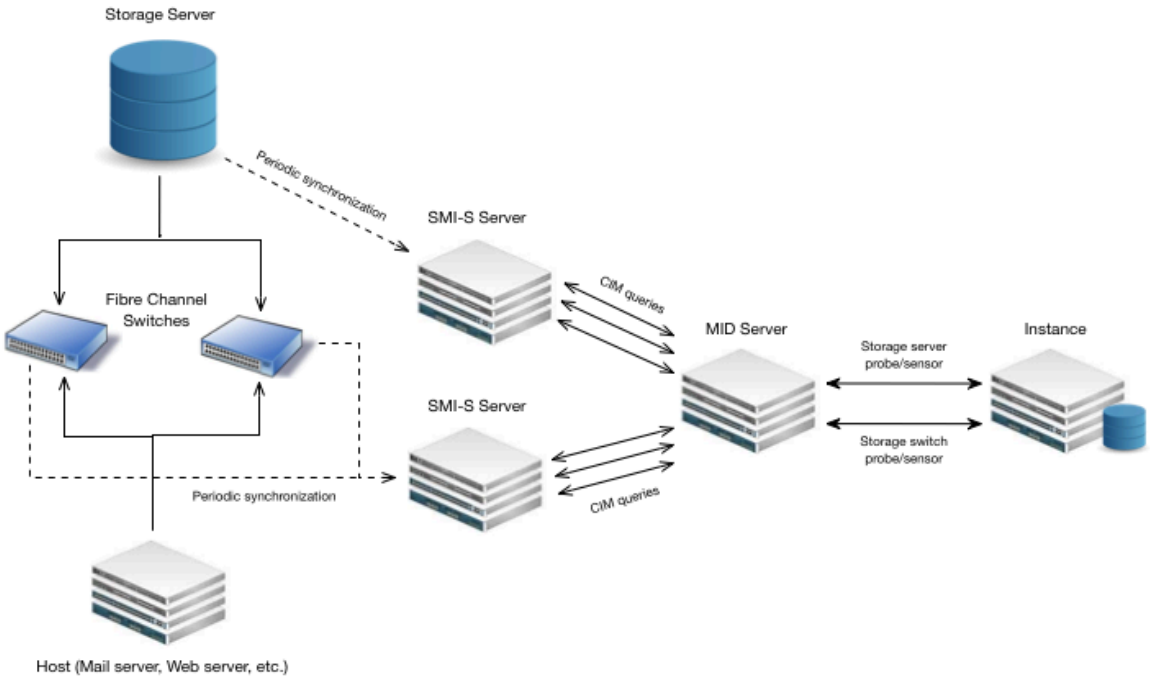
Anforderungen

- Ein CIM-Server mit SMI-S 1.4 oder höher
- Mindestens ein CIM-Server pro Speicheranbieter
- NAS- und SAN-Systeme wichtiger Lieferanten wie EMC, Hitachi, HP und NetApp. SAN-Speichergeräte müssen FC verwenden.
- FC-Switches großer Anbieter wie Brocade und Cisco
- Die CIM-Anmeldeinformationen Muss für die SMI-S-Konfiguration verfügbar sein. Die CIM-Anmeldeinformationen können sich von den Anmeldeinformationen für das System unterscheiden, auf dem der CIM-Server gehostet wird.
- Stellen Sie sicher, dass SMI-S für Ihr Speicherprodukt aktiviert ist.
- Stellen Sie sicher, dass eine Verbindung zwischen dem MID Server und dem CIM-Server besteht.
- Neue CIM-Anmeldeinformationen müssen in der Instanz konfiguriert werden. Die Anmeldeinformationen für den CIM-Server können von denen für das System abweichen, auf dem der erforderliche CIM-Server gehostet wird.

Hinweis: Da der SMI-S Provider Informationen über Speichergeräte zwischenspeichert, hat die Discovery-Abfrage an den Provider keine Auswirkungen auf die Leistung der Speichergeräte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMI-S Discovery-Architektur



CIM-Architektur

CIM-Probes können jedes Gerät basierend auf dem Common Information Model (CIM) erkennen, indem sie einen CIM-Server abfragen, der auch als CIMOM (Common Information Model Object Manager) bezeichnet wird. Standardmäßig verwendet Discovery CIM-Probes zum Untersuchen von Speichersystemen sowie zum Abrufen der Seriennummern von ESX-Servern.

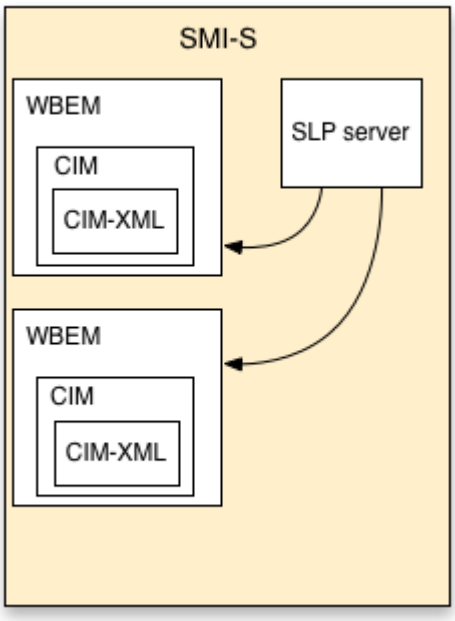
Discovery fragt SMI-S-konforme Speichergeräte mithilfe von CIMIQL-Abfragen ab.

Die folgenden Komponenten sind Teil von CIM:

- Common Information Model (CIM): Mit CIM können mehrere Parteien Informationen über verwaltete Elemente austauschen. CIM stellt diese verwalteten Elemente und die Verwaltungsinformationen dar und stellt gleichzeitig den Mechanismus zur aktiven Steuerung und Verwaltung der Elemente bereit.
- Storage Management Initiative Specification (SMI-S): SMI-S ist ein Nutzungsstandard, der Methoden für die Speichererkennung auf Anbieterseite beschreibt. ServiceNow verwendet SMI-S, um zu bestimmen, wie CIM erkannt wird. SMI-S basiert auf den Standards Common Information Model (CIM) und Web-Based Enterprise Management (WBEM), die Verwaltungsfunktionen über HTTP definieren. Das Hauptziel von SMI-S besteht darin, die Verwaltung unterschiedlicher Speicherprodukte zu ermöglichen. ServiceNow unterstützt SMI-S Version 1.4 oder höher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIM SMI-S-Standard – Diagramm



- Web-Based Enterprise Management (WBEM): WBEM definiert eine bestimmte Implementierung von CIM, einschließlich Protokollen zum Erkennen und Zugreifen auf CIM-Implementierungen.
- Service Location Protocol (SLP): SLP ist ein Ad-hoc-Protokoll zum Abrufen und Zuordnen von Konfigurationsinformationen über CIM-Server, zum Beispiel Standardpfade, Fähigkeiten und der genaue Interop-Namespace. Discovery ruft den Interop-Namespace von CIM-Servern über SLP ab und übergibt diese Informationen an die Probe „CIM Classify“. SLP, hier als SLP-Server bezeichnet, verwendet Service Agents (SA), um Informationen zu einem CIM-Server in einem Subnetz zu sammeln und zu verbreiten. Ein Subnetz kann über mehrere Service Agents verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

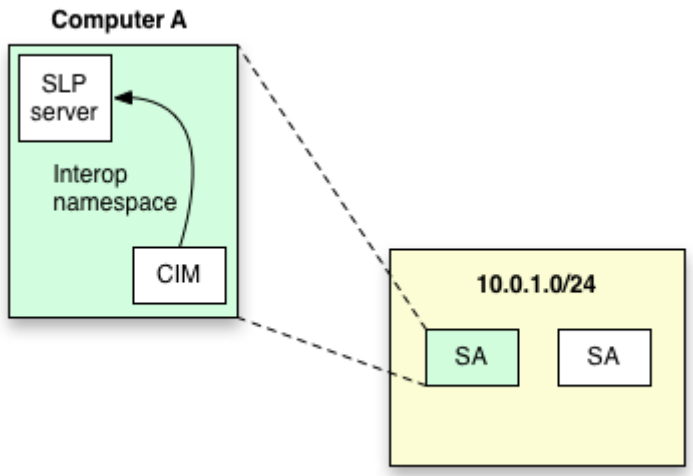
Hinweis:

Die Systemeigenschaft `mid.cim.interop.namespace` vier Standardspeicher-Namespaces:

- interop
- root/interop
- root/pg_interop
- pg_interop

Wenn Sie mehrere Speicheranbieter mit anwenderdefinierten Namespaces verwenden, die nicht als Standard angegeben sind, fügen Sie die neuen Namespaces der kommagetrennten Liste in dieser Eigenschaft hinzu. Wenn Sie einen der Standard-Namespaces weiterhin verwenden möchten, müssen Sie diese in die Eigenschaft aufnehmen.

CIM-Agent – Diagramm



SLP- und WBEM-Unterstützung

SLP ist für CIM Discovery erforderlich, da es Teil des SMI-S-Stapels (Storage Management Initiative Specification) ist. Einige Speichergeräte unterstützen womöglich das WBEM-Protokoll, aber SLP nicht.

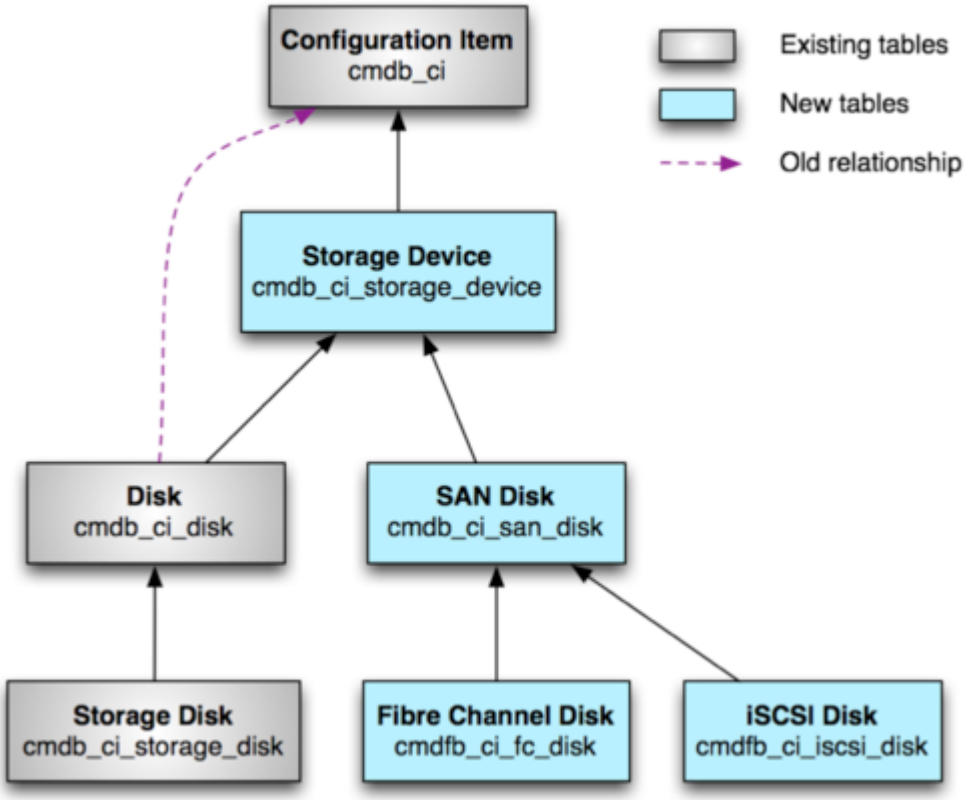
Sie können die WBEM-Services mit einem gängigen Linux-Tool wie `slptool` manuell für SLP registrieren. Dieses Tool stellt eine Befehlszeilenschnittstelle bereit, mit der Sie SLPv2-UA-Anforderungen (User Agent) erstellen können, die normalerweise zum Lieferumfang des SLP-Daemon-Pakets gehören. Zum Registrieren eines Service geben Sie eine URL und eine Liste von Attributen an. Beispiele können mit demselben Tool von einem funktionierenden SLP-Server extrahiert werden.

Tabellenschema für Speichererkennung

In folgendem Diagramm ist das hierarchische Datenträgerschema für die Speichererkennung dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hierarchisches Datenträgerschema



Tabellen und Probes zur Speichererkennung

Discovery verwendet die folgenden Tabellen und Probes, um Informationen über Speichergeräte zu erfassen, die von einem SMI-S Provider verwaltet werden.

Erfasste Daten

Tabelle	Probe
Datenträger [cmdb_ci_disk]	SMI 1.5 - Storage Server
Fibre Channel-Export [cmdb_ci_fc_export]	SMI 1.5 - Storage Server
Fibre-Channel-Port [cmdb_ci_fc_port]	SMI 1.5 - Storage Server
SAN-Export [cmdb_ci_san_export]	SMI 1.5 - Storage Server
Speichercontroller [cmdb_ci_storage_controller]	SMI 1.5 - Storage Server
Speicherexport [cmdb_ci_storage_export]	SMI 1.5 - Storage Server
Speicherdateifreigabe [cmdb_ci_storage_fileshare]	SMI - Array - File Shares
Speicherpool [cmdb_ci_storage_pool]	SMI 1.5 - Storage Server
Speicherserver [cmdb_ci_storage_server]	CIM - Identity
Speicher-Switch [cmdb_ci_storage_switch]	CIM - Identity
Speichervolume [cmdb_ci_storage_volume]	SMI 1.5 - Storage Server
Speichergerät [cmdb_ci_storage_device]	SMI 1.5 - Storage Server
Storage Area Network [cmdb_ci_san]	SMI - Fabric

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Daten (Fortsetzung)

Tabelle	Probe
SAN-Verbindung [cmdb_ci_san_connection]	SMI - Fabric
SAN-Endpunkt [cmdb_ci_san_endpoint]	SMI - Fabric
SAN-Fabric [cmdb_ci_san_fabric]	SMI - Fabric
SAN-Zone [cmdb_ci_san_zone]	SMI - Fabric
SAN-Zonenalias [cmdb_ci_san_zone_alias]	SMI - Fabric
SAN-Zonenaliasmitglied [cmdb_ci_san_zone_alias_member]	SMI - Fabric
SAN-Zonenmitglied [cmdb_ci_san_zone_member]	SMI - Fabric
SAN-Zonensatz [cmdb_ci_san_zone_set]	SMI - Fabric

Die folgenden Probes sind verfügbar, werden aber derzeit nicht verwendet:

- SMI - Storage Server
- SMI - Array - Controllers
- SMI - Array - Disks
- SMI - Array - Pools
- SMI - Array - Ports
- SMI - Array - Volumes

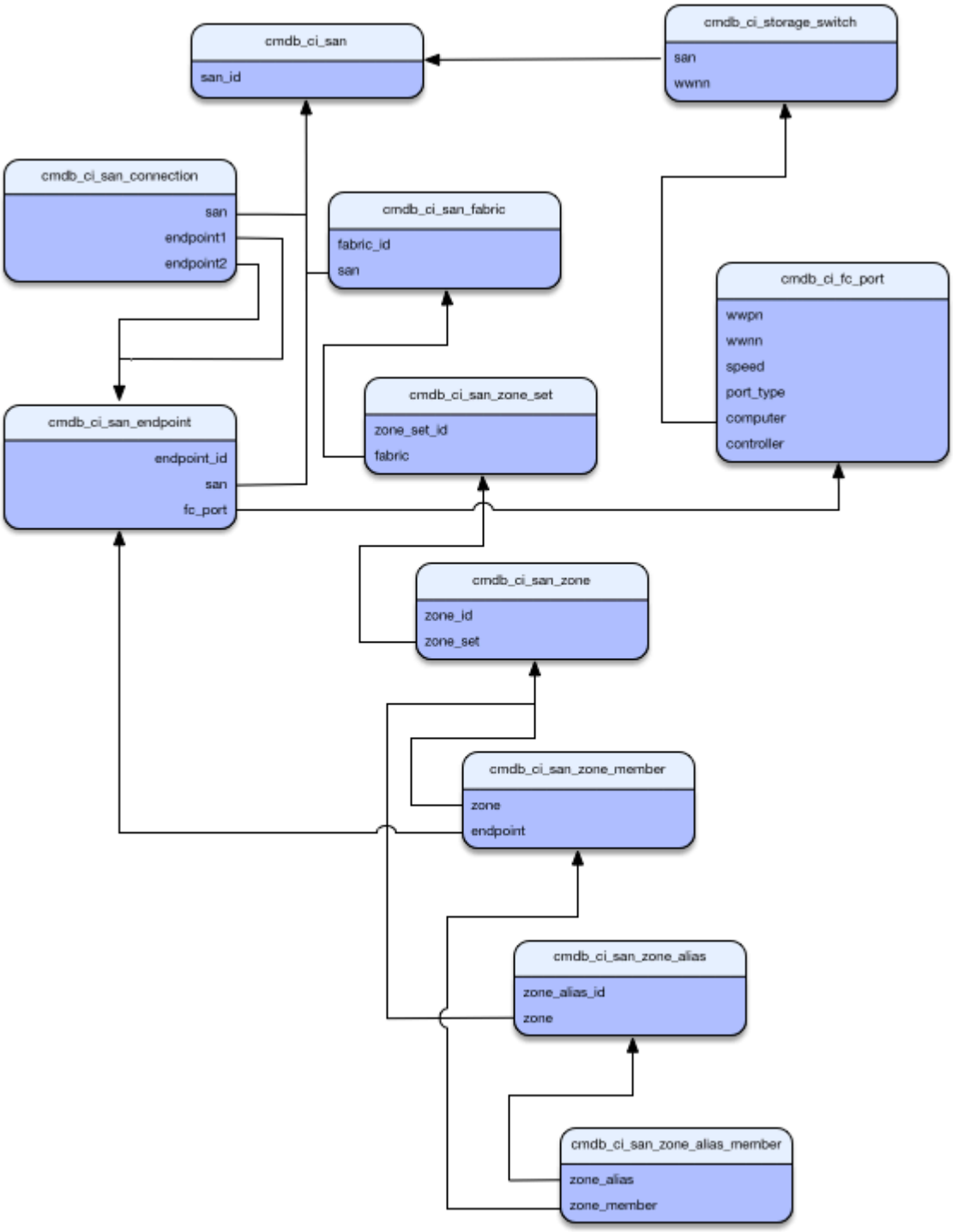
Erkennung von Storage Area Networks (SAN)

Discovery erfasst Informationen über Speichernetzwerke von spezialisierten Geräten wie Speicher-Arrays und Fibre Channel Switches (FC-Switches) und erzeugt bestimmte Referenzen zwischen den Tabellen im SAN-Schema.

SAN-Schema von ServiceNow

Im folgenden Diagramm sind die Tabellen im SAN-Schema und die zwischen ihnen definierten Standardreferenzen dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

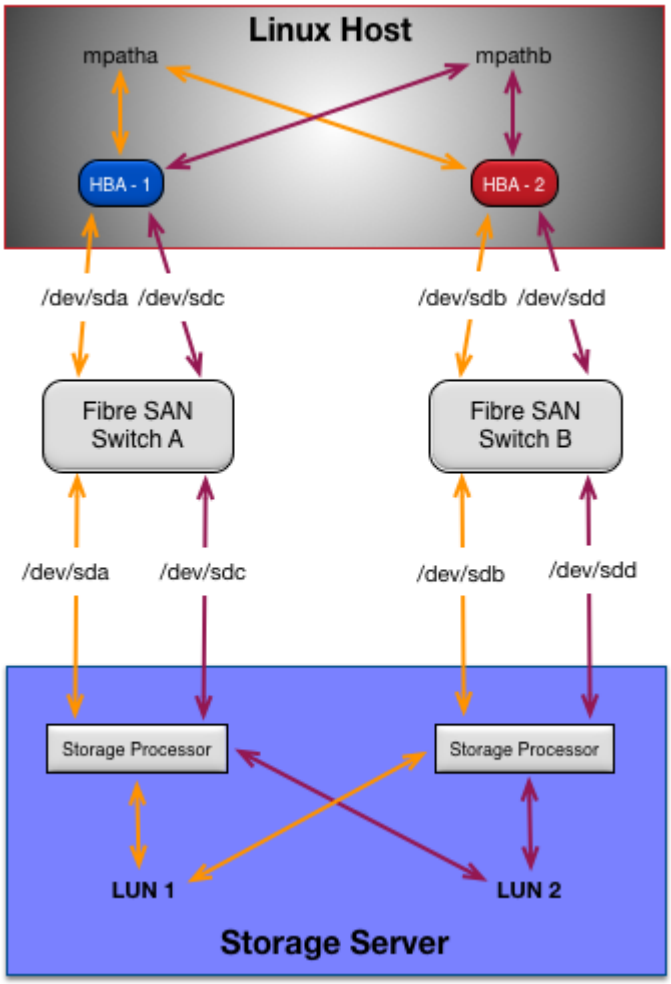


Automatische Übersetzung

Beispiel für Multipfad-SAN-Speicher

In diesem Diagramm ist die Beziehung von SAN-Speichervolumes zu einem Hostcomputer dargestellt. Der Speicher, auf den der Linux-Host zugreifen kann, besteht aus zwei physischen Fibre Channel-Datenträgern (mpatha und mpathb), die über ein Multipfad-FC-SAN mit dem Host verbunden sind. Die beiden HBAs auf der Hostschnittstelle sind mit jeweils zwei Glasfaserkabeln verbunden, um FC-Switches für die Failover-Funktionalität zu trennen. Die FC-Fabric Switches sind mit zwei FC-Speicherprozessoren auf dem Speicherserver verbunden. In folgendem Beispiel sind alle Speicherprozessoren mit den Speichervolumes **LUN 1** und **LUN 2** verbunden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Funktionsweise der CIM-Erkennung

Im folgenden ist der Verarbeitungsablauf für die Klassifizierung von CIM-Speichersystemen (Common Information Model) dargestellt.

Verarbeitungsablauf

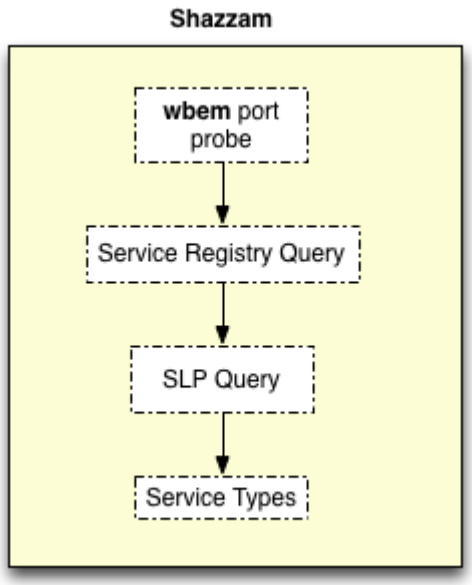
1. Die Shazzam-Probe startet die Port-Probe „wbem“ als Teil der Netzwerkerkennung.
2. Die wbem-Portprobe erkennt Aktivitäten an den Zielports SLP 427, CIM 5989 und 5988 und untersucht dann den **Serviceregistrierungsabfragen** Zugehörige Liste, um **Discovery-Definition** > **Anschlussprobes**, Für die SLP-Abfrage. Das Basissystem stellt diese Abfrage zur Erkennung des Servicetyps „service:wbem“ bereit, der das Vorhandensein eines SLP-Servers anzeigt.
3. Die Shazzam-Probe startet einen Scanner für den WBEM-Servicetyp. Der Scanner ruft Folgendes ab:
   - Die Attribute des Service vom SLP-Server
   - Die interop-Namespaces der CIM-Server im Netzwerk
4. Der Scanner hängt die gefundenen Namespace-Werte an die Ergebnisse der Port-Probe an.
5. Die Port-Probe „wbem“ hängt die enthaltenen SLP-Daten an die Probes vom Typ „CIM - Classify“ an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Die Probe „CIM Classify“ verwendet diese Informationen, um die CIM-Server zu untersuchen.

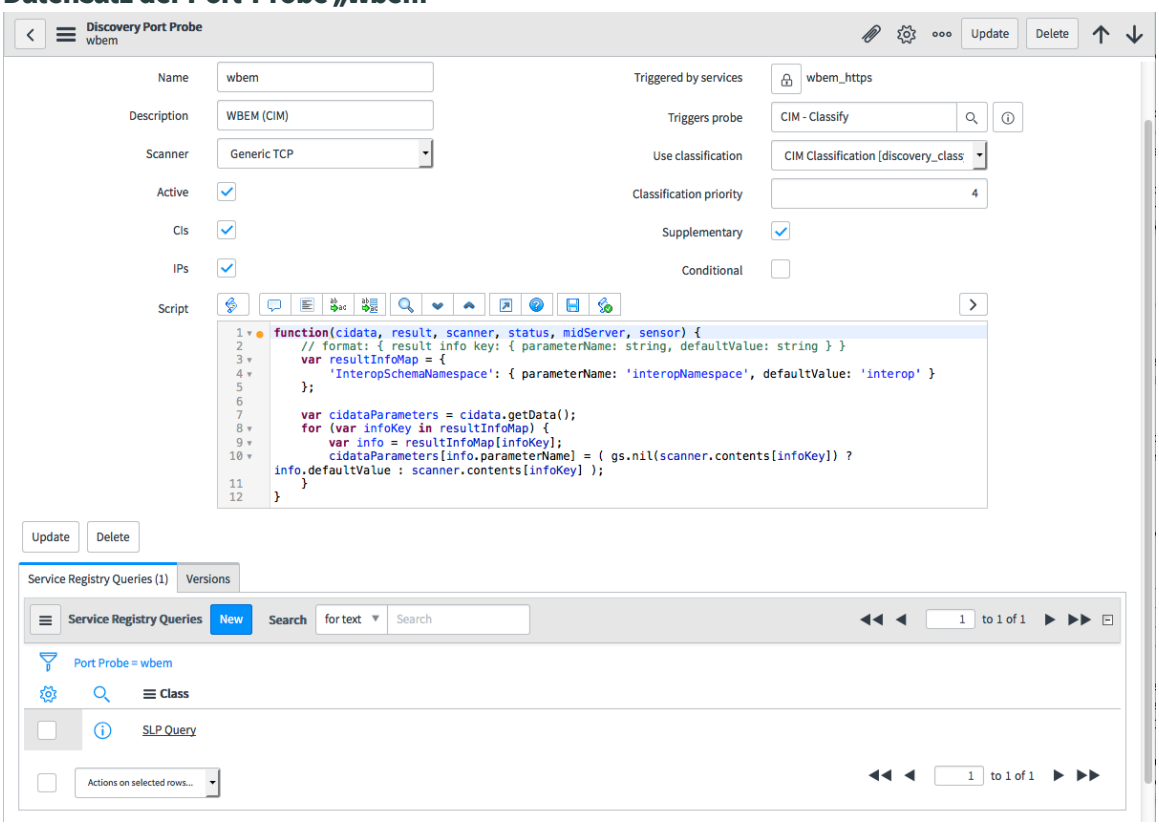
CIM-Shazzam-Verarbeitungsdiagramm



Port-Probe „wbem“

Die Probe **wbem** speichert die abgerufenen Daten in der Tabelle „CIM-Klassifizierung“ [discovery_classy_cim]. Um die wbem-Port-Probe anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Anschlussprobes**an.

Datensatz der Port-Probe „wbem“



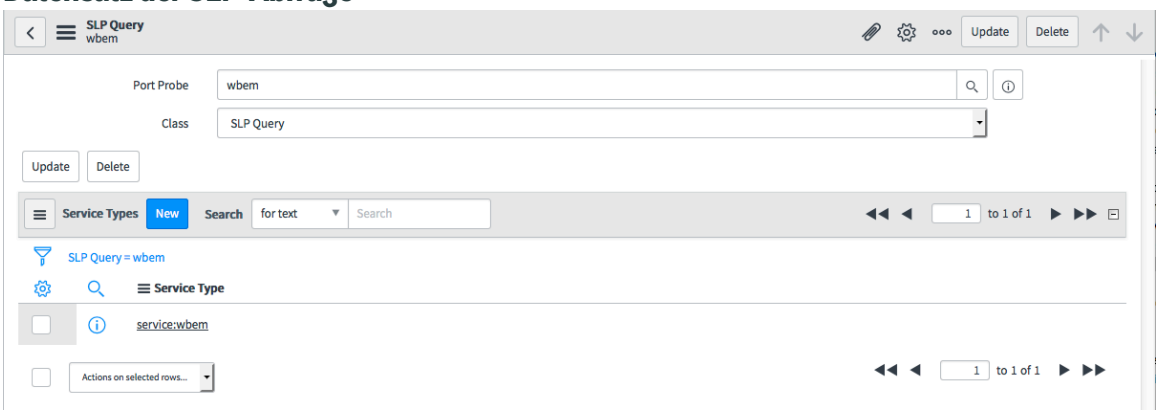
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLP-Abfrage

Die SLP-Abfrage erkennt den Service wbem (service:wbem) auf einem SLP-Server und erfasst seine Attribute. Öffnen Sie zum Anzeigen des SLP-Abfragedatensatzes den Datensatz der Port-Probe „wbem“, und wählen Sie **SLP-Abfrage** in der zugehörigen Liste **Service- Registry-Abfragen** aus.

Datensatz der SLP-Abfrage



Probe „CIM - Classify“

Die Port-Probe „wbem“ hängt die enthaltenen SLP-Daten einschließlich Namespaces an der Probe „CIM - Classify“ an, bevor er diesen startet. Die CIM-Klassifizierungs-Probe extrahiert VMware ESX-Seriennummern und Connector-Beziehungen zwischen den SAN- und NAS-Komponenten von CIM-Servern im Netzwerk.

Um auf die CIM-Klassifizierungsprobe zuzugreifen, navigieren Sie zu **Discovery-Definition** > **Probes** Und wählen Sie aus **CIM: Klassifizieren** Aus der Liste der Probes.

Hinweis:

Die Systemeigenschaft `mid.cim.interop.namespace` vier Standardspeicher-Namespaces:

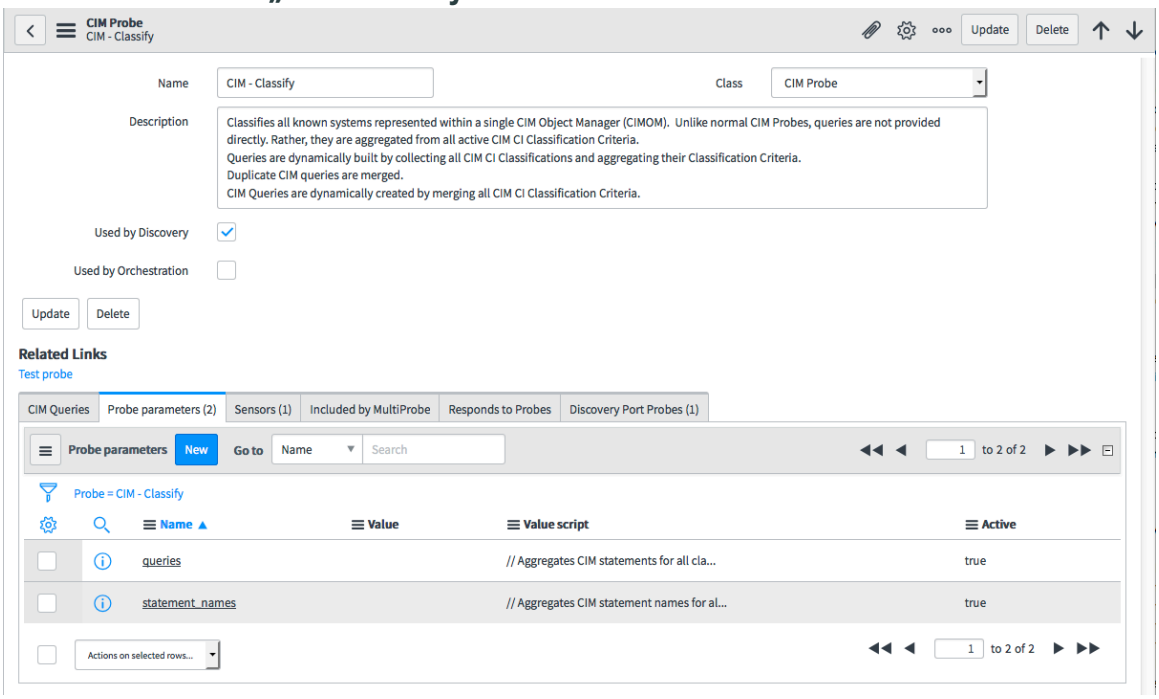
- interop
- root/interop
- root/pg_interop
- pg_interop

Wenn Sie mehrere Speicheranbieter mit anwenderdefinierten Namespaces verwenden, die nicht als Standard angegeben sind, fügen Sie die neuen Namespaces der kommagetrennten Liste in dieser Eigenschaft hinzu. Wenn Sie einen der Standard-Namespaces weiterhin verwenden möchten, müssen Sie diese in die Eigenschaft aufnehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatz der Probe „CIM - Classify“



SMI-S- und CIM-Probes und -Sensoren

SMI-S- und CIM-Probes und -Sensoren

Probe/Sensor	Beschreibung
CIM - Identity	Identifiziert ein System über CIM mithilfe von SMI-S
SMI - Array - Controllers	Ruft Controller-Informationen ab
SMI - Array - Disks	Ruft Informationen zum Speicherdatenträger ab
SMI - Array - File Shares	Listet NAS-Dateifreigaben von einem Speicherserver auf
SMI - Array - Pools	Ruft Speicherpools ab
SMI - Array - Ports	Ruft Speicherports ab
SMI - Array - Volumes	Ruft Speichervolumes ab
SMI - Fabric	Ruft SANs, Fabrics, Zonensätze, Zonen, Zonenaliase, Endpunkte und Verbindungen ab
SMI - Fibre Channel Switch	Ruft FC-Switches ab
SMI - NAS Head - Component Systems	Ruft alle virtuellen Dateiserver in einem NAS-Head-Profil ab
SMI - NAS Head - File Server IPs	Ruft IP-Adressen für jeden NAS-Dateiserver ab
SMI - NAS Head - File Servers	Ruft NAS-Dateiserver wie Common Internet File System (CIFS) und Network File System (NFS) ab
SMI - NAS Head - File Shares	Ruft Dateifreigaben für jeden NAS-Dateiserver ab
SMI - Storage Server	Ruft SAN- und NAS-Arrays und -Server ab
SMI - WBEM Service	Ruft Informationen zum WBEM-Service wie Profile und die SMI-S-Version ab

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SMI-S Provider zur Speichererkennung konfigurieren

Verwenden Sie dieses Verfahren zum Konfigurieren eines eigenständigen Speichergeräts mit dem erforderlichen SMI-S Provider für Discovery.

Vorbereitungen

Erforderliche Rolle: Administrator

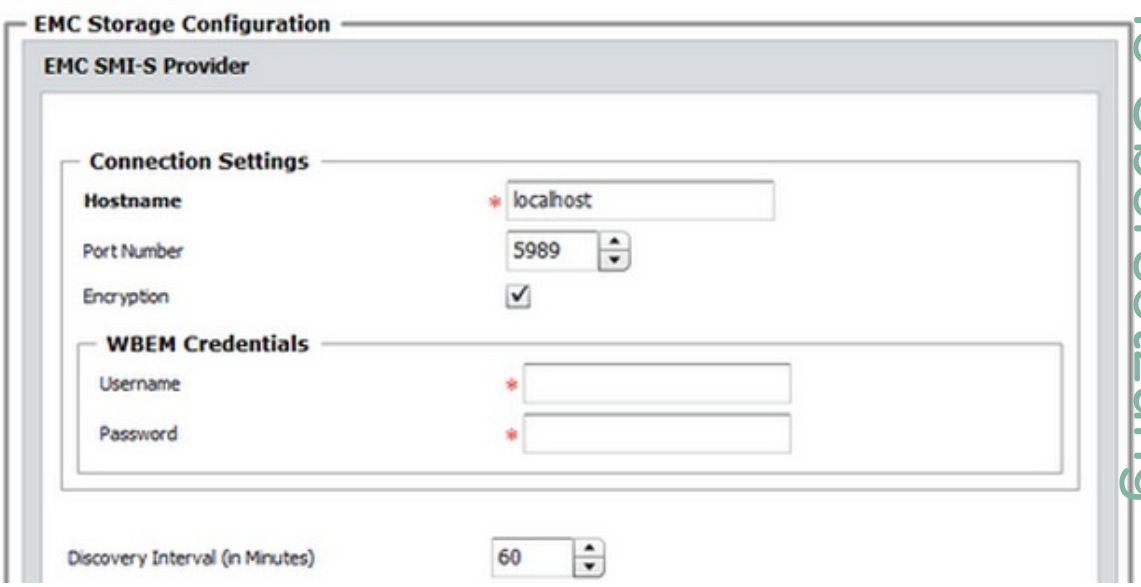
Prozedur

1. Wenn der SMI-S Provider auf dem Speichergerät nicht vorhanden ist, installieren Sie die SMI-S Provider-Software.
   Die SMI-S Provider-Software ist häufig Teil der Geräteverwaltungssoftware. Um weitere Informationen zu erhalten, laden Sie sich für die Anweisungen zum SMI-S Provider von der Website des Speicheranbieters herunter.
2. Für NetApp Speichergeräte, Installieren Sie den SMI-S-Agent Auf dem Speichergerät-Host.

   Hinweis: Discovery kann auch eine native Discovery von durchführen NetApp Server ohne Zugriff auf den SMI-S-Server. Weitere Informationen finden Sie unter NetApp Server und Cluster Discovery.

3. Starten Sie den SMI-S Provider-Service.
4. Konfigurieren Sie im SMI-S Provider oder Agent das **Discovery-Intervall** mit einer Synchronisierungsrate, die es der Probe „wbem“ ermöglicht, während der Erkennung die aktuellen Informationen zu empfangen. Legen Sie beispielsweise das **Discovery-Intervall** für Speicher von EMC fest.

   Beispiel für den Anbieter EMC

5. Richten Sie in der ServiceNow-Instanz ein CIM-Anmeldeinformationen .
6. Erstellen Sie einen Erkennungszeitplan mit den IP-Adressen der einzelnen SMI-S Provider.
7. **Wahlweise:** Erstellen Sie einen Discovery-Verhalten Die eine Funktionsdefinition mit verwendet *wbem*Port-Probe, um die anfängliche Port-Scan-Phase (Shazzam) effizienter zu gestalten.
8. Führen Sie eine einfache Discovery für IP-Adressen aus.

Von Discovery auf Speichergeräten erfasste Daten

Discovery identifiziert und klassifiziert Informationen über Speichergeräte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Tabelle „Speicherdatenträger“ [cmdb_ci_Storage_Disk] erkannte Ressourcen

Feld	Beschreibung
Name	Name des Speicherdatenträgers
Computer	Verweis auf das Host-CI.
Schnittstelle	Schnittstellentyp, mit dem der Speicherdatenträger mit dem Host verbunden ist.
Größe	Größe des Speicherdatenträgers.
Freier Speicherplatz (GB)	Freier Speicherplatz in GV, der auf dem Datenträger verfügbar ist.
Hersteller	Hersteller des Speicherdatenträgers.
Modell-ID	Modellname des Datenträgers.

Ressourcen, die in der Tabelle „Speicherdateifreigaben“ [cmdb_ci_Storage_fileshare] erkannt wurden

Feld	Beschreibung
Name	Name des CI.
Pfad	Pfad zur Dateifreigabe.

In der Tabelle „Speicherpools“ [cmdb_ci_Storage_Pool] erkannte Ressourcen

Feld	Beschreibung
Name	Name des Speicherpools.
Größe	Größe des Speicherpools.
Freier Speicherplatz	Freier Speicherplatz im Pool.
Gehosted von	Verweis auf das CMDB-CI.

In der Tabelle „Speicherports“ [cmdb_ci_Storage_Port] erkannte Ressourcen

Feld	Beschreibung
Name	Name des Speicherports.
WWPN	Eindeutiger Worldwide Port Name (WWPN) für den Speicherport.
Geschwindigkeit	Geschwindigkeit des Speicherports.

In der Tabelle „Speicher-HBAs“ [cmdb_ci_Storage_hba] erkannte Ressourcen

Feld	Beschreibung
Name	Name des Speicher-Host-Bus-Adapters (HBA).
Modell-ID	Modellname des HBA.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Tabelle „Speicher-HBAs“ [cmdb_ci_Storage_hba] erkannte Ressourcen (Fortsetzung)

Feld	Beschreibung
Computer	Verweis auf das Computer-CI.

In der Tabelle „Speicherserver“ [cmdb_ci_Storage_Server] erkannte Ressourcen

Feld	Beschreibung
Name	Name des CI.
Hersteller	Hersteller des Speicherservers.
Modell-ID	Modellname des Speicherservers.
Betriebssystem	Betriebssystem (OS) des Speicherservers.
BS-Version	BS-Version des Speicherservers.
Beschreibung	Kurzbeschreibung des Speicherservers.

In der Tabelle „Speichervolumes“ [cmdb_ci_Storage_Volume] erkannte Ressourcen

Feld	Beschreibung
Name	Name des Speichervolumes.
Objekt-ID	Eindeutige ID für das Speichervolume.
Status	Status des Speichervolumes.
Größe	Größe des Speichervolumes.
Speichertyp	Typ des Speichervolumes.

Speicherbeziehungen

Discovery stellt die richtigen Beziehungen zwischen NAS-Speichergeräten (Network Attached Storage) und remote bereitgestellten Client-Servern her, die den Speicher verbrauchen. Discovery ordnet NAS-Dateifreigaben zu. Die Zuordnung erfolgt anhand der IP oder des Hostnamens eines remote bereitgestellten Datenträgers auf dem Clientcomputer. Anschließend wird sie mit der IP oder dem Hostnamen des Speicherservers abgeglichen, der das exportierte Dateisystem bereitstellt.

Discovery erstellt die folgenden Beziehungen für Speicher-CIs, die in Speicherbereichsnetzwerken ausgeführt werden.

SAN-CI-Beziehungen

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
Speichervolume [cmdb_ci_storage_volume]	Exportieren nach::Importieren von	Fibre Channel-Datenträger [cmdb_ci_fc_disk]
Speichervolume [cmdb_ci_storage_volume]	Exportieren nach::Importieren von	iSCSI [cmdb_ci_iscsi_disk]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery ordnet NAS-Dateifreigaben zu. Die Zuordnung zu einer IP-Adresse erfolgt durch Auflösung des Hostnamens eines remote bereitgestellten Datenträgers auf dem Clientcomputer. Anschließend wird sie mit der IP-Adresse des Speicherservers abgeglichen, der das exportierte Dateisystem bereitstellt. Discovery extrahiert den Hostnamen oder die IP-Adresse aus dem NAS-Pfad, um die Identität des Speicherservers zu bestimmen. Wenn der Hostname ein tatsächlicher Hostname ist, löst das System diesen Wert sofort in eine IP-Adresse auf. Außerdem wird sie im Feld **nas_ip_address** der Tabelle „NAS-Dateisystem“ [cmdb_ci_nas_file_system] gespeichert.

Discovery erstellt die folgenden Beziehungen für Speicher-CIs, die in Network Attached Storage (NAS) ausgeführt werden. Diese Beziehungen sind für Linux- und Windows-Betriebssystemhosts identisch.

NAS-CI-Beziehungen

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
NAS-Dateisystem [cmdb_ci_nas_file_system]	Zugeordnet von::Zugeordnet zu	Speicherdateifreigabe [cmdb_ci_storage_fileshare]

Daten erfasst für Veritas Volume-Manager auf Linux

Discovery erfasst Datenträger- und Volume-Informationen für Veritas Volume Manager (VxVM) auf Linux Auf gemountete Dateisysteme für Hosts und Zuordnungen Veritas Volumes an den vorgelagerten Speicheranbieter.

Hinweis: Stellen Sie sicher, dass VxVM ordnungsgemäß installiert und konfiguriert ist. Wenn Sie Treiber von Drittanbietern verwenden, müssen Sie die sudo-Berechtigung für `vxdmpadm` konfigurieren.

Tabellenschema

VxVM-Tabellen

Tabelle	Erweitert Tabelle
Veritas-Datenträger [cmdb_ci_veritas_disk]	Speicherpool [cmdb_ci_storage_pool]
Veritas-Datenträgergruppe [cmdb_ci_veritas_disk_group]	Konfigurationselement [cmdb_ci]
Veritas-Plex [cmdb_ci_veritas_plex]	Speicherpool [cmdb_ci_storage_pool]
Veritas-Teildatenträger [cmdb_ci_veritas_subdisk]	Speicherpoolmitglied [cmdb_ci_storage_pool_member]
Veritas-Laufwerk [cmdb_ci_veritas_volume]	Speicherpool [cmdb_ci_storage_pool]

Erfasste Daten

Erfasste VxVM-Daten

Tabelle	Felder	Beziehung
Veritas-Datenträger [cmdb_ci_veritas_disk]	• Name • size_bytes • disk_group	Beziehung vom Typ „Bereitgestellt von::Stellt bereit“ zum physischen Datenträger

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste VxVM-Daten (Fortsetzung)

Tabelle	Felder	Beziehung
Veritas-Datenträgergruppe [cmdb_ci_veritas_disk_group]	Name	Beziehung vom Typ „Enthält::Enthalten in“ zu Veritas-Datenträgern in der Gruppe
Veritas-Plex [cmdb_ci_veritas_plex]	• Name • size_bytes • layout (CONCAT, STRIPE, RAID)	
Veritas-Teildatenträger [cmdb_ci_veritas_subdisk]	• partition_number • source_start_offset: Offset auf dem Datenträger, von dem dieser Teildatenträger partitioniert ist • source_end_offset: Offset auf dem Datenträger, von dem dieser Teildatenträger partitioniert ist • start_offset: Offset dieses Teildatenträgers im Plex, der ihn verwendet • end_offset: Offset dieses Teildatenträgers im Plex, der ihn verwendet • size_bytes	
Veritas-Laufwerk [cmdb_ci_veritas_volume]	Name	Beziehung vom Typ „Gespeichert auf::Stellt Speicher bereit für“ zu Veritas-Datenträgern, auf denen das Volume gespeichert ist

Daten anzeigen

VxVM Discovery ordnet Dateisysteme den Datenträgern zu, die Speicher bereitstellen. Standardmäßig handelt es sich dabei um die einzigen Informationen, die in der Benutzeroberfläche angezeigt werden. Die Beziehung zwischen Dateisystem und Datenträger wird im Formular „Dateisystem“ als vorgelagerte Beziehung vom Typ **Gespeichert auf** angezeigt. Zum Anzeigen der restlichen Informationen, die Discovery für VxVM erfasst, müssen Sie dem Formular „Linux-Server“ die entsprechende zugehörige Liste hinzufügen. Folgende Listen sind verfügbar:

- Veritas Disk Group
- Veritas-Laufwerk
- Veritas-Plex
- Veritas Subdisk (Computer)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Veritas Subdisk (Speicher)
- Veritas-Laufwerk

NetApp Server und Cluster Discovery

Discovery Und Service-MappingSuchen NetApp Server und Cluster, die beide verwenden CIM Probes Oder-Muster. Um einige dieser Ressourcen zu erkennen, muss aktualisiert werden Muster für Discovery und Service-Mapping Anwendung aus dem ServiceNow Store.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie ServiceNow Store Um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Informationen zu kumulativen Release-Hinweisen für alle veröffentlichten Apps finden Sie unter ServiceNow Store Release-Hinweise zum Versionsverlauf an.

NetApp Discovery wird für nicht unterstützt NetApp-Server in AWS Cloud. Um mehr über die Komponenten und Versionen von zu erfahren NetApp Server und Cluster, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

NetApp Server- und Cluster-Discovery-Methoden

Methode	Unterstützte Modi	Upgrades
Erkennung mit Mustern mithilfe der ONTAP-API. Diese Muster unterstützen die native Discovery von NetApp Server, ohne dass die Discovery des SMI-S-Servers erforderlich ist.	• NetApp 7-Modus • NetApp Clustermodus	Standardmäßig aktiviert.
Discovery mit Mustern mithilfe der HTTP-REST-API.	NetApp Clustermodus	Verfügbar am Muster für Discovery und Service-Mapping Speichern Anwendung Ab August 2023.
Erkennung mit Probes und Sensoren mit SMI-S	• NetApp 7-Modus • NetApp Clustermodus	Legacy

NetApp Discovery-Eigenschaften

Um Discovery mit Mustern zu verwenden, navigieren Sie zu **Discovery-Definition** > **Eigenschaften** Und aktivieren Sie diese Eigenschaften:

Eigenschaftsbezeichnung	Name
Für 7-Modus NetApp Speicherserver verwenden native Discovery anstelle von SMI-S.	glide.discovery.sensors.netapp_native_7mode

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsbezeichnung	Name
Für Clustermodus NetApp Speicherserver verwenden native Discovery anstelle von SMI-S.	glide.discovery.sensors.netapp_native_cluster_mode

Hinweis: Wenn Sie bereits durchgeführt haben NetApp Discovery mit Probes und aktivieren Sie dann diese Eigenschaften. Bei der nächsten Ausführung wird ein Migrationsskript ausgeführt NetApp Discovery. Dieses Skript kann CIs für Elemente wie Speicherpools löschen, die von Probes, aber nicht von Mustern erkannt werden. Es werden auch Beziehungen erstellt.

Voraussetzungen

Allgemeine Voraussetzungen

Überprüfen Sie, ob die Anwendungen aktuell sind:

- Muster für Discovery und Service-Mapping
- Visibility Content

Deaktivieren Sie SSLv3, und aktivieren Sie TLS für das Ziel NetApp Server, als Java Runtime, die von verwendet wird MID-Server Aktiviert SSLv3 standardmäßig nicht. Der Schlüssel zum Verschlüsseln des Zertifikats muss mindestens 1024 Bit aufweisen.

SNMP-basierte Discovery-Voraussetzungen

Konfigurieren Sie SNMP-Community-Anmeldeinformationen, um zu klassifizieren NetApp Server. Weitere Informationen finden Sie unter SNMP-Community-Anmeldeinformationen .

Aktivieren **Schreibgeschützt** Zugriff auf die ONTAP-API auf der NetApp Server.

- Clustermodus: Der Anwender kann eine schreibgeschützte Rolle mit Standardzugriff haben.
- 7-Modus: Der Anwender muss über eine anwenderdefinierte Rolle mit den folgenden Fähigkeiten verfügen:
  - `login-snmp, login-ndmp, login-sp, and login-http-admin`
  - `Api-*`

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den schreibgeschützten Anwender. Weitere Informationen finden Sie unter Virtual Server Interface .

REST-basierte Discovery-Voraussetzungen

Deaktivieren Sie die SNMP-basierte Discovery. Weitere Informationen finden Sie unter Deaktivieren Sie SNMP-basiert NetApp Speicher-Cluster-Discovery.

Überprüfen Sie, ob der Anwendungsanwender über einen verfügt **Schreibgeschützt** Rolle.

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den schreibgeschützten Anwender. Weitere Informationen finden Sie unter Virtual Server Interface .

Discovery wird ausgeführt.

So führen Sie die Discovery anhand von Mustern aus: Erstellen Sie einen Discovery-Zeitplan Die auf die Verwaltungs-IP-Adresse von ausgerichtet ist NetApp Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: NetApp Erstellt verschiedene Speichervolume-Bezeichner, wenn sie mit verschiedenen Protokollen ausgeführt werden. Bei der Ausführung der Discovery mit HTTP nach der Ausführung der Discovery mit SNMP werden doppelte CIs für dasselbe Speichervolume erstellt. Ein CI wird für den eindeutigen Bezeichner (UUID) erstellt. NetApp ONTAP-API stellt bereit, und für den eindeutigen Bezeichner (UUID) wird ein CI erstellt. NetApp HTTP-REST-API STELLT BEREIT.

Von erfasste Daten NetApp Cluster-SNMP-Muster

In den folgenden Tabellen sind die Daten aufgeführt, die Discovery Kann finden, wenn Sie ausführen NetApp Discovery-Muster.

Tabelle	Felder
cmdb_ci_storage_server	Name firmware_version serial_number manufacturermode model_id cim_object_path short_description ip_address
cmdb_ci_storage_cluster	short_description ip_address manufacturer
cmdb_ci_storage_cluster_node	Name operational_status
cmdb_ci_storage_node_element	Cluster short_description manufacturer serial_number model_id ram cpu_type cpu_manufaturer cpu_core_count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Felder
cmdb_ci_network_adapter	Name ip_address netmask cmdb_ci
cmdb_serial_number	serial_number serial_number_type
cmdb_ci_ip_address	ip_address netmask nic ip_version (Storage-7 mode) Name
cmdb_ci_disk	Name device_id serial_number manufacturer model_id storage_type device_interface size_bytes Computer
cmdb_ci_storage_fileshare	Pfad Name
cmdb_ci_storage_pool	Name short_description free_space_bytes pool_id size_bytes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Felder
cmdb_ci_storage_volume	Name lun volume_id
cmdb_ci_iscsi_export	Name lun initiator_iqn iqn export_id
cmdb_ci_storage_controller	Name device_id
cmdb_ci_fc_export	initiator_wwpn export_id Name lun
cmdb_ci_fc_port	speed Name wwnn wwpn

Hinweis: Weitere Informationen zu finden NetApp Discovery mit CIM, siehe Speichererkennung über SMI-S und CIM.

Daten erfasst von NetApp Cluster-HTTP-Muster

Die folgenden Daten werden beim Deaktivieren von erkannt **NetApp-Cluster-SNMP** Muster.

Tabelle	Felder
cmdb_ci_storage_server	ip_address cluster_version serial_number

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Felder
cmdb_ci_storage_node_element	Cluster ip_address_Range
cmdb_ci_storage_cluster_node	Name operational_status Cluster
cmdb_ci_storage_server	firmware_version Beschreibung ip_address_Range
cmdb_serial_number	serial_number serial_number_type
cmdb_ci_ip_address	name netmask nic
cmdb_ci_disk	Computer Schnittstelle size_bytes
cmdb_ci_storage_pool	name size_bytes free_space_bytes
cmdb_ci_fc_port	speed
cmdb_ci_storage_fileshare	path
cmdb_ci_storage_volume	name volume_id size_bytes free_space_bytes
cmdb_ci_iscsi_export	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Felder
	lun export_id initiator_iqn iqn
cmdb_ci_storage_controller	Name device_id
cmdb_ci_fc_export	name lun export_id initiator_wwpn

CI-Beziehungen

CI	Beziehungstyp	CI
cmdb_ci_storage_node_element	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_storage_cluster_node	Gehostet auf::Hostet	cmdb_ci_storage_node_element
cmdb_ci_storage_cluster_node	Cluster Von:Clustern	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Wird Ausgeführt Am:Ausführungen	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeteilt An: Zugeteilt Von	cmdb_ci_storage_node_element
cmdb_ci_storage_node_element	Besitzt:Im Besitz Von	cmdb_ci_network_adapter
cmdb_ci_storage_server	Besitzt:Im Besitz Von	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzt:Im Besitz Von	cmdb_ci_ip_address
cmdb_ci_storage_server	Besitzt:Im Besitz Von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_storage_node_element	Enthält::Enthalten in	cmdb_ci_storage_pool
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_pool
cmdb_ci_storage_server	Besitzt:Im Besitz Von	cmdb_ci_fc_port
cmdb_ci_storage_fileshare	Bereitgestellt Von: Stellt Bereit	cmdb_ci_storage_server
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_controller	Controller Für:Gesteuert Von	cmdb_ci_fc_port
cmdb_ci_iscsi_export	Gehostet auf::Hostet	cmdb_ci_storage_server
cmdb_ci_fc_export	Gehostet auf::Hostet	cmdb_ci_storage_server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Deaktivieren Sie SNMP-basiert NetApp Speicher-Cluster-Discovery

Deaktivieren Sie die standardmäßige SNMP-basiert NetApp Speicher-Cluster-Discovery und verwenden Sie stattdessen die REST-basierte Discovery, um die Sicherheit zu erhöhen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **SNMP**an.
2. In **Name** Feld, suchen Sie nach NetApp Storage Server-Cluster-Modus .
3. Wählen Sie den Datensatz NetApp Storage Server Cluster-Mode aus.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für einen Anwender mit einer schreibgeschützten Rolle. Weitere Informationen finden Sie unter Virtual Server Interface .

Zugehörige Informationen

NetApp Server und Cluster Discovery

Große Speichernutzlasten in Linux und Solaris verwalten

Hohe Nutzlasten für direkt angeschlossenen Linux- und Solaris-Speicher können zu Fehlern aufgrund von Speichermangel führen, wenn sie nicht für die Serialisierung der Verarbeitung der Nutzlast konfiguriert sind.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Linux- oder Solaris-Speichersensoren Nutzlasten großer Datenträger-Arrays verarbeiten, werden Worker-Threads gleichzeitig ausgeführt, was dazu führen kann, dass einem Instanzknoten der Arbeitsspeicher ausgeht und er neu gestartet werden muss. Um das zu verhindern, steuert die Tabelle [discovery_sensor_yield] das Verhalten von Worker-Threads, die zur Verarbeitung großer Nutzlasten verwendet werden. Wenn Discovery einen Sensor verarbeitet, wird die Tabelle [discovery_sensor_yield] für diesen Sensor überprüft. Wenn der Sensor in der Tabelle aufgeführt ist und die Nutzlastgröße den in der Tabelle konfigurierten Grenzwert überschreitet, versucht der Worker vor der Verarbeitung der Nutzlast, eine Sperre zu setzen. Wenn die Sperre nicht verfügbar ist, da ein anderer Worker bereits eine große Nutzlast verarbeitet, plant der wartende Worker die Neuausführung des Auftrags in 30 Sekunden und fährt mit anderen Aufgaben fort. Der Auftrag wartet dann in der Tabelle „Zeitplanelement“ [sys_trigger] darauf, dass ein inaktiver Worker ihn abholt. Diese Serialisierung erfolgt knotenweise, sodass mehrere Knoten gleichzeitig hohe Nutzlasten verarbeiten können. Das Verarbeitungsintervall von 30 Sekunden ist nicht konfigurierbar.

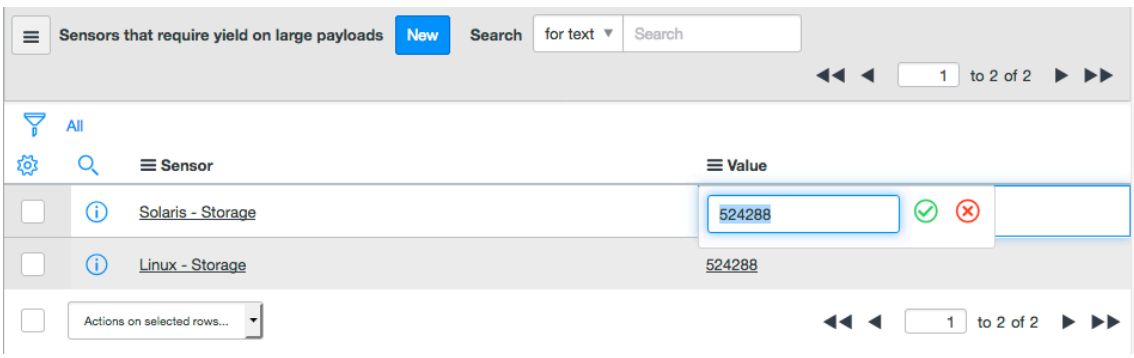
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Diese Schwellenwerte wurden nur für Linux- und Solaris-Speichersensoren erstellt und sollten in den meisten Fällen nicht geändert werden. Wenn Ihrer Instanz nicht genügend Arbeitsspeicher zur Verfügung steht, während gleichzeitig mehrere große Speichernutzlasten verarbeitet werden, sollten Sie die Erkennung dieser Systeme zu Zeiten geringerer Aktivität planen. Wenn dies nicht möglich ist, überprüfen Sie die ECC-Warteschlange, um zu bestimmen, welcher Speichersensor möglicherweise das Problem verursacht, und notieren Sie sich die Größe der Nutzlast. Wenn die Nutzlastgröße unter dem Schwellenwert in der Tabelle [discovery_sensor_yield] liegt, senken Sie den Schwellenwert weit genug, damit die Nutzlast serialisiert wird. Wenn ein anderer Sensor als der Linux- oder Solaris-Speichersensor verantwortlich ist, können Sie diesen Sensor der Tabelle [discovery_sensor_yield] hinzufügen. Stellen Sie sicher, dass der Schwellenwert für die Nutzlastgröße richtig festgelegt ist. Die Serialisierung der Sensorverarbeitung kann Discovery verlangsamen.

Prozedur

1. Geben Sie im Anwendungsnavigatorfilter **discovery_sensor_yield.list** ein.
   Das Discovery-Basissystem serialisiert die folgenden Sensoren, wenn ihre Nutzlasten 512 KB überschreiten:
   - **Solaris - Storage**
   - **Linux - Storage**
2. Um den Schwellenwert zu ändern, doppelklicken Sie in der Liste in die Spalte **Wert**, und bearbeiten Sie die Größe.

Schwellenwert für Sensorlast bearbeiten



3. Um einen weiteren Sensor hinzuzufügen und für die Nutzlastserialisierung zu konfigurieren, klicken Sie auf **Neu**, und füllen Sie die Felder im Formular aus.
   - **Sensor**: Zu konfigurierender Speichersensor
   - **Wert**: Schwellenwertgröße für den Sensor
4. Klicken Sie auf **Absenden**.

Beispiele für die Speichererkennung

Discovery erstellt Konfigurationselemente (CI) und CI-Beziehungen für physische und logische Speicherkomponenten, die direkt an Anwendungs- und Datenbankserver oder über Fibre Channel Switched Fabric in einer Multipfadkonfiguration angeschlossen sind.

Direct Attached Storage

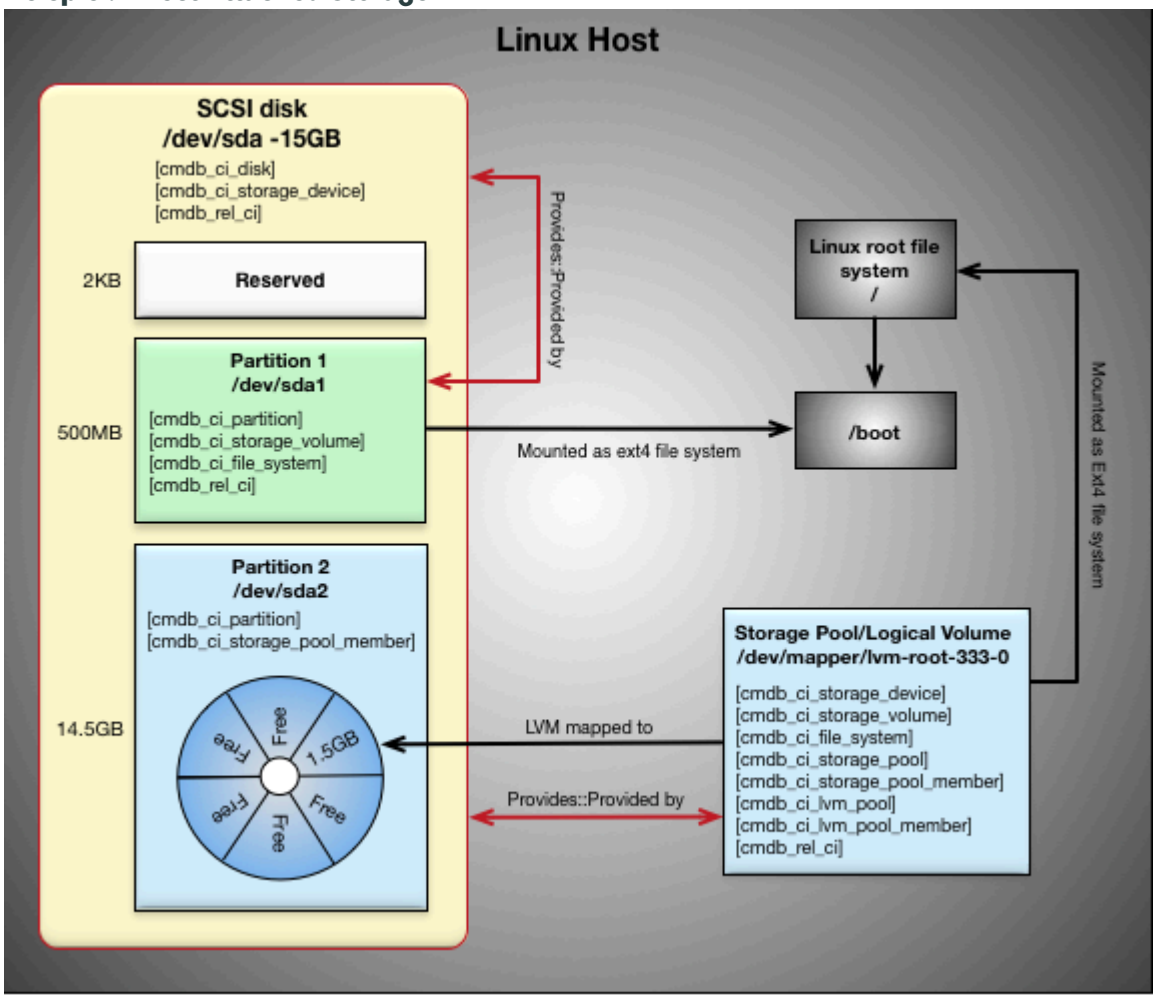
In diesem Beispiel für Direct Attached Storage (DAS) wird ein SCSI-Laufwerk mit den beiden Partitionen `/dev/sda1` und `/dev/sda2` an einen Linux-Host angeschlossen. Die Partition `/dev/sda1` ist startfähig und unterstützt die Systemsoftware. Die Partition `/dev/sda2` enthält ein logisches Volume, das als Speicherpool konfiguriert und von Logical Volume Management (LVM) in das Linux-Stammdateisystem geladen wurde. Der Speicherpool

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet nur 1,5 GB der Partition, sodass 13 GB Speicherplatz für weitere logische Volumes zur Verfügung stehen.

Beispiel: Direct Attached Storage



Für Direct Attached Storage (DAS) erstellte Konfigurationselemente und Beziehungen

Konfigurationselement	Beschreibung	Tabellen	Schlüsselreferenz und Beziehungen
/dev/sda	Physisches SCSI-Speichergerät	• [cmdb_ci_disk] • [cmdb_ci_storage_device] • [cmdb_rel_ci]	[cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/sda1
			[cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/mapper/lvm-root-333-0

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Direct Attached Storage (DAS) erstellte Konfigurationselemente und Beziehungen (Fortsetzung)

Konfigurationselement	Beschreibung	Tabellen	Schlüsselreferenz und Beziehungen
/dev/sda1	Partition 1 auf SCSI-Speichergerät	• [cmdb_ci_partition] • [cmdb_ci_storage_volume] • [cmdb_ci_file_system] • [cmdb_rel_ci]	[cmdb_ci_file_system] • **Bereitstellungspunkt**: /boot • **Dateisystem**: Ext4 [cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/sda1
/dev/sda2	Partition 2 auf SCSI-Speichergerät	• [cmdb_ci_partition] • [cmdb_ci_storage_pool_member]	[cmdb_ci_storage_pool_member] • **Pool**: /dev/mapper/lvm-root-333-0 • **Speicher**: /dev/sda2
/dev/mapper/lvm-root-333-0	Logisches Linux-Volume, das mit LVM einer physischen Plattenspeicherpartition zugeordnet ist	• [cmdb_ci_storage_device] • [cmdb_ci_storage_volume] • [cmdb_ci_file_system] • [cmdb_ci_Storage_Pool] • [cmdb_ci_storage_pool_member] • [cmdb_ci_lvm_pool] • [cmdb_ci_lvm_pool_member] [cmdb_rel_ci]	[cmdb_ci_file_system] • **Bereitstellungspunkt**: / • **Dateisystem**: Ext4 [cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/mapper/lvm-root-333-0 [cmdb_ci_storage_pool_member] • **Pool**: /dev/mapper/lvm-root-333-0 • **Speicher**: /dev/sda2

Multipfad-Fibre Channel-Speicher

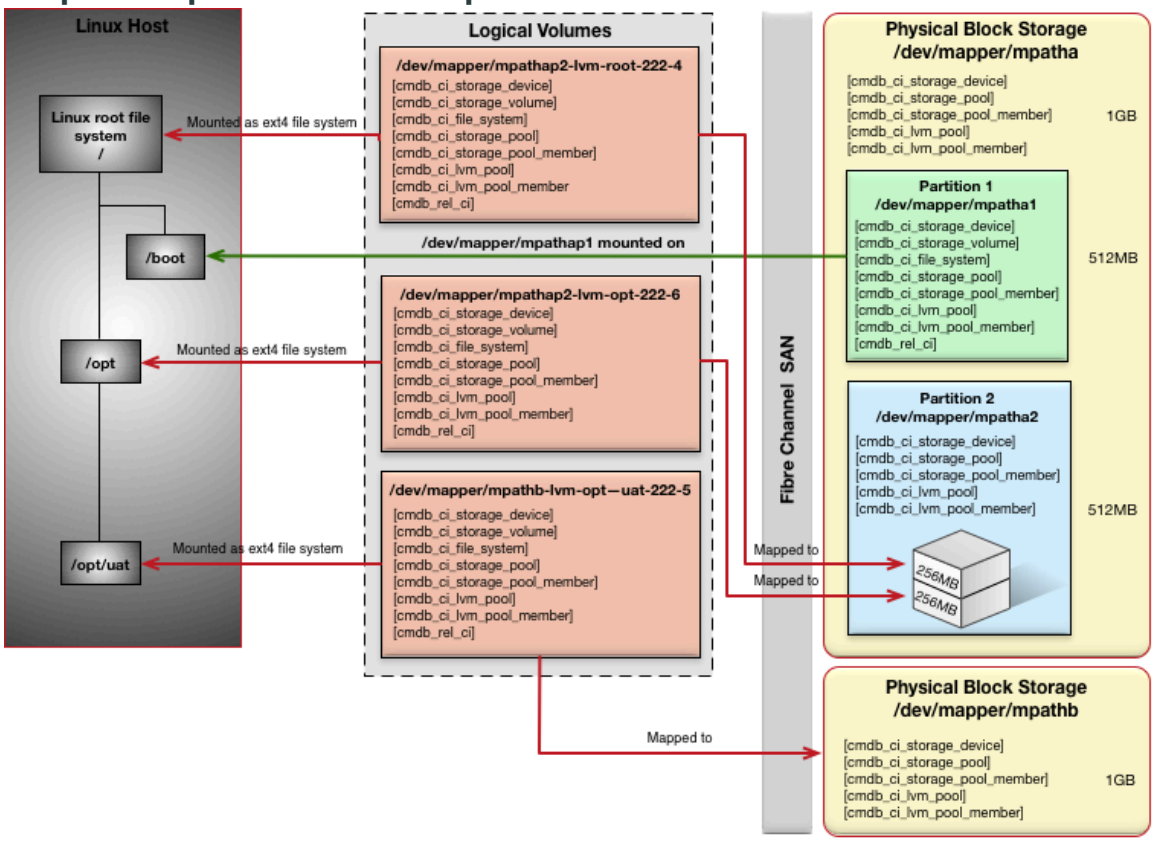
In diesem Beispiel eines Fibre Channel-SAN (Storage Area Network) werden die beiden physischen Speichergeräte mpatha und mpathb über Fibre Channel Switches mit einem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Host verbunden, die Failover-Funktionen bereitstellen. Das Laufwerk mpatha enthält die beiden Partitionen mpatha1 und mpatha2. Die erste Partition wird in /boot direkt auf dem Linux-Host bereitgestellt. Drei logische Volumes werden der Partition mpatha2 und dem physischen Gerät mpathb zugeordnet. Die logischen Volumes werden als Ext4-Dateisysteme in Ordnern in der Linux-Stammstruktur bereitgestellt. Das folgende Beispiel zeigt die CIs, die Discovery für jede Komponente verwaltet, und die Bereitstellungspunkte für die logischen Volumes auf dem Linux-Host.

Beispiel: Multipfad-Fibre Channel-Speicher



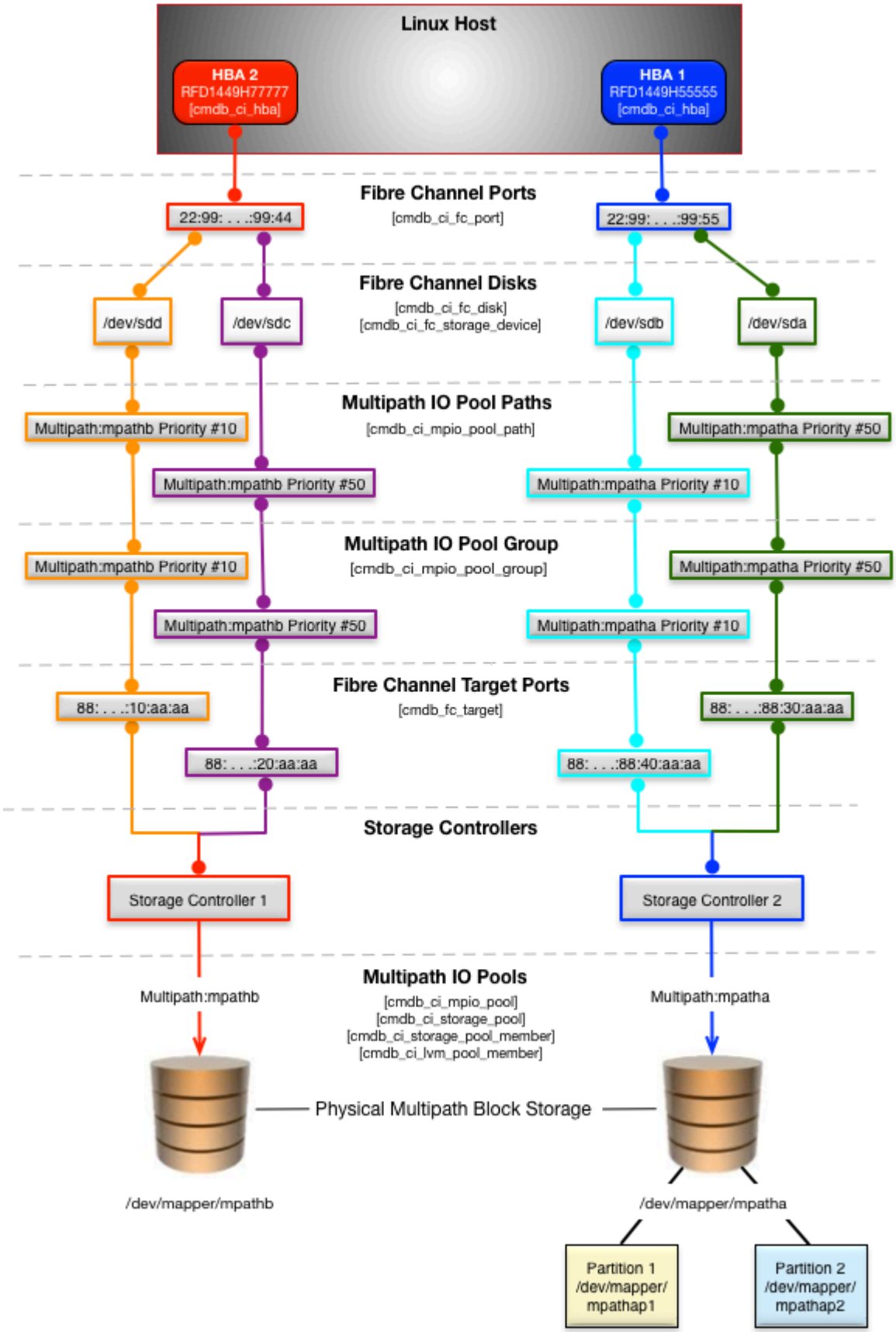
Details zu Switched Fibre Fabrics

Discovery erstellt CIs für die logischen Unterkomponenten in NAS- und SAN-Umgebungen, zum Beispiel Fibre Channel-Datenträger und Poolkomponenten sowie für Hostbusadapter (HBA) und physischen Blockspeicher. In Multipfadumgebungen erstellt Discovery CI-Beziehungen innerhalb der Switched Fibre Fabrics, die den Linux-Host mit den physischen Speichergeräten verbinden. In diesem Diagramm verfügen die Fibre Fabrics über redundante Pfade, die in der SAN-Umgebung beim Ausfall von Verbindungen für Failover verwendet werden können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Redundante Fibre Fabric-Pfade



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz zu ITOM-Transparenz und CSDM

ITOM-Transparenz Besteht aus zwei ServiceNow Produkte: Discovery Und Service-Mapping. Diese Produkte sind für die Erstellung von Konfigurationselementen (Configuration Items, CIs) in verantwortlich CMDB Und verknüpfen. Das Ziel dieser Produktansicht besteht darin, Ihnen zu helfen, wie zu verstehen ITOM-Transparenz Funktioniert mit dem Kern CSDM Framework.

Aspekte von ITOM-Transparenz

Discovery

Discovery findet Computer, Server, Drucker, eine Vielzahl von IP-fähigen Geräten und die darauf ausgeführten Anwendungen. Dann können die CIs in aktualisiert werden CMDB Mit den erfassten Daten.

Service-Mapping

Service-Mapping Erkennt alle Anwendungsservices in Ihrer Organisation und erstellt eine umfassende Übersicht aller Geräte, Anwendungen und Konfigurationsprofile, die die zugehörigen Business-Services unterstützen.

Service-Mapping Ordnet Abhängigkeiten basierend auf den Verbindungen zwischen Geräten und Anwendungen zu. Diese Methode, die als Top-Down-Zuordnung bezeichnet wird, hilft Ihnen, die Auswirkungen eines problematischen Objekts auf den Rest der Anwendungsservices sofort zu erkennen.

Implementierung CMDB Daten

Für Details zur Implementierung CMDB Daten, die mit übereinstimmen sollen CSDM Framework, siehe Implementierung des CSDM-Frameworks in Phasen .

Einzelheiten erfahren Sie von

CSDM-Modell erkunden .

Implementierung des CSDM-Frameworks in Phasen .

Discovery-Grundlagen .

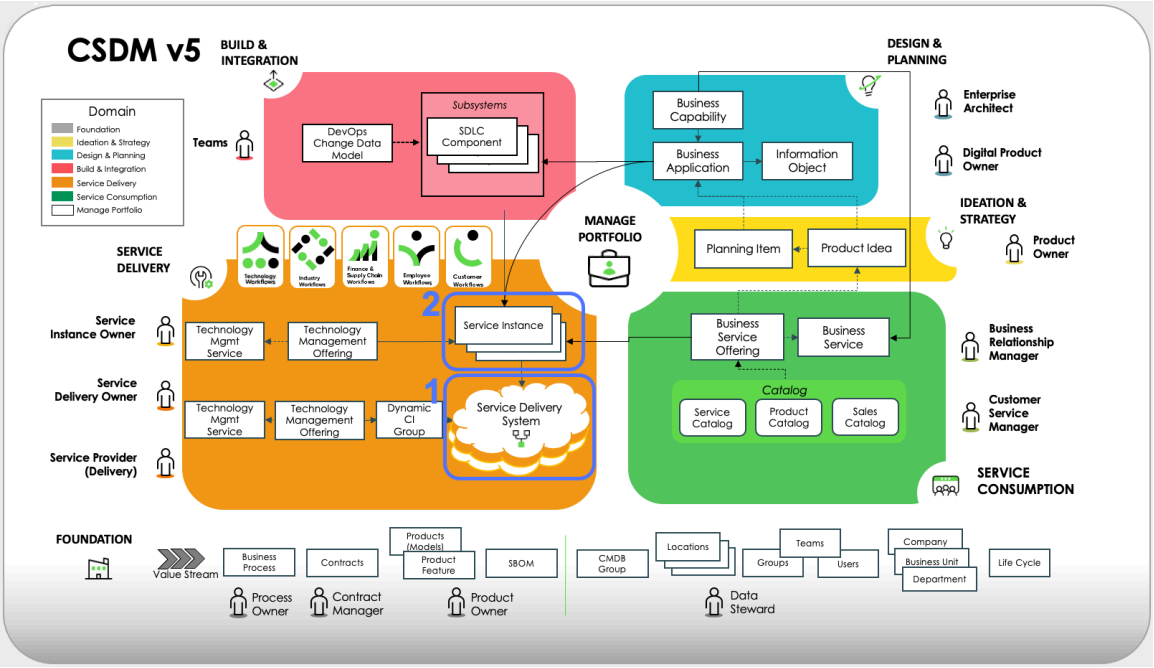
Service-Mappingan.

ITOM-Transparenz und CMDB-Tabellen

ITOM-Transparenz verwaltet und verwendet CMDB-Tabellen. Mehrere ServiceNow-Produkte profitieren von ITOM-Transparenz und fügen der Anwendung Mehrwert hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellen, die ITOM-Transparenz Verwaltet



Zugeordnete Anwendungsservicetabellen

Die Tabellen, die ITOM-Transparenz Verwaltet abhängig von der Methode, die zum Zuordnen der Serviceinstanz verwendet wurde (die Bezeichnung für die Tabelle war früher Anwendungsservice) . Sie können den Anwendungsservice-Assistenten verwenden, um einen Anwendungsservice auszufüllen.

- Ordnen Sie die Serviceinstanz mithilfe der Top-Down-Discovery von CI-Verbindungen zu. Diese Methode erfordert Service-Mapping, Die Rolle sm_admin und die aktuelle Domäne müssen eine untergeordnete Domäne sein. Dies ist die beste Option für Genauigkeit und vollständige Zuordnung. ITOM-Transparenz Verwaltet die Tabelle „zugeordneter Anwendungsservice“ [cmdb_ci_Service_Discovered]
- Ordnen Sie die Serviceinstanz mithilfe einer Tag-Liste oder einer Tag-Familie zu. Diese Methode erfordert Service-Mapping Und wird für die öffentliche oder private Cloud bevorzugt, in der Tags normalerweise verwendet werden. ITOM-Transparenz Verwaltet die Tag-basierte Zuordnungstabelle [cmdb_ci_Service_by_Tags].
- Ordnen Sie die Serviceinstanz manuell zu. Diese Methode erfordert, dass Sie bestimmte CIs auswählen – es wird keine Automatisierung verwendet. ITOM-Transparenz Verwaltet die Tabelle „Servicezuordnungen“ [cmdb_ci_Service_Manual].
- Verwenden Sie den dynamischen Service, um manuell erstellte CI-Beziehungen mit einer Servicezuordnungsansicht zu synchronisieren.

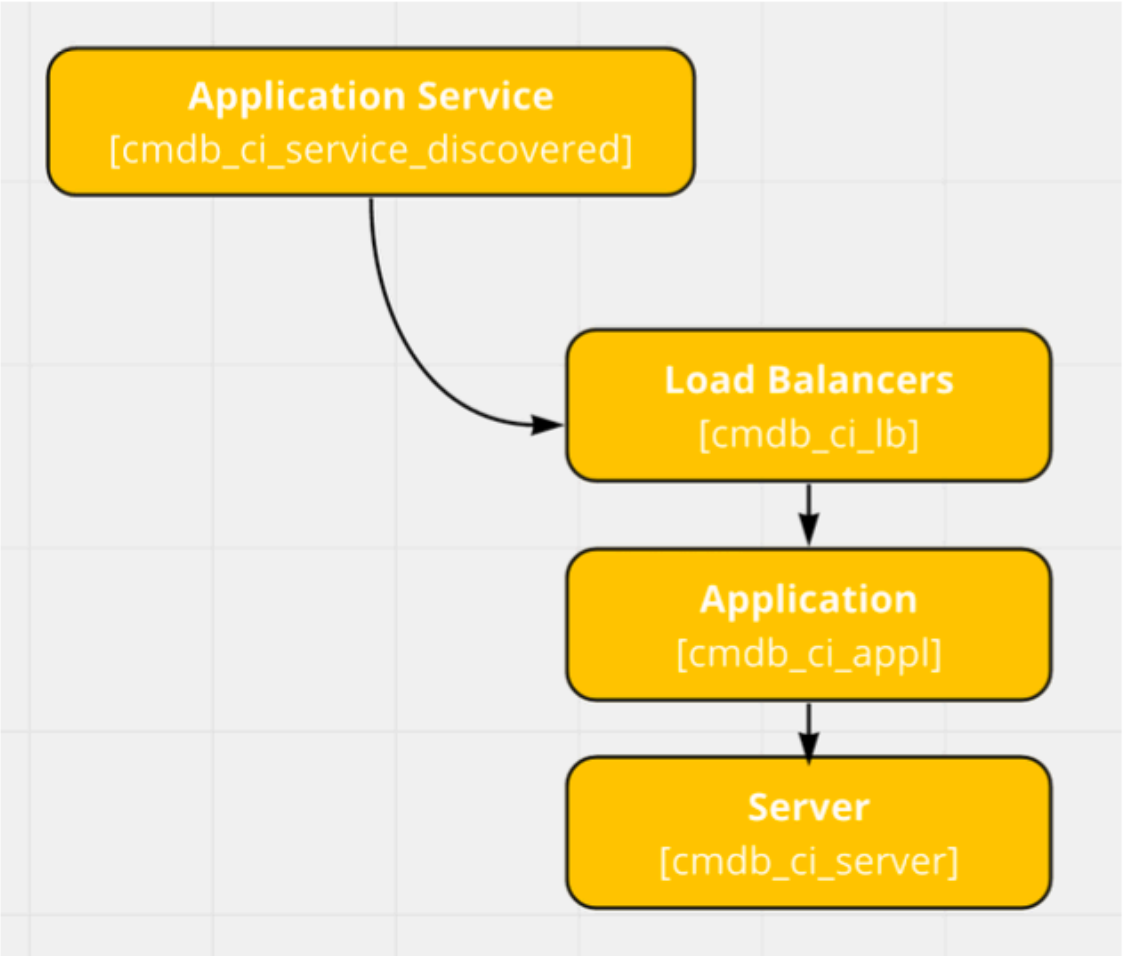
Tabellen für Konfigurationselemente (CIs) [cmdb_ci_*]

- Tabelle „Anwendung“ [cmdb_ci_appl]
- Tabelle „Server“ [cmdb_ci_server]
- Tabelle „Virtuelle Maschinen“ [cmdb_ci_vm_instance]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

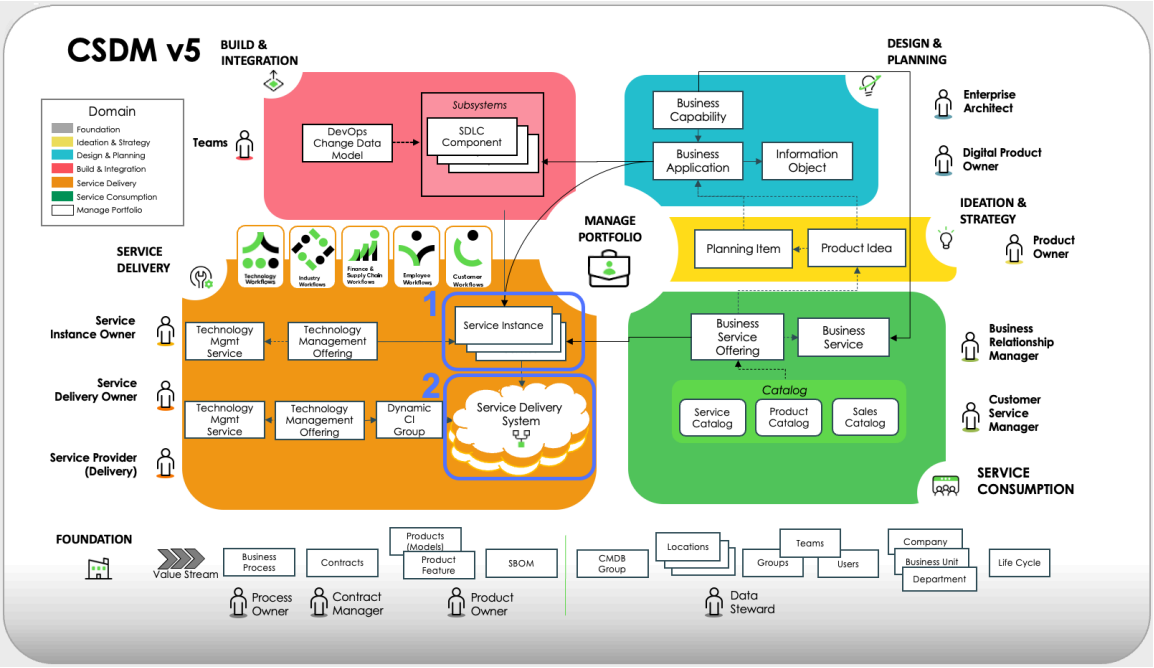
- Tabelle „Lastenausgleichsmodul“ [cmdb_ci_lb]
- Tabelle „Netzwerkgerät“ [cmdb_ci_netgear]



Tabellen, die ITOM-Transparenz Verwendet

1. Dynamische CI-Gruppentabelle [cmdb_ci_query_based_Service]
2. Produktmodelltabellen (für Technologie-Portfoliomanagement [TPM]) Software- und Hardwaremodelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Produkte, die von ITOM-Transparenz profitieren

- IT Service Management
- Kundenservice-Management (CSM)
- Ereignismanagement
- Cloud-Management
- Asset-Management(Hardware Asset Management Und Software Asset Management)
- Strategisches Portfoliomanagement(Finanzmanagement– Showback-Anweisungen, Anwendungs-Portfoliomanagement[APM])
- Security Operations (Incident Response, Software-Schwachstellenmanagement)

Implementierung CMDB Daten

Für Details zur Implementierung CMDB Daten, die mit übereinstimmen sollen CSDM Framework, siehe Implementierung des CSDM-Frameworks in Phasen .

ITOM-Transparenz – Anwendungsfall

Die ITOM-Transparenz Anwendungsfälle werden in diesem Abschnitt beschrieben.

Discovery – Anwendungsfall

- Verschaffen Sie sich einen besseren Einblick in Ihre lokalen und Cloud-Ressourcen.
- Verfolgen Sie Änderungen an Ihrer lokalen, Cloud- und serverlosen Infrastruktur in der nach Configuration Management Database (CMDB).
- Schaffen Sie eine solide Grundlage mit genauen Daten und Beziehungsansichten für ServiceNow Produkte, einschließlich Change-Management, Software Asset Management, Kundenservice-Management (CSM), Und Security Operations.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hauptfunktionen des Anwendungsfalls für Discovery

- Einrichten und verwalten Discovery Aufträge.
- Sehen Sie sich IT-Ressourcen und -Abhängigkeiten auf einen Blick an.
- Erstellen Sie Abfragen, um erkannte IT-Ressourcen zu validieren.
- Verwalten Sie Ihre PKI-Zertifikate (Public Key Infrastructure) in einem Dashboard.

Ergebnisse des Anwendungsfalls für Discovery

Die CSDM Framework gibt Discovery Ein vorgeschriebenes Modell für die Beziehung von Infrastruktur- und Software-CIs zu anderen Bereichen, z. B. Anwendungsservices, Geschäftsanwendungen und Assets.

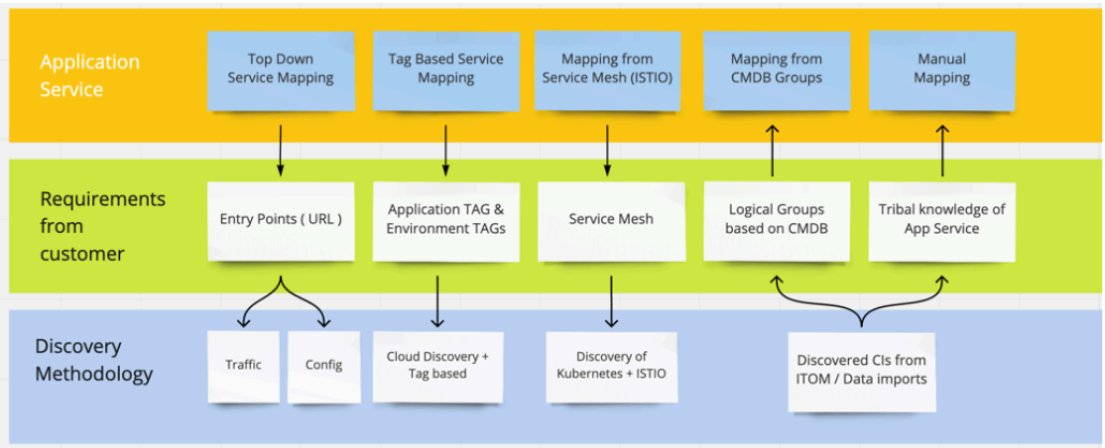
Service-Mapping – Anwendungsfall

Sie können Anwendungsservices manuell, über eine API oder über erstellen Service-Mapping Entdecken Sie sie. Unabhängig von der Erstellungsmethode werden alle Anwendungsservices in der Tabelle „zugeordneter Anwendungsservice“ [cmdb_ci_Service_Discovered] gespeichert.

Ergebnisse des Anwendungsfalls für Service-Mapping

Service-Mapping Automatisiert einen kritischen Aspekt von CSDM Mit einem konsistenten, automatisierten Ansatz zur Verbindung der logischen Ebene von CSDM Modell zu den physischen Modell-CIs in der CMDB. Mit diesem Ansatz können Sie Ihre Geschäftsanwendungen effektiver verwalten. Mit dem Ansatz können Sie auch die Modellierung Ihrer Geschäftsanwendungen für die Auswirkungsbewertung und -Analyse automatisieren. Für Auswirkungsbewertungen und -Analysen können Sie eine Anzahl von verwenden ServiceNow Produkte einschließlich Change-Management, Incident-Management, Oder CMDB Abfragegenerator.

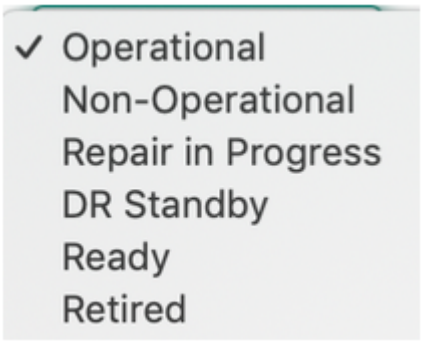
Anwendungsservices-Flow



Anwendungsservices in anzeigen Betreiber-Arbeitsbereich

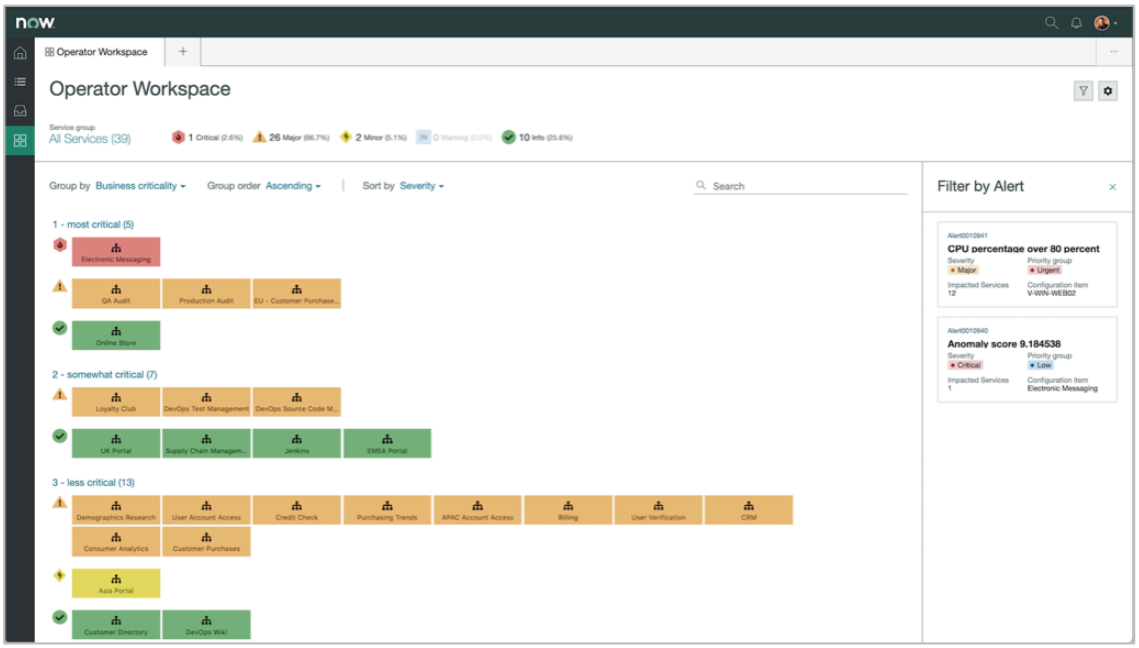
Sie können einen Lebenszyklusstatus für einen Anwendungsservice angeben. Anwendungsservices mit dem Status „Betriebslebenszyklus“ können in Servicezuordnungen für die relevanten Workflows verwendet werden, z. B. Workflows für künstliche Intelligenz für IT Operations (AIOPs).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können Informationen zu den Services, z. B. die Relevanz, in anzeigen Betreiber-Arbeitsbereich.

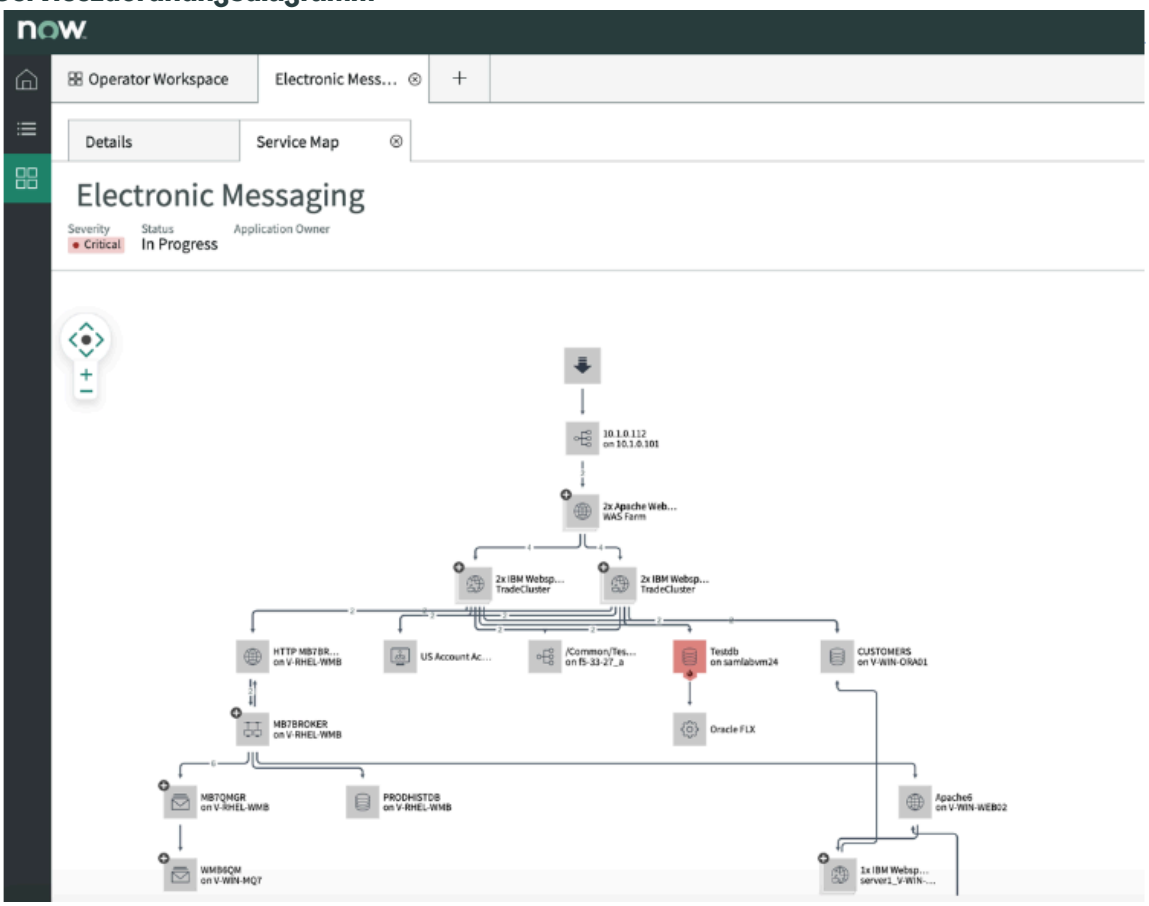
Betreiber-Arbeitsbereich



Auf der Registerkarte „Servicezuordnung“ wird eine visuelle Darstellung des Service angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicezuordnungsdiagramm



Zugehörige Informationen

Lebenszyklus von Dokument- und Vertragsentitäten

Lebenszyklus von materiellen/physischen CIs

Lebenszyklus von Standortentitäten

Lebenszyklus immaterieller/logischer Entitäten

Lebenszyklus von Produktentitäten

ITOM-TransparenzÜberlegungen zu CSDM Framework

Berücksichtigen Sie bei der Implementierung des CSDM-Frameworks die folgenden Punkte.

Sie können verwenden Service-Mapping Zum Definieren von Anwendungsservices.

Hier sind alternative Methoden zum Definieren von Anwendungsservices:

- Manuell definieren.
- Verwenden Sie eine dynamische CI-Gruppe basierend auf einer Abfrage.
- Verwenden Sie einen Tag-basierten Ansatz (häufig für Cloud-Integrationen verwendet).

Weitere Informationen zum Erstellen von Anwendungsservices finden Sie unter Erstellen Sie einen Anwendungsservice .

Optionen für Discovery-Zeitpläne ausführen

Sowohl die horizontale als auch die Top Down-Discovery verwenden diese Ausführungsoptionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Planausführungsoptionen

Option ausführen	Beschreibung
Bei Bedarf	Wird nicht nach einem Zeitplan ausgeführt. Wählen Sie Aus **Entdecken Sie jetzt** ist die Standardoption.
Täglich	Läuft jeden Tag. Verwenden Sie das Feld**Zeit**, um die Uhrzeit anzugeben.
Wöchentlich	Läuft an einem bestimmten Wochentag. Verwenden Sie das Feld **Zeit**, um die Uhrzeit anzugeben
Monatlich	Läuft an einem bestimmten Tag jedes Monats. Verwenden Sie das Feld **Tag**, um den Tag des Mo das Feld **Zeit**, um die Uhrzeit anzugeben. Wenn der festgelegte Tag nicht im Monat liegt, wird de ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan nicht im Februar ausgefü
Regelmäßig	Wird jedes festgelegte Mal ausgeführt. Verwenden Sie **Wiederholungsintervall** F in Tagen, Stunden, Minuten und Sekunden. Das erste Mal, wenn Discovery zu der Zeitpunkt ausgeführt wird. Die nachfolgenden Erkennungen werden nach Ablauf Zeitraums ausgeführt.
Einmal	Einmal ausführen, wie durch das Datum und die Uhrzeit festgelegt, die im festgelegt sind **Begin**
An Wochentagen	Läuft jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag. Verwenden Sie das Feld **Zeit** z
An Wochenenden	Läuft jeden Samstag und Sonntag. Verwenden Sie das Feld **Zeit** zur Auswahl der Tageszeit.
Letzter Tag des Monats	Führen Sie den letzten Tag jedes Monats aus. Verwenden Sie das Feld **Zeit** zur Auswahl der Tage
Ende des Kalenderquartals	Läuft am 31. März, 30. Juni, 30. September und 31. Dezember. Verwenden Sie das Feld **Zeit** zur das Skript `DiscoveryScheduleRunType`, um das Datum zu ändern.
Nach Discovery	Ermöglicht die sequenzielle Staffelung des Zeitplans. Verwenden Sie diese Optio dem im Feld **Ausführen nach** bezeichneten Discovery auszuführen. Aktivieren Sie **bei Abbruch**, um anzugeben, dass diese Erkennung auch dann ausgeführt werde Discovery vor Abschluss abgebrochen wird. • Diese Option ist nicht gültig, wenn Discovery Wird über DiscoverNow oder bei V erkennen“ gestartet. • Sie können keinen inaktiven angeben Discovery Zeitplan. • Sie können keine Schleife erstellen, indem Sie die Ausführung nach angeben D Discovery. • Dies Discovery Wird nicht ausgeführt, wenn **Ausführen nach** Discovery Wird nich der Ausnahme, dass **Auch wenn abgebrochen** Das Kontrollkästchen ist aktivier abgebrochen.

Automatische Übersetzung

Zugehörige Informationen

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Horizontale Erkennung planen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen ITOM-Transparenz

Tabellen, die die mit installierten Plugins oder Anwendungen auflisten ITOM-Transparenz Anwendungen. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Discovery

Mit installierte Plugins oder Anwendungen Discovery(Com.snc.Discovery)

Plugin- oder Anwendungsname	Beschreibung
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Service Watch-Suite – Commons (com.snc.service-watch.commons)	Enthält allgemeine UI-Komponenten für Discovery Und Service-Mapping.
Discovery – IP-basiert (com.snc.Discovery.ip_based)	Enthält gemeinsam genutzte Komponenten der horizontalen Discovery, die von verwendet werden Discovery Und Service-Mapping.

Discovery-Administratorarbeitsbereich

Plugin mit aktiviert Discovery-Administratorarbeitsbereich(sn_Disco_Workspace)

Plugin- oder Anwendungsname	Beschreibung
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.

Service-Mapping

Mit installierte Plugins oder Anwendungen Service-Mapping(com.snc.service-mapping)

Plugin- oder Anwendungsname	Beschreibung
Service-Mapping – Karte (com.itom-map-app)	Ein abhängiges internes Plugin, das erforderlich ist, um die Kernkomponenten von zu unterstützen Service-Mapping, Ereignismanagement, Und Service Operations-Arbeitsbereich ITOM Anwendungen.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Ereignismanagement Und Service-Mapping Kern (com.snc.service-watch)	Besteht aus den gemeinsamen Komponenten von Ereignismanagement und Service-Mapping.
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Service-Mapping(com.snc.service-mapping) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
	Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Musterdesigner (NG-Version) (com.snc.ng.pattern.designer)	Die NG-Version (nächste Generation) von Musterdesigner, mit der Sie Muster erstellen, bearbeiten und debuggen können, die von der horizontalen Erkennung und der Erkennung von oben nach unten verwendet werden.
Service-Mapping Plus (sn_sm_Scoped_App)	Bietet erweiterte Funktionen für Service-Mapping, Und falls zugehörig ServiceNow® Store Anwendungen und Plugins sind nicht bereits installiert, sie werden installiert.

Tag-Governance

Mit installierte Plugins oder Anwendungen Tag-Governance(sn_itom_Tag)

Plugin- oder Anwendungsname	Beschreibung
Cloud-Zugriffsschnittstelle (sn_cai)	Bietet einfachen Zugriff auf die Cloud durch Skripting. Sie können dies verwenden ServiceNow Store Anwendung zum Ausführen von Aktionen auf virtuellen Computern, die auf bereitgestellt wurden Amazon Web Services(AWS) Und Microsoft Azure.
Zertifizierungskern (com.snc.certification_Core)	Enthält Core-Zertifizierungsstrukturen wie Filter und Vorlagen und bietet Compliance-Funktionalität.
ITOM-Transparenz Lizenz (com.snc.itom.vis.license)	Aktiviert die Aktivierung von beliebig ServiceNow Store Anwendung, die erfordert ITOM-Transparenz Lizenzierung.
ITOM/OT SU-Lizenzierung (sn_itom_Lizenzierung)	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Flow Designer-Aktionsschritt – Skript auf MID (com.glide.hub.action_step.script_mid)	Stellt einen Aktionsschritt zum Ausführen von anwenderdefiniertem JavaScript innerhalb einer wiederverwendbaren Aktion für einen MID-Server bereit.

Cloud Operations Workspace

Mit installierte Plugins oder Anwendungen Cloud Operations Workspace(sn_Cloud_OPS_WS)

Plugin- oder Anwendungsname	Beschreibung
Muster für Discovery und Service-Mapping (sn_itom_pattern)	Stellt die neuesten im ServiceNow Store veröffentlichten Versionen von Muster für Discovery und Service-Mapping bereit. ServiceNow veröffentlicht im ServiceNow® Store jeden Monat neue Muster, damit Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Cloud Operations Workspace(sn_Cloud_OPS_WS) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Performance Analytics Inhaltspaket für Cloud-Ressourcen (sn_Disco_cd)	Zeigt die zusammengefasste Ansicht aller Ihrer Cloud-Ressourcen an. Es bietet auch Analytics-Tabellen und -Ansichten, die Tags mit Ressourcen verknüpfen, sodass Sie eigene anwenderdefinierte Dashboards und Berichte erstellen können.
Musterdesigner (NG-Version) (com.snc.ng.pattern.designer)	Die NG-Version (nächste Generation) von Musterdesigner, mit der Sie Muster erstellen, bearbeiten und debuggen können, die von der horizontalen Erkennung und der Erkennung von oben nach unten verwendet werden.

Agent Client Collector Visibility – Inhalt

Mit installierte Plugins oder Anwendungen Agent Client Collector Visibility – Inhalt(sn_ACC_Visibility)

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Visibility – Inhalt Inhalt (sn_ACC_VIS_content)	Stellt Agent-basierte Infrastruktur-Discovery und -Sammlungen bereit Software Asset Management(SAM) zu unterstützende Metriken Discovery Und Digitale Endanwender-Experience(DEX) Anwendungen.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

Agent Client Collector Visibility – Inhalt Inhalt

Mit installierte Plugins oder Anwendungen Agent Client Collector Visibility – Inhalt Inhalt (sn_ACC_VIS_content)

Plugin- oder Anwendungsname	Beschreibung
Erweitertes Modell und Asset-Klassen (sn_ent)	Stellt neue, erweiterte Modellklassen, Asset-Klassen und Modellkategorien bereit, die im Basissystem enthalten sind und durch ServiceNow definiert werden. Installieren Sie das Plugin „Asset-Management“ (com.snc.asset_management) als Voraussetzung zur Nutzung dieser Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Agent Client Collector Visibility – Inhalt Inhalt (sn_ACC_VIS_content) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Discovery – IP-basiert (com.snc.Discovery.ip_based)	Enthält gemeinsam genutzte Komponenten der horizontalen Discovery, die von verwendet werden Discovery Und Service-Mapping.
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

Zugehörige Informationen

Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate

Mit installierte Plugins oder Anwendungen ITOM-Integrität

Mit aktivierte Plugins ITOM-Optimierung

Mit Now Assist für ITOM installierte Anwendungen

ITOM-Integrität

Das Produkt ServiceNow® ITOM-Integrität umfasst die Anwendungen ServiceNow® Ereignismanagement und ServiceNow® Metrikdaten, die Ihnen helfen, die Integrität von Services in Ihrer Organisation nachzuverfolgen und aufrechtzuerhalten.

Funktionen von ITOM-Integrität

Ereignismanagement

Ereignismanagement sammelt Warnungen von Infrastruktur-Events, die von Überwachungstools von Drittanbietern erfasst werden. Ereignismanagement verwendet IT-bezogene Informationen, die von Discovery gesammelt wurden, um Konfigurationselemente Warnungen zuzuordnen. Basierend auf den erfassten Informationen stellt Ereignismanagement Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen.

Agent Client Collector

Mit der Anwendung ServiceNow® Agent Client Collector können Sie die Serviceverfügbarkeit überwachen, Integrität und Leistung Ihrer Umgebung untersuchen und sicherstellen, dass Ihre Infrastruktur und die darin enthaltenen Anwendungen ordnungsgemäß ausgeführt werden. Sie können Metrikdaten auch verwenden, um Ihre IT-Infrastruktur proaktiv zu analysieren und so Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von erweitertem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur ermittelt die Anwendung Metrikdaten automatisch dynamische Schwellenwerte und identifiziert Anomalien, die auf potenzielle Serviceausfälle hindeuten.

Health Log Analytics

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung ServiceNow® Health Log Analytics prognostiziert IT-Probleme, bevor Benutzer durch diese beeinträchtigt werden. Die Anwendung hilft Ihnen, Probleme schneller zu lösen, indem maschinell generierte Protokolldaten in Echtzeit erfasst, interpretiert und korreliert werden. Sie erkennt jede Abweichung vom normalen Verhalten, sobald sie auftritt, und warnt Sie vor möglichen geschäftlichen Auswirkungen. Health Log Analytics empfängt und verarbeitet Protokolle über den MID-Server und sendet Events an die Anwendung ServiceNow® Ereignismanagement.

Service-Observability

Die ServiceNow® Service-Observability Die Anwendung hilft Betriebsteams bei der Selektierung und Verwaltung von Incidents in einem komplexen und verteilten Produktionssystem. Es kombiniert die Telemetrie externer APM-Systeme (Application Performance Monitoring) mit zugehörigen Daten aus dem Configuration Management Database (CMDB) Und werden in einem einzelnen Workflow in angezeigt Service Operations-Arbeitsbereich.

Synthetische Überwachung

Er ServiceNow® Synthetische Überwachung Mit der Anwendung können Unternehmen die Leistung und Verfügbarkeit kritischer Services proaktiv verwalten und verbessern. Durch die Simulation von Anwendertransaktionen auf API-Endpunkten identifiziert diese Lösung Leistungsengpässe, trägt zur Gewährleistung der Betriebszeit bei und optimiert die Anwender-Experience.

Service Operations-Arbeitsbereich für ITOM

Service Operations-Arbeitsbereich for ITOM ist ein konfigurierbarer Arbeitsbereich, der eine einheitliche Experience für mehrere IT Operations Management-Workflows bietet. Mit Service Operations-Arbeitsbereich for ITOM können Sie den Lebenszyklus von Warnungen verwalten, einschließlich der Ausführung von Aktionen zum Auflösen von Warnungen und Identifizieren des zugrunde liegenden Problems einer Warnung.

ITOM-Integrität Lizenzierung

Bei der für ServiceNow AI Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Integrität Anwendungen. ITOM-Integrität Und Health Log Analytics Sind als separate Lizenzen verfügbar. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Guided Setup zum Implementieren von IT Operations Management-Anwendungen

Das IT Operations Management-Guided Setup mit Anleitung bietet eine Reihe an Aufgaben, die Sie beim Konfigurieren von IT Operations Management-Anwendungen auf Ihrer ServiceNow-Instanz unterstützen. Zum Öffnen IT Operations Management Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an. Weitere Informationen zur Nutzung der Guided Setup-Benutzeroberfläche finden Sie unter Guided Setup verwenden .

MID-Webservererweiterung konfigurieren

Dank der Erweiterung „MID Web Server“ können externe Clients Metrikdaten per Push an den MID Server übertragen. Konfigurieren Sie die MID-Webservererweiterung, um die ITOM Health-Funktionen (Ereignismanagement, Agent Client Collector und Health Log Analytics) zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM-Integrität – Anwendungsfall

Moderne Organisationen wenden sich innerhalb von IT Operations (AIOps) Technologien der künstlichen Intelligenz (KI) zu, um die eskalierenden Mengen und die Vielfalt von Daten zu bewältigen. AIOps-Plattformen bieten Lösungen für die Analyse von Daten, die Automatisierung von Prozessen und die präventive Vorhersage von Problemen, um die wachsende Komplexität von IT-Umgebungen zu bewältigen.

Wichtige Funktionen von ITOM-Integrität Anwendungsfalleinbindung:

- Ereignisse und Metriken werden über erfasst Basissystem Integrationen mit ausgewählten Überwachungssystemen.
- Ereignisse und Metriken werden verarbeitet, um Warnungen zu erstellen.
- Korrelation von Warnungen und Durchführung einer Ursachenanalyse.
- Erkennung von Anomalien im System.
- Berechnung der Auswirkung auf Anwendungsservices.
- Verwendung des Service Operations-Arbeitsbereichs für das Betriebsmanagement.
- Automatisieren von Korrekturaktionen basierend auf Warnungen.

Anwendungsservice-Zuordnungen sind für Network Operations Center (NOC)-Betreiber an zentralen Hubs von entscheidender Bedeutung, da sie eine präzise Vorhersage von Ursachenwarnungen und die Korrelation dieser Warnungen mit erkannten Topologiedaten erleichtern. Diese Korrelation ermöglicht eine genaue Vorhersage der Serviceauswirkungen und ermöglicht eine effektive Auswirkungsanalyse, um die Auswirkungen auf Anwendungsservices zu bestimmen, die in der Anwendungsservice-Zuordnung visualisiert werden.

Produkte, die ITOM-Integrität Mehrwert hinzufügen

Im Kontext von ITOM-Integrität, Das sich auf die Aufrechterhaltung der Integrität und Leistung von IT-Systemen und -Infrastrukturen konzentriert, gibt es mehrere ServiceNow Produkte, die einen erheblichen Wert hinzufügen können:

Discovery

Discovery Identifizieren und sammeln Sie automatisch Informationen zu IT-Assets, Konfigurationen und Beziehungen, um Organisationen einen umfassenden Bestand zur effektiven Verwaltung und Überwachung ihrer IT-Infrastruktur zu bieten.

Service-Mapping

Service-Mapping Bietet detaillierte Informationen zu Anwendungsinstanzservices in der Tabelle [cmdb_ci_Service_detected]. Diese Daten helfen beim Herstellen von Verbindungen zwischen Infrastruktur- und Anwendungskonfigurationselementen (CIs), die in der Tabelle [cmdb_ci_appl] gespeichert sind, wodurch die Transparenz in IT-Umgebungen verbessert und effiziente Verwaltungs- und Überwachungsprozesse erleichtert werden.

Service-Portfoliomanagement

Service-Portfoliomanagement(SPM) Bietet das zugehörige Produktmodell, während an Software Asset Management(SAM) und Hardware Asset Management(HAM) Geben Sie Lebenszyklusdaten für an Technologie-Portfoliomanagement(TPM). Zusammen ermöglichen sie eine umfassende Verwaltung von IT-Assets, wodurch eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

effektive Nutzung, Compliance und Optimierung während ihres gesamten Lebenszyklus sichergestellt wird.

Produkte, die von ITOM-Integrität profitieren

Incident-Management

Incident-Management Tools nutzen nachgelagerte Informationen von Ereignismanagement Um Incidents schnell zu erstellen, um eine rechtzeitige Lösung von Problemen sicherzustellen.

Kundenservice-Management (CSM)

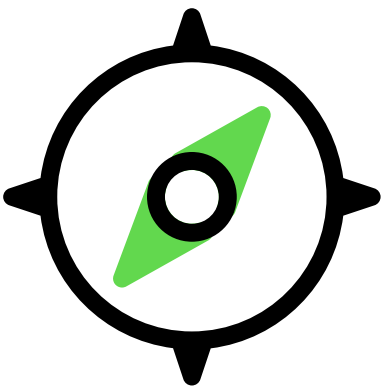
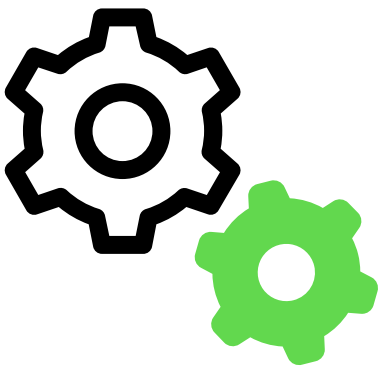
Kundenservice-Management (CSM) Systeme profitieren von ITOM-Integrität Durch die Verwendung von Auswirkungsdaten für Anwendungsservices, um betroffene Anwender umgehend zu identifizieren, wodurch die Effizienz und Zufriedenheit des Kundensupports verbessert wird.

Ereignismanagement

ServiceNow® Ereignismanagement Ist eine robuste Anwendung, die dazu beiträgt, dass Ihre IT-Systeme funktionsfähig sind, indem Probleme schnell erkannt und behoben werden. Es erfasst Ereignisse aus verschiedenen Quellen, ermittelt, was die Probleme verursacht, und konvertiert sie in Warnungen. Diese Warnungen werden dann analysiert, gruppiert und bearbeitet, um Probleme zu lösen und die Systemintegrität zu erhalten.

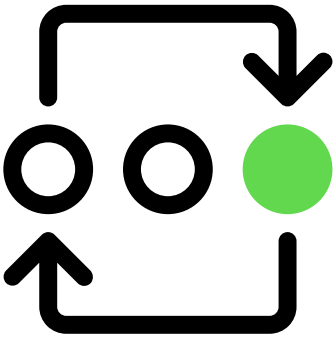
Ereignismanagement Lässt sich über Connectors und Listener nahtlos in verschiedene Überwachungstools integrieren, um eine umfassende Datensammlung und Korrelation zu ermöglichen. Verfügbar als separates Abonnement vom Hauptabonnement ServiceNow Plattform, Ereignismanagement Ermöglicht Unternehmen, ihre Nutzung an bestimmte Anforderungen anzupassen und ein effektives und effizientes Incident-Management ohne unnötigen Aufwand zu gewährleisten.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erkunden Sie die verschiedenen Arten der Warnungsgruppierung und die Regeln für die Korrelation	Setup Ereignismanagement	Zeigen Sie Warnungsinformationen an, und überwachen Sie die Serviceintegrität

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen	Ereignisverarbeitung	Referenz
		
Erfahren Sie, wie Sie integrieren können Ereignismanagement Mit anderen Überwachungssystemen	Machen Sie sich mit der Analyse und Verwaltung von Ereignissen vertraut	Rufen Sie Details zur Domänentrennung in ab Ereignismanagement

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Fragen in der Event Management Community stellen oder beantworten
- Technischen Support von ServiceNow kontaktieren
- Video: Erste Schritte mit Ereignismanagement
- Videos: Erste Schritte mit ITOM
- Entwicklerschulungen
- Entwicklerdokumentation

Ereignismanagement erkunden

Erkunden Ereignismanagement Um die Übersicht, den Prozess-Flow, die Anwenderrollen und die Vorteile für eine umfassende Überwachung und Lösung von IT-Problemen zu verstehen.

Ereignismanagement Bietet umfassende Überwachung, Analyse und Behebung von IT-Problemen durch effektive Verwaltung verschiedener Komponenten in einer IT-Umgebung. Diese Komponenten umfassen erkannte Services, Anwendungsservices, dynamische CI-Gruppen und Warnungsgruppen.

- Erkannte Services: Definiert durch Interrelated Configuration Items (CIs) aus der CMDB, wird ein erkannter Service durch Service-Mapping identifiziert. Es enthält eine Servicezuordnung mit Zuordnungsbeziehungen, eine Auswirkungsstruktur mit dem Schweregrad des Ausfalls, aktiven und zugehörigen Warnungen und CI-Eigenschaften. Diese Serviceinformationen werden in Dashboards, der Warnungsliste und der Ereignisliste angezeigt.
- Anwendungsservices: Anwendungsservices werden durch die Auswahl bestimmter CIs erstellt und ermöglichen eine gezielte Überwachung und Verwaltung. Weitere Informationen finden Sie in der Dokumentation zu Anwendungsservices.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dynamische CI-Gruppen: Dies sind Sammlungen von CIs, die basierend auf gemeinsam genutzten Kriterien gruppiert sind, z. B. Standort. Dynamische CI-Gruppen helfen beim Ausfüllen von Anwendungsservices und vereinfachen die Verwaltung.
- Warnungsgruppen: Warnungsgruppen organisieren Warnungssätze, um Wartung und Verwaltung zu optimieren und so die effiziente Reaktion auf IT-Probleme zu erleichtern.

Prozessablauf

Ereignismanagement Empfängt externe Ereignisse und generiert Warnungen basierend auf vordefinierten Regeln. Die MID-Server Fragt externe Ereignisnachverfolgungstools ab und sendet Daten an Ereignismanagement Für Speicherung und Verarbeitung. Ereignisse werden in der Tabelle „Ereignis“ [em_event] gespeichert, und Warnungen werden durch übereinstimmende Ereignisregeln erstellt. Warnungen werden dann transformiert und mit zusätzlichem Inhalt angereichert, kumuliert, wenn Schwellenwerte erfüllt werden, und bestimmten Feldern zugeordnet. Das System sucht nach übereinstimmenden Nachrichtenschlüsseln, um vorhandene Warnungen zu aktualisieren oder neue zu erstellen und zugehörige Ereignisse einer einzelnen Warnung zuzuordnen. Warnungen sind für die Ursachenanalyse an bestimmte Konfigurationselemente (Configuration Items, CIs) gebunden. Weitere Informationen finden Sie unter Prozess-Flow in Ereignismanagement.

Anwender

Rollentitel [Name]	Beschreibung
Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement. **Hinweis:** Seien Sie mit der Rolle „evt_mgmt_admin“ vorsichtig, da sie auf die Administratorrolle hochgestuft werden kann. Ein Anwender mit der Rolle „evt_mgmt_admin“ kann Skripts hinzufügen und ändern, die in einem globalen Bereich ausgeführt werden. Stellen Sie eine ordnungsgemäße Zugriffssteuerung sicher. Mit dieser Rolle kann der Anwender die folgenden Skripts erstellen und/oder aktualisieren: • Regeln zur Warnungskorrelation • Warnungsverwaltungsregeln • Wartungsregeln • Erweiterte Skripts • Ereignisfeldzuordnung • Skripts vor und nach der Bindung
Operator [evt_mgmt_operator]	Verwaltet Warnungen, einschließlich Schließen und Bestätigen. Überwacht den Gesamt Ereignismanagement Prozess, um sicherzustellen, dass Ereignisse ordnungsgemäß kategorisiert, priorisiert und zur Lösung weitergeleitet werden.
Teamoperator [evt_Team_Operator]	Verwaltet Ereignismanagement Vorgänge in einem bestimmten Team, wie in definiert **Zuweisungsgruppe** Feld. Mit dieser Rolle kann der Operator Warnungen ausschließlich für sein zugewiesenes Team lesen und schreiben. Darüber

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
	hinaus kann der Betreiber Konfigurationsänderungen für sein Team vornehmen, einschließlich Updates für Warnungsautomatisierung und das Integrations-Launchpad. **Hinweis:** Die Rolle „evt_Team_Operator“ muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keiner Gruppe zugeordnet ist, denen Warnungen zugewiesen sind, kann der Operator keine Warnungen sehen.
Anwender [evt_mgmt_user]	Verwaltet den Lebenszyklus von Warnungen, einschließlich der Ausführung grundlegender Vorgänge wie Anzeigen und Bestätigen.

Vorteile

- Schnelle Problemerkennung: Identifiziert schnell potenzielle IT-Probleme und hebt sie hervor.
- Effiziente Warnungsverarbeitung: Aggregiert Warnungen und korreliert sie für eine optimierte Verwaltung.
- Automatisierte Aktionen: Initiiert automatische Korrekturprozesse, um die Problemlösung zu beschleunigen.
- Umfassende Überwachung: Lässt sich in mehrere Tools integrieren, um eine vollständige Systemübersicht zu erhalten.
- Ursachenanalyse: Bietet Tools zur Identifizierung zugrunde liegender Ursachen von Problemen.
- Anpassbare Regeln: Passt Ereignis- und Warnungsverwaltungsregeln an bestimmte Anforderungen an.
- Reduzierte Ausfallzeit: Minimiert Systemausfallzeiten mit prompter Problemlösung.
- Verbesserte Transparenz: Echtzeit-Dashboards bieten Einblicke in die Systemintegrität.
- Kosteneffizienz: Senkt die Betriebskosten, indem längere Probleme vermieden werden.

Prozess-Flow in Ereignismanagement

Ereignismanagement Erfasst, analysiert und konvertiert Ereignisse in Warnungen, um eine effiziente Nachverfolgung und Korrektur zu ermöglichen.

Ereignismanagement empfängt externe Events und generiert Warnungen basierend auf den Event- und Warnungsverwaltungsregeln. Ereignisse werden direkt über E-Mail-Server, Skript, SNMP-Trap oder Webservice-API an Ihre Instanz gesendet. Die entsprechenden Warnungen werden zu Nachverfolgungs- und Nachbesserungszwecken in Dashboards angezeigt.

Während der Computer, die Software oder der Service Events generiert, ruft der MID-Server das externe Event-Nachverfolgungstool ab. Die MID-Server, Aufrechterhaltung einer Verbindung mit Ereignismanagement, Sendet die Informationen zur Speicherung, Verarbeitung und Korrektur an Ihre Instanz.

Die Instanz speichert Ereignisse in der Tabelle „Ereignis“ [em_event] und versucht, Warnungen basierend auf vordefinierten Regeln und Ereigniszuordnungen zu generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unabhängig davon, ob eine Warnung generiert wird, steht das ursprüngliche Ereignis zur Überprüfung und Korrektur zur Verfügung. Warnungen werden gemäß dem folgenden Prozess-Flow generiert.

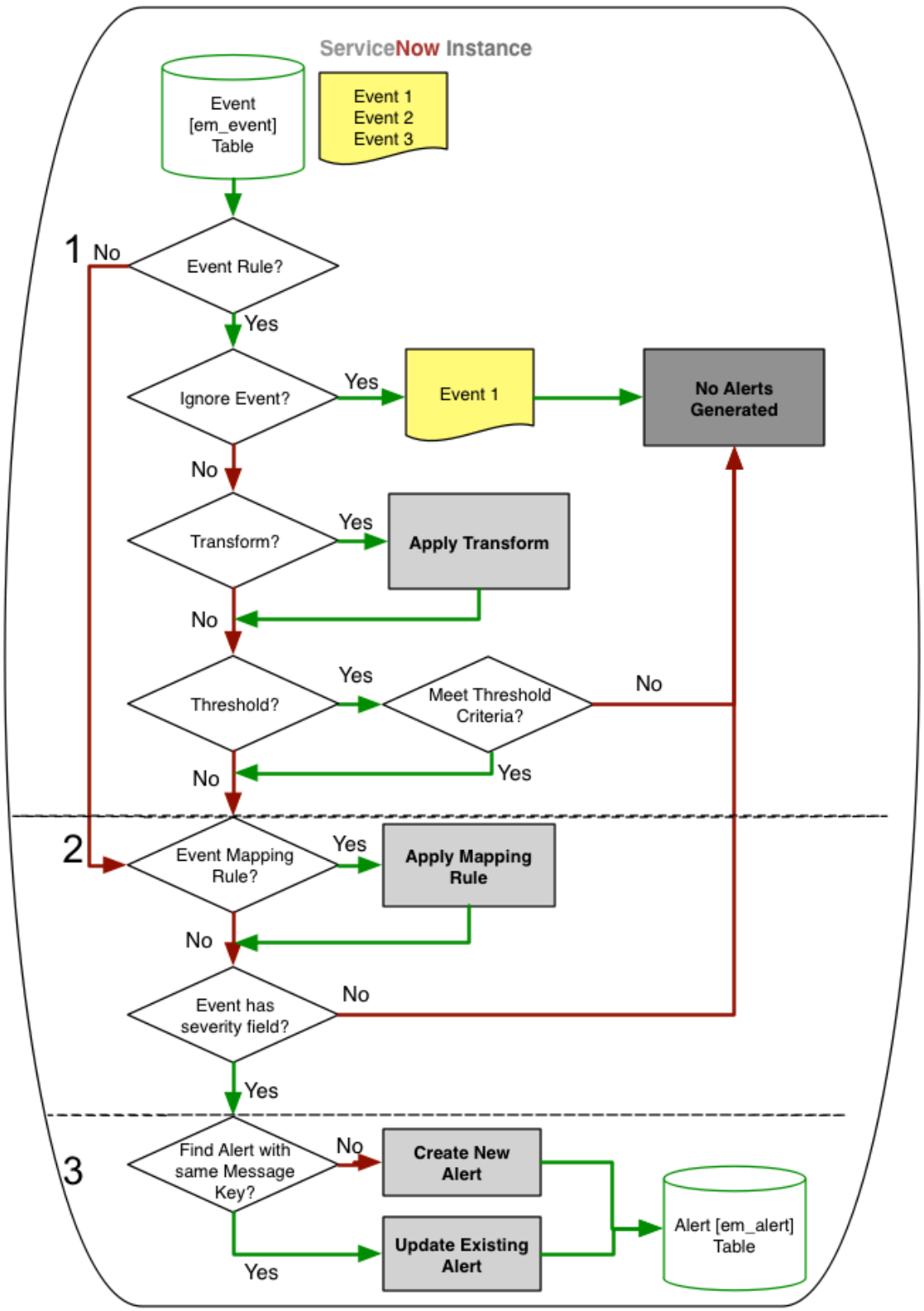
1. Ereignisregel abgleichen: Finden Sie die Ereignisregel mit der besten Übereinstimmung für ein Ereignis.

   Eine Regel wird abgeglichen, wenn die Quelle des Ereignisses mit der in einer vorhandenen Regel angegebenen Quelle übereinstimmt. Darüber hinaus wird eine Regel abgeglichen, wenn das Ereignis mit dem optionalen Regelfilter übereinstimmt und der Wert des Ereignisses „additional_info“ mit dem Filter „zusätzliche Informationen“ der Regel übereinstimmt. Eine Regel ohne Filter wird ignoriert, z. B. wenn der Quellfilter oder der Filter „zusätzliche Informationen“ fehlt. Wenn mehrere Regeln für denselben Ereignistyp definiert sind, verwenden Sie die Regelreihenfolge, um die Reihenfolge der Regelanwendung zu bestimmen.

2. Regel ignorieren: Wenn die Regel **Ignorieren** Kontrollkästchen ist aktiviert, es wird keine Warnung generiert. Das Event steht jedoch weiterhin zur Überprüfung und Nachbesserung zur Verfügung.
3. Transformationen Anwenden:
   - Wenn Umwandlungen definiert wurden, wenden Sie sie an.
   - Wenn Erstellungsparameter festgelegt sind, wenden Sie den zusätzlichen Inhalt an, der dem Benutzer in der Warnung angezeigt wird.
4. Schwellenwertakkumulation: Wenn im Abschnitt „Schwellenwert“ aktiv ausgewählt ist, akkumulieren Sie alle Ereignisse, bis der Schwellenwert erreicht ist, und generieren Sie dann eine einzelne Warnung für die Ereignisse.
5. Ereignisfeldzuordnung
   - Suchen Sie nach einer Event-Feldzuordnung, auch wenn keine Event-Regel vorhanden war.
   - Wenn eine Event-Feldzuordnung gefunden wird, wenden Sie die Zuordnungsinformationen an.
   - Wenn das Event nach den Event-Umwandlungen keinen Schweregrad aufweist, behalten Sie das Event zu Referenzzwecken bei und generieren Sie keine Warnung.
6. Warnungsgenerierung
   - Durchsuchen Sie die Warnungstabelle [em_alert] nach einem passenden Nachrichtenschlüssel.
   - Wenn ein passender Nachrichtenschlüssel vorhanden ist, aktualisieren Sie die Warnung entsprechend den Event-Informationen.
   - Wenn kein passender Nachrichtenschlüssel vorhanden ist, erstellen Sie eine Warnung.
   - Wenn ein anderes Event denselben übereinstimmenden Schlüssel aufweist, ordnen Sie die Events einer einzelnen Warnung zu.
   - Binden Sie die Warnung zur Ursachenanalyse an ein bestimmtes Konfigurationselement (Configuration Item, CI).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Workflow



Automatische Übersetzung

Ereignismanagement-Architektur

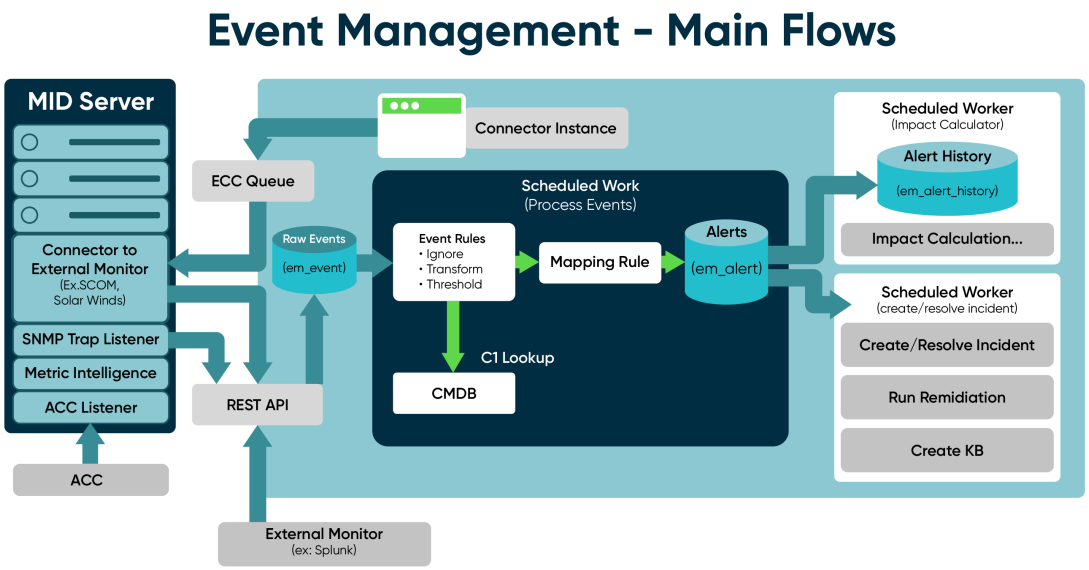
Ereignismanagement Die Architektur integriert die Datenerfassung, -Verarbeitung und -Warnung in einem einheitlichen System für eine optimierte Erkennung und Lösung von IT-Problemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur

Wenn Ereignisse auf verschiedenen Systemen auftreten, wird die MID-Server Die Connector-Instanz sendet sie an die Hauptinstanz. Ereignismanagement Generiert Warnungen, wendet Warnungsverwaltungsregeln an und priorisiert Warnungen für die Korrektur und Ursachenanalyse. Diese Informationen können in Dashboards, in der Warnungsliste in Alert Intelligence oder in einer Servicezuordnung angezeigt werden.

Ereignismanagement-Architektur



Ereignismanagement konfigurieren

Ereignismanagement-Administratoren verwalten Events, verwalten und überwachen Warnungen, fassen Warnungen zusammen und prüfen und überwachen den Status von Services mit dem Service Monitor des Betreiber-Arbeitsbereich s.

Ereignismanagement-Operatoren suchen nach Warnungen, analysieren sie und ergreifen Maßnahmen zur Lösung des zugrunde liegenden Problems.

Event Management für Anforderungen

Ereignismanagement Plugin (com.glideapp.itom.snac) erfordert ein separates Abonnement und muss von aktiviert werden ServiceNow Personal. Dieses Plugin enthält Demodaten und aktiviert zugehörige Plugins, wenn sie nicht bereits aktiv sind.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

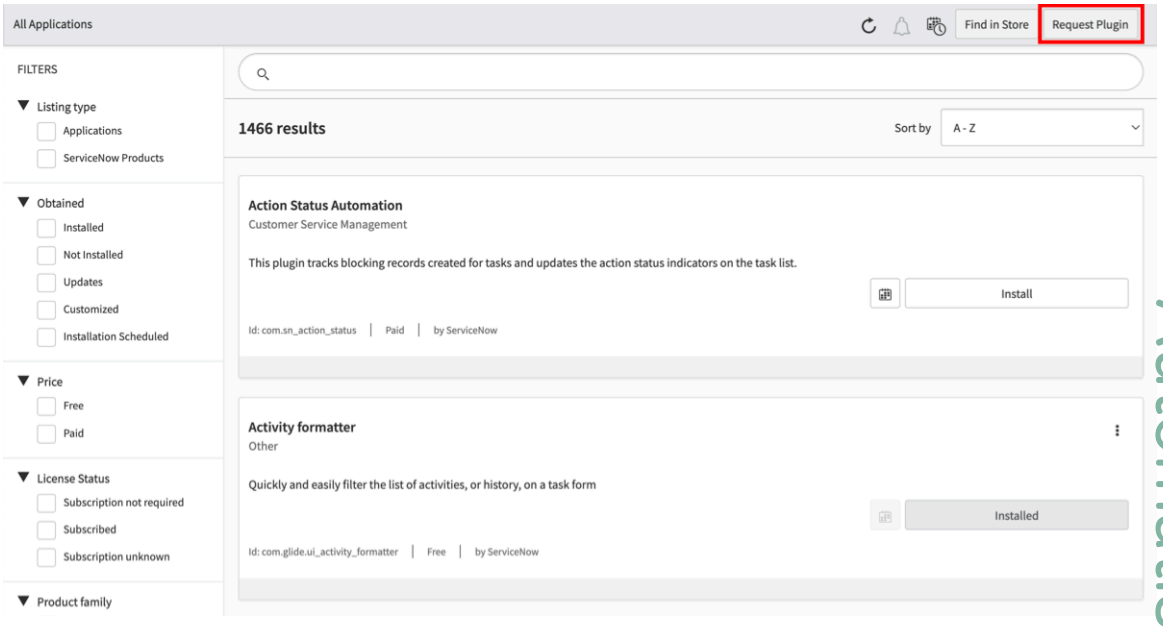
Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

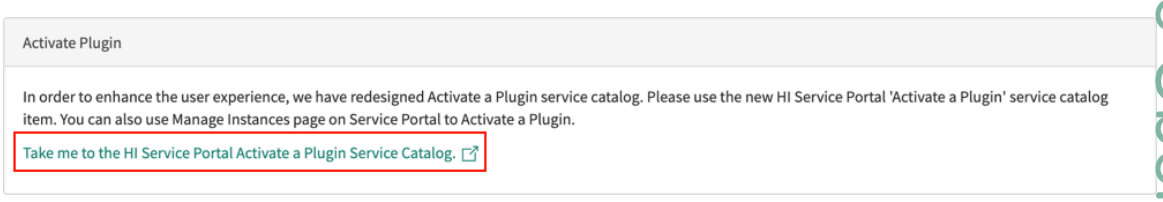
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins

Automatische Übersetzung

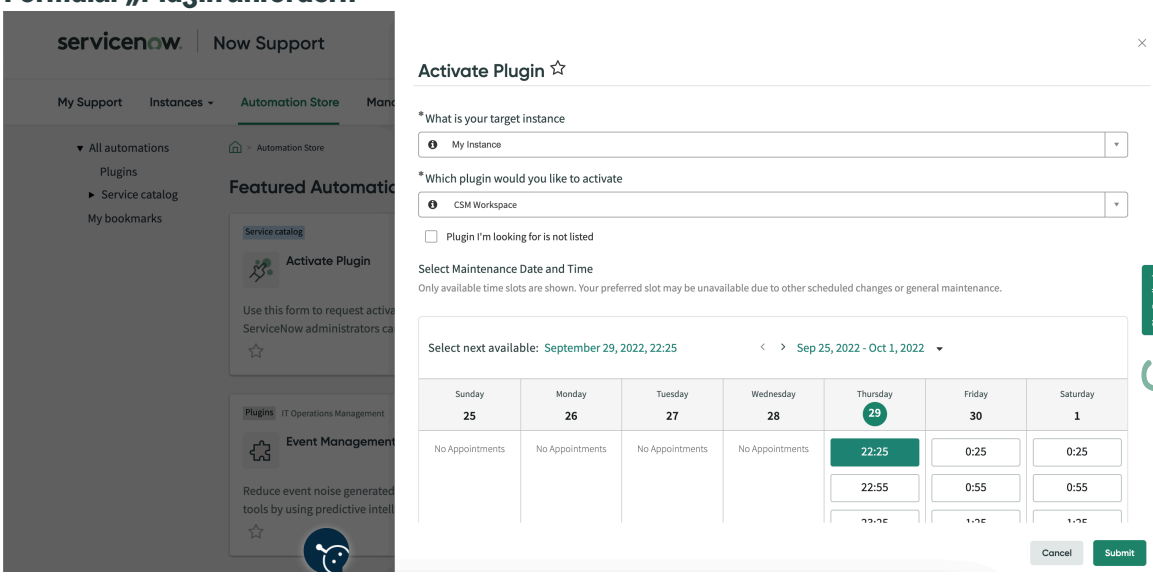
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement installieren

Laden Sie aus dem ServiceNow® Store die aktuellen Apps für die Anwendung Ereignismanagement (com.glideapp.itom.snac) herunter. Überprüfen Sie den ServiceNow® Store regelmäßig auf neue App-Versionen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Ereignismanagement installiert:

- Rollen
- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter Mit Ereignismanagement installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie die Anwendung ITOM-Integrität über die Filterkriterien und die Suchleiste.

   Wenn Sie die Anwendung nicht finden können, fordern Sie sie über den ServiceNow Store an.
3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation” die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von Plugins oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Ereignismanagement installieren können.
4. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

   (Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.
5. Wählen Sie **Installieren** aus.

Ereignismanagement-Leistung verbessern

Das Beschleuniger-Plugin Ereignismanagement stellt sicher, dass Ereignismanagement die Leistung auf hohem Niveau hält. Dieses Plugin ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die Tabellen *em_alert_history* und *em_impact_status* können sehr groß werden, was sich negativ auf die Leistung von Ereignismanagement auswirkt. Durch Installieren des Beschleuniger-Plugins Ereignismanagement stellen Sie sicher, dass Ereignismanagement die Leistung auf hohem Niveau hält. Das Plugin enthält Korrekturskripts, die fehlende Daten ausfüllen, Schlüsselfelder aktualisieren, um die Datengenauigkeit zu erhalten, und Indizes erstellen, um die Leistung zu verbessern. Diese Aktionen helfen dabei, große Datensätze zu optimieren und die Auswirkungen auf die Abfragegeschwindigkeit und die allgemeine Systemreaktionsfähigkeit zu reduzieren.

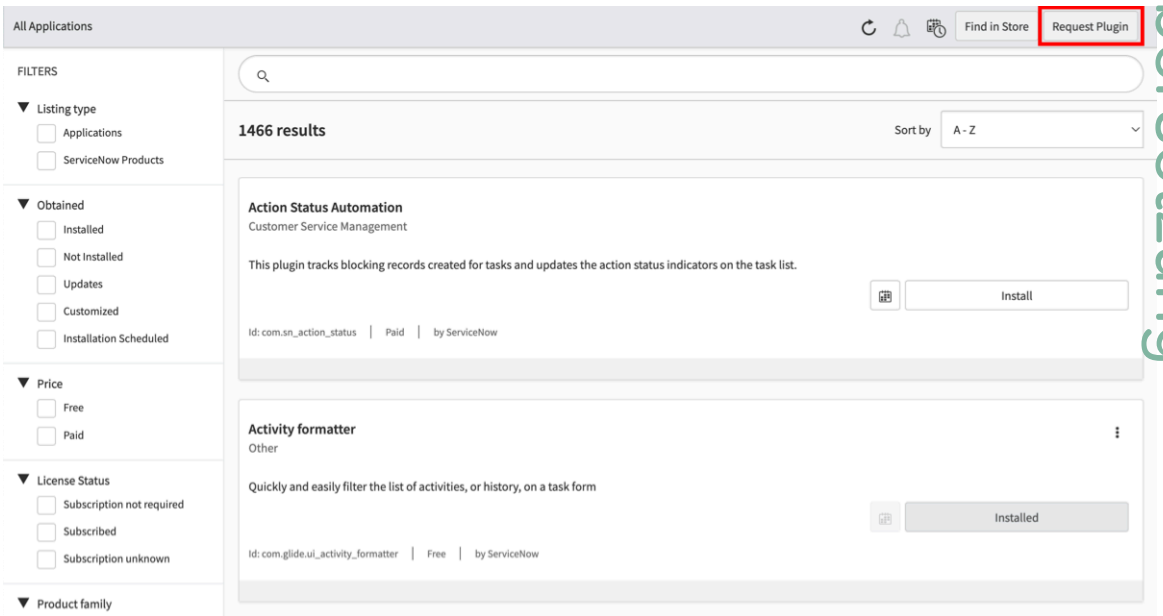
Beim Upgrade von einer früheren Version mit mehr als 5 Millionen Datensätzen in den Tabellen *em_alert_history* oder *em_impact_status* müssen Sie dieses Plugin manuell aktivieren. Wenn weniger als 5 Millionen Datensätze vorhanden sind, wird sie automatisch ausgeführt. Sie können diese Zahl anpassen, indem Sie die Eigenschaft *evt_mgmt.plugin_activation.table_max_size* ändern.

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Prozedur

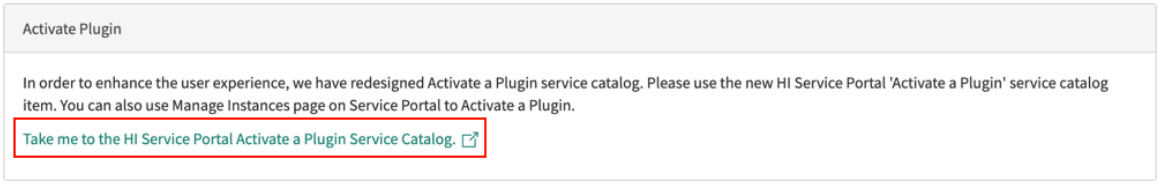
1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

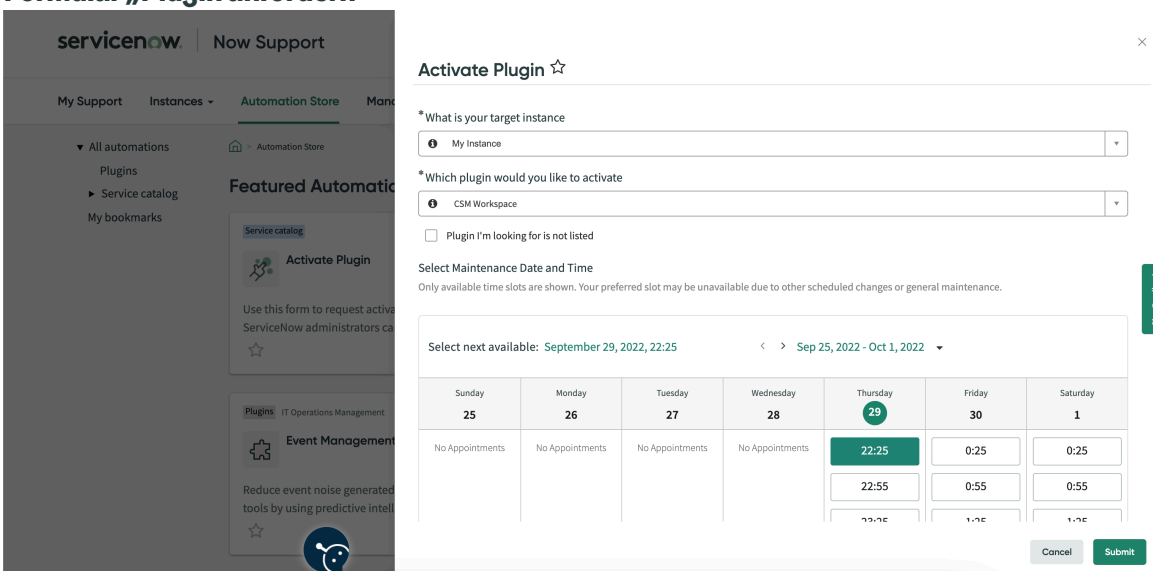
Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-artikel [KB0751715] in Now Support Knowledge Base an.

Setup von Ereignismanagement

Nach der Aktivierung von Ereignismanagement richten Sie es so ein, dass es Events empfängt und verarbeitet sowie Warnungen generiert und analysiert.

Einrichtung von Ereignismanagement ohne Guided Setup

Richten Sie Ereignismanagement ein, indem Sie diese Aufgaben in der folgenden Reihenfolge ausführen:

1. Konfigurieren Sie ein MID-Server Dient zum Empfangen und Verarbeiten von Ereignissen über MID-Server.
2. MID-Webserver erweiterung konfigurieren.
3. Konfigurieren Sie Konfigurieren Ereignismanagement Connectors.
4. Konfigurieren Ereignisfeldzuordnungen Und Warnungen werden an CIs gebunden Dient zum Verwalten der Warnungsgenerierung.
5. Warnungsverwaltungsregeln zum Auflösen von Warnungen, Ausführen und CI-Korrektur Für Warnungsmanagement.
6. Service-Mapping Anfordern Und erhalten Sie einen Top Down Discovery Zum Empfangen von CI-Beziehungen für Software und Hardware.
7. Konfigurieren Sie die Auswirkungsberechnung für Services, um die Priorität für die Warnungsauflösung festzulegen.
8. Konfigurieren Sie Warnungsgruppen, um zugehörige Warnungen zu konsolidieren.
9. Konfigurieren Sie das Plugin Predictive Intelligence (com.glide.platform_ml), um maschinelles Lernen und die Suche nach ähnlichen Warnungen zu ermöglichen.
10. Konfigurieren Sie gegebenenfalls alle anderen allgemeinen Aufgaben, die in diesem Abschnitt angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ereignismanagement unterstützt nicht das Erstellen von Incidents auf Remote-Instanzen.

Einrichtung von Ereignismanagement mit Guided Setup

Das Guided Setup für Ereignismanagement stellt eine Reihe von Aufgaben bereit, die Sie beim Konfigurieren von Ereignismanagement in Ihrer ServiceNow-Instanz unterstützen. Zum Öffnen Ereignismanagement Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**an. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Ereignismanagement während eines Plattform-Upgrades

Während eines Plattform-Upgrades werden weiterhin Ereignismanagement-Jobs ausgeführt, deren Flag für **sicheres Upgrade** als „true“ markiert ist.

Während eines Upgrades der Plattform funktionieren die Ereignismanagement-Connectors und rufen weiterhin Events ab. Die Events werden verarbeitet und mithilfe von Event-Regeln in eine Warnung umgewandelt. Wenn eine geeignete Warnungsverwaltungsregel vorhanden ist, wird eine Aufgabe erstellt. Die Auswirkungsberechnung wird jedoch während des Plattform-Upgrades nicht unterstützt. Beim Anwenden von Konfigurationsänderungen oder -Upgrades werden alle betroffenen MID-Server neu gestartet.

Hinweis: Ereignismanagement-Jobs, die vor Beginn des Plattform-Upgrades gestartet wurden, werden während des Upgrades weiterhin ausgeführt.

Folgendes Ereignismanagement Aufträge werden weiterhin als ausgeführt **Upgrade Safe** Kennzeichnung ist als markiert Wahr :

- Ereignismanagement – Connector-Ausführung
- Ereignismanagement –Update abgebrochen
- Ereignismanagement – Warteschlange für Warnungspriorität
- Ereignismanagement – Fluktuierende Warnungen schließen
- Ereignismanagement – Schwellenwertwarnung schließen
- Ereignismanagement – Bereichsbezogene Warnungsregelverwaltung0 Auswerten
- Ereignismanagement – Wartungsrechner
- Ereignismanagement – Events verarbeiten

Während des Plattform-Upgrades warten alle anderen Ereignismanagement-Jobs, bis das Plattform-Upgrade abgeschlossen ist.

Hinweis: Während eines Ereignismanagement-Plugin-Upgrades funktionieren nicht alle Ereignismanagement-Jobs.

MID-Webserver

Der MID-Webserver ist Teil der allgemeinen Infrastruktur des MID-Server s.

Die MID-Webserver erweiterung bietet Optionen für Authentifizierung und Datensicherheit und wird ausgeführt, solange sie aktiviert ist. Von der Erweiterung wird ein Webserver auf dem MID-Server gestartet, von dem Webanforderungen von externen Systemen verarbeitet werden. Die Rohdaten werden von einem Client oder mithilfe eines benutzerdefinierten Skripts an die Erweiterung übertragen. Die Daten werden vom MID-Server erfasst und dann zur ServiceNow-Instanz übertragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die MID-Webserver erweiterung unterstützt MID-Server-Cluster, die für Failover konfiguriert sind. Wenn Sie die Option für MID Server-Cluster auswählen, wird mit einem Algorithmus ermittelt, auf welchem MID-Server im Cluster die Erweiterung ausgeführt wird. Die Erweiterung kann nur auf einem MID-Server ausgeführt werden. Bei einem Ausfall des MID-Server s im Cluster, auf dem die MID-Webserver erweiterung ausgeführt wird, wird die Erweiterung automatisch auf dem sekundären MID-Server ausgeführt, der bei einem Ausfall des primären MID-Server s aktiviert wird.

Zugehörige Informationen

MID-Webserver erweiterung konfigurieren

Sichere MID-Webserver erweiterung konfigurieren

MID-Webserver erweiterung konfigurieren

Der MID-Webserver ist eine MID-Server erweiterung, die die Entwicklung von REST APIs zum Senden von Events und Metriken an den MID-Server ermöglicht. Die Erweiterung wird von anderen MID-Server-Erweiterungen genutzt, z. B. Metrikdaten, MID-WebService-Event-Listener und der Agent Client Collector-Websocket-Endpunkterweiterung.

Vorbereitungen

- Stellen Sie einen MID-Server bereit, und starten Sie ihn.
- Aktivieren Sie das MID-Webserver-Plugin [com.snc.sa.mid.webserver].

Erforderliche Rolle: agent_admin.

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector unterstützt die folgenden Authentifizierungsstrategien:

- **Schlüsselbasiert**: Nur für Abwärtskompatibilität (vor Zurich-Release). Weitere Informationen finden Sie unter Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren.
- **API-Schlüssel**: Siehe API-Schlüsselauthentifizierung für MID-Webserver konfigurieren.
- **mTLS**: Siehe MID-Webserver Und Agent-mTLS-Authentifizierung.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Erweiterungen** > **MID-Webserver**an.
2. In MID-Webserver Liste der Kontexte klicken Sie auf **Neu** .
3. Geben Sie die Werte im Formular „Ereignismanagement MID-Webserver erweiterung“ ein.
4. Klicken Sie auf **Speichern**, um die Daten zu speichern.
5. Starten Sie die MID-Webserver erweiterung neu, um Ihre Änderungen anzuwenden.
6. Navigieren zu **Alle** > **MID-Server** > **Erweiterungen** > **MID-Webserver** Und wählen Sie aus MID-Server Sie haben gerade erstellt.
7. Klicken Sie im Abschnitt **Zugehörige Links** auf **Start**, um die Erweiterung zu starten.

Sichere MID-Webserver erweiterung konfigurieren

Konfigurieren Sie einen TLS-Listener für zusätzliche Sicherheit und Verschlüsselung von Daten, die an die und von der MID-Webserver erweiterung übertragen werden. Greifen Sie über einen Java-Schlüsselspeicher auf einen privaten Schlüssel und ein Zertifikat (oder eine Zertifikatkette) zu, um sie während des TLS-Handshake zu verwenden, bei dem sich der MID-Webserver und der Client gegenseitig bestätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **MID-Server** > **Erweiterungen** > **MID-Webserver**an.
2. Wählen Sie **Neu**.
3. Wählen Sie im Feld **Authentifizierungstyp** einen zu verwendenden Authentifizierungstyp aus.
   - Schlüsselbasiert – Siehe Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren
   - Standard – Standardmäßige Authentifizierung mit Benutzername/Passwort
   - API-Schlüssel – Siehe API-Schlüsselauthentifizierung für MID-Webserver konfigurieren
   - mTLS – Siehe MID-Webserver Und Agent-mTLS-Authentifizierung
4. Wählen Sie entweder den einheitlichen MID-Schlüsselspeicher oder den Webserver-Schlüsselspeicher aus. Der einheitliche MID-Webserver-Schlüsselspeicher ist die effizienteste Option. Wenn Sie die Abwärtskompatibilität und die Möglichkeit zum Speichern von Schlüsselpaaren in einem zusätzlichen Schlüsselspeicher aktivieren möchten, verwenden Sie den Webserver-Schlüsselspeicher (mit dem Sie auch den einheitlichen MID-Schlüsselspeicher verwenden können).

Option	Beschreibung
Einheitlicher MID-Schlüsselspeicher	**a.** Aktivieren Sie das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden**. **b.** Geben Sie einen Aliasnamen in das Feld **Schlüsselspeicher-Zertifikatalias** ein oder lassen Sie das Feld leer, um den Standardalias des Schlüsselspeichers zu verwenden. Weitere Informationen finden Sie unter **Installieren Sie anwenderdefinierte Zertifikate im zentralen Schlüsselspeicher DES MID-Servers** Abschnitt in Einheitlicher Schlüsselspeicher FÜR MID-Server . **Wichtig:** Wenn Sie das Feld **Schlüsselspeicher-Zertifikatalias** leer lassen, wird bei Clients, bei denen eine Verbindung hergestellt wird, die Zertifikatverifizierung übersprungen. Stattdessen wird vom MID-Server sein eigenes selbstsigniertes Zertifikat verwendet.
Webserver-Schlüsselspeicher	**a.** Deaktivieren Sie das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden**. **b.** Geben Sie einen Aliasnamen in das Feld **Schlüsselspeicher-Zertifikatalias** ein oder lassen Sie das Feld leer, wenn Sie einen einzigen Alias in diesem Schlüsselspeicher haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	c. Wenn sich das Passwort für den privaten Schlüssel des erforderlichen Alias vom Schlüsselspeicher-Passwort unterscheidet, geben Sie den Alias im Feld **Schlüsselpasswort des Schlüsselspeichers** an. **d.** Geben Sie in dem Feld **Schlüsselspeicher-Passwort** das Passwort des Schlüsselspeichers ein.

Zugehörige Informationen

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet

Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren

Bieten Sie Ihrer MID-Webservererweiterung zusätzliche Sicherheit, indem Sie schlüsselbasierte Authentifizierung verwenden. Generieren Sie ein Authentifizierungstoken, das im Autorisierungsheader eingehender Client-Anforderungen gesendet werden soll.

Vorbereitungen

Hinweis: Dieses Verfahren dient nur der Kompatibilität mit Releases vor Zurich. Weitere Informationen zum Verfahren im Release Zurich für die Konfiguration des MID-Webserver s finden Sie unter MID-Webserver erweiterung konfigurieren.

- Stellen Sie einen MID-Server bereit, und starten Sie ihn.
- Konfigurieren Sie eine MID-Webserver-Erweiterung und wählen Sie „Schlüsselbasiert“ als Authentifizierungstyp aus. Weitere Informationen finden Sie unter Konfigurieren Sie die MID-Webservererweiterung .

Erforderliche Rolle: agent_admin

Prozedur

1. Erstellen Sie mit einem Skriptprogramm ein Token, indem Sie mithilfe definierter Elemente der HTTP/HTTPS-Anforderung (HTTP-Verb, Inhaltstypheader und Anforderungspfad, die vom Client empfangen werden, der auf die Endpunkte der MID-Webserver erweiterung zugreift) eine Zeichenfolge erstellen.
2. Erstellen Sie einen HMAC (Hash Message Authentication Code) der Zeichenfolge, indem Sie die generierte Zeichenfolge mit dem automatisch generierten geheimen Schlüssel signieren, der unter **Geheimer Key** angezeigt wird.
   Dieser Schlüssel ist pro Kontext eindeutig.
3. Geben Sie Informationen an, um dieses Authentifizierungstoken im Autorisierungsheader der Anforderung zu übermitteln.

Element	Wert
Pfad zu einer Webservice-API zum Senden von Rohdaten	URL-Format: https://<MID Server-IP-Adresse>:<Portnummer>/api/mid/sa/metrics

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Wert
	Verwenden Sie eine Portnummer, die einer der in der Webservererweiterung eingerichteten Portnummern entspricht. Beispiel: http://10.10.10.10:8097/api/mid/sa/metrics
Anforderungstyp	POST
Datumsformat	`yyyy-MM-dd'T'HH:mm:ss.SSS'Z'` Beispiel: 2016-06-08T20:54:58.917Z
Content-Type	Anwendung/JSON

Verwenden Sie die folgenden Anforderungselemente, um die erforderliche Zeichenfolge zu generieren: HTTP-Verb, Inhaltstyp, Datum und Anforderungspfad. Geben Sie diese Elemente an, und platzieren Sie sie in dieser Reihenfolge:

- HTTP-Verb + „\n“ +
- Inhaltstyp + „\n“ +
- Datum + „\n“ +
- Anforderungspfad

In diesem Beispiel lautet die Anforderungszeichenfolge:

```
POST\napplication/json\n2016-06-08T20:54:58.917Z\n/api/mid/sa/metrics
```

Für die Zeitstempelanforderung ist zur Authentifizierung der Anforderung ist ein gültiger Zeitstempel erforderlich, der den HTTP-Datumsheader verwendet. Stellen Sie sicher, dass der Zeitstempel nicht mehr als 15 Minuten von der Zeit des MID Servers abweicht.

Example: So generieren Sie den HMAC der Zeichenfolge, die definierte Elemente der HTTP/HTTPS-Anforderung verwendet, mit Java

```
package sample;
import com.glide.util;
import java.security.SignatureException;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

public class AuthUtil {

private static final String HMAC_SHA1_ALGORITHM = "HmacSHA1";

/***
 * Generates base64-encode the HMAC(Hash Message Authentication Code) of input data
 *
 * @param data
 * @param key
 * @return
 * @throws java.security.SignatureException
 */
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
public static String signData(String data, String key) throws java.security.SignatureException {
 String result;
 try {
  // get an hmac_sha1 key from the raw key bytes
  SecretKeySpec signingKey = new SecretKeySpec(key.getBytes(), HMAC_SHA1_ALGORITHM);

  // create hmac_sha1 Mac instance and initialize with the signing key
  Mac = Mac.getInstance(HMAC_SHA1_ALGORITHM);
  mac.init(signingKey);

  // compute the hmac on input data bytes
  byte[] rawHmac = mac.doFinal(data.getBytes("UTF-8"));

  // base64-encode the hmac
  result = Base64.encode(rawHmac);

 } catch (Exception e) {
  throw new SignatureException("Failed to generate HMAC : " + e.getMessage());
 }
 return result;
}
}
```

API-Schlüsselauthentifizierung für MID-Webserver konfigurieren

Authentifizieren Sie von Clients eingehende Anforderungen an die MID-Webserver erweiterung mithilfe der API-Schlüsselauthentifizierung. Die API-Authentifizierung ist eine sichere und einfache Möglichkeit, Ihre Anforderung zu authentifizieren. Sie können einen MID-Webserver-API-Schlüssel erstellen oder ändern.

Vorbereitungen

Erstellen Sie eine MID-Webserver erweiterung, um die API-Schlüsselauthentifizierung zu verwenden, wie in MID-Webserver erweiterung konfigurieren beschrieben. Stellen Sie sicher, dass Sie im Feld **Authentifizierungstyp** der Erweiterung **API-Schlüssel** auswählen.

Erforderliche Rolle: event_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Sie in einer Instanz maximal 10 API-Schlüssel erstellen. Um diese Zahl zu ändern, ändern Sie auf der Seite „Systemeigenschaften“ den Wert der Eigenschaft `mid.webserver.max.api.keys`.

Wenn Sie in der globalen Domäne arbeiten, während die Domänentrennung aktiviert ist, sind API-Schlüssel für alle Erweiterungen verfügbar, unabhängig von ihrer Domäne. Wenn Sie in einer bestimmten Domäne arbeiten, stehen API-Schlüssel für Erweiterungen in dieser Domäne, den übergeordneten Domänen und der globalen Domäne zur Verfügung.

Sie können API-Schlüssel so konfigurieren, dass sie an einem bestimmten Datum ablaufen.

Wenn Sie eine neue Erweiterung mit API-Schlüsselauthentifizierung erstellen (oder eine vorhandene aktualisieren, um die API-Schlüsselauthentifizierung zu verwenden), wird vom System nach einem verfügbaren API-Schlüssel für die Erweiterung gesucht. Wenn kein API-Schlüssel verfügbar ist, wird vom System einer erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Profile und Bereitstellungen** > **MID-Webserver API-Schlüssel**an.
2. Erstellen Sie entweder einen neuen API-Schlüssel oder ändern Sie einen vorhandenen API-Schlüssel.
   - So erstellen Sie einen neuen API-Schlüssel:
     a. Wählen Sie **Neu**.
     b. Füllen Sie im Formular „MID-Webserver API-Schlüssel“ die Felder aus.

Formular „MID-Webserver API-Schlüssel“

Feld	Beschreibung
Name	Name für den API-Schlüssel
Aktiv	Option zur Aktivierung des API-Schlüssels
Authentifizierungsschlüssel	Schreibgeschützter codierter Wert des Authentifizierungsschlüssels. Erst nach der Konfiguration des Schlüssels wird ein Wert angezeigt.
Läuft ab	Option zum Festlegen eines Ablaufdatums für den API-Schlüssel. Abgelaufene, deaktivierte oder gelöschte API-Schlüssel werden von der Webservererweiterung nicht akzeptiert.

     c. Wählen Sie **Absenden** aus, um den API-Schlüssel zu speichern.

     Der API-Schlüssel wird auf der Seite „MID-Webserver API-Schlüssel“ angezeigt.

   - So ändern Sie einen vorhandenen API-Schlüssel:
     a. Navigieren zu **MID-Server** > **Profile und Bereitstellungen** > **MID-Webserver API-Schlüssel**an.
     b. Wählen Sie auf der Seite einen API-Schlüssel aus.
     c. Wählen Sie im Abschnitt **Zugehörige Links** die Option **API-Schlüssel anzeigen** aus.
     d. Kopieren Sie den API-Schlüssel, der im Dialogfeld „MID-Webserver“ angezeigt wird.

     Wenn Sie eine Verbindung mit einer MID-Webserver erweiterung herstellen, die mit der API-Schlüsselauthentifizierung konfiguriert ist, fügen Sie einen API-Schlüssel, auf den die Erweiterung zugreifen kann, im Autorisierungsheader der Anforderung im folgenden Format ein:

     `Key <API_KEY>`

     Dabei ist `<API_KEY>` der Wert des API-Schlüssels, der nach Auswahl von **API-Schlüssel anzeigen** angezeigt wird.

     e. Wählen Sie **Absenden** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-Webserver Und Agent-mTLS-Authentifizierung

Die gegenseitige Authentifizierung mit dem Transport Layer Security Protocol (mTLS) ist ein sicheres, zertifikatbasiertes Authentifizierungsschema. Bei mTLS wird der Server (der MID-Webserver Erweiterung) und der Client (der Agent) authentifizieren sich gegenseitig.

Die TLS-Authentifizierung erfolgt, wenn ein Client (z. B. ein Webbrowser) den Server authentifiziert, auf den er zugreift, indem er das vom Server präsentierte Zertifikat validiert. Vom Client wird überprüft, ob das Zertifikat (oder die Zertifikatkette) von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert ist. Der Client muss Zugriff auf ein Paket von CA-Zertifikaten haben, mit dem das Serverzertifikat validiert wird.

Wenn mTLS konfiguriert ist, wird vom Client ein Zertifikat oder eine Zertifikatkette dem Server vorgelegt und vom Server wird der Client auf die gleiche Weise authentifiziert wie der Server vom Client (gegenseitige Authentifizierung).

Bei einigen TLS-Implementierungen wird nicht nur die Zertifikatsignatur überprüft, sondern auch der Sperrstatus des Zertifikats. In diesen Fällen wird das Online Certificate Status Protocol (OCSP) verwendet. In diesem Protokoll sendet die verifizierende Partei eine Anforderung an den OCSP Responder, der von der CA eingerichtet wurde, die das vorgelegte Zertifikat ausgestellt hat. (Die Adresse des Beantworters ist normalerweise in die VON DER CA ausgestellten Zertifikate eingebettet.) Die Antwort gibt an, ob das präsentierte Zertifikat widerrufen wurde.

Bevor Sie mTLS aktivieren, müssen Sie zuerst Schlüssel und Zertifikate erstellen und die PEM-Datei auf Ihrem installieren MID-Server, Und verbinden Sie den Service Desk-Mitarbeiter mit Ihrem MID-Server.

Zugehörige Informationen

MID-Webserver erweiterung konfigurieren

mTLS-Authentifizierung für einen MID-Webserver konfigurieren

Erstellen Sie Schlüssel und Zertifikate

Erstellen Sie Schlüssel und Zertifikate in Ihrem Stammverzeichnis, um das Setup von Transport Layer Security (TLS) zu aktivieren. Das TLS-Setup ist erforderlich, bevor Sie mTLS auf dem konfigurieren können MID-Webserver Und Service Desk-Mitarbeiter.

Vorbereitungen

- Stellen Sie sicher, dass im zentralen MID-Schlüsselspeicher keine Schlüssel installiert sind, indem Sie den folgenden Befehl ausführen:

  ```
  bin/scripts/manage-certificates.(sh/bat) -l
  ```

  Wenn keine Schlüssel installiert sind, lautet die Ausgabe: `Standardvorgabenederhandle`

- Erklären Sie Ihr für ungültig MID-Server.

  Wenn in der Ausgabe zusätzliche Schlüssel vorhanden sind, installieren Sie diese Schlüssel nach dem Ungültigmachen von neu MID-Server.

- Stellen Sie sicher, dass MID-Server Ist mit der Instanz verbunden.
- Wählen Sie ein Verzeichnis aus, in dem Sie Zertifikate erstellen möchten, das als bezeichnet werden soll *root*Verzeichnis.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die im folgenden Verfahren angegebenen Befehle sind nur für einen Centos7-Host relevant. Verwenden Sie bei der Arbeit mit einem anderen Betriebssystem die für Ihren Host relevanten Befehle.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Erstellen Sie in Ihrem Stammverzeichnis Unterverzeichnisse für Ihre Zertifikate.

```
mkdir -p labca labmid labacc;
```

2. In Ihrem Stammverzeichnis:

   a. Generieren Sie ein anwenderdefiniertes Zertifizierungsberechtigungsschlüsselpaar.

```
openssl ecparam -list_curves;
openssl ecparam -out labca/ec-labcakey.pem -name prime256v1 -genkey;
ls labca/;
```

   Die generierte Ausgabe ist ec-labcakey.pem Datei.

   b. Führen Sie die folgenden Befehle aus:

```
openssl ecparam -in labca/ec-labcakey.pem -text -noout;
openssl req -x509 -new -nodes -key labca/ec-labcakey.pem -sha512 -days 365 -out
 labca/labcacert.pem -subj "/C=<country>/ST=<state>/L=<location>/O=<organization>
 Lab/OU=<organization unit>/CN=<cn abbreviation>";
openssl verify labca/labcacert.pem;
```

   Die generierte Ausgabe lautet:

   - Labca/labcacert.pem: C = <country>, ST = <state>, L = <location>, O = <organization>, OU = <organization unit>, CN = <cn abbreviation>
   - Fehler 18 bei Tiefensuche 0: Selbstsigniertes Zertifikat
   - OK

   Hinweis: Die Fehler Nachricht kann ignoriert werden.

3. Bereiten Sie den vor MID-Webserver Schlüssel und Zertifikat.

   a. Führen Sie die folgenden Befehle im Stammverzeichnis aus:

```
sudo cp -a labca/labcacert.pem /etc/pki/ca-trust/source/anchors/;
sudo update-ca-trust extract;
openssl verify labca/labcacert.pem
```

   Die generierte Ausgabe lautet: Labca/labcacert.pem: OK

   b. Führen Sie den Befehl aus „Hostname –-all-fqdns“ Um alle gültigen Hostnamen für die spezifische VM abzurufen.

   c. Führen Sie die folgenden Befehle aus:

```
openssl req -new -newkey rsa:4096 -keyout labmid/rsa-labmidkey.pem -sha512 -nodes
 -out labmid/mid.csr -subj
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"/C=<country>/ST=<state>/L=<location>/O=<organization>/OU=<organization
unit>/CN=<hostname>";
openssl x509 -req -days 365 -in labmid/mid.csr -CA labca/labcacert.pem
-CAkey labca/ec-labcakey.pem -CAcreateserial -extensions SAN -extfile
<(cat /etc/pki/tls/openssl.cnf <(printf "\n[SAN]\nsubjectAltName=DNS:<hostname>"))
-out labmid/mid.crt;
```

Geben Sie den FQDN als ein `<hostname>` Wert im vorherigen Befehl. Wenn der Befehl mehr als einen fqdn-Wert zurückgibt, verwenden Sie den Wert im folgenden Format: hostname.domain.domain.com .

Die generierte Ausgabe lautet: Signatur OK Betreff=/C=<country>/ST=<state>/ L=<location>/O=<organization>/OU=<organization unit>/CN=<MID-Server-Host-fqdn>: Privater CA-Schlüssel wird abgerufen

4. Kombinieren Sie in Ihrem Stammverzeichnis die Schlüssel- und Zertifizierungsdateien in einer Datei mit dem Namen Mid.Pem .

```
cat labmid/rsa-labmidkey.pem labmid/mid.crt > labmid/mid.pem;
```

Nächste Maßnahme

Installieren Sie die PEM-Datei im zentralen MID-Schlüsselspeicher, und richten Sie den ein MID-Webserver.

Installieren Sie die PEM-Datei im zentralen MID-Schlüsselspeicher, und richten Sie den ein MID-Webserver

Installieren Sie die PEM-Datei im zentralen MID-Schlüsselspeicher, und richten Sie den ein MID-Webserver Um die Konfiguration von mTLS auf Ihrem zu aktivieren MID-Webserver Und Service Desk-Mitarbeiter.

Vorbereitungen

Kopieren Sie Labmid/Mid.Pem Datei (erstellt in Erstellen Sie Schlüssel und Zertifikate Verfahren) an Ihren MID-Webserver Hostverzeichnis.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Greifen Sie auf zu Service Desk-Mitarbeiter Unterverzeichnis unter MID-Server Hostverzeichnis von .
2. Führen Sie die folgenden Befehle aus:

```
bin/scripts/manage-certificates.sh -a midwss /<path>/mid.pem;
bin/scripts/manage-certificates.sh -l;
```

Der relevante Teil der Ausgabe ist: „Defaultsecuritypairhandle,midwss“

3. Validieren Sie Ihren MID-Server In der Instanz.
4. Wählen Sie aus MID-Server Wählen Sie in der -Instanz aus **Richten Sie den ACC-Listener ein** .
Ein neuer MID-Webserver Wird erstellt.
5. Navigieren Sie zu neu erstellt MID-Webserver Datensatz (*`ecc_agent_ext_context_webserver`*) In der Instanz.
6. Wählen Sie in der -Instanz die aus MID-Webserver Und legen Sie fest **Schlüsselspeicher-Zertifikatalias** Wert bis **Mitte der Zeit** .
7. Wählen Sie **Speichern**.
8. Starten Sie neu MID-Webserver.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Webserver Mit TLS.

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Webserver Mit TLS

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Webserver Um die Konfiguration von mTLS auf Ihrem zu aktivieren MID-Webserver Und Service Desk-Mitarbeiter.

Vorbereitungen

Stellen Sie sicher, dass Sie die PEM-Datei installiert und eingerichtet haben MID-Webserver. Details finden Sie unter Installieren Sie die PEM-Datei im zentralen MID-Schlüsselspeicher, und richten Sie den ein MID-Webserver.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Fügen Sie hinzu Labcacert.pem Datei im Truststore Ihres Agent-Hosts.

```
sudo cp -a /<path>/<to>/labcacert.pem /etc/pki/ca-trust/source/anchors/;
sudo update-ca-trust extract
openssl verify /<path>/<to>/labcacert.pem
```

   Die generierte Ausgabe ist /<path>/labcacert.pem: OK

2. Konfigurieren Sie acc.yml Datei zur Verwendung von TLS.

   a. Legen Sie fest *`insecure-skip-tls-verify`*Eigenschaft bis **Falsch** .

   b. Legen Sie fest *`backend-url`*Eigenschaft zur Verwendung von MID-Server FQDN von .

      Back-End-url="wss://<MID-Server-fqdn>:<MID-Webserver-Port>/WS/Events"

3. Starten Sie den Service Desk-Mitarbeiter neu.

```
systemctl restart acc;
```

4. Überprüfen Sie in den Protokollen, ob der Service Desk-Mitarbeiter mit verbunden ist MID-Server.

Nächste Maßnahme

mTLS-Authentifizierung für einen MID-Webserver konfigurieren.

mTLS-Authentifizierung für einen MID-Webserver konfigurieren

Verbessern Sie die Sicherheit in der MID-Webserver erweiterung, indem Sie die mTLS-Authentifizierung aktivieren.

Vorbereitungen

Stellen Sie sicher, dass Sie Transport Layer Security (TLS) für den Service Desk-Mitarbeiter aktiviert haben. Details finden Sie unter Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet.

Stellen Sie sicher, dass *`insecure-skip-tls-verify`*Parameter in acc.yml Konfigurationsdatei ist auf festgelegt **Falsch** . Für Details zu acc.yml Datei, siehe Konfigurationsdateioptionen.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die MID-Webserver Die Erweiterung durchsucht die folgenden Standorte (in der angegebenen Reihenfolge), um auf den Truststore-Speicherort und das Passwort zuzugreifen:

- Truststore-Speicherort: Die JVM-Systemeigenschaft *mid.webserver.truststore.path*.

  Wenn diese Eigenschaft leer ist, wird von der Erweiterung der Speicherort aus der JVM-Systemeigenschaft *javax.net.ssl.trustStore* abgerufen.

  Wenn kein Speicherort angegeben ist, wird standardmäßig der absolute Pfad der cacerts-Datei der JRE verwendet, auf der der MID-Server ausgeführt wird.

- Truststore-Passwort: Das Feld **Truststore-Passwort** im Erweiterungsformular in der Instanz.

  Wenn dieses Feld leer ist, wird vom System das Passwort aus der JVM-Systemeigenschaft *javax.net.ssl.trustStorePassword* abgerufen.

  Wenn kein Speicherort angegeben ist, lautet das Passwort standardmäßig *changeit*.

Prozedur

1. Navigieren Sie zum Stammordner von MID-Server.
2. Führen Sie den folgenden Befehl aus, um Ihr Zertifikat dem MID Trust Store hinzuzufügen:

   ```
   ./jre/bin/keytool -importcert -file /etc/pki/ca-trust/source/anchors/labcacert.pem
    -destkeystore ./jre/lib/security/cacerts -alias mtlsca
   ```

3. Geben Sie Ein **Änderung** Wenn Sie zur Eingabe eines Passworts aufgefordert werden.
4. Wählen Sie Aus **ja** Im Bestätigungsnachrichtenfenster, um anzugeben, dass Sie dem Zertifikat vertrauen.
5. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass Ihr Zertifikat erfolgreich dem MID-Truststore hinzugefügt wurde.

   ```
   ./jre/bin/keytool -list -keystore ./jre/lib/security/cacerts -alias mtlsca
   ```

6. Geben Sie Ein **Änderung** Wenn Sie zur Eingabe eines Passworts aufgefordert werden.
7. In MID-Server Wrapper-Konfigurationsdatei überschreiben (Wrapper-override.conf , Befindet sich in Startseite/Konf. Verzeichnis von MID-Server), konfigurieren Sie den Widerruf von Clientzertifikaten in *mid.webserver.cert.revocation.check.enabled*Eigenschaft.
   - Wenn Sie ein anwenderdefiniertes internes Zertifikat haben, legen Sie auf fest **Falsch** Durch Hinzufügen der folgenden Zeile zu Conf/Wrapper-override.conf Datei auf dem MID-Server:

     ```
     wrapper.java.additional.4=-Dmid.webserver.cert.revocation.check.enabled=false
     ```

   - Beim Aktivieren dieser Eigenschaft (**Wahr**), konfigurieren Sie *mid.webserver.ocsp.responder.url*Eigenschaft mit der OCSP-Responder-URL. Dieser Wert überschreibt jede im Zertifikat eingebettete URL.
8. Wenn Sie Eigenschaften in der Konfigurationsdatei für die Wrapper-Überschreibung geändert haben, starten Sie den MID-Server neu.
9. Auf Ihrem ServiceNow®-Instanz, greifen Sie auf zu MID-Server Zeichnen Sie den Wert von auf, und ändern Sie ihn **Authentifizierungstyp** Feld bis **MTLs** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Starten Sie neu MID-Webserver.
11. Überprüfen Sie, ob MID-Webserver Und websocket-Endpunkt werden ausgeführt.

Nächste Maßnahme

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet.

Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet

Bevor Sie die mTLS-Authentifizierung für den Agent konfigurieren, müssen Sie eine Reihe von Befehlen ausführen, die die Konfiguration der TLS-Authentifizierung (Transport Layer Security) ermöglichen.

Vorbereitungen

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben:

1. Erstellen Sie Schlüssel und Zertifikate
2. Installieren Sie die PEM-Datei im zentralen MID-Schlüsselspeicher, und richten Sie den ein MID-Webserver
3. Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Webserver Mit TLS
4. mTLS-Authentifizierung für einen MID-Webserver konfigurieren
5. Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Generieren Sie einen Schlüssel für Ihren Service Desk-Mitarbeiter.

```
openssl ecparam -out labacc/acc.key -name prime256v1 -genkey
```

2. Generieren Sie eine Zertifikatanforderung für Ihren Service Desk-Mitarbeiter im folgenden Format:

```
openssl req -new -key labacc/acc.key -out labacc/acc.csr -subj
 "/C=<country>/ST=<state>/L=<location>/O=<organization>/OU=<organization
 unit>/CN=<cn abbreviation>/emailAddress=<email address>"
```

   Zum Beispiel:

```
openssl req -new -key labacc/acc.key -out labacc/acc.csr
 -subj "/C=US/ST=NC/L=Raleigh/O=ServiceNow/OU=ITOM
 Lab/CN=acclinux/emailAddress=john.smith@servicenow.com"
```

3. Generieren Sie ein signiertes Zertifikat für Ihren Service Desk-Mitarbeiter.

```
openssl x509 -req -days 365 -in labacc/acc.csr -CA labca/labcacert.pem -CAkey
 labca/ec-labcakey.pem -CAcreateserial -extensions client -out labacc/acc.crt
```

4. In Laborwert Ordner, kopieren Sie Ihre Schlüssel- und Zertifikatdateien auf die virtuelle Maschine des Agent-Hosts.

```
cp ./acc.key <agent host config folder>
cp ./acc.crt <agent host config folder>
```

   Die Pfade des Konfigurationsordners hängen von Ihrem Betriebssystem ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Linux: /Etc/servicenow/Agent-Client-Collector/
- Windows: C:\ProgramData\servicenow\Agent-Client-Collector\config\
- macOS: /Library/Application\ Support/servicenow/Agent-Client-Collector/

5. Navigieren Sie zu dem Speicherort, an den Sie kopiert haben .Schlüssel Und .crt Dateien von.
6. Führen Sie die folgenden Befehle aus, um die Leseberechtigungen der Dateien zu aktualisieren und dem Service Desk-Mitarbeiter zu ermöglichen, daraus zu lesen.
   - Linux:
     a. Chown servicenow:servicenow acc.key
     b. Chmod 0400 acc.key
   - Windows:
     a. Wählen Sie aus, und halten Sie (oder klicken Sie mit der rechten Maustaste) .Schlüssel Datei und wählen Sie aus **Sicherheit** Registerkarte in den Dateieigenschaften.
     b. Fügen Sie hinzu *servicenow*Anwender zur Liste der Anwender mit Lesezugriff auf die Datei.
   - macOS:
     a. Chown _servicenow:_servicenow acc.key
     b. Chmod 0400 acc.key

   Hinweis: Der Service Desk-Mitarbeiter muss mit dem standardmäßigen servicenow-Anwender ausgeführt werden.

7. Fügen Sie in der Konfigurationsdatei ACC.yml die folgenden Parameter hinzu, um den Pfad zu Ihren Schlüssel- und Zertifikatdateien anzugeben.

```
key-file: "<path to acc.key file>/acc.key"
cert-file: "<path to acc.cert file>/acc.crt"
```

8. Starten Sie den Service Desk-Mitarbeiter neu.
   - Linux: Systemctl Neustart gemäß
   - Windows:
     a. Öffnen Sie die Anwendung Services.
     b. Wählen Sie aus, und halten Sie (oder klicken Sie mit der rechten Maustaste) Agent Client Collector Eintrag und auswählen **Starten Sie Neu** .
   - macOS:
     a. Launchctl entladen – W /Library/LaunchDaemons/com.sn.acc.plist
     b. Launchctl load – W /Library/LaunchDaemons/com.sn.acc.plist
9. Überprüfen Sie die Protokolle, um sicherzustellen, dass der Service Desk-Mitarbeiter über TLS eine Verbindung zur Instanz herstellen konnte.

   Agent Client Collector Protokolle sind zugänglich von:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Linux: /Var/log/servicenow/Agent-Client-Collector/acc.log
- Windows: Der von angegebene Standort `Protokolldatei` Konfigurationskennzeichnung. Der Standardspeicherort lautet: C:/ProgramData/ServiceNow/agent-client-collector/log/acc.log.

  Wenn das Verzeichnis C:/ProgramData ausgeblendet ist (z. B. bei älteren Windows-Versionen), ändern Sie den Explorer-Filter, um ausgeblendete Elemente anzuzeigen.
- macOS: Der Standardstandort ist: /Library/Application\ Support/servicenow/Agent-Client-Collector/log/acc.log

Zugehörige Informationen

MID-Webserver Und Agent-mTLS-Authentifizierung

Ereignismanagement-Konfigurationspräferenzen

Bevorzugte Einstellungen für Eigenschaften und allgemeine Konfiguration.

Verwenden Sie das Known Error-Portal und die Community zur Suche nach weiteren Informationen.

Allgemeine Präferenzen

Selbstintegrität

Standardmäßig ist die Selbstintegritätsüberwachung nicht aktiviert. Navigieren Sie zu , um es zu aktivieren **Ereignismanagement** > **Einstellungen** > **Eigenschaften** Und wählen Sie aus **Ja** Für *`Enable Event Management self-health monitoring`*(evt_mgmt.self_health_active) Eigenschaft. Verwenden Sie dieses Feature zum Überwachen und Nachverfolgen vieler Ereignismanagement-Funktionen

Hinweis: Im Selbstintegritätsservice verwendete CIs werden in der CMDB erstellt.

Verwenden Sie die folgenden Einstellungen, um einer Verschlecherung der Leistung vorzubeugen.

Thema	Details
Business Rules	• Schreiben Sie keine Business Rules für Event-Tabellen [em_event], da sie nicht in der aktuellen Standard-REST-URL ausgeführt werden, die für die Event-Injektion verwendet wird. • Business Rules, die für Warnungstabellen [em_alert] geschrieben werden, müssen sehr effizient sein, da sie sonst zu einer Verschlechterung der Leistung führen können. Überlegen Sie, anstatt eine Geschäftsregel zu schreiben, ob besser ein Job geschrieben werden sollte. Eine ineffiziente Geschäftsregel kann dazu führen, dass die Incident-Erstellung fehlschlägt und die Berechnung der Warnungsauswirkung fehlschlägt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Details
	• Schreiben Sie keine asynchronen Business Rules für Warnungstabellen. • Business Rules dürfen das Feld **Kategorie** in Event-Tabellen [em_event] nicht ändern.
Hochskalierung	Überprüfen Sie die durchschnittliche Event-Verarbeitungszeit, bevor Sie den Event-Durchsatz beim ersten Start mit Ereignismanagement hochskalieren. Führen Sie diese Überprüfung nach einem ersten Flow von Events durch, wenn alle Regeln vorhanden sind. Wenn die Verarbeitungszeit pro Event einige Millisekunden dauert, ermitteln Sie die Ursache für die Verlangsamung der Verarbeitung, bevor Sie mit der Skalierung fortfahren. Die Leistungsdauer kann in der Tabelle Leistungsstatistiken [sa_performance_statistics] überprüft werden.
Für große Umgebungen konfigurieren	• Legen Sie die Eigenschaft **Event-Verarbeitung für mehrere Knoten aktivieren** (*evt_mgmt.event_processor_enable_multi_node*) auf **Ja** fest. Aktivieren Sie Mehrknotenpunkte in Produktionsumgebungen, und legen Sie Werte basierend auf der Größe der Bereitstellung und der erwarteten Event-Rate fest. • Legen Sie die **Anzahl der Scheduled Jobs zur Event-Verarbeitung** (*evt_mgmt.event_processor_job_count*) auf `4` fest. • Wenn Sie Events aus einer benutzerdefinierten Quelle senden, stellen Sie sicher, dass Events über **Nachrichtenschlüssel** oder die Daten **Quelle**, **Knoten**, **Typ** und **Ressource** verfügen.
Latenzprobleme beim Empfang von Events	Überprüfen Sie die folgenden Einstellungen: • Stellen Sie sicher, dass das **Bucketfeld** in der Event-Tabelle [em_event] auf einen Wert festgelegt ist, der größer als Null (*0*) ist. • Navigieren zu **Systemzeitplaner** > **Geplante Aufgaben** Und suchen Sie nach *- process events**. Überprüfen Sie, ob alle *- process events**-Jobs gemäß der Eigenschaftskonfiguration der **Anzahl der geplanten Events** (*event_processor_job_count*) zur Verarbeitung von Events vorhanden sind. Stellen Sie sicher, dass der **Status** *Running* oder *Ready* ist. Wenn der Status *Queued* oder *Error* ist, setzen Sie den Jobstatus auf *Ready*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Details
Events archivieren	• Vermeiden Sie, die standardmäßige Aufbewahrungszeit für Events zu ändern. • Um Events länger zu protokollieren, erstellen Sie eine Archivtabelle und einen Job, der neue Events kopiert. Führen Sie dazu einen Auftrag durch, um Events [em_event] regelmäßig in einer benutzerdefinierten Tabelle zu sichern. • Erweitern Sie die Tabellenrotation nicht um weitere Tage.

Event-Integration

SNMP-Traps

- Verwenden Sie zum Senden von SNMP-Traps ein Überwachungstool, anstatt sie direkt von Geräten zu senden.
- Um zu vermeiden, dass Event-Regeln neu geschrieben werden müssen, laden Sie MIBs hoch, bevor Sie die Event-Regeln definieren.

Webservice-API

- Die Verwendung einer Webservice-API für die Integration kann die Anzahl der erforderlichen Event-Regeln reduzieren. Diese Aktion verhindert, dass Events umgewandelt werden müssen (vorbereitete Daten werden in einem Event an die Instanz gesendet).
- Verwenden Sie dedizierte Anmeldeinformationen für die Integration. Geben Sie optional Anmeldeinformationen an, die für jede Event-Quelle spezifisch sind.

CloudWatch

Verwenden Sie dedizierte Anmeldeinformationen für die Integration von CloudWatch mit ServiceNow.

E-Mail

Verwenden Sie E-Mail nur, wenn die Quelle ein geringes Volumen hat und andere Optionen nicht verfügbar sind, z. B. Ausführen eines Skripts oder Weiterleiten eines SNMP-Traps.

Event-Regeln

Regeln für Konfigurationseinstellungen bei der Erstellung von Event-Regeln:

- Schreiben Sie Event-Regeln, um sie auf möglichst viele Events anzuwenden. Spezifischere Regeln können dann je nach Bedarf erstellt werden und sollten einen Wert niedrigerer Ordnung verwenden.
- Wenn eine allgemeinere Regel zum gleichen Ergebnis führen kann, vermeiden Sie das Schreiben von Event-Regeln, die nur für eine bestimmte Teilmenge von Events gelten.
- Wenn Event-Regeln auf Events angewendet werden, werden keine Änderungen am ursprünglichen Event vorgenommen. Die gesamte Verarbeitung erfolgt im Arbeitsspeicher. Verwenden Sie daher das Feld **Verarbeitungshinweise** und/oder verwenden Sie den Link **Prozess der Event-UI-Aktion überprüfen**, um Fehler zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine Regel/Umwandlung ändern, die über Zuordnungsregeln verfügt, sollten Sie tatsächliche und/oder simulierte Events überprüfen und erneut testen.
- Stellen Sie sicher, dass der Wert im Feld **Von** genau mit einer Zeichenfolge im JSON-Text im Feld *additional_info* eines Events übereinstimmt. Diese Zuordnung erfolgt, wenn eine Regel basierend auf Informationen in einer MIB-Datei konfiguriert wurde. Wenn die MIB-Datei nicht hochgeladen wird, zeigt die JSON für die SNMP-Trap varbinds (Variablenbindung) mit gepunkteten Namen anstelle des übersetzten Namens in der MIB an. Die Zuordnungsregel für das Event-Feld kann dann nicht angewendet werden.
- Erstellen Sie eine konsistente Namenskonvention. Eine gängige Konvention ist: *<customer acronym>.<Event Source>.<Description>*. Beispiel: *ACME.OEM.Normalize*
- Wenn für zwei Event-Regeln ähnliche Bedingungen festgelegt sind, verwenden Sie das Feld **Reihenfolge**, um zu steuern, welche Event-Regel ausgeführt wird.
- Verwenden Sie Event-Regeln, um eine Warnung einem CI zuzuordnen.

Zusätzliche Einstellungen zum Erstellen von Event-Regeln:

Gewünschtes Ergebnis	Erforderliche Aktivität
Effektive Deduplizierung und Aktivierung einer effizienten parallelen Event-Verarbeitung	Füllen Sie die Felder **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** aus.
CI-Bindung	• An Host binden – durch Ausfüllen des **Knotenfelds** und optional von **CI-Bezeichnern**. • Bindung an Anwendung und/oder Gerät – durch Ausfüllen der Felder **CI-Bezeichner** und **Zusätzliche Informationen**.
Warnungskorrelation mithilfe von Warnungszusammenfassung	Füllen Sie die Felder **Ressource** und **Metrikname** aus. **Hinweis:** Wenn das CI auch gebunden ist, wird die Warnungskorrelation verbessert.

Benutzerdefinierte Event-Felder

Fügen Sie zusätzliche Felder nur in das Feld **Zusätzliche Informationen** des Events ein.

Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen.

Fügen Sie der Event-Tabelle [em_event] keine Spalten hinzu.

Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Deduplizierung

Konfigurationseinstellungen für Deduplizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld **message_key** wird für die Deduplizierung verwendet. Wenn beim Quell-Event keine zuverlässigen Nachrichtenschlüsselwerte bereitgestellt werden, ist ein gut definierter Plan für die Erstellung dieser Bezeichner wichtig.
- Wenn der Nachrichtenschlüssel nicht definiert ist, lautet der Standard-Nachrichtenschlüssel <*Source + Node + Type + Resource + Metric Name*> .
- Die Leitlinie besteht darin, dass die Event-Quelle die <*Source + Node + Type + Resource + Metric Name*>-Felder vorab ausfüllt und den Nachrichtenschlüssel ausfüllt. Diese Aktion ermöglicht eine bessere Verteilung der Event-Verarbeitung zwischen Instanzarbeitern und Knoten.
- Wenn das Quell-Event keine Werte für diese Felder enthält, müssen Sie sie mithilfe von Umwandlungsregeln ausfüllen. Diese Aktion wirkt sich nicht auf die Event-Verarbeitung aus, wird jedoch zur Deduplizierung verwendet. Füllen Sie so viele dieser Felder wie möglich aus, bevor sie an die Instanz gesendet werden. Diese Aktion bietet eine bessere Verteilung von Events auf die Prozessorarbeiter und somit einen besseren Durchsatz und eine bessere Skalierung.

CI-Bindung

- Versuchen Sie nach Möglichkeit immer, eine Warnung an ein CI zu binden.

  Hinweis: Obwohl Event-Regeln für Events definiert sind, sind CIs an Warnungen gebunden, die aus diesen Events resultieren, und nicht an das Event selbst.

- Um einen Host, Computer oder ein beliebiges Gerät mit einer IP zu binden, füllen Sie das **Event-Knotenfeld** mit einem eindeutigen Hostnamen, FQDN, einer IP-Adresse oder einer MAC-Adresse aus. Wenn zur Identifizierung eines Hosts andere Bezeichner erforderlich sind, füllen Sie das Feld „ci_identifiers“ mit einem JSON-Format aus. Das JSON-Format muss den **CMDB**-Feldnamen und -Wert enthalten, um die Übereinstimmung durchzuführen.

  Hinweis: Das **Event-Knotenfeld** muss aus einer Event-Regel oder mit einem eindeutigen Hostnamen aus der Quelle ausgefüllt werden, bevor das Event eingefügt wird.

- Die primäre Bindungsstrategie besteht in der Verwendung des Felds **Knoten**. Wenn das **Knotenfeld** im Event nicht bereits ausgefüllt ist, kann es mithilfe von Event-Regeln ausgefüllt werden.

Warnungseinstellungen

Warnungslebenszyklus

Allgemeine Warnungsfunktionalität:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine Warnung wird immer dann geöffnet, wenn ein Event nicht ignoriert wird oder dessen Schwellenwert von einer Event-Regel überschritten wird und die Deduplizierung das Event nicht als zu einer vorhandenen Warnung gehörig identifiziert.
- Eine Warnung wird geschlossen, wenn ein Abschluss-Event auf demselben Nachrichtenschlüssel gesendet wird, oder wenn die Warnung manuell geschlossen wird.
- Eine Warnung wird erneut geöffnet, wenn eine Eröffnungswarnung mit demselben Nachrichtenschlüssel innerhalb des in den Eigenschaften definierten Zeitrahmens gesendet wird (Standard ist eine Stunde).
- Wenn eine Warnung in schneller Abfolge (gemäß der Definition in den Eigenschaften) geöffnet und geschlossen wird, wechselt sie in den Status „Fluktuierend“. Wenn diese Öffnungs- und Schließungsrate aufhört, verliert die Warnung ihren Status „Fluktuierend“.
- Wenn ein Incident aus einer Warnung geöffnet wird, bleibt diese Warnung offen, solange der Incident offen bleibt. Standardmäßig wird beim Schließen des Incidents oder der Warnung auch der jeweils andere geschlossen. Dieses Verhalten kann mithilfe von Eigenschaften konfiguriert werden.
- Schließen Sie keine Warnung, wenn Sie einen entsprechenden Incident erstellen.
- Löschen Sie keine offenen Warnungen. Schließen Sie zuerst eine Warnung, und löschen Sie sie dann.
- Verwenden Sie `Bestätigen`, um anzugeben , dass die Warnung bekannt ist und vorübergehend ignoriert werden kann.
- Verwenden Sie `Bestätigen` nicht, um eine Warnung mit einem Handlungsbedarf zu versehen.
- Erstellen Sie keine Warnungen in einem der folgenden Status:
  - `Geschlossen`
  - `OK`
  - `Offen`
- Die Eigenschaft `evt_mgmt.alert_auto_close_interval` schließt Warnungen nach dem angegebenen Zeitraum automatisch. Geben Sie nicht 0 an, da dieser Wert die Funktion deaktiviert und zu einer Verschlechterung der Leistung führen kann.
- Erstellen Sie keine Warnungen im Status `OK`. In einigen Überwachungssystemen bedeutet `OK`, dass ein Problem gelöst wurde, während in anderen Überwachungssystemen `OK` verwendet wird, um Events zu kennzeichnen, die keine operative Bedeutung haben. Im ersten Fall verwenden Sie `Löschen` anstatt `OK` mithilfe einer Zuordnungsregel. Im letzteren Fall müssen Sie eine Ignorieren-Regel verwenden, es sei denn, die Events haben einen bestimmten Wert.

Warnungsaktionsregeln

- Bei einem Scheduled Job werden alle 11 Sekunden Warnungsaktionsregeln auf neue Warnungen angewendet. Wenn eine Warnungsregel nicht sofort gestartet wird, warten Sie 10–15 Sekunden, bevor Sie mit der Problembehandlung beginnen.
- Wenn für zwei Warnungsregeln ähnliche Bedingungen festgelegt sind, verwenden Sie das Feld **Reihenfolge**, um zu steuern, welche Warnungsregel ausgeführt wird.
- Verwenden Sie Warnungsaktionsregeln mit Aufgabenvorlagen, um statische Werte in einem Incident auszufüllen. Verwenden Sie das Ausfüllerskript, um dynamische Werte im Incident zuzuweisen. Das Ausfüllerskript kann den Wert `false` zurückgeben, um die Incident-Erstellung abzubrechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie einen Benutzer namens Ereignismanagement (oder einen ähnlichen Namen). Anschließend kann das Feld **Erstellt von** in einer Aufgabenvorlage (z. B. **Incident**) festgelegt werden, um anzugeben, dass der Benutzer die Quelle der Aufgabe war.
- Verwenden Sie die Skripteinbindung **EvtMgmtCustomIncidentPopulator**, um dynamische Wertzuweisungen durchzuführen oder dynamische OOB-Wertzuweisungen zu überschreiben.

Fehlerkorrektur

- Legen Sie für die Fehlerkorrekturaufgaben-Tabelle [em_remediation_task] immer Eigenschaften für den Orchestrierungs-Workflow fest.
- Verwenden Sie ECC-Warteschlange und **Workflow** > **Live-Workflow** > **Alle Kontexte** Um detailliertere Informationen zu Korrekturaktivitäten zu erhalten.

Business-Regeln

- Business Rules, die für Warnungstabellen erstellt werden, sollten nicht länger als einige Millisekunden dauern. Anstatt eine Geschäftsregel zu verwenden, sollten Sie in Betracht ziehen, ob die gleiche Funktionalität mit einem Job erreicht werden kann.
- Verwenden Sie keine Business Rules, um eine Warnung einem CI zuzuordnen. Verwenden Sie Event-Regeln für Bindungen anstelle von Business Rules.

Planung

- Organisieren Sie die Konfiguration der Event-Quelle von Filtern, Modulen usw. in mehreren parallelen Vorgängen anstatt in seriellen.
- Validieren Sie verarbeitete Event-Formate, um sicherzustellen, dass die analysierten Daten mit den gewünschten Ergebnissen übereinstimmen.
- Testen Sie Produktions-Events in einer Umgebung außerhalb der Produktion. Integrieren Sie sie mit Elementmanagern und ServiceNow-Instanzen außerhalb der Produktion. Wenn Elementmanager außerhalb der Produktion nicht verfügbar sind, senden Sie Events von Elementmanagern sowohl an Produktionsumgebungen als auch an Nichtproduktionsumgebungen.

Services und Dashboard

- Verwenden Sie Servicegruppen, um Services in logischen Gruppen zu gruppieren, um die Anzahl der Services zu reduzieren, die im Dashboard „Serviceintegrität“ angezeigt werden.
- Importieren Sie manuell erstellte Servicezuordnungen.

Metrikdaten-Sammlerprotokolle und -dateien

Metrikdaten-Sammlerprotokolle und -dateien befinden sich unter dem Pfad $(MID_SERVER_DIR)/agent. Verwenden Sie diese Protokolle und Dateien für die Fehlerbehebung und Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standort von Metrikdaten Sammlerprotokolle und -Dateien

Protokoll oder Datei	Pfad
Protokolldatei für PowerShell-Metriksammler	Protokolle/retrieve_metrics{connector instance ID}.log
PowerShell-Ausgabedatei	work/metrics/metrics_output_{connector instance ID}.txt
PowerShell-Ausgabedatei	work/metrics/parameters_{connector instance ID}.txt

Die Metrikdaten-Leistung kann in der MID-Server-Protokolldatei überprüft werden, wenn sich der Parameter *mid.log.level* MID-Server im Debug-Modus befindet.

Metrikdaten-Leistungszahlen sind in der Tabelle „Leistungsstatistiken“ [sa_performance_statistics] verfügbar. Um die Leistungsnummern anzuzeigen, filtern Sie die Liste der Leistungsstatistiken für **Metriksammler**.

Zugehörige Informationen

Rotieren Sie die Ereignis- und Warnungstabelle für die Bereinigung

Domain Separation und Ereignismanagement

Die Domänentrennung wird in Ereignismanagement unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Ereignismanagement

Wenn Domänen in Ereignismanagement getrennt sind, können Benutzer nur Warnungen und Events in ihrer eigenen (Mandanten-)Domäne sehen und verwalten.

Für Ereignismanagement-Tabellen, die im Basissystem bereitgestellt werden, ist eine Domänenspalte vorhanden. In der Spalte wird der Name der Domäne angezeigt, zu der das Event oder die Warnung gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn die Domänenspalte nicht in der Liste angezeigt wird, klicken Sie auf , und fügen Sie die gewünschte Spalte hinzu. Darüber hinaus können Sie eine Spalte hinzufügen, die den Domänenpfad anzeigt.

Informationen zu Einschränkungen der Domänentrennung in Ereignismanagement finden Sie unter Ereignismanagement-Domain Separation konfigurieren.

Zugehörige Informationen

Domänentrennung für Service Provider

Ereignismanagement-Domain Separation konfigurieren

Sie können Ereignismanagement für die **Domain Separation** konfigurieren, um logisch definierte Domänen zu erstellen, die den nicht autorisierten Zugriff auf Daten beschränken. Wenn Domänen in Ereignismanagement getrennt sind, können Benutzer nur Warnungen und Events in ihrer eigenen (Mandanten-)Domäne sehen und verwalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie das Plugin **Domain Support – Domain Extension Installer** und konfigurieren Sie den MID Server für Ereignismanagement.

Die folgenden Funktionen von Ereignismanagement unterstützen die Domain Separation nur eingeschränkt.

Funktionen mit eingeschränkter Domain Separation

Funktion	Support
Event – Warnungs-Flow	Unterstützt. Die Trennung basiert auf dem Domänenbenutzer, der Events gesendet hat. Benutzerzugriff ist für die Anmeldeinformationen der sendenden API-Events oder in der Konfiguration der MID Server-Reporting-Events erforderlich. In einer Umgebung mit mehreren Domänen kann jeder MID Server je nach verwendetem Integrationsbenutzer nur eine Domäne bedienen. Stellen Sie in der Konfiguration der Connector-Instanz sicher, dass der MID-Server dieselbe Domäne wie die Connector-Instanz hat. Informationen zum Konfigurieren von Pull-Connectors zur Unterstützung der anwenderdefinierten Domänentrennung finden Sie unter Personalisieren Sie Domänen für Pull-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen.
Auswirkungsberechnung	Unterstützt. Segregation basiert auf der Art und Weise, wie CIs getrennt werden.
Anwendungsservices	Teilweise unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen mit eingeschränkter Domain Separation (Fortsetzung)

Funktion	Support
	Segregation basiert auf der Art und Weise, wie CIs getrennt werden.
Dynamische CI-Gruppen	Teilweise unterstützt. Segregation basiert auf der Art und Weise, wie CIs getrennt werden. **Hinweis:** Der Discovery-Prozess trennt CIs nicht nach Domäne.
Fehlerkorrektur	Unterstützt. Beim Bearbeiten von Warnungsverwaltungsregeln können Benutzer nur relevante Workflows anwenden. Weitere Informationen zur Domain Separation im Flow Designer finden Sie unter Domänentrennung und Flow Designer.
Warnungszusammenfassung	Unterstützt. In domänengetrennten Umgebungen werden Warnungsgruppen nur für Warnungen in derselben Domäne erstellt.

Prozedur

1. Aktivieren Sie das Plugin „Domain Support – Domain Extension Installer“, wenn es noch inaktiv ist.
2. Konfigurieren Sie die Connector-Instanz so, dass sie sich in derselben Domäne wie der MID-Server befindet.

Ereignismanagement-Integrationen

Ein Event ist eine Benachrichtigung von einem oder mehreren Überwachungstools, die anzeigt, dass etwas von Interesse aufgetreten ist, z. B. eine Protokollnachricht, eine Warnung oder ein Fehler.

Events werden verarbeitet und Warnungen werden basierend auf den folgenden Faktoren generiert:

- Konfiguration des Eventsammlers über einen MID-Server, ein Skript, einen SNMP-Trapsammler oder eine E-Mail-Nachricht.
- Eine Event-Regel, Warnungsbindung oder Event-Feldzuordnungskonfiguration für die Verarbeitung von Events aus verschiedenen Quellen.

Wenn ein Event-Paket verarbeitet wird, das Events mit einem benutzerdefinierten (nicht unterstützten) Status enthält, werden die Events mit dem benutzerdefinierten Status nicht verarbeitet.

Integration mit externen Events

Ereignismanagement empfängt externe Events über eine Integration oder Skripts. Wenn Sie ein Skript zum Erfassen von Events verwenden, ist keine Konfiguration erforderlich. Alle anderen Integrationen müssen konfiguriert werden.

Nach der Konfiguration einer Integration kann Ereignismanagement Events erfassen, die direkt an die ServiceNow AI Platform-Instanz oder über den MID Server, den SNMP-Trap oder per E-Mail gesendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integration mit externen Systemen kann von einer ServiceNow AI Platform-Instanz mithilfe eines Pull-Connector oder von einem externen System mithilfe eines Push-Mechanismus initiiert werden.

Integration über eine ServiceNow AI Platform-Instanz

Die ServiceNow AI Platform-Instanz enthält Push-Connectors, mit denen sich externe Überwachungssysteme direkt mit Ereignismanagement integrieren lassen.

Sie können die Authentifizierung in der ServiceNow AI Platform-Instanz konfigurieren und die externen Überwachungssysteme so aktualisieren, dass Endpunkte zum Senden der Events für die verfügbaren Push-Connectors verwendet werden. Weitere Informationen finden Sie unter Push-Connectors.

Integration über MID Server

Der MID Server ermöglicht die Kommunikation und den Transport von Daten zwischen externen Anwendungen, Datenquellen, Services und der ServiceNow AI Platform-Instanz.

Connector-Vorgang	Beschreibung
Pull	Sie können Connector-Instanzen zur Verwendung von Connector-Definitionen (Skriptanweisungen) konfigurieren. Dadurch kann sich der MID Server mit externen Servern verbinden, um Event-Informationen über einen Pull-Vorgang abzurufen.
Veröffentlichen	Sie können externe Systeme so konfigurieren, dass Event-Informationen an die ServiceNow AI Platform-Instanz über den MID Server übertragen werden. Konfigurieren Sie beispielsweise den MID WebService-Event-Sammler zum Übertragen von Event-Nachrichten an den MID Server. Weitere Informationen finden Sie unter Ereignisse werden an übertragen MID-Server Webservice-API wird verwendet.

Standard-Event-Formular

Ein Standard-Event-Formular muss von allen Events verwendet werden, unabhängig davon, wie sie bei der ServiceNow AI Platform-Instanz eintreffen. Weitere Informationen finden Sie unter Event-Feldformat für die Event-Erfassung.

Ereignismanagement Personalisierung der Connectors-Domäne

Erstellen Sie Ereignisse in verschiedenen Domänen für alle Ereignismanagement Connectors, die nur eine einzelne Connector-Instanz verwenden, indem Domänentrennung von personalisiert wird Ereignismanagement Connectors.

Wie die Domäne identifiziert wird

In einem ServiceNow Instanz, Ereignisse werden in angemeldetem oder erstellt MID-Server Anwenderdomänen. Sie können jedoch Ereignisse in einer anderen Domäne erstellen, indem Sie Metadatenwerte in der Ereignis-HTTP-Anforderung angeben, einschließlich URL, Header, Anforderungstext (Nutzlast) und Connector-Parameter.

Der angemeldete Anwender oder der MID-Server Anwender muss Zugriff auf die angegebene Domäne haben. Der Connector löst die Domäne basierend auf dem angegebenen Bezeichner auf und erstellt Ereignisse in dieser Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften stellen die Standardmetadaten bereit, die die domänengetrennte Tabelle zur Identifizierung der Domäne festlegen. Weitere Informationen finden Sie unter Mit installierte Domäneneigenschaften Ereignismanagement.

Connector-Ausnahmen

Sie können die Domänentrennung für die folgenden Pull-Connectors nicht personalisieren:

- SCOM
- IBM Netcool (unterstützt nur IBM Netcool_v2)
- HPOM
- Hyperic

Sie können die Domänentrennung für die folgenden Push-Connectors nicht personalisieren:

- SAP SolMan-Transformationsskript
- BmcTrueSight-Transformationsskript
- Transformieren Sie generische Ereignisse MID
- TransformEvents_xmlSample

Zugehörige Informationen

Domain Separation und Ereignismanagement

Personalisieren Sie Domänen für Pull-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen

Konfigurieren Sie Pull-Connectors, um die Domänentrennung von Ereignissen zu personalisieren, damit Sie sie zum Erstellen von Ereignissen in anderen Domänen als den derzeit angemeldeten oder des Anwenders verwenden können MID-Server Domäne.

Vorbereitungen

Stellen Sie sicher, dass Sie das folgende Setup haben:

- Sie haben Lesezugriff auf die Domäneninformationstabelle für die Rolle „evt_mgmt_Integration“ (Standardtabelle: Core_Company). Weitere Informationen finden Sie unter Konfigurieren Sie eine ACL-Regel .
- Sie haben aktiviert *evt_mgmt.connector_enable_custom_domain_separation*Systemeigenschaft .
- Sie haben die folgenden Plugins auf Ihrem installiert ServiceNow Instanz:
  - Ereignismanagement *com.glideapp.itom.snac* Plugin
  - Ereignismanagement Connectors *sn_em_connector*Plugin
  - Domänensupport: Installationsprogramm Für Domänenerweiterungen *com.glide.domain.msp_extensions.installer*Plugin

  Sie können die Plugins aus dem herunterladen ServiceNow Store .

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen** > **an.**
2. Auf der **Connector-Instanzen** Deaktivieren Sie die Connector-Instanz des Connectors, für den Sie die Domänentrennung konfigurieren möchten, indem Sie sie auswählen und löschen **Aktiv** Kontrollkästchen.
3. Wählen Sie **Aktualisieren**.
4. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen**an.
5. Von **Connector-Definitionen** Wählen Sie Ihre Connector-Definition aus.
6. Legen Sie fest, ob alle Ereignisse in einer angegebenen Domäne erstellt oder durch eine Domäne bestimmt werden sollen, die in der Nutzlast jedes Ereignisses angegeben ist.

   a. In **Connector-Parameter** Tabelle, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein**

   b. Wählen Sie den Speicherort der Domänendefinition für die Ereigniserstellung aus.

   - Geben Sie ein, damit alle Ereignisse in der angegebenen Domäne erstellt werden PayloadDomainInfoFieldValue In **Name** Spalte.
   - Geben Sie ein, damit Ereignisse in der in der Nutzlast des Ereignisses angegebenen Domäne erstellt werden PayloadDomainInfoFeldName In **Name** Spalte.

   Hinweis: Wenn beides *payloadDomainInfoFieldValue*Und *payloadDomainInfoFieldName*Werden angegeben, hat die in der Nutzlast des Ereignisses angegebene Domäne Vorrang.

   c. Wählen Sie **Aktualisieren**.

7. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
8. Auf der **Connector-Instanzen** Wählen Sie Ihre Connector-Instanz aus der Liste aus.
9. Geben Sie in der Liste Connector-Instanzwerte einen Wert in an **Wert** Feld der Parameter.

Parameter	Wert
payloadDomainInfoFieldValue	Der Wert, der zum Abgleichen des Domänendaten-satzes verwendet wird. Beispiel: ServiceNow.

payloadDomainInfoFieldName	Der Schlüssel in der Nutzlast mit dem Domänenbezeichner. Beispiel: Wenn der Nutzlastschlüssel **Unternehmen** Enthält den Domänenbezeichner und dann den Wert in **Wert** Spalte würde die Unternehmensinfor–mationen enthalten. Zum Beispiel:
	Unternehmen
	{
	„Quelle“: „SolarWinds“,
	„Host“: „127.0,0.1“,
	„Unternehmen“: „ServiceNow“
	}

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
	Hinweis: Dot-Walking wird nicht unterstützt.

10. Wählen Sie **Speichern**.
11. Wählen Sie Aus **Testen Sie Den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
    - Wenn der Test erfolgreich ist, wird eine Bestätigungsmeldung angezeigt.
    - Wenn der Test fehlschlägt, enthält eine Meldung Anweisungen zur Behebung des Problems.

    Bei einem erfolgreichen Test wird eine Meldung auf dem Bildschirm angezeigt. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen auf dem Bildschirm, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

    Hinweis: Verwenden Sie ein Netzwerktool wie *`Ping`* Dient zum Überprüfen, ob die Anmeldeinformationen korrekt sind und eine Netzwerkverbindung von der hergestellt wird MID-Server Zum Connector-Server.

12. Nachdem der Connector verifiziert wurde, wählen Sie aus **Zurück zur Connector-Instanz** Link.
13. Aktivieren Sie die Connector-Instanz, indem Sie auswählen **Aktiv** Und **Aktualisieren** .
14. **Wahlweise:** Konfigurieren Sie die Domäne für Ereignisse, indem Sie Domänenmetadaten über die Connector-Parameter bereitstellen.

    Beispiel: Um die Anwendertabelle [sys_user] für eine einzelne Connector-Instanz in zu verwenden **Connector-Definitionen** Erstellen Sie Parameter mit den folgenden Namen, und fügen Sie ihre Werte in hinzu **Connector-Instanz** Formular.

    - *`connectorDomainInfoTableName`* – Sys_user

      Hinweis: Die Tabelle muss domänengetrennt sein.

    - *`connectorDomainInfoColumnName`* – User_Name
    - *`connectorDomainIdColumnName`* – Sys_Domain
    - *`connectorDomainPathColumnName`* – Sys_Domain_path

    Weitere Informationen finden Sie unter Metadaten der Connector-Domäne.

Ergebnis

Die Ereignismanagement Connector ist für Domänentrennung eingerichtet.

Personalisieren Sie Domänen für Push-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen

Konfigurieren Sie Push-Connectors, um die Domänentrennung von Ereignissen zu personalisieren, damit Sie sie zum Erstellen von Ereignissen in anderen Domänen als den derzeit angemeldeten oder des Anwenders verwenden können MID-Server Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Sie das folgende Setup haben:

- Sie haben Lesezugriff auf die Domäneninformationstabelle für die Rolle „evt_mgmt_Integration“ (Standardtabelle: Core_Company). Weitere Informationen finden Sie unter Konfigurieren Sie eine ACL-Regel .
- Sie haben aktiviert *evt_mgmt.connector_enable_custom_domain_separation*.System-Eigenschaft.
- Sie haben die folgenden Plugins in installiert ServiceNow AI Platform® Instanz:
  - Ereignismanagement (*com.glideapp.itom.snac*)
  - Ereignismanagement Connectors (*sn_em_connector*)
  - Domänensupport: Installationsprogramm Für Domänenerweiterungen (*com.glide.domain.msp_extensions.installer*)

    Sie können die Plugins aus dem herunterladen ServiceNow Store .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**an.
2. Öffnen Sie einen Push-Connector.
3. Auf der **Push-Connector** Bildschirm, scrollen Sie nach unten zum **Push-Connector-Konfigurationen** Liste und auswählen **Neu** .

   Hinweis: Wenn diese Liste nicht angezeigt wird, müssen Sie einen Push-Connector-Konfigurationsparameter erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Push-Connector-Konfigurationsparameter.

4. In **Push-Connector-Konfigurationen** Bestimmen Sie, ob Ereignisse in der angegebenen Domäne oder in der in der Nutzlast jedes Ereignisses angegebenen Domäne erstellt werden sollen.

Speicherort der Domänenerstellung	Parameter und Werte
Die angegebene Domäne	○ **Feldname** : PayloadDomainInfoFieldValue ○ **Wert** : Domänenbezeichner
Die in der Nutzlast jedes Ereignisses angegebene Domäne	○ **Feldname** : PayloadDomainInfoFieldName ○ **Wert** : Feldname in Nutzlast Beispiel: Wenn der Nutzlastschlüssel „Unternehmen“ den Domänenbezeichner enthält, ist „Unternehmen“ der Wert. **„Unternehmen“** { „Quelle“: „SolarWinds“, „Host“: „127.0,0.1“, „Unternehmen“: „ServiceNow“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherort der Domänenerstellung	Parameter und Werte
	}

Hinweis: Wenn beides `payloadDomainInfoFieldValue`Und `payloadDomainInfoFieldName`Parameter werden angegeben, dann die `payloadDomainInfoFieldName`Hat Vorrang.

5. Wählen Sie **Absenden**.

Ergebnis
Ereignisse werden in der Domäne erstellt, auf die der Domänenbezeichner verweist.

Hinweis: Die Tabelle, in der Domäneninformationsdatensätze gespeichert werden (z. B. Core_Company), muss domänengetrennt sein. Weitere Informationen finden Sie unter Domäne: Trennen Sie eine anwenderdefinierte Tabelle .

Zugehörige Informationen

Integration mit Push-Connectors

Metadaten der Connector-Domäne

Konfigurieren Ereignismanagement Connectors

Ereignismanagement stellt viele Connectors zum Abrufen oder Veröffentlichen von Events von externen Geräten bereit. Connectors sind auch im ServiceNow-Store und von Drittanbietern verfügbar. Zudem können Sie benutzerdefinierte Connectors erstellen.

Bereitgestellte Connectors (Pull)
Diese Tabelle enthält die mit Ereignismanagement bereitgestellten Connectors.

Hinweis:

- Die Connectors für Azure-Metriken und AWS CloudWatch-Metriken werden im Basissystem nur angezeigt, wenn das Operational Intelligence-Plugin (com.snc.sa.metric) aktiviert ist.
- Alle Connectors unterstützen externe Anmeldeinformationsspeicherlösungen. Weitere Informationen zur Konfiguration des externen Anmeldeinformationsspeichers finden Sie unter Konfiguration des externen Anmeldeinformationsspeichers .

Connectors	Unterstützte Version	Beschreibung
Azure Monitor		Sendet Warnungsstatusänderungen an das Azure-Portal
HPOM	08.60.005	Empfangen von Events vom HP Operations Manager (HPOM)
Hyperic	5.8.4.0	Empfangen von Events vom VMware vRealize Hyperic-Server
Logicmonitor	156	Empfangen von Events vom Logicmonitor-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Unterstützte Version	Beschreibung
IBM Netcool	8.1.0	Empfangen von Events von IBM Netcool/OMNIbus-Objektservern und Auswirkungsservern.
Icinga2	2.4.1	Empfangen von Events vom Icinga2-Server
Apache Kafka Consumer Connector	• 3.0.0 • 3.2.0	Empfangen Sie Ereignisse vom Apache Kafka-Server.
ServiceNow Cloud Observability	2.1.1 oder höher	Empfangen Sie Ereignisse von ServiceNow Cloud Observability Plattform.
NagiosXI	5.5.2	Empfangen von Events vom Nagios XI-Server
NNMi	10.30.653	Empfangen von Events vom NNMi-Server
OBM, auch als OMi v2 bezeichnet	10.01, 10.10, 10.11, 10.12, 10.60, 10.61 und 11.01	Empfangen von Warnungen vom OBM-Server.
OMi	10.01, 10.10, 10.11, 10.12, 10.60 und 10.61	Empfängt Warnungen vom OMi-Server
Op5	7.3.15	Empfangen von Warnungen von einem OP5-Monitor
Opsview	5.4.0	Empfangen von Warnungen von einem Opsview-Monitor
PRTG	21.3.71	Empfangen von Warnungen von einer Paessler PRTG Network Monitor-Quelle
SAP Solution Manager	7.2 740 SP16	Empfangen von Warnungen von einer SAP Solution Manager Monitor-Quelle
SCOM	• 2007 – Version 6.1.7221.0 • 2012 – Version 7.1.10226.0 • 2016 – Version 7.2.117190	Warnungs- und Metriksammlung aus Microsoft System Center Operations Manager (SCOM).
SolarWinds	• NPM 12.0 • SAM 6.2.4	Empfangen von Events vom SolarWinds-Monitor
vCenter	6.5	Empfangen von Events aus Ihrer VMware vSphere-Umgebung
vRealize	VMware vRealize Operations Manager	Empfangen von Events vom vRealize-Betriebsprotokoll und den Ereignismanagement-Servern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Unterstützte Version	Beschreibung
	Unterstützte Version: 8.10.0	
Zabbix	5.0.9	Empfangen von Events vom Zabbix-Server

Bereitgestellte Connectors (Push)

Diese Tabelle enthält die mit Ereignismanagement bereitgestellten Connectors. Generische Push-Connectors werden ebenfalls bereitgestellt, einer für die Event-Erfassung über den MID-Server und der andere über die Instanz.

Bevor Sie beginnen, stellen Sie sicher, dass das Plugin „Ereignismanagement Connectors“ in der ServiceNow AI Platform-Instanz installiert ist. Sie können das -Plugin aus herunterladen ServiceNow Store Website.

Connectors	Beschreibung	Unterstützte Authentifizierung
AWS	Verwenden Sie den Connector, um AWS-Warnungen (Amazon Web Services) als Events zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	N/V
Azure	Verwenden Sie die OAuth-Authentifizierung, um Event-Nachrichten der Azure-Plattform zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	• Azure Monitor mit OAuth-Authentifizierung integrieren • Azure Monitor mit Standardauthentifizierung integrieren
Bidirektionalen Azure Monitor-Connector konfigurieren	Verwenden Sie den Azure Monitor-Pull-Connector, um Informationen von zu senden ServiceNow Ereignismanagement Zum Azure-Portal.	Standardauthentifizierung
Microsoft Azure MID Push Connector	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Microsoft Azure gesendet wurden. Die Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
BMC TrueSight	Erfassen von JSON-formatierten Event-Nachrichten, die von BMC TrueSight Operations Management (TrueSight) gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
New Relic	Erfassen Sie JSON-formatierte Event-Nachrichten, die von New Relic gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
Dynatrace	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Dynatrace gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren Dynatrace Mit OAuth-Authentifizierung • Integrieren Dynatrace Mit Standardauthentifizierung
Datadog	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Datadog gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren Datadog Mit OAuth-Authentifizierung • Integrieren Datadog Mit Standardauthentifizierung
Catchpoint	Konfigurieren Sie den Catchpoint-Connector für den Empfang von Catchpoint-Ereignissen. Von Ereignismanagement können die Catchpoint-Ereignisse als ServiceNow-Ereignisse verarbeitet werden.	Standardauthentifizierung
Google Cloud Platform (GCP)	Erfassen Sie Event-Nachrichten im JSON-Format, die von GCP gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Google Cloud Platform (GCP) MID Push Connector	Erfassen Sie Event-Nachrichten im JSON-Format, die von GCP gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
Logicmonitor	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Logicmonitor gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Logicmonitor MID Push-Connector	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Logicmonitor gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
Oracle Cloud Push-Connector	Verwenden Sie die Standardauthentifizierung, um Oracle Cloud-Warnungen zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Prometheus	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Prometheus gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Sentry	Konfigurieren Sie den Sentry-Connector, um Sentry-	Standardauthentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
	Ereignisse zu empfangen. Von Ereignismanagement können die Sentry-Ereignisse als ServiceNow-Ereignisse verarbeitet werden.	
SNMP-Traps	SNMP-Traps als Events verarbeiten.	Standardauthentifizierung
ThousandEyes	Erfassen Sie JSON-formatierte Event-Nachrichten, die von ThousandEyes gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren von ThousandEyes mit OAuth-Authentifizierung • Integrieren von ThousandEyes mit Standardauthentifizierung
E-Mail	Konfigurieren Sie eine Aktion für eingehende E-Mails, um E-Mail-Benachrichtigungen zu senden, wenn Events und Warnungen ausgelöst werden.	Standardauthentifizierung
Oracle Enterprise Manager-Trap-Erfassung	Konfigurieren Sie den SNMP-Trap-Connector für den Empfang von Oracle Enterprise Manager Cloud Control-SNMP-Traps. Ereignismanagement kann diese Traps als Events verarbeiten.	Standardauthentifizierung
Grafana	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Grafana gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
EIF-Listener	Konfigurieren Sie den EIF-Listener-Kontext für den Empfang von EIF-Events. Ereignismanagement kann diese EIF-Events als ServiceNow-Events verarbeiten.	Standardauthentifizierung
Honeycomb-Ereignisse integrieren	Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen von Honeycomb, indem Sie Honeycomb als Datenquelle authentifizieren. Legen Sie auf der Honeycomb-Plattform die ServiceNow AI Platform mit einem Webhook als REST-Endpunkt fest.	Standardauthentifizierung
Instana-Events integrieren	Konfigurieren Sie Instana mit Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in der Instana-Konsole.	Standardauthentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
Scout APM-Ereignisse integrieren	Aktivieren Sie die Erfassung von Ereignissen aus Scout APM, indem Sie Scout APM als Datenquelle authentifizieren, mit der sie integriert werden kann Ereignismanagement	Standardauthentifizierung
Panopta als Datenquelle integrieren	Konfigurieren Sie die cloudbasierte Panopta-Überwachungslösung mit Ereignismanagement.	Standardauthentifizierung
URL-Format für generisches JSON Diese URL kann unverändert verwendet werden und erfordert die Konfiguration einer Event-Regel.	Konfigurieren Sie die folgende generische JSON-Ziel-URL und eine Event-Regel zum Erfassen von Events: https://<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source=genericJson.	N/V

ServiceNow-Store – Connectors

Connectors sind im ServiceNow-Store verfügbar. Laden Sie die erforderlichen Inhalte aus dem ServiceNow-Store herunter.

Connectors von Drittanbietern

Connectors sind auch von Drittanbietern verfügbar. Weitere Informationen über verfügbare Connectors und Listeners erhalten Sie von Ihrem Vertriebsmitarbeiter.

Connectors von Drittanbietern	Link
AppDynamics-Servicemodellintegration Verwenden Sie diese Integration, um zu ermöglichen, dass Ihre Instanz AppDynamics Application Performance Monitoring-Daten in Ereignismanagement einspeist.	AppDynamics-Servicemodellintegration
Juniper Mist Verwenden Sie diese Integration, um Managed Service Providern und großen Unternehmen die Möglichkeit zu geben, Echtzeitereignisse und Warnungen von Juniper Mist mit zu integrieren ServiceNow Plattformen Ereignismanagement. Diese Fähigkeit bietet einen standardisierten Ansatz zum Transformieren und Beibehalten von Juniper Mist-Ereignissen in der Tabelle „Ereignismanagement“. Die Ereignisdaten in ServiceNow Ermöglicht Kunden, eigene Incidents basierend auf Standard- oder anwenderdefinierten Warnungsregeln zu	https://store.servicenow.com/$appstore.do#!/store/application/e89296eb1b95561019a8a753604bcb24/1.0.0?referer=%2Fstore%2Fsearch%3Flistingtype%3Dallintegrations%25253Bancillary_app%25253Bcertified_apps%25253Bcontent%25253Bindustry_solution%25253Boem%25253Butility%25253Btemplate%25253Bgenerative_ai%25253Bsnow_solution%26q%3DJuniper%2520Mist&sl=sh

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors von Drittanbietern	Link
erstellen, ohne mit dem Mist-Dashboard zu interagieren.	
Netscout – nGeniusONE-Warnungsintegration Mit dem NETSCOUT-Integrationsmodul kann nGeniusONE erweiterte Warnungen für generieren ServiceNow ITOM mit kontextbezogener Startfähigkeit für Service-Selektierung. ServiceNow ITOM-Anwender können Abfragen in nGeniusONE aus jeder anderen Warnung mit diesem Kontext starten. NGeniusONE-Dashboards und -Berichte unterstützen die Visualisierung dieser Warnungsbedingungen für und von ServiceNow ITOM	Netscout – nGeniusONE-Warnungsintegration
Panopta-Integration Integration dieser Anwendung für die Übertragung von Events in eine Richtung von Panopta an Ereignismanagement.	Panopta-Integration
Splunk Integration Integrieren Sie das Splunk-Add-on mit ServiceNow Damit Splunk-Anwender Incidents und Ereignisse in erstellen können Ereignismanagement. Weitere Informationen zur Konfiguration dieser Integration finden Sie unter Splunk-Add-on für ServiceNow .	Splunk-Integration
ScienceLogic Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von ScienceLogic an Event Management	ScienceLogic-Integration
SevOne Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von SevOne an Event Management	SevOne-Integration
Site24X7 Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von Site24x7 an Event Management	Site24x7-Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen benutzerdefinierten Pull-Connector

Sie können einen benutzerdefinierten Pull-Connector erstellen, der ein Skript, eine Connector-Definition und eine Connector-Instanz erfordert, um Events im Namen einer Event-Quelle abzurufen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein benutzerdefiniertes Connector-Skript kann Remote-API-Aufrufe für eine neue Event-Quelle ausführen, um Events an die ServiceNow-Instanz zu senden. Sie können ein Skript erstellen und es dann als Teil einer neuen Ereignismanagement-Connector-Definition und Connector-Instanz hinzufügen. Dieses Verfahren erstellt automatisch eine JavaScript-Codedatei mit dem Namen, den Sie in eingeben **Name** Feld als Dateiname. Der anwenderdefinierte JavaScript-Code, der diese Aktionen durchführt, muss:

- Verbindung mit einem Event-Überwachungstool herstellen
- Events aus einem Event-Überwachungstool abrufen
- Events mithilfe einer Webservice-API an die Tabelle Event [em_event] senden Siehe REST-API .

Jede Connector-Definition ist spezifisch für einen Event-Quellenanbieter. Die Connector-Definition gibt die MID Server-Skripteinbindung an, die Events aus der externen Event-Quelle abruft. Darüber hinaus gibt die Connector-Definition an, welche Connector-Instanzwertparameter erforderlich sind, um eine Verbindung mit dem externen Event-Quellhost herzustellen.

Prozedur

1. Erstellen Sie eine benutzerdefinierte MID Server-Skripteinbindung.
   In diesem Beispiel wird Groovy (veraltet) verwendet. Anstelle einer Skripteinbindung in Groovy wird die Verwendung von JavaScript empfohlen.

   a. Implementieren Sie diese Methoden:
      - `@Override OperationStatus testConnection()`
      - `@Override OperationStatus execute()`

   b. Entwerfen Sie die Klasse, um den `ThirdPartyConnector` zu erweitern.

      Example

      ```
      public class HypericConnector extends ThirdPartyConnector
      ```

   c. Importieren Sie Plattformklassen für Event-Erstellung, -versand, -protokollierung und Connector-Basisklassen von Drittanbietern.

      Example

      ```
      package com.service_now.mid.probe.tpcon.test

      import com.glide.util.Log
      import com.service_now.mid.MIDServer
      import com.service_now.mid.probe.event.IEventSender
      import com.service_now.mid.probe.event.SNEventSender
      import com.service_now.mid.probe.tpcon.OperationStatus
      ```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
import com.service_now.mid.probe.tpcon.OperationStatusType
import com.service_now.mid.probe.tpcon.ThirdPartyConnector
import com.snc.commons.eventmgmt.Event
```

d. Stellen Sie über die vom Sammler bereitgestellte API eine Verbindung zum Datensammler her, z. B. SCOM oder VMware vRealize Hyperic (Hyperic).

e. Verwenden Sie die *`context`*-Parameter, um die Ereignisfeldwerte festzulegen, die von einer Connector-Instanz stammen.

Example

```
def authString = (context.username +
 ':'+ context.password).getBytes().encodeBase64().toString()
def urlStr = 'http://'+context.host + ':' + context.parameters.port + '/' + apiFunction
```

f. Implementieren Sie die *`Ausführungsfunktion`* im Skript.
Es liest Events vom Connector mithilfe seiner API, um Event-Objekte zu erstellen und an die ServiceNow-Instanz zu senden. Zum Beispiel:

Example

```
GPathResult alertsResponse1 = readAlerts('hqu/hqapi1/alert/find.hqu?begin=' +
 lastSignatureStr +
'&end='+ tillStr +'&count=1000000&severity=1&inEscalation=false&notFixed=false');
Event event = new Event()
event.emsSystem = context.name
event.source = "Hyperic"
event.description = it.@reason
event.type = it.@name
...
IEventSender eventSender = MIDServer.getSingleton(SNEventSender.class)
   for (Event event  : list) {
      eventSender.sendEvent(event)
    }
```

2. Navigieren zu **MID-Server** > **MID-Serverskriptdateien** Und erstellen Sie ein Skript.
3. Geben Sie das Feld **Übergeordnet** als *`Groovy`* an, füllen Sie das Formular entsprechend aus, und klicken Sie dann auf **Senden**.
4. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen** Und erstellen Sie eine Connector-Definition.
5. Wählen Sie im Feld **Auszuführendes Groovy-Skript** die MID Server-Skriptdatei aus und füllen Sie das Formular entsprechend aus.
   Zusätzlich zum **Benutzernamen** oder **Host** können Sie weitere Parameter, z. B. **Port**, hinzufügen und dann auf **Senden** klicken.
6. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen** Und erstellen Sie eine Connector-Instanz.
7. Wählen Sie im Feld **Connector-Definition** die Connector-Definition aus, füllen Sie das Formular entsprechend aus, und klicken Sie dann auf **Senden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Zum Bestätigen oder Debuggen des Skripts verwenden Sie Debug-Ausdrucke von Groovy im MID Serverprotokoll.
9. Um eingehende Ereignisse mit der anwenderdefinierten Connector-Instanz zu überwachen, navigieren Sie zu **ECC** > **Warteschlange** Und filtern nach **ConnectorProbe** .
10. Erstellen Sie eine anwenderdefinierte Connector-Definition.
    a. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen**an.
    b. Klicken Sie auf **Neu**.
    c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Connector-Definition ein.
    d. Wählen Sie im Feld **Skripttyp** die Option **Javascript** aus.
    e. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
    Das Feld **Javascript ausführen** wird automatisch mit dem Namen der JavaScript-Vorlagendatei ausgefüllt.
11. Klicken Sie zum Bearbeiten der standardmäßigen JavaScript-Datei auf das Informationssymbol ( ) Rechts neben dem JavaScript-Dateinamen, und führen Sie die folgenden Schritte aus:
    a. Geben Sie die erforderlichen Informationen für die Funktion **testConnection** an.
    Diese Funktion testet die Connector-Definition, um sicherzustellen, dass die Verbindung mit dem Ziel gültig ist.
    b. Geben Sie die erforderlichen Informationen für die Funktion **execute** an.
    Diese Funktion ruft die Informationen aus der externen Quelle ab.
    c. Geben Sie die erforderlichen Informationen für die Funktion **retrieveKpi** an.
    Diese Funktion ruft die Metrikdaten aus der externen Quelle ab.
12. **Wahlweise:** Sie können das Standard-JavaScript durch Ihren JavaScript-Code ersetzen.
13. Füllen Sie die Felder entsprechend aus.

Formular Connector-Definition

Feld	Beschreibung
Standardzeitplan	Die Anzahl der Sekunden zwischen Versuchen, Events zu empfangen.
Bidirektional	Geben Sie an, dass das externe Überwachungssystem aktualisiert werden soll, wenn die Warnung geändert wird. Für SCOM ist eine Standardimplementierung vorhanden.
Bezeichner für Warnungsfeld	Geben Sie an, dass das externe Überwachungssystem aktualisiert werden soll, wenn das Warnungsfeld manuell geändert wird. **Hinweis:** Dieses Feld ist nur sichtbar, wenn **Bidirektional** ausgewählt ist.
Metriken erfassen	Wählen Sie diese Option aus, um die Erfassung von Metriken zu aktivieren. **Hinweis:** Metriken werden nur für externe SCOM-Event-Quellen erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standardzeitplan für Metrikerfassung (Sekunden)	Geben Sie die Anzahl der Sekunden an Informationen an, die erfasst werden müssen. Der Standardwert beträgt 10 Sekunden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn **Metriken erfassen** ausgewählt ist.
Connector-Parameter	Geben Sie die Parameter an, um die Kommunikation mit einem Event-Server zu ermöglichen.
Connector-Definition zu MID-Server-Fähigkeiten	Der MID-Server-Name zur Verarbeitung von Events vom Event-Server. Wenn nicht angegeben, wird ein verfügbarer MID-Server verwendet.

14. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen Pull-Connector

Konfigurieren Sie einen Pull-Connector, um die Häufigkeit der Ereigniserfassung zu planen .

Vorbereitungen

Bevor Sie dieses Verfahren beginnen:

- Suchen oder definieren Sie eine Connector-Definition.
- Erstellen Sie die Anmeldeinformationen, um eine Verbindung zur Event-Quelle herzustellen.
- Wenn die Connector-Instanz für die Sammlung von verwendet werden soll Metrikdaten Metrikdaten, die Metrikdaten Plugin muss aktiviert sein.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Connector-Instanz verwenden, um den Ort und die Art und Weise zu steuern, in der Events aus externen Quellen ankommen. Sie können optional zum Sammeln auswählen Metrikdaten Informationen aus den externen Quellen, mit denen Sie eine Verbindung herstellen. Die Metrikdaten Die Funktion dient zur Analyse von Trends, Schwellenwertdefinitionen und Anomalieerkennung. Sie können einen Test ausführen, um zu bestätigen, dass Connector-Instanzparameter zulassen, dass der MID-Server Events von einer unterstützten externen Event-Quelle an die Event-Tabelle [em_event] empfängt. Der Test bestätigt auch:

- Der MID-Server wird ausgeführt.
- Der Host wird mit der IP-Adresse ausgeführt, die sich im Feld **Host-IP** befindet.
- Sowohl der MID-Server als auch der Host werden in derselben Domäne ausgeführt.
- Die Wertfelder der Connector-Instanz sind gültig.
- Zum Abrufen von Events kann über die API eine Verbindung zur Event-Quelle hergestellt werden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder entsprechend aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Ein eindeutiger Name für den Connector-Instanzdatensatz, z. B. der Name des Event-Quellhosts.
Beschreibung	Alle optionalen Informationen, die der Administrator zur Identifizierung dieses Datensatzes verwenden möchte.
Connector-Definition **Hinweis:** Metrikdaten Connectors (z. B. AWS CloudWatch und AzureConnector) werden im Basissystem nur angezeigt, wenn der Metrikdaten Plugin (com.snc.sa.metric) ist aktiviert.	Lieferant und Protokoll, die zum Sammeln von Ereignissen aus der externen Quelle verwendet werden. Wählen Sie die Connector-Definition aus, die der Quelle externer Events entspricht. Die im Basissystem verfügbaren Optionen sind z. B.: ○ AWS CloudWatch ○ AzureConnector ○ HPOM ○ IBM Netcool ○ NagiosXI ○ NNMi ○ OMi ○ SCOM ○ SolarWinds ○ Op5 ○ PRTG ○ vCenter ○ Zabbix Eine Liste der im Basissystem verfügbaren Connector-Definitionen finden Sie unter Konfigurieren Ereignismanagement Connectors.
Host-IP	Die IP-Adresse des Event-Quellhosts. Das System verwendet diese IP-Adresse, um den entsprechenden MID-Server für die Kommunikation mit dem Event-Quellhost auszuwählen.
Anmeldeinformationen	Der Datensatz aus der Tabelle „Anmeldeinformationen“ [discovery_credentials], der gültige Anmeldeinformationen für den Event-Quellhost enthält.
Zeit der letzten Ausführung der Event-Erfassung	Datum und Uhrzeit des letzten Event-Imports. Das Feld wird automatisch mit einem Wert ausgefüllt.
Letzter Event-Erfassungsstatus	Der Status des letzten Imports. Das Feld wird automatisch mit einem Wert ausgefüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Keine**– Es wurde noch keine gültige Verbindung hergestellt. ○ **Erfolgreich** – Es wurde eine erfolgreiche Verbindung hergestellt. ○ **Fehler** – Es wurde eine Verbindung hergestellt. Die externe Event-Quelle wurde jedoch nicht aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events aus der externen Event-Quelle sucht. Dieser Wert darf nicht unter dem Mindestwert für die Zeitplan-Eigenschaft liegen, die standardmäßig 120 Sekunden beträgt.
Letzte Fehlermeldung	Letzte Fehlermeldung, die vom Connector empfangen wurde Wenn der Test-Connector fehlschlägt, wird in diesem Feld eine Fehlermeldung angezeigt.
Aktiv	Diese Option wird erst angezeigt, nachdem das Formular gespeichert wurde. Aktivieren Sie dieses Kontrollkästchen erst, nachdem Sie die Verbindung zwischen MID-Server und dem Connector getestet haben. Aktivieren Sie dieses Kontrollkästchen, um das Abrufen von Events aus dieser externen Event-Quelle zu aktivieren.
Bidirektional	Wählen Sie diese Option, um die bidirektionale Option aufzurufen. Diese Option ist nur verfügbar, wenn die angegebene Connector-Definition mit bidirektionalen Werten konfiguriert wurde. Wenn diese Option ausgewählt ist, ermöglicht sie den bidirektionalen Austausch von Werten mit der externen Ereignis-Quelle. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt ist. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Letzter bidirektionaler Status	Das Feld wird automatisch mit einem Wert ausgefüllt. Die Statuswerte sind: ○ **Keine**– Es wurde noch keine gültige Verbindung hergestellt. ○ **Erfolgreich** – Es wurde eine erfolgreiche Verbindung hergestellt. ○ **Fehler** – Es wurde eine Verbindung hergestellt. Die externe Event-Quelle wurde jedoch nicht aktualisiert. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikensammlung	Gibt die Sammlung von an Metrikdaten Metrikdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Der Metrik-Connector unterstützt das Arbeiten mit der SCOM-Datenbank (MSSQL), die für die Verwendung mit SSL konfiguriert ist. Diese Option wird nur angezeigt, wenn die Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Zeit der letzten Ausführung der Metrikerfassung	Das Datum und die Uhrzeit der letzten Metrikdatenerfassung. Das Feld wird automatisch mit einem Wert ausgefüllt.
Letzter Metrikerfassungsstatus	Status der Aktivität zur Erfassung von Metrikdaten. Das Feld wird automatisch mit einem Wert ausgefüllt. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die **Metrikerfassung** (z. B. SCOM) unterstützt und die Option „ Metrikerfassung“ ausgewählt ist.
Zeitplan für Metrikerfassung (Sekunden)	Die Zeit in Sekunden zur Wiederholung des geplanten Auftrags zur Metrikdatenerfassung. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die **Metrikerfassung** (z. B. SCOM) unterstützt und die Option „ Metrikerfassung“ ausgewählt ist.
Metrikdatenbank-Host	Geben Sie entweder die IP-Adresse oder den Hostnamen des Metrikdatenbank-Hosts ein. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Verbindung mithilfe einer benannten Instanz	Bei Auswahl dieser Option geben Sie die benannte MSSQL-Instanz an, mit der eine Verbindung hergestellt werden soll. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikendatenbank – benannte Instanz	Der Name der Metrikdatenbank-Instanz. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Metrikdatenbank-Port	Der von der Metrikdatenbank verwendete Port. Die Verbindung wird über JDBC hergestellt. Der Basissystemwert ist 1.433. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Datenbankanmeldung mit Windows-Authentifizierung	Bei Auswahl dieser Option erfolgt die Datenbankanmeldung mit dem Anmeldebenutzernamen, der im MID Server-Service definiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikensammlung wird ausgeführt	Wenn diese Option ausgewählt ist, wird angegeben, dass Metrikdaten Sammlung wird ausgeführt. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Metrikdatenbank-Anmeldeinformationen	Anmeldeinformationen für die Metrikdatenbank. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Connector-Instanzwerte	Die zugehörige Liste mit Verbindungsparametern für den Event-Quellenhost. Die Liste der Parameter hängt von der ausgewählten Connector-Definition ab.
MID Server für Connectors	Der Name des MID-Server zur Verarbeitung von Events vom Event-Server.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Klicken Sie auf **Connector testen**, um sicherzustellen, dass der MID-Server mit dem externen Serverhost kommunizieren kann.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen auf der Seite, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus. Die Beschreibung der Fehlerursache wird im MID-Server-Protokoll entsprechend dem Fehlertyp angezeigt, z. B. Events, Metriken oder bidirektional.
7. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.
8. Bestätigen Sie, dass Ereignismanagement Events mit dieser Connector-Instanz verarbeitet, indem Sie ein Event manuell erstellen.

Zugehörige Informationen

Konfigurieren Ereignismanagement Connectors

Standardmäßigen MID Server für Connectors konfigurieren

Sie können einen standardmäßigen MID Server für Connectors festlegen, um sicherzustellen, dass immer ein MID Server für den Empfang von externen Events verfügbar ist.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Der standardmäßige MID Server muss Konnektivität zu allen externen Event-Quellen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein, um die Tabelle zu den Systemeigenschaften [sys_properties] zu öffnen.
2. Wählen Sie die Systemeigenschaft mid.server.connector_default aus.
3. Füllen Sie im Formular die Felder aus.

Aufgabenvorlagenformular

Feld	Beschreibung
mid.server.connector_default	Standardmäßiger MID Server für Connectors Bestimmt die zu verwendenden MID Server-Connectors, wenn kein MID Server angegeben ist. Muss mit einem MID Server-Namen übereinstimmen. ○ **Typ**: Wählen Sie Zeichenfolge aus der Liste aus. ○ **Wert**: Geben Sie den Namen eines vorhandenen MID Servers ein, z. B. SNC MID Server. ○ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Hinweis: Sie können den standardmäßigen MID Server zurücksetzen, indem Sie die Eigenschaft *mid.server.connector_default* löschen oder den Wert dieser Eigenschaft auf einen anderen MID Server aktualisieren. Diese Eigenschaft wird nicht in allen Szenarien automatisch zurückgesetzt.

4. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie Dynatrace Metriken-Connector-Instanz

Konfigurieren Sie Dynatrace Zu empfangende Connector-Instanz Metrikdaten Rohdaten aus dem Dynatrace Server.

Vorbereitungen

Um die Metriksammlung zu aktivieren, stellen Sie sicher, dass MID-Server Die Metriken abruft, wird mit konfiguriert Metrikdaten Erweiterung und , in der sich die Erweiterung befindet **Gestartet** Modus. Weitere Informationen finden Sie unter Konfigurieren Sie manuell Metrikdaten Erweiterung.

- Erstellen Sie ein Zugriffstoken in Dynatrace Mit Umfangsberechtigungen „Metriken lesen“ (metrics.read), um das Abrufen von Metrikdaten zu ermöglichen. Dieses Token wird im -Connector zum Aufrufen von verwendet Dynatrace REST-API.
- Konfigurieren Sie den Service Graph Connector für Dynatrace. Dies wird in der Instanz konfiguriert und wird erkannt Dynatrace CIs. Weitere Informationen zum Konfigurieren dieses Connectors finden Sie unter Konfigurieren Service Graph Connector für Observability – Dynatrace Mit geführtem Setup .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ist Dynatrace Service Graph Connector erkennt CIs und unterstützt die Metrikerfassung für die folgenden Entitätstypen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- HOST
- ANWENDUNG
- SERVICE
- PROCESS_GROUP_INSTANCE

Konfigurieren Sie andere Entitätsmetriken für die Sammlung, wenn Sie Ereignisregeln für die CI-Bindung erstellen.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie Aus **Neu** Und erstellen Sie eine Connector-Instanz.
   Details zu den Feldern der Connector-Instanz, die auf der Seite angezeigt werden, finden Sie unter Dynatrace Formular „Connector-Instanz“.
3. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. **Wahlweise:** Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen bearbeiten Dynatrace Parameter.
   Details zu den Parametern des Connector-Instanzwerts finden Sie unter Dynatrace Parameter des Connector-Instanzwerts.
5. In MID Servers Fügen Sie für den Abschnitt „Connectors“ ein hinzu MID-Server Für Dynatrace Zu verwendender Connector.
6. Wählen Sie im Abschnitt zugehörige Links die Option aus **Konfigurieren Sie die zu erfassenden Metriken** .
   Nur Metriken mit dem Wert **Aktiv=wahr** Werden von der Instanz erfasst.
7. Konfigurieren Sie die Metriken, die die Instanz mit dem Wert erfassen soll **Aktiv=wahr** .
   Metriken mit dem Wert **Aktiv=falsch** Werden nicht von der Instanz erfasst.
8. **Wahlweise:** Wählen Sie Aus **Neu** Zum Erstellen neuer Metriken.
   Konfigurieren Sie die Felder auf der Seite „Connector-Instanzmetriken – neuer Datensatz“ (sn_em_Connector_instance_metric).

Seite mit Connector-Instanzmetriken – neuer Datensatz

Feld	Beschreibung
Metrikname	Anzeigename für die Metrik, die in konfiguriert werden soll ServiceNow Instanz.
Metrik-Connector-Instanz	Standardmäßig auf festgelegt **Dynatrace-Connector-Instanz** . Alle Metriken werden für erfasst Dynatrace Connector-Instanz.
Metriktyp	Der Name des Dynatrace Entitätstyp, zu dem die Metrik gehört.
Metrik-ID	Die Dynatrace Metrik-ID der erfassten Metrik.
Aktiv	Wählen Sie für die zu erfassenden Metriken aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass die CIs im Zusammenhang mit den Metriken in der Instanz vorhanden sind.
- Erstellen Sie eine Ereignisregel, um die CI-Bindung nach Bedarf durchzuführen. Details finden Sie unter Event-Regel erstellen oder bearbeiten.

9. Wählen Sie Aus **Testen Sie Den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
10. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

Konfigurieren Sie die Connector-Instanz für Nagios-Metriken

Konfigurieren Sie die zu empfangende Nagios-Metrik-Connector-Instanz Metrikdaten Rohdaten vom Nagios-Server.

Vorbereitungen

Um die Metriksammlung zu aktivieren, stellen Sie sicher, dass MID-Server Die Metriken abruft, wird mit konfiguriert Metrikdaten Erweiterung und , in der sich die Erweiterung befindet **Gestartet** Modus. Weitere Informationen finden Sie unter Konfigurieren Sie manuell Metrikdaten Erweiterung.

- Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung auf ServiceNow Instanz mit Anwendername und Passwort der Nagios SQL-Datenbank.
- ServiceNow Unterstützt Discovery für Nagios nicht. Erstellen Sie daher den CI-Eintrag manuell in der entsprechenden Tabelle unter Verwendung des auf der Nagios-Plattform konfigurierten Hostnamens.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig erfolgt die CI-Bindung für die folgenden Entitäten:

- HOST-HTTP-Endpunkt: Die Ereignisregel gilt für die Nagios-Metrik HTTP, wenn Sie eine Prüfung ausführen, die „command_Name“ als „Service_http“ enthält.
- MySQL-Instanz: Die Ereignisregel gilt für die Nagios-Metrik MySQL, wenn Sie eine Prüfung ausführen, die „command_Name“ als mysql enthält.

Wenn Sie andere Prüfungen an HTTP-Endpunkten oder MySQL ausführen, können Sie die vorhandene Ereignisregel bearbeiten, um Command_Name hinzuzufügen. Konfigurieren Sie für andere Entitäten Ereignisregeln basierend auf CI-Bindungsanforderungen.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie Aus **Neu** Und erstellen Sie eine Connector-Instanz.
   Details zu den Feldern der Connector-Instanz, die auf der Seite angezeigt werden, finden Sie unter Formular „Nagios-Connector-Instanz“.
3. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Wahlweise:** Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen Nagios-Parameter bearbeiten.
   Details zu den Parametern des Connector-Instanzwerts finden Sie unter Nagios-Connector-Instanzwertparameter.
5. In MID Servers Fügen Sie für den Abschnitt „Connectors“ ein hinzu MID-Server Für den zu verwendenden Nagios-Connector.
6. Stellen Sie sicher, dass die CIs im Zusammenhang mit den Metriken in der Instanz vorhanden sind.
7. Erstellen Sie eine Ereignisregel, um die CI-Bindung nach Bedarf durchzuführen.
   Details finden Sie unter Event-Regel erstellen oder bearbeiten.
8. Wählen Sie Aus **Testen Sie Den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
9. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

Konfigurieren Sie die Connector-Instanz für Zabbix-Metriken

Konfigurieren Sie die zu empfangende Zabbix Metric-Connector-Instanz Metrikdaten Rohdaten vom Zabbix-Server.

Vorbereitungen

Um die Metriksammlung zu aktivieren, stellen Sie sicher, dass MID-Server Die Metriken abruft, wird mit konfiguriert Metrikdaten Erweiterung und , in der sich die Erweiterung befindet **Gestartet** Modus. Weitere Informationen finden Sie unter Konfigurieren Sie manuell Metrikdaten Erweiterung.

Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung auf ServiceNow Instanz mit Zabbix-Server-Anwendername und Passwort.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

ServiceNow Unterstützt keine Discovery für Zabbix, daher müssen CI-Einträge manuell in der entsprechenden Tabelle mit dem in der Zabbix-Plattform konfigurierten Hostnamen erstellt werden.

- Erstellen Sie eine Ereignisregel, um bestimmte CIs zu binden.
- Anwender können Zabbix-Elementen Tag-Informationen hinzufügen, und die relevanten Tags werden in die Metrik-zu-CI-Datensätze aufgenommen. Diese Tags können auch als Filterbedingungen in der Ereignisregel für die CI-Bindung verwendet werden.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie Aus **Neu** Und erstellen Sie eine Connector-Instanz.
   Details zu den Feldern der Connector-Instanz, die auf der Seite angezeigt werden, finden Sie unter Zabbix Formular „Connector-Instanz“.
3. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. **Wahlweise:** Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen Zabbix-Parameter bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zu den Parametern des Connector-Instanzwerts finden Sie unter Parameter des Zabbix-Connector-Instanzwerts.

5. In MID Servers Fügen Sie für den Abschnitt „Connectors“ ein hinzu MID-Server Für den Zabbix-Connector zu verwenden.
6. Wählen Sie Aus **Testen Sie Den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
7. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

Hinweis: ServiceNow Unterstützt nur nicht signierte Gleitkommazahlen und Ganzzahlmetriktypen ohne Signatur für Zabbix.

Konfigurieren Sie die SolarWinds-Metriken-Connector-Instanz

Konfigurieren Sie die SolarWinds-Connector-Instanz für den Empfang Metrikdaten Rohdaten vom SolarWinds-Server.

Vorbereitungen

Um die Metriksammlung zu aktivieren, stellen Sie sicher, dass MID-Server Die Metriken abruft, wird mit konfiguriert Metrikdaten Erweiterung und , in der sich die Erweiterung befindet **Gestartet** Modus. Weitere Informationen finden Sie unter Konfigurieren Sie manuell Metrikdaten Erweiterung.

Konfigurieren Sie den Service Graph Connector für SolarWinds. Dies wird in der Instanz konfiguriert und erkennt SolarWinds-CIs. Weitere Informationen zum Konfigurieren dieses Connectors finden Sie unter Service Graph Connector für SolarWinds .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig erfasst SolarWinds Metric Connector Metriken aus den folgenden Tabellen:

- Orion.CPULaden
- Orion.NPM.InterfaceTraffic
- Orion.VolumeLeistungsverlauf
- Orion.VolumeNutzungsverlauf
- Orion.Antwortzeit

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie Aus **Neu** Und erstellen Sie eine Connector-Instanz.
   Details zu den Feldern der Connector-Instanz, die auf der Seite angezeigt werden, finden Sie unter Formular „SolarWinds-Connector-Instanz“.
3. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. **Wahlweise:** Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen SolarWinds-Parameter bearbeiten.
   Details zu den Parametern des Connector-Instanzwerts finden Sie unter Parameter für SolarWinds-Connector-Instanzwert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In MID Servers Fügen Sie für den Abschnitt „Connectors“ ein hinzu MID-Server Für den SolarWinds-Connector zu verwenden.
6. Wählen Sie im Abschnitt zugehörige Links die Option aus **Konfigurieren Sie die zu erfassenden Metriken** .
   Nur Metriken mit dem Wert **Aktiv=wahr** Werden von der Instanz erfasst.
7. Konfigurieren Sie die Metriken, die die Instanz mit dem Wert erfassen soll **Aktiv=wahr** .
   Metriken mit dem Wert **Aktiv=falsch** Werden nicht von der Instanz erfasst.
8. **Wahlweise:** Wählen Sie Aus **Neu** Zum Erstellen neuer Metriken.
   Konfigurieren Sie die Felder auf der Seite „Connector-Instanzmetriken – neuer Datensatz“ (sn_em_Connector_instance_metrics_solarwinds).

Seite mit Connector-Instanzmetriken – neuer Datensatz

Feld	Beschreibung
Metrikname	Name für die Metrik, die in konfiguriert werden soll ServiceNow Instanz.
Metrik-Connector-Instanz	Standardmäßig auf festgelegt **SolarWinds-Connector-Instanz** . Alle Metriken werden für die SolarWinds-Connector-Instanz erfasst.
Zusätzliche Spalten	(Optional) Liste zusätzlicher Spalten, die für CI-bezogene Informationen abgerufen werden sollen. Beispiel: Datetime, Knoten, Ressource. Wenn **Datum/Uhrzeit** Ist nicht angegeben, die aktuelle Zeit wird als Metrikzeitstempel verwendet. Wenn **Knoten** Und **Ressource** Werden angegeben, werden sie entsprechend ausgefüllt. Um Felder aus einer übergeordneten Tabelle zu referenzieren, verwenden Sie das Dot-Walking-Format, z. B. `Schnittstelle.Schnittstellenname` . Ob ein Feld ein bestimmtes Standardfeld ausfüllen soll (z. B. **Ressource**), verwenden Sie einen Alias mit demselben Namen. Beispiel: Zu verwenden `Schnittstellenname` Geben Sie sie als Ressource an `Interface.InterfaceName ALS Ressource` .
Tabellenname	Name der Tabelle, aus der Metriken erfasst werden.

   - Stellen Sie sicher, dass die CIs im Zusammenhang mit den Metriken in der Instanz vorhanden sind.
   - Erstellen Sie eine Ereignisregel, um die CI-Bindung nach Bedarf durchzuführen. Details finden Sie unter Event-Regel erstellen oder bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie Aus **Testen Sie Den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
10. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

> **Hinweis:** Stellen Sie sicher **Registrierungsmodus** Ist für die SolarWinds-Quelle in der Tabelle „Metrikquellen“ aktiviert.

Event-Erfassung von HP OMi konfigurieren

Konfigurieren Sie die Connector-Instanz von HP Operations Manager (OMi) für den Empfang von Warnungen vom HP OMi-Server.

Vorbereitungen

Unterstützte Versionen: 10.01, 10.10, 10.11, 10.12, 10.60, und 10.61.
Der OMi-Connector wird in Versionen unter Version 10 nicht unterstützt.

Erstellen Sie den Standardauthentifizierungstyp für Anmeldeinformationen, um eine Verbindung mit OMI herzustellen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

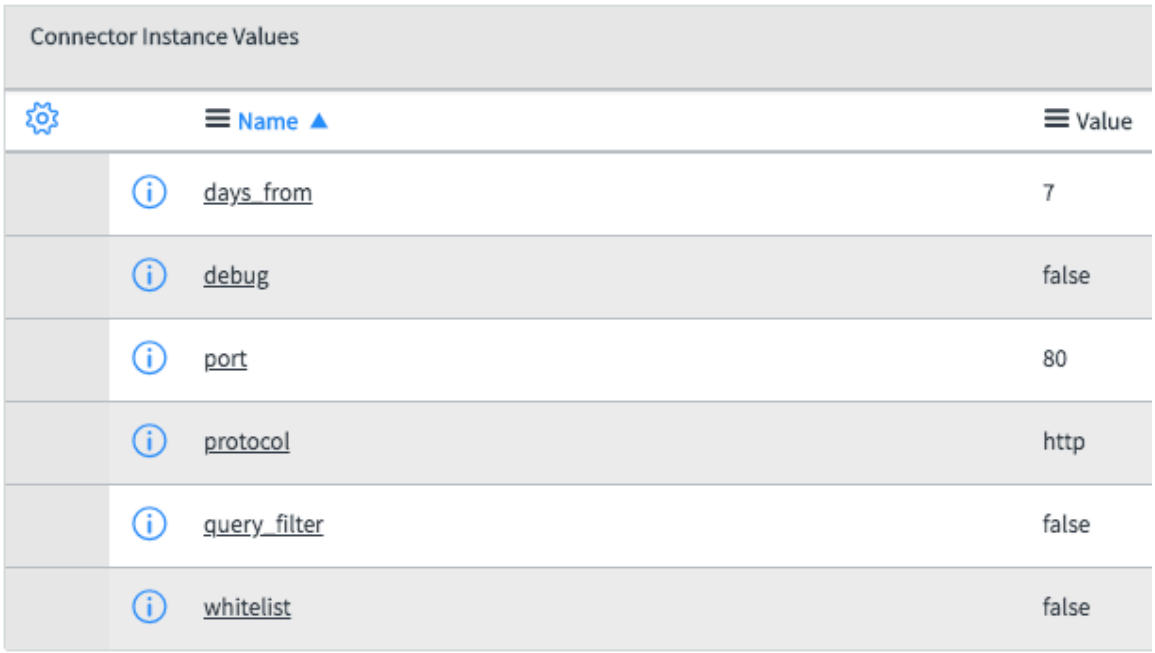
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den OMi-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OMi-Event-Erfassung.
Host-IP	Geben Sie die OMi-IP-Adresse an.
Anmeldeinformationen	Klicken Sie in das Feld **Anmeldeinformationen**. Wählen Sie Anmeldeinformationen für die Standardauthentifizierung aus der Liste aus, oder klicken Sie auf das Suchsymbol. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen mit dem Typ „Standardauthentifizierung“. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „OMiOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von OMi sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Connector-Definition	Wählen Sie **OMi** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt MID-Server für Connectors einen an MID-Server Das ist aktiv und gültig. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.



4. Geben Sie im Abschnitt Connector-Instanzwerte die OMi-Werte an.

   a. **days_from**.
   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen.
   Standardwert: `7`.

   b. **debug**.
   Standardwert: `false`. Zum Aufrufen des Debug-Modus geben Sie `true` an.

   c. **port**.
   Standardwert: `80`.

   d. **protocol**.
   Standardwert: `http`.

   e. **query_filter**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardwert: false. Wenn Sie diesen zusätzlichen Filter zum Abfragen von Events verwenden möchten, geben Sie die Event-Attribute an. Beispiel: assigned_user = „admin“ UND title = „My Title“. Die Abfragefilterkriterien sind:

- Eine Filtereigenschaft, die ein Event-Attribut angibt, z. B. related_ci
- Ein unterstützter Operator, z. B. ODER oder UND
- Ein Wert für die Filtereigenschaft, z. B. admin oder integrator

Alles aus dem Feld „query_filter“ wird einer URL-Codierung unterzogen und dann als Parameter an den OMi-API-Aufruf übergeben. Ausführliche Informationen zum Erstellen der Filterabfrage finden Sie unter „Filtern nach Event-Attributen: query“ im HP OMi-Erweiterungsleitfaden. Um beispielsweise die Events nach einer Liste von Events abzufragen, die dem Administrator zugewiesen sind, geben Sie Folgendes an:

```
event_list?query=assigned_user%20EQ%20"admin"
```

Zum Verschachteln von query_filter-Event-Attributen geben Sie die Hierarchie in eckigen Klammern „[]“ an.

f. Aufnahmeliste.
Standardwert: false. Geben Sie eine kommagetrennte Liste an, damit dieses Feature Attribute hinzufügt, die erfasst und dem Feld Ereignismanagement **Zusätzliche Informationen** hinzugefügt werden sollen.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum HP OMi-Server zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Event-Erfassung von HPOM konfigurieren

Konfigurieren Sie die Connector-Instanz von HPOM für den Empfang von Events vom HP Operations Manager (HPOM).

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin
Unterstützte Version: 08.60.005.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine HPOM-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die HPOM-Connector-Instanz an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Host-IP	Geben Sie die HPOM-IP-Adresse an.
Anmeldeinformationen	Klicken Sie in das Feld **Anmeldeinformationen**. Wählen Sie Anmeldeinformationen aus der Liste aus, oder klicken Sie auf das Suchsymbol. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „HPOMOPS“.
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von HPOM sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der HPOM-Ereignissammlung ein.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie die **HPOM**-Connector-Definition aus.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**. Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen HPOM-Parameter an.
   - **driver**. Geben Sie den Treiber an, der für den Aufruf verwendet werden soll. Dieser Treiber ist spezifisch für den Typ der Datenbank, die Sie aufrufen.
     - Geben Sie für einen IBM DB2 Universal-Treiber Folgendes ein: com.ibm.db2.jcc.DB2Driver
     - Geben Sie für einen Oracle-Treiber Folgendes ein: oracle.jdbc.OracleDriver
     - Geben Sie für einen Microsoft SQL-Treiber Folgendes ein: com.microsoft.sqlserver.jdbc.SQLServerDriver
     - Geben Sie für einen MySQL-Treiber Folgendes an: com.mysql.jdbc.Driver
     - Geben Sie für einen Sybase-Treiber Folgendes an: com.sybase.jdbc3.jdbc.SybDriver
   - **url**. Geben Sie eine URL an. Das JDBC-Protokoll verwendet eine Verbindungszeichenfolge, um die Authentifizierung herzustellen, und andere Parameter, um eine Verbindung zwischen dem Client und der Datenbank herzustellen. Jede Datenbank verfügt über ein eigenes Format für Verbindungszeichenfolgen. Ersetzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie in den folgenden URLs die Variablen, z. B. <username> und <password> mit Ihren Werten.

- Geben Sie für eine universelle IBM DB2-URL Folgendes an: [jdbc:db2://sysmvs1.stl.ibm.com:<port number>/<database name>:user=<username>;password=<password>]

  Beispiel: jdbc:db2://sysmvs1.stl.ibm.com:5021/regionsdb:user=example;password=wlrs21.

- Geben Sie für eine Oracle-URL Folgendes an: [jdbc:oracle:thin:@<IP address>:<port number>:<database name>]

  Beispiel: jdbc:oracle:thin:@172.31.255.255:4028:OracleMain.

- Geben Sie für eine Microsoft SQL-URL Folgendes an: [jdbc:sqlserver://<IP address>;user=<username>;password=<password>]

  Beispiel: jdbc:sqlserver://localhost;user=example;password=w3lrs2.

- Geben Sie für eine MySQL-URL Folgendes an: [jdbc:mysql://<IP address>/database?user=<username>;password=<password>]

  Beispiel: jdbc:mysql://localhost/database?user=example;password=65wlrs.

- Geben Sie für eine Sybase-URL Folgendes an: [jdbc:sybase:Tds:<IP address>:<port number>/<database name>?user=<username>;password=<password>]

  Beispiel: jdbc:sybase:Tds:172.31.255.255:4100/SYBMAIN?user=example;password=wlrs1m.

5. Verwenden Sie ein Netzwerk-Tool wie Ping, um sicherzustellen, dass der HPOM-Server ausgeführt wird und die IP-Adresse mit dem Wert im Feld *Host IP* übereinstimmt.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem HPOM-Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum HPOM-Server zu überprüfen.

8. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

Event-Erfassung von Hyperic konfigurieren

Konfigurieren Sie die Hyperic-Connector-Instanz für den Empfang von Events vom VMware vRealize Hyperic-Server.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Version: 5,8.4,0.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Hyperic-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die Hyperic-Connector-Instanz an.
Host-IP	Geben Sie die Hyperic-IP-Adresse an.
Anmeldeinformationen	Klicken Sie im Formular Anmeldeinformationen auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Speichern Sie die Anmeldeinformationen unter einem eindeutigen und erkennbaren Namen, z. B. „HypericOPS“.
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von Hyperic sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der Hyperic-Ereignissammlung ein.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie die **Hyperic**-Connector-Definition aus.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen Hyperic-Parameter an.
   a. **port** Standardwert: 7080.
   b. **protocol** Standardwert: http.
5. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum Hyperic-Server zu überprüfen.

7. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

Event-Erfassung von IBM Netcool konfigurieren

Konfigurieren Sie IBM Netcool_V2-Connector, von dem Ereignisse empfangen werden sollen IBM Netcool-/OMNIbus-Objektserver und Impact-Server. Die IBM Der Netcool_V2-Connector verwendet REST-API-Aufrufe und ist bidirektional.

Vorbereitungen

Für den Connector IBM Netcool_2:

- Erforderliche Rolle: evt_mgmt_admin
- Führen Sie die Connector-Validierung für IBM NetCool/OMNIbus Version 8.1.0 durch.

Warum und wann dieser Vorgang ausgeführt wird

Zu verwenden IBM Netcool_V2-Connector: Konfigurieren Sie eine Connector-Instanz für den MID-Server.

Hinweis: Die IBM Netcool-Connector ist nur und veraltet IBM Netcool_V2-Connector wird unterstützt.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die Netcool-Connector-Instanz an.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der Netcool-Ereignissammlung ein.
Host-IP	Geben Sie die Netcool-IP-Adresse an.
Anmeldeinformationen	Klicken Sie im Formular „Anmeldeinformationen“ auf **Neu**, und erstellen Sie die erforderlichen Anmeldeinformationen. Speichern Sie die Anmeldeinformationen unter einem eindeutigen und erkennbaren Namen, z. B. „NetcoolOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Der letzte Ausführungsstatus wird automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events von Netcool sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie IBM Netcool_V2 aus, um Ereignisse aus der externen Ereignisquelle zu erfassen.
MID Server (Abschnitt MID Server für Connectors)	Geben Sie einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**. Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussparameter“ den Wert der erforderlichen Netcool-Parameter an.

Connector	Erforderliche Parameter
IBM Netcool_V2	**port**: Nummer des Ports, auf dem IBM Netcool ausgeführt wird. Beispiel: 8080 **initial_sync_in_days**: Anzahl der Tage, über die Daten beim ersten Abruf abgerufen wurden. Der Standardwert lautet 3. Er kann jedoch entsprechend Ihren Anforderungen geändert werden.

5. Stellen Sie sicher, dass die Netcool-Server aktiv sind und ausgeführt werden:
Verwenden Sie für den Connector IBM Netcool_V2 den folgenden REST API-Aufruf, um zu überprüfen, ob die Netcool-API aktiv ist und ausgeführt wird: `http://hostname:port/objectserver/restapi/alerts/status`
6. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Netcool-Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
9. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

Event-Erfassung über einen Icinga2-Connector konfigurieren

Konfigurieren Sie die Icinga-2-Connector-Instanz (Icinga), um bei der Überwachung Ihrer Netzwerkressourcen Events zu empfangen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Version: 2,4.1.

Prozedur

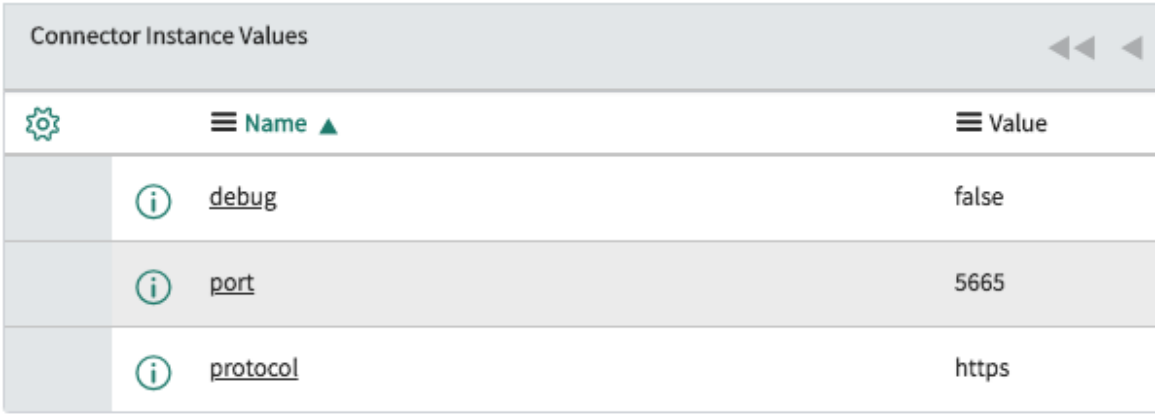
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den Icinga-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der Icinga-Ereignissammlung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **Icinga2** aus.
Host-IP	IP-Adresse, unter der Icinga installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit Icinga. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Verwenden Sie die Anmeldeinformationen für die Standardauthentifizierung. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „ICINGA2CHCK“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von Icinga sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Debuggen: Debug-Nachrichten anzeigen. Standardwert: Falsch. Geben Sie true an, um Debug-Nachrichten anzuzeigen.

b. LogPayloadForDebug: Nutzlastbezogene Debug-Nachrichten anzeigen. Standardwert: Falsch. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

5. Überprüfen Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz, und ändern Sie sie bei Bedarf.

Feld	Beschreibung
debug	Debug-Nachrichten anzeigen. Standardwert: `false`. Geben Sie `true` an, um Debug-Nachrichten anzuzeigen.
port	Nummer des Connector-Ports. Standardwert: `5665`.
protocol	Protokolltyp. Standardprotokolltyp: `https`.
Alert_type	Geben Sie die Details zum Icinga-Warnungstyp an. Es gibt 2 Arten von Warnungen in Icinga2: WEICH und HART WEICH: Die Connector-Instanz ruft eine weiche Warnung ab. HART: Die Connector-Instanz ruft eine harte Warnung ab.

6. **Wahlweise:** Geben Sie im Abschnitt MID-Server für Connectors einen an MID-Server Die aktiv ist und gültig ist.
Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

8. Testen Sie die Verbindung zwischen dem MID-Server und dem Connector Icinga.

a. Klicken Sie auf **Connector testen**.
Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum externen Überwachungs-Tool zu überprüfen.

b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Event-Erfassung von Logicmonitor konfigurieren

Der LogicMonitor-Pull-Connector sendet Informationen von Ereignismanagement An LogicMonitor. Er sendet Antworten, die von einem Push-Connector in einer bidirektionalen Umgebung empfangen wurden, an Logicmonitor.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Beginnend mit Xanadu Release, haben die OOTB-Regeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

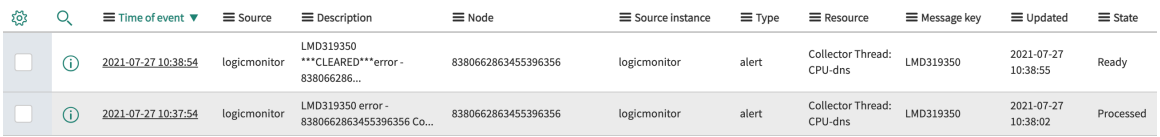
Prozedur

1. Navigieren zu**Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
   Die **Connector-Instanz – Neuer Datensatz** Seite wird angezeigt.
3. Geben Sie Werte in die erforderlichen Felder ein, die durch ein rotes Sternchen gekennzeichnet sind.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Connector-Definition	Suchen und wählen Sie aus **Logiküberwachung** .
Anmeldeinformation	Wählen Sie Aus **Standardauthentifizierung** Für Standardauthentifizierung. Geben Sie access_id und access_key aus der Token-basierten API-Authentifizierung von Logicmonitor in den Anmeldeinformationen als Benutzername und Passwort für die Standardauthentifizierung an.
Host-IP	Die Logicmonitor IP-Adresse.

Beim Hinzufügen der bidirektionalen Funktionalität für einen Push-Connector muss der Name der Connector-Instanz mit dem Feld „Quellinstanz“ des von dieser Quelle generierten Events übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Time of event	Source	Description	Node	Source instance	Type	Resource	Message key	Updated	State
2021-07-27 10:38:54	logicmonitor	LMD319350 ***CLEARED***error - 838066286...	8380662863455396356	logicmonitor	alert	Collector Thread: CPU-dns	LMD319350	2021-07-27 10:38:55	Ready
2021-07-27 10:37:54	logicmonitor	LMD319350 error - 8380662863455396356 Co...	8380662863455396356	logicmonitor	alert	Collector Thread: CPU-dns	LMD319350	2021-07-27 10:38:02	Processed

Die Quelle von Ereignissen ist **LogicMonitor** Daher sollten Sie eine Instanz mit dem Namen erstellen

All > Active = true

Name	Active	Event collection last run time	Connector definition	Last event collection signature	Last event collection status
logicmonitor	true	2021-07-27 11:21:41	Logic Monitor		Success

LogicMonitor.

Hinweis: Die Geschäftsregel „Update-Warteschlange“ der Warnungstabelle identifiziert jede manuelle Aktualisierung der Warnung und aktualisiert die Connector-Warteschlange dementsprechend. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt.

4. Wählen Sie aus **Aktiv** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Speichern** .
   Der LogicMonitor-Pull-Connector ruft keine Ereignisse ab oder füllt die Tabelle „Ereignisse“ [em_event] aus.

Event-Erfassung von NNMi konfigurieren

Konfigurieren Sie die HP Network Node Manager i (NNMi)-Connector-Instanz, um bei der Überwachung Ihrer Netzwerkressourcen Events zu empfangen.

Vorbereitungen

Unterstützte Version: 10.30.653.
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den NNMi-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der NNMi-Ereignissammlung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **NNMi** aus.
Host-IP	IP-Adresse, unter der NNMi installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit NNMi. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „NNMiCHCK“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Für die ausgewählten Anmeldeinformationen wird die Standardauthentifizierung verwendet.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von NNMi sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
Die Connector-Instanzwerte werden dem Formular hinzugefügt,
und die für den Connector relevanten Parameter werden angezeigt.

5. Überprüfen Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz, und ändern Sie sie bei Bedarf.

Feld	Beschreibung
days_from	Anzahl der Tage, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7` Tage. **Hinweis:** Die maximale Anzahl vergangener Events, die erfasst werden können, beträgt 3.000. Bei der ersten Ausführung des Connectors werden alle Events (bis zur Grenze von 3.000) erfasst, die zwischen dem Datum von `days_from` und dem aktuellen Datum erstellt wurden.
debug	Debug-Nachrichten anzeigen. Standardwert: `false`. Geben Sie `true` an, um Debug-Nachrichten anzuzeigen.
port	Nummer des Connector-Ports. Standardwert: `80`.
protocol	Protokolltyp. Standardprotokolltyp: `http`.

6. **Wahlweise:** Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID Server an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn ja MID-Server Ist nicht verfügbar, der nächste wird ausgewählt usw. MID-Server werden nach der Reihenfolge sortiert, in der ihre Details in eingegeben wurden MID-Server Für Abschnitt „Connectors“.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. Testen Sie die Verbindung zwischen dem MID-Server und dem Connector NNMi.

   a. Klicken Sie auf **Connector testen**.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum externen Überwachungstool zu überprüfen.

   b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Event-Erfassung von NagiosXI konfigurieren

Konfigurieren Sie die NagiosXI-Connector-Instanz für den Empfang von Events vom Nagios Core-Monitor.

Vorbereitungen

Unterstützte Version: 5,5.2.
Die NagiosXI-Connector-Instanz erfordert Anmeldeinformationen, mit denen die Instanz auf NagiosXI-Serverkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen. Weitere Informationen finden Sie unter Erstellen Sie Nagios XI-Server-Anmeldeinformationen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Beschreibender Name für den Nagios-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der NagiosXI-Ereignissammlung.
Host-IP	Geben Sie die Nagios XI-IP-Adresse an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Weitere Informationen finden Sie unter Erstellen Sie Nagios XI-Server-Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Stellen Sie sicher, dass das Benutzerpasswort den NagiosXI-Benutzer-API-Schlüssel enthält, z. B. 04lquEPqf4JimWCm8RWbJokOpW8LYBUfEvJp9OSHSRYe4QDrHPFnc
Zeit der letzten Ausführung der Ereignissammlung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events von Nagios sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **NagiosXI** aus.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt MID-Server für Connectors einen an MID-Server Das ist aktiv und gültig. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
5. Geben Sie im Abschnitt Connector-Instanzwerte die Nagios-Werte an.
   - **initial_sync_in_days**. Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7` Tage.
   - **port**. Standardwert: `80`.
   - **protocol**. Standardprotokolltyp: `http`.
   - **time_zone**. Die Standardzeitzone ist `GMT`. Aktualisieren Sie diesen Wert auf die Nagios-Zeitzone. Wenn Nagios beispielsweise die Ereignisse gemäß der EDT-Zeitzone sendet, aktualisieren Sie diesen Wert auf `GMT-04:00` (Abkürzungen wie **EDT** Werden nicht unterstützt).
   - **severity_by_state_type**. Der Standardwert ist „`false`“. Wenn auf festgelegt `Wahr` , State_type wird zusammen mit dem Status verwendet, um den Schweregrad zu bestimmen, der weniger kritische Ereignisse erstellt, wie in der folgenden Zuordnungstabelle angezeigt.

Zuordnungstabelle

_state_type(Connect Definitionsparamete	Status (Nagios-JSON-Nutzlastattribut)	State_type (Nagios-JSON-Nutzlastattribut)	ServiceNow Schweregrad
falsch	2	0/1	1 (Kritisch)
falsch	1	1	1(Kritisch)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

_state_type(Connect Definitionsparamete	Status (Nagios-JSON-Nutzlastattribut)	State_type (Nagios-JSON-Nutzlastattribut)	ServiceNow Schweregrad
falsch	1	0	2(Schwerwiegend)
falsch	0	0/1	5 (OK)
wahr	0	0/1	5 (OK)
wahr	1	0	4 (Warnung-weich -> Warnung)
wahr	2	0	2(Kritisch-weich -> Schwerwiegend)
wahr	3	0	4(Unbekannt-weich -> Warnung)
wahr	1	1	3(Warnung-hart -> Gering)
wahr	2	1	1(Kritisch-hart -> Kritisch)
wahr	3	1	3(Unbekannt-hart -> Gering)

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
   Wenn diese Meldung angezeigt wird: Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu Nagios im Test-Connector. Ungültiger API-Schlüssel, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die Nagios-Events gelesen werden können.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum Überwachungs-Tool Nagios Core zu überprüfen.

9. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Erstellen Sie Nagios XI-Server-Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um auf den Nagios XI-Server zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie Nagios-Authentifizierung nennen.
Benutzername	Name zum Identifizieren des Benutzers. Stellen Sie sicher, dass das Benutzerpasswort den NagiosXI-Benutzer-API-Schlüssel enthält, z. B. 04lquEPqf4JimWCm8RWbJokOpW8LYBUfEvJp9OSHSRYe4QDr
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: 100

5. Klicken Sie auf **Absenden**.

Ergebnis

Die Anmeldeinformationen für die Verwendung mit dem Nagios XI-Server-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Event-Erfassung von OBM konfigurieren

Konfigurieren Sie die Connector-Instanz von Operation Bridge Manager (OBM), auch als OMi v2 bezeichnet, für den Empfang von Warnungen vom OBM-Server. Das OBM-Connector-Skript OBM v2 ist nach der Installation der App Ereignismanagement Connectors verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Versionen: 10.01, 10.10, 10.11, 10.12, 10.60, 10.61 und 11.01.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den OBM-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OBM-Ereignissammlung.
Host-IP	Geben Sie die OBM-IP-Adresse an.
Anmeldeinformationen	Wählen Sie die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu**, und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und leicht wiedererkennbaren Namen, z. B. „OBMOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von OBM sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **OBM V2** aus. **Hinweis:** Dieses Skript ist nach der Installation der bereichsbezogenen App Ereignismanagement Connectors verfügbar.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Geben Sie den MID-Server zur Ausführung der OBM-Connector-Instanz an. Sie können mehrere MID Servers konfigurieren. Wenn der erste Server nicht verfügbar ist, wird der nächste MID-Server verwendet, wenn dieser MID-Server nicht verfügbar ist, wird der übernächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die für den OBM-Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussinstanzwerte“ die OBM-Werte an.

   a. **days_from**.
   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Der Standardwert beträgt 7 Tage, und Daten können maximal 7 Tage aus dem OBM-System abgerufen werden.

   b. **debug**.
   Der Standardwert ist „false“. Um in den Debug-Modus zu wechseln, ändern Sie den Wert in true.

   c. **port**.
   Der Standardwert beträgt 80.

   d. **protocol**.
   Der Standardwert ist http.

   e. **query_filter**.
   Der Standardwert ist „false“. Wenn Sie diesen zusätzlichen Filter zum Abfragen von Events verwenden möchten, geben Sie die Event-Attribute an. Beispiel: assigned_user = „admin“ UND title = „My Title“. Die Abfragefilterkriterien sind:

   - Eine Filtereigenschaft, die ein Event-Attribut angibt, z. B. related_ci
   - Ein unterstützter Operator, z. B. ODER oder UND
   - Ein Wert für die Filtereigenschaft, z. B. admin oder integrator

   Alles aus dem Feld „query_filter“ wird einer URL-Codierung unterzogen und dann als Parameter an den OBM-API-Aufruf übergeben. Ausführliche Informationen zum Erstellen der Filterabfrage finden Sie unter „Filtern nach Event-Attributen: query“ im OBM-Erweiterungsleitfaden. Um beispielsweise die Events nach einer Liste von Events abzufragen, die dem Administrator zugewiesen sind, geben Sie Folgendes an:

   ```
   event_list?query=assigned_user%20EQ%20"admin"
   ```

   Zum Verschachteln von query_filter-Event-Attributen geben Sie die Hierarchie in eckigen Klammern „[]“ an.

   f. **Aufnahmeliste**.
   Der Standardwert ist „false“. Geben Sie eine kommagetrennte Liste an, damit dieses Feature Attribute hinzufügt, die erfasst und dem Feld Ereignismanagement **Zusätzliche Informationen** hinzugefügt werden sollen.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um sicherzustellen, dass der OBM-Server ausgeführt wird und die IP-Adresse mit dem Wert im Feld **Host-IP** übereinstimmt.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

OP5- oder OP5_v2-Connector konfigurieren

Konfigurieren Sie die OP5- oder OP5_v2-Monitor-Connector-Instanz, um Warnungen von einer OP5-Monitor-Quelle zu erhalten.

Vorbereitungen

Der OP5_v2-Connector wird in Ereignismanagement-Connectors, Version 2.3.0, August 2022, unterstützt – verfügbar im ServiceNow Store .

Unterstützte Version:

- OP5: 7.3.15
- OP5_v2: 8.3.8

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den OP5- oder OP5_v2-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OP5- oder OP5_v2-Ereignissammlung.
Host-IP	Geben Sie die OP5- oder OP5_v2-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. OP5OPS.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Der letzte Ausführungsstatus wird automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Zeitplan für Ereignissammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von OP5 oder OP5_v2 sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Anschlussdefinition	Wählen Sie **OP5** oder **OP5_v2** aus.
Abschnitt Connector-Instanzwerte	Die für **OP5** oder **OP5_v2** spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussinstanzwerte“ die OP5- oder OP5_v2-Werte an.

   a. **days_from**.
   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: 7 Tage.

   b. **debug**.
   Zeigt Debug-Nachrichten an. Standardwert: Falsch. Geben Sie „wahr“ an, um Debug-Nachrichten anzuzeigen

   c. **logPayloadForDebug**.
   Zeigt Payload-bezogene Debug-Nachrichten an. Standardwert: Falsch. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

   d. **port**.
   Standardwert: 443.

   e. **state_types**.
   Geben Sie Filter für die Event-Erfassung basierend auf dem Attribut **state_types** an. Sie können Events basierend auf dem Statustyp filtern. Geben Sie den Typ an, z. B. weich oder hart.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie den Opsview_v2-Connector

Konfigurieren Sie die Opsview_V2-Connector-Instanz, um Warnungen von einer Opsview Monitor-Quelle zu erhalten.

Vorbereitungen

Stellen Sie sicher, dass Sie über die unterstützte Version des Opsview_V2-Connectors verfügen: 6,7.0.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den Opsview-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der Opsview-Ereignissammlung.
Host-IP	Geben Sie die Opsview-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „OpsviewOPS“. **Hinweis:** Der Anwender muss über die Rolle „CONFIGUREVIEW“ mit Zugriff auf „ALLE ANZEIGEN, KEINE ÄNDERN“ verfügen.
Zeit der letzten Ausführung der Eventsammlung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Ereignissammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von Opsview sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie Aus **Opsview_v2** .
Abschnitt Connector-Instanzwerte	Die für Opsview_V2 spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Instanzwerte die Opsview_v2-Werte an.

   a. **days_from**.

   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: 7 Tage.

   b. **debug**.
   Debug-Nachrichten anzeigen. Standardwert: Falsch. Geben Sie true an, um Debug-Nachrichten anzuzeigen.

   c. **logPayloadForDebug**.
   Zeigen Sie nutzlastbezogene Debug-Meldungen an. Standardwert: Falsch. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

   d. **eventtype_filter**.
   Geben Sie Filter für die Event-Erfassung basierend auf dem Attribut eventtype an. Geben Sie einen dieser Werte 0,1.2,3 an.

   e. **port**.

   Der Standardwert ist 80.

   an.

   f. **protocol**.
   Standardprotokolltyp: HTTPS.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Wählen Sie aus, um die Verbindung zwischen dem MID-Server und dem Connector zu überprüfen **Testen Sie Den Connector** .
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
   Wenn diese Meldung angezeigt wird: Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu Opsview im Test-Connector. Ungültiger API-Schlüssel, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die Opsview-Events gelesen werden können.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zur Opsview-Monitor-Quelle zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

PRTG-Connector konfigurieren

Konfigurieren Sie die PRTG-Connector-Instanz, um Warnungen von einer Paessler PRTG-Monitor-Quelle zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin
Unterstützte Version: 21.3,71.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den PRTG-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der PRTG-Ereignissammlung.
Host-IP	Geben Sie die PRTG-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. PRTGOPS.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Status der letzten Ereignissammlung	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Ereignissammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von PRTG sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **PRTG** aus.
Abschnitt Connector-Instanzwerte	Die für **PRTG** spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Instanzwerte die PRTG-Werte an.

   a. **add_columns**.
   Geben Sie an, welche Spalten vom Connector zurückgegeben werden sollen. Trennen Sie die Namen durch ein Komma, ohne Leerzeichen zwischen den Namen. Die Ausgabe wird im Feld **Zusätzliche**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen des Events gespeichert. Standardwert: `false`. Wenn `false` angegeben ist, wird nur die Standardliste der Spalten abgerufen: parent, name, type, objid, tags, message, status, priority, datetime, actions, baselink, basetype, modifiedby.

Hinweis: Es können nur Spaltennamen, die für den **Nachrichteninhaltstyp** gelten, angegeben werden.

b. date_format.
Das Datums- und Uhrzeitformat. Standardformat M/T/jjjj/ h:mm:ss a. Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, ändern Sie diesen Wert so, dass es dem Format des eingehenden Events entspricht. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *`2019/06/27/ 11:25:00 a`* ankommt, ändern Sie den Wert **date_format** in *`yyyy/M/d/ h:mm:ss a`*, damit es dem Format des empfangenen Events entspricht.

In **date_format** steht `a` für morgens und `p` für nachmittags.

c. In **Days_from** Geben Sie die Anzahl der Tage an, für die Ereignisse beim ersten Erfassungszyklus erfasst werden müssen.
Standardwert: `7` Tage.

d. debug.
Standardwert: `false`.

e. port.
Standardwert: `80`.

f. protocol.
Standardprotokolltyp: `http`.

g. prtg_api_fetched_events_num.
Maximale Anzahl von Events pro Abfrage, die vom PRTG-Client auf den MID-Server abgerufen werden können. Standardanzahl: `50.000`.

h. time_zone.
Die Standardzeitzone ist `GMT`. Aktualisieren Sie diesen Wert auf die PRTG-Zeitzone. Beispiel: Wenn PRTG Ereignisse gemäß sendet `EDT` Zeitzone, aktualisieren Sie diesen Wert auf `GMT-4` (Abkürzungen wie EDT werden nicht unterstützt.)

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
Wenn diese Meldung angezeigt wird: `Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu PRTG im Test-Connector. Ungültiger API-Schlüssel`, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die PRTG-Events gelesen werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zu PRTG zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Apache Kafka Consumer Connector

Die Apache Kafka Mit der Verbraucher-Connector-Instanz können Sie Ereignisse aus Nachrichten erstellen, die von erfasst wurden Apache Kafka Thema als JSON-Nutzlast, die wichtige Informationen in einem Datenblock enthält.

Apache Kafka ist ein verteiltes Publish/Subscribe-Messagingsystem, das Daten aus unterschiedlichen Quellsystemen empfängt und die Daten in Echtzeit für Zielsysteme verfügbar macht.

Sie können diesen Connector zum Erstellen verwenden ServiceNow Ereignisse aus Kafka-Nachrichten. Nachrichten im Kafka-Thema müssen im JSON-Format vorliegen.

Wie andere Nachrichten-Broker-Systeme erleichtert Kafka den asynchronen Datenaustausch zwischen Prozessen, Anwendungen und Servern.

Kafka-Software wird auf einem oder mehreren Servern ausgeführt. Jeder Knoten, der als Broker bezeichnet wird, in einem Kafka-Cluster hilft Erstelleranwendungen, Daten in Themen zu schreiben, in denen Datensätze gespeichert und veröffentlicht werden. Verbraucheranwendungen lesen aus Themen. Themen sind in Partitionen unterteilt, um sie leichter zu verwalten, und Kafka garantiert eine starke Reihenfolge für jede Partition.

Konfigurieren Sie Apache Kafka Verbraucher-Connector

Konfigurieren Sie Apache Kafka Verbraucher-Connector-Instanz zum Erstellen von Ereignissen aus Streaming-Nachrichten, die von erfasst wurden Apache Kafka Connector.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular Connector-Instanz

Feld	Wert
Name	Beschreibender und eindeutiger Name für den Kafka-Verbraucher-Connector.
Beschreibung	Beschreibung, die von der Instanz der Kafka-Verbraucher-Ereigniserfassung verwendet werden soll.
Connector-Definition	Name der erforderlichen Connector-Definition, die in diesem Fall Kafka-Verbraucher sein sollte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Host-IP	Die Host-IP. **Hinweis:** Dieses Feld muss einen Wert enthalten, um den Erstellungsprozess abzuschließen, daher sollte der Platzhalter 1.1.1.1 als temporärer Wert eingegeben werden.
Zeit der letzten Ausführung der Eventsammlung	Dieses Feld wird automatisch auf den letzten Laufzeitwert festgelegt.
Status der letzter Eventsammlung	Dieses Feld wird automatisch auf den letzten Laufzeitstatus festgelegt.
Zeitplan für Eventsammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom Kafka Consumer sucht. Der Standardwert beträgt 60 Sekunden.
Letzte Fehlermeldung	Dieses Feld wird automatisch auf die letzte Fehlermeldung festgelegt.

4. Für NUR-TEXT oder SASL_PLAINTEXT in **Anmeldeinformationen** Feld, erstellen Sie Anmeldeinformationen für die Standardauthentifizierung.
   Verwenden Sie **Kafka-SSL-Anmeldeinformationen** Geben Sie eine neue Kafka-Pull-Connector-Instanz mit ein **SASL_PLAINTEXT** Authentifizierung. Fahren Sie mit Schritt 5 fort.

   Verwenden Die **Kafka-SSL-Anmeldeinformationen** Geben Sie ein, wenn der Kafka-Server ist **sasl.enabled.Mechanismen** Oder **sasl.Mechanismus** Parameterwert ist nicht gleich **EINFACH** . Fahren Sie mit Schritt 5 fort.

   a. Wählen Sie das Suchsymbol aus Neben **Anmeldeinformationen** Feld.

   b. Wählen Sie im Bildschirm Anmeldeinformationen die Option aus **Neu** .

   c. Wählen Sie in der Liste der verfügbaren Anmeldeinformationen die Option aus **Anmeldeinformationen Für Standardauthentifizierung** .

   d. Geben Sie auf dem Bildschirm „Standardauthentifizierung“ entweder Informationen für die NUR-TEXT-Authentifizierung an, die keine Anmeldeinformationen erfordert, oder für die SASL_PLAINTEXT-Authentifizierung, die Anmeldeinformationen erfordert.

   - Für die NUR-TEXT-Authentifizierung in **Name** Feld einen beliebigen Wert eingeben und belassen **Anwendername** Und **Passwort** Felder leer.
   - Geben Sie für die SASL_PLAINTEXT-Authentifizierung einen Namen für die Anmeldeinformationen in an **Name** Feld, vorzugsweise mit vorangestelltem SASL . Geben Sie den Anwendernamen und das Passwort in an **Anwendername** Und **Passwort** Felder.

   e. Wählen Sie **Absenden**.

5. Für SASL_PLAINTEXT-, SSL- oder SASL_SSL-Authentifizierungsanmeldeinformationen im **Anmeldeinformationen** Feld erstellen Sie eine Kafka-SSL-Anmeldeinformation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie das Suchsymbol aus Neben **Anmeldeinformationen** Feld.

b. Wählen Sie im Bildschirm Anmeldeinformationen die Option aus **Neu** .

c. Wählen Sie in der Liste der verfügbaren Anmeldeinformationen die Option aus **Kafka-SSL-Anmeldeinformationen** .

d. Füllen Sie im Bildschirm Kafka-SSL-Authentifizierung die Felder für Kafka-SSL-Anmeldeinformationen aus.
Beschreibungen der Felder für Kafka-SSL-Anmeldeinformationen finden Sie unter .

Hinweis: Wenn Sie löschen **Deaktivieren Sie die Hostnamenverifizierung** Feld, dann in **Zusätzliche Kafka-Verbrauchereigenschaften** Geben Sie den Wert des ein `ssl.endpoint.identification.algorithm`Parameter ist identisch mit dem Kafka-Server-Parameterwert. Zum Beispiel:

```
ssl.enabled.protocols=TLSv1.2,TLSv1.1,TLSv1;
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required
 username=<username> password=<password>;
sasl.enabled.mechanisms=PLAIN;ssl.endpoint.identification.algorithm=;
```

e. Wählen Sie **Absenden**.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Überprüfen Sie in der Tabelle mit den Connector-Instanzwerten die ausgefüllten Connector-Instanzwerte basierend auf Ihrem Kafka-Setup und der Nachricht (JSON-Nutzlast), die Sie vom Kafka-Thema erhalten haben.

   Ändern Sie bei Bedarf die Werte der Connector-Instanz.

Tabelle der Connector-Instanzwerte

Feld	Beschreibung
authentication_type	Der Authentifizierungstyp des Kafka-Verbrauchers. Die derzeit unterstützten Werte sind: ○ NUR-TEXT (keine Authentifizierung) (Standard) ○ SASL_PLAINTEXT (Standardauthentifizierung – Anwendername und Passwort)
bootstrap_servers	Die Server, die die Verbindung zum Kafka-Cluster herstellen. Werte in diesem Feld müssen das Format host1:port1, host2:port2 usw. aufweisen (kommagetrennt).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dies ist ein Pflichtfeld.
consumer_group_name	Verbrauchergruppenname. Wenn dasselbe Kafka-Thema von zwei verschiedenen Instanzen verbraucht wird, verwenden Sie verschiedene Verbrauchergruppennamen, damit alle Ereignisse für beide Instanzen erfasst werden. Dies ist ein Pflichtfeld.
time_of_event_field	Der Name des Felds in der JSON-Nutzlast/Nachricht, das die Zeit des Ereignisses enthält. Wenn ein Feld in der JSON-Nutzlast/-Nachricht die Zeit des Ereignisses enthält, muss dieser Wert der Wert für diesen Parameter sein. Wenn kein Zeitfeldwert angegeben ist, wird die Empfangszeit des Ereignisses in angegeben ServiceNow Instanz ist als time_of_event festgelegt. Das Feld „time_of_event“ muss ein Feld der ersten Ebene in der JSON-Nutzlast/-Nachricht sein. Geschachtelte Feldnamen sind nicht zulässig.
Feld	Die Zeitzone des Felds time_of_event in der JSON-Nutzlast/-Nachricht. Der Zeitzonenwert wird nicht verwendet, wenn das Feld time_of_event leer ist. Wenn sich beispielsweise die Zeit_des_Ereignisses in der Nutzlast/Nachricht in der ist-Zeitzone befindet, wäre der Wert GMT+0530. Standardwert: GMT.
date_format	Das Format date_time des Felds time_of_event in der JSON-Nutzlast/-Nachricht. Wenn kein Zeitfeldwert angegeben ist, wird die Zeit verwendet, zu der das Ereignis in der Instanz empfangen wurde, in GMT-Zeit. Der Wert date_time wird nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	verwendet, wenn das Feld time_of_event leer ist. Standardwert: jjjj-MM-tt HH:mm:ss.
debuggen	Zeigt Debug-Nachrichten an. Standardwert: Falsch. Geben Sie true an, um Debug-Nachrichten anzuzeigen.
logPayloadForDebug	Zeigt Payload-bezogene Debug-Nachrichten an. Standardwert: Falsch. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.
Thema	Das Kafka-Thema, aus dem die Nachrichten abgerufen werden. Dies ist ein Pflichtfeld.

8. In **MID-Server für Connectors** Geben Sie einen Abschnitt an MID-Server Die aktiv ist und gültig ist.

   Hinweis: Sie können mehrere MID Servers konfigurieren. Wenn der erste Server ausgefallen ist, der nächste MID-Server Wird verwendet. Wenn ja MID-Server Ist nicht verfügbar, der nächste wird ausgewählt usw. MID Servers Werden in der Reihenfolge sortiert, in der ihre Details in eingegeben wurden **MID-Server für Connectors** Abschnitt.

   Wenn Sie keinen angeben MID-Server, Ein verfügbar MID-Server Wird verwendet, der einen übereinstimmenden IP-Bereich hat.

9. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
10. Testen Sie die Verbindung zwischen MID-Server Und den Kafka-Verbraucher-Connector.

    a. Wählen Sie **Connector testen**.

    b. Wenn die Testverbindung fehlschlägt, überprüfen Sie, ob die Anmeldeinformationen gültig sind und ob das Netzwerk über verbunden ist MID-Server Zum Kafka-Broker.

    Hinweis: Die Validierung des Kafka-Themennamens findet nur in statt **Testen Sie Den Connector** Validierung.

11. Aktivieren Sie nach einem erfolgreichen Test die Connector-Instanz, indem Sie auswählen **Aktiv** Kontrollkästchen.
12. Wählen Sie aus **Aktualisieren** Schaltfläche.

Nächste Maßnahme

Nachdem der Connector erstellt wurde, müssen Sie die Felder zuordnen. Weitere Informationen finden Sie unter Nutzlastattribute der Kafka-Nachricht an Warnungsfelder zuordnen.

Nutzlastattribute der Kafka-Nachricht an Warnungsfelder zuordnen

Ordnen Sie Kafka-Nachrichtenattribute Warnungsfeldern zu, um Warnungen basierend auf den Nachrichten aussagekräftiger zu machen. Verwenden Sie die Ereignisfeldzuordnung, um Kafka-Schweregradwerte entsprechend zuzuordnen ServiceNow Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Je nach Nutzlast können Sie Ereignisfeldzuordnungen verwenden, um umfassendere Informationen in einer Ereigniswarnung bereitzustellen, indem Sie Werte aus der Ereignisfeldzuordnungsregel in das Ereignis ersetzen. Wandeln Sie je nach Nutzlast Informationen in Ereignissen um, um die angegebenen Warnungsfeldwerte auszufüllen, und verfassen Sie Warnungsfelder aus verschiedenen Werten, um Warnungen zur Nachverfolgung und Korrektur zu generieren. Verwenden Sie bei Bedarf sowohl Ereignisfeldzuordnungen als auch Warnungsregeln.

Die folgende Tabelle vergleicht eine von einem Thema empfangene Nachricht mit einer reduzierten Nutzlast im Ereignis **Zusätzliche Informationen** Feld. Die von einem Thema empfangene Nachricht wird als einzelnes Feld reduziert und im Ereignis angezeigt **Zusätzliche Informationen** Feld. Verwenden Sie diese reduzierten Nachrichten, um Ereignisregeln und -Zuordnungen zu erstellen.

Tatsächliche vs. Reduzierte Nutzlast

Tatsächliche Nutzlast, die in ein Thema eingefügt wurde	Reduzierte Nutzlast im Feld „zusätzliche Informationen“

<pre>{
"version": "v0.1.0",
"name": "fibsrc",
"id": "mnop6789",
"trigger_description": "Triggers on duration_ms goes above 5K",
"status": "TRIGGERED",
"alert_type": "on_true",
"summary": "Triggered: fibsrc",
"description": "Current value (12.296815 k) greater than threshold value (5 k)",
"operator": "greater than",
"threshold": 5000,
"groups": [
{
"Group": "GroupA",
"Result": 12296.815478000368
}</pre>
	<pre>{
	"flattened.alert_type": "on_true",
	"flattened.description": "Current value (12.296815 k) greater than threshold value (5 k)",
	"flattened.id": " mnop6789",
	"flattened.kafkaKey": "null",
	"flattened.kafkaOffset": "28",
	"flattened.kafkaPartition": "0",
	"flattened.kafkaTopicName": "topic123",
	"flattened.name": "fibsrc",
	"flattened.operator": "greater than",
	"flattened.status": "TRIGGERED",
	"flattened.summary": "Triggered: fibsrc",
	"flattened.trigger_description": "Triggers on duration_ms goesa above 5K",
	"flattened.version": "v0.1.0",
	"flattened.version": 5000,</pre>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tatsächliche vs. Reduzierte Nutzlast (Fortsetzung)

Tatsächliche Nutzlast, die in ein Thema eingefügt wurde	Reduzierte Nutzlast im Feld „zusätzliche Informationen“

<pre>],
"trigger": {
"Result": 12296.815478000368
}
}</pre>
	<pre>"flattened.groups.0.Group": "GroupA",
	"flattened.groups.0.Result": 12296.815478000368,
	"flattened.trigger.Result": 12296.815478000368
	}</pre>

Prozedur

1. Um die Kafka-Nachrichtenattribute den vordefinierten Warnungsfeldern zuzuordnen, um Warnungen durch Erstellen von Ereignisfeldzuordnungen zu generieren.
   a. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisfeldzuordnung**an.
   b. Wählen Sie im Fenster Ereignisfeldzuordnung die Option aus **Neu** .
   c. Geben Sie im Feld Name einen Namen für die Feldzuordnung ein.
   d. Geben Sie im Feld Quelle den Wert ein **Kafka-Verbraucher** .
   e. Wählen Sie im Feld Zuordnungstyp den entsprechenden Zuordnungstyp aus
   f. Eine Liste der verfügbaren Zuordnungstypen finden Sie unter Ereignisfeldzuordnungen .
2. Um die Kafka-Nachrichtenattribute den vordefinierten Warnungsfeldern zuzuordnen, um Warnungen durch Erstellen von Ereignisregeln zu generieren.
   a. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
   b. Wählen Sie Aus **Neu** .
   c. Geben Sie im Feld Name einen Namen für die Ereignisregel ein.
   d. Geben Sie im Feld Quelle den Wert ein **Kafka-Verbraucher** .
   e. Wählen Sie Aus **Ereignisfilter** .
   f. Geben Sie den entsprechenden Filter entsprechend Ihrer Anforderung ein.
   g. Wählen Sie Aus **Transformieren und verfassen Sie die Warnungsausgabe** .

   Beim Erstellen von Ereignisregeln werden die Ereignisfelder auf den Registerkarten Ereignisregeln transformieren und Warnungsausgabe verfassen angezeigt. Da die Kafka-Nachricht von Anwender zu Anwender variiert, müssen Sie die Ereignisfelder in Warnungsfelder umwandeln, um die Details in der Warnung anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Da der Schweregradwert zum Erstellen einer Warnung erforderlich ist, müssen Sie zuordnen **Schweregrad** Feld mit Ereignisregeln oder Ereignisfeldzuordnungen. Wenn das Feld Schweregrad leer ist, wird das Ereignis nicht verarbeitet und in einen Fehlerstatus versetzt.

h. Ordnen Sie die Felder des Ereignisses und zu **Zusätzliche Informationen** Feld zu den Feldern der Warnung.

i. Wählen Sie Aus **Bindung** .

j. Geben Sie die entsprechende Bindung entsprechend Ihren Anforderungen ein.

k. Wählen Sie **Absenden**.
Weitere Informationen finden Sie unter Event-Regel erstellen oder bearbeiten.

3. Überprüfen Sie im Bildschirm „alle Ereignisse“, ob sich eines der Ereignisse aus Kafka aufgrund einer fehlenden Ereignisregel in einem Fehlerstatus befindet, und geben Sie fehlende Regeln an.

a. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.

b. Öffnen Sie in der Tabelle alle Ereignisse ein Kafka-Verbrauchereereignis, das Fehler als Status in anzeigt **Schweregrad** Spalte.

Die vom Kafka-Verbraucher empfangene Nachricht kann variieren. Da der Connector die empfangenen Attribute nicht kennen kann, müssen Sie zuordnen **Schweregrad** Feld oder andere Ereignisfelder zu den Feldern in der Nachricht, um sicherzustellen, dass Warnungsfelder korrekt ausgefüllt sind.

c. Erstellen Sie auf dem Bildschirm alle Ereignisse eine neue Ereignisregel, indem Sie auswählen **Erstellen Sie Eine Ereignisregel** .
Weitere Informationen zum Erstellen von Ereignisregeln finden Sie unter Ereignisregeln.

Wenn keine Ereignisfeldzuordnungen vorhanden sind, um den neuen Ereignistyp zu verarbeiten, erstellen Sie Ereignisfeldzuordnungen. Weitere Informationen finden Sie unter Event-Feldzuordnungen erstellen.

Ergebnis

Ihr Apache Kafka-Verbraucher-Connector ist konfiguriert. Wenn neue Nachrichten im Kafka-Thema eintreffen, werden sie in empfangen ServiceNow Instanz als Ereignisse , Und -Warnungen werden dann aus diesen Ereignissen erstellt.

SAP Solution Manager-Connector konfigurieren

Konfigurieren Sie die Connector-Instanz von SAP Solution Manager (Solman), um die Kommunikation zwischen SAP Solution Manager und Ereignismanagement zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: admin
Unterstützte Versionen: Getestet in SAP Solution Manager 7.2. Funktioniert möglicherweise auch mit anderen Versionen.

Warum und wann dieser Vorgang ausgeführt wird

Mit dieser Konfiguration können Sie den SAP Solution Manager mit den Status aktualisieren, die von ServiceNow aktualisiert wurden. Allgemeine Informationen zum SAP Solution Manager finden Sie unter SAP-Konfigurationen zur Aktivierung des SAP Solution Manager-Connectors.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz.
3. Füllen Sie die Felder im Formular aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender Name für den SAP Solman-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der SAP Solman-Ereignissammlung.
Aktiv	Option, die die Connector-Instanz aktiviert. Wählen Sie diese Option nur nach erfolgreichem Test aus.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie **SAP Solman** aus.
Host-IP	Die IP-Adresse, unter der SAP Solman installiert ist.
Anmeldeinformationen	Erforderliche Anmeldeinformationen wurden entweder durch Auswahl aus den Ergebnissen einer Suche über das Suchsymbol oder durch Klicken auf **Neu** eingegeben. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. SAPSOLMANOPS.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von SAP Solman sucht.
Bidirektional	Wählen Sie diese Option aus, um den bidirektionalen Austausch von Werten mit der externen Ereignis-Quelle auszulösen. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt wird.
Letzter bidirektionaler Status	Dieses Feld ist nur sichtbar, wenn **Bidirektional** ausgewählt ist. Dieses Feld wird automatisch mit dem neuesten bidirektionalen Status ausgefüllt.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Abschnitt Connector-Instanzwerte	Die für SAP Solman spezifischen Parameter, die beim Speichern des Formulars automatisch angezeigt werden.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Aktiver und gültiger MID-Server. Sie können mehrere MID Servers so konfigurieren, dass bei Ausfall des ersten Servers der nächste MID-Server verwendet wird. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

5. Geben Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz an.
   - **Client**: Standardwert = `001`
   - **Port**: Standardwert = `8000`
6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie *`Ping`*, um die Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum Überwachungs-Tool SAP Solman zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken auf **Aktualisieren**.

Zugehörige Informationen

Pull-Connector des SAP Solution Manager verwenden

SAP-Konfigurationen zur Aktivierung des SAP Solution Manager-Connectors

Konfigurieren Sie Ihre SAP-Umgebung für die Verwendung mit der ServiceNow Ereignismanagement-Plattform, damit Sie den SAP Solution Manager-Connector verwenden können.

Bei der Integration Ihrer SAP-Umgebung mit Ereignismanagement werden Events von SAP Solution Manager über einen MID-Server an Ereignismanagement gesendet, das aus dem Event eine Warnung generiert.

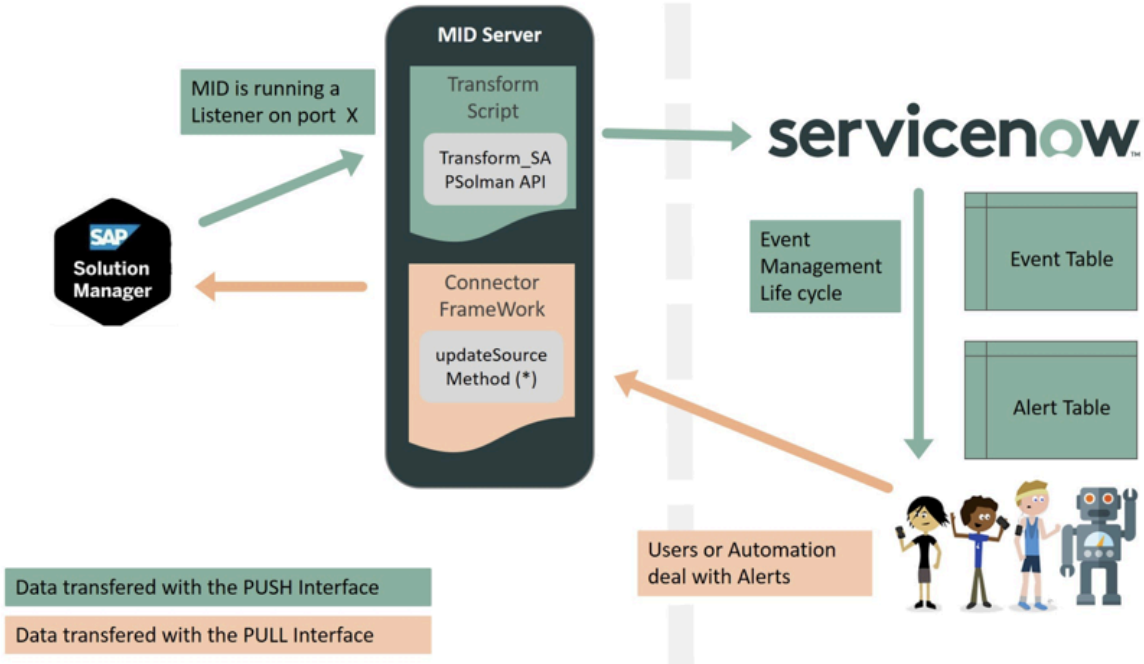
Nachdem der MID-Server Events verarbeitet hat, können Sie in SAP Solution Manager die folgenden Aktionen ausführen:

- Kommentare hinzufügen
- Warnungen bestätigen
- Den Status auf **Extern verwaltet** festlegen

Das folgende Diagramm veranschaulicht den Datenfluss zwischen SAP und Ereignismanagement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP Solution Manager-Connector



Daten werden mithilfe von Push- und Pull-Schnittstellen zwischen SAP und Ereignismanagement verschoben.

- **Pull-Schnittstelle**:

  Die Tabelle der Connector-Update-Warteschlangen [em_connector_update_queue] listet manuelle Updates von Warnungen auf und sendet sie an den SAP Solution Manager.

  Die Geschäftsregel der Tabelle identifiziert jede manuelle Aktualisierung von Warnungen in Ereignismanagement und aktualisiert die Connector-Warteschlange mit diesen Änderungen. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt. Informationen zum Anpassen dieser Einstellung finden Sie in der Dokumentation zum SAP Solution Manager.

  Mit der regelmäßigen Aufgabe „Ereignismanagement – Warteschlangen-Connector-Prozessor“ werden Warnungsänderungen aus der Warteschlange entfernt und an den MID-Server gesendet. Standardmäßig führt das System diesen Prozess in Batches von 1.000 Warnungen aus. Sie können die Batch-Größe anpassen, indem Sie die `evt_mgmt.max_update_source_records`-Einstellung ändern.

  Hinweis: Sie müssen die Pull-Schnittstelle definieren, um die bidirektionale Funktionalität im SAP Solution Manager-Connector zu aktivieren. Weitere Informationen finden Sie in der Dokumentation zum SAP Solution Manager.

- **Push-Schnittstelle**: Da SAP Daten nur an eine externe Quelle weitergeben kann, verwendet die Integration die Push-Schnittstelle, um von SAP an Ereignismanagement gesendete Warnungen zu speichern.

  SAP-Warnungen erstellen Events in Ereignismanagement, die sowohl Event-Regeln als auch CI-Identifizierungsregeln verwenden, um Ereignismanagement-Warnungen zu erstellen.

  Nachdem Ereignismanagement Warnungen erstellt hat, wartet eine Geschäftsregel auf eine Änderung der Warnung. Wenn eine Änderung erkannt wird, aktualisiert Ereignismanagement die Warnungen des SAP Solution Manager.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Ereignismanagement-Integrationen

Pull-Connector des SAP Solution Manager verwenden

Pull-Connector des SAP Solution Manager verwenden

Der Pull-Connector des SAP Solution Manager sendet Informationen aus Ereignismanagement an den SAP Solution Manager. Der Pull-Connector sendet Antworten, die von einem Push-Connector in einer bidirektionalen Umgebung empfangen wurden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

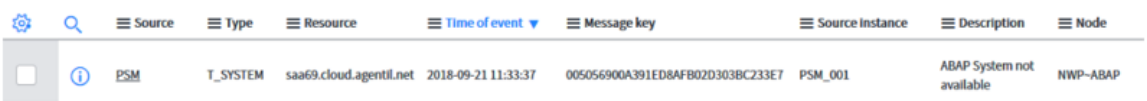
1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
   Die Seite **Connector-Instanz – Neuer Datensatz** wird angezeigt.
3. Geben Sie Werte in die erforderlichen Felder ein, die durch ein rotes Sternchen gekennzeichnet sind.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Connector-Definition	Suchen Sie nach **SAP Solution Manager** und wählen Sie ihn aus.
Anmeldeinformationen	Wählen Sie **Standardauthentifizierung** für die Standardauthentifizierung aus.
Host-IP	Die IP-Adresse des SAP Solution Manager.

Die Tabelle der Connector-Update-Warteschlangen [*em_connector_update_queue*] listet manuelle Updates von Warnungen auf und sendet mithilfe der Pull-Schnittstelle ein Event an den SAP Solution Manager.

Hinweis: Beim Hinzufügen der bidirektionalen Funktionalität für einen Push-Connector muss der Name der Connector-Instanz mit dem Feld „Quellinstanz“ des von dieser Quelle generierten Events übereinstimmen. Der Feldwert **Connector-Instanz** ist eine Kombination aus SID + _ + Mandant.

Das folgende Bild zeigt beispielsweise ein Event, das von der Instanzquelle **PSM_001**generiert wurde. Um das Zurücksenden von Informationen zu ermöglichen, müssen Sie Ihre Connector-Instanz **PSM_001** nennen.



4. Legen Sie die folgenden Werte für die Connector-Instanz fest:
   - **Client**: Stellt den Clientwert in SAP dar, normalerweise 001.
   - **Port**: Der WebService-Port von SAP Solution Manager. Standardwert = 8000.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie in Ereignismanagement ausführen können, und die daraus resultierenden Aktualisierungen im SAP Solution Manager.

Ereignismanagement-Aktionen und SAP Solution Manager-Updates

Aktion in Ereignismanagement	Ergebnis in SAP Solman
Eine Warnung schließen.	Bestätigt eine Warnung im Warnungs-Posteingang. Die Warnung wird entfernt.
Wählen Sie die Einstellung **Wartung** in einer Warnung aus.	Fügt einen Kommentar hinzu, der angibt, dass sich die Warnung im Wartungsmodus befindet.
Heben Sie die Einstellung **Wartung** in einer Warnung auf.	Entfernt den Wartungsmodus-Kommentar.
Wählen Sie die Einstellung **Bestätigt** in einer Warnung aus.	Fügt einen Kommentar hinzu, der angibt, dass sich die Warnung im bestätigten Modus befindet.
Heben Sie die Einstellung **Bestätigt** in einer Warnung auf.	Entfernt den Kommentar zum bestätigten Modus.

Achten Sie auf die folgenden Verhaltensweisen:

- Die Geschäftsregel „Update-Warteschlange“ der Warnungstabelle identifiziert jede manuelle Aktualisierung der Warnung und aktualisiert die Connector-Warteschlange dementsprechend. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt.
- Der Job Ereignismanagement-Warteschlangen-Connector-Prozessor entfernt Warnungsänderungen aus der Warteschlange und sendet sie an den MID Server. Standardmäßig führt Ereignismanagement diesen Dequeue-Prozess in Batches von 1.000 Warnungen aus. Sie können die Batch-Größe konfigurieren, indem Sie die Eigenschaft `evt_mgmt.max_update_source_records` festlegen.

Pull-Connector des SAP Solution Manager verwenden

Mit dem Eventsammler des MID Server-Webservice können Sie Warnungen erfassen, die vom SAP Solution Manager über Event Stream-Benachrichtigungsfunktionen gesendet wurden. Die Schnittstelle führt sowohl eine Push- als auch eine Pull-Schnittstelle aus, um direkt mit dem SAP Solution Manager zu interagieren.

Vorbereitungen

- Stellen Sie den MID Server bereit und starten Sie ihn.
- Konfigurieren Sie einen MID Web Server.
- Konfigurieren und starten Sie den Ereignissammler des MID Server-Webservice.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

SAP Solution Manager sendet Event-Nachrichten im JSON-Format an den MID Server. Der MID Server analysiert die erfassten Warnungsnachrichten und wandelt sie mit dem SAP Solman-Umwandlungsskript [*TransformEvents_SAPSolman*] um.

JSON-formatierte Nachrichten werden mithilfe der Standardauthentifizierung erfasst. Weitere Informationen zu anderen unterstützten Authentifizierungsmethoden finden Sie unter MID-Webserver erweiterung konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**an.
2. Wählen Sie aus **SAP Solman-Transformationsskript** Skript.
3. Verwenden Sie die folgende URL, um Warnungsmeldungen von SAP Solution Manager zum MID Server zu verschieben:
   http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_SAPSolman, wobei Folgendes zutrifft:
   - **MID_Server_IP** ist die IP-Adresse der MID-Webservererweiterung
   - **MID_Web_Server_Port** ist der Listener-Port der MID-Webservererweiterung

Nächste Maßnahme

Erstellen Sie einen Remote Function Call (RFC) im SAP Solution Manager, und installieren Sie einen Transport, wie in RFC im SAP Solution Manager konfigurieren beschrieben.

Zugehörige Informationen

MID-Server werden konfiguriert

MID-Webserver erweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

Einrichtungskonfiguration des SAP Solution Manager

Als Teil der Einrichtung von SAP Solution Manager müssen Sie mehrere Konfigurationen durchführen, damit SAP Solution Manager mit Ereignismanagement interagieren kann.

RFC im SAP Solution Manager konfigurieren

Im Rahmen der Aktivierung der Kommunikation mit Ereignismanagement müssen Sie in SAP Solution Manager einen Remote Function Call (RFC) erstellen und eine Übertragung installieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Laden Sie die folgenden psm-Dateien herunter, und importieren Sie sie in das SAP Solution Manager-System.

- product/event-management/files/K900249.PSM
- product/event-management/files/R900249.PSM

Prozedur

1. Geben Sie auf der SAP-UI den Transaktionscode SM59 ein, und erstellen Sie auf der Registerkarte **Technische Einstellungen** einen neuen RFC mit den folgenden Parametern:

RFC-Parameter

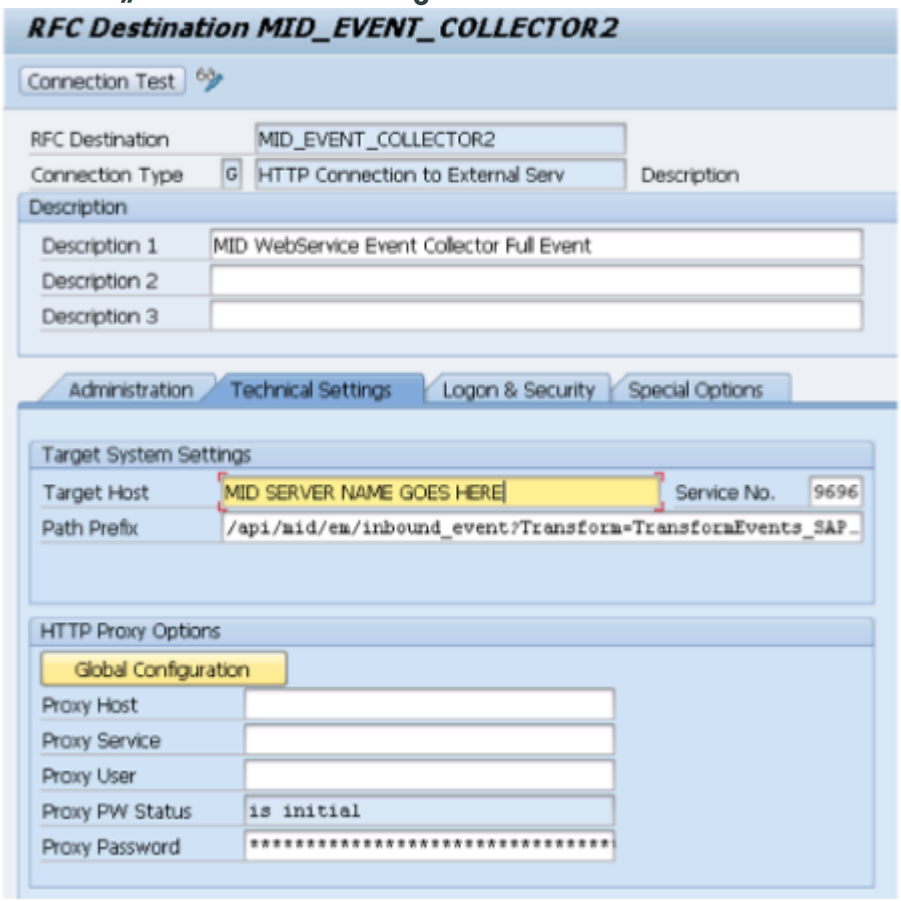
SAP-Parameter	Wert
RFC-Ziel	MID_EVENT_COLLECTOR2
Zielhost	Name des MID-Server s
Service-Nr.	Listener-Port auf dem MID-Server

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

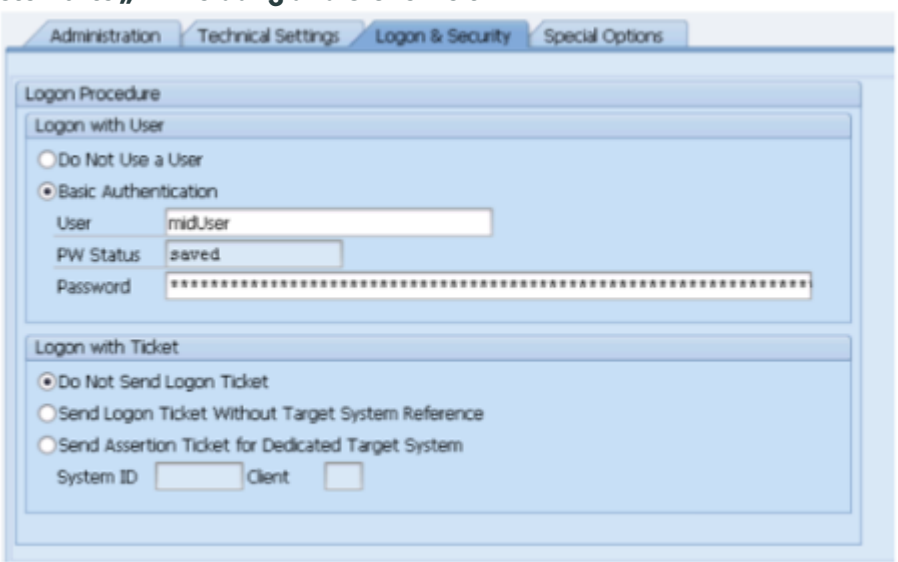
SAP-Parameter	Wert
Pfadpräfix	URL des MID-Server-Transformationsskripts: /api/mid/em/inbound_event?Transform=TransformEvents_SAPSolman

Registerkarte „Technische Einstellungen“



2. Auf der Registerkarte **Anmeldung & Sicherheit** wählen Sie **Standardauthentifizierung** und geben Ihre Ereignismanagement-Anmeldeinformationen in den Feldern **Benutzer** und **Kennwort** ein.

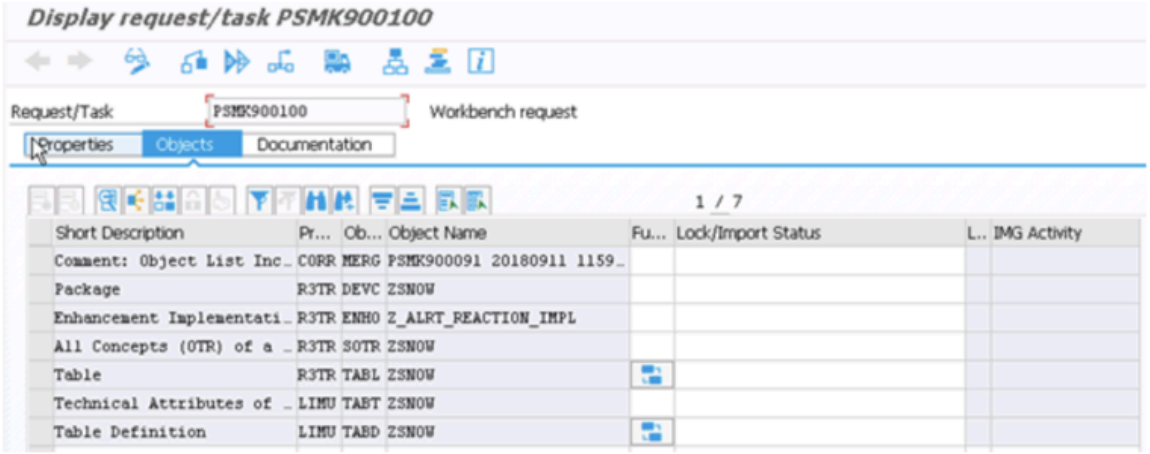
Registerkarte „Anmeldung und Sicherheit“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein benutzerdefiniertes SAP BADI (Business Add-in) namens Z_ALRT_REACTION_IMPL wird erstellt und als Workbench-Transportauftrag gespeichert. Nach der Installation ruft dieses BADI den RFC auf, um eine Verbindung mit Ereignismanagement herzustellen.



SAP konfigurieren, um Warnungen an Ihr BADI weiterzuleiten

Nach der Einrichtung der Überwachung des SAP Solution Manager müssen Sie SAP so konfigurieren, dass Warnungen an das BADI (Business Add-in) weitergeleitet werden, das Sie als ersten Schritt in der Einrichtung der SAP-Integration erstellen.

Vorbereitungen

Erforderliche Rolle: evt_mgt_admin

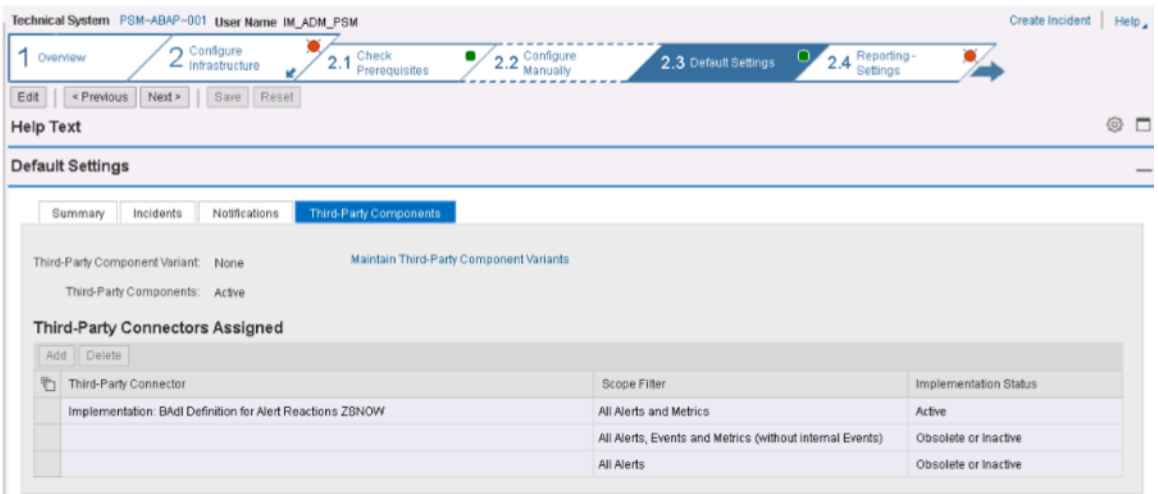
Warum und wann dieser Vorgang ausgeführt wird

Warnungen von Dritten werden global weitergeleitet. Sie können die Warnungsreaktion nur für eine bestimmte Überwachungsvorlage konfigurieren.

Prozedur

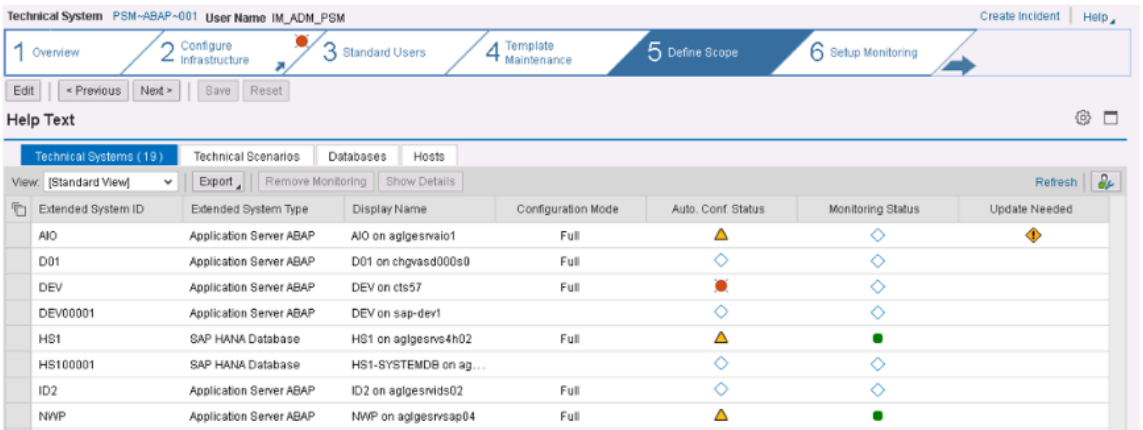
1. Navigieren Sie in der SAP-UI zu **Anwendungsvorgänge** > **Systemüberwachung**an.
2. Wählen Sie im Menüband oben auf der Konfigurationsseite der Systemüberwachung die Option aus **2 Konfigurieren Sie Die Infrastruktur** > **2,3 Standardeinstellungen**an.
   Die Seite **Standardeinstellungen** wird angezeigt.

Seite Standardeinstellungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Konfigurieren und aktivieren Sie eine Fremdkomponente.
   a. Wechseln Sie in den Bearbeitungsmodus, indem Sie auf die Schaltfläche **Bearbeiten** klicken.
   b. Wählen Sie die Registerkarte **Fremdkomponenten** aus.
   c. Klicken Sie auf **Hinzufügen** und fügen Sie den folgenden Wert als Fremd-Connector hinzu: Implementierung: BADI-Definition für Warnungsreaktionen ZSNOW mit Bereich = Alle Warnungen und Metriken.
   d. Klicken Sie auf **Speichern**, um Fremdkomponenten global zu aktivieren.
4. Definieren Sie die Objekte, denen die Überwachungsvorlage zugewiesen wird.
   a. Wählen Sie im Menüband oben auf der Seite **5 Umfang definieren** aus.
   Die Seite „Umfang definieren“ wird angezeigt.



   b. Wählen Sie das verwaltete Objekt aus, dem Sie die Überwachungsvorlage zuweisen möchten.
   Die Überwachungsvorlage wird den ausgewählten Objekten zugewiesen.
5. Aktivieren Sie die Überwachung von Vorlagen erneut.
   a. Wählen Sie **6 Setup-Überwachung**.
   b. Suchen Sie Einträge mit **Setup-Status = Neukonfigurieren erforderlich** und weisen Sie diesen Einträgen die Überwachungsvorlage zu.
   c. Wählen Sie **Anwenden** und **Aktivieren** aus.
   Stellen Sie nach Abschluss der Aufträge sicher, dass der **Zuweisungsstatus** grün ist.
   Alle Vorlagen und aktiven Warnungen, die den ausgewählten Objekten zugewiesen sind, verwenden die neue Weiterleitungsmethode.

Nächste Maßnahme

Zeigen Sie in SAP Solution Manager generierte Warnungen an, um alle dringenden Probleme anzuzeigen (siehe Warnungen im Posteingang von SAP Solution Manager anzeigen) .

Alert-Eingang in SAP Solution Manager konfigurieren

Konfigurieren Sie SAP Solution Manager, um Warnungen auf dem System abzurufen, indem Sie den Alert-Eingang mit dem SOA-Manager aktivieren.

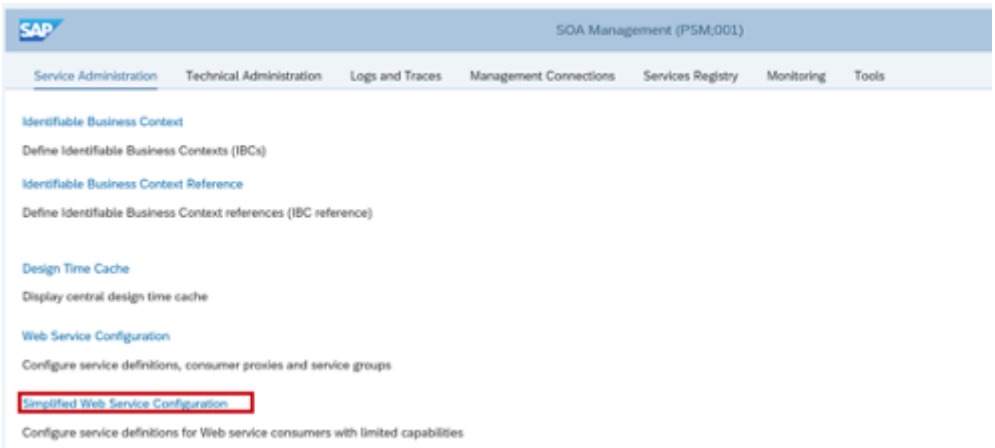
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie in Ihrem Lösungsmanager zu SOA-Manager: /sap/bc/webdynpro/sap/appl_SOAP_Management?sap-Client=XXX&sap-language=EN#
2. Wählen Sie Aus **Vereinfachte Webservicekonfiguration** , Validieren Sie dann das Formular, um den Service zu aktivieren.
   Sie müssen den vereinfachten Modus verwenden, andernfalls unterscheiden sich die resultierenden Webservices von anderen Modi und sind nicht mit dem Connector kompatibel.



3. Klicken Sie auf **Search** (Suchen).
4. Überprüfen Sie die Zeile mit dem Erstellungstyp **Einfacher Verbraucherbezug** .
   Wenn etwas schief geht, überprüfen Sie dies Service Provider konfigurieren (vereinfacht)

Nächste Maßnahme

Zeigen Sie in SAP Solution Manager generierte Warnungen an, um alle dringenden Probleme anzuzeigen (siehe Warnungen im Posteingang von SAP Solution Manager anzeigen) .

Warnungen im Posteingang von SAP Solution Manager anzeigen

Sie können in SAP Solution Manager generierte Warnungen anzeigen, um alle dringenden Probleme anzusehen. Alle Warnungen werden auch automatisch an Ereignismanagement weitergeleitet.

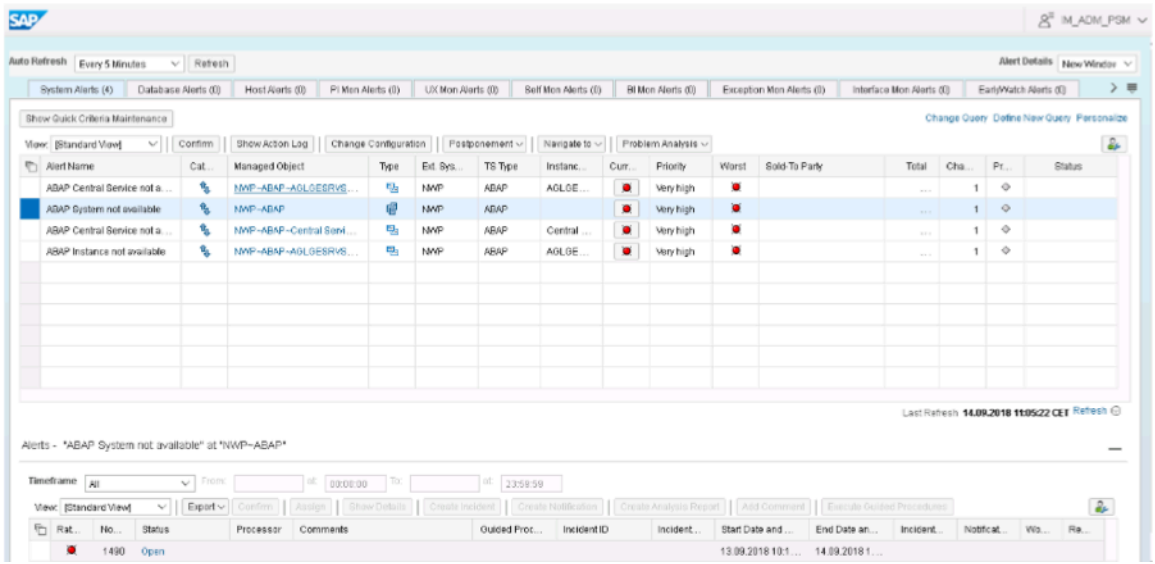
Vorbereitungen

Erforderliche Rolle: evt_mgt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

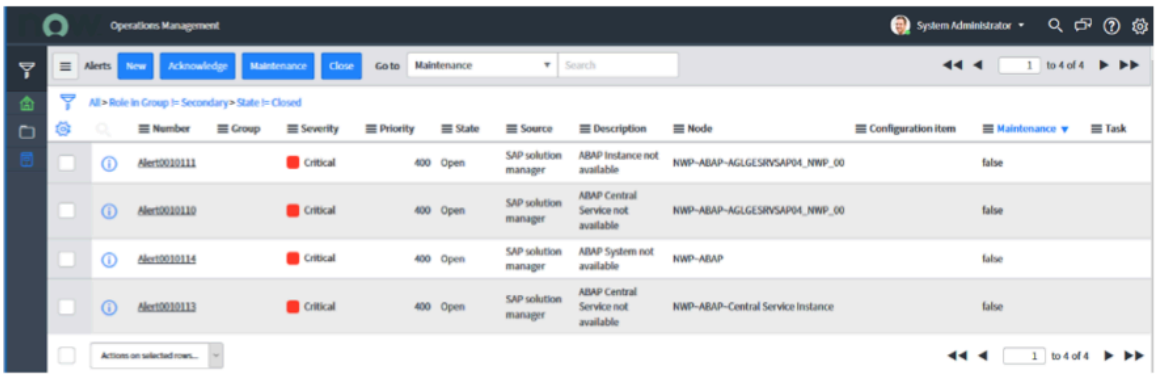
Prozedur

1. Öffnen Sie auf der SAP-UI den Solution Manager und wählen Sie die Registerkarte **Systemwarnungen** aus.



Die Systemwarnungen werden auf der Seite aufgelistet.

2. Navigieren Sie zu (**Ereignismanagement** > **Alle Warnungen)** Um die Warnungen in anzuzeigen Ereignismanagement.



In der folgenden Tabelle wird die Feldzuordnung zwischen SAP Solution Manager und Ereignismanagement für Warnungen beschrieben.

Feldzuordnung für SAP Solution Manager und Ereignismanagement

SAP-Feld	Event Management-Feld	Beschreibung
severity	severity	SAP verwendet eine Zahl von 1 (weniger kritisch) bis 9 (kritischer)
message_key	message_key	SAP-Nachrichtengruppen-ID, messageGUID
description	description	Event-Beschreibung
source	source	SAP-System-ID

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP-Feld	Event Management-Feld	Beschreibung
managed_object_type	type	Der Typ des Objekts, z. B. Host oder Instanz
Knoten	Knoten	Objektname
managed_object_name	Ressource	Knotenname Solution Manager
N. z. (von SAP ist kein Wert angegeben. Ereignismanagement generiert das angegebene Feld.)	source instance	Die Ereignisklasse muss mit dem Namen der Connector-Abrufinstanz und der Struktur übereinstimmen <Source>_<Client> .
Quelle	additional_info.sid	SAP-System-ID
rating	additional_info.rating	Event-Farbe in SAP
resource	additional_info.mandant	SAP-Mandant
metric_name	metric_name	Metrikname für das SAP-Ereignis
time_of_event	time_of_event	Zeit des Events in SAP

Example: Hohe CPU-Auslastung auf SAP-Host

Szenario: In SAP Solution Manager wird eine Warnung generiert, wenn die CPU-Auslastung auf einem kritischen Host mehr als 10 Minuten lang 90 % überschreitet.

SAP Solution Manager-Warnung

Feld	Wert
Schweregrad	8 (Kritisch)
Nachrichtenschlüssel	CPU_Overload_12345
Beschreibung	Hohe CPU-Auslastung auf SAPHost01
Quelle	SAP_Prod
Typ	Host
Knoten	SAPNode_01
Zeit	2024-07-31T14:23:00Z

So wird die Warnung in zugeordnet Ereignismanagement:

Zugeordnet Ereignismanagement Warnung

Feld	Wert
Schweregrad	8
Nachrichtenschlüssel	CPU_Overload_12345
Quelle	SAP_Prod
Typ	Host
Knoten/Ressource	SAPNode_01
Quelleninstanz	SAP_Prod_100

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugeordnet Ereignismanagement Warnung (Fortsetzung)

Feld	Wert
SID	SAP_Prod
Bewertung	Rot
Mandant	100

SAP Solution Manager-Zertifikat anzeigen und aktualisieren

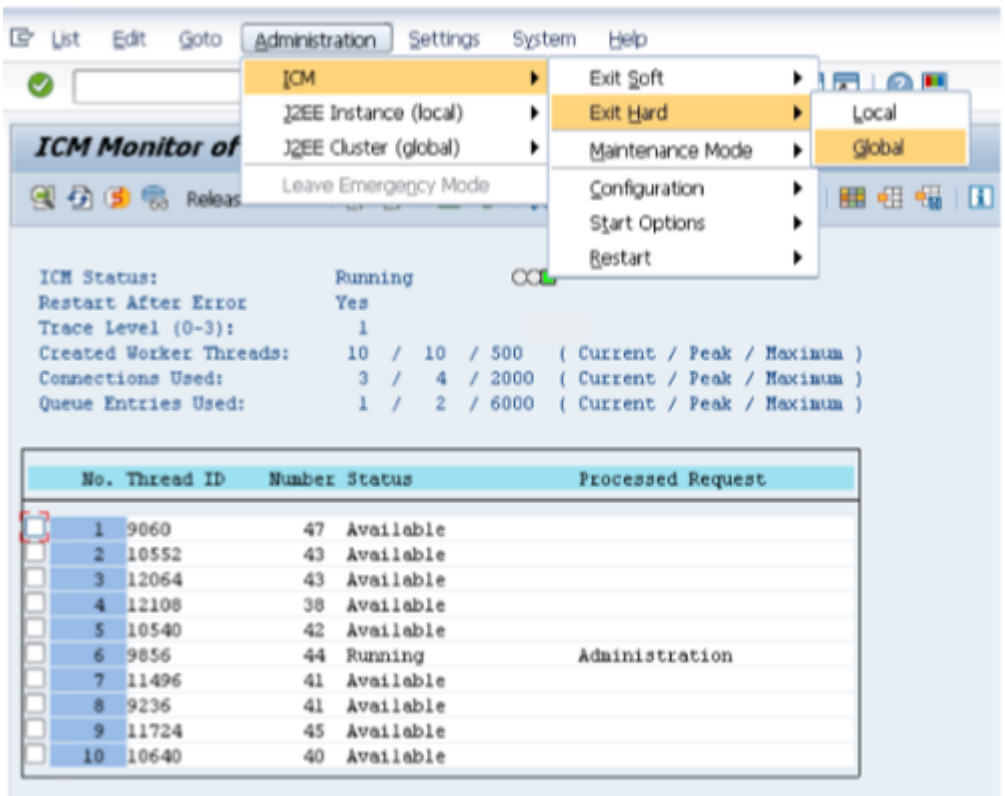
Zeigen Sie Ihr SAP Solution Manager-Zertifikat an und aktualisieren Sie es gegebenenfalls.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Stellen Sie eine Verbindung zu SAP auf Client 00 her.
2. Geben Sie die `strust`-Transaktion ein.
3. Öffnen Sie in der Trust Manager-UI den SSL-Client.
4. Importieren Sie das SSL-Zertifikat, und speichern Sie es.
5. Verwenden Sie die Transaktion `smicm`, um das System mit HTTP- und HTTPS-Clients zu verbinden.
6. Navigieren zu **Administration** > **ICM** > **Hart Beenden** > **Global**an.



Das ICM-Modul wird neu gestartet.

SAP-Schnittstellenprotokoll anzeigen

Zeigen Sie das SAP-Schnittstellenprotokoll an, um Probleme zu debuggen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

Wählen Sie eine Transaktion in der SAP-UI aus.
Die Debugging-Tabelle der ZSNOW-Schnittstelle wird angezeigt.

SAP Solution Manager-Transaktionscodes

Die Transaktionscode-Abkürzungen, die Sie in der SAP-Schnittstelle verwenden können, wenn Sie mit dem SAP Solution Manager-Connector arbeiten.

SAP Solution Manager-Transaktionscodes

Transaktionscode	Beschreibung
ALRTINBOX	Zeigt den Warnungs-Posteingang an.
SOAMANGER	Öffnet und aktiviert den Webservice *`Sap_Solman_Alert_Inbox`*.
SRT_UTIL	Zeigt die SOA-Manager-Protokolle an.
SOLMAN_WORKCENTER	Öffnet die Oberfläche des SAP Solution Manager in einem Browser.
SM59	Zeigt die gesamte Ausgabeschnittstelle an.
SE38	Führt den ABAP-Code (Advanced Business Application Programming) aus. (Der entsprechende ServiceNow-Code ist *`ZTEST_SNOW_CONNECTOR`*.)
MAI_TOOLS	Zeigt das Warnungstool an.
SE16	Zeigt die Schnittstellen-Debugging-Tabelle (ZSNOW) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von SCOM konfigurieren

Warnungen vom Microsoft System Center Operations Manager (SCOM) werden mit der SCOM-Connector-Instanz erfasst.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die SCOM-Connector-Instanz erfordert eine Konfiguration, bevor Warnungen und empfangen werden können Metrikdaten Rohdaten vom SCOM-Server. Sie können die Erfassung von SCOM-Warnungen auf die Warnungen beschränken, die zu der von Ihnen angegebenen SCOM-Gruppe gehören.

Prozedur

1. Konfigurieren Sie die SCOM-Connector-Instanz.
2. Konfigurieren Sie die Microsoft System Center Operations Manager (SCOM)-Connector-Instanz, um Warnungen und Metric Intelligence-Rohdaten vom SCOM-Server zu empfangen.
3. Beschränken Sie gesammelte SCOM-Warnungen auf bestimmte SCOM-Gruppen.

SCOM-Connector-Instanz konfigurieren

Konfigurieren Sie die Connector-Instanz des Microsoft System Center Operations Managers (SCOM), um Warnungen und Metrikdaten-Rohdaten vom SCOM-Server zu empfangen.

Vorbereitungen

Zum Aktivieren **Metriksammlung** , Stellen Sie sicher, dass MID-Server Die Metriken abruft, wird mit konfiguriert Metrikdaten Erweiterung und , in der sich die Erweiterung befindet **Gestartet** Modus. Weitere Informationen finden Sie unter Konfigurieren Sie manuell Metrikdaten Erweiterung.

Windows Die Authentifizierung wird vom Connector für den Zugriff auf die SCOM-Datenbank (OperationsManagerDW) verwendet. Daher wenn **Metriksammlung** Ist und ausgewählt **Datenbankanmeldung mit Windows-Authentifizierung** Die Option ist ebenfalls ausgewählt. Stellen Sie sicher, dass die Option ausgewählt ist MID-Server Der Service wird mit einem Anwender ausgeführt, der Lesezugriff auf die SCOM-Datenbank hat. Stellen Sie sicher, dass die richtigen Anmeldeinformationen verwendet werden:

1. Wählen Sie in den lokalen Services die aus, und halten Sie sie gedrückt (oder klicken Sie mit der rechten Maustaste darauf) MID-Server Service und wählen Sie aus **Eigenschaften** .
2. In **Melden Sie Sich An** Registerkarte, stellen Sie sicher, dass **Dieser Account** Ist ausgewählt. Fügen Sie die Details von hinzu Windows Domänenanwender, der Lesezugriff auf die SCOM-Datenbank hat.

Bevor Sie mit dem Verfahren zum Konfigurieren des Connectors beginnen, stellen Sie Folgendes sicher:

- Die MID-Server Wird mit einem Anwender ausgeführt, der über lokale Administratorberechtigungen zum Aktivieren von verfügt MID-Server Zum Ausführen von PowerShell.
- Die MID-Server Anwender hat Lesezugriff auf die SCOM-API.
- Die MID-Server Befindet sich in derselben Domäne wie der SCOM-Server.
- Die MID-Server Verwendet dieselbe Zeitzone wie der SCOM-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die MID-Server Wird unter Windows ausgeführt.
- Die MID-Server Hat .NET Framework Version 3,5.

Wenn **Bidirektional** ausgewählt ist, stellen Sie Folgendes sicher:

- PowerShell Version 3.0 ist unter Windows installiert.
- Die MID-Server Wird mit einem Anwender ausgeführt, der über lokale Administratorberechtigungen verfügt, um die Ausführung von PowerShell zu aktivieren.

So aktualisieren Sie einen vorhandenen SCOM-Connector:

1. Auf der Seite „Connector-Instanz – SCOM-Connector“ (**Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**), löschen Sie **Erfassen Sie Metriken** Kontrollkästchen.
2. Installieren Sie *em-connectors*Plugin aus dem Store.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Um SCOM-Warnungen zu erhalten, können Sie die verteilbaren SCOM-Dateien von Ihrer SCOM-Anwendung abrufen. Fügen Sie die Dateien dem MID-Server hinzu und konfigurieren Sie dann eine SCOM-Connector-Instanz, um die Warnungen und Metrikdaten-Rohdaten zu erfassen.

Die Erfassung von Metrikdaten wird mithilfe von JavaScript ausgeführt; hier wird JDBC anstelle von PowerShell ausgeführt.

Sie können dieses Setup auch für die von SCOM verwaltete Instanz auf verwenden Azure.

Für diesen Connector ist der Protokollparameter *logPayloadForDebug* aktiviert. Dadurch werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Unterstützte Versionen:

- 2007 – Version 6.1.7221.0
- 2012 – Version 7.1.10226.0
- 2016 – Version 7.2.117190 und 7.3.13261.0
- 2019 – Version 10.19.10050.0
- 2022: Version 10.22.10118.0

Prozedur

1. Laden Sie auf dem SCOM-Server die folgenden Dateien auf einen lokalen Computer herunter.

Version	SCOM-Pfad- und Bibliotheksnamen
SCOM 2012R2 oder SCOM 2012	%ProgramFiles%\Microsoft System Center 2012 R2 or 2012\Operations Manager\Ser–ver\SDK Binaries

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version	SCOM-Pfad- und Bibliotheksnamen
	○ Microsoft.EnterpriseManagement.Core.dll ○ Microsoft.EnterpriseManagement.Operati–onsManager.dll ○ Microsoft.EnterpriseManagement.Runtime–.dll
SCOM 2007	%ProgramFiles%\System Center Operations Manager 2007\SDK Binaries ○ Microsoft.EnterpriseManagement.Operati–onsManager.Common.dll ○ Microsoft.EnterpriseManagement.Operati–onsManager.dll **Hinweis:** Fügen Sie nicht 2007 an die Da-tei Microsoft.EnterpriseManagement–.OperationsManager.Common.dll an.
SCOM 2016	%ProgramFiles%\Microsoft System Center 2016\Operations Manager\Server\SDK Bina–ries ○ Microsoft.EnterpriseManagement.Core.dll ○ Microsoft.EnterpriseManagement.Operati–onsManager.dll ○ Microsoft.EnterpriseManagement.Runtime–.dll **Hinweis:** Die MID-Server Muss mit .NET 4,6 oder höher installiert werden.
SCOM 2019	%ProgramFiles%\Microsoft System Center 2019\Operations Manager\Server\SDK Bina–ries ○ Microsoft.EnterpriseManagement.Core.dll ○ Microsoft.EnterpriseManagement.Operati–onsManager.dll ○ Microsoft.EnterpriseManagement.Runtime–.dll **Hinweis:** Die MID-Server Muss mit .NET 4,6 oder höher installiert werden.
SCOM 2022	○ Microsoft.EnterpriseManagement.Core.dll ○ Microsoft.EnterpriseManagement.Operati–onsManager.dll ○ Microsoft.EnterpriseManagement.Runtime–.dll

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version	SCOM-Pfad- und Bibliotheksnamen
	Hinweis: Die MID-Server Muss mit .NET 4,6 oder höher installiert werden.

Hinweis: Eine Verbindung zu SCOM 2012/SCOM 2016/SCOM 2019/SCOM 2022 und SCOM 2007 kann nicht von derselben hergestellt werden MID-Server. Um sowohl mit SCOM 2012/SCOM 2016/SCOM 2019/SCOM 2022 (beliebig) als auch mit SCOM 2007 in Ihrer Instanz zu arbeiten, gehen Sie vor dem Hochladen von Dateien in Ihre Instanz wie folgt vor:

a. Fügen Sie .2012 an das Ende von an Microsoft.EnterpriseManagement.Betriebsmanager.DLL Datei, also wird sie: Microsoft.EnterpriseManagement.Betriebsmanager.DLL.2012 . Führen Sie dies für 2012/2016/2019/2022 aus.

b. Hängen Sie .2007 an das Ende der Microsoft.EnterpriseManagement.OperationsManager.dll- Datei an, die sich im Pfad 2007 befindet.

Durch die Verwendung dieser geänderten Dateinamen wird relevant MID-Server Zum Laden der anwendbaren DLL, wenn beide SCOM-Versionen bereitgestellt werden. Fügen Sie nicht 2007 an die Datei Microsoft.EnterpriseManagement.OperationsManager.Common.dll an (für SCOM 2007).

Sie können jederzeit Connectors für SCOM 2007, SCOM 2012/2016 oder SCOM2019 definieren. Da SCOM 2012 und SCOM 2016 dieselben Bibliotheksdateien verwenden, können sie gleichzeitig arbeiten. Da allerdings von SCOM 2019 die verschiedenen SCOM-DLL-Dateien verwendet werden, können Sie SCOM 2012, 2016 und 2019 nicht zusammen konfigurieren. Jeder SCOM-Connector kann die Datenbank eines anderen Connectors für Metrikunterstützung verwenden.

2. Navigieren zu **MID-Server** > **JAR-Dateien**an.
3. Wählen Sie Aus **Neu** Und fügen Sie für jede der DLL-Dateien, die Sie vom SCOM-Server heruntergeladen haben, einen separaten Datensatz für die SCOM-Version hinzu.

   a. Geben Sie im Feld **Name** die SCOM-Version und einen Bezeichner an, um den Namen eindeutig zu machen, z. B. 2012 1.
   Wenn Sie SCOM 2016 verwenden, geben Sie 2012 als Version an.

   b. Wählen Sie das Büroklammer-Symbol im Formularheader aus, und hängen Sie dann eine der entsprechenden DLL-Dateien an, die Sie heruntergeladen haben.

   c. Wählen Sie **Absenden**.

4. Wiederholen Sie Schritt 3, und erstellen Sie für jede der verbleibenden DLL-Dateien einen separaten Datensatz.
   Stellen Sie sicher, dass Sie nach der SCOM-Version für jede angehängte Datei einen eindeutigen Bezeichner haben, z. B. 2012 2.
5. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
6. Klicken Sie Auf **Neu** Und erstellen Sie eine neue Connector-Instanz.
   Details zu den Feldern der Connector-Instanz, die auf der Seite angezeigt werden, finden Sie unter Formular „SCOM-Connector-Instanz“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
8. Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen SCOM-Parameter bearbeiten.

   a. **login_with_windows_authentication** Standardwert: **false**.
   Auf **true** festlegen, um die SCOM-Event-Erfassung und den bidirektionalen Austausch von Event-Werten für die Windows-Authentifizierung zu aktivieren.

   Stellen Sie beim Aufrufen dieses Werts sicher, dass Sie im Folgendes tun MID-Server:

   i. Navigieren Sie zur Liste der lokalen Services, wählen Sie aus, und halten Sie (oder klicken Sie mit der rechten Maustaste) MID-Server Service, und wählen Sie aus **Eigenschaften** .

   ii. Stellen Sie auf der Registerkarte **Anmelden** sicher, dass **Dieses Konto** mit den Details des Benutzers in der Windows-Domäne ausgewählt ist, der Lesezugriff auf die SCOM-Datenbank hat.

   b. **Metrik_Chunk_size** : Standardwert: 50000.

   c. **scom_date_Format** : Standardformat: M/d/jjjj/ h:mm:ss a
   Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, ändern Sie diesen Wert so, dass es dem Format des eingehenden Events entspricht. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

   Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *`2019/06/27/ 11:25:00 a`* ankommt, ändern Sie den Wert **scom_date_format** in *`yyyy/ M/d/ h:mm:ss a`*, damit es dem Format des empfangenen Events entspricht.

   In **scom_date_format** steht `a` für morgens und `p` für nachmittags.

   d. **scom_initial_Sync_in_days** : Standardwert: 7.

   e. **scom_Version** : Die Angabe der SCOM-Version ist obligatorisch.
   Wählen Sie 2022, 2019, 2016, 2012 oder 2007 aus.

   f. **Stop_isMonitorAlert_bidirektional** : Boolescher Wert.
   Auf festlegen **Wahr** Um nur bidirektional SCOM-Überwachungswarnungen zu stoppen. Das Stoppen von SCOM-Überwachungswarnungen kann falsche Alarme in der SCOM-Konsole verhindern, wenn versucht wird, die Warnungen zu aktualisieren. Wenn auf festgelegt **Falsch** , SCOM-Überwachungswarnungen werden für alle Arten von SCOM-Warnungen weiterhin bidirektional ausgeführt.

   Standardwert = falsch.

9. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
10. Starten Sie neu MID-Server Service zum Kopieren der Dateien.
11. Wählen Sie Aus **Testen Sie den Connector** Dient zum Überprüfen der Verbindung zwischen MID-Server Und der Connector.
    Wenn der Test fehlschlägt, beheben Sie das Problem, indem Sie die Anweisungen der Fehlermeldung befolgen, und führen Sie dann einen weiteren Test aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerktool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität von zu überprüfen MID-Server An SCOM.

12. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

Hinweis:

Die Standardbindungsregeln, die SCOM als externe Quelle enthalten und für IT-Warnungen und Metrikdaten-Rohdaten gelten, sind die folgenden SCOM Management Packs:

- Alle BS-Management Packs
- MS SQL-Server
- IIS

Example:
Wenn bidirektional konfiguriert ist, ist der bidirektionaler Austausch von Werten mit der externen Event-Quelle möglich.
Diese Szenarien beschreiben die bidirektionale Standardfunktionalität für SCOM-Connectors:

- Wenn eine Warnung in SCOM gelöst wird, wird sie in ServiceNow automatisch geschlossen. Sie wird jedoch unabhängig von der bidirektionalen Funktion aktualisiert, da während jedes Erfassungszyklus alle Warnungsänderungen aktualisiert werden.
- Wenn eine Warnung in ServiceNow manuell geschlossen wird, wird sie in SCOM automatisch geschlossen. Wenn der Warnungsstatus in **Erneut öffnen** geändert wird, wird SCOM auch aktualisiert.
- Wenn ein Incident erstellt und einer Warnung in ServiceNow zugeordnet wird, erhält SCOM die Incident-Nummer als Ticket-ID. Der Status des Incidents ist jedoch in SCOM nicht verfügbar. Daher wird bei der Lösung des Incidents in ServiceNow SCOM nicht aktualisiert, da die Incident-Nummer gleich bleibt. Wenn die Warnung einem neuen Incident zugeordnet ist, wird die neue Incident-Nummer in SCOM aktualisiert.

Erfasste SCOM-Warnungen auf bestimmte SCOM-Gruppen beschränken

Sie können die Erfassung von SCOM-Warnungen auf die Warnungen beschränken, die zu der von Ihnen angegebenen SCOM-Gruppe gehören.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Verwenden Sie den SCOM-Authoring-Arbeitsbereich und die Betriebskonsole, um eine SCOM-Gruppe zu definieren und sicherzustellen, dass die Gruppe die erforderlichen Computer oder Instanzen enthält. Weitere Informationen zu SCOM-Gruppen finden Sie in der SCOM-Dokumentation.
2. Erstellen Sie eine Rolle mit dem Umfang der SCOM-Gruppe.
3. Fügen Sie dem SCOM-Benutzer die neue Rolle hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Weisen Sie die Rolle dem Benutzer zu, der in den Anmeldeinformationen für die SCOM-Connector-Instanz definiert ist.
5. Entfernen Sie alle anderen Rollen vom Benutzer.

Ergebnis
Nur Warnungen aus der angegebenen SCOM-Gruppe kommen bei der Instanz an.

SCOM-Metrikereignisregeln

Das Basissystem enthält Metrikereignisregeln für Microsoft System Center Operations Manager (SCOM). SCOM-Metrikereignisregeln binden Ereignismetriken an Konfigurationselemente (Configuration Items, CIs).

Wenn die Metriken eines Ereignisses den Ereignisfilterbedingungen entsprechen, werden die Metriken an das angegebene CI gebunden. Die Ereignisregeln, die mit dem Basissystem geliefert werden, sind:

Ereignisregeln der Basissystemmetrik

Regelname	CI-Typ
SCOM-Metriken: Windows Server	cmdb_ci_win_server
SCOM-Metriken: IIS-Webserver	cmdb_ci_microsoft_iis_web_server
SCOM-Metriken: SQL Server Reporting-Services	cmdb_ci_DB_mssql_Reporting
SCOM-Metriken: MS SQL-Datenbank	cmdb_ci_db_mssql_database
SCOM-Metriken: MSFT SQL-Instanz	cmdb_ci_db_mssql_instance

Sie können eine anwenderdefinierte Ereignisregel erstellen, um Metriken an andere CI-Typen zu binden. Details finden Sie unter Event-Regel erstellen oder bearbeiten.

Wenn der Ereignisregelfilter nicht übereinstimmt, wird die Standardregel *`SCOM Metrics - Default`*(CI-Typ = *`cmdb_ci_hardware`*) Wird aufgerufen. Die Reihenfolgenummer der standardmäßigen Ereignisregel muss höher sein als die Reihenfolgenzahl aller SCOM-Ereignisregeln (sowohl diejenigen, die im Basissystem enthalten sind, als auch alle anwenderdefinierten Regeln), damit alle anderen Regeln auf Übereinstimmung überprüft werden, bevor die Standardregel aufgerufen wird. Details zu Ereignisregeln finden Sie unter Event-Regeln.

Event-Erfassung vom SolarWinds-Monitor konfigurieren

Konfigurieren Sie die SolarWinds-Monitor-Connector-Instanz für den Empfang von Events vom SolarWinds-Monitor.

Vorbereitungen
Unterstützte Versionen:

- SAM 6.2.1
- NPM 2024.1

Hinweis: Die SolarWinds-Monitor-Connector-Instanz kann Events importieren aus:

- Network Performance Monitor (NPM)
- SolarWinds-Service- und Anwendungsüberwachung (SAM)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die SolarWinds-Connector-Instanz erfordert Anmeldeinformationen, mit denen die Instanz auf SolarWinds-Monitorkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen. Der angegebene Anwender muss Zugriff auf die SolarWinds-API haben, um Ereignisse vom SolarWinds-Connector zu empfangen.

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den SolarWinds-Monitor-Connector ein.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der SolarWinds-Monitor-Ereignissammlung ein.
Connector-Definition	Wählen Sie Aus **SolarWinds_v2** .
Host-IP	Geben Sie die IP-Adresse des SolarWinds-Monitors an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Weitere Informationen finden Sie unter SolarWinds-Monitoranmeldeinformationen erstellen.
Zeit der letzten Ausführung der Event-Erfassung	Der letzte Wert der Ausführungszeit des Scheduled Job. Dieses Feld wird automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Der letzte Event-Erfassungsstatus. Dieses Feld wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom SolarWinds-Monitor-Server sucht.
Letzte Fehlermeldung	Die letzte vom Connector empfangene Fehlermeldung wird automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
5. Geben Sie im Abschnitt Connector-Instanzwerte diese Felder an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
initial_sync_in_days	Geben Sie an, wie viele Tage der erste Abruf zum Abrufen von Events enthalten muss. Der Standardwert lautet 7 Tage.
nodes_custom_properties	Geben Sie die SolarWind-Monitor-Eigenschaftsnamen, die dem entsprechenden Knoten zugeordnet sind, an. Diese Informationen werden dem Feld **Zusätzliche Informationen** des Events im JSON-Format hinzugefügt. Bei den benutzerdefinierten Eigenschaften des SolarWinds-Monitors handelt es sich um benutzerdefinierte Felder, z. B. Land, Gebäude oder Seriennummer, die Sie überwachten Netzwerkobjekten zuordnen können. Trennen Sie mehrere Einträge durch ein Komma.
port	Geben Sie den Wert des Ports an. Standardmäßig ist der Wert 1777 4. **Hinweis:** Für Version 2023,1 und höher ist der Port 17774.

6. **Wahlweise:** Der Name des MID Servers.
   Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden. Die Berechtigungen, die für das Benutzerkonto erforderlich sind, das für den MID Server zum Erfassen von Events vom SolarWinds-Monitor verwendet wird, sind die von evt_mgmt_integration.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem SolarWinds-Monitor-Connector zu überprüfen.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum SolarWinds-Monitor-Connector zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

SolarWinds-Monitoranmeldeinformationen erstellen

Erstellen Sie Anmeldeinformationen, um auf den SolarWinds-Monitor zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie SolarWinds-Authentifizierung nennen.
Benutzername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: 100

5. Klicken Sie auf **Absenden**.

Ergebnis

Die Anmeldeinformationen für die Verwendung mit dem SolarWinds-Monitor-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Event-Erfassung von vCenter konfigurieren

Konfigurieren Sie die VMware vCenter Server-Connector-Instanz (vCenter oder vCenter_V2), um Ereignisse aus Ihrer VMware vSphere-Umgebung zu empfangen.

Vorbereitungen

Von diesem Connector erfasste Events sind Events, die der Event-Regel von vCenter ESX Servers entsprechen. Unterstützte Version: 7,0.2,00500.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

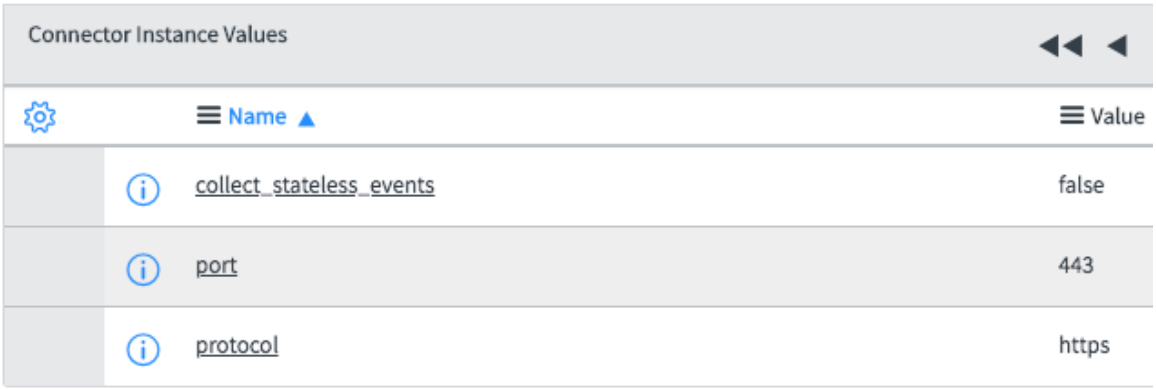
Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den vCenter-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der vCenter-Ereignissammlung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **vCenter** oder **vCenter_V2** aus (vCenter_V2 befindet sich im Bereich der Ereignismanagement-Connectors).
Host-IP	IP-Adresse, unter der vCenter installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit vCenter. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „vCenterCHCK“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von vCenter sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Connector-Instanzwerte werden dem Formular hinzugefügt,
und die für den Connector relevanten Parameter werden angezeigt.



5. Geben Sie im Abschnitt Connector-Instanzwerte die vCenter-Werte an.

Feld	Wert
collect_stateless_events	Events, die einen Status (statusbehaftet) haben, werden erfasst, wenn dieses Feld auf `false` (Standard) festgelegt ist. Diese Events sind vom Typ „AlarmStatusChangedEvent“ und „AlarmClearedEvent“. Wenn dieses Feld auf `true` festgelegt ist, werden auch Events anderer Typen erfasst.
port	Geben Sie den Wert des Ports an. Standardwert: `443`.
protocol	Geben Sie das Protokoll an. Standardwert: `https`.

6. **Wahlweise:** Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an.
Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

   Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. Testen Sie die Verbindung zwischen dem MID-Server und dem vCenter-Connector.

   a. Klicken Sie auf **Connector testen**.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   > **Hinweis:** Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum externen Überwachungs-Tool zu überprüfen.

   b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von vRealize konfigurieren

Konfigurieren Sie die VMware vRealize Operations-Connector-Instanz (vRealize oder vRealize_V2), um Ereignisse von den vRealize Operations Log- und Ereignismanagement-Servern zu empfangen. VRealize verwendet die Standardauthentifizierung. VRealize_V2 verwendet eine Token-basierte Authentifizierung.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Version: 8.10.0.

Hinweis: Stellen Sie eine Verbindung zu vRealize her, indem Sie einen lokalen Konto mit mindestens der Berechtigung für schreibgeschützte vRealize Operations verwenden. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu** und erstellen Sie eine vRealize Operations-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die vRealize Operations-Connector-Instanz an.
Host-IP	Geben Sie die IP-Adresse von vRealize Operations an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Von vRealize_V2 wird eine tokenbasierte Authentifizierung verwendet, sofern der Benutzer das Token generieren kann. Weitere Informationen finden Sie unter vRealize-Anmeldeinformationen erstellen.
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von vRealize Operations sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung des vRealize Operations-Connectors ein.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie **vRealize** oder **vRealize_V2** aus (vRealize_V2 befindet sich im Bereich der Ereignismanagement-Connectors).
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen vRealize Operations-Parameter an.

   a. **port**: Standardwert = `443`

   b. **protocol**: Standardwert = `https`

   c. **Days_from** :
   Anzahl der Tage, die bei der ersten Ausführung der Ereigniserfassung abgerufen werden sollen. Standardwert = `14`. Die Option **days_from** ist nur verfügbar, wenn vRealize_V2 verwendet wird.
5. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem vRealize Operations-Connector zu überprüfen.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zu vRealize zu überprüfen.
7. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

vRealize-Anmeldeinformationen erstellen

Erstellen Sie Anmeldeinformationen, um auf vRealize zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie den Standardauthentifizierungstyp für Anmeldeinformationen, um eine Verbindung mit vRealize herzustellen.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Beispiel: `NewvRealize`.
Benutzername	Name zum Identifizieren des Benutzers. ○ Wenn der Benutzername in vRealize intern ist, verwenden Sie ihn unverändert. ○ Wenn vRealize in Active Directory (AD) integriert ist, verwenden Sie das Format `DOMAIN\username@sourceauth`. Beispiel: `local\administrator@All vCenter Servers`.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Klicken Sie auf **Absenden**.

Ergebnis
Die Anmeldeinformationen für die Verwendung mit dem vRealize-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Event-Erfassung vom Zabbix-Server konfigurieren

Konfigurieren Sie die Zabbix-Server-Connector-Instanz für den Empfang von Warnungen vom Zabbix-Server.

Vorbereitungen
Unterstützte Versionen: Von 3.0.0 bis 7.0.0

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Connector-Instanz des Zabbix-Servers erfordert Anmeldeinformationen, mit denen die Instanz auf Zabbix-Serverkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Connector ist der Protokollparameter *logPayloadForDebug* aktiviert. Dadurch werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

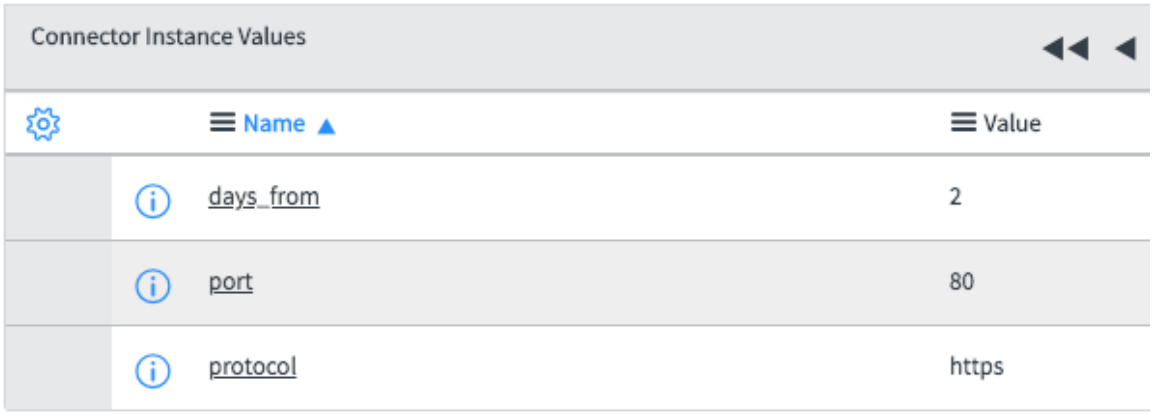
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Host-IP	IP-Adresse für den Zabbix-Server.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Weitere Informationen finden Sie unter Erstellen Sie Zabbix-Server-Anmeldeinformationen.
Zeitplan (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom Zabbix-Server sucht.
Beschreibung	Beschreibung für die Verwendung der Instanz der Ereignissammlung des Zabbix-Servers.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **Zabbix** aus.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Letzte Ausführungszeit	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Ausführungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden



angezeigt.

5. Überprüfen und ändern Sie die Werte nach Bedarf.
Im Abschnitt Connector-Instanzwerte erscheinen die Standardwerte der Connector-Instanz.

Felder im der Abschnitt Connector-Instanzwerte

Feld	Beschreibung
days_from	Anzahl der Tage, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: 2 **Hinweis:** Die maximale Anzahl vergangener Events, die erfasst werden können, beträgt 3.000. Bei der ersten Ausführung dieses Connectors wird die Anzahl der vergangenen Ereignisse in der Vergangenheit ab dem aktuellen Datum gezählt.
port	Port-Nummer. Standardwert: 80.
protocol	Protokolltyp. Standardwert: https.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum Zabbix-Server zu überprüfen.

9. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

Erstellen Sie Zabbix-Server-Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um auf den Zabbix-Server zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie Zabbix-Authentifizierung nennen.
Benutzername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: 100

5. Klicken Sie auf **Absenden**.

Ergebnis

Die Anmeldeinformationen zur Standardauthentifizierung für die Verwendung mit dem Zabbix-Server-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Konfigurieren Sie einen Push-Connector

Sie können Listener und Connectors so konfigurieren, dass Event-Informationen an die Instanz oder den MID-Server übertragen werden.

Ereignismanagement empfängt externe Events über einen Push-Connector oder ein Skript. Wenn Sie ein Skript zum Erfassen von Events verwenden, ist keine Konfiguration erforderlich. Alle anderen Methoden zum Erfassen von Events müssen konfiguriert werden.

Nach der Konfiguration der Event-Erfassung kann Ereignismanagement Events erfassen, die direkt an die Instanz oder über den MID-Server, den SNMP-Trap oder per E-Mail gesendet werden.

Hinweis: Die Integration mit Push-Connectors ist nur durch die Installation des Plugin „Ereignismanagement Connector“ aus dem ServiceNow Store möglich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Event-Formular

Ein Standard-Event-Formular muss von allen Events verwendet werden, unabhängig davon, wie sie bei der Instanz ankommen. Weitere Informationen finden Sie unter Event-Feldformat für die Event-Erfassung.

Event-Erfassung

Ereignismanagement ermöglicht die Kommunikation und den Transport von Daten zwischen externen Anwendungen, Datenquellen, Services und der ServiceNow AI Platform-Instanz.

Event-Erfassungsmodi	Beschreibung
Vom Basissystem bereitgestellt	Mit der Anwendung Ereignismanagement bereitgestellte Listener und Connectors: • AWS CloudWatch, siehe AWS-Plattform als Datenquelle integrieren • Azure-Event-Nachrichten, siehe Azure Monitor als authentifizierte Datenquelle integrieren • BMC TrueSight-Events, siehe Ereignissammlung von BMC TrueSight und BMC TrueSight_v2 • Datadog-Events, siehe Integrieren Datadog Plattformereignisse • Dynatrace-Events, siehe Integrieren Dynatrace Plattformereignisse • Google Cloud Platform (GCP)-Events, siehe Google Cloud Platform (GCP)-Events integrieren • New Relic-Events, siehe Events der New Relic-Plattform integrieren • Allgemeine Event-Erfassung über den MID-Server • Allgemeine Event-Erfassung über die Instanz Wenn Event-Nachrichten in XML empfangen werden, können Sie ein Skript verwenden, das auf dem im Basissystem bereitgestellten XML-Transformationsskript basiert.
Über MID WebService	Sie können den MID-Webservice-Ereignissammler so konfigurieren, dass Ereignisnachrichten an gesendet werden MID-Server. Weitere Informationen finden Sie unter Ereignisse werden an übertragen MID-Server Webservice-API wird verwendet.
Eigenen Inhalt erstellen	Sie können Ihren eigenen Listener konfigurieren: • Über die MID-Webserver-API. Weitere Informationen finden Sie unter Ereignisse werden mithilfe der Webservice-API an die Instanz übertragen. • Über benutzerdefinierte Transformation. Weitere Informationen finden Sie unter Event-Erfassung aus benutzerdefinierten Nutzlasten.
Über SNMP.	Mit der Anwendung Ereignismanagement bereitgestellte SNMP-Listener: Generisches SNMPv2. Weitere Informationen finden Sie unter #unique_1474. Darüber hinaus können Sie Ihren eigenen benutzerdefinierten Listener erstellen. Weitere Informationen finden Sie unter Integration mit Push-Connectors.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassungsmodi	Beschreibung
Per E-Mail	E-Mail-Listener. Weitere Informationen finden Sie unter Event-Erfassung per E-Mail konfigurieren.

Zugehörige Informationen

Push-Connector-Instanzformular

Konfigurieren ServiceNow Cloud Observability Ereignissammlung

Integrieren ServiceNow Cloud Observability Mit Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in ServiceNow Cloud Observability Plattform. Laden Sie herunter Ereignismanagement Connector-Plugin aus dem ServiceNow Store Damit Sie in integrieren können ServiceNow Cloud Observability.

Vorbereitungen

- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Authentifizieren ServiceNow Cloud Observability Als zu aktivierende Datenquelle Ereignismanagement Dient zum Sammeln von Ereignissen aus ServiceNow Cloud Observability. In Ihrem ServiceNow Cloud Observability Plattform verwenden Sie einen Standard-Webhook, um Ihren festzulegen ServiceNow AI Platform Instanz als Rest-Endpunkt.

Prozedur

1. Erstellen Sie ein CI.

> **Hinweis:** Discovery für ServiceNow Cloud Observability Services werden nicht unterstützt. Erstellen Sie ein CI manuell in einem ServiceNow Instanz (Tabelle cmdb_ci_Service_Auto) zum Aktivieren der Bindung.

a. Navigieren zu **Alle** > **Konfiguration** > **Anwendungsservice**an.

b. Wählen Sie **Neu**.

c. Geben Sie im Formular den Namen ein.
Der Name muss der in angegebene Servicename sein ServiceNow Cloud Observability Plattform.

d. Legen Sie in der Liste „Betriebsstatus“ den Betriebsstatus auf fest **Betriebsbereit** .

e. Wählen Sie **Weiter**.

f. Wählen Sie **Fertig**.

2. In Ihrem ServiceNow Cloud Observability Plattform: Erstellen Sie ein Benachrichtigungsziel.

a. Klicken Sie in der Navigationsleiste auf **Warnungen** .

b. Wählen Sie aus **Benachrichtigungsziele** #Registerkarte.

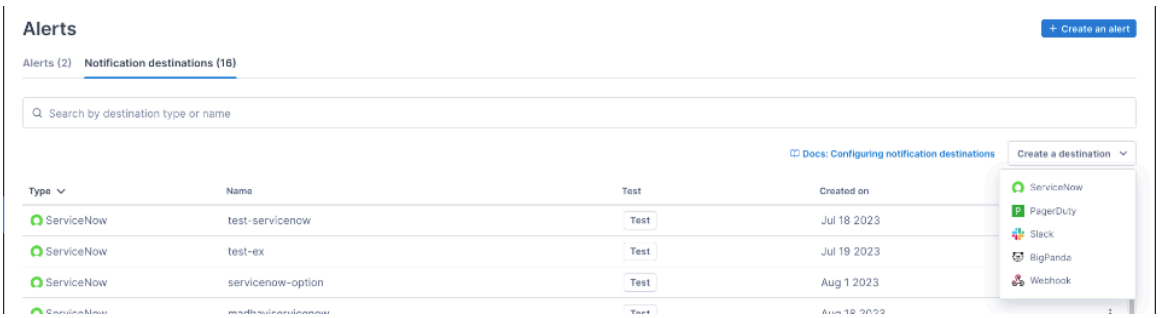
c. Wählen Sie Aus **Erstellen Sie ein Ziel** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie Aus **Webhook** .

Wählen Sie Webhook Aus



e. Geben Sie im Feld Name einen Namen für ein Webhook .

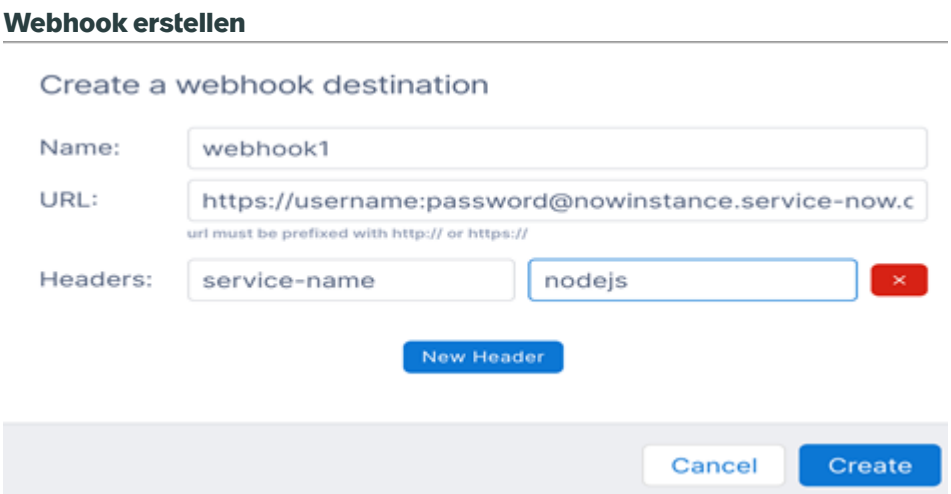
f. Geben Sie im Feld „URL“ die Webhook-URL an.
Dies ist das Standardformat#der URL, von der Ereignisse übertragen werden sollenServiceNow Cloud Observability Zu ServiceNow AI Platform Instanz. Dieses Format verwenden: `https//<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=lightstep`

g. Wählen Sie Aus **Neuer Header** .

h. Geben Sie im Feld Header den ein **Servicename** Und definieren Sie es **Wert** .

Hinweis: In einem ServiceNow Instanz, CI-Bindung erfolgt nur, wenn **Servicename** Der Headerwert stimmt mit den Namensfeldern des CI überein, das Sie in erstellt haben **Tabelle „cmdb_ci_Service_Auto“** .

Webhook erstellen



i. Klicken Sie auf **Erstellen**.

3. In ServiceNow Cloud Observability Plattform, konfigurieren Sie eine Warnung.

a. Klicken Sie in der Navigationsleiste auf **Warnungen** .

b. Wählen Sie Aus **Erstellen Sie eine Warnung** Und geben Sie einen Warnungsnamen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Definieren Sie im Bereich „Warnmeldungskonfiguration“ den Schwellenwert.

d. Wählen Sie im Bereich Benachrichtigungsregeln in den Feldern Benachrichtigungen senden an das Benachrichtigungsziel aus **Webhook** Und suchen Sie nach dem Zielnamen für den Webhook, den Sie in Schritt 2 erstellt haben.

e. Wählen Sie **Speichern**.
Der Standard-Schweregrad für Stream-basierte Warnungen ist **Kritisch**. Sie können den Standard im#Bereich Push-Connector-Konfiguration eines ändernServiceNow AI Platform Instanz. Die gültigen Schweregradwerte sind:

- 1 - Kritisch
- 2 - Schwer
- 3 – Gering
- 4 – Warnung
- 5 - Info

MID-Server zur Event-Erfassung mithilfe eines Push-Vorgangs (Listener) konfigurieren

Der MID-Server unterstützt die Erfassung von Event-Nachrichten mithilfe des MID-Webservers, der Daten aus externen Quellen erfasst und in das für Event-Felder in der Event-Tabelle [em_event] erforderliche Format umwandelt (analysiert). Die transformierten Events werden dann an die Instanz übertragen.

Vorbereitungen
Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Dank der MID-Webservererweiterung können externe Clients Metrikdaten per Push an den MID-Server übertragen. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren. Verwenden Sie den MID WebService-Event-Sammler, um mit einer URL-Methode Event-Nachrichten an den MID-Server zu übertragen. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Konfigurieren Sie einen MID-Server entweder mit *`EventManagement`* oder *`All`* in der Liste der unterstützten Anwendungen.

Um die Unterbrechung von Services zu vermeiden, können Sie ein MID-Server-Failover-Cluster konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**an.
2. Doppelklicken Sie auf den MID-Server, den Sie konfigurieren möchten, oder klicken Sie auf **Neu**, um einen neuen MID-Server zu erstellen.
3. Klicken Sie im Abschnitt **Unterstützte Anwendungen** auf **Bearbeiten**.
   a. Klicken Sie auf **Bearbeiten**.
   b. Wählen Sie im Slushbucket entweder **Event Management** oder **ALLE** aus, und klicken Sie auf die Schaltfläche **>** Hinzufügen.
   c. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um sicherzustellen, dass MID-Server Ist validiert, wählen Sie unter zugehörige Links die Option aus **Validieren** .
   Weitere Informationen finden Sie unter Validiert einen MID-Server .
5. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Konfigurieren Sie den MID WebService-Event-Sammler, um mit einer URL-Methode Event-Nachrichten an den MID-Server zu übertragen. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Zugehörige Informationen

Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren

MID-Webserver erweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

Ereignisse werden an übertragen MID-Server Webservice-API wird verwendet

Konfigurieren Sie den MID WebService-Eventsammler, damit eine URL-Methode Event-Nachrichten an den MID-Server übertragen kann.

Der MID WebService-Event-Sammler ermöglicht Ihnen standardmäßig das Herstellen einer Verbindung zu einem Event-Generator und das Senden von Event-Nachrichten über den MID-Server mithilfe einer URL im folgenden Format: http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2.

Das JSON v2-Format ist mit dem Format identisch, das Clients zum Senden von Event-Nachrichten an die Instanz verwenden. Diese URL bietet eine gute Leistung.

Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Hinweis: Ereignismanagement akzeptiert Events in der Zeitzone des MID-Server, über den der Listener die Event-Nachricht gesendet hat. Wenn Sie eine andere Zeitzone benötigen, können Sie das Skript nach Bedarf konfigurieren, siehe Integration mit Push-Connectors.

URL zum Verschieben von benutzerdefinierten Nutzlasten

Der MID-Server kann auch eine benutzerdefinierte Nutzlast im JSON-, XML- oder Nur-Text-Format empfangen. In diesem Fall transformiert der MID-Server die Event-Nachrichten mithilfe der von Ihnen angegebenen Skripteinbindung und sendet die Events dann an die Instanz. Die URL lautet in diesem Fall:

`http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Transform_script_name}` Für ein Beispiel für eine Skripteinbindung siehe die Standard-Skripteinbindung `TransformEvents_xmlSample`.

Ein Beispiel für die Umwandlung von JSON-formatierten Event-Nachrichten durch den MID WebService-Eventsammler finden Sie unter Ereignissammlung von BMC TrueSight und BMC TrueSight_v2.

Zum Senden von Events im allgemeinen JSON-Format können Sie die URL in folgendem Format verwenden:

`http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform=TransformEvents_MidJsonGeneric`

In diesem Fall transformiert die MID-Einbindung `TransformEvents_MidJsonGeneric`, die in der Basisinstanz bereitgestellt wird, die Event-Nachrichten in die Event-Felder. Alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder werden als Felder **Zusätzliche Informationen** dem generierten ServiceNow-Event hinzugefügt.

Hinweis: Die URL im Format http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name} wird ebenfalls unterstützt.

Die URL der REST API zum Überprüfen der Konnektivität lautet: http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/ping.

Skripteinbindung zur Transformation erfasster Events

Verwenden Sie die erforderliche Skripteinbindung MID-Server, um erfasste Event-Nachrichten umzuwandeln (zu analysieren) und in das zugeordnete Event-Feld einzufügen. Der Name der Skripteinbindung MID-Server besteht aus einem Präfix und einem Suffix. Das Präfix ist der obligatorische Text TransformEvents_ und das Suffix ist der Transformationsname in der URL, z. B. http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/xmlSample . Der Name des zusammengesetzten Skripts lautet daher TransformEvents_xmlSample.

Sie müssen eine Skripteinbindung angeben, die die Event-Nachrichten in einer Textvariablen empfängt. Das Skript muss über eine transform ()-Funktion verfügen, die die Transformation durchführt und das Rückgabe-Array von Event-Objekten vorbereitet. Wenn das Ereignismanagement-Plugin aktiviert ist, erhalten Sie das TransformEvents_xmlSample-Beispielskript, das Events aus dem XML-Format umwandelt.

Hinweis: Event-Felder, die nicht mit Feldern in der Event-Tabelle identisch sind, werden im Feld **Zusätzliche Informationen** gespeichert.

Event-Nachrichtenheader

Geben Sie den entsprechenden Anforderungsheaderwert für das Feld **Inhaltstyp** entsprechend dem Format der Event-Nachricht an.

Header-Werte für den Content-Type anfordern

Nachrichtenformat	Content-Typenwert
JSON	Anwendung/JSON
XML	application/xml
text	text/plain

Authentifizierungs- und Datensicherheitsoptionen

Optionen für Authentifizierung und Datensicherheit:

- **Authentifizierungstyp** , Die auf entweder festgelegt werden kann API-Schlüssel , MTLs , Oder Standard .
- Mit **Sichere Verbindung** können Sie auswählen, ob eingehende und ausgehende Daten bei der Übertragung gesichert werden. Wenn Sie die Option für erweiterte Sicherheit auswählen, müssen Sie ein Zertifikat von einer bekannten Zertifizierungsstelle abrufen und dann den **Schlüsselspeicher-Zertifikat-Alias** und das **Schlüsselspeicher-Passwort** angeben.
- **Einheitlichen MID-Schlüsselspeicher verwenden**: Diese Option bietet Verschlüsselungsschutz und ermöglicht es Ihnen, ein benutzerdefiniertes Zertifikat im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einheitlichen MID-Server-Schlüsselspeicher zu installieren. Weitere Informationen finden Sie unter Installieren Sie anwenderdefinierte Zertifikate im zentralen Schlüsselspeicher DES MID-Servers .

- Benutzer müssen eine Skripteinbindung angeben, die JSON-, XML- oder Text-formatierte Event-Nachrichten in einer Textvariablen empfängt. Das Skript muss über eine transform ()-Funktion verfügen, die die Transformation durchführt und das Rückgabe-Array von Event-Objekten vorbereitet. Die Skripteinbindung TransformEvents_xmlSample, die Events aus dem XML-Format umwandelt, wird als Beispiel angegeben, wenn das Ereignismanagement-Plugin aktiviert ist.

Weitere Informationen zu Authentifizierung und Datensicherheit finden Sie unter MID-Webserver erweiterung konfigurieren.

Zugehörige Informationen

Ereignisse werden mithilfe der Webservice-API an die Instanz übertragen

Ereignisse werden mithilfe der Webservice-API an die Instanz übertragen

Sie können eine Webservice-Schnittstelle mit ServiceNow verwenden, die auf dem JSON-Objekt als Dateneingabe- und -ausgabeformat aufbaut.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie diese Webservice-API, um Datensätze mit einem einzelnen Aufruf in die Event-Tabelle [em_event] einzufügen:
https://<instancename>.service-now.com/api/global/em/jsonv2

Hinweis: Business Rules in der Event-Tabelle werden nicht aufgerufen, wenn diese URL verwendet wird.

Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen. Zusätzliche Felder sollten im Feld **Zusätzliche Informationen** [additional_info] des Events eingeschlossen werden. Weitere Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Die URL im folgenden Format: http://<instancename>.service-now.com/em_event.do?JSONv2&sysparm_action=insertMultiple Wird auch unterstützt, wenn Sie Business-Regeln aktivieren möchten. Die Leistung der ersten URL ist jedoch überlegen.

Um mit der URL zu arbeiten, die auf = insertMultiple endet, fügen Sie dem MID Server die folgenden Eigenschaften mit ihren entsprechenden Werten hinzu:

- „mid.probe.event.queue.compress“ – Wert: false
- „mid.probe.event.bulk_size“ – Wert: 100
- „mid.probe.event.endpoint.url“ – Wert: em_event.do?JSONv2%26sysparm_action=insertMultiple

Prozedur

1. Senden Sie die Anforderung mit diesen Headern:

Parameter	Typ	Beschreibung
Akzeptieren	Zeichenfolge	Der zulässige Typ für diese Nachricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Typ	Beschreibung
		Der Standardwert ist `application/json`.
Content-Type	Zeichenfolge	Der Inhaltstyp für diese Nachricht. Der Standardwert ist `application/json`.
POST	Zeichenfolge	Der Anforderungstyp ist POST mit mindestens einem nachstehenden Datensatz.

2. Mindestens ein Event im JSON-Format kann als Nutzlast des Webservice-Aufrufs gesendet werden. Folgende Event-Felder müssen ausgefüllt werden:

Variable	Beschreibung
Quelle	Der Name des Event-Quelltyps. Beispielsweise SCOM oder SolarWinds.
event_class	Spezifische Instanz der *source*. Beispiel: `SCOM 2012 am 10.20.30.40`
node	Das **Knotenfeld** muss einen Bezeichner für den Host (Server/Switch/Router usw.) enthalten, für den das Event ausgelöst wurde. Der Wert des **Knotenfelds** kann einer der folgenden Bezeichner des Hosts sein: ○ Name ○ FQDN ○ IP ○ Mac-Adresse Wenn in der CMDB vorhanden, wird dieser Wert auch verwendet, um das Event an das entsprechende ServiceNow-CI zu binden.
resource	Wenn sich das Event auf ein Gerät bezieht, z. B. Datenträger, CPU oder Netzwerkadapter, oder auf eine Anwendung oder einen Service, die bzw. der auf einem Host ausgeführt wird, muss der Name des Geräts oder der Anwendung in dieses Feld eingetragen werden. Zum Beispiel: `Disk C:\` oder `Nic 001` oder `Webanwendung Handel`.
metric_name	Name der Metrik, die die Warnung ausgelöst hat. Zum Beispiel: `Verwendeter Arbeitsspeicher` oder `Gesamte CPU-Auslastung`.
type	Der Typ des Events: Dieser Typ ähnelt möglicherweise dem Feld **metric_name**, wird jedoch für die allgemeine Gruppierung von Event-Typen verwendet.
message_key	Dieser Wert wird für die Deduplizierung von Events verwendet. Beispielsweise kann es zwei Events für dasselbe CI geben, wobei ein Event eine CPU von 50 % und das nächste Event eine CPU von 99 % hat. Wenn beide Events derselben ServiceNow-Warnung zugeordnet werden müssen, müssen sie denselben Nachrichtenschlüssel haben. Das Feld kann leer gelassen werden. In diesem Fall lautet der Feldwert standardmäßig `source +node+type+resource+metric_name` . Das Feld **message_key** darf nur ausgefüllt werden, wenn ein besserer Bezeichner als der Standardwert vorhanden ist.
severity	Der Schweregrad des Events. ServiceNow-Werte für den Schweregrad reichen von 1 – Kritisch bis 5 – OK, mit dem Schweregrad 0 – Löschen. Ursprüngliche Schweregradwerte sollten als Teil der zusätzlichen Informationen gesendet werden.
additional_info	Dieses Feld hat das JSON-Schlüssel-/Wert-Format und soll alle Informationen enthalten, die für den Anwender von Nutzen sein könnten. Es wird keinem vordefinierten ServiceNow-Event-Feld zugeordnet. Beispiele: IDs von Objekten in der Event-Quelle,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
	Event-Priorität (wenn nicht gleich Schweregrad), Zuweisungsgruppeninformationen usw. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Format normalisiert, wenn das Event verarbeitet wird.
time_of_event	Zeit, zu der das Event am Event-Ursprung aufgetreten ist. Das Format lautet: jjjj-MM-tt HH:mm:ss. Die angegebene Zeit muss GMT entsprechen.
resolution_state	Optional – Um anzugeben, dass ein Event gelöst wurde oder nicht mehr auftritt, verwenden einige Event-Überwachungen den Schweregrad „löschen“, während andere Event-Überwachungen einen Wert für den Schweregrad „schließen“ verwenden. Dieses Feld wird für die Monitore verwendet, die Letzteres anbieten. Gültige Werte sind Neu und Schließen.

3. Zum Erstellen mehrerer Datensätze mit einem einzigen Aufruf lösen Sie den Event-Webservice mit der folgenden URL aus, wobei die Variable <instance name> durch den Namen der erforderlichen Instanz ersetzt wird:
https://<instancename>.service-now.com/api/global/em/jsonv2

Example
Beispiel für die Nutzlast von zwei Events, die in einem Webservice-Aufruf gesendet werden:

```
{
 "records": [
  {
   "source": "SCOM",
   "event_class": "SCOM 2012 on scom.server.com",
   "resource": "D:",
   "node": "name.of.node.com",
   "metric_name": "Percentage Logical Disk Free Space",
   "type": "Disk space",
   "severity": "4",
   "description": "The disk D: on computer V-W2K8-abc.abc.com is running out of disk
space. The value that exceeded the threshold is 38% free space.",
   "additional_info": {
    "scom-severity": "Medium",
    "metric-value": "38",
    "os_type": "Windows.Server.2008"
   }
  },
  {
   "source": "SCOM",
   "event_class": "SCOM 2012 on scom.server.com",
   "resource": "MSSQL-database-name",
   "node": "other.node.com",
   "metric_name": "DB Allocated Size (MB)",
   "type": "Database Storage",
   "severity": "3",
   "description": "High number of active connections for MSSQL-database-name running on
name.of.node.com. Active connections exceed 5000.",
   "additional_info": {
    "scom-severity": "Medium",
    "metric-value": "38",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "os_type": "Windows.Server.2008"
    }
   }
 ]
}
```

4. Zum Erstellen eines Datensatzes mit einem einzigen Aufruf lösen Sie den Event-Webservice mit der folgenden URL aus, wobei die Variable <instancename> durch den Namen der erforderlichen Instanz ersetzt wird:
`https://<instancename>.service-now.com/api/global/em/jsonv2`

Example

Beispiel für die Nutzlast von einem Event, das in einem Webservice-Aufruf gesendet wird:

```
{
 "records": [
  {
   "source": "SCOM",
   "event_class": "SCOM 2007 on scom.server.com",
   "resource": "C:",
   "node": "name.of.node.com",
   "metric_name": "Percentage Logical Disk Free Space",
   "type": "Disk space",
   "severity": "4",
   "description": "The disk C: on computer V-W2K8-dfg.dfg.com is running out of disk space.
The value that exceeded the threshold is 41% free space.",
   "additional_info": {
    "scom-severity": "Medium",
    "metric-value": "38",
    "os_type": "Windows.Server.2008"
   }
  }
 ]
}
```

Example

Beispiel: Curl-Anforderung:

```
{
 curl -X POST "https://<instancename>.service-now.com/api/global/em/jsonv2" \
 --header "Content-Type: application/json" \
 --user "username:password" \
 --data '{
  "records": [
   {
    "source": "SCOM",
    "event_class": "SCOM 2007 on scom.server.com",
    "resource": "C:",
    "node": "name.of.node.com",
    "metric_name": "Percentage Logical Disk Free Space",
    "type": "Disk space",
    "severity": "4",
    "description": "The disk C: on computer V-W2K8-dfg.dfg.com is running out of disk
space. The value that exceeded the threshold is 41% free space.",
    "additional_info": {
     "scom-severity": "Medium",
     "metric-value": "38",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "os_type": "Windows.Server.2008"
    }
   }
  ]
}'
```

Zugehörige Informationen

Ereignisse werden an übertragen MID-Server Webservice-API wird verwendet

MID-WebService-Event-Sammlerkontext konfigurieren

Konfigurieren Sie den MID-WebService-Event-Sammlerkontext, damit eine URL-Methode Event-Nachrichten von einer externen Quelle an den MID-Server übertragen kann.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Standardformat der URL zum Versenden von Eventnachrichten aus einer externen Quelle an den MID-Server ist `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2`. Diese URL bietet eine gute Leistung.

Aus einer externen Quelle lautet das URL-Format für Push-Event-Nachrichten, die nicht im jsonv2-Format vorliegen: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Name_of_Transform_Script}`, wobei die Variable *`{Name_of_Transform_Script}`* der vollständige Name des Skripts ist und immer mit dem Text: `TransformEvents_` beginnt.

Nehmen Sie beispielsweise die folgenden Werte an:

- {MID_Server_IP}: 10.118.69.27
- {MID_Web_Server_Port}: 8097
- Name des Transformationsskripts: EventsToProcess

Die zu verwendende URL lautet daher: `http://10.118.69.27:8097/api/mid/em/inbound_event/TransformEvents_EventsToProcess`

Hinweis:

- Die URL im Format `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name}` wird ebenfalls unterstützt.
- Das Datumsformat für Events ist jjjj-Md h:mm:ss.

  Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, müssen Sie ein `{transform_script_name}` verwenden, das für das Datumsformat des eingehenden Events geeignet ist. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

  Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *`2019/06/27/ 11:25:00 a`* ankommt, verwenden Sie ein `{transform_script_name}` mit dem Datumsformat *`yyyy/MM/dd/ HH:mm:ss a`*, damit es dem Format des empfangenen Events entspricht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **MID-WebService-Ereignis-Listener**an.
2. Klicken Sie in der Liste MID WebService Event-Sammlerkontexte auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular für MID WebService-Event-Sammlerkontext

Feld	Beschreibung
Name	Ein eindeutiger Name für diesen Sammler zur einfachen Identifizierung.
Kurzbeschreibung	Geben Sie eine kurze, aussagekräftige Beschreibung dieses Sammlers ein.
MID-Webservererweiterung	Angeben und dann die MID-Webserver-Erweiterung starten. Die unterstützten Authentifizierungsmethoden werden im Feld **Authentifizierungstyp** der MID-Webserver-Erweiterung aufgeführt. Informationen zum Konfigurieren einer MID-Webserver-Erweiterung finden Sie unter MID-Webserver konfigurieren.
Status	Dieses Feld wird automatisch mit dem Status der MID-Webserver-Erweiterung ausgefüllt. Dieses Feld ist leer, bis die MID-Webserver-Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die MID-Webserver-Erweiterung wird einer der folgenden Werte angezeigt: ○ **Gestartet**: Der Sammler läuft. ○ **Angehalten**: Der Sammler läuft nicht. ○ **Offline**: Der MID-Server ist nicht erreichbar. ○ **Fehler**: Der Sammler ist mit einem Fehler fehlgeschlagen (die Fehlermeldung wird im Feld **Fehlermeldung**angezeigt). ○ **Warnung**: Eine Laufzeitausnahme ist aufgetreten.
Ausführen auf	**Bestimmter MID-Server** Oder **Spezifischer MID-Server-Cluster** , Wie in der angegebenen MID-Webservererweiterung definiert.
MID-Server	Der **spezifische MID Server** oder **spezifische MID Servercluster**, wie in der angegebenen MID-Webserver-Erweiterung definiert.
Ausführung auf	Der Name des MID-Server, auf dem die MID-Webserver-Erweiterung ausgeführt wird.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
5. Klicken Sie unter **Zugehörige Links** auf **Starten**, um den Sammler zu starten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehle im Kontextformular Ereignismanagement

Zugehöriger Link	Beschreibung
Starten	Startet den Sammler, falls er nicht läuft. Diese Aktion überprüft, ob ein Webservice-API-Endpunkt mit der Ereignismanagement-Anwendung auf MID-Server ausgeführt wird.
Stoppen	Hält den laufenden Sammler auf dem konfigurierten MID-Server an. Wenn der Sammler nicht ausgeführt wird, wird keine Aktion ausgeführt.
Neu starten	Stoppt und startet den Sammler auf dem konfigurierten MID-Server.
Parameter aktualisieren	Sendet aktualisierte Parameter an den Sammler. Parameter werden auch aktualisiert, wenn die Kontexterweiterung Ereignismanagement MID-Server aktualisiert wird. Wenn Sie auf dieses Steuerelement klicken, während der Sammler nicht ausgeführt wird, wird keine Aktualisierung vorgenommen.

Example:
Zeigt die Verwendung der URL zum Umwandeln von JSON v2-formatierten Event-Nachrichten an

Angenommen, Event-Nachrichten im JSON v2-Format werden an MID-Server gesendet. Bei Verwendung der `jsonv2-` URL ist keine Skripteinbindung erforderlich.

Daten für das JSON v2-Beispiel

Feld	Wert
MID_Server_IP	10.218.64.27
MID_Web_Server_Extension_Port	8097
Event-Nachrichtenformat	jsonv2

Ersetzen Sie die Variablen im Standardformat der URL `http://<my-instance>.service-now.com/api/global/em/jsonv2` mit Werten aus der vorherigen Tabelle: `http://10.218.64.27:8097/api/global/em/jsonv2`

Beispiel für die URL für Push-Nachrichten, die nicht im jsonv2-Format vorliegen

Das URL-Format für Push-Event-Nachrichten aus einer externen Quelle, die nicht im jsonv2-Format vorliegen, lautet: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Name_of_Transform_Script}`, wobei die Variable {Name_of_Transform_Script} der vollständige Name des Skripts ist und immer mit dem Text: TransformEvents_ beginnt. Der Skriptname muss als Header-Parameter `Transform` angegeben werden und muss immer mit dem Präfix `TransformEvents_` beginnen.

Nehmen Sie in diesem Beispiel an, dass der Skriptname EventsToProcess lautet. Die URL lautet daher:`http://10.138.64.27:8097/api/mid/em/inbound_event/TransformEvents_EventsToProcess`

Beispiel für Event-Nachrichten im JSON v2-Format

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

```
curl -v -H "Accept: application/json" -H "Content-Type: application/json" -X POST --data "{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "records":
  [ {
      \"source\" : \"Simulated\",
     \"node\" : \"nameofnode\",
     \"type\" : \"High Virtual Memory\",
     \"resource\" : \"C:\",
     \"severity\" : \"5\",
     \"description\" : \"Virtual memory usage exceeds 98%\",
     \"ci_type\":\"cmdb_ci_app_server_tomcat\",
     \"additional_info\":\"{\\\"name\\\":\\\"My Airlines\\\"}\"
    },
    {
    \"source\" : \"Simulated\",
    \"node\" : \"01.myairlines.com\",
    \"type\" : \"High CPU Utilization\",
    \"resource\" : \"D:\",
    \"severity\" : \"5\",
    \"description\" : \"CPU on 01.my.com at 60%\"
    }
  ]
}" -u UserName:Password http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2
```

Example:
Beispiel mit JSON v2-formatierten Ereignisnachrichten mit MID-Webserver-API-Schlüssel

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

```
curl --location -g --request POST
 'http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: key <mid_webserver_api_key>' \
--data-raw '{
  "records":
  [ {
      \"source\" : \"Simulated\",
     \"node\" : \"nameofnode\",
     \"type\" : \"High Virtual Memory\",
     \"resource\" : \"C:\",
     \"severity\" : \"5\",
     \"description\" : \"Virtual memory usage exceeds 98%\",
     \"ci_type\":\"cmdb_ci_app_server_tomcat\",
     \"additional_info\":\"{\\\"name\\\":\\\"My Airlines\\\"}\"
    },
    {
    \"source\" : \"Simulated\",
    \"node\" : \"01.myairlines.com\",
    \"type\" : \"High CPU Utilization\",
    \"resource\" : \"D:\",
    \"severity\" : \"5\",
    \"description\" : \"CPU on 01.my.com at 60%\"
    }
  ]
}'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

MID-Webserver erweiterung konfigurieren

Event-Erfassung von BMC TrueSight

Event-Erfassung aus Microsoft Azure Monitor

Event-Erfassung aus Google Cloud Platform

Event-Erfassung aus benutzerdefinierten Nutzlasten

Mit dem MID WebService-Eventsammler können Sie Event-Informationen aus benutzerdefinierten Nutzlasten im JSON-, XML- oder Nur-Text-Format erfassen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Der MID-Server transformiert die erfassten Event-Nachrichten und füllt die Event-Tabellenfelder (em_table) in der Instanz aus. Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung. Weitere Informationen zu unterstützten Authentifizierungsmethoden finden Sie unter MID-Webserver erweiterung konfigurieren.

Das Format der erforderlichen MID-Server-URL ist: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Transform_script_name}`. Der Name der MID-Server-Skripteinbindung setzt sich aus dem Anfügen eines Suffixes an das Standardpräfix `TransformEvents_` zusammen. Informationen zur Erfassung von JSON v2-Event-Nachrichten finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Hinweis: Die URL im Format `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name}` wird ebenfalls unterstützt.

Prozedur

1. Konfigurieren Sie den MID-WebService-Eventsammler, siehe MID-WebService-Event-Sammlerkontext konfigurieren.
2. Starten Sie den MID-WebService-Eventsammler.

Example:

Transformation von XML-formatierten Event-Nachrichten mithilfe der benutzerdefinierten Nutzlast-URL

Angenommen, Event-Nachrichten im XML-Format werden an MID-Server gesendet. Verwenden Sie dieses Beispiel, um ein Array von Event-Objekten aus den erfassten Event-Nachrichten zurückzugeben. Der Name der MID-Server-Skripteinbindung setzt sich aus dem Anfügen eines Suffixes an das Standardpräfix `TransformEvents_` zusammen. Für die Zwecke dieses Beispiels hat der Benutzer die xmlSample-Skripteinbindung angegeben. Anhand dieser Details lautet der Name der MID-Server-Skripteinbindung `TransformEvents_xmlSample`. Der MID-Server wandelt die erfassten Event-Nachrichten um, indem er die Nachrichten mit der Skripteinbindung analysiert und dann an die Instanz übermittelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten für das XML-Beispiel

Feld	Wert
MID_Server_IP	10.218.64.27
MID_Web_Server_Extension_Port	8097
transform_script_suffix_name	xmlSample

Ersetzen Sie die Variablen in der URL durch die Werte aus der obigen Tabelle:
http://10.218.64.27:8097/api/mid/em/xmlSample

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

Beispiel für Event-Nachrichten im XML-Format:

```
<records>
  <event>
  <source>My Source</source>
  <node>host1</node>
  <type>type1</type>
  <severity>3</severity>
  <description>Virtual memory usage exceeds 98%</description>
  </event>
  <event>
  <source>My Source</source>
  <node>host2</node>
  <type>type2</type>
  <severity>2</severity>
  <description>Virtual memory usage exceeds 90%</description>
  </event>
  </records>
```

Zugehörige Informationen

MID-Webserver erweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

Integration mit Push-Connectors

Integrieren Sie einen Push-Connector, um eine Verbindung zu einer externen Ereignisquelle herzustellen. Push-Connectors verarbeiten die gesammelten Event-Nachrichten und transformieren sie in das erforderliche Event-Format.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Ereignismanagement Connectors“ (sn_em_connector) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Beim Upgrade einer ServiceNow AI Platform-Instanz von Paris oder früher können Sie veraltete Listener-Transformationsskripts verwenden. Weitere Informationen finden Sie unter Veraltete Listener-Transformationsskripts verwenden.

Warum und wann dieser Vorgang ausgeführt wird

Die Push-Connectors akzeptieren Event-Nachrichten, die von externen Event-Quellen generiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen Connector für die Überwachung einer externen Event-Quelle. Verwenden Sie einen benutzerdefinierten Push-Connector, um die Event-Nachrichten entweder über den MID-Server oder die Instanz zu senden.

Hinweis: Sie können die folgende generische JSON-Ziel-URL zum Erfassen von Events verwenden: `https:/<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source=genericJson`. Diese URL kann unverändert verwendet werden und erfordert die Konfiguration einer Event-Regel.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**an.
2. Klicken Sie auf **Neu**, oder klicken Sie auf den Push-Connector, den Sie ändern möchten, z. B. AWS oder Azure.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Eindeutiger Name für diesen Push-Connector zur einfachen Identifizierung
Beschreibung	Geben Sie eine Beschreibung für die Verwendung des Push-Connectors ein.
Header-Name	Geben Sie den Header-Namen an, für den der Wert festgelegt werden soll, z. B. Set-Header.
Header-Wert	Der Header-Wert, für den der Wert festgelegt werden soll, z. B. Set-Header.
Typ	Wählen Sie diese Option aus, um Events entweder an die Instanz oder über den MIDzu senden. Verwenden Sie jeweils die URL des ausgewählten Typs. Weitere Informationen finden Sie in der Beschreibung des Felds **URL-Parameterwert**.
Aktiv	Aktivieren, um das Abrufen von Events aus dieser externen Event-Quelle zu aktivieren.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
URL-Parameterwert	○ Senden Sie Events an die Instanz. Verwenden Sie die URL im folgenden Format für alle Connectors:`https://<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source={URL_parameter_value}`. ○ Senden Sie Events über den MID-Server. Verwenden Sie die URL in diesem Format:`http://{MID_Server_IP}:{MID_Web_Server_Port}/`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	api/mid/em/inbound_event?Transform={Transform_script} **Hinweis:** Das Senden von Events an den MID-Server erfordert die vorherige Konfiguration der Erweiterung für MID-WebService-Event-Listener.

4. Im Abschnitt Skript:
   - Wenn der für das Feld **Typ** ausgewählte Wert MID ist, wird das Feld **Umwandlungsskript** angezeigt. In diesem Feld geben Sie den Namen der MID-Skripteinbindung an, die Event-Nachrichten akzeptiert, die von der erforderlichen externen Event-Quelle generiert werden und die das Skript im erforderlichen Event-Format analysiert, oder suchen Sie nach diesem Namen. Verwenden Sie diese Namenskonvention für das Skript: TransformEvents_<your source>
   - Wenn der für das Feld **Typ** ausgewählte Wert **Instanz** ist, wird der **Skript**-Editor angezeigt. Im **Skript**-Editor geben Sie das benutzerdefinierte Skript an, das Event-Nachrichten akzeptiert, die von der erforderlichen externen Event-Quelle generiert werden und die das Skript im erforderlichen Event-Format analysiert.

Example

Dieses Beispiel zeigt, wie die transformierten Felder einem Event-Formular hinzugefügt werden.

```
(function process(/*RESTAPIRequest*/ request, body) {
 /*Function that receives a JSON object, adding all its fields to the Additional information
 object. The field name is a concatenation of the field key and the parent field key if it
 exists.*/
 function updateAdditionalInfo(event, field,jsonObject,additionalInfo) {
       for (var key in jsonObject) {
          var newKey = key;
          if (field != "") {
             newKey = field + '_' + key;
          }
  // You can do some transformation here and set fields on the event
  //if(key == "MySource")
  //   event.source = jsonObject[key];
          additionalInfo[newKey] = jsonObject[key];
       }
  }

   try
{
       gs.info("TransformEvents_generic received body:" + body);
 var jsonObject = JSON.parse(body);
       var event = new GlideRecord('em_event');
 event.source = "GenericJson"; //TODO: Need to define
       event.event_class = "GenericJsonClass"; //TODO: Need to define
       event.severity = "5";

       var additionalInfo = {};
       updateAdditionalInfo(event, "",jsonObject,additionalInfo);
 /*Iterates over Additional information JSON object and adds all nested objects' fields as
fields of the Additional information object*/
       var notDone = true;
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      while (notDone) {
         notDone = false;
         for (var key in additionalInfo) {
            if (Object.prototype.toString.call(additionalInfo[key]) == '[object Object]') {
               notDone = true;
               updateAdditionalInfo(event, key,additionalInfo[key],additionalInfo);
   additionalInfo[key] = "";
            }
         }
      }
 gs.info("TransformEvents_generic generated additional information:" +
JSON.stringify(additionalInfo));
      event.additional_info = JSON.stringify(additionalInfo);
      event.insert();
}
 catch(er){
  gs.error(er);
  status=500;
  return er;
}
 return "success";
})(request, body);
```

Veraltete Listener-Transformationsskripts verwenden

Verwenden Sie veraltete Listener-Transformationsskripts, wenn Sie eine ServiceNow AI Platform-Instanz von Paris oder früher aktualisieren. Diese Skripts können als Teil vorhandener integrierter Systeme oder gemeinsam mit Ereignismanagement-Push-Connectors ausgeführt werden.

Sie können Listener-Transformationsskripts verwenden, um sicherzustellen, dass vorherige Integrationen unterstützt werden. Wenn Sie beispielsweise den Endpunkt https:/<instance-name>.service-now.com/api/global/em/inbound_event in verschiedenen Integrationen verwenden, können Sie diesen Endpunkt in einer Quebec- oder einer späteren ServiceNow AI Platform-Instanz weiterverwenden.

Wenn Sie verwenden möchten Ereignismanagement Push-Connectors, Laden Sie das Plugin aus dem herunter ServiceNow Store Website. Sie können dann auf die Push-Connectors in der ServiceNow AI Platform-Instanz zugreifen, und der Endpunkt https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event wird ebenfalls erstellt.

Veralteten Endpunkte mit Push-Connectors verwenden

Sie können den Endpunkt https:/<instance-name>.service-now.com/api/global/em/inbound_event mit den Push-Connectors weiterverwenden, indem Sie die entsprechenden Transformationsskripts deaktivieren. Um ein Skript zu deaktivieren, navigieren Sie zu **Ereignismanagement** > **Integrationen** > **Listener-Transformationsskripts**an. Klicken Sie dann in der angezeigten Liste auf das entsprechende Skript, und deaktivieren Sie das Kontrollkästchen **Aktiv** im Formular.

Veralteten Endpunkt verwenden und alle Listener-Transformationsskripts deaktivieren

Sie können auch den Endpunkt https:/<instance-name>.service-now.com/api/global/em/inbound_event weiterverwenden, müssen dazu aber Sie die Listener-Transformationsskripts deaktivieren, damit stattdessen die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Connectors verwendet werden. Um alle Skripts zu deaktivieren, navigieren Sie zu **Systemeigenschaften** > **Alle Eigenschaften**, Suchen Sie nach *sn_em_connector_listener_table_for_InboundEvent*Und legen Sie ihren Wert auf fest **Wahr** .

Anwenderdefinierte Listener-Transformationsskripts zum Push-Connectors-Modul migrieren

Falls Sie benutzerdefinierte Listener-Transformationsskripts erstellt haben, müssen diese zum Push-Connectors-Modul migriert werden, wenn Sie den neuen Endpunkt https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event verwenden möchten. Um das anwenderdefinierte Skript zu migrieren, navigieren Sie zu **Ereignismanagement** > **Integrationen** > **Listener-Transformationsskripts**, Klicken Sie auf das entsprechende Listener-Transformationsskript, und wählen Sie das angezeigte Skript aus. Navigieren Sie dann zu **Integrationen** > **Push-Connectors**, Klicken Sie auf **Neu** , Und fügen Sie das Skript ein, das Sie aus dem Listener-Transformationsskript kopiert haben.

AWS-Plattform als Datenquelle integrieren

Integrieren Sie Amazon Web Services (AWS) mit Ereignismanagement. Um die AWS-Plattform als Datenquelle hinzuzufügen, muss die AWS-Plattform entsprechend konfiguriert werden.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Laden Sie herunter Ereignismanagement Plugin „Connectors“ aus dem ServiceNow Store.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine AWS-Plattformwarnung eingeht, führt Ereignismanagement Folgendes aus:

- Extrahiert Informationen aus der ursprünglichen AWS-Plattformwarnung, um erforderliche Event-Felder auszufüllen, und fügt das Event in die Datenbank ein.
- Erfasst den Inhalt im Feld **additional_info**.

Die AWS Plattform-Push-Connector befindet sich in **Ereignismanagement** > **Integrationen** > **Push-Connectors**an. Klicken Sie auf der Seite Push-Connectors auf **Push-Connector für AWS-Ereignisse** .

Hinweis: Die AWS Push-Connector, der in den Basissystem-Handles bereitgestellt wird AWS Nur Cloudwatch-Alarme und nicht CloudWatch-Ereignisse, die über Ereignisregeln erstellt wurden. Dient zur Verarbeitung von Simple Notification Service (SNS)-Alarmen, die sich von unterscheiden AWS Cloudwatch, erstellen Sie einen neuen Push-Connector, oder passen Sie an AWS Push-Connector.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In AWS Plattformkonsole, wählen Sie aus **Einfacher Benachrichtigungsservice** .
   Wenn kein SNS-Thema vorhanden ist, erstellen Sie eines.
2. Erstellen Sie unter dem SNS-Thema ein neues Abonnement.

   a. Übernehmen Sie **Thema-ARN** aus dem von Ihnen erstellten Thema.
   Der Amazon-Ressourcenname (ARN) ist für die Bindung einer Ereignismanagement-Warnung an ein CI erforderlich.

   b. Legen Sie **Protokoll** als `https` fest.

   c. In ServiceNow Instanz erstellen Sie einen Anwenderaccount, oder identifizieren Sie einen vorhandenen ServiceNow Anwender für diese Integration.
   Stellen Sie außerdem sicher, dass ServiceNow sys_user die Rolle evt_mgmt_integration zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   d. Festlegen **Endpunkt** An: `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=aws`

   Wenn die Multi-Faktor-Authentifizierung (MFA) der AWS-Plattform aktiviert ist, werden bei der Anmeldung bei der Website der AWS-Plattform Benutzername und Passwort sowie ein Authentifizierungscode vom MFA-Gerät der AWS-Plattform des Benutzers abgefragt.
3. Warten Sie, bis das Abonnement von Ausstehend in Bestätigt geändert wird und die Abonnement-ARN ausgefüllt ist.
   Dies kann ein paar Minuten dauern.
4. Erstellen Sie Alarme in AWS Plattform, an die gesendet werden soll Ereignismanagement Und verknüpfen Sie die Alarme mit dem von Ihnen erstellten SNS-Thema.
   Die Zustellung von Rohnachrichten darf im AWS-Alarm nicht aktiviert sein. Die folgenden Ereignisregeln werden mit dem Basissystem bereitgestellt:

Ereignisregel	Beschreibung
AWS-Hostbindung	Binden AWS Plattformalarme, entweder auf dem Host oder auf der VM, an das Host-Hardware-CI.
AWS – Allgemein	Binden Sie AWS-Plattformalarme auf dem Lastenausgleichsmodul an das CI des Cloud-Lastenausgleichsmoduls, Amazon Relational Database Service (RDS) an das CI der Cloud-Datenbank sowie den Host oder die virtuelle Maschine (VM) an das CI der VM-Instanz. **Hinweis:** Um Events vom Host oder von der virtuellen Maschine an das Instanz-CI der virtuellen Maschine zu binden, deaktivieren Sie die AWS-Hostbindungsregel.

Hinweis: Damit der Push-Connector das eingehende Ereignis verarbeiten kann, müssen Sie einen Anforderungsheader senden **X-amz-sns-message-type** Mit Wert **Benachrichtigung** .

Dieses Beispiel zeigt eine JSON-Zeichenfolge für AWS VM-Bindung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
"Type" : "<type>",
"MessageId" : "<message ID #>",
"TopicArn" : "<topic arn>",
"Subject" : "ALARM: \"<alarm type>\" in <location>",
"Message" : "{\"AlarmName\":\"<alarm name>\",\"AlarmDescription\":<alarm
 description>,\"AWSAccountId\":\"<account ID
 #>\",\"NewStateValue\":\"ALARM\",\"NewStateReason\":\"Threshold Crossed:
 <threshold and datapoint which it crossed>.\",\"StateChangeTime\":\"<date and
 time>\",\"Region\":\"<location>\",\"OldStateValue\":\"OK\",\"Trigger\":{\"MetricName\":
\"CPUUtilization\",\"Namespace\":\"<namespace>\",\"Statistic\":\"<statistic
 name>\",\"Unit\":null,\"Dimensions\":[{\"name\":\"InstanceId\",\"value\":\"<dimension
 value>\"}],\"Period\":<period number>,\"EvaluationPeriods\":<number of evaluation
 periods>,\"ComparisonOperator\":\"GreaterThanOrEqualToThreshold\",
\"Threshold\":<threshold number>}}",
"Timestamp" : "<date and time>",
"SignatureVersion" : "<version number>",
"Signature" : "<signature>",
"SigningCertURL" : "<URL>",
"UnsubscribeURL" : "<URL>"
}
```

5. Damit mehrere Mitgliedsaccounts CloudWatch- oder EventBridge-Ereignisse an einen zentralen Account weiterleiten können, wo sie von einem einzelnen SNS-Thema an den ServiceNow-Ereigniserfassungs-Endpunkt übermittelt werden, müssen Sie die Konfiguration auf AWS-Seite vornehmen. Informationen zum Konfigurieren finden Sie unter https://repost.aws/knowledge-center/cloudwatch-cross-account-sns . Dieses Design vereinfacht die Integration, vermeidet das Duplizieren von SNS-Themen über Accounts hinweg und bietet einen einzigen Einstiegspunkt für alle Überwachungsereignisse, die in fließen ServiceNow.

Zugehörige Informationen

Event-Feldformat für die Event-Erfassung

Integration mit Push-Connectors

Integrieren Sie AWS mit REST API-Schlüssel-Token

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

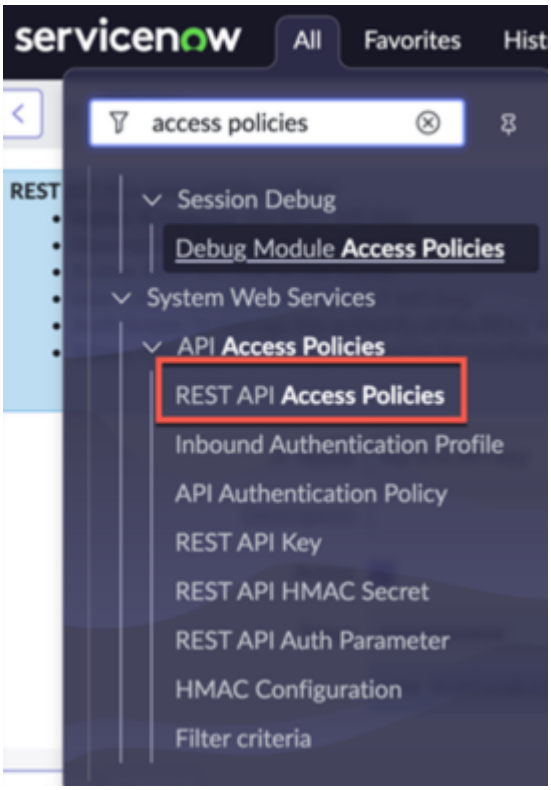
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Hinweis: Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

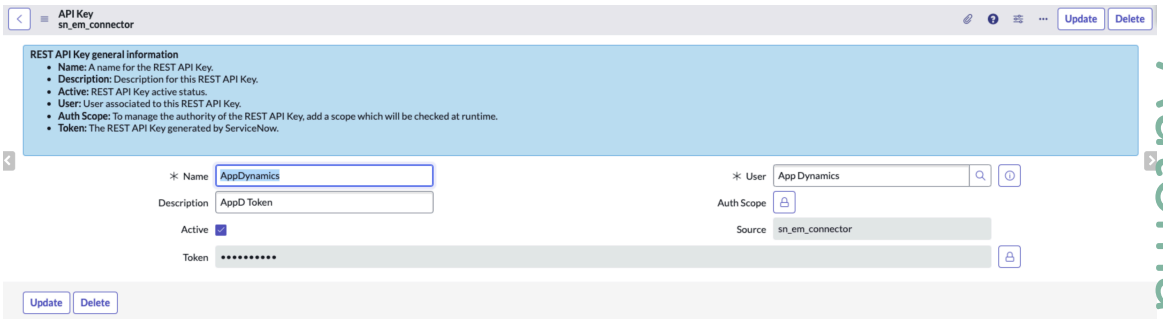
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Azure Monitor als authentifizierte Datenquelle integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure Monitor als authentifizierte Datenquelle hinzufügen.

Sie können die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure Monitor konfigurieren, indem Sie Ihre ServiceNow AI Platform-Instanz als REST-Endpunkt festlegen.

Sobald der Endpunkt konfiguriert ist, wenn Azure Eingehende Warnungsnachricht überwachen, Ereignismanagement:

- Authentifiziert Azure Warnungsnachricht mit dem entsprechenden überwachen ServiceNow Anwender, der die OAuth-Konfiguration oder einen Standard-Webhook verwendet.
- Extrahiert Informationen aus dem Original AzureÜberwachen Sie die Warnungsnachricht, um erforderliche Ereignisfelder auszufüllen und das Ereignis in einzufügen ServiceNow AI Platform Datenbank.
- Erfasst spezifischen Inhalt im Feld **Zusätzliche Informationen** des Event-Formulars

Welche Authentifizierung wird verwendet?

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung wird mit durchgeführt Azure V1- oder V2-Zugriffstoken überwachen. Weitere Informationen finden Sie unter Azure Monitor mit OAuth-Authentifizierung integrieren.
- Standard-Webhook-Authentifizierung: Bietet einen Standardstandard der Authentifizierung, ohne dass dies erforderlich ist Azure Active Directory. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE oder nützlich sein DevOps Teams. Weitere Informationen finden Sie unter Azure Monitor mit Standardauthentifizierung integrieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Was Sie wissen sollten, bevor Sie beginnen

Sie können Ihren integrierten verwenden AzureÜberwachen Sie nur als Datenquelle, nachdem Sie Folgendes überprüft haben:

- Für beide Authentifizierungsmethoden wurde dem relevanten ServiceNow-sys_user die Rolle evt_mgmt_integration zugewiesen.
- In der ServiceNow AI Platform-Instanz wurde das Plugin „Ereignismanagement Connectors“ installiert. Sie können das -Plugin aus herunterladen ServiceNow Store Website.
- Azure Cloud-Discovery Muss ausgeführt werden, um sicherzustellen, dass die erstellten Warnungen an die Konfigurationselemente in gebunden sind ServiceNow AI Platform. Weitere Informationen finden Sie unter Erkennung von Azure-Clouds.

Event-Regeln und Event-Feldzuordnungen

Die folgenden Ereignisregeln und Ereignis-Feldzuordnungen werden mit dem Basissystem bereitgestellt:

Modul	Beschreibung
Ereignisregeln	**Azure Monitor**: Allgemeine Event-Regel zur Verarbeitung aller Azure Monitor-Events.
Event-Feldzuordnungen	**Azure-Monitor - ci_type**: Zum Zuordnen des ci_type von Events basierend auf dem resourceType-Feld. Ein Basissatz von Zuordnungspaaren wird bereitgestellt.

Die folgenden Zuordnungen werden mit dem Basissystem in **Azure Monitor - ci_type** bereitgestellt:

Wertpaare Transformieren

Event Mapping Pairs

Key	Value
microsoft.compute/virtualmachines	cmdb_ci_vm_object
microsoft.documentdb/databaseaccounts	cmdb_ci_cloud_database
microsoft.sql/servers	cmdb_ci_cloud_database
microsoft.web/sites	cmdb_ci_cloud_webserver
microsoft.cache/redis	cmdb_ci_cloud_database
microsoft.documentdb	cmdb_ci_cloud_database
microsoft.sql/servers/databases	cmdb_ci_cloud_database

Hinweis: Sie können der Event-Feldzuordnung - **Azure Monitor - ci_type** je nach Anforderung neue Zuordnungspaare hinzufügen, um Events dem entsprechenden ci_type basierend auf resourceType zuzuordnen.

Beginnend mit Xanadu Release, haben die OOTB-Regeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Schweregradzuordnung von Azure-Schweregrad zu ServiceNow Ereignisschweregrad

Azure-Schweregradbedingung	ServiceNow Ereignisschweregrad
Wenn eine Azure-WarnungsmonitorCondition ausgelöst wird	
Azure Sev0	ServiceNow Kritisch (Schweregrad „1“)
Azure Sev1	ServiceNow Schwerwiegend (Schweregrad „2“)
Azure Sev2 und Sev3	ServiceNow Warnung (Schweregrad „4“)
Azure Sev4	ServiceNow OK (Schweregrad „5“)
Wenn eine Azure-WarnungsmonitorCondition aufgelöst wird	
Beliebiger Azure-Schweregrad	ServiceNow LÖSCHEN (Schweregrad „0“)

Azure Monitor mit Standardauthentifizierung integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure Monitor einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rollen: evt_mgmt_admin und web_service_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure, indem Sie Azure Monitor als Datenquelle authentifizieren. Legen Sie in Ihrem Azure Monitor-Portal Ihre ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Im Azure-Portal werden Warnungskorrelationsregeln über definiert `Correlate alerts`Einstellung in Warnungsverarbeitungsregeln. Wenn `Correlate alerts`Ist im Azure-Portal zugewiesen, die Azure Monitor-Warnungen, die auf empfangen wurden ServiceNow® Instanzen innerhalb von 60 Minuten werden mithilfe von Tag-basiertem Warnungs-Clustering gruppiert.

Prozedur

1. Erstellen Sie in ServiceNow AI Platform ein Benutzerkonto, oder identifizieren Sie einen vorhandenen ServiceNow-Benutzer für diese Integration.
   Stellen Sie außerdem sicher, dass ServiceNow sys_user die Rolle evt_mgmt_integration zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.
2. Aktualisieren Sie in Ihrem Azure Monitor-Portal die Azure Monitor-Warnungsregeln, um eine Aktionsgruppe mit einen Standard-Webhook zu verwenden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Erstellen Sie eine Aktionsgruppe mit `action type=webhook` und geben Sie die URL an, die die Benutzer-ID und das Passwort des ServiceNow-Benutzers im Endpunkt enthält.
Zum Beispiel:

https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=azuremonitor

> **Hinweis:** Wenn Sie mehrere Mandanten im Azure-Portal haben und bidirektionale Funktionen verwenden möchten, um eine Warnung im Azure-Portal zu bestätigen, zu schließen oder erneut zu öffnen, muss die URL für den Webhook das folgende Format aufweisen: `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=azuremonitor&event_class=<new_connector_instance_name>` . Der <new_connector_instance_name> ist die neue Azure-Pull-Connector-Instanz, die Sie für jeden Mandanten mit anderen Azure-Serviceprinzipalanmeldeinformationen erstellen müssen. Informationen zum Erstellen des Pull-Connectors finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

b. Stellen Sie im Abschnitt „Webhook“ sicher, dass für **Enable the common alert schema (Gemeinsames Warnungsschema aktivieren)** die Option **Ja** ausgewählt ist.

Ergebnis
Die Übertragung von Warnungen von Azure Monitor in das Plugin Event Management beginnt. Das Plugin extrahiert die Informationen aus der ursprünglichen Azure Monitor-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Nächste Maßnahme
Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Integrieren Sie Azure mit REST API-Schlüssel-Token

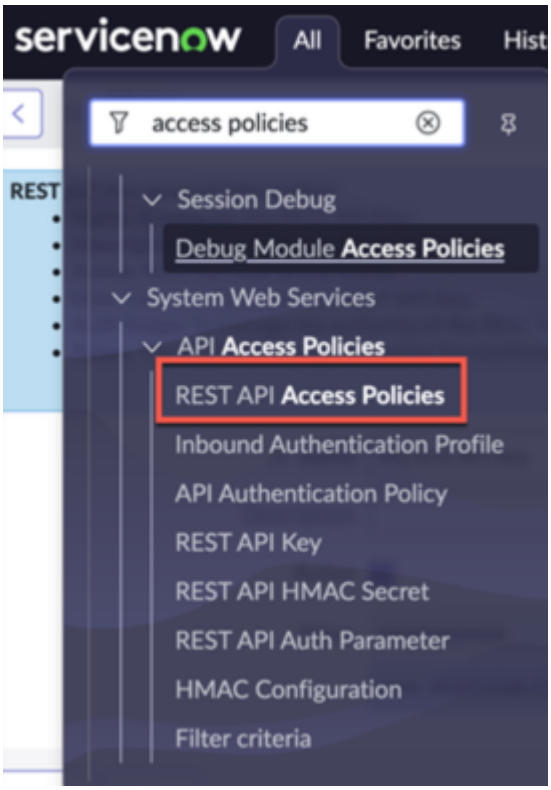
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

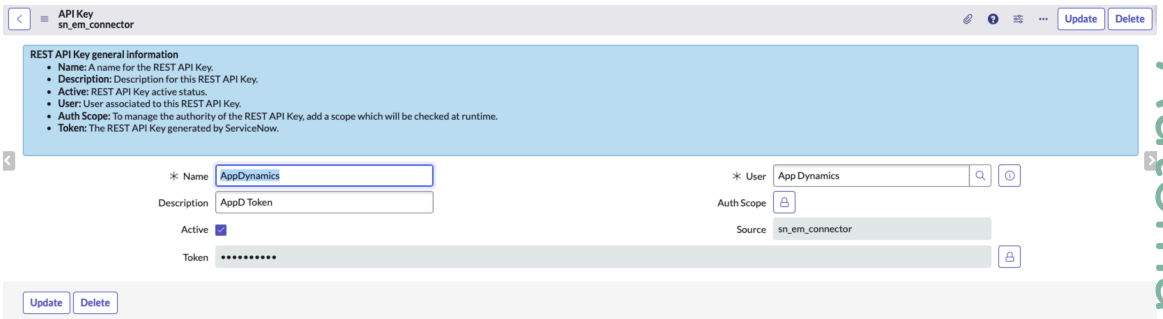
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Azure Monitor mit OAuth-Authentifizierung integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure V1- oder V2-Token im Azure-Monitor authentifizieren.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Im Azure-Portal werden Warnungskorrelationsregeln über definiert `Correlate alerts`Einstellung in Warnungsverarbeitungsregeln. Wenn `Correlate alerts`Ist im Azure-Portal zugewiesen, die Azure Monitor-Warnungen, die auf empfangen wurden ServiceNow® Instanzen innerhalb von 60 Minuten werden mithilfe von Tag-basiertem Warnungs-Clustering gruppiert.

Erforderliche Rollen: evt_mgmt_admin, web_service_admin und oauth_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure Monitor. Legen Sie in Ihrem Azure Monitor-Portal Ihre ServiceNow AI Platform-Instanz mithilfe von V1- oder V2-Token als REST-Endpunkt fest.

Prozedur

1. Im Azure Monitor-Portal:

   a. Führen Sie die App-Registrierung durch, und stellen Sie eine API bereit.
   Weitere Informationen zum Registrieren einer App und zum Bereitstellen einer API in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Erstellen Sie eine Aktionsgruppe mit einem sicheren Webhook, und geben Sie den REST-Endpunkt als https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=azuremonitor an.

> **Hinweis:** Wenn Sie mehrere Mandanten im Azure-Portal haben und bidirektionale Funktionen verwenden möchten, um eine Warnung im Azure-Portal zu bestätigen, zu schließen oder erneut zu öffnen, muss die URL für den sicheren Webhook das folgende Format aufweisen: `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=azuremonitor&event_class=<new_connector_instance_name>` . Der <new_connector_instance_name> ist die neue Azure-Pull-Connector-Instanz, die Sie für jeden Mandanten mit anderen Azure-Serviceprinzipalanmeldeinformationen erstellen müssen. Informationen zum Erstellen des Pull-Connectors finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Für servicenowservices.com Instanzen muss der Rest-Endpunkt sein https://<instance-name>.servicenowservices.com/api/sn_em_connector/em/inbound_event?source=azuremonitor .

Weitere Informationen zum Hinzufügen eines sicheren Webhooks zu einer Aktionsgruppe finden Sie unter https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups .

c. Navigieren zu **Alerts** > **Verwalten Sie Warnungsregeln**an.

d. Stellen Sie im Abschnitt „Secure Webhook“ (Sicherer Webhook) sicher, dass **Ja** für die Option **Enable the common alert schema (Gemeinsames Warnungsschema aktivieren)** ausgewählt ist.

e. Fügen Sie die Aktionsgruppe mit dem sicheren Webhook einer Warnungsregel hinzu.

2. Überprüfen Sie im Azure Monitor-Portal, welches Azure-Token von Ihrer registrierten Anwendung verwendet wird.

a. Navigieren Sie zu **App Registration** (App-Registrierung), und wählen Sie die registrierte Anwendung aus.

b. Klicken Sie im Abschnitt „Verwalten“ auf **Manifest**.

c. Wählen Sie im Editor-Bildschirm die aus **Microsoft Graph App-Manifest** Registerkarte und suchen Sie nach *`requestedAccessTokenVersion`*Parameter, oder wählen Sie aus **AAD Graph App-Manifest** Registerkarte und suchen Sie nach *`accessTokenAcceptedVersion`*Parameter. Wenn der Wert von *`requestedAccessTokenVersion`*Oder *`accessTokenAcceptedVersion`*Ist **2** , Die Integration muss V2-Token verwenden.

Wenn der Wert von *`requestedAccessTokenVersion`*Oder *`accessTokenAcceptedVersion`*Ist **1** Oder **Null** , Die Integration muss V1-Token verwenden.

3. Stellen Sie in Ihrer ServiceNow AI Platform-Instanz sicher, dass dem ServiceNow-Benutzer die richtige Anwendungs-ID (Client-ID) oder der URI mit der richtigen Anwendungs-ID zugewiesen ist.
Stellen Sie außerdem sicher, dass ServiceNow sys_user die Rolle evt_mgmt_integration zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Systemsicherheit** > **Anwender und Gruppen** > **Anwender**an.

> **Hinweis:** Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

b. Stellen Sie sicher, dass das Feld **Quelle** für den ServiceNow-sys_user mit der richtigen Anwendungs-ID (Client-ID) oder dem URI mit der richtigen Anwendungs-ID ausgefüllt ist, wie im Azure Monitor-Portal definiert.
Wenn die Anwendung ein Azure V1-Token verwendet, muss in das Feld **Quelle** der URI der Anwendungs-ID der registrierten Anwendung eingetragen werden. Wenn die Anwendung ein Azure V2-Token verwendet, muss in das Feld **Quelle** die Anwendungs-ID (Client-ID) der registrierten Anwendung eingetragen werden.

Wenn das Feld **Quelle** nicht angezeigt wird, ändern Sie das Formularlayout so, dass dieses Feld angezeigt wird. Klicken Sie auf das Kontextmenüsymbol ( ), und wählen Sie **Konfigurieren > Formularlayout** aus. Verschieben Sie **Quelle** in die Liste „Ausgewählt“.

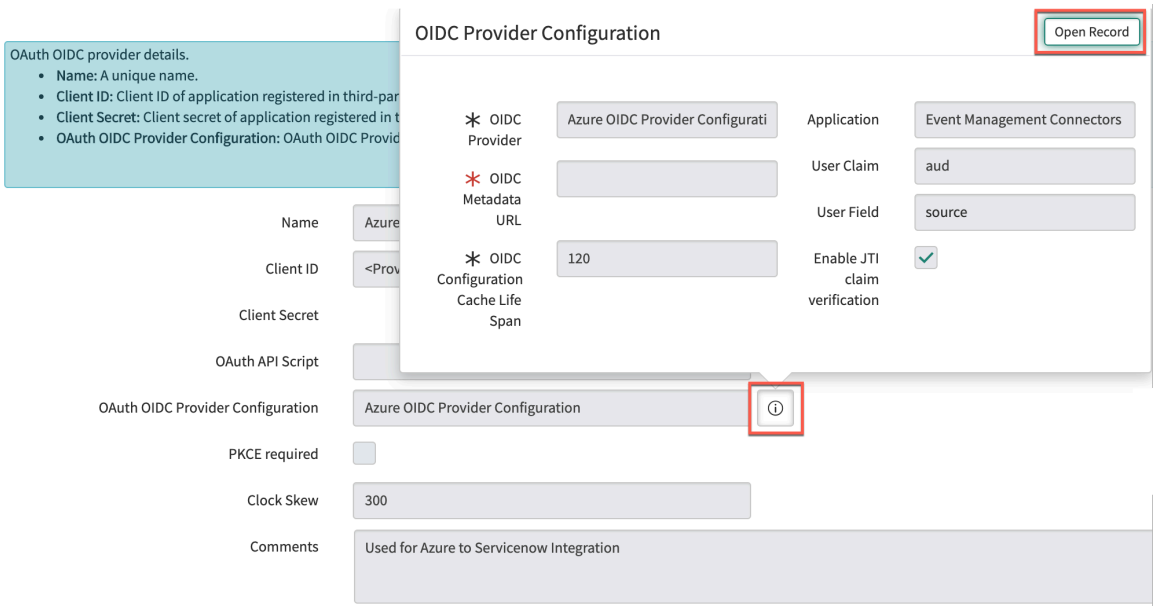
> **Hinweis:** Wenn Version Ihrer ServiceNow AI Platform-Instanz Paris Patch 2 oder Orlando Patch 9 oder früher ist, muss der Wert im Feld **Quelle** in eckige Klammern eingeschlossen werden. Beispiel: [api://azuretest].

4. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Ereignismanagement** > **Integrationen** > **Azure OAuth-Konfiguration**an.
5. Klicken Sie auf **Azure OAuth OIDC Entry (Azure OAuth OIDC-Eintrag)**, und geben Sie die Client-ID ein.
Wenn die registrierte Anwendung ein Azure V2-Token verwendet, muss die Client-ID mit der Anwendungs-ID (Client-ID) der im Azure Monitor-Portal definierten App-Registrierungen identisch sein.

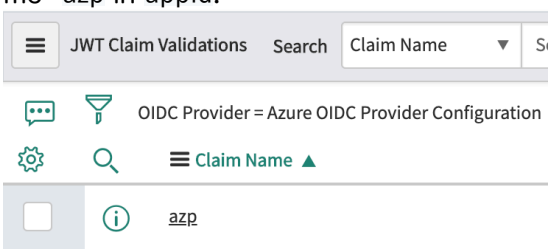
   Wenn die registrierte Anwendung ein Azure V1-Token verwendet, muss die Client-ID mit dem URI der Anwendungs-ID der im Azure Monitor-Portal definierten App-Registrierungen identisch sein (der bereitgestellten API).

6. Klicken Sie im Feld **OAuth-OIDC-Providerkonfiguration** auf das Info-Symbol ( ).
7. Klicken Sie im Fenster „OIDC-Provider-Konfiguration“ auf **Datensatz öffnen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Geben Sie ein OIDC-Metadaten-URL Gemäß dem Azure-Token, das von der registrierten Anwendung verwendet wird, wie in der folgenden Tabelle dargestellt.

Azure-Token	OIDC-Metadaten-URL
V2	Fügen Sie im Formular „OIDC-Provider-Konfiguration“ im Feld **OIDC-Metadaten-URL** die folgende URL hinzu: https://login.microsoftonline.com/<tenant-id>/v2.0/.well-known/openid-configuration Achten Sie darauf, dass <tenant-id> durch die richtige Azure-Mandanten-ID ersetzt wird. **Hinweis:** Wenn Sie versuchen, Azure Gov Cloud in den ServiceNow Azure Monitor Connector zu integrieren, denken Sie daran, den Anspruchswert in zu ändern F1f34126-d4e–f-40e1-ad4b-bf5d47b4860d .
V1	Gehen Sie im Formular „OIDC-Provider-Konfiguration“ wie folgt vor: ○ Ändern Sie in der Spalte „Anspruchna–me“ azp in appid. 

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Token	OIDC-Metadaten-URL
	Hinweis: Wenn Sie versuchen, Azure Gov Cloud in den ServiceNow Azure Monitor Connector zu integrieren, denken Sie daran, den Anspruchswert in zu ändern `F1f34126-d4ef-40e1-ad4b-bf5d47b4860d` . ○ Fügen Sie im Feld **OIDC-Metadaten-URL** die folgende URL hinzu: https://log–in.microsoftonline.com/<tenant-id>/.well-known/openid-configuration Achten Sie darauf, dass <tenant-id> durch die richtige Azure-Mandanten-ID ersetzt wird.

Ergebnis

Wenn in Azure Monitor eine Warnung als Teil der Warnungsregel erstellt wird, wird die Benachrichtigung über den sicheren Webhook-Endpunkt an die ServiceNow AI Platform gesendet. Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen. Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren .

Bidirektionalen Azure Monitor-Connector konfigurieren

Vom Azure Monitor-Pull-Connector werden Informationen aus ServiceNow Ereignismanagement an das Azure-Portal gesendet. Vom Pull-Connector werden die Warnungsstatusänderungen aus der ServiceNow-Umgebung an das Azure-Portal gesendet.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Wenn eine Warnung im Azure-Portal ausgelöst wird, wird ein sicherer Webhook erstellt, um die Warnungsbenachrichtigungen an zu senden ServiceNow. Die Azure Monitor Connector Erhält die Warnungsbenachrichtigung als Ereignis in ServiceNow Instanz.

Der bidirektionale Azure Monitor-Connector wird in den folgenden ServiceNow AI Platform-Versionen unterstützt:

- Quebec, Patch 9 oder höher
- Rome, Patch 3 oder höher
- San Diego

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie den bidirektionalen Azure Monitor-Connector konfigurieren, wird der bidirektionale Austausch von Werten an und von der externen Ereignisquelle aktiviert. Wenn eine Warnung ist **Bestätigt** / **Geschlossen** / **Erneut Geöffnet** Auf der ServiceNow Instanz ändert sich der Status in der Azure Portal-Warnung mithilfe des bidirektionalen Connectors.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Szenarien beschreiben die bidirektionale Standardfunktionalität für den Azure Monitor-Connector:

- Wenn eine Warnung im Azure-Portal geschlossen wird, wird sie in ServiceNow automatisch geschlossen. Sie wird jedoch unabhängig von der bidirektionalen Funktion aktualisiert, da durch das Schließen des über das Azure-Portal empfangenen Events die Warnung geschlossen wird.
- Wenn eine Warnung im ServiceNow-System manuell geschlossen wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal geschlossen.
- Wenn der Warnungsstatus in ServiceNow in **Erneut geöffnet** geändert wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal geöffnet.
- Wenn eine Warnung im ServiceNow-System **Bestätigt** wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal bestätigt.

Hinweis: Zum Ändern des Warnungsstatus im Azure-Portal erhält der MID-Server das Zugriffstoken, das eine Verbindung mit herstellt https://login.microsoftonline.com/ Und um den Warnungsstatus im Azure-Portal zu ändern, ruft der MID-Server die Changestate-API für die URL auf https://management.azure.com/ Wie in beschrieben https://learn.microsoft.com/en-us/rest/api/monitor/alertsmanagement/alerts/change-state?view=rest-monitor-alertsmanagement-2023-07-12-preview&tabs=HTTP .

Prozedur

1. Führen Sie für einen einzelnen Mandanten die folgenden Schritte aus:
   - Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
   - Wählen Sie Aus **Azure-Monitor** .
   - Aktivieren Sie die Checkbox **Aktiv**.

     Für diese Konfiguration ist **Host-IP** Das Feld hat keine funktionalen Auswirkungen und wird nicht verwendet, daher wird eine Dummy-IP-Adresse (1,1.1,1) bereitgestellt.
   - In **Anmeldeinformationen** Fügen Sie die Azure Service Principal-Anmeldeinformationen hinzu, die über die Berechtigung zum Ausführen von Aktionen verfügen.

     Um den Warnungsstatus zu ändern, muss der Serviceprinzipal über verfügen Microsoft.Warnungsverwaltung Berechtigungen und Beitragender Wird Überwacht Rolle.
   - Wählen Sie den MID-Server aus, der für diesen Connector verwendet werden soll, oder fügen Sie ihn hinzu.

     Wenn Warnungen im MS Azure-Portal nicht wie erwartet aktualisiert werden, überprüfen Sie die MID-Server Protokolliert Fehler.
2. Führen Sie für mehrere Mandanten die folgenden Schritte aus:
   - Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
   - Wählen Sie **Neu**.
   - In **Name** Feld den Namen des <new_connector_instance_name> eingeben, den Sie in der URL für den sicheren Webhook unter angegeben haben Azure Monitor mit OAuth-Authentifizierung integrieren.
   - Geben Sie im Feld Host-IP eine beliebige Dummy-IP-Adresse ein, z. B. 1,1.1,1.
   - In **Anmeldeinformationen** Fügen Sie die Azure Service Principal-Anmeldeinformationen des Mandanten hinzu, der über die Berechtigung zum Ausführen von Aktionen verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie aus **Bidirektional** Kontrollkästchen.
- Wählen Sie den MID-Server aus, der für diesen Connector verwendet werden soll, oder fügen Sie ihn hinzu.
- Wählen Sie **Absenden**.
- Aktivieren Sie die Checkbox **Aktiv**.
- Wählen Sie **Aktualisieren**.

Nächste Maßnahme

Mehrere Warnungen aus dem Azure-Portal können einer einzelnen ServiceNow-Warnung durch Deduplizierung zugeordnet werden. Die Zuordnung zwischen der ServiceNow-Warnung und den Azure-Warnungen wird in der Tabelle sn_em_connector_event_data verwaltet. Die Aufbewahrung von Datensätzen hängt vom Status der Warnung ab:

- Wenn der bidirektionale Azure-Connector nicht aktiv ist, werden die Datensätze nach 2 Tagen gelöscht.
- Wenn der bidirektionale Azure-Connector aktiv ist:
  - Wenn sich die Warnung im Status „Geschlossen“ befindet, werden die Daten 7 Tage lang aufbewahrt. Diese Dauer kann durch die Systemeigenschaft sn_em_Connector.eventdata_closedevent_interval angepasst werden.
    - Wenn die geschlossene Warnung innerhalb von 7 Tagen erneut geöffnet wird, werden die entsprechenden geschlossenen Warnungen aus dem Azure-Portal erneut geöffnet.
    - Wenn die geschlossene Warnung nach 7 Tagen erneut geöffnet wird, werden die entsprechenden geschlossenen Warnungen aus dem Azure-Portal nicht erneut geöffnet.
  - Wenn sich die Warnung im Status „Offen“ befindet, werden die Daten 30 Tage lang aufbewahrt. . Diese Dauer kann von sn_em_Connector.eventdata_openevent_interval angepasst werden.
    - Wenn Sie eine offene ServiceNow-Warnung innerhalb von 30 Tagen schließen oder bestätigen möchten, können Sie alle entsprechenden Azure-Warnungen im Azure-Portal schließen oder bestätigen.
    - Wenn Sie eine offene ServiceNow-Warnung nach 30 Tagen schließen oder bestätigen möchten, können Sie alle entsprechenden Azure-Warnungen im Azure-Portal nicht schließen oder bestätigen.

Event-Erfassung von Microsoft Azure Monitor

Mit dem MID WebServer-Event-Sammler können Sie Event-Nachrichten im JSON-Format erfassen, die vom Microsoft Azure-Portal gesendet wurden.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Siehe MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Azure-Portal werden Warnungskorrelationsregeln über definiert `Correlate alerts`Einstellung in Warnungsverarbeitungsregeln. Wenn `Correlate alerts`Ist im Azure-Portal zugewiesen, die Azure Monitor-Warnungen, die auf empfangen wurden ServiceNow® Instanzen innerhalb von 60 Minuten werden mithilfe von Tag-basiertem Warnungs-Clustering gruppiert.

Event-Nachrichten im JSON-Format werden von Microsoft Azure gesendet. Die MID-Server Wandelt die gesammelten Ereignisnachrichten um, indem sie mithilfe der Skripteinbindung TransformEvents_MidAzureMonitor analysiert werden, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**an. Klicken Sie auf der Seite „Push-Connectors“ auf **Azure Monitor Mid Push Connector**.

Das Standardformat der URL zum Übertragen von Push-Event-Nachrichten von Microsoft Azure an den MID-Server lautet: `http://<MID_Web_Server_User>:<MID_Web_Server_Password>@<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidAzureMonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Anwenders des MID-Webservers.

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Ereignisnachrichten mit Standardauthentifizierung.

Prozedur

1. Stellen Sie im Azure Monitor-Portal sicher, dass die MID-Server-IP über das Azure-Portal und der MID-Rest-Punkt über zugänglich ist Microsoft Azure Oder installieren Sie MID-Server Geben Sie auf einer Azure-VM die öffentliche Azure-VM-Adresse in der URL an, und lassen Sie den MID_Web_Server_Port in zu **Azure-VM** > **Netzwerkeinstellungen** > **Regeln für eingehende Ports**an.
2. Erstellen Sie eine Aktionsgruppe mit Webhook, und geben Sie wie folgt den REST-Endpunkt an: `http://<MID_Web_Server_User>:<MID_Web_Server_Password>@<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidAzureMonitor`.

   Hinweis: Weitere Informationen zum Hinzufügen eines Webhook zu einer Aktionsgruppe finden Sie unter Aktionsgruppen im Azure-Portal erstellen und verwalten auf der Microsoft-Dokumentationswebsite.

3. Stellen Sie im Abschnitt „Webhook“ sicher, dass für **Enable the common alert schema** (Gemeinsames Warnungsschema aktivieren) die Option **Ja** ausgewählt ist.
4. Navigieren zu **Alerts** > **Verwalten Sie Warnungsregeln**an.
5. Fügen Sie die Aktionsgruppe mit dem Webhook einer Warnungsregel hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Ereignissammlung von BMC TrueSight und BMC TrueSight_v2

Der MID WebService-Ereignissammler ermöglicht Ihnen das Erfassen von JSON-formatierten Ereignisnachrichten, die von BMC TrueSight Operations Management (TrueSight), früher bekannt als BMC ProactiveNet Performance Management (BPPM), gesendet werden, und nutzt Ereignis-Stream-Benachrichtigungsfunktionen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Siehe MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Event-Nachrichten im JSON-Format werden von BMC TrueSight gesendet. Die MID-Server Wandelt die gesammelten Ereignisnachrichten um, indem sie mithilfe der Skripteinbindung TransformEvents_bmcTrueSight analysiert werden, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **Listener-Transformationsskripts**an. Klicken Sie auf der Seite „Listener-Umwandlungsskripts“ auf **TransformEvents_bmcTrueSight**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von BMC TrueSight auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_bmcTrueSight`.

Das Standardformat der URL zum Verschieben von Ereignisnachrichten von BMC TrueSight_v2 an die MID-Server Ist `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/Mid/em/inbound_event?Transform=TransformEvents_bmcTrueSight_v2` .

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Benutzers der MID-Webserver-Erweiterung. Codieren Sie das Passwort jedoch in BASE64. Beispiel: Wenn das Passwort der MID-Webserver-Erweiterung `admin` ist, verwenden Sie in diesem Fall `YWRtaW4=` als Passwort für MID_Web_Server_Password.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variablen in der Standard-URL (Fortsetzung)

Variable	Beschreibung
	Um den BASE64-Wert zu bestimmen, können Sie das Dienstprogramm auf dieser Website verwenden: https://www.base64encode.org/

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung. Weitere Informationen zu unterstützten Authentifizierungsmethoden finden Sie unter MID-Webserver erweiterung konfigurieren.

Prozedur

1. Legen Sie in BMC TrueSight den MID WebService-Eventsammler als Ziel für die BMC TrueSight-Benachrichtigung fest, indem Sie diese Parameter verwenden:

Variablen in der generischen BMC-URL

Variable	Beschreibung
serverHost	Name des BMC TrueSight-Servers.
port	Nummer des BMC TrueSight-Ports.

2. Ersetzen Sie im Nachrichtentext und der generischen BMC-URL die Parameter durch die Werte in der vorherigen Tabelle, und stellen Sie eine Verbindung mit BMC TrueSight her.
Verwenden Sie den REST-Ansatz von BMC „Veröffentlichen/Abonnieren“, um ein Stream-Event-Abonnement zu erstellen und Event-Nachrichten im JSON-Format zu senden. Das generische Format der BMC-URL zum Erstellen eines Stream-Ereignisabonnements lautet: `http|https://<serverHost>:<port>/bppmws/api/Stream/subscribe?datatype=event` . Beispiel: `http://TrueSight1server:40/bppmws/api/stream/subscribe?dataType=event`.

Ergebnis

Beispiel für die Zuordnung von Event-Nachrichten zu Event-Feldern in der Tabelle Event (em_event)

Ereignisfeld	Ereignisnachricht
node	mc_host
type	mc_object_class
metric_name	mc_parameter
resource	mc_object
severity	severity
time_of_event	date_reception
description	msg

Example:
Beispiel für den Nachrichtentext.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
"action": "create",
"data": {
"mc_abstracted": [],
"itsm_operational_category3": "",
"mc_object_class": "CPU",
"source": "MySource",
"adapter_host": "",
"itsm_operational_category2": "",
"itsm_location": "",
"itsm_operational_category1": "",
"mc_abstraction": [],
"mc_tool_id": "",
"mc_original_priority": "PRIORITY_1",
"event_handle": "3172",
"mc_modhist": [],
"mc_tool_class": "",
"mc_origin": "",
"mc_tool_uri": "",
"mc_service": "",
"mc_smc_type": "",
"mc_object_owner": "",
"mc_object": "CPU_0",
"mc_notes": [],
"itsm_model_version": "",
"mc_origin_key": "",
"mc_tool_address": "",
"mc_ueid": "mc.pncell_bmcswetsom96.1829b8ed.0",
"mc_bad_slot_names": [],
"date": "20161114081525.000000-300",
"itsm_item": "",
"mc_timeout": "0",
"mc_priority": "PRIORITY_1",
"itsm_type": "",
"itsm_manufacturer": "",
"mc_tool_key": "",
"itsm_product_name": "",
"mc_smc_impact": "NOT_ELECTED",
"mc_parameter": "MEMFreeMem",
"mc_bad_slot_values": [],
"itsm_incident_id": "",
"mc_incident_report_time": "0",
"mc_event_model_version": "1.1.00",
"mc_relationships": "0/0",
"CLASS": "EVENT",
"mc_using_organization": "",
"mc_tool_sev": "",
"mc_parameter_threshold": "",
"mc_smc_effects": [],
"mc_smc_priority": "0",
"itsm_company": "",
"date_reception": "1479129325",
"mc_smc_alias": "bmcswetsom96_2",
"pn_detail_diag_count": "0",
"mc_effects": [],
"mc_object_uri": "",
"mc_date_modification": "1479129325",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"mc_incident_time": "0",
"status": "OPEN",
"msg": "Free Memory Low",
"pn_detail_diag": "0",
"mc_host": "bmcswetsom97",
"repeat_count": "69",
"mc_host_address": "",
"mc_tool_suggestion": "",
"mc_using_organization_id": "",
"mc_collectors": ["1.1", "3.1.1", "4.1", "5.1"],
"mc_account": "",
"mc_long_msg": "",
"mc_owner": "",
"mc_history": ["pncell_bmcswetsom96:3172"],
"itsm_category": "",
"mc_host_class": "",
"mc_tool_rule": "",
"mc_local_reception_time": "1479129325",
"mc_associations": [],
"mc_relation_source": "",
"mc_propagations": [],
"mc_client_address": "172.16.173.131",
"itsm_incident_status": "",
"mc_tool_time": "0",
"mc_origin_class": "",
"mc_tool": "",
"mc_action_count": "0",
"mc_cause": "0",
"mc_origin_sev": "",
"mc_host_id": "0",
"mc_event_relations": [],
"mc_operations": [],
"mc_event_category": "CONFIGURATION_MANAGEMENT",
"pn_device_name": "",
"mc_arrival_time": "1479129325",
"severity": "OK",
"mc_notification_history": [],
"mc_smc_causes": [],
"mc_acl": [],
"mc_original_severity": "CRITICAL",
"duration": "0",
"mc_location": "Unknown",
"mc_smc_id": "",
"mc_parameter_value": "20",
"administrator": "",
"mc_event_subcategory": "OTHER",
"mc_parameter_unit": ""
},
"subscriptionId": "af18f6ba-a2d3-4574-81c8-7f366ca70ebd",
"type": "EVENT"
}
```


Integrieren Dynatrace Plattformereignisse

Integrieren Dynatrace Mit Ereignismanagement Durch Hinzufügen von DynatraceÜberwachen Sie als authentifizierte Datenquelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Welche Authentifizierung wird verwendet?

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung wird mit durchgeführt Dynatrace V1- oder V2-Zugriffstoken überwachen. Weitere Informationen finden Sie unter Integrieren Dynatrace Mit OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Standardstandard der Authentifizierung, ohne dass dies erforderlich ist Dynatrace Active Directory. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE oder nützlich sein DevOps Teams. Weitere Informationen finden Sie unter Integrieren Dynatrace Mit Standardauthentifizierung.

Hinweis: Wenn ein Problem in Dynatrace erneut geöffnet wird, wird die ursprüngliche Startzeit beibehalten und nicht auf den Zeitpunkt der erneuten Öffnung aktualisiert. Dieses Verhalten ist beabsichtigt und spiegelt wider, wie Dynatrace den Problemlebenszyklus verwaltet. Probleme, die innerhalb des definierten Zeitraums der erneuten Öffnung (normalerweise 30 Minuten) erneut geöffnet wurden, werden als Fortsetzung des ursprünglichen Problems behandelt. Die Startzeit spiegelt weiterhin den Zeitstempel des frühesten auslösenden Ereignisses wider, auch nach dem erneuten Öffnen.

Verwenden Sie den Zeitstempel für Nachweisdetails nicht als Ersatz für die Startzeit des Problems. Der Nachweiszeitstempel bezieht sich auf einzelne beitragende Ereignisse innerhalb des Problems. Sie ist Teil der Ursachenanalyse (Root Cause Analysis, RCA) und gibt nicht den Start oder die Dauer des Gesamtproblems an.

Beginnend mit Xanadu Release, die mit dem Connector bereitgestellten Basissystemregeln, die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), haben jetzt die **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Integrieren Dynatrace Mit Standardauthentifizierung

Integrieren Sie Dynatrace mit Ereignismanagement, indem Sie der Dynatrace-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie sicher, dass Konfigurationselemente für die von verwalteten Hosts vorhanden sind Dynatrace Ist in vorhanden ServiceNow AI Platform Instanz. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder Cloud-Discovery erkannt werden.

Erforderliche Rollen: evt_mgmt_integration und web_service_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Ereignismanagement Umgebung für die Sammlung von Ereignissen aus Dynatrace durch Authentifizierung Dynatrace Als Datenquelle. Legen Sie in Ihrer Dynatrace-Konsole die ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. In Ihrem Dynatrace Konsole, definieren Sie Hostbenennungsregeln:
   a. Navigieren zu **Einstellungen** > **Überwachung** > **Hostbenennung**an.
   b. Definieren Sie die Hostbenennungsregeln für jeden Cloud-Anbieter (Azure/AWS/GCP), um ein CI aus ServiceNow eindeutig zu identifizieren.
   Dadurch wird sichergestellt ServiceNow CIs können anhand der von empfangenen Nutzlast eindeutig identifiziert werden Dynatrace.

   Hinweis: Sie müssen keine Hostbenennungsregel für erstellen VMware Computer aufgrund Dynatrace Verwaltet sie als physische Server.

2. Definieren Sie Erkennungsregeln für Anomalien:
   a. Navigieren zu **Einstellungen** > **Anomalie-Erkennung** > **Infrastruktur**an.
   b. Definieren Sie auf der Registerkarte **Hosts** Regeln, wann Warnungen auf den verwalteten Hosts erstellt werden sollen.
3. Definieren Sie die Integrationseinstellungen:
   a. Navigieren zu **Einstellungen** > **Integration** > **Problembenachrichtigungen** > **Benachrichtigungen hinzufügen**an.
   b. Fügen Sie im Formular „Set up custom integration“ (Benutzerdefinierte Integration einrichten) die Webhook-URL hinzu: https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=dynatrace.
   Wählen Sie für die Standardauthentifizierung aus **Erstellen Sie den Header für die Basisautorisierung** . Sie können die Felder Anwendername und Passwort für den Anwender anzeigen.
   c. Geben Sie Anwendername und Passwort des entsprechenden Anwenders ein.

      Hinweis: Stellen Sie sicher, dass die Rolle „evt_mgmt_integration“ dem ausgewählten Benutzer zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   d. Fügen Sie im Abschnitt „Custom payload“ (Anwenderdefinierte Nutzlast) die folgende Nutzlaststruktur für die zu generierenden Ereignisse hinzu.

```
{
 "connectionId": <connections_alias_sys_id>,
 "ImpactedEntities": {ImpactedEntities},
 "ImpactedEntity": "{ImpactedEntity}",
 "PID": "{PID}",
 "ProblemDetailsHTML": "{ProblemDetailsHTML}",
 "ProblemDetailsJSONv2": {ProblemDetailsJSONv2},
 "ProblemDetailsMarkdown": "{ProblemDetailsMarkdown}",
 "ProblemDetailsText": "{ProblemDetailsText}",
 "ProblemID": "{ProblemID}",
 "ProblemImpact": "{ProblemImpact}",
 "ProblemSeverity": "{ProblemSeverity}",
 "ProblemTitle": "{ProblemTitle}",
 "ProblemURL": "{ProblemURL}",
 "State": "{State}",
```

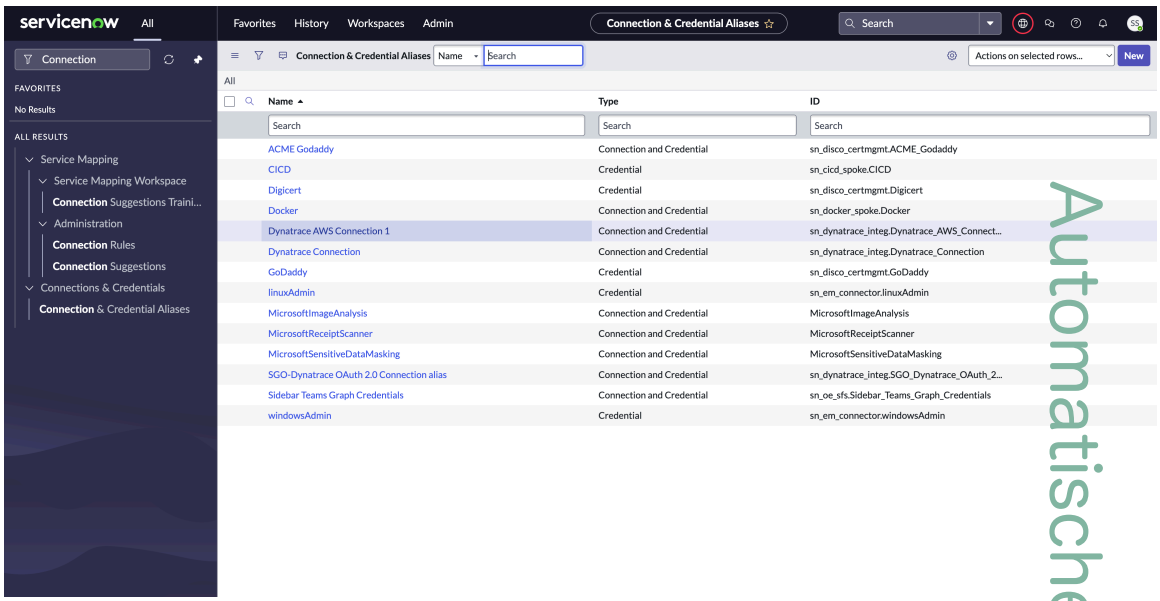

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 "Tags": "{Tags}"
}
```

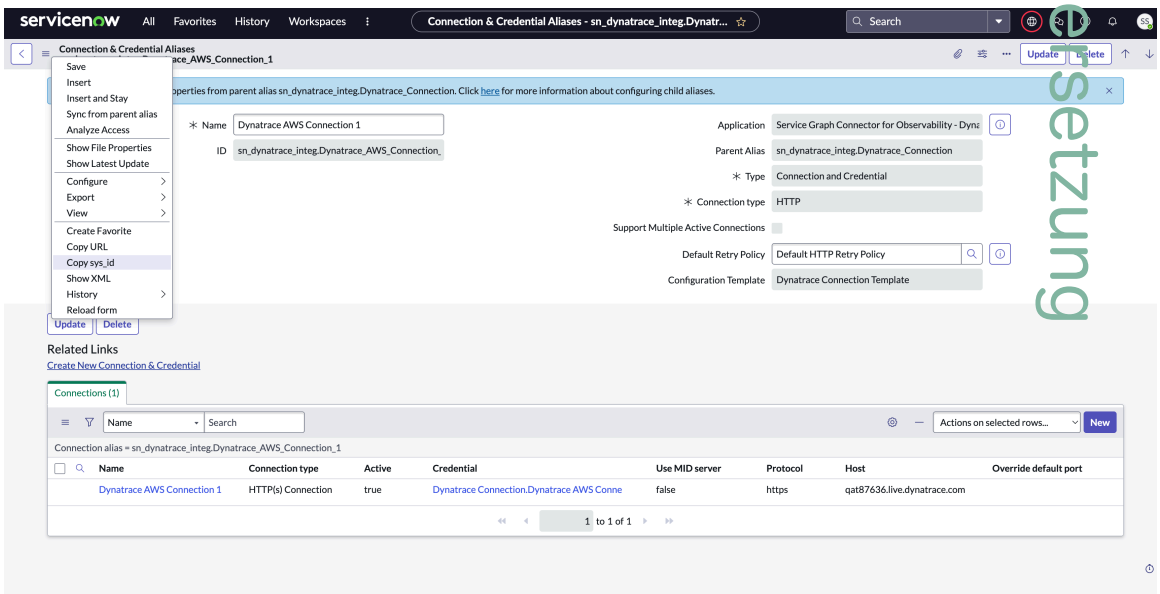
Hinweis: Für den <connections_alias_sys_id>:

i. Navigieren zu **Alle** > **IntegrationHub** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.

ii. Wählen Sie diese Option aus, um den Connector zu öffnen, für den Sie den <connections_alias_sys_id> abrufen möchten.



iii. Klicken Sie mit der rechten Maustaste auf das Kontextmenü ( ) Und dann auswählen **Kopieren Sie die sys_ID** .



Ergebnis

Warnungen beginnen aus dem zu fließen Dynatrace Konsole in das Ereignismanagement-Plugin. Das Plugin extrahiert Informationen aus der ursprünglichen Dynatrace-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für aktiviert Dynatrace Ereignisse für alle Anbieter (Azure/ AWS/ Google). Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Event-Regel **Dynatrace - Allgemein** aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Dynatrace Mit OAuth-Authentifizierung

Integrieren Dynatrace Mit Ereignismanagement Durch Authentifizierung Dynatrace V1- oder V2-Token in DynatraceÜberwachen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.

Vergewissern Sie sich, dass Konfigurationselemente für die von Dynatrace verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Dynatrace Die Integration mit OAuth-Authentifizierung ist ab verfügbar Washington DC Plattformversion oder höher.

Prozedur

1. Konfiguration auf der ServiceNow Instanz.

a. Erstellen *glide.oauth.inbound.client.credential.grant_type.enabled*Systemeigenschaft zur Verwendung des Gewährungstyps „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen.

- Typ: true|false
- Wert: true

b. Erstellen Sie einen OAuth-Entitätsendpunkt, damit Clients auf die Instanz zugreifen können.

i. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und wählen Sie dann aus **Neu** .

ii. Wählen Sie auf der Seite „Interceptor“ die Option aus **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** Und füllen Sie dann das Formular aus.

iii. Um einen OAuth-Client-Datensatz zu erstellen, wählen Sie aus **Übermitteln** .

c. Fügen Sie dem erstellten OAuth-Client-Datensatz den OAuth-Anwendungsanwender und den Standardgewährungstyp hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Fügen Sie im Formular „OAuth-Entität“ hinzu **OAuth-Anwendungsanwender** Und **Standardgewährungstyp** Felder zur Verwendung des Gewährungstyps „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen.

ii. Öffnen Sie den erstellten OAuth-Client-Datensatz.

iii. Wählen Sie im Seitenheader die Option aus **Mehr** Symbol „Optionen“.

iv. Auswahlvorgang **Konfigurieren** > **Formularlayout**

v. Fügen Sie auf der Seite „Formularlayout“ hinzu **OAuth-Anwendungsanwender und Standardgewährungstyp** Aus der Liste der Felder.

vi. **Speichern** Oder **Aktualisieren** Das Formular.

vii. Für **OAuth-Anwendungsanwender** Wählen Sie den Anwender aus.

Der Anwender muss über die Rolle „evt_mgmt_Integration“ verfügen, die zum Erstellen der von gesendeten Ereignisse verwendet wird Dynatrace.

Hinweis: Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

viii. Festlegen **Standardgewährungstyp** Feldwert bis **Client-Anmeldeinformationen** .

2. In Dynatrace Konsole, definieren Sie die Integrationseinstellungen.

a. Navigieren zu **Einstellungen** > **Integration** > **Problembenachrichtigungen** > **Benachrichtigungen einrichten**an.

b. Geben Sie im Formular „Anwenderdefinierte Integration einrichten“ die Webhook-URL ein.

`https://<Instanzname>.service-now.com/api/sn_em_connector/em/inbound_event?source=dynatrace`

c. Aktivieren **Verwenden Sie OAuth 2,0 für die Authentifizierung** .

d. Führen Sie im Abschnitt „OAuth 2.0-Anmeldeinformationen“ die folgenden Schritte aus.

i. Geben Sie die Zugriffstoken-URL als an `https://<instance_name>.service-now.com/oauth_token.do` .

ii. Geben Sie den Wert für an **Client-ID** Mit der Client-ID des in erstellten OAuth-Entitäts-Clients ServiceNow Instanz.

iii. Geben Sie „Client-Geheimnis“ mit dem Client-Geheimnis des in erstellten OAuth-Entitäts-Clients an ServiceNow Instanz.

iv. Wählen Sie **Speichern**.

e. Fügen Sie im Abschnitt „Custom payload“ (Anwenderdefinierte Nutzlast) die folgende Nutzlaststruktur für die zu generierenden Ereignisse hinzu. Stellen Sie sicher `Betroffene Entitäten` Und `ProblemDetailsJSONv2` Werden als JSON-Objekte übergeben, nicht als Zeichenfolgen.

```
{
 "ImpactedEntities": {ImpactedEntities},
 "ImpactedEntity": "{ImpactedEntity}",
 "PID": "{PID}",
 "ProblemDetailsHTML": "{ProblemDetailsHTML}",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 "ProblemDetailsJSONv2": {ProblemDetailsJSONv2},
 "ProblemDetailsMarkdown": "{ProblemDetailsMarkdown}",
 "ProblemDetailsText": "{ProblemDetailsText}",
 "ProblemID": "{ProblemID}",
 "ProblemImpact": "{ProblemImpact}",
 "ProblemSeverity": "{ProblemSeverity}",
 "ProblemTitle": "{ProblemTitle}",
 "ProblemURL": "{ProblemURL}",
 "State": "{State}",
 "Tags": "{Tags}"
}
```

Ergebnis
Warnungen beginnen ab zu fließen Dynatrace Service Desk-Mitarbeiter in Ereignismanagement Plugin. Das Plugin extrahiert Informationen aus der ursprünglichen Dynatrace-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein.
In Ihrem ServiceNow AI Platform Instanz navigieren Sie zu alle Ereignisse, um die Ereignisse anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für aktiviert Dynatrace Ereignisse für (AWS/ Azure/ GCP) Anbieter. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dies zu beheben, müssen Sie aktivieren Dynatrace– Allgemeine Ereignisregel. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Events der New Relic-Plattform integrieren

Integrieren Sie New Relic mit Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in den alten und neuen Konsolen New Relic.

Vorbereitungen
Überprüfen Sie, ob Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus New Relic, indem Sie New Relic als Datenquelle authentifizieren. Legen Sie fest ServiceNow AI Platform Instanz als Rest-Endpunkt mit einem Standard-Webhook. Verwenden Sie den Verfahrensschritt 1 für die neue Konsole. Verwenden Sie den Verfahrensschritt 2 für die alte Konsole.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Für die neue Konsole:

   a. Erstellen Sie ein Ziel.

      i. Navigieren zu**Warnungen und KI** > **Ziele**an.

      ii. In **Fügen Sie Ziele hinzu** Wählen Sie den Abschnitt aus **Webhook** Kanaltyp.

      iii. In **Webhook-Name** Geben Sie den Webhook-Namen ein.

      iv. In **Endpunkt-URL** Feldeingabe: https://<InstanceName>.service-now.com/api/sn_em_connector/em/inbound_event?source=newrelic

      v. In **Standardauthentifizierung** Geben Sie Ihren Anwendernamen und Ihr Passwort ein.

      Hinweis: Überprüfen Sie, ob die Rolle „evt_mgmt_Integration“ dem ausgewählten Anwender zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

      vi. Wählen Sie Aus **Ziel speichern** .

   b. Erstellen Sie eine Richtlinie.

      i. Navigieren zu**Warnungen und KI** > **Warnungsbedingungen Und -Richtlinien**an.

      ii. Wählen Sie Aus **Neue Warnungsrichtlinie** Und definieren Sie eine Richtlinie.

      iii. Wählen Sie Aus **Richten Sie Benachrichtigungen ein** .

      iv. In **Kanal Hinzufügen** Abschnittsauswahl **Webhook** , Und wählen Sie dann das Ziel aus, das Sie im vorherigen Teilschritt erstellt haben.

      v. In **Nutzlastvorlage** Fügen Sie die folgende JSON-Nutzlast ein.

```
{ "account_id": {{nrAccountId}}, "account_name": {{json accumulations.tag.account.[0]}},
"closed_violations_count": {{closedIncidentsCount}}, "open_violations_count":
{{openIncidentsCount}}, "condition_description": "{{escape
accumulations.conditionDescription.[0]}}", "condition_family_id":
{{accumulations.conditionFamilyId.[0]}}, "condition_name": "{{escape
accumulations.conditionName.[0]}}", "current_state": {{json state}}, "details": {{json
issueTitle}}, "duration": {{#if issueDurationMs}}{{issueDurationMs}}{{else}}0{{/if}},
"event_type": "INCIDENT", "incident_acknowledge_url": {{json issueAckUrl}},
"incident_id": {{json issueId}}, "incident_url": {{json issuePageUrl}},
"metadata": { {{#if locationStatusesObject}}"location_statuses": {{json
locationStatusesObject}},{{/if}} {{#if accumulations.metadata_entity_type}}"entity.type":
{{json accumulations.metadata_entity_type.[0]}},{{/if}} {{#if
accumulations.metadata_entity_name}}"entity.name": {{json
accumulations.metadata_entity_name.[0]}},{{/if}} "section": "metadata" },
"owner": {{json owner}}, "policy_name": {{json accumulations.policyName.[0]}},
"policy_url": {{json policyUrl}}, "runbook_url": {{json accumulations.runbookUrl.[0]}},
"severity": {{json priority}}, "targets": [ { "id": "{{labels.targetId.[0]}}", "name": "{{#if
accumulations.targetName}}{{escape accumulations.targetName.[0]}}{{else if
entitiesData.entities}}{{escape entitiesData.entities.[0].name}}{{else}}N/A{{/if}}",
"link": "{{issuePageUrl}}", "product": "{{accumulations.conditionProduct.[0]}}",
"type": "{{#if entitiesData.types.[0]}}{{entitiesData.types.[0]}}{{else}}N/A{{/if}}",
"labels": { {{#each accumulations.rawTag}}"{{escape @key}}": {{#if this.[0]}}{{json
this.[0]}}{{else}}"empty"{{/if}}{{#unless @last}},{{/unless}}{{/each}} } } ], "timestamp":
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{{updatedAt}}, "violation_callback_url": {{json issuePageUrl}}, "violation_chart_url":
{{json violationChartUrl}} }
```

vi. Wählen Sie Aus **Testbenachrichtigung senden** Um das Testereignis in abzurufen ServiceNow Instanz.

vii. Wählen Sie Aus **Nachricht speichern** .

viii. Wählen Sie Aus **Aktivieren Sie den Workflow** Zum Aktivieren des Workflows.

c. Erstellen Sie Warnungsbedingungen, die auf die Richtlinie angewendet werden sollen:

i. Navigieren zu**Warnungen und KI** > **Warnungsbedingungen Und -Richtlinien**an.

ii. Wählen Sie Aus **Warnungsbedingung erstellen** , Definieren Sie die erforderlichen Warnungsdetails, und fügen Sie sie der Richtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.

iii. Wählen Sie Aus **Bedingung Speichern** .

2. Für die alte Konsole:

a. Erstellen Sie einen Benachrichtigungskanal.

i. Navigieren zu**Warnungen und KI** > **Benachrichtigungskanäle**an.

ii. In **Kanaldetails** Wählen Sie die Registerkarte aus **Webhook** Kanaltyp.

iii. In **Basis-Url** Textfeld eingeben: https://<InstanceName>.service-now.com/api/sn_em_connector/em/inbound_event?source=newrelic

iv. Geben Sie im Abschnitt „Basisauth.“ Benutzername und Passwort des entsprechenden Benutzers ein.

> **Hinweis:** Überprüfen Sie, ob die Rolle „evt_mgmt_Integration“ dem ausgewählten Anwender zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

v. In **Anwenderdefinierte Nutzlast** Abschnitt auswählen **Fügen Sie Eine Anwenderdefinierte Nutzlast Hinzu** , Und wählen Sie aus **JSON** Nutzlasttyp.

vi. Fügen Sie die folgende JSON-Nutzlast in ein **Anwenderdefinierte Nutzlast** .

```
{ "account_id": "$ACCOUNT_ID", "account_name": "$ACCOUNT_NAME",
"closed_violations_count_critical": "$CLOSED_VIOLATIONS_COUNT_CRITICAL",
"closed_violations_count_warning": "$CLOSED_VIOLATIONS_COUNT_WARNING",
"condition_description": "$DESCRIPTION", "condition_family_id":
"$CONDITION_FAMILY_ID", "condition_name": "$CONDITION_NAME",
"current_state": "$EVENT_STATE", "details": "$EVENT_DETAILS", "duration":
"$DURATION", "event_type": "$EVENT_TYPE", "incident_acknowledge_url":
"$INCIDENT_ACKNOWLEDGE_URL", "incident_id": "$INCIDENT_ID", "incident_url":
"$INCIDENT_URL", "metadata": "$METADATA", "open_violations_count_critical":
"$OPEN_VIOLATIONS_COUNT_CRITICAL", "open_violations_count_warning":
"$OPEN_VIOLATIONS_COUNT_WARNING", "owner": "$EVENT_OWNER",
"policy_name": "$POLICY_NAME", "policy_url": "$POLICY_URL", "runbook_url":
"$RUNBOOK_URL", "severity": "$SEVERITY", "targets": "$TARGETS", "timestamp":
"$TIMESTAMP", "violation_callback_url": "$VIOLATION_CALLBACK_URL",
"violation_chart_url": "$VIOLATION_CHART_URL" }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Erstellen Sie eine Richtlinie.

i. Navigieren zu**Warnungen und KI** > **Richtlinien**an.

ii. Wählen Sie Aus **Neue Warnungsrichtlinie** Und definieren Sie eine Richtlinie.

iii. In **Benachrichtigungskanäle** Abschnitt auswählen **Hinzufügen** , Wählen Sie aus **Webhook** , Und wählen Sie dann den Kanal aus, den Sie im vorherigen Schritt erstellt haben.

c. Erstellen Sie Warnungsbedingungen, die auf die Richtlinie angewendet werden sollen:

i. Navigieren zu**Infrastruktur** > **Einstellungen** > **Alerts**an.

ii. Wählen Sie Aus **Warnungsbedingung erstellen** , Definieren Sie die erforderlichen Warnungsdetails, und fügen Sie sie der Richtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.

iii. Wählen Sie Aus **Erstellen** .

Ergebnis

Die Übertragung von Warnungen aus der New Relic-Konsole in das Plugin Event Management beginnt. Das Plugin extrahiert die Informationen aus der ursprünglichen New Relic-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Alle Ereignisse** Um die Ereignisse anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für New Relic-Events für alle Provider (Azure /AWS/GCP) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dies zu beheben, müssen Sie aktivieren **Neue Relic: Allgemein** Ereignisregel. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Sie New Relic mit REST API-Schlüssel-Token

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

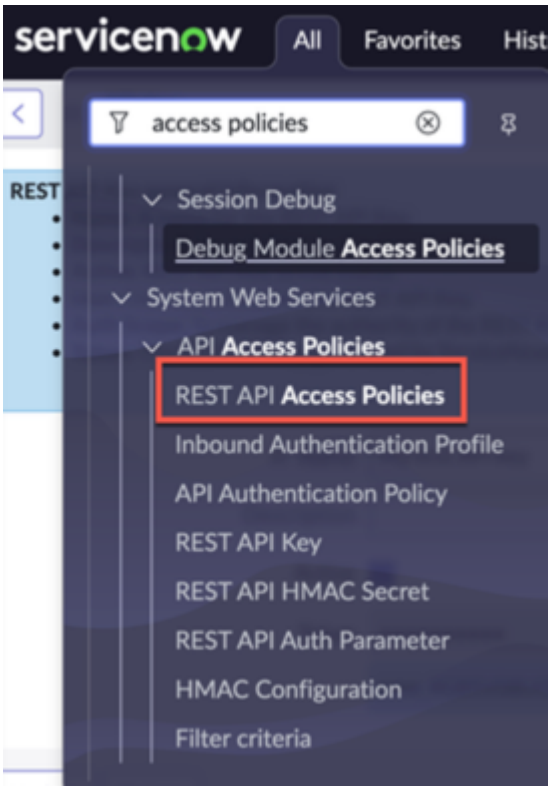
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Hinweis: Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

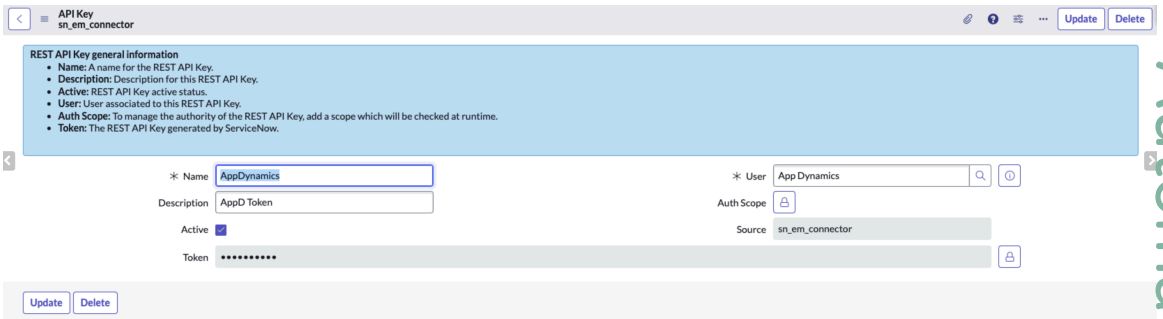
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Catchpoint-Ereignisse integrieren

Integrieren Sie Catchpoint mit Ereignismanagement, indem Sie auf der Catchpoint-Plattform einen Warnungs-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen aus Catchpoint, indem Sie Catchpoint als Datenquelle authentifizieren. Legen Sie auf der Catchpoint-Plattform die ServiceNow AI Platform mit einem Webhook als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie auf der Catchpoint-Plattform ein Warnungs-Webhook-Ziel.

   a. Melden Sie sich bei der Catchpoint-Plattform an.

   b. Navigieren zu **Catchpoint** > **Einstellung** > **API** > **Warnungsdaten-Webhook** Zum Festlegen des Webhook-Endpunkts.

   c. Geben Sie im API Alert Webhook (API-Warnungs-Webhook) die folgenden Details an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „API Alert Webhook“ (API-Warnungs-Webhook)

Feld	Wert
Name	Beliebiger Name basierend auf Ihren Anforderungen.
URL	Das Standardformat der URL zum Übertragen von Ereignissen von Catchpoint an die ServiceNow AI Platform-Instanz ist https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=catchpoint.
On Failure Alert (Bei Fehlerwarnung)	E-Mail-Adresse für den API-Warnungs-Webhook.
Notification Trigger (Benachrichtigungsauslöser)	Wählen Sie diesen je nach Ihren Anforderungen aus. Der Standardwert ist 3.
Add the following headers (Folgende Header hinzufügen)	▪ Autorisierung: **Basic {Base 64 | username:password}** ▪ Inhaltstyp: **application/json**
Format	Wählen Sie **Vorlage** aus, und fügen Sie die folgende Vorlage hinzu: { "Source": "CatchPoint", "severity": "${notificationLevelId}", "alertType": "${AlertType}", "time_of_event": "${alertCreateDateUtc(YYYY-MM-DD HH:MI:SS)}", "monitorType": "${Switch(${MonitorTypeId},'0', 'IE','2', 'Object','3','Emulated','8', 'Ping','9', 'Tracert','10', 'DNS-Traversal','11', 'Ping-TCP','12', 'DNS-Exp', '13','DNS-Direct', '14','Tracert-UDP', '15', 'Port-TCP','16', 'FTP','17', 'Data-Push-API','18', 'Chrome','19', 'Playback', '20', 'Playback-Mobile', '21', 'SMTP', '22', 'Port-UDP', '23', 'Ping-UDP', '24', 'Streaming', '25', 'API', '26', 'Mobile', '27', 'SFTP', '28', 'SSH', '29', 'Tracert-TCP')}", "testName": "${TestName}", "testId": "${TestId}", "testUrl": "${TestUrl}", "testPath": "${testPath}", "testLink": "${testLink}", "productName": "${ProductName}", "clientId": "${ClientId}", "productId": "${productId}", "nodeName":"${nodeDetails("${nodeName}")}",

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	"nodeClientServerAddress":"${nodeDetails(\"${NodeClientAddress},\"),}", "nodeServerAddress": "${nodeDetails(\"${nodeServerAddress},\"),}", "Labels" : "${testLabels}", "addtionalInformation": "Test initial URL: ${testUrl}\n\nAlert type: ${AlertType}\n\nScatter Chart: ${scatterplotChartURL}\n\nWaterfall Chart: ${waterfallChartURL}\n\nTest properties: ${testLink}\n\nTest time of run / Test time of alert (Central Time): ${reportDateLocal(YYYY-MM-DD HH:MI:SS)} / ${alertCreateDateLocal(YYYY-MM-DD HH:MI:SS)}"}

2. Erstellen Sie für die Tests zur HTTP-Endpunktüberwachung in der ServiceNow-Instanz ein CI (Configuration Item).

   Hinweis: Der Catchpoint-Connector bietet Unterstützung für mehrere Arten von Überwachungstests wie Endpunkt, Netzwerk und andere. Die folgenden Schritte gelten nur für die Tests zur HTTP-Endpunktüberwachung.

   a. Navigieren zu **Konfiguration** > **CI-Klassen Manager**an.

   b. Klicken Sie auf **Hierarchie** und suchen Sie nach **HTTP(S)-Endpunkt**.

   c. Wählen Sie im Feld „CI-Typ“ **cmdb_ci_endpoint_http** aus.
   Wenn die Services nicht modelliert werden, sollten Sie die CIs manuell unter der Tabelle [cmdb_ci_endpoint_http] hinzufügen. Außerdem sollte der manuelle Endpunkt vor der automatischen Erkennung von Services entfernt werden. Für CI-Bindungen anderer Typen von Tests können Sie Ereignisregeln basierend auf den jeweiligen Anforderungen erstellen.

Ergebnis

Die Übertragung von Warnungen vom Catchpoint-Connector in das Plugin „Event Management“ beginnt. Aus folgender Tabelle ist ersichtlich, wie die Zuordnung des Catchpoint-Schweregrads in die Zuordnung im ServiceNow-System übertragen wird.

Vergleich der Schweregradstufen zwischen Catchpoint und ServiceNow

Catchpoint-Schweregrad	ServiceNow-Schweregrad
0	Warnung
1	Kritisch
2/3	Leeren

Integrieren Datadog Plattformereignisse

Integrieren Sie Datadog mit Ereignismanagement, indem Sie der Datadog-Konsole einen Standard-Webhook hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Welche Authentifizierung wird verwendet?

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung wird mit durchgeführt Datadog V1- oder V2-Zugriffstoken überwachen. Weitere Informationen finden Sie unter Integrieren Datadog Mit OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Standardstandard der Authentifizierung, ohne dass dies erforderlich ist Datadog Active Directory. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE oder nützlich sein DevOps Teams. Weitere Informationen finden Sie unter Integrieren Datadog Mit Standardauthentifizierung.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Integrieren Datadog Mit Standardauthentifizierung

Integrieren Sie Datadog mit Ereignismanagement, indem Sie der Datadog-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

- Erforderliche Rolle: evt_mgmt_integration
- Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.
- Vergewissern Sie sich, dass Konfigurationselemente für die von Datadog verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Datadog. Legen Sie in Ihrer Datadog-Konsole die ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Prozedur

1. In Datadog Konsole, Cloud-Provider-Tags hinzufügen:
   a. Navigieren zu **Menü** > **Infrastruktur** > **Infrastrukturliste**
   b. Klicken Sie Auf **Überprüfen** Für die VM, auf der Datadog Agent ist installiert.
   c. Klicken Sie auf **Tags bearbeiten**. und fügen Sie das Tag `cloud_provider` hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dem Tag sollte ein Suffix mit dem Wert **aws**, **azure** oder **gcp** vorangestellt werden, um die AWS-, Microsoft Azure- oder Google Cloud Platform (GCP)-Anbieteroptionen zu identifizieren. Beispiel: cloud_provider:aws

d. Klicken Sie auf **Tags speichern**, um das neue Tag zu speichern.

Hinweis: Datadog Fügt hinzu `Cloud_Provider` Tag standardmäßig, wenn die Azure- und Google-Integration auf installiert ist Datadog Service Desk-Mitarbeiter. Tags können auch auf Cloud-Provider-Ebene hinzugefügt werden. Datadog Sammelt alle Tags, die auf VM-Ebene in der Cloud definiert sind.

2. In Datadog Konsole, fügen Sie einen Webhook hinzu:

a. Navigieren zu **Menü** > **Integration** > **Integrationen**, Und suchen Sie nach Webhooks.

b. Erstellen Sie einen Webhook, der die Benutzer-ID und das Passwort des ServiceNow-Benutzers im Endpunkt enthält.
Verwenden Sie beispielsweise https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=datadog.

Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

c. Fügen Sie ihn in der folgenden Nutzlaststruktur hinzu.

```
{
   "body": "$EVENT_MSG",
   "last_updated": "$LAST_UPDATED",
   "event_type": "$EVENT_TYPE",
   "title": "$EVENT_TITLE",
   "date": "$DATE",
   "org": {
      "id": "$ORG_ID",
      "name": "$ORG_NAME"
   },
   "id": "$ID",
   "alert_id": "$ALERT_ID",
   "alert_metric": "$ALERT_METRIC",
   "metric_namespace": "$METRIC_NAMESPACE",
   "alert_priority": "$ALERT_PRIORITY",
   "alert_transition": "$ALERT_TRANSITION",
   "alert_status": "$ALERT_STATUS",
   "alert_title": "$ALERT_TITLE",
   "alert_type": "$ALERT_TYPE",
   "host_name": "$HOSTNAME",
   "priority": "$PRIORITY",
   "tags": "$TAGS",
   "alert_scope": "$ALERT_SCOPE"
}
```

3. In Datadog Konsole, Regeln definieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Menü** > **Monitore** > **Überwachungen Verwalten**, Und konfigurieren Sie Regeln darüber, wann ein Problem aus erstellt werden soll Datadog Auf den verwalteten Hosts.

b. Wählen Sie im Abschnitt **Notify your team** (Team benachrichtigen) den Webhook aus, für den das Problem gemeldet werden soll.

Ergebnis

Warnungen beginnen ab zu fließen Datadog Service Desk-Mitarbeiter in das Ereignismanagement-Plugin. Das Plugin extrahiert Informationen aus der ursprünglichen Datadog-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für aktiviert Datadog Ereignisse für (AWS/ Azure/ GCP) Anbieter. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Event-Regel **Datadog - Allgemein** aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Datadog Mit OAuth-Authentifizierung

Integrieren Datadog Mit Ereignismanagement Durch Authentifizierung Datadog V1- oder V2-Token in DatadogÜberwachen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.

Vergewissern Sie sich, dass Konfigurationselemente für die von Datadog verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Datadog Die Integration mit OAuth-Authentifizierung ist ab verfügbar Washington DC Plattformversion oder höher.

Prozedur

1. Konfiguration auf der ServiceNow Instanz.

a. Erstellen `glide.oauth.inbound.client.credential.grant_type.enabled`Systemeigenschaft zur Verwendung des Gewährungstyps „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen.

- Typ: true|false
- Wert: true

b. Erstellen Sie einen OAuth-Entitätsendpunkt, damit Clients auf die Instanz zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und wählen Sie dann aus **Neu** .

ii. Wählen Sie auf der Seite „Interceptor“ die Option aus **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** Und füllen Sie dann das Formular aus.

iii. Um einen OAuth-Client-Datensatz zu erstellen, wählen Sie aus **Übermitteln** .

c. Fügen Sie dem erstellten OAuth-Client-Datensatz den OAuth-Anwendungsanwender und den Standardgewährungstyp hinzu.

i. Fügen Sie im Formular „OAuth-Entität“ hinzu **OAuth-Anwendungsanwender** Und **Standardgewährungstyp** Felder zur Verwendung des Gewährungstyps „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen.

ii. Öffnen Sie den erstellten OAuth-Client-Datensatz.

iii. Wählen Sie im Seitenheader die Option aus **Mehr** Symbol „Optionen“.

iv. Auswahlvorgang **Konfigurieren** > **Formularlayout**

v. Fügen Sie auf der Seite „Formularlayout“ hinzu **OAuth-Anwendungsanwender und Standardgewährungstyp** Aus der Liste der Felder.

vi. **Speichern** Oder **Aktualisieren** Das Formular.

vii. Für **OAuth-Anwendungsanwender** Wählen Sie den Anwender aus.

Der Anwender muss über die Rolle „evt_mgmt_Integration“ verfügen, die zum Erstellen der von gesendeten Ereignisse verwendet wird Datadog.

Hinweis: Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

viii. Festlegen **Standardgewährungstyp** Feldwert bis **Client-Anmeldeinformationen** .

2. In Datadog Konsole, fügen Sie Cloud-Provider-Tags hinzu.

a. Navigieren zu **Menü** > **Infrastruktur** > **Infrastrukturliste**an.

b. Wählen Sie Aus **Überprüfen** Für die VM, auf der Datadog Agent ist installiert.

c. Wählen Sie Aus **Bearbeiten Sie Tags** Und fügen Sie das Cloud_Provider-Tag hinzu.

Das Tag muss mit dem Wert aws, Azure oder gcp als Suffix versehen sein, um die Anbieteroptionen AWS, Microsoft Azure oder Google Cloud Platform (GCP) zu identifizieren. Beispiel: Cloud_Provider:aws.

d. Wählen Sie Aus **Speichern Sie Tags** .

Hinweis: Datadog Fügt standardmäßig das Cloud_Provider-Tag hinzu, wenn die Azure- und Google-Integration auf installiert ist Datadog Service Desk-Mitarbeiter. Tags können auch auf Cloud-Provider-Ebene hinzugefügt werden. Datadog Sammelt alle Tags, die auf VM-Ebene in der Cloud definiert sind.

3. Fügen Sie in der Datadog-Konsole einen Webhook hinzu:

a. Navigieren zu **Menü** > **Integration** > **Integrationen** Und suchen Sie nach Webhooks.

b. Wählen Sie auf der Webhook-Kachel aus **Konfigurieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie aus **Authentifizierungsmethoden** Registerkarte und wählen Sie dann aus **Neue Authentifizierungsmethode** .

d. Geben Sie den Namen ein, und wählen Sie das Protokoll als aus **OAuth 2,0-Client-Anmeldeinformationen** .

e. Geben Sie die Zugriffstoken-URL als an https://<instance_name>.service-now.com/oauth_token.do .

f. Geben Sie den Wert für an **Client-ID** Mit der Client-ID des in erstellten OAuth-Entitäts-Clients ServiceNow Instanz.

g. Geben Sie „Client-Geheimnis“ mit dem Client-Geheimnis des in erstellten OAuth-Entitäts-Clients an ServiceNow Instanz.

h. Wählen Sie **Speichern**.

i. Erstellen Sie die Webhook-URL als

https://<Instanzname>.service-now.com/api/sn_em_connector/em/inbound_event?source=datadog

j. Wählen Sie die in den vorherigen Schritten erstellte OAuth-Methode in der Dropdown-Liste „AuthMethod“ aus.

k. Fügen Sie ihn in der folgenden Nutzlaststruktur hinzu.

```
{
   "body": "$EVENT_MSG",
   "last_updated": "$LAST_UPDATED",
   "event_type": "$EVENT_TYPE",
   "title": "$EVENT_TITLE",
   "date": "$DATE",
   "org": {
      "id": "$ORG_ID",
      "name": "$ORG_NAME"
   },
   "id": "$ID",
   "alert_id": "$ALERT_ID",
   "alert_metric": "$ALERT_METRIC",
   "metric_namespace": "$METRIC_NAMESPACE",
   "alert_priority": "$ALERT_PRIORITY",
   "alert_transition": "$ALERT_TRANSITION",
   "alert_status": "$ALERT_STATUS",
   "alert_title": "$ALERT_TITLE",
   "alert_type": "$ALERT_TYPE",
   "host_name": "$HOSTNAME",
   "priority": "$PRIORITY",
   "tags": "$TAGS",
   "alert_scope": "$ALERT_SCOPE"
}
```

Ergebnis

Warnungen beginnen ab zu fließen Datadog Service Desk-Mitarbeiter in Ereignismanagement Plugin. Das Plugin extrahiert Informationen aus der ursprünglichen Datadog-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. In Ihrem ServiceNow AI Platform Instanz navigieren Sie zu alle Ereignisse, um die Ereignisse anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Standardmäßig ist die Hostbindung für aktiviert Datadog Ereignisse für (AWS/ Azure/ GCP) Anbieter. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dies zu beheben, müssen Sie aktivieren Datadog– Allgemeine Ereignisregel. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Google Cloud Platform (GCP)-Events integrieren

Integrieren Sie Google Cloud Platform (GCP) mit Ereignismanagement, indem Sie der GCP-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.
- Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.
- Vergewissern Sie sich, dass Konfigurationselemente für die von GCP verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.
- Das Plugin „Ereignismanagement Connector“ unterstützt nur GCP-Warnungsdaten im JSON 1.2-Format.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus GCP. Legen Sie in Ihrer GCP-Konsole die ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Fügen Sie in der GCP-Konsole einen Webhook hinzu:

   a. Navigieren zu **Überwachung** > **Warnungen**, Und klicken Sie auf **Bearbeiten Sie Benachrichtigungskanäle** .

   b. Klicken Sie im Abschnitt „Webhooks“ auf **Neu hinzufügen**.

   c. Aktivieren Sie das Kontrollkästchen **Use HTTP Basic Auth (HTTP-Standardauthentifizierung verwenden)**, und geben Sie Benutzername und Passwort des entsprechenden ServiceNow-Benutzers ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

d. Geben Sie die Endpunkt-URL ein.
Verwenden Sie zum Beispiel https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=googlemonitor .

2. Erstellen Sie in der GCP-Konsole eine Warnungsrichtlinie.

a. Navigieren zu **Überwachung** > **Warnungen**, Und wählen Sie aus **Richtlinie Erstellen** .

b. Konfigurieren Sie Richtlinienbedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.

c. Wählen Sie den Webhook aus, für den das Problem gemeldet werden soll.

> **Hinweis:** Wenn Sie einen Incident direkt in öffnen müssen GCP Konsole Navigieren Sie in der Warnung zu **Schnelle Antwort (in Warnung)** > **Incident in GCP-Konsole anzeigen**an.

Ergebnis

Die Übertragung von Warnungen von GCP in das Plugin Event Management beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen GCP-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Alle Ereignisse** Um die Ereignisse anzuzeigen.

Von GCP werden in der Nutzlast keine Werte wie der Schweregrad gesendet. Der Standardschweregrad ist gering, Die in geändert werden kann `Push Connector Configuration`Abschnitt von **Push-Connectors** > **Google Monitor-Push-Connector**an. Die gültigen Werte für den Schweregrad sind **1: Kritisch** , **2: Schwerwiegend** , **3 – Geringfügig** , **4: Warnung** , Und **5: Informationen** .

> **Hinweis:**
>
> Um zuzuordnen GCP Hosts für **cmdb_ci_Server** Datensatz anstelle von **cmdb_ci_vm_object** , Deaktivieren Sie **Google Monitor: Allgemein** Ereignisregel für erstellt GCP. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Event-Erfassung von Google Cloud Platform (GCP)

Mit dem MID WebService-Event-Sammler können Sie Event-Nachrichten im JSON-Format erfassen, die vom Google Cloud Platform (GCP) gesendet wurden.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Siehe MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Event-Nachrichten im JSON-Format werden von Google Cloud Platform gesendet. Die MID-Server Wandelt die gesammelten Ereignisnachrichten um, indem sie mithilfe der Skripteinbindung TransformEvents_MidGoogleMonitor analysiert werden, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**an. Klicken Sie auf der Seite „Push-Connectors“ auf **Google Monitor Mid Push Connector**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von GCP auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidGoogleMonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Anwenders des MID-Webservers.

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung.

Prozedur

1. Stellen Sie in der Google Cloud Platform (GCP)-Konsole sicher, dass die MID Server-IP von der GCP-Konsole und der MID-REST-Punkt von GCP aus zugänglich ist, oder installieren Sie den MID-Server auf einer GCP-VM, und geben Sie die externe IP-Adresse der GCP-VM in der URL an.
   Erstellen Sie in der GCP-Konsole eine Firewall-Regel.
   a. Navigieren zu **VPC-Netzwerk** > **Firewall** > **Firewall erstellen**an.
   b. Legen Sie die Richtung auf **Eingehend** fest, damit mid_web_server_port eine Verbindung herstellen kann.
   c. Fügen Sie die GCP-VM, auf der MID-Server installiert ist, der Liste **Applicable to instances** (Anwendbar auf Instanzen) hinzu.
2. Fügen Sie in der GCP-Konsole einen Webhook hinzu:
   a. Navigieren zu **Überwachung** > **Warnungen** Und klicken Sie auf **Bearbeiten Sie Benachrichtigungskanäle** .
   b. Klicken Sie im Abschnitt „Webhooks“ auf **Neu hinzufügen**.
   c. Aktivieren Sie das Kontrollkästchen **Use HTTP Basic Auth** (HTTP-Standardauthentifizierung verwenden), und geben Sie Benutzername und Passwort des entsprechenden MID Webserver-Benutzers ein.

   Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Geben Sie die Endpunkt-URL ein.
Verwenden Sie zum Beispiel http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidGoogleMonitor.

3. Erstellen Sie in der GCP-Konsole eine Warnungsrichtlinie.

a. Navigieren zu **Überwachung** > **Warnungen** Und klicken Sie auf **Richtlinie Erstellen** .

b. Konfigurieren Sie Richtlinienbedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.

c. Wählen Sie den Webhook-Benachrichtigungskanal aus, für den das Problem gemeldet werden soll.

d. Aktivieren Sie das Kontrollkästchen **Notify on incident closure** (Beim Schließen des Incident benachrichtigen), um die Abschluss-Events an MID-Server zu senden und die Warnungsrichtlinie zu speichern.

Hinweis: Wenn Sie einen Incident direkt in öffnen müssen GCP Konsole Navigieren Sie in der Warnung zu **Schnelle Antwort (in Warnung)** > **Incident in GCP-Konsole anzeigen**an. Weitere Informationen zum Erstellen einer Warnungsrichtlinie finden Sie unter Warnungsrichtlinien verwalten auf der Google Cloud-Dokumentationswebsite.

Ergebnis

GCP sendet keine Werte wie den Schweregrad an die Payload. Der Standardschweregrad ist gering, der in geändert werden kann *Push Connector Configuration*Abschnitt von **Push-Connectors** > **Google Monitor MID-Push-Connector**an. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

Grafana-Events integrieren

Integrieren Sie Grafana mit Ereignismanagement, indem Sie der Grafana-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.
- Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.
- Die CI-Bindung erfolgt über die IP, Instanzen müssen als Server erkannt werden, um die Bindung zu initiieren. Über die Cloud oder CIs in erkannte CIs **cmdb_ci_vm_object** Nicht begrenzt werden, da Grafana keine Informationen für Objekt-IDs bereitstellt.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Grafana. Legen Sie in Ihrer Grafana-Konsole die ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhook als REST-Endpunkt fest.

Hinweis: Führen Sie die Schritte 1 und 2 für Grafana v7.4.3 aus. Für Grafana v9.3.2. Fahren Sie mit Schritt 3 fort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Grafana v7.4.3

1. Erstellen Sie in Ihrer Grafana-Konsole einen Benachrichtigungskanal.

   a. Navigieren zu **Warnungen** > **Benachrichtigungskanäle**an.

   b. Klicken Sie auf **Neuer Kanal**, und wählen Sie als Typ **Webhook** aus.

   c. Geben Sie eine URL ein.
   Verwenden Sie beispielsweise https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=grafana.

   d. Unter **Optionaler Webhook** Einstellungen, wählen Sie die HTTP-Methode aus, **VERÖFFENTLICHEN** , Und geben Sie den Anwendernamen und das Passwort des entsprechenden ein ServiceNow Anwender.

   Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   e. Klicken Sie auf **Test**, um die Verbindung zu testen.

2. Erstellen Sie in der Grafana-Konsole Warnungsregeln.

   a. Klicken Sie im erforderlichen Bereich auf **Bearbeiten** und dann auf **Warnung erstellen**.

   b. Fügen Sie auf der Registerkarte **Warnung** die folgenden Tags hinzu:

Tags	Beschreibung
Schweregrad	(Dieses Tag ist optional und muss in kleinerer Groß-/Kleinschreibung liegen.) Schweregrad, mit dem die Warnung erstellt werden muss.
Anzahl	(Dieses Tag ist erforderlich, andernfalls werden die Warnungen in nicht automatisch geschlossen ServiceNow.) Die Anzahl der Geräte, Hosts oder Server, die von dieser Warnungsregel überwacht werden.

   c. Fügen Sie den Benachrichtigungskanal unter **Benachrichtigungen** in der Warnungsregel hinzu.

   d. Klicken Sie auf **Speichern**.

   e. Navigieren zu **Warnungen** > **Warnungsregeln** Um auf die erstellte Regel zuzugreifen.

Grafana v9.3.2.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie in der Grafana-Konsole einen Kontaktpunkt.

   a. Navigieren zu **Warnungen** > **Kontaktpunkte**an.

   b. Klicken Sie Auf **Neuer Kontaktpunkt** Geben Sie einen Namen ein, und wählen Sie den Typ aus **Webhook** .

   c. Geben Sie eine URL ein.
   Verwenden Sie beispielsweise https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=grafana.

   d. Unter **Optionaler Webhook** Einstellungen, wählen Sie die HTTP-Methode aus, **VERÖFFENTLICHEN** , Und geben Sie den Anwendernamen und das Passwort des entsprechenden ein ServiceNow Anwender.

   Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   e. Klicken Sie Auf **Speichern** Und **Testen** Dient zum Überprüfen der Verbindung.

4. Erstellen Sie in der Grafana-Konsole eine Benachrichtigungsrichtlinie.

   a. Navigieren zu **Warnungen** > **Benachrichtigungsrichtlinien**an.

   b. Wählen Sie Aus **Neue Richtlinie** , Fügen Sie Matcher hinzu.
   Übereinstimmungen sind Bezeichnungen, die Warnungsregeln an den Kontaktpunkt weiterleiten.

   c. Wählen Sie Ihren Kontaktpunkt aus.

   d. Wählen Sie Aus **Richtlinie Speichern** .

5. Erstellen Sie in der Grafana-Konsole Warnungsregeln.

   a. Navigieren zu **Warnungen** > **Warnungsregel**an.

   b. Wählen Sie Aus **Neue Regel** .

   c. Legen Sie die Abfrage- und Warnungsbedingung fest.

   d. Legen Sie die Datenquelle, Metriken und die erforderlichen Filter fest.

   e. Legen Sie das Verhalten der Warnungsauswertung fest.

   f. Geben Sie den Regelnamen ein.

   g. Fügen Sie im Abschnitt „Zusammenfassung und Anmerkungen“ eine Zusammenfassung oder Beschreibung hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Wählen Sie im Scrollen nach unten aus **+Neu Hinzufügen** .

i. Geben Sie den Knoten, die Ressource und die Metrikinformationen ein.
Diese Informationen sind für die Felder „Knoten“, „resource“ und „metric_Name“ für das Ereignis erforderlich.

Hinweis: Verwenden Sie die Wertzeichenfolge, um diese Werte zu übergeben. Ein Knoten kann beispielsweise {{ $values.C0.Labels.instance }} sein.

j. Geben Sie unter anwenderdefinierte Bezeichnungen die erforderlichen Bezeichnungen an, um Ihre Benachrichtigungen an den entsprechenden Kontaktpunkt zu leiten.

Hinweis: Sie können den Schweregrad auch unter anwenderdefinierten Bezeichnungen übergeben. Dasselbe wird für Ereignisse verwendet. Die verfügbaren Schweregradoptionen sind: Kritisch, schwerwiegend, gering, Warnung.

k. Klicken Sie auf **Speichern**.

Ergebnis

Die Übertragung von Warnungen von Grafana in das Plugin Event Management beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Grafana-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Hinweis:

- Für Grafana v7.4.3 werden möglicherweise zusätzliche klare Ereignisse angezeigt, die in eingehen ServiceNow Die nicht an eine Warnung gebunden sind. Ignorieren Sie sie, da sie erstellt wurden, um das Problem zu beheben, dass Grafana keine Informationen in der eindeutigen Benachrichtigung sendet.
- Ein Schweregradparameter wird hinzugefügt, der nur für Grafana 8 und höher verwendet wird. Der angegebene Wert wird als Schweregrad für ein Ereignis verwendet, wenn der Schweregrad nicht in anwenderdefinierten Bezeichnungen übergeben wird.

Integrieren Sie Grafana mit REST API-Schlüssel-Token

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

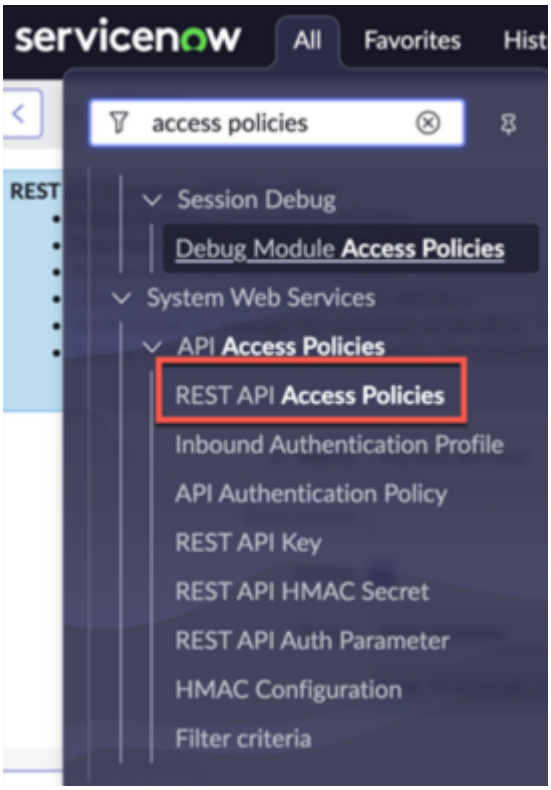
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

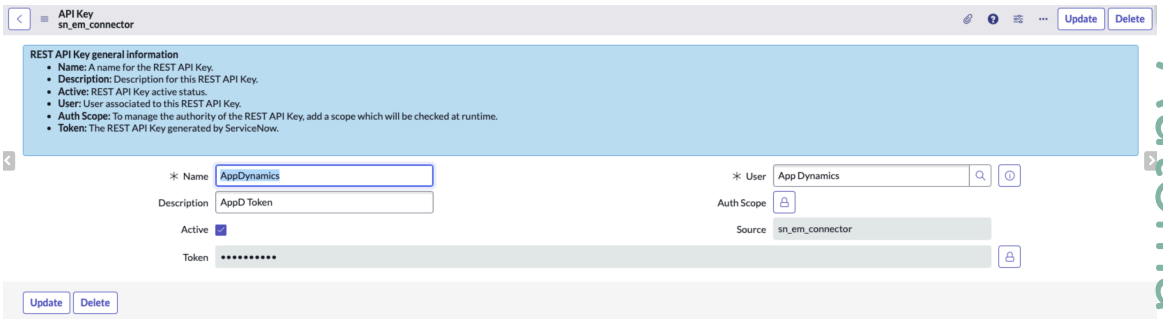
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Honeycomb-Ereignisse integrieren

Integrieren Sie Honeycomb mit Ereignismanagement, indem Sie einen Webhook erstellen und ihn auf der Honeycomb-Plattform als Auslöser konfigurieren.

Vorbereitungen

Discovery für Honeycomb-Services und -Datensätze wird nicht unterstützt. Damit die Ereignis-/CI-Bindung funktioniert, erstellen Sie in der ServiceNow-Instanz manuell ein CI (Configuration Item).

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen von Honeycomb, indem Sie Honeycomb als Datenquelle authentifizieren. Legen Sie auf der Honeycomb-Plattform die ServiceNow AI Platform mit einem Webhook als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie auf der Honeycomb-Plattform eine Integration von `type=webhook`.
   a. Navigieren zu **Monatlich** > **Integrationen**an.
   b. Klicken Sie auf die Schaltfläche **Add Integration** (Integration hinzufügen).
   c. Geben Sie Werte in die Felder **Name** und **Webhook URL** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie beim Eingeben der Webhook-URL das folgende Format: https://<USERNAME>:<PASSWORD>@<INSTANCE_NAME>.service-now.com/api/sn_em_connector/em/inbound_event?source=honeycomb.

d. Wählen Sie im Feld **Provider** (Anbieter) die Option **Webhook** aus.

e. Wählen Sie **Add** (Hinzufügen), um die Webhook-Erstellung abzuschließen.

2. Fügen Sie den Webhook einem Auslöser hinzu.

a. Navigieren zu **Wiederholungen** > **Neuen Auslöser erstellen**an.

b. Fügen Sie in den entsprechenden Feldern einen Namen und eine Beschreibung für den Auslöser hinzu.

c. Konfigurieren Sie im Abschnitt **Alerts** (Warnungen) den Schwellenwert und die Häufigkeit in den entsprechenden Feldern.

d. Wählen Sie im Abschnitt **Recipients** (Empfänger) die Option **Add Recipient** (Empfänger hinzufügen) aus, und wählen Sie den in Schritt 1 erstellten Webhook aus.

e. Wählen Sie **Save Trigger** (Auslöser speichern) aus.

Hinweis: Um den Auslöser auf der Honeycomb-Plattform anzuzeigen, navigieren Sie zu **Quick Response (in Alert)** (Schnelle Antwort (in Warnung)), und wählen Sie **Show Trigger in Honeycomb** (Auslöser in Honeycomb anzeigen) aus.

Ergebnis

Warnungen werden vom Honeycomb-Connector in das Ereignismanagement-Plugin weitergeleitet. Vom Plugin werden Informationen aus der ursprünglichen Honeycomb-Auslösermeldung zum Füllen der erforderlichen Ereignisfelder extrahiert. Außerdem wird das Ereignis in die Datenbank eingefügt. Sie können die Ereignisse in der ServiceNow AI Platform-Instanz anzeigen, indem Sie zu **Alle Ereignisse** navigieren.

In der Auslösermeldung werden von Honeycomb keine Informationen zum Schweregrad gesendet. Der Standardschweregrad für die Honeycomb-Warnung ist `3 - Minor`, Die im Abschnitt „Push-Connector-Konfiguration“ von geändert werden kann **Push-Connectors** > **Honeycomb-Push-Connector** . Die gültigen Schweregrade lauten: `1- Critical`, `2- Major`, `3- Minor`, `4- Warning` und `5- Info`.

Instana-Events integrieren

Integrieren Sie Instana mit Ereignismanagement, indem Sie der Instana-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie in der Instana-Konsole zu **Einstellungen** > **Ereignisse Und Warnungen** > **Warnungskanäle**an.

2. Öffnen Sie die Dropdown-Liste **Add Alert Channel** (Warnungskanal hinzufügen) und wählen Sie die Option **Generic Webhook** (Generischer Webhook) aus.

3. Erstellen Sie im Feld **Webhook-URLs** einen Warnungskanal, indem Sie die folgende URL eingeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

https://<instance>.service-now.com/api/sn_em_connector/em/inbound_event?source=instana

4. Um die ServiceNow-URL zu authentifizieren, geben Sie unter **Custom HTTP Request Headers** (Benutzerdefinierte HTTP-Anforderungsheader) Folgendes ein:

Feld	Wert
Schlüssel	Autorisierung
Wert	Standard <base64_encoded username:password>

5. Konfigurieren Sie Instana, um Warnungen für Event-Typen oder Events zu erstellen.

   a. Navigieren zu **Einstellungen** > **Ereignisse Und Warnungen** > **Alerts**an.

   b. Wählen Sie **New Alert** (Neue Warnung) aus.

   c. Wählen Sie im Abschnitt **Events** eine der folgenden Optionen aus:

      - Alert on Event Type(s) (Warnung zu Event-Typ(en))
      - Warnung zu Ereignis(sen)

   d. Beim Erstellen von Warnungen für Event-Typen:

      i. Wählen Sie den Typ der Events aus, für die Warnungen erstellt werden sollen, z. B. **Critical Issues** (Kritische Probleme), **Alle Incidents**, **Warning issues** (Warnungsprobleme) usw.

      ii. Wählen Sie im Abschnitt **Warnungen** den Warnungskanal **servicenow** aus.

   e. Beim Erstellen von Warnungen für Events:

      i. Wählen Sie die Events aus, für die Warnungen erstellt werden sollen.

      ii. Wählen Sie im Abschnitt **Warnungen** den Warnungskanal **servicenow** aus.

   Wenn Instana eine Warnung erstellt, wird die Warnung an die ServiceNow-Instanz gesendet. Für die Hostentität erstellte Warnungen werden an die Tabelle „Server“ (cmdb_ci_server) gebunden und für die Website-Entität erstellte Warnungen werden an die Tabelle „HTTP(S)“ (cmdb_ci_endpoint_http) gebunden.

   Fügen Sie der Tabelle „Instana – ci_type-Ereignis-Feldzuordnung“ weitere Entitätstypen hinzu, um sicherzustellen, dass die Entität mit dem richtigen CI in der ServiceNow-Instanz verbunden ist.

6. Um das Event im Instanza-Quellsystem anzuzeigen, können Sie über eine ServiceNow-Instanz darauf zugreifen:

   a. Navigieren zu **Alle** > **Ereignismanagement** > **Service Operations-Arbeitsbereich**an.

   b. Wählen Sie **Alle Warnungen** aus.

   c. Wählen Sie die entsprechende Warnung aus.

   d. Suchen Sie auf der Registerkarte **Details** rechts auf der Seite den Abschnitt **Aktionen** und wählen Sie in der Zelle **Show Event on Instana UI** (Event in Instana-UI anzeigen) die Option **App starten** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrieren ServiceNow Cloud Observability Ereignisse

Integrieren ServiceNow Cloud Observability Mit Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in ServiceNow Cloud Observability Plattform. Laden Sie herunter Ereignismanagement Connector-Plugin aus dem ServiceNow Store Damit Sie in integrieren können ServiceNow Cloud Observability.

Vorbereitungen

- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Authentifizieren ServiceNow Cloud Observability Als zu aktivierende Datenquelle Ereignismanagement Dient zum Sammeln von Ereignissen aus ServiceNow Cloud Observability. In Ihrem ServiceNow Cloud Observability Plattform verwenden Sie einen Standard-Webhook, um Ihren festzulegen ServiceNow AI Platform Instanz als Rest-Endpunkt.

Hinweis: Stellen Sie sicher, dass die Rolle „evt_mgmt_integration“ dem ausgewählten Benutzer zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Erstellen Sie ein CI.

Hinweis: Discovery für ServiceNow Cloud Observability Services werden nicht unterstützt. Erstellen Sie ein CI manuell in einer Serviceinstanz-Tabelle (cmdb_ci_Service_Auto), um die Bindung zu aktivieren.

a. Navigieren zu **Alle** > **Konfiguration** > **Anwendungsservice**an.

b. Wählen Sie **Neu**.

c. Geben Sie im Formular den Namen ein.
Der Name muss der in angegebene Servicename sein ServiceNow Cloud Observability Plattform.

d. Legen Sie in der Liste „Betriebsstatus“ den Betriebsstatus auf fest **Betriebsbereit** .

e. Wählen Sie **Weiter**.

f. Wählen Sie **Fertig**.

2. In Ihrem ServiceNow Cloud Observability Plattform: Erstellen Sie ein Benachrichtigungsziel.

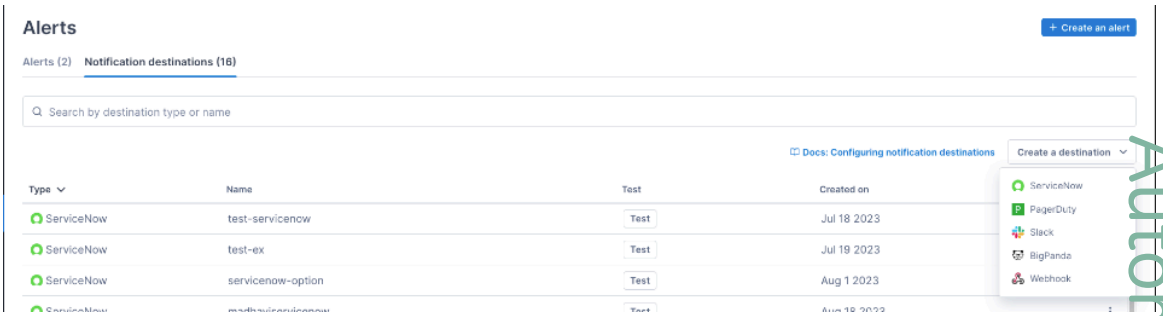
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie in der Navigationsleiste aus **Warnungen** .

b. Wählen Sie aus **Benachrichtigungsziele** Registerkarte.

c. Wählen Sie Aus **Erstellen Sie ein Ziel** .

d. Wählen Sie Aus **ServiceNow** Oder **Webhook** .
Verwenden Sie ServiceNow Ziel, das nur mit verbunden werden soll ServiceNow Plattform. Wenn Sie Probleme mit haben ServiceNow Ziel, dann verwenden **Webhook** Zieloption.



3. In Ihrem ServiceNow Cloud Observability Plattform, erstellen Sie eine ServiceNow Benachrichtigungsziel.

a. In **Name** Geben Sie einen Namen für ein ServiceNow Ziel.

b. In **URL** Feld, geben Sie an ServiceNow Instanz-URL.
Dies ist das Standardformat der URL, von der Ereignisse übertragen werden sollen ServiceNow Cloud Observability Zu ServiceNow AI Platform Instanz. Dieses Format verwenden: https//<instance-name>.servicenow.com/api/sn_em_connector/em/inbound_event?source=lightstep

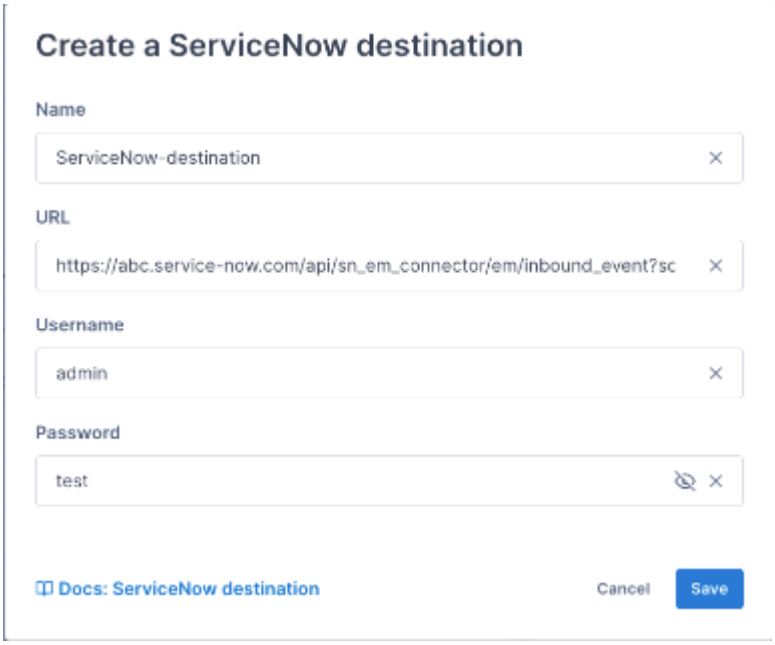
c. In **Anwendername** Geben Sie ein ServiceNow Anwendername.

d. In **Passwort** Geben Sie ein ServiceNow Anwenderpasswort.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein ServiceNow-Ziel



Hinweis: In einem ServiceNow Instanz, CI-Bindung erfolgt nur, wenn der Name des Service in der angegeben ist ServiceNow Cloud Observability Der Plattformwert stimmt mit den Namensfeldern des CI überein, das Sie in erstellt haben `cmdb_ci_service_auto`Tabelle.

e. Wählen Sie **Speichern**.

4. **Hinweis:** Wenn Sie Probleme mit haben ServiceNow Ziel im vorherigen Schritt, dann verwenden **Webhook** Zieloption.

In Ihrem ServiceNow Cloud Observability Plattform, erstellen Sie eine **Webhook** Benachrichtigungsziel.

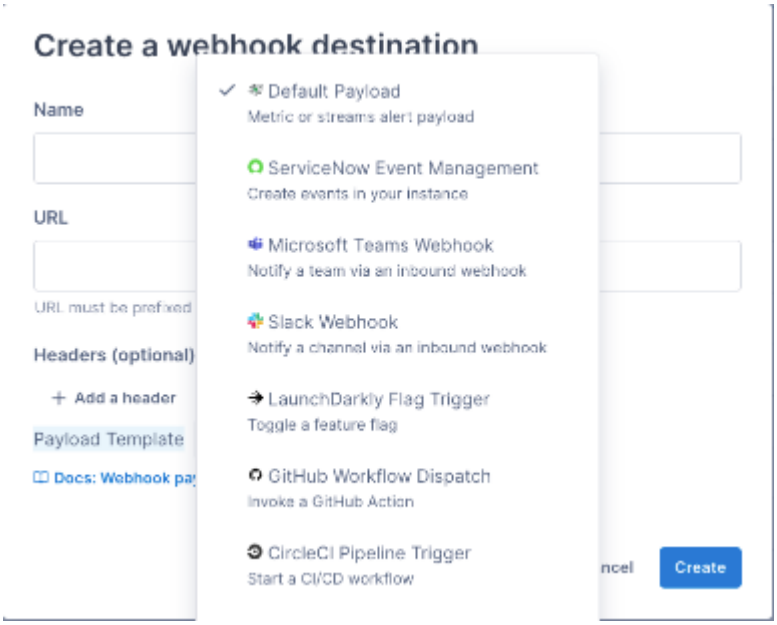
a. In **Name** Geben Sie einen Namen für ein Webhook Ziel.

b. In **URL** Geben Sie die Webhook-URL an.
Dies ist das Standardformat der URL, von der Ereignisse übertragen werden sollen ServiceNow Cloud Observability Zu ServiceNow AI Platform Instanz. Dieses Format verwenden: https//<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=lightstep

c. Wählen Sie Aus **Nutzlastvorlage** .

d. Wählen Sie aus **ServiceNow-Ereignismanagement** Option.

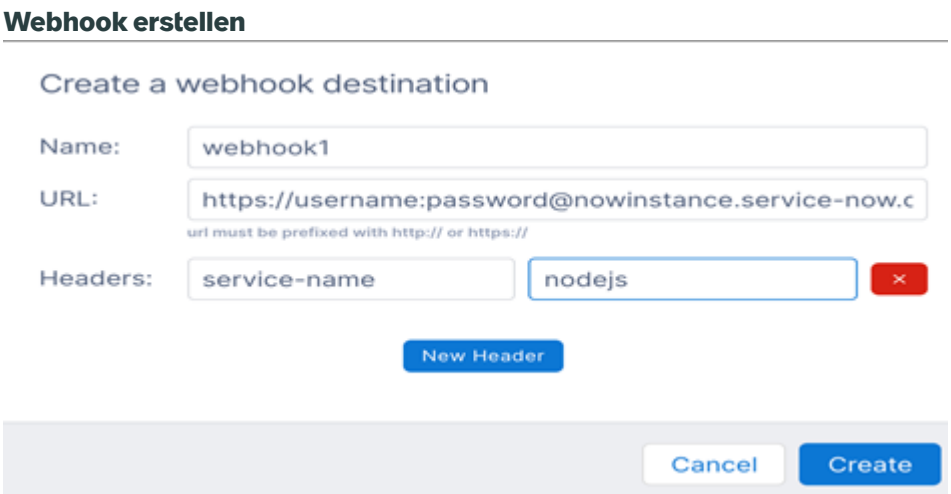
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: In einem ServiceNow Instanz, CI-Bindung erfolgt nur, wenn der Name des Service in der angegeben ist ServiceNow Cloud Observability Der Plattformwert stimmt mit den Namensfeldern des CI überein, das Sie in erstellt haben `cmdb_ci_service_auto`Tabelle.

e. Wenn Sie ausgewählt haben **Standardvorlage** Option im vorherigen Teilschritt, und wählen Sie dann aus **Neuer Header** Und in **Header** Geben Sie ein **Servicename** Und definieren Sie es **Wert** .

Hinweis: In einem ServiceNow Instanz, CI-Bindung erfolgt nur, wenn **Servicename** Der Headerwert stimmt mit den Namensfeldern des CI überein, das Sie in erstellt haben **Tabelle „cmdb_ci_Service_Auto“** .



f. Wählen Sie **Erstellen** aus.

5. In ServiceNow Cloud Observability Plattform, konfigurieren Sie eine Warnung.

a. Wählen Sie in der Navigationsleiste aus **Warnungen** .

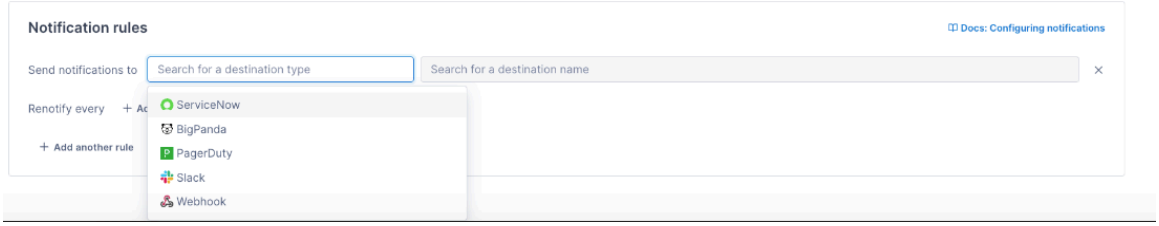
b. Wählen Sie Aus **Erstellen Sie eine Warnung** Und geben Sie einen Warnungsnamen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Definieren Sie im Bereich „Warnmeldungskonfiguration“ den Schwellenwert.

d. Entsprechend dem Ziel, das Sie in erstellt haben **Benachrichtigungsregeln** Bereich, in **Benachrichtigungen senden an** Wählen Sie Ihren Benachrichtigungszieltyp aus, und suchen Sie nach dem Zielnamen.



e. Wählen Sie **Speichern**.
Der Standardschweregrad für Stream-basierte Warnungen ist **Kritisch** . Sie können den Standard im Bereich Push-Connector-Konfiguration eines ändern ServiceNow AI Platform Instanz. Die gültigen Schweregradwerte sind:

- 1 - Kritisch
- 2 - Schwer
- 3 – Gering
- 4 – Warnung
- 5 - Info

Logicmonitor-Events integrieren

Integrieren Logicmonitor mit Ereignismanagement zum Senden von Ereignissen in ServiceNow, indem Sie einen Webhook mit Standardauthentifizierung hinzufügen. Dieser wird auch mit bidirektionaler Funktionalität zur Verfügung stehen.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.
- Das Plugin „Ereignismanagement“ muss in der ServiceNow AI Platform-Instanz installiert sein.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Logicmonitor. Legen Sie in Ihrer Logicmonitor-Konsole die ServiceNow AI Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie in der Logicmonitor-Konsole eine benutzerdefinierte HTTP Delivery-Integration.
   a. Navigieren zu **Einstellungen** > **Integrationen** Und klicken Sie auf **Hinzufügen** > **Anwenderdefinierte HTTP-Delivery-Integration**an.
   b. Füllen Sie im Formular „Manage Custom HTTP Delivery Integration“ die Felder **Name** und **Description** aus und aktivieren Sie das Kontrollkästchen **Use the same URL and data to notify on various alert activity**.
   c. Geben Sie durch die Auswahl der Kontrollkästchen **Acknowledged**, **Cleared** und **Escalated/De-escalated** an, wann eine Benachrichtigung über Alarmaktivitäten versendet werden soll.

      Hinweis: Wenn Sie das bidirektionale Connector-Update verwenden, wählen Sie nicht aus **Bestätigt** Kontrollkästchen. Dadurch kann eine Schleife zurück zur Warnung ausgelöst und der Warnungsdatensatz unbeabsichtigt geschlossen werden.

   d. Wählen Sie im Menü „HTTP Method“ die Option **HTTP POST** aus.
   e. Füllen Sie das Feld **Benutzername** und **Passwort** aus, und geben Sie eine URL im Format `https://{Instance-name}.service-now.com/api/sn_em_connector/em/inbound_event?source=logicmonitor` ein.
   f. Wählen Sie im Abschnitt „Alert Data“ die Option **Raw** aus, und wählen Sie das Format als **JSON** aus.
   g. Fügen Sie die benutzerdefinierte Nutzlast hinzu, die in der Beschreibung des Connectors angegeben ist.
   h. Klicken Sie auf **Test Alert Delivery**, um die Verbindung zu überprüfen, oder auf **Save**.
2. Wenn Sie mit dem Erstellen der Integration fertig sind, erstellen Sie eine Eskalationskette für die Warnungseinstellungen.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Eskalationsketten** Klicken Sie dann auf **Hinzufügen**.
   b. Füllen Sie im Formular „Manage Testing chain“ die Felder **Name** und **Description** aus, und wählen Sie die Rate aus, mit der über die Warnungen benachrichtigt werden soll.
   c. Wählen Sie im Abschnitt „Stages“ das Hinzufügungssymbol , um eine Phase hinzuzufügen, und klicken Sie dann auf **Save**.
   d. Wenn Sie die neue Phase erstellen, wählen Sie erneut das Symbol zum Hinzufügen aus, um nach dem Benutzer zu suchen und die Integration als Kontaktmethode hinzuzufügen, und klicken Sie dann auf **Save**.
3. Nachdem Sie die Eskalationskette erstellt haben, konfigurieren Sie Warnungsregeln für die von Ihnen erstellte Kette.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Warnungsregeln**, Und klicken Sie auf **Hinzufügen** .
   b. Konfigurieren Sie im Fenster „Add Alert“ Bedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie im Menü „Escalation chain“ die von Ihnen erstellte Eskalationskette aus.

d. Klicken Sie auf **Speichern**.

Hinweis: Um das CI dem **cmdb_ci_vm_object**-Datensatz anstelle von **cmdb_ci_server** zuzuordnen, aktivieren Sie die für Logicmonitor erstellte Event-Regel. Der Sammlername des Logicmonitors, der als Hostname in der Payload eingeht, muss mit der object_id der virtuellen Maschine übereinstimmen, die im Datensatz **cmdb_ci_vm_object** erkannt wurde.

Event-Erfassung von Logicmonitor

Mit dem MID WebService-Eventsammler können Sie Event-Nachrichten im JSON-Format von Logicmonitor erfassen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Siehe MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

JSON-formatierte Event-Nachrichten werden von Logicmonitor gesendet. Die MID-Server Wandelt die gesammelten Ereignisnachrichten um, indem sie mithilfe der Skripteinbindung TransformEvents_MidLogicmonitor analysiert werden, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**an. Klicken Sie auf der Seite „Push-Connectors“ auf **Logicmonitor Mid Push-Connector**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von Logicmonitor auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidLogicmonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Benutzers des MID-Webservers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie in der Logicmonitor-Konsole eine benutzerdefinierte HTTP Delivery-Integration.
   a. Navigieren zu **Einstellungen** > **Integrationen** Und klicken Sie auf **Hinzufügen** > **Anwenderdefinierte HTTP-Delivery-Integration**an.
   b. Füllen Sie im Formular „Manage Custom HTTP Delivery Integration“ die Felder **Name** und **Description** aus und aktivieren Sie das Kontrollkästchen **Use the same URL and data to notify on various alert activity**.
   c. Geben Sie durch die Auswahl der Kontrollkästchen **Acknowledged**, **Cleared** und **Escalated/De-escalated** an, wann eine Benachrichtigung über Alarmaktivitäten versendet werden soll.
   d. Wählen Sie im Menü „HTTP Method“ die Option **HTTP POST** aus.
   e. Füllen Sie die Felder **Username** und **Password** aus, und geben Sie eine URL im Format `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidLogicmonitor` ein.
   f. Wählen Sie im Abschnitt „Alert Data“ die Option **Raw** aus, und wählen Sie das Format als **JSON** aus.
   g. Fügen Sie die benutzerdefinierte Nutzlast hinzu, die in der Beschreibung des Connectors angegeben ist.
   h. Klicken Sie auf **Test Alert Delivery**, um die Verbindung zu überprüfen, oder auf **Save**.
2. Wenn Sie mit dem Erstellen der Integration fertig sind, erstellen Sie eine Eskalationskette für die Warnungseinstellungen.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Eskalationsketten** Klicken Sie dann auf **Hinzufügen**.
   b. Füllen Sie im Formular „Manage Testing chain“ die Felder **Name** und **Description** aus, und wählen Sie die Rate aus, mit der über die Warnungen benachrichtigt werden soll.
   c. Wählen Sie im Abschnitt „Stages“ das Hinzufügungssymbol , um eine Phase hinzuzufügen, und klicken Sie dann auf **Save**.
   d. Wenn Sie die neue Phase erstellen, wählen Sie erneut das Symbol zum Hinzufügen aus, um nach dem Benutzer zu suchen und die Integration als Kontaktmethode hinzuzufügen, und klicken Sie dann auf **Save**.
3. Nachdem Sie die Eskalationskette erstellt haben, konfigurieren Sie Warnungsregeln für die von Ihnen erstellte Kette.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Warnungsregeln**, Und klicken Sie auf **Hinzufügen** .
   b. Konfigurieren Sie im Fenster „Add Alert“ Bedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.
   c. Wählen Sie im Menü „Escalation chain“ die von Ihnen erstellte Eskalationskette aus.
   d. Klicken Sie auf **Speichern**.

Hinweis: Um das CI dem **cmdb_ci_vm_object**-Datensatz anstelle von **cmdb_ci_server** zuzuordnen, aktivieren Sie die für Logicmonitor erstellte Event-Regel. Der Sammlername des Logicmonitors, der als Hostname in der Payload eingeht, muss mit der object_id der virtuellen Maschine übereinstimmen, die im Datensatz **cmdb_ci_vm_object** erkannt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Cloud Infrastructure-Alarme integrieren

Integrieren Sie Oracle Cloud Infrastructure(OCI)-Alarme mit Ereignismanagement, um Events an das ServiceNow-System zu senden, indem Sie mithilfe der Standardauthentifizierung ein https-Abonnement hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.
- Oracle Cloud Discovery muss ausgeführt werden, damit gewährleistet ist, dass die erstellten Warnungen an die Konfigurationselemente auf der ServiceNow AI Platform gebunden sind. Weitere Informationen finden Sie unter Oracle Cloud Infrastructure-Discovery .
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Mit dem Oracle Cloud Notifications-Service können Sie Kommunikationskanäle zum Veröffentlichen von Nachrichten mithilfe von Themen und Abonnements einrichten. Wenn eine Nachricht in einem Thema veröffentlicht wird, wird die Nachricht vom Benachrichtigungsservice an alle Abonnements des Themas gesendet.

Wenn eine Oracle Management Cloud-Warnung ausgelöst wird, sich der Schweregrad dieser erhöht oder sie gelöscht wird, empfiehlt es sich, dass Sie aktiv über eine benutzerdefinierte https-URL an die ServiceNow-Instanz benachrichtigt werden. Der Oracle Cloud-Connector wird zum Erstellen von Events im ServiceNow®-System verwendet.

Sie können die Ereignismanagement-Umgebung für die Erfassung von Alarmen aus Oracle Cloud konfigurieren, indem Sie Ihre Instanz der ServiceNow AI Platform als https-Abonnement festlegen.

Prozedur

1. Richten Sie in der Oracle Cloud-Konsole ein https-Abonnement ein.

   a. Wählen Sie im Formular „Create Subscription“ (Abonnement erstellen) im Abschnitt „Configure Subscription“ (Abonnement konfigurieren) in der Liste „Protocol “ (Protokoll) die Option **HTTPS (Custom URL)** (HTTPS (Benutzerdefinierte URL)) aus.

   Hinweis: Wenn das Abonnement erstellt wird, wird das Passwort nicht in Klartext angezeigt.

   b. Geben Sie im Feld „URL“ eine URL im Format `https://<username>:<password>@<instancename>.service-now.com/api/sn_em_connector/em/inbound_event/oraclecloud` ein.
   Beispiel: `https://oracleevents:oracleevents@instance1.service-now.com/api/sn_em_connector/em/inbound_event/oraclecloud`.
   Wenn das Abonnement mit der URL der ServiceNow-Instanz erstellt wird, erhält der Oracle Cloud Push-Connector eine Nutzlast, die das Abonnement bestätigt, und wird in der Oracle Cloud-Konsole in den Status **Aktiv** versetzt.

2. In der Oracle Cloud-Konsole können Sie eine Alarmdefinition erstellen und das Benachrichtigungsziel mit dem Thema festlegen, das das ServiceNow-https-Abonnement enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

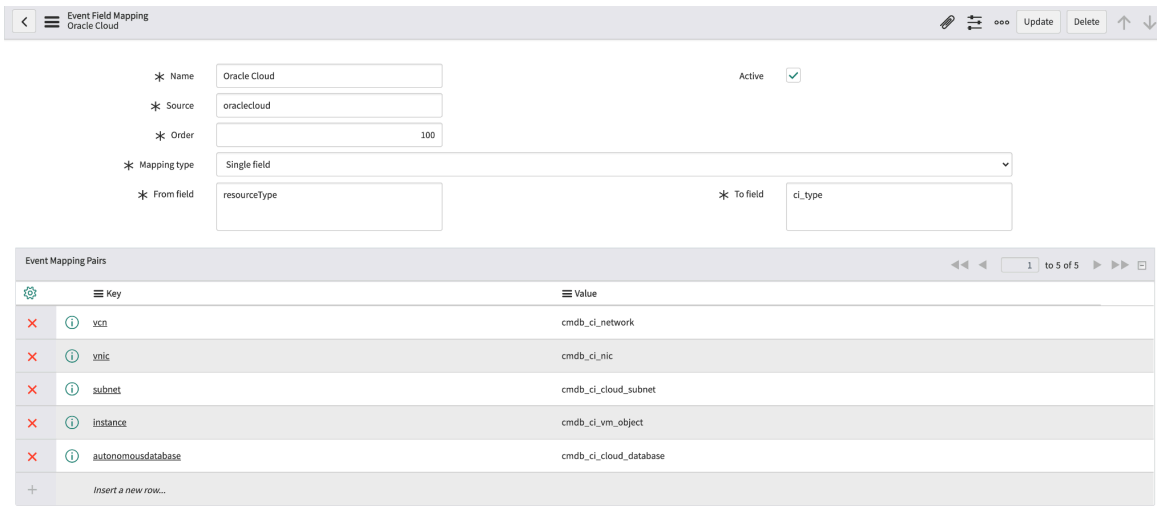
a. Navigieren zu **Erkennbarkeit Und Management** > **Alarmdefinitionen**an.

b. Klicken Sie auf **Create Alarm** (Alarm erstellen) oder wählen Sie einen vorhandenen Alarm aus, für den Sie das Thema festlegen möchten, das das ServiceNow-https-Abonnement enthält.

c. Wählen Sie im Abschnitt „Destinations“ (Ziele) in der Themenliste das Thema mit dem ServiceNow-https-Abonnement aus.
Wenn in der Oracle Cloud-Konsole ein Alarm ausgelöst wird, wird derselbe Alarm im Oracle Cloud Push-Connector in der ServiceNow-Instanz empfangen und ein Event wird erstellt.

Ergebnis

Abhängig von der Oracle Cloud-Alarmressource wird die Warnung mithilfe der folgenden Event-Feldzuordnung an das CI gebunden:



Sie können andere Ereignisregeln erstellen oder die Ereignis-Feldzuordnung ändern, um andere Ressourcentypen zuzuordnen.

Sobald das https-Abonnement konfiguriert ist und durch einen Oracle Cloud-Alarm eine Nachricht in Ereignismanagement ausgelöst wird, geschieht Folgendes:

- Durch die Nachricht wird die Oracle Cloud-Alarmmeldung mit dem entsprechenden ServiceNow-Benutzer authentifiziert, der im https-Abonnement angegeben ist.
- Durch die Nachricht werden Informationen aus der ursprünglichen Oracle Cloud-Alarmmeldung extrahiert, damit die erforderlichen Ereignisfelder ausgefüllt werden. Außerdem wird das Event in die ServiceNow AI Platform-Datenbank eingefügt.
- Erfasst spezifischen Inhalt im Feld **Zusätzliche Informationen** des Event-Formulars

Prometheus-Events integrieren

Integrieren Sie Prometheus mit Ereignismanagement, indem Sie einen Standard-Webhook in den Warnungsmanager von Prometheus einfügen.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.
- Vergewissern Sie sich, dass Konfigurationselemente für die von Prometheus verwalteten Hosts im ServiceNow-System vorhanden sind. Diese CIs können physisch oder virtuell sein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Prometheus.

Beginnend mit Xanadu Release, haben die OOTB-Ereignisregeln (sofort einsatzbereit), die mit dem Connector bereitgestellt werden und die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert oder geändert), jetzt **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit dieser Änderung können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Fügen Sie in der Prometheus-Instanz einen Webhook hinzu.
   a. Navigieren Sie zu Alertmanager.yml und fügen Sie einen Webhook-Eintrag unter den Empfängern hinzu.
   b. Geben Sie die Endpunkt-URL ein. Verwenden Sie beispielsweise `https://<instance-name>/service-now.com/api/sn_em_connector/em/inbound_event?source=prometheus`.
   c. Geben Sie `basic_auth` unter *`http_config`* ein.
   d. Fügen Sie unter *`basic_auth`* einen Benutzernamen und ein Passwort hinzu und fügen Sie dann den erstellten Webhook-Namen im Empfänger unter *`route`* hinzu.
2. Erstellen Sie in der Prometheus-Instanz eine Warnungsregel.
   a. Erstellen Sie eine Datei für die Warnungsregel und fügen Sie ihren Pfad in prometheus.yml unter *`rules_files`* hinzu.
   b. Erstellen Sie die Warnungsregel gemäß dem Prometheus-Format mit PromQL.
   c. Starten Sie AlertManager und Prometheus neu, um die Änderungen zu übernehmen.

Ergebnis

Die Übertragung von Warnungen von Prometheus in das Ereignismanagement-Plugin beginnt. Vom Plugin werden Informationen aus der ursprünglichen Prometheus-Warnmeldung extrahiert, sodass die erforderlichen Ereignisfelder gefüllt werden. Außerdem wird das Event in die Datenbank eingefügt. Navigieren Sie in Ihrer ServiceNow AI Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Wenn der Schweregrad in der Nutzlast nicht empfangen wird, ist der Standardschweregrad „schwerwiegend“, der in geändert werden kann *`Push Connector Configuration`*Abschnitt von **Push-Connectors** > **Prometheus-Push-Connector**an. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

Hinweis:

Um Hosts dem *`cmdb_ci_vm_object`*-Datensatz anstelle von *`cmdb_ci_hardware`* zuzuordnen, aktivieren Sie die für Prometheus erstellte Ereignisregel **Prometheus-VM-Bindung**. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sentry-Ereignisse integrieren

Integrieren Sie Sentry mit Ereignismanagement, indem Sie auf der Sentry-Plattform einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Discovery für Sentry-Services wird nicht unterstützt. Sie müssen ein CI manuell in der Tabelle [cmdb_ci_Service_Auto] erstellen, um die Bindung zu aktivieren, indem Sie die folgenden Schritte ausführen:

1. Wechseln Sie in der Navigationsleiste zu **Konfiguration/Anwendungsservice**.
2. Geben Sie den Namen des Projekts an, das Sie in der Sentry-Anwendung überwachen.
3. Legen Sie den Betriebsstatus auf **Funktionsfähig** fest.
4. Klicken Sie auf **Weiter** und dann auf **Fertig**.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Ereignismanagement für die Erfassung von Ereignissen aus Sentry, indem Sie Sentry als Datenquelle authentifizieren. Legen Sie auf der Sentry-Plattform die ServiceNow AI Platform mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie in der Sentry-Konsole eine interne Integration.

   a. Navigieren zu **Einstellungen** > **Entwicklereinstellungen**an.

   b. Klicken Sie auf **New Internal Integration** (Neue interne Integration).

   c. Füllen Sie auf der Seite „Sentry Integration Details“ (Details der Sentry-Integration) im Abschnitt „Internal Integration Details“ (Details der internen Integration) die Felder aus.

Sentry Integration Details (Details der Sentry-Integration)

Felder	Beschreibung
Name	Name der Integration.
Webhook-URL	Standardformat der URL zum Übertragen von Ereignissen von Sentry an die Instanz der ServiceNow AI Platform. Beispiel: https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=sentry.
Alert Rule Action (Warnungsregelaktion)	Option zum Aktivieren der Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder	Beschreibung
	Hinweis: Wenn diese Option aktiviert ist, ist die Integration in den Regeln für Problemwarnungen und Metrikwarnungen in Sentry verfügbar. Die Warnungen werden an die ServiceNow-Instanz gesendet.
Schema	Schema für UI-Komponenten. Dieses Feld muss leer bleiben.
Übersicht	Beschreibung für die Integration.
Autorisierte JavaScript-Ursprünge	Authentifizierungstoken aus dem Browser zum Aktivieren der Ursprünge der Seiten, von denen Anforderungen erstellt werden. Dieses Feld muss leer bleiben.

d. Geben Sie im Abschnitt „Permissions“ (Berechtigungen) unter „Issue & Event“ (Problem und Ereignis) die gewünschte Zugriffsebene an.
Sie können **Read** (Lesen), **Read & Write** (Lesen und Schreiben) oder **Admin** auswählen.

e. Aktivieren Sie im Abschnitt „Webhooks“ das Kontrollkästchen **Issue** (Problem).

f. Klicken Sie auf **Änderungen speichern**.

2. Erstellen Sie in der Sentry-Konsole Warnungsregeln, und konfigurieren Sie diese so, dass Warnungen für Probleme von Sentry an die ServiceNow-Instanz empfangen werden.

a. Navigieren zu **Alerts** > **Warnungsregel Erstellen**an.

b. Wählen Sie den Warnungstyp aus, und klicken Sie auf **Set Conditions** (Bedingungen festlegen).

Hinweis: Vom Warnungstyp „Probleme“ werden Problemwarnungen erstellt. Von den anderen Warnungsoptionen werden Metrikwarnungen erstellt.

c. Erstellen Sie auf der Seite „Alert Rule“ (Warnungsregel) entweder eine Problemwarnung oder eine Metrikwarnung.

Warnungsregel

Optionen	Beschreibung
Issue alert (Problemwarnung)	**i.** Geben Sie die Umgebung, das Team und den Warnungsnamen für die Warnung ein. **ii.** Geben Sie unter „Set Conditions“ (Bedingungen festlegen) die Bedingungen **When** (Wann) und **If** (Wenn) ein, die die Warnung auslösen. **iii.** Wählen Sie für die Bedingung **Then** (Dann) die Option **Send a notification via an integration** (Benachrichtigung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen	Beschreibung
	über eine Integration senden) aus, und wählen Sie die interne Integration aus der Liste aus. **iv.** Legen Sie das Aktionsintervall für die Warnung fest.
Metric Alert (Metrikwarnung)	**i.** Fügen Sie Ihren Transaktionen einen Filter hinzu. **ii.** Wählen Sie die Funktion und das Zeitintervall aus. **iii.** Legen Sie die Schwellenwerte fest, bei denen die Warnung ausgelöst wird. **iv.** Fügen Sie die Aktionen hinzu, die ausgeführt werden sollen, wenn die festgelegten Schwellenwerte erreicht werden. **v.** Fügen Sie die interne Integration aus der Liste der Liste der Aktionen hinzu, um die Warnungen zu erhalten. **vi.** Fügen Sie einen Regelnamen und ein Team für die Warnung hinzu.

d. Klicken Sie auf **Save Rule** (Regel speichern).

Scout APM-Ereignisse integrieren

Aktivieren Sie die Erfassung von Ereignissen aus Scout APM, indem Sie Scout APM als Datenquelle authentifizieren, mit der sie integriert werden kann Ereignismanagement.

Vorbereitungen

Das Plugin „Ereignismanagement“ (com.glideapp.itom.snac) muss installiert sein.

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Discovery für Scout APM-Anwendungen wird nicht unterstützt. Um die Bindung zu aktivieren, müssen Sie manuell ein CI in einem erstellen ServiceNow Instanz in der Tabelle „Serviceinstanz“ [cmdb_ci_Service_Auto].

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Aktivieren Sie die Scout APM-Überwachung als Anwendungsservice auf Ihrem ServiceNow Instanz.

a. Navigieren zu **Konfiguration** > **Anwendungsservice**an.

b. Geben Sie den Namen der Anwendung an, die Sie überwachen.

c. Legen Sie den Betriebsstatus auf Funktionsfähig fest.

d. Wählen Sie **Weiter** aus.

e. Wählen Sie **Fertig**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Melden Sie sich bei der Scout APM-Konsole an.
3. Erstellen Sie einen Benachrichtigungskanal.
   a. Navigieren zu **Organisation** > **Warnungen Und Benachrichtigungen**an.
   b. Wählen Sie **New Webhook** (Neuer Webhook) aus.
   c. Geben Sie den Namen des Webhooks und die Webhook-URL an.
      Verwenden Sie das folgende URL-Format: https://<USERNAME>:<PASSWORD>@<INSTANCE_NAME>.service-now.com/api/sn_em_connector/em/inbound_event?source=scout
   d. Überprüfen Sie, ob der Webhook funktionsfähig ist, indem Sie auswählen **Testwarnung Senden** .
      Ein neues Ereignis wird auf Ihrem angezeigt ServiceNow Instanz in den Ereignissen [EM_event] Tabelle mit der Datenquelle „Scout APM“.
4. Erstellen Sie im Abschnitt „Organisation“ eine neue Benachrichtigungsgruppe.
   a. Auf der **Warnungen Und Benachrichtigungen** Seite, navigieren Sie zu **Organisation** > **Benachrichtigungsgruppen**an.
   b. Fügen Sie einen Namen für die Gruppe hinzu, und wählen Sie den von Ihnen erstellten Webhook-Kanal aus.
   c. Wählen Sie aus **Erstellen Sie Eine Benachrichtigungsgruppe** Schaltfläche.
5. Erstellen Sie im Abschnitt „Anwendung“ Warnungsbedingungen, und konfigurieren Sie sie, um Warnungen für Benachrichtigungen von Scout APM an zu erhalten ServiceNow Instanz.
   a. Navigieren zu **Anwendungen** > **Warnungsbedingungen**an.
   b. Wählen Sie den Typ der Warnungsbedingung aus.
      Weitere Informationen finden Sie in der Scout APM-Dokumentation.
   c. Wählen Sie Aus **Warnungsbedingung erstellen** .
   d. Wählen Sie in der Tabelle „Warnungsbedingungen“ die Benachrichtigungsgruppe aus, die Sie erstellt haben.
      Die Warnungsbedingung wird in der Scout-Konsole angezeigt.
6. Konfigurieren Sie Fehlerbenachrichtigungen, um Warnungen für Fehler vom Scout APM an zu erhalten ServiceNow Instanz.
   a. Navigieren zu **Anwendung** > **Fehlerbenachrichtigungen**an.
   b. Fügen Sie einen Namen und eine Beschreibung für die Benachrichtigung hinzu.
   c. Wählen Sie die Benachrichtigungsgruppe aus, die Sie erstellt haben.
      Der Scout APM-Benachrichtigungskanal wird mit den Fehlerbenachrichtigungen konfiguriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie aus **Fügen Sie Eine Benachrichtigungsgruppe Hinzu** Schaltfläche.
Für jede neue Fehlerbenachrichtigung in der Scout APM-Anwendung wird ein neues Ereignis in der Ereignistabelle [em_event] generiert.

Ergebnis

Sie können alle Benachrichtigungen auf Ihrem anzeigen ServiceNow Instanz in der Tabelle „Ereignisse“ [em_event] mit der Datenquelle „Scout APM“.

Integrieren Sie Sumo Logic-Ereignisse

Verwenden Sie den Sumo Logic-Push-Connector, um Sumo Logic in zu integrieren Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in der Sumo Logic-Plattform.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Das Plugin des Connectors ist auf installiert ServiceNow AI Platform Instanz.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Ereignismanagement Umgebung für die Sammlung von Ereignissen aus Sumo Logic durch Authentifizierung von Sumo Logic als Datenquelle. Legen Sie auf der Sumo Logic-Website Ihren fest ServiceNow AI Platform Instanz als Rest-Endpunkt mit einem Webhook.

Prozedur

1. Erstellen Sie auf der Sumo Logic-Website ein Benachrichtigungsziel.
2. Wechseln Sie zu Überwachung, und wählen Sie aus **Anwenderdefinierter Webhook** .
3. Füllen Sie das Formular mit dem Namen, der Beschreibung und der URL aus.

   Verwenden Sie dieses URL-Format, um Ereignisse aus der Sumo-Logik an die zu übertragen ServiceNow Instanz . https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=sumologic

   Hinweis: Verwenden Sie Anmeldeinformationen mit der Rolle „evt_mgmt_Integration“ als Anwendername und Passwort.

   Verwenden Sie im Abschnitt Nutzlast die folgende Vorlage:

```
{
  "type": "{{MonitorType}}",
  "node": "{{ResultsJSON._sourceHost}}",
  "metric_name": "{{Name}}",
  "description": "monitor Query: {{Query}}\n Trigger Condition:{{TriggerCondition}}\n
Trigger Value:{{TriggerValue}}\n Trigger Time Range:{{TriggerTimeRange}}\n View Trigger
Query:{{TriggerQueryURL}}\n View Monitor:{{QueryURL}} \n Results:{{ResultsJSON}}",
  "name": "{{Name}}",
  "short_description": "{{Description}}",
  "MonitorType": "{{MonitorType}}",
  "Query": "{{Query}}",
  "QueryURL": "{{QueryURL}}",
  "ResultsJson": "{{ResultsJson}}",
  "NumQueryResults": "{{NumQueryResults}}",
  "Id": "{{Id}}",
  "DetectionMethod": "{{DetectionMethod}}",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "TriggerType": "{{TriggerType}}",
  "TriggerTimeRange": "{{TriggerTimeRange}}",
  "time_of_event": "{{TriggerTime}}",
  "TriggerCondition": "{{TriggerCondition}}",
  "TriggerValue": "{{TriggerValue}}",
  "TriggerTimeStart": "{{TriggerTimeStart}}",
  "TriggerTimeEnd": "{{TriggerTimeEnd}}",
  "SourceURL": "{{SourceURL}}",
  "alertResponseUrl": "{{alertResponseUrl}}"
}
```

Ereignisse vom Typ „Protokollüberwachung“ können ohne CI-Bindung erstellt werden, da Sie den Knotenwert als „node“ erhalten: „{{ResultsJSON._sourceHost}“ in der Ereignisnutzlast von Sumo Logic. Sie können Ereignisse erstellen, aber nicht binden, da Sie sie nicht als Hostnamen für den Protokollüberwachungstyp abrufen. Ein Push-Connector-Parameter wurde erstellt – „create_log_monitorType_Events“ mit dem Wert „falsch“. Wenn der Parameterwert „falsch“ ist, wird die Nutzlast ignoriert, und „Protokoll“-Ereignisse werden nicht erstellt. Wenn Sie den Parameter in „wahr“ ändern, werden Ereignisse erstellt, und Sie müssen Ereignisregeln für die CI-Bindung definieren.

Weitere Informationen finden Sie im Folgenden ServiceNow Schweregradzuordnung mit Sumo Logic TriggerType-Tabelle:

Schweregradzuordnung

Sumo-Logik-Auslösertyp	Schweregrad
Kritisch	Kritisch
Warnung	Kleiner
MissingData	Warnung
ResolvedCritical/ResolvedWarning/ ResolvedMissingData	Leeren

Integrieren Sie Sumo Logic mit REST API-Schlüssel-Token

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

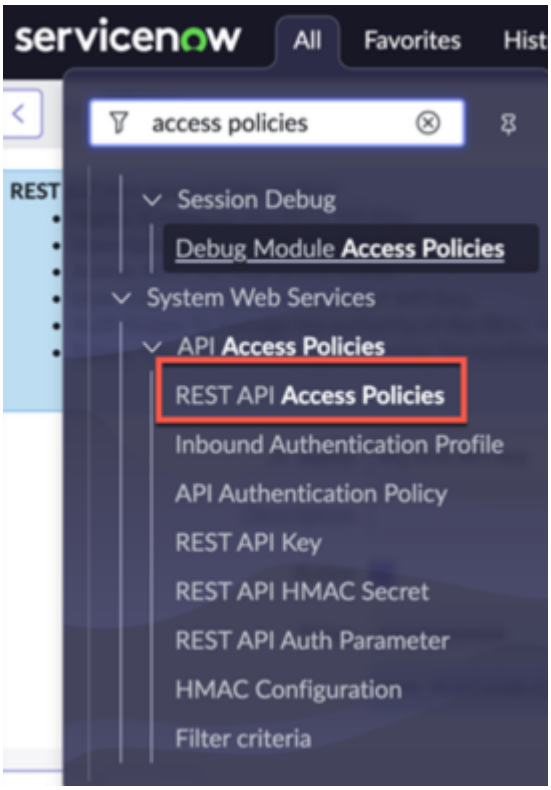
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der von generierte REST-API-Schlüssel ServiceNow AI Platform. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.

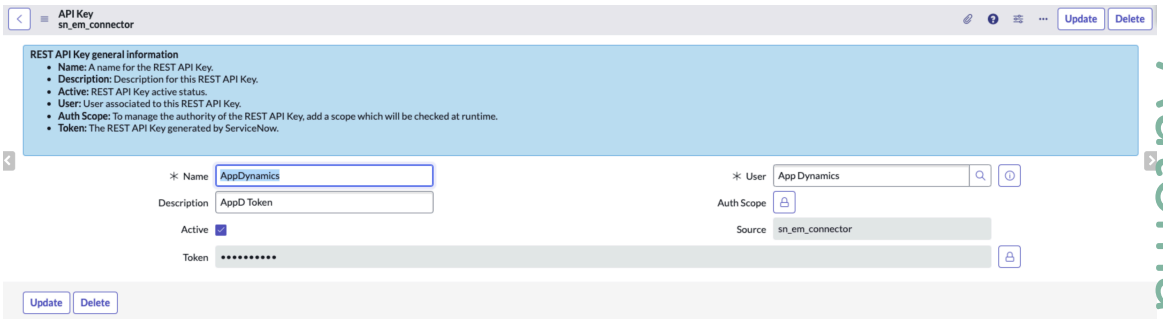
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Integrieren Sie ThousandEyes-Plattformereignisse

Integrieren Sie ThousandEyes mit Ereignismanagement Durch Hinzufügen eines Standard-Webhooks in der ThousandEyes-Konsole.

Welche Authentifizierung wird verwendet?

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung wird mit ThousandEyes Monitor V1- oder V2-Zugriffstoken durchgeführt. Weitere Informationen finden Sie unter Integrieren von ThousandEyes mit OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Standardstandard der Authentifizierung, ohne dass ThousandEyes Active Directory erforderlich ist. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE oder nützlich sein DevOps Teams. Weitere Informationen finden Sie unter Integrieren von ThousandEyes mit Standardauthentifizierung.

Integrieren von ThousandEyes mit Standardauthentifizierung

Integrieren Sie ThousandEyes mit Ereignismanagement, indem Sie einen Webhook in der ThousandEyes-Plattform hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Discovery für ThousandEyes-Services wird nicht unterstützt, daher müssen Sie manuell ein CI in der ServiceNow-Instanz erstellen, damit die Event-Bindung funktioniert.

Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus ThousandEyes, indem Sie ThousandEyes als Datenquelle authentifizieren. Legen Sie auf der ThousandEyes-Plattform Ihre Instanz der ServiceNow AI Platform mithilfe eines Webhooks als REST-Endpunkt fest.

Prozedur

1. Führen Sie in der ServiceNow-Instanz die folgenden Schritte aus, um ein CI zu erstellen.
   a. Navigieren Sie in der Navigationsleiste zu **Alle** > **Konfiguration** > **CI-Klassen Manager**an.
   b. Klicken Sie auf **Hierarchie** und suchen Sie nach `HTTP(S)-Endpunkt`.
   c. Wählen Sie **CI-Liste** aus und erstellen Sie ein neues CI.
2. Erstellen Sie auf der ThousandEyes-Plattform ein Benachrichtigungsziel.
   a. Navigieren Sie in der Navigationsleiste zu **Alerts** > **Warnungsregeln**an.
   b. Klicken Sie auf eine vorhandene Warnungsregel und wählen Sie die Registerkarte **Notification** (Benachrichtigung) aus.
   c. Auswahlvorgang **Bearbeiten Sie Den Webhook** Und geben Sie die folgenden Informationen ein.

Webhooks bearbeiten

Feld	Beschreibung
Name	Geben Sie einen Namen für den Webhook ein.
URL	Geben Sie die Webhook-URL an. **Hinweis:** Das Standardformat der URL zum Übertragen von Events von ThousandEyes an die ServiceNow-Instanz ist `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=thousandeyes`.
Auth Type	Wählen Sie **Basic** (Standard) aus.

   d. Klicken Sie auf **Add New Webhook** (Neuen Webhook hinzufügen).

Ergebnis

Der Standardschweregrad für die ThousandEyes-Warnung ist **Schwerwiegend -2** , Die in geändert werden kann *`Push Connector Configuration`*Abschnitt von **Push-Connectors** > **ThousandEyes-Push-Connector**an. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

Die Standardzeitzone der ThousandEyes-Warnung ist GMT. Wenn Sie die Warnung in einer anderen Zeitzone senden möchten, kann sie in geändert werden *`Push Connector Configuration`*Abschnitt von **Push-Connectors** > **ThousandEyes-Push-Connector**an. Das gültige Wertformat ist **GMT+01:00**, **GMT+02:00**, **GMT-05:30**, **GMT-02:00** usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrieren Sie ThousandEyes mit REST API-Schlüssel-Token

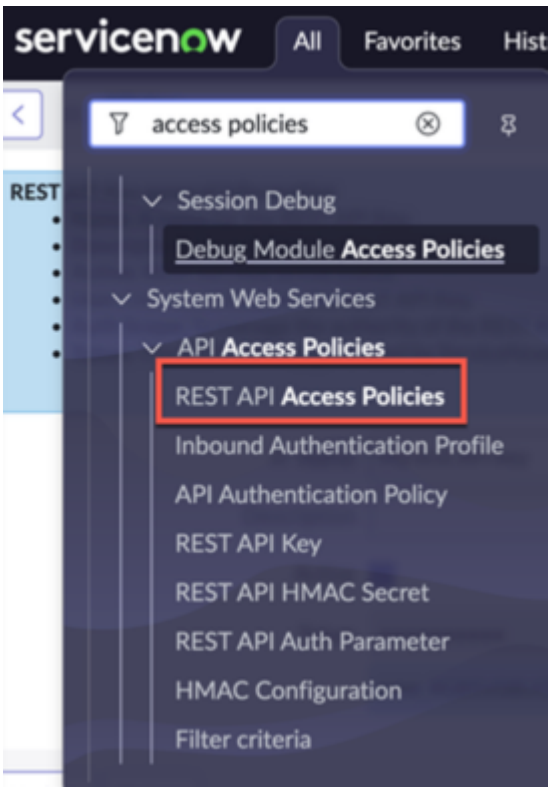
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und verbessert die betriebliche Effizienz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**an.



2. Wählen Sie **Neu**.

3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle „evt_mgmt_Integration“ erstellt werden. Erstellen Sie eine neue in der Tabelle „sys_user“, die hier verwendet werden soll, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.

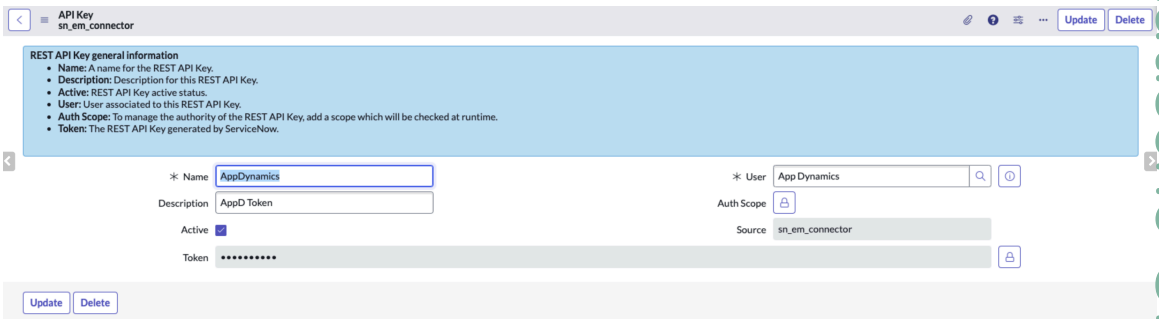
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST API-Schlüssels zu verwalten.
Token	Der generierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeit, nach der die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie Folgendes hinzu: Useraccount.
5. Verwenden Sie das Formularmenü, und wählen Sie aus **Speichern** .

   Das System generiert ein Token und speichert es im **Token** Feld. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie die Inhaltsanzeige unter dem Feld. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Ergebnis

Jetzt sind Sie bereit, mit dem Senden von Ereignissen zu beginnen. In Ihrem Überwachungstool können Sie Ereignisse entweder mit dem Header oder der Abfrage senden Parameter: X-sn-apikey . Zum Beispiel:

```
https://[INSTANCENAME].service-now.com/api/sn_em_connector/em/inbound_event?source=[SOURCENAME]&sys_id=[SYSID OF PUSH CONNECTOR INSTANCE]&x-sn-apikey=[AUTH TOKEN]
```

Integrieren von ThousandEyes mit OAuth-Authentifizierung

Erstellen Sie Anmeldeinformationen in der Instanz, und konfigurieren Sie den ThousandEyes-Webhook.

Vorbereitungen

Erforderliche Rolle: web_service_admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** Und wählen Sie dann aus **Neu** .
2. Wählen Sie Aus **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** .
3. Kopieren Sie das automatisch generierte Feld **Client-ID** .
   Die **Client-ID** Wird beim Konfigurieren der ThousandEyes SeviceNow-Integration verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Entsperren Sie **Umleitungs-URL** Feld und weisen Sie den Wert zu: **https://app.thousandeyes.com/webhooks-oauth-callback/**
5. Konfigurieren Sie die Lebensdauer von Zugriffs- und Aktualisierungstoken, indem Sie einen Wert in Sekunden angeben.
6. Öffnen Sie die ThousandEyes-Webhook-Konfiguration, und füllen Sie die folgenden Felder aus:

   Name

   Beliebiger Name

   URL

   Endpunkt des ThousandEyes-Push-Connectors von ServiceNow

   Authentifizierungstyp auswählen

   OAuth

   Gewährungstyp

   Implizit

   Authentifizierungs-URL

   https://servicenow_instanz>.service-now.com/oauth_auth.do

   Client-ID

   Fügen Sie die in Schritt 3 automatisch generierte Client-ID ein.

7. Wählen Sie Aus **Token Abrufen** .
8. Wählen Sie aus, sobald der ThousandEyes-Connector zu einer Webseite navigiert ist, auf der eine Verbindung mit Ihrem ServiceNow-Account angefordert wird **Zulassen** .
9. Geben Sie Account-Anmeldeinformationen an, die über verfügen **Web_Service_admin** Rolle.

Panopta als Datenquelle integrieren

Integrieren Sie die cloudbasierte Überwachungslösung von Panopta in Ereignismanagement. Zum Hinzufügen von Panopta als Datenquelle ist eine Konfiguration in Panopta erforderlich.

Konfigurieren Sie Panopta

Um Panopta als Datenquelle vorzubereiten, folgen Sie dem Verfahren, das unter diesem Link beschrieben wird: Wie kann ich ServiceNow integrieren?

Wenn die Ereignismanagement-Integration in Panopta konfiguriert ist, fügen Sie die Integration einer Ihrer Panopta-Warnungszeitachsen hinzu, damit die ServiceNow-Instanz Incident-Events entsprechend empfängt.

Optionale Ereignismanagement-Konfiguration

Konfigurieren Sie eine Warnungsaktionsregel für den Start im Kontext von Panopta. Weitere Informationen finden Sie unter Webanwendung aus Warnung starten und Warnungsaktionsregel erstellen oder bearbeiten.

Zugehörige Informationen

Konfigurieren Ereignismanagement Connectors

Event-Connector für Event Integration Format (EIF) integrieren

Verwenden Sie den Push-Connector, mit dem Events von Produkten (im Allgemeinen von IBM) weitergeleitet werden können, die das EIF-Format (Event Integration) an einen MID-Server unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz.

Stellen Sie sicher, dass dem MID Server entweder EventManagement oder ALLE Anwendungen zugewiesen sind.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Produkten, die das EIF-Format unterstützen, an einen MID-Server.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Kontext des EIF-Listeners**an.
2. Klicken Sie auf **Neu**.
3. Erstellen Sie einen neuen EIF-Listener-Kontext, indem Sie das entsprechende Formular ausfüllen:

   a. Füllen Sie die Felder des Formulars aus.

Formular „Kontext des EIF-Listeners“

Feld	Beschreibung
Name	Eindeutiger Name für den EIF-Listener-Kontext.
Kurzbeschreibung	Kurzbeschreibung des Ausführungskontexts der MID-Server-Erweiterung.
Port	Port für den EIF-Listener zum Empfangen von EIF-Events. Der Standardwert ist **9998**. Wenn der Port jedoch bereits verwendet wird, können Sie stattdessen einen anderen freien Port verwenden.
Status	Status des EIF-Listener. Dieses Feld ist leer, bis der Listener ausgeführt wird. Nachdem der Listener ausgeführt wurde, wird der Wert automatisch auf einen der folgenden Status gesetzt: ▪ Gestartet: Der Listener läuft. ▪ Angehalten: Der Listener läuft nicht. ▪ Offline: Der MID-Server ist nicht verfügbar. ▪ Fehler: Der Listener ist mit einem Fehler fehlgeschlagen.
Ausführen auf	MID-Server-Verzeichnis für die Ausführung dieses Listener.
MID Server	Den Namen des dedizierten MID-Server, wenn Sie **Spezifischer MID Server** im Feld **Ausführen auf** ausgewählt haben.
Ausführung auf	Name des MID-Server, auf dem die Erweiterung ausgeführt wird. Dieses Feld wird automatisch mit dem Namen des MID-Server gefüllt, auch wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	er nicht verfügbar ist. Wenn Sie die Erweiterung stoppen, ist dieses Feld leer.

b. Im Formular können Sie auf die zugehörigen Links im Formular „Kontext des EIF-Listeners“ klicken.

Im Formular „Kontext des EIF-Listeners“ verfügbare Befehle

Zugehöriger Link	Beschreibung
Start	Wählen Sie diese Option, wenn der Listener nicht ausgeführt wird. Der Listener wird auf dem konfigurierten MID-Server mit der konfigurierten Portnummer gestartet.
Stoppen	Wählen Sie diese Option, um den ausgeführten Listener auf dem konfigurierten MID-Server anzuhalten.
Neu starten	Klicken Sie hierauf, um den Listener auf dem konfigurierten MID-Server mit der Portnummer zu starten.
Parameter aktualisieren	Wählen Sie diese Option, wenn Sie Änderungen an der Listener-Konfiguration des derzeit ausgeführten Listener vornehmen möchten. Wenn die Parameter gültig sind, trennt sich der Listener und stellt die Verbindung mit den neuen Parametern wieder her.
Parameter testen	Wählen Sie diese Option, um zu testen, ob der Port eine gültige Nummer ist.

4. Wenn Sie fertig sind, klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie **Speichern** aus.
5. Klicken Sie auf **Aktualisieren**.
6. Wenn Sie den eingehenden EIF-Datenverkehr überprüfen möchten, gehen Sie wie folgt vor:
   a. Navigieren zu **MID-Server** > **Server**an.
   b. Wählen Sie den MID-Server aus, auf dem die EIF-Erweiterung ausgeführt wird.
   c. Fügen Sie auf der Registerkarte **Konfigurationsparameter** die **mid.log.level**-Eigenschaften hinzu.

Nächste Maßnahme

Wenn der MID-Server nicht gestartet werden kann, können Sie die MID-Server-Protokollfehler überprüfen.

Schweregrad von Warnungen bezüglich EIF-Events

Wenn die Nutzlast des EIF-Event einen Warnungsschweregrad hat, wird sie in der ServiceNow-Instanz anders zugeordnet.

Schweregrad von EIF-Events	Schweregradzuordnung von ServiceNow-Events
UNBEKANNT	Warnung
Warnung	Kleiner
Kleiner	Schwerwiegend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad von EIF-Events	Schweregradzuordnung von ServiceNow-Events
Kritisch	Kritisch
Fatal (Schwerwiegend)	Kritisch

Erstellen Sie einen Push-Connector-Konfigurationsparameter

Einige Connectors haben keine Parameter, die sofort geliefert werden. Daher ist es erforderlich, den Parameter zu erstellen und der Liste der Push-Connector-Konfigurationen im Formularlayout hinzuzufügen, bevor der neue Parameter hinzugefügt wird.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, personalize_Form

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**an.
2. Öffnen Sie einen Push-Connector.
3. Auf der **Push-Connector** Formular, klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Konfigurieren** > **Formularlayout**an.
4. In **Verfügbar** Liste, suchen Sie nach **Push-Connector-Konfigurationen** > **Push-Connector**, Und verschieben Sie es in **Ausgewählt** Liste.
5. Wählen Sie **Speichern**.
6. In Push-Connector-Konfigurationen [sn_em_Connector_Push_config] Tabelle, doppelklicken Sie auf **Fügen Sie eine neue Zeile ein** Zum Hinzufügen eines neuen Push-Connector-Konfigurationsparameters.
7. Wählen Sie **Aktualisieren**.

Ergebnis
Liste der Push-Connector-Konfigurationen wurde dem Layout des Push-Connector-Formulars hinzugefügt. Sie können jetzt Push-Connector-Parameter erstellen.

Konfigurieren Eine Push-Connector-Instanz

Konfigurieren Sie eine Push-Connector-Instanz, um die Ereignisse von einem externen System zu empfangen.

Vorbereitungen
Stellen Sie sicher, dass Sie eine Push-Connector-Definition definiert haben.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Connector-Instanz verwenden, um die Ereignisse aus externen Quellen zu empfangen. Sie können den folgenden Typ von Push-Connector-Instanzen erstellen:

- Instanztyp
- MID-Typ

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connector-Instanzen**an.
2. Wählen Sie Aus Die Connector-Instanz, die Sie konfigurieren oder auswählen möchten **Neu** Dient zum Erstellen einer Push-Connector-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Auf der **Push-Connector-Instanz** Formular , Füllen Sie die Felder aus.

   Weitere Einzelheiten finden Sie unter Push-Connector-Instanzformular.

4. Wählen Sie **Absenden** oder **Aktualisieren** aus.

Ergebnis
Das Push-Connector-Instanzformular wird gespeichert, und jetzt können Sie die Ereignisse von einem externen System empfangen.

Event-Erfassung per E-Mail konfigurieren

Konfigurieren Sie eine Aktion für eingehende E-Mails, um E-Mail-Benachrichtigungen zu senden, wenn Events und Warnungen ausgelöst werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie eine Aktion für eingehende E-Mails zum Senden von E-Mails hinzufügen, verwendet Ereignismanagement Aktionen für eingehende E-Mails, um eingehende E-Mails auf die gleiche Weise wie jedes externe Event zu verarbeiten. Der E-Mail-Inhalt wird zum Generieren und Aktualisieren von Events verwendet. Verwenden Sie Regeln zum Generieren von Warnungen oder ändern Sie den Event-Schweregrad. Der Schweregrad wird nach der Auswirkungsberechnung aktualisiert und in der Tabelle em_impact_status gespeichert.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **E-Mail-Eigenschaften**an.
2. Wählen Sie im Abschnitt **Konfiguration für eingehende E-Mails** unter **E-Mail-Empfang aktiviert** die Option **Ja** aus, um die Erfassung von Events per E-Mail zu ermöglichen.
3. Zum Konfigurieren der E-Mail-Informationen, an die übergeben werden soll Ereignismanagement Navigieren Sie zur Ereignis- und Warnungsverarbeitung zu **Systemrichtlinie** > **E-Mail** > **Eingehende Aktionen** Und in der Liste der eingehenden E-Mail-Aktionen suchen und öffnen Sie den Standard **Ereignis erstellen** Formular.

   a. Auf der **Aktionen Für Eingehende E-Mails** Formular: Geben Sie diese Werte an.

Feld	Wert
Aktiv	Aktivieren Sie die Checkbox, um die E-Mail-Benachrichtigung zu aktivieren.
Zieltabelle	Wählen Sie **Event [em_event]** aus.
Aktionstyp	Wählen Sie **Datensatz für Aktion** aus.

   b. Wählen Sie aus **Beschreibung** Registerkarte und geben Sie eine Beschreibung für die E-Mail-Nachricht ein.

   c. Wählen Sie aus **Aktionen** Registerkarte und wählen Sie diese aus **Feldaktionen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **[Schweregrad] [An] [<Event-Schweregrad>]**
- **[Typ] [E-Mail von] [<Teil der E-Mail>]**

  Beispielsweise können Sie **Betreff** als den zu verwendenden Teil der E-Mail auswählen.

4. Fügen Sie ein **Skript** hinzu, um die Eingangsparameter anzupassen und den Text Event-Variablen zuzuordnen.

   Example
   Beispiel:

```
current.source = 'email';
current.event_class = 'email';
current.description = email.body_text;
current.time_of_event = new GlideDateTime();
current.insert();
```

5. Senden Sie von der Instanz aus eine E-Mail mit übereinstimmenden Daten, und bestätigen Sie dann, dass die Event- oder Warnungsinformationen in Ereignismanagement angezeigt werden.
   Weitere Informationen zum Senden von E-Mail-Nachrichten zum Erstellen einer Instanz finden Sie unter Aktionen für eingehende E-Mails .

   Hinweis: Stellen Sie sicher, dass der Benutzer, der die E-Mail sendet, die Rolle **evt_mgmt_integration** hat.

6. Wählen Sie **Absenden**.

Ergebnis

Die eingehende E-Mail wird an die Tabelle em_event gesendet, und reguläre Ereignismanagement-Prozesse werden fortgesetzt, z. B. werden Event-Regeln und Warnungs-Management-Regeln ausgeführt.

Ereignisweiterleitung

Beschleunigen Sie den Testlebenszyklus der Ereignisverarbeitung, indem Sie einen Ereignisstrom von Ihrem weiterleiten ServiceNow Produktionsumgebung in Ihre Umgebung außerhalb der Produktion.

Verwenden Sie die Ereignisweiterleitung, um Ereignisse von einer Instanz an eine andere weiterzuleiten, z. B. von einer Produktionsinstanz an eine Instanz außerhalb der Produktion. Mit der Ereignisweiterleitung können Sie Ereignisregeln, Ereignisfeldzuordnungen, Warnungsverwaltungsregeln, Warnungskorrelation usw. testen und bewerten. ohne Auswirkungen auf Ihre Produktionsumgebung zu haben.

Nicht alle Überwachungsquellen können Ereignisse an mehrere Zielinstanzen senden. In solchen Fällen können Sie eine geplante Aufgabe konfigurieren, um den Ereignisstrom regelmäßig von Ihrem weiterzuleiten ServiceNow Instanz, die mit der überwachten Quelle mit anderen Instanzen verbunden ist.

Richten Sie die Ereignisweiterleitung ein

Erstellen Sie einen Konfigurationsdatensatz für die Ereignisweiterleitung, um den Flow von Ereignissen aus einem zu ermöglichen ServiceNow Instanz zu einer anderen Instanz. Das Weiterleiten von Ereignissen an mehrere Zielinstanzen erfordert die Erstellung separater Konfigurationsdatensätze für jede Zielinstanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Sie müssen über Anmeldeinformationen mit der Rolle „evt_mgmt_Integration“ verfügen, mit der Sie Ereignisse in der Zielinstanz erstellen können. Wenn Sie nicht über diese Anmeldeinformationen verfügen, lesen Sie unter Erstellen Sie Anmeldeinformationen für den Server für die Standardauthentifizierung Um Informationen zum Erstellen zu erhalten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Quellinstanz, die Ereignisse an eine Zielinstanz weiterleitet, muss über einen Anwender mit der Rolle „evt_mgmt_Integration“, ein Passwort für die Anmeldeinformationen und einen neuen Ereignisweiterleitungsdatensatz verfügen. Die Zielinstanz, die Ereignisse von der Quelle empfängt, muss über Anmeldeinformationen mit demselben Anwendernamen und Passwort wie die Quellinstanz verfügen.

Der Ereignisweiterleitungsdatensatz enthält Details zum Ziel ServiceNow Instanz-URL, an die Ereignisse zusammen mit den Anmeldeinformationen weitergeleitet werden sollen, um eine Verbindung herzustellen.

Sie müssen einen separaten Konfigurationsdatensatz für jede Zielinstanz erstellen, um Ereignisse an mehrere Zielinstanzen weiterzuleiten. Ereignisse werden dann an jede Zielinstanz mit einer aktiven Ereignisweiterleitungskonfiguration gesendet.

Prozedur

1. Navigieren Sie in Ihrer Quellinstanz zu **Alle** Und geben Sie ein sn_em_Connector_event_Sync_Configuration.list Im Filternavigator.
2. Auf der **Konfigurationen Der Ereignissynchronisierung** Seite auswählen **Neu** .
3. Auf der **Konfiguration Der Ereignissynchronisierung** Seite, in **Instanz-url** Feld das Ziel eingeben ServiceNow URL zum Empfangen von Ereignissen im Format https://<your_instance>.Service – now.com .
4. In **Anmeldeinformationen** Geben Sie die Anmeldeinformationen für die Zielinstanz an, indem Sie sie entweder eingeben oder danach suchen.
   - Um Ihre Anmeldeinformationen einzugeben, beginnen Sie mit der Eingabe, und wählen Sie dann die Anmeldeinformationen aus der Dropdown-Liste aus.
   - Um nach Ihren Anmeldeinformationen zu suchen, wählen Sie das Symbol „Suchen mit Liste“ ( ), um Ihre Anmeldeinformationen aus der Suchtabelle für Anmeldeinformationen auszuwählen.
5. Wählen Sie **Speichern**.
6. Wählen Sie Aus **Verbindung Testen** Dient zum Validieren der Verbindung zum Ziel ServiceNow Instanz.
   - Wenn die Verbindung erfolgreich war, wird eine Bestätigungsmeldung angezeigt.
   - Wenn die Verbindung nicht erfolgreich war, überprüfen Sie Ihre Anmeldeinformationen und die Instanz-URL.
7. Wählen Sie nach der Validierung die aus **Aktiv** Kontrollkästchen, um die Ereignisweiterleitung an die Zielinstanz zu aktivieren und auszuwählen **Übermitteln** .
   Die Konfiguration wird erstellt und wird im aufgeführt **Konfigurationen Der Ereignissynchronisierung** Seite.
8. Wiederholen Sie für mehrere Ziele die Schritte für einen separaten Konfigurationsdatensatz für jede Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Führen Sie regelmäßig einen Ereignisweiterleitungsauftrag aus

Führen Sie regelmäßig einen Ereignisweiterleitungsauftrag aus

Planen Sie einen Ereignisweiterleitungsauftrag, um regelmäßig Ereignisse an alle Zielinstanzen mit aktiven Ereignisweiterleitungskonfigurationen zu senden, wenn die Überwachungsquelle keine Ereignisse an mehrere Zielinstanzen senden kann.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können anpassen *`event-forwarding`*Auftragsverhalten durch zugehörige Systemeigenschaften. Weitere Informationen finden Sie unter Eigenschaften der Ereignisweiterleitung.

Hinweis: Um die Auswirkungen auf die Leistung zu minimieren, sendet die geplante Aufgabe Ereignisse, die nicht älter als die letzte Stunde sind, wenn sie zum ersten Mal nach dem Einrichten der Ereignisweiterleitung ausgeführt wurde.

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgaben** > **Ereignismanagement: Ereignisweiterleitungsauftrag**an.
2. Auf der **Geplante Skriptausführung** Wählen Sie Seite aus **Aktiv** Kontrollkästchen.
3. In **Wiederholungsintervall** Feld das entsprechende Zeitintervall für die regelmäßige Ausführung des Auftrags festlegen.

   Der Standardwert ist, dass der Auftrag jede Minute ausgeführt wird.
4. Wählen Sie **Aktualisieren**.

Ergebnis

Der Ereignisweiterleitungsauftrag wird regelmäßig basierend auf dem von Ihnen festgelegten Wiederholungsintervall ausgeführt. Ereignisse werden an alle Ziele gesendet ServiceNow Instanzen mit aktiven Konfigurationsdatensätzen für die Ereignisweiterleitung.

Wenn der Administratoraccount deaktiviert ist, konfigurieren Sie den Anwender der geplanten Aufgabe. Standardmäßig ist dies Administrator, in diesem Fall muss er jedoch geändert werden.

Hinweis:

Wenn die Ereignisweiterleitung an die Instanz aus irgendeinem Grund fehlgeschlagen ist, wird **Status der letzten Ereignisweiterleitung** Feld wird angezeigt Fehlgeschlagen Mit einer entsprechenden Fehlermeldung, die in angezeigt wird **Letzter Ereignisweiterleitungsfehler** Feld. Die Zielinstanz generiert während der nächsten erfolgreichen Ereignisweiterleitung ein Selbstintegritätsüberwachungsereignis, das den Fehler bei der Ereignisweiterleitung für den angegebenen Zeitraum anzeigt.

Erstellen Sie Anmeldeinformationen für den Server für die Standardauthentifizierung

Erstellen Sie Anmeldeinformationen, um auf zuzugreifen ServiceNow Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung**.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Anwendername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: 100

5. Wählen Sie **Absenden**.

Ergebnis

Die Anmeldeinformationen für die Standardauthentifizierung zur Verwendung mit der Serverinstanz werden erstellt.

Ereignisse werden verarbeitet

Ereignisverarbeitung ist der Prozess, bei dem Ereignisse oder Streams von Ereignissen erfasst, analysiert und automatische Maßnahmen ergriffen werden. Der Prozess umfasst die Anzeige von Ereignissen, Ereignisbindung, Ereignisregeln und Ereignisfeldzuordnung.

Ein Event ist eine Benachrichtigung von einem oder mehreren Überwachungstools, die anzeigt, dass etwas von Interesse aufgetreten ist, z. B. eine Protokollnachricht, eine Warnung oder ein Fehler. Events werden verarbeitet und Warnungen werden basierend auf den folgenden Faktoren generiert:

Konfiguration der Ereignissammlung über einen MID-Server, ein Skript, einen SNMP-Trap-Sammler oder eine E-Mail-Nachricht.

Eine Event-Regel, Warnungsbindung oder Event-Feldzuordnungskonfiguration für die Verarbeitung von Events aus verschiedenen Quellen. Wenn ein Event-Paket verarbeitet wird, das Events mit einem benutzerdefinierten (nicht unterstützten) Status enthält, werden die Events mit dem benutzerdefinierten Status nicht verarbeitet.

Weitere Informationen finden Sie unter Ereignismanagement erkunden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Events anzeigen

Ereignismanagement verfolgt einzelne Events zur Verwaltung externer Systeme. Diese Ereignisse sind Benachrichtigungen von Überwachungstools, die auf interessante Vorkommen hinweisen, z. B. Protokollnachrichten, Warnungen oder Fehler. Ereignismanagement Sammelt Ereignisse aus externen Quellen und speichert sie in der Tabelle „Ereignis“ [em_event], die eine Liste eingehender Rohereignisse bietet.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator, evt_mgmt_user, oder evt_mgmt_integration

Hinweis: Stellen Sie sicher, dass Sie den Wert des **Klassifizierungsfelds** in Event-Tabellen [em_event] weder manuell noch per Skript oder Event-Regel ändern.

Warum und wann dieser Vorgang ausgeführt wird

Das Event-Überwachungstool generiert die Werte der Quell- und Ressourcenfelder. Ereignismanagement-Implementierer können Event-Typen definieren und Knoten registrieren, um eingehende Events eindeutig zu identifizieren und Warnungen für die spezifischen Anforderungen des Unternehmens zu erstellen. Ereignismanagement verwendet diese Informationen, um zu bestimmen, ob eine Warnung erstellt oder eine vorhandene aktualisiert werden soll.

Eine Event-Quelle kann doppelte Events mit denselben identifizierenden Informationen generieren. Bei Events mit übereinstimmenden Identifizierungsinformationen bestimmt Ereignismanagement anhand des Zeitintervalls zwischen Events, ob die Events ein vorhandenes Problem oder ein neues Problem darstellen.

Zusätzliche Felder sollten im Feld **Zusätzliche Informationen** des Events eingeschlossen werden. Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen. Weitere Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Hinweis: Vermeiden Sie das Schreiben von Business Rules für Event-Tabellen [em_event], da dies zu einer Verschlechterung der Leistung führen kann.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.

   Die Liste „Alle Events“ zeigt die folgenden Spalten.

Liste „Alle Events“

Spalte	Beschreibung	Ausgefüllt mit
Zeit des Events	Zeit des Auftretens des Events in der Zeitzone des Netzwerkknotens. Das System unterstützt die Zeitauflösung in Sekunden.	Externes Event-Überwachungstool
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Beschreibung	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen	Externes Event-Überwachungstool

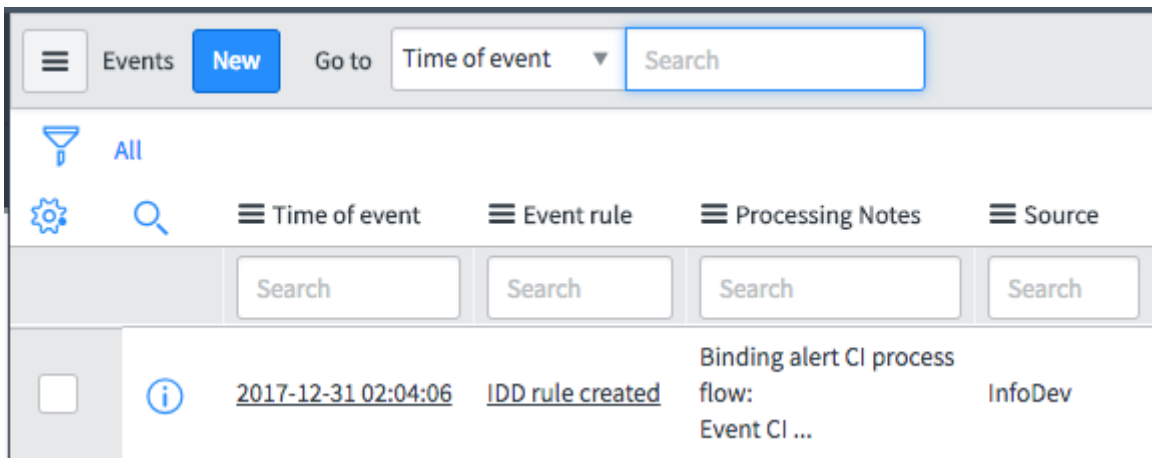
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung	Ausgefüllt mit
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Ressource	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Metrikname	Eindeutiger Name, der beschreibt, welche Metriken erfasst werden und für welche diese Warnung erstellt wurde.	Externes Event-Überwachungstool
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen	Externes Event-Überwachungstool
Status	Der Status des Events: ○ **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. ○ **In der Warteschlange**: Das Event wird vom Event-Verarbeitungsauftrag in die Warteschlange gestellt. ○ **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. ○ **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer. ○ **Ignoriert**: Dieser Wert wird nicht verwendet.	Event
Schweregrad	Obligatorisch. Die Optionen werden normalerweise wie folgt interpretiert: ○ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ○ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist.	Event

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung	Ausgefüllt mit
	○ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ○ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.	
Warnung	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.	Eine übereinstimmende Event-Regel oder Event-Feldzuordnung

2. Um ein einzelnes Event anzusehen, klicken Sie auf die gewünschte Zeile in der Spalte **Zeit des Events**.
3. Zum Überprüfen der Event-Regeln, die das Event verarbeitet haben, klicken Sie im Abschnitt **Zugehörige Links** auf **Event-Prozess überprüfen**.
   Für weitere Möglichkeiten zum Anzeigen der Event-Regeln, die auf das Event angewendet wurden, können Sie die Felder Ereignisregel und Verarbeitungsnotizen in der Event-Liste anzeigen.



Optionale Event-Felder zum Anzeigen der angewendeten Event-Regel

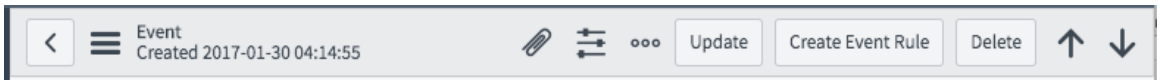
Spalte	Beschreibung
Regel für übereinstimmende Events	Event-Regel, die den aktuellen Event-Regeldefinitionen entspricht. Diese Informationen werden hauptsächlich zum Erstellen von Event-Regelempfehlungen für Events verwendet, die derzeit nicht von Regeln abgedeckt sind. Wenn Event-Regeln geändert wurden, können diese Informationen aus dem unten beschriebenen Feld „Verarbeitungsnotizen“ abgerufen werden. **Hinweis:** Dieses Feld zeigt nicht den Verlauf der Event-Regeln an, die auf das Event angewendet wurden.
Verarbeitungsnotizen	Informationen zur Bindung an den CI-Typ und zu den Event-Regeln, die auf das Event angewendet wurden

4. So erstellen Sie eine Event-Regel für ein Event, das keiner Event-Regel zugeordnet ist:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf das Event.

Das Event wird im Event-Formular geöffnet.



b. Klicken Sie auf **Event-Regel erstellen**.
Die Felder der neuen Event-Regel werden mit Daten aus dem Event ausgefüllt. Sie können die Event-Informationen beispielsweise verwenden, wenn Sie Felder für Warnungen verfassen.

Teambasierte Integrationen in Ereignismanagement

Teambasierte Integrationen ermöglichen es Teams, die Ereignisverarbeitung in zu optimieren Ereignismanagement Zur Verbesserung der Effizienz und betrieblichen Effektivität.

Teambasierte Integrationen bieten die folgenden Fähigkeiten:

- Weisen Sie Teams bestimmten Connectors zu, um einen strukturierten Ansatz für Integrationsbemühungen zu bieten.
- Ermöglichen Sie jedem Team, anwenderdefinierte Regeln zu definieren und anzuwenden, um eine gezieltere und einfachere Behandlung der Ereignisverarbeitung zu ermöglichen.
- Leiten Sie Warnungen automatisch an die entsprechenden Teammitglieder weiter, die für die integrierten Systeme verantwortlich sind, basierend auf dem Besitz der Integration und dem Besitz des Konfigurationselements (Configuration Item, CI).
- Ermöglichen Sie eine nahtlose Integration und Automatisierung durch die automatische Zuweisung von Warnungen an entsprechende Teammitglieder basierend auf dem Besitz von Integrationen und Konfigurationselementen (Configuration Item, CI).

Passen Sie Ereignisregeln, Ereigniszuordnung und den Vorrang von Teamregeln für teambasierte Integrationen an. Weitere Informationen finden Sie unter Teambasierte Integrationseigenschaften.

Zugehörige Informationen

Event-Regeln

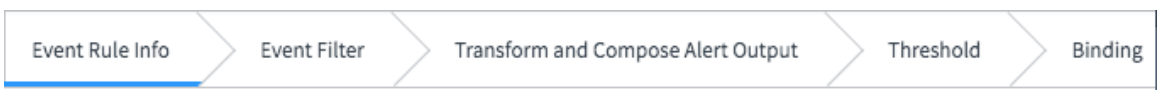
Konfiguration der Event-Feldzuordnung

Warnungszuweisungsgruppen für Teams

Event-Regeln

Verwenden Sie Event-Regeln, um Warnungen für die Nachverfolgung und Nachbesserung zu generieren. Event-Regeln werden in der Event-Regeltabelle [em_match_rule] gespeichert. Konfigurieren und passen Sie Event-Regeln an, um Events und die Generierung von Warnungen zu verwalten.

Event-Regeln ändern die Event-Datensätze in der Event-Tabelle nicht. Änderungen an Event-Daten werden im Instanzspeicher ServiceNow gespeichert.



Verwenden Sie den Event-Regeldesigner zum Erstellen und Konfigurieren von Event-Regeln. Mit den Standard-Ereignisregeln oder Ereignisregeln, die Sie erstellt haben, können Sie folgende Aktionen durchführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Event-Regelfilter anwenden, um zu bestimmen, ob die Regel für ein Event gilt.
- Umwandlung mit **Event-Abgleichsfeldern** und optionalen **Event-Erstellungsfeldern** anwenden, um den Warnungstext zu formatieren.
- Anwenden eines Grenzwerts zum Erstellen anwenderdefinierter Warnungen für schnell wiederkehrende Ereignisse.
- Automatisch Warnungen erstellen oder schließen.
- Warnungen an CI-Informationen aus der CMDB binden.

- Führen Sie mehrere sequenzielle Regeln aus, die für dasselbe Ereignis definiert sind, indem Sie auswählen **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen. Die Ereignisregeln werden in aufsteigender Reihenfolge ausgeführt, wie in definiert **Reihenfolge** Feld. Ereignisregeln, die auf Zuweisungsgruppen angewendet werden, werden erst ausgeführt, nachdem die globalen Regeln ausgeführt wurden.

Event-Regel erstellen oder bearbeiten

Sie können Event-Regeln erstellen, um Warnungen für die Nachverfolgung und Nachbesserung zu generieren. Verwenden Sie teambasierte Integrationen in Ereignisregeln, um sicherzustellen, dass Connector-Besitz und -Ausführung allgemeinen Regeln Vorrang geben. Teams können Konsistenz und Hierarchie beibehalten und gleichzeitig Flexibilität und Anpassungsoptionen bieten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die Liste der verfügbaren Ereignisregeln in an **Ereignisregeln** Seite, um zu bestimmen, ob Sie eine Ereignisregel erstellen oder bearbeiten möchten.

Sie können Regeln erstellen, die:

- Informationen in Events verwandeln, um bestimmte Warnungsfeldwerte auszufüllen und Warnungsfelder aus verschiedenen Werten zu erstellen.
- Schwellenwertregeln konfigurieren, die Warnungen nur dann erstellen oder schließen, wenn die eingehenden übereinstimmenden Ereignisse den angegebenen Schwellenwert überschreiten.
- Warnungen mittels CI-Bezeichnern an CIs binden.

Optionen zum Erstellen der Regel sind:

- Erstellen Sie eine Event-Regel und weisen Sie Event-Felder für die Generierung von Warnungen zu.
- Erstellen Sie eine Regel aus einem vorhandenen Ereignis oder einer Gruppe von Ereignissen, die keine Regel haben. In diesem Fall werden die Event-Felder in den Abschnitt „Event-Abgleichsfelder“ der Regel kopiert.
- Bearbeiten Sie eine vorhandene Event-Regel.
- Wählen Sie für teambasierte Integrationen eine Zuweisungsgruppe aus.

- Führen Sie mehrere sequenzielle Regeln aus, die für dasselbe Ereignis definiert sind, indem Sie auswählen **Wenden Sie zusätzliche Übereinstimmungsregeln an** Kontrollkästchen. Die Ereignisregeln werden in aufsteigender Reihenfolge ausgeführt, wie in definiert **Reihenfolge** Feld. Ereignisregeln, die auf Zuweisungsgruppen angewendet werden, werden erst ausgeführt, nachdem die globalen Regeln ausgeführt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

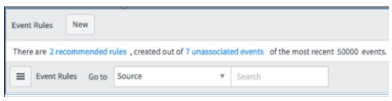
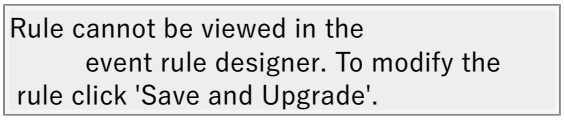
Sie können eine vorhandene Ereignisregel mit neuen Ereignisdaten aktualisieren. Weitere Informationen finden Sie unter Aktualisieren Sie Ereignisregeln.

Hinweis:

- Ereignisregeln, die nicht zum Ausführen einer Aktion konfiguriert sind, werden übersprungen. Wenn die Regel nicht als Ignorieren, Schwellenwert oder Bindung konfiguriert ist, ist es wichtig, entweder die Übereinstimmung oder die verfassten Felder anzugeben.
- Stellen Sie sicher, dass Sie nicht ändern **Klassifizierung** Feldwert in Ereignistabellen [em_event], entweder manuell, nach Skript oder nach Ereignisregel.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln** Und führen Sie eine der folgenden Aktionen aus.

Option	Bezeichnung
Event-Regel aus einem vorhandenen Event erstellen	**a.** Wählen Sie den Link für nicht zugeordnete Ereignisse oder gruppierte Ereignisse aus, die den Regeln nicht zugeordnet sind.  **b.** Wählen Sie das Event aus, das Sie zum Erstellen der Regel verwenden möchten. Die Event-Felder werden in den Abschnitt „Event-Feldregeln“ der Regel kopiert.
Vorhandene Event-Regel bearbeiten	Wählen Sie in der Ereignisregelliste die erforderliche Ereignisregel aus, die geändert werden soll. Die Event-Regel wird im Event-Regeldesigner geöffnet, in dem Sie die Werte der Felder ändern können. Wählen Sie Aus **Speichern und aktualisieren** Dient zum Ändern der Regel, wenn die folgende Bannernachricht angezeigt wird und Sie die Ereignisregel konvertieren möchten. 
Event-Regel erstellen	Wählen Sie **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Stellen Sie sicher, dass **Aktiv**

ausgewählt ist.
Wenn die Regel deaktiviert ist, findet Event Management eine andere Event-Regel und wendet sie an. Für das Event wird weiterhin eine Warnung erstellt, es sei denn, `Ignore` wird in einer anderen zutreffenden Regel ausgewählt oder wenn der Filter für diese Event-Regel konfiguriert wird.

3. Geben Sie einen eindeutigen und aussagekräftigen Namen ein und füllen Sie das Formular aus.

Event-Regel-Infoformular

Feld	Beschreibung
Quelle	Kategorie, für die diese Übereinstimmungsregel gilt. Die Zuordnungsregel gilt nur für Events mit demselben Event-Klassenwert. Wenn dieser Wert leer ist, wenden Sie die Regel auf alle Events an.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
Beschreibung	Geben Sie zusätzliche Informationen ein, die die Event-Regel beschreiben.
Zusätzliche Abgleichsregeln anwenden	Wählen Sie diese Option aus, um zusätzliche Ereignisübereinstimmungsregeln gemäß dem Feld Reihenfolge anzuwenden. Die letzte Regel mit Bindungseinstellungen legt die CI-Bindung fest. Wenn diese Option ausgewählt ist, ist die Registerkarte Schwellenwerte inaktiv.
Zuweisungsgruppe	Wählen Sie für teambasierte Integrationen eine Zuweisungsgruppe aus. Wenn in der Ereignisregel keine Zuweisungsgruppe definiert ist, wird diese Ereignisregel als globale Regel betrachtet. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln und dann die Regeln ausgeführt, die zur Zuweisungsgruppe gehören, zu der die Quellinstanz des Ereignisses gehört.

4. **Wahlweise:** Definieren Sie die Ereignisregel mit diesen Funktionen des Ereignisregel-Designers.

Option	Bezeichnung
Ereignisfilter	Definieren Sie einen Filter, um einzuschränken, auf welche Events die Event-Regel angewendet werden muss. Weitere Informationen finden Sie unter Events filtern, für die eine Event-Regel gilt.
Warnungsausgabe umwandeln und verfassen	Konfigurieren Sie die Anpassung des Warnungsinhalts. Weitere Informationen finden Sie unter Event-Regel konfigurieren, um den Warnungsinhalt anzupassen.
Schwellenwert	Erstellen oder schließen Sie Warnungen gemäß dem angegebenen Schwellenwert. Weitere Informationen finden Sie unter Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken.
Bindung	Konfigurieren Sie Event-Regeln, um Warnungen automatisch an CI-Informationen aus der CMDB zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	binden. Weitere Informationen finden Sie unter Warnungen werden an CIs gebunden.

5. Wählen Sie **Speichern**, **Absenden** oder **Aktualisieren** aus.

Zugehörige Informationen

Musterabgleich

Event-Eingabeinformationen verwenden

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Aktualisieren Sie Ereignisregeln

Ereignisverarbeitung simulieren

Events filtern, für die eine Event-Regel gilt

Event-Eingabeinformationen verwenden

Der Bereich **Event-Eingabe**, der in den Schritten zur Erstellung einer Event-Regel enthalten ist, bietet einen Verweis auf die Informationen, die Sie zur Konfiguration einer Event-Regel nutzen können.

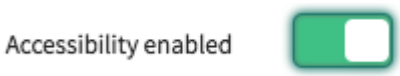
Im Bereich **Warnungsausgabe umwandeln und verfassen** können Sie die Informationen auch in die erforderlichen Felder ziehen, um den Warnungsinhalt anzupassen. Die Felder im rechten Bereich werden als Verweis darauf angezeigt, welche Felder, Ausdrücke und deren Werte beim Arbeiten im Event-Regeldesigner verfügbar sind. Die Felder, die im linken Arbeitsbereich der Warnungsausgabe „Umwandeln und verfassen“ angezeigt werden, werden zu Feldern im generierten Warnungsformular. Darüber hinaus können Sie Warnungs-Tags definieren, die spezifisch für die Anpassung sind.

Allgemeine Komponenten und Navigation

Der Bereich „Event-Eingabe“ besteht aus folgenden Abschnitten:

- Zusätzliche Ereignisinformationen
- Ausdrücke
- Rohinformationen zum Event

Der Bereich „Event-Eingabe“ wird in allen Abschnitten des Event-Regeldesigners angezeigt, mit Ausnahme des Abschnitts „Event-Regelinformationen“. Die Felder im rechten Bereich können nur im Abschnitt „Warnungsausgabe umwandeln und verfassen“ geändert werden. In allen anderen Abschnitten ist der Bereich „Event-Eingabe“ schreibgeschützt und zu Referenzzwecken verfügbar.

Hinweis: Wenn die **Eingabehilfe aktiviert** 

in den Systemeinstellungen ausgewählt ist, ist der Standardbearbeitungsmodus nicht verfügbar .

Bearbeitungsmodi

Modus	Beschreibung
Standardbearbeitungsmodus	Text, der im linken Arbeitsbereich ausgewählt wurde, kann nicht bearbeitet werden. Rückgängig machen ist nicht verfügbar. In diesem Modus können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modus	Beschreibung
	Sie den Text oder die Werte nur markieren und umwandeln, indem Sie einen Feldnamen auswählen.
Bearbeitungsmodus reguläre Ausdrücke	Bearbeiten Sie Text im linken Arbeitsbereich, indem Sie ihn nach Bedarf auswählen. Nachdem Sie den Text bearbeitet haben, können Sie nicht mehr in den Standardmodus zurückkehren. **Rückgängig machen** ist nicht verfügbar. **Zurücksetzen** ist jedoch verfügbar, wodurch das Feld auf seinen ursprünglichen Wert zurückgesetzt wird. Sie können Text mit Formatkonventionen für reguläre Ausdrücke verfassen. Geben Sie beispielsweise (. *) ein, um einen Feldnamen zu erstellen. Sie können keine der folgenden Feldwerte eingeben: „$“, um den Wert eines Felds einzubeziehen und den Namen des Felds in Klammern {} anzugeben. Sie können Sonderzeichen in ein Feld einfügen, indem Sie diesen „ausweichen“, d. h. indem Sie dem Zeichen ein „\“ voranstellen. Um beispielsweise einen „\“ in Ihren Text einzufügen, geben Sie „\\“ ein.

Zusätzliche Event-Informationen

Der Abschnitt „Zusätzliche Event-Informationen“ zeigt Standardformularfelder für Events sowie Felder an, die zur Anzeige in Warnungen erstellt wurden und dem Abschnitt **Zusätzliche Informationen** der Warnung hinzugefügt werden.

Beim Konfigurieren von Text in den Feldern im linken Arbeitsbereich können Sie Feldnamen und/oder deren Wert aus diesem Abschnitt in die Felder ziehen.

Ausdrücke

Der Abschnitt „Ausdrücke“ ist nur verfügbar, wenn ein zusätzliches Informationsfeld erstellt wurde. Sie können Ausdrücke aus Event-Rohdaten oder aus zusätzlichen Informationsdaten erstellen.

1. Klicken Sie sich in ein Feld im Bereich der **Event-Eingabe**, um Transformationsaktionen durchzuführen.
2. Erstellen Sie einen Ausdruck, indem Sie Informationen umwandeln und einem Feldnamen zuordnen. Wählen Sie entweder einen Feldnamen aus der vorgeschlagenen Liste aus, oder erstellen Sie je nach Bedarf einen Feldnamen.

3. Klicken Sie sich in ein Feld im Bereich der **Event-Eingabe**. Wählen Sie im linken Arbeitsbereich die erforderlichen Informationen aus.

Erstellen Sie Ausdrücke, indem Sie Informationen umwandeln und einem Feldnamen zuordnen. Wählen Sie einen Feldnamen aus der vorgeschlagenen Liste aus, oder erstellen Sie je nach Bedarf einen Feldnamen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rohinformationen zum Event

Der Abschnitt „Rohinformationen zum Event“ ist immer verfügbar. Sein Inhalt sind die Felder aus dem Event-Formular.

Zum Umwandeln von Text klicken Sie auf ein Feld im rechten Bereich, um ihn im Arbeitsbereich auf der linken Seite im Abschnitt „Ausdrücke markieren“ zu öffnen. Sie können Text im Abschnitt **Ausdrücke markieren** auswählen, wo der ausgewählte Text zum Wert eines neu erstellten Felds wird. Benennen Sie das neue Feld. Dieses neue Feld wird dem Abschnitt Ausdrücke hinzugefügt.

Hinweis: Wenn Sie einen regulären Ausdruck für Eingaben erstellen, stellen Sie sicher, dass Sie Eingaben mit den Variablen in sequenzieller Reihenfolge erstellen. Variablen können zwar für die Aufnahme übersprungen werden, die ausgewählte Reihenfolge muss jedoch beibehalten werden.

Steuern, wie Felder angezeigt werden:

- Verwenden Sie die Ausschlussliste [em_event_rule_black_list], um Felder im rechten Bereich auszublenden.
- Verwenden Sie das Formular em_event_rule_order, um die Position der einzelnen Felder zu sortieren.
- Felder, die nicht in der Ausschlussliste enthalten und auch nicht Teil der Tabelle em_event_rule_order sind, erscheinen noch im Event-Regeldesigner, im rechten Bereich und auf der Registerkarte **Warnungsausgabe umwandeln und verfassen**.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Events filtern, für die eine Event-Regel gilt

Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Events filtern, für die eine Event-Regel gilt

Definieren Sie einen Filter, um einzuschränken, auf welche Events die Event-Regel angewendet werden muss. Konfigurieren Sie den Filter, indem Sie eine Reihe von Bedingungen bereitstellen, die jedes Event erfüllen muss, um von der Anwendung auf die Event-Regel entweder ausgeschlossen oder in sie eingeschlossen zu werden.

Vorbereitungen

Stellen Sie sicher, dass ein Name für die Event-Regel angegeben ist.
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Erstellen der erforderlichen Bedingungsanweisung können Sie Event-Felder sowie zusätzliche Felder verwenden, die im Feld **Zusätzliche Informationen** des Events definiert sind. Verwenden Sie diese Felder, um Bedingungen zu konfigurieren, die Events ausschließen können. Alternativ können Sie eingehende Events filtern, um sicherzustellen, dass nur die Events einbezogen werden, die die erforderlichen Bedingungen erfüllen.

Hinweis: Beim Ereignisregelfilter wird zwischen Groß- und Kleinschreibung unterschieden.

Während der Arbeit auf der Registerkarte „Event-Filter“:

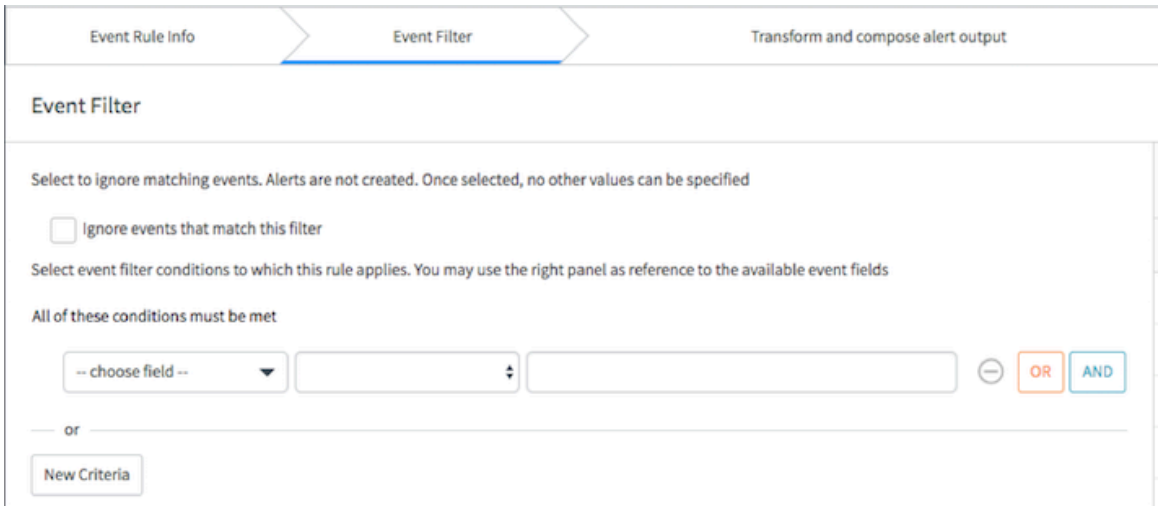
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie in der Event-Regelliste eine empfohlene Regel oder eine vorhandene Regel ausgewählt haben, werden die Filterfelder mit Werten aus diesen Events ausgefüllt. Sie können diese Filterfelder zum Erstellen von Filterbedingungen verwenden.
- Sie können auf eine andere Registerkarte (z. B. **Schwellenwert**) klicken, in diesem Bereich arbeiten und dann im Bereich „Event-Filter“ ohne Verlust von Informationen zur Arbeit zurückkehren.
- Verwenden Sie den rechten Bereich als Referenzquelle dafür, welche Felder zum Erstellen von Filterbedingungen verfügbar sind.

Hinweis: Ereignisfilter, die für Felder „additional_info“ erstellt wurden, führen nur einen Zeichenfolgenvergleich und keinen numerischen Vergleich durch, auch wenn die in das Feld „Wert“ eingegebenen Informationen wie in der folgenden Grafik dargestellt angezeigt werden:

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Klicken Sie auf **Neu**, oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Event-Filter**.



4. Um Events zu ignorieren, wählen Sie **Events ignorieren, die diesem Filter entsprechen** aus. Alle Events, die dieser Event-Regel entsprechen, werden ignoriert. Sie können dem Filter weitere Bedingungen hinzufügen, indem Sie entweder auf **ODER** oder **UND** klicken.

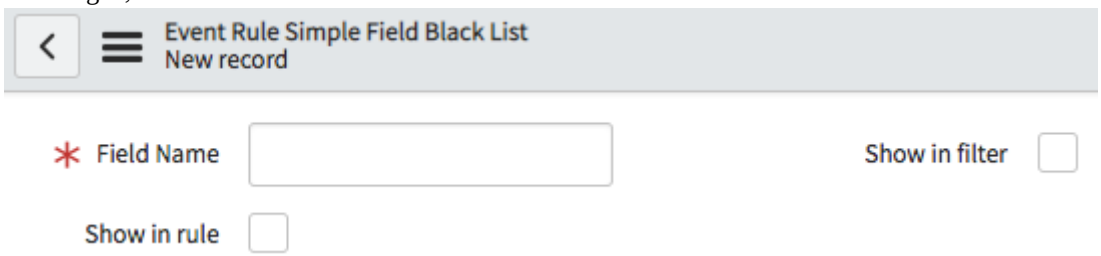
   Hinweis: Auch wenn ein Event von einer Event-Regel ignoriert wird, wird es in der Event-Tabelle [em_event] aufgezeichnet. Wählen Sie diese Option aus, um die Erstellung einer Warnung und deren Zuordnung zum Event zu verhindern.

5. Zum Konfigurieren von Bedingungen, für die die Event-Regel gelten muss, klicken Sie auf **Neue Kriterien**. Sie können weitere Bedingungen hinzufügen, indem Sie entweder auf **ODER** oder **UND** klicken.

   Hinweis: Das Zeichen **%** wird in Filterbedingungen nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Sie können Feldnamen zur Tabelle „Schwarze Listen für einfache Event-Regeln“ [em_event_rule_black_list] hinzufügen, um Felder im Filter ein- oder auszublenden.

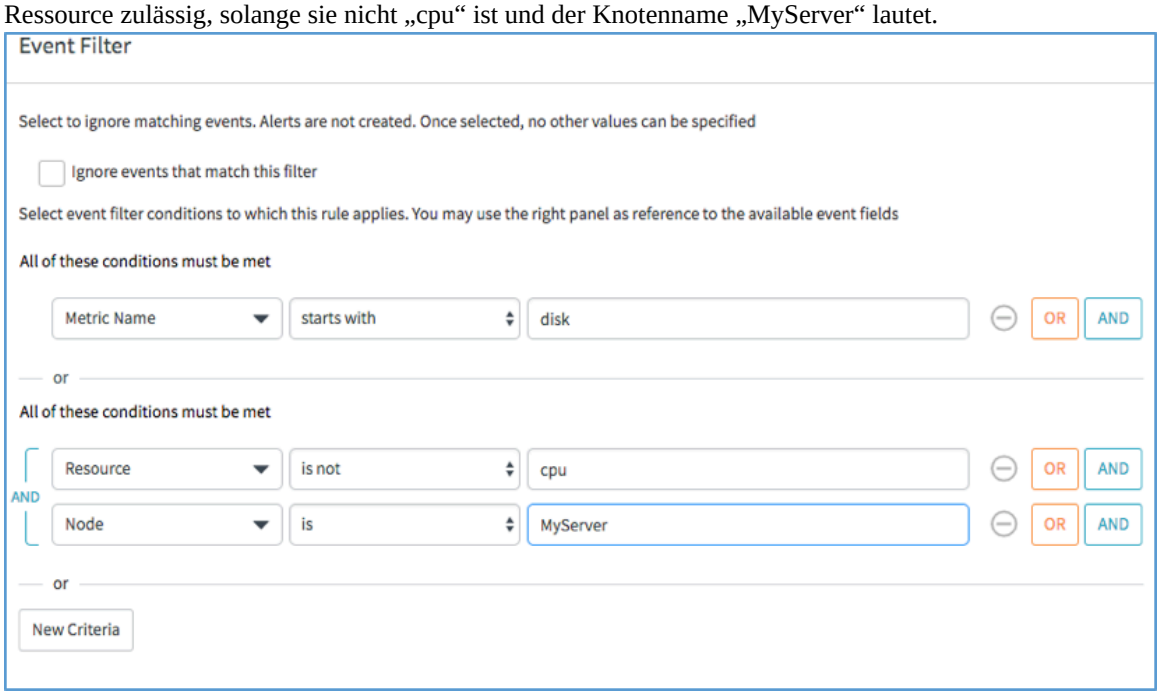


   - Um Felder aus dem Filter und dem rechten Bereich zu entfernen, fügen Sie ein neues Feld für schwarze Listen hinzu, in dem die Option **In Regel anzeigen** nicht ausgewählt ist.
   - Um Felder nur aus dem Filter zu entfernen und sie im rechten Bereich angezeigt zu lassen, fügen Sie ein neues Feld für die Ausschlussliste hinzu, in dem die Option **In Regel anzeigen** ausgewählt ist.

7. Klicken Sie entweder auf **Speichern** oder auf **Absenden**.

Example:

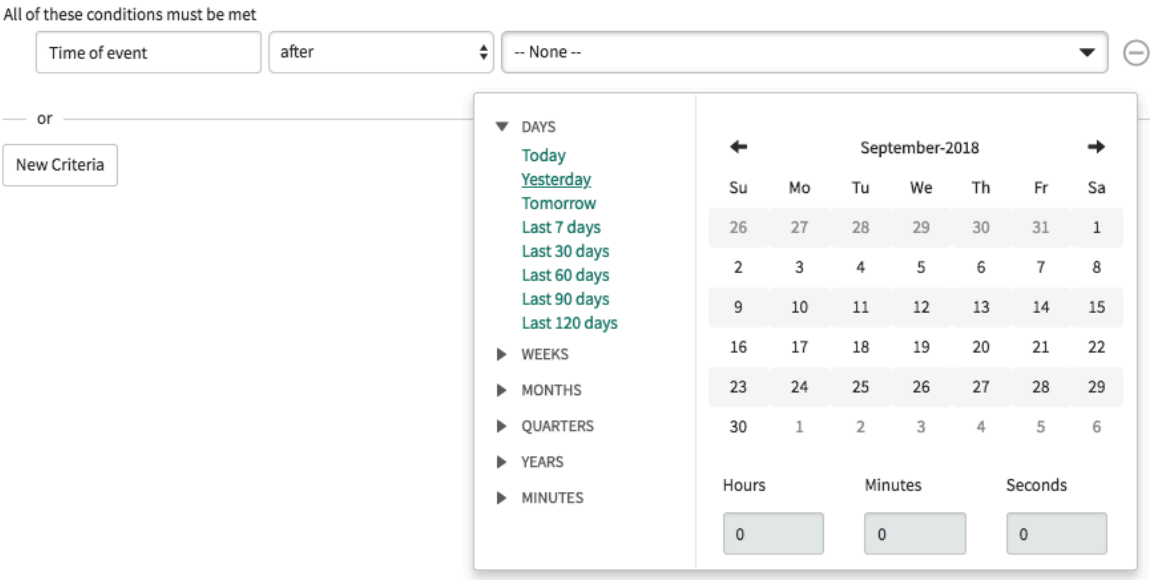
Beispiel für Filterbedingungen, die zum Ausführen einer Regel angegeben sind, wenn der Metrikname mit dem Wort „Disk“ beginnt. In diesem Beispiel ist jede Ressource zulässig, solange sie nicht „cpu“ ist und der Knotenname „MyServer“ lautet.



Beispiel für das Filtern von Events anhand von Zeitbedingungen. Wählen Sie im Feld **Feld auswählen oder neu hinzufügen** die Zeit des Events aus.

Geben Sie die erforderlichen Zeitbedingungen an, z. B. jederzeit nach gestern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zugehörige Informationen

- Event-Regel erstellen oder bearbeiten
- Event-Eingabeinformationen verwenden
- Event-Regel konfigurieren, um den Warnungsinhalt anzupassen
- Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Events finden, die nicht mit Regeln übereinstimmen

Suchen Sie nach Events, die keinen Regeln entsprechen, und stellen Sie fest, ob Event-Regeln zu deren Verwaltung erforderlich sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

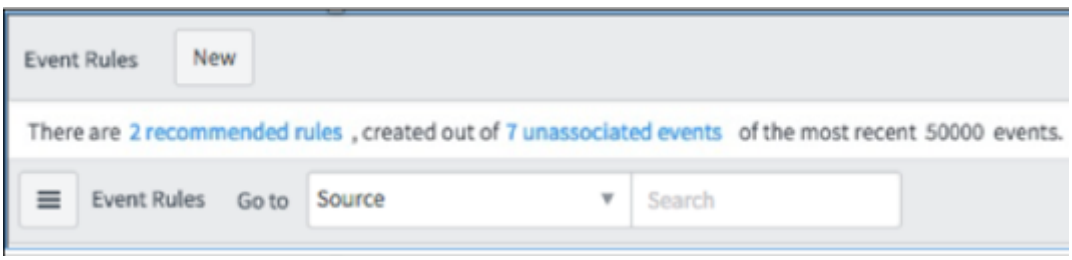
Warum und wann dieser Vorgang ausgeführt wird

In dieser Aufgabe wird beschrieben, wie Ereignisse gefunden werden, die nicht mit Regeln übereinstimmen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Klicken Sie oben im Formular auf den Link für Ereignisse oder gruppierte Ereignisse, die nicht Regeln zugeordnet sind.

Example



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Erstellen Sie eine Event-Regel. Beispielsweise sind Event-Regeln für die Verwaltung von Ereignissen nützlich, die regelmäßig auftreten.

Event-Regeln anzeigen

Sie können alle Event-Regeln in der Event-Regelliste anzeigen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.

Event-Regelliste

Feld	Beschreibung
Name	Der Name der Event-Regel.
Standardbindung überschreiben	Veraltete Bindungskriterien. Wenn im Abschnitt **Bindung** keine Kriterien angegeben wurden oder die angegebenen Bindungskriterien nicht erfüllt werden, werden die veralteten Bindungskriterien berücksichtigt.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Aktualisiert	Aktualisierung von Datum und Uhrzeit für die Regel.

Hinweis: Sie können die Event-Regelliste filtern, um die erforderliche Teilmenge der Informationen anzuzeigen. Wenn Sie jedoch nach dem Filtern einen Favoritenlink erstellen und auf den Link klicken, wird in der Liste der Event-Regeln nicht der richtige Filter angezeigt.

Zugehörige Informationen

Events anzeigen

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Sie können eine Event-Regel konfigurieren, um den Warnungsinhalt anzupassen. Sie können die Reihenfolge der Felder anpassen und auswählen, welche Felder angezeigt werden. Die Felder, die im linken Arbeitsbereich des Abschnitts **Warnungsausgabe umwandeln und verfassen** einer Event-Regel angezeigt werden, sind die Felder in der generierten Warnung.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Warnungsinhalte anpassen, indem Sie die erforderlichen Event-Felder hinzufügen und den Text in den Feldern ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen regulären Ausdruck für Eingaben erstellen, stellen Sie sicher, dass Sie Eingaben mit den Variablen in sequenzieller Reihenfolge erstellen. Variablen können zwar für die Aufnahme übersprungen werden, die ausgewählte Reihenfolge muss jedoch beibehalten werden.

Formatieren Sie den Warnungstext mit einer oder beiden dieser Methoden:

Warnungstext formatieren

Formatierungsmethode	Beschreibung
Umwandeln	Erstellen Sie ein Feld, das in einer Warnung angezeigt wird. Das Feld und sein Wert werden in angezeigt **Zusätzliche Informationen** Abschnitt oder in **Warnungs-Tags** Abschnitt. Im Bereich **Event-Eingabe** wird das neue Feld im Abschnitt **Ausdrücke** aufgeführt.
Verfassen	Bestimmen Sie, welcher Text im ausgewählten Feld angezeigt werden soll.

Hinweis:

- Bestimmen Sie durch Konfiguration der Ausschlussliste [em_event_rule_black_list], welche Felder im Fenster **Ereigniseingabe** angezeigt werden.

  Ein Feld, das der Ausschlussliste hinzugefügt wurde und bereits in einer vorhandenen Event-Regel enthalten ist, wird nicht aus der Regel entfernt. Stattdessen wird es in den Abschnitt **Manuelle Attribute** in der Regel verschoben.

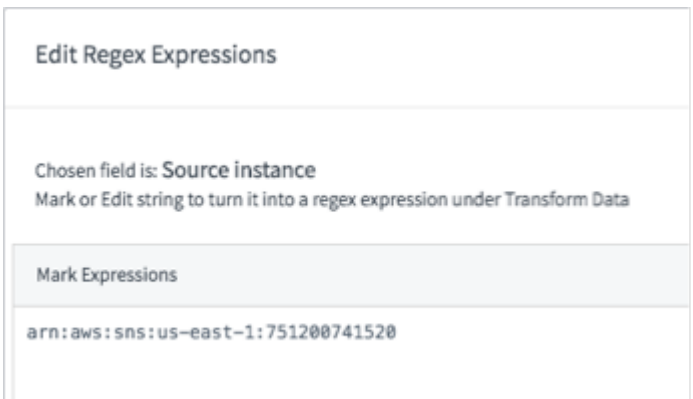
- Steuern Sie die Reihenfolge der Event-Formularfelder, indem Sie em_event_rule_order konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Klicken Sie auf **Neu**, oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Warnungsausgabe umwandeln und verfassen**.
   In diesem Abschnitt können Sie den **Umwandlungsmodus** und den **Verfassungsmodus** verwenden.
4. So wandeln Sie Informationen in Felder um – Standardmodus:

   Hinweis: In diesem Schritt erfolgt die Auswahl des Texts im Standardbearbeitungsmodus. In diesem Modus ist Rückgängigmachen verfügbar.

   a. Klicken Sie auf das erforderliche Feld im Bereich der Event-Eingabe. Der Wert und der Inhalt des ausgewählten Felds werden im Arbeitsbereich auf der linken Seite angezeigt.



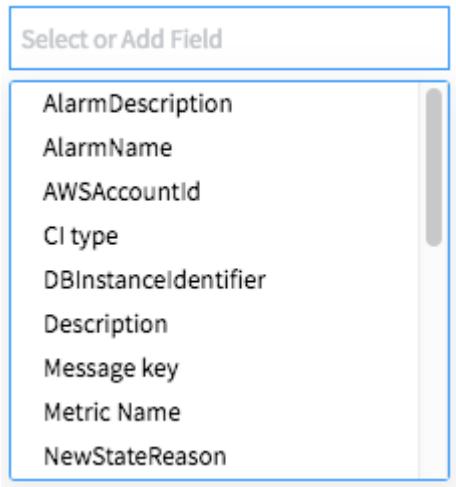
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Standardbearbeitungsmodus auswählen .

c. Markieren Sie den erforderlichen Text mit dem Bleistift-Cursor. Sie können auf Text im Feld doppelklicken, um ein Wort oder den erforderlichen Text und die gewünschten Symbole auszuwählen.

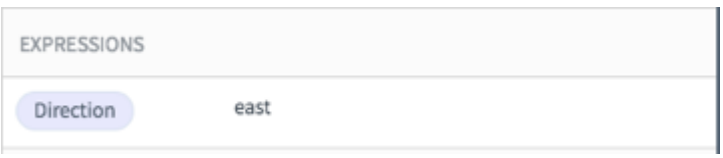
Hinweis: Wenn die **Eingabehilfe aktiviert** Accessibility enabled in den Systemeinstellungen ausgewählt ist, ist der Standardbearbeitungsmodus nicht verfügbar .

d. Wählen Sie einen Feldnamen aus der Liste aus, oder geben Sie den Namen des erforderlichen Ausdrucks ein. Felder, die in der Liste angezeigt werden, sind vorhandene Ereignisfelder, Felder mit zusätzlichen Informationen oder zuvor definierte Warnungs-Tags (Felder mit Präfix „t_“). Der Feldname wird im Bereich **Ausdrücke** angezeigt, und der ausgewählte Text wird hervorgehoben. Sowohl der Text als auch der Ausdrucksname werden in der gleichen Farbe hervorgehoben. Jeder zusätzliche Ausdruck, den Sie erstellen, und sein Wert wird in einer anderen Farbe hervorgehoben.



Hinweis: Umwandlungsfeldnamen dürfen kein ' (einzelnes Anführungszeichen) enthalten.

e. Klicken Sie auf **Erledigt**. Der Ausdrucksname wird im Abschnitt **Ausdrücke** des **Event-Eingabebereichs** angezeigt.



f. Wenn Sie auf einen Ausdruck oder seinen Wert im **Event-Eingabebereich** klicken, werden die Details im Arbeitsbereich auf der linken Seite angezeigt.

5. So wandeln Sie Informationen in Felder um – Modus regulärer Ausdruck:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Im Modus „regulärer Ausdruck“ ist Rückgängigmachen nicht verfügbar.
- Platzieren Sie beim Erstellen eines regulären Ausdrucks aus Variablen, die im Event hervorgehoben sind, die ausgewählten Variablen in der Reihenfolge, in der sie im Event-Feld angezeigt werden.
- Geben Sie beim Erstellen des regulären Ausdrucks der Event-Regel die Begriffe mithilfe einer genauen Übereinstimmung mit der Eingabe aus den Event-Feldern an. Beispiel: Für den Text `vhxy2stlgwc_8888_hec03v012979` sieht der reguläre Ausdruck

  ```
  ^([^_]+)_
  ```

  so aus, als ob er den Text `vhxy2stlgwc` abfangen soll, der vor dem Unterstrich angezeigt wird. Es funktioniert jedoch nicht, da dieser Text keine exakte Übereinstimmung ist. Verwenden Sie den vollständigen regulären Ausdruck wie folgt:

  ```
  ^([^_]+)_.*
  ```

- Als Engine für den regulären Ausdruck wird der Parser Java Matcher verwendet. Stellen Sie sicher, dass Sie einen Java-Parser verwenden, um den regulären Ausdruck zu testen.
- Wenn der reguläre Ausdruck beim Analysieren von Daten nicht mit der gesamten Zeichenfolge übereinstimmt, erfasst die Event-Regel das Event nicht, und es findet keine Analyse statt.
- Die Übereinstimmungsmethode der Java-Engine für reguläre Ausdrücke wird verwendet. Mit dieser Implementierung versucht die Engine für reguläre Ausdrücke, die gesamte Eingabesequenz mit dem angegebenen Muster abzugleichen. Andere Abgleichmethoden, z. B. die Find-Methode, werden nicht unterstützt.
- Standardmäßig sind keine Flags für reguläre Ausdrücke festgelegt, außer dem `Pattern.DOTALL`-Flag. Mit dieser Implementierung von Java für reguläre Ausdrücke entspricht das DOT-Zeichen „.“ einem beliebigen Zeichen, einschließlich Zeilenendezeichen.
- Abgesehen von `Pattern.DOTALL`können andere Flags für reguläre Ausdrücke nicht geändert werden.
- `Lookahead` wird unterstützt. `Lookbehind` wird jedoch nicht unterstützt.

a. Klicken Sie auf das erforderliche Feld im Bereich der Event-Eingabe. Der Wert und der Inhalt des ausgewählten Felds werden im Arbeitsbereich auf der linken Seite angezeigt.

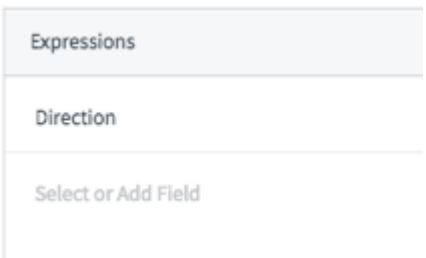
b. Wählen Sie den Bearbeitungsmodus reguläre Ausdrücke

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

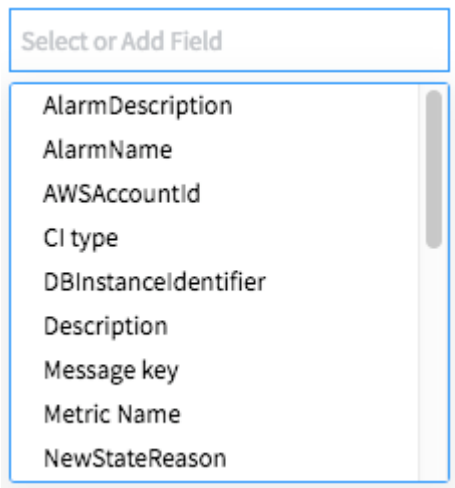
c. Wählen Sie den erforderlichen Text und die Symbole aus

. Ersetzen Sie den hervorgehobenen Text durch (. *), um einen regulären Ausdruck zu erstellen.

d. In **Ausdrücke** Klicken Sie auf den Bereich **Wählen Sie Feld aus oder fügen Sie Feld hinzu** Feld.



e. Wählen Sie einen Feldnamen aus der Liste aus, oder geben Sie den Namen des erforderlichen Ausdrucks ein. Felder, die in der Liste angezeigt werden, sind vorhandene Ereignisfelder, Felder mit zusätzlichen Informationen oder zuvor definierte Warnungs-Tags (Felder mit Präfix „t_“). Der Feldname wird in angezeigt **Ausdrücke** Bereich.



Hinweis: Umwandlungsfeldnamen dürfen kein ' (einzelnes Anführungszeichen) enthalten.

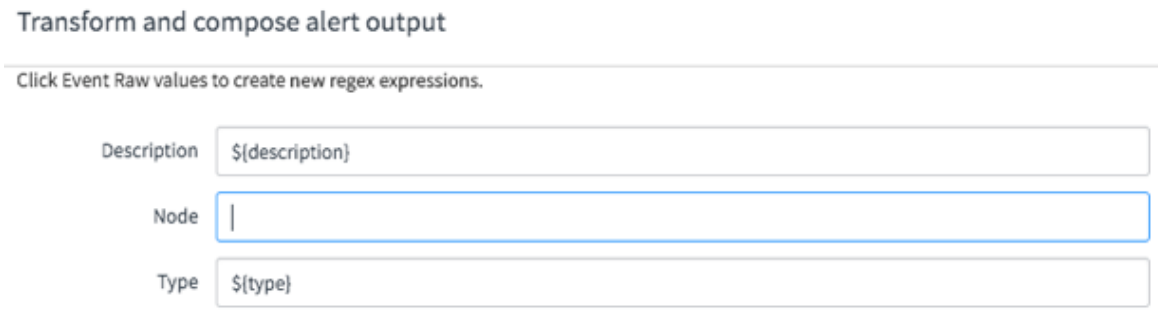
f. Klicken Sie auf **Erledigt**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Platzieren Sie beim Erstellen eines regulären Ausdrucks aus Variablen, die im Event hervorgehoben sind, die ausgewählten Variablen in der Reihenfolge, in der sie im Event-Feld angezeigt werden.
- Geben Sie beim Erstellen des regulären Ausdrucks der Event-Regel die Begriffe mithilfe einer genauen Übereinstimmung mit der Eingabe aus den Event-Feldern an. Beispiel: Für den Text „vhxy2stlgwc_8888_hec03v012979“ sieht der reguläre Ausdruck ^ ([^ _] +) _ so aus, als ob er den Text „vhxy2stlgwc“ abfangen soll, der vor dem Unterstrich angezeigt wird. Es funktioniert jedoch nicht, da dieser Text keine exakte Übereinstimmung ist. Verwenden Sie den vollständigen regulären Ausdruck wie folgt: ^([^_]+)_.*

6. Zum Verfassen von Text klicken Sie sich im Abschnitt „Warnungsausgabe umwandeln und verfassen“ in das erforderliche Feld.



Verfassen Sie Text in den Warnungsfeldern, indem Sie eine der folgenden Aktionen ausführen:

- Ziehen Sie ein Feld aus dem Event-Informationsbereich in das erforderliche Feld.
- Verwenden Sie den Event-Informationsbereich als Referenz für verfügbare Felder. Schreiben Sie die Feldnamendetails im Format ${<fieldname>}, wobei „$“ für „Wert verwenden“ steht. Zwischen den Klammern ersetzt der Name des Event-Felds die Variable <fieldname>.
- Geben Sie Text mit Leerzeichen oder Sonderzeichen ein. Verwenden Sie beispielsweise Leerzeichen oder Unterstriche (_), um den Text im Warnungsfeld lesbar zu machen.

7. Um Felder anzugeben, die in der generierten Warnung angezeigt werden sollen, wählen Sie aus **Manuelle Attribute** Kontrollkästchen.

Hinweis: Diese Felder und ihre Werte werden im angezeigt **Zusätzliche Informationen** Abschnitt oder in **Warnungs-Tags** Abschnitt für Attribute mit dem Präfix „t_“.

a. Geben Sie in der linken Spalte einen Wert ein.

b. Ziehen Sie in der rechten Spalte entweder einen Wert aus den Feldern Hinzufügen oder Ausdruck, oder geben Sie einen Wert ein.
Bei der Eingabe eines Werts mit Attributen mit dem Präfix „t_“ wird eine Dropdown-Liste mit allen zuvor definierten „t_“-Attributen angezeigt.

8. Klicken Sie auf **Speichern** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sie können Event-Regeln filtern. Weitere Informationen finden Sie unter Events filtern, für die eine Event-Regel gilt.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

Event-Eingabeinformationen verwenden

Warnungstags

Events filtern, für die eine Event-Regel gilt

Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Der Event-Schwellenwert ist die Rate, mit der Ereignismanagement eine Warnung generiert. Der Empfang mehrerer Events für ein Gerät in einem kurzen Intervall kann die Erstellung einer Warnung rechtfertigen, da die Bedingung schwerwiegend sein kann. Der Empfang von Events über einen längeren Zeitraum kann jedoch auf eine weniger schwerwiegende Situation hinweisen, die das Erstellen einer Warnung nicht rechtfertigt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Eigenschaften in einer Event-Regel konfigurieren, um Warnungen zu erstellen, die Warnungsgenerierung zu unterdrücken oder vorhandene Warnungen gemäß einem bestimmten Schwellenwert zu schließen. Der Schwellenwert basiert auf dem Wert von Event-Feldern oder der Anzahl der Vorkommen über einen angegebenen Zeitraum.

Hinweis: **Feldname** kann im Feld **Zusätzliche Informationen** des Events der Name eines numerischen Feldes sein. Deshalb gilt: Wenn die `CPU` ein zusätzliches Informationsfeld für ein bestimmtes Event ist, dann kann die `CPU` als **Feldname**verwendet werden.

Angenommen, Sie möchten eine Warnung generieren, wenn die CPU-Auslastung dreimal mit maximal 20 Sekunden zwischen zwei aufeinanderfolgenden Ereignissen 80 % erreicht oder überschreitet. Erstellen Sie eine Event-Regel mit diesen Einstellungen (eine Erklärung für jeden Wert finden Sie in Klammern):

- **Warnoperator erstellen**: >= (Operator, um zu bestimmen, ob die Nutzung des **Feldnamens** den angegebenen Wert erreicht oder überschreitet)
- **Feldname**: *`CPU`* (Events im Zusammenhang mit hoher CPU-Auslastung)
- **Schwellenwert**: *`80`* (Prozent)
- **Vorkommnisse**: *`3`* (drei Events, bei denen die CPU-Auslastung bei „> =“ 80 % oder darüber liegt)
- **Über Zeitraum (Sekunden)**: *`20`* (20 Sekunden oder weniger zwischen Events)

Zum Demonstrieren der Auswertung der vorherigen Einstellungen wird davon ausgegangen, dass die folgenden Events empfangen werden:

Szenario	Ergebnis
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event:	In diesem Szenario wird keine Warnung generiert, da ein Event eine CPU-Auslastung aufweist, die unter 80 % liegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Ergebnis
• Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 80 • Verstrichene Zeit seit dem dritten Event 60, CPU = 70	
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event: • Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 90 • Verstrichene Zeit seit dem dritten Event 70, CPU = 95	In diesem Szenario wird keine Warnung generiert, da die verstrichene Zeit in einem Event die angegebenen 20 Sekunden überschreitet.
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event: • Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 95 • Verstrichene Zeit seit dem dritten Event 60, CPU = 90	In diesem Szenario wird eine Warnung generiert, da die verstrichene Zeit in allen Events innerhalb der angegebenen Zeit liegt und die CPU-Auslastung über 80 % beträgt.

Hinweis:

- Beim Konfigurieren einer Event-Regel zum Erstellen oder Schließen von Warnungen gemäß einem Schwellenwert werden Events, die zur gleichen Sekunde eintreffen, wie vom Feld `time_of_event` bestimmt, übersprungen. Dies geschieht, da diese Events als Duplikate betrachtet werden.
- Wenn Schwellenwertbedingungen konfiguriert sind, werden Warnungen geschlossen, wenn die Bedingung für **Warnoperator schließen** erfüllt wird, und nicht, wenn ein Event mit **Schweregrad = Klar** oder **Lösungsstatus = Schließen**empfangen wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Erstellen oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Schwellenwert**.
4. Wählen Sie **Aktiv** aus.
   Wenn **Aktiv** nicht ausgewählt ist, werden die Felder auf dieser Seite nicht angezeigt.
5. Wählen Sie im Feld **Warnoperator erstellen** einen Operator aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie **Anzahl** wählen, geben Sie die entsprechenden Werte für **Vorkommnisse** und **Über Zeitraum (Sekunden)** an.
- Wenn Sie einen anderen Operator als auswählen **Anzahl** , **Feldname** Und **Schwellenwert** Felder werden angezeigt. Geben Sie die erforderlichen Werte in diese Felder ein.

  Hinweis: Der Wert von **Schwellenwert** Die Eigenschaft kann der Name eines beliebigen Felds in sein **Zusätzliche Informationen** Des Ereignisses. Beispiel: Wenn `CPU` Ist ein Feld in **Zusätzliche Informationen** Für ein bestimmtes Ereignis dann `CPU` Kann als verwendet werden **Schwellenwert** .

- Geben Sie im Feld **Vorkommnisse** den erforderlichen Wert an.
- Geben Sie im Feld **Über Zeitraum (Sekunden)** den erforderlichen Zeitraum an.

6. Zum automatischen Schließen von Warnungen wählen Sie im Feld **Warnoperator schließen** einen Operator aus.
   Entsprechend Ihrer Auswahl werden zusätzliche Felder angezeigt.
   - Wenn **Anzahl** als Operator für das Feld **Warnoperator erstellen** angegeben ist, dann ist die Auswahl im Feld **Warnoperator schließen** entweder `Keine` oder `Inaktiv`. Geben Sie den erforderlichen Wert an.
   - Wenn Sie **Inaktiv**auswählen, konfigurieren Sie das Feld **Über Zeitraum (Sekunden)**.
   - In **Schließen Sie Den Warnungsoperator** Feld, wenn Sie einen anderen Operator als auswählen **Inaktiv** , Konfigurieren Sie dann **Schwellenwert** , **Tritt Auf** , Und **Über (Sekunden)** Felder.
7. Klicken Sie auf **Speichern** oder auf **Absenden**.

Example:
So erstellen Sie eine Warnung, wenn ein bestimmtes Event fünf Mal in 10 Minuten auftritt – unter **Schwellenwert**:

1. In **Feldname** Feld den Namen eines beliebigen Felds angeben, das in vorhanden ist **Zusätzliche Informationen** Feld im Ereignis. Der Wert des Felds ist irrelevant.
2. Wählen Sie im Feld **Warnoperator erstellen** `Anzahl` aus.
3. Geben Sie im Feld **Vorkommnisse** `5` an.
4. Geben Sie im Feld **Über Zeitraum** `600` (10 * 60 Sekunden) an.
5. Klicken Sie auf **Speichern** oder auf **Absenden**.

So erstellen Sie eine Warnung, wenn ein bestimmtes Event fünf Mal in 10 Minuten auftritt – mit einem Metrikwert über 55. Nehmen Sie an, dass „metric_value“ ein Feld in den **Zusätzlichen Informationen** des Events ist. Geben Sie Folgendes an:

1. Aktivieren Sie das Kontrollkästchen *`Active`*.
2. Wählen Sie im Feld **Warnoperator erstellen** `>=` aus.
3. In **Feldname** Feld angeben **Metrik_Wert** .
4. In **Schwellenwert** Feld angeben `55` .
5. Geben Sie im Feld **Vorkommnisse** `5` an.
6. Geben Sie im Feld **Über Zeitraum** `600` (10 * 60 Sekunden) an.
7. Klicken Sie auf **Speichern** oder auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

Event-Eingabeinformationen verwenden

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Events filtern, für die eine Event-Regel gilt

Warnungen werden an CIs gebunden

Die CI-Bindung oder -Verknüpfung ist der Prozess zum Suchen und Verbinden eines Konfigurationselements (Configuration Item, CI) aus dem Configuration Management Database (CMDB) Zu einer Warnung unter Verwendung der in Ereignisregeln definierten Logik. Dies trägt dazu bei, sicherzustellen, dass Warnungen an die richtigen IT-Komponenten gebunden sind, um die Transparenz zu verbessern und Probleme schneller zu lösen.

CI-Bindung verstehen

Durch die Bindung von Warnungen an CIs werden eingehende Warnungen mit dem richtigen Konfigurationselement (Configuration Item, CI) verknüpft, das einen bestimmten Host darstellt, z. B. einen Computer, Server, Router oder eine virtuelle Maschine in Ihrer IT-Infrastruktur. Dies stellt eine genaue Warnungsnachverfolgung sicher, vereinfacht die Problembehandlung, indem die Ursache von Problemen identifiziert wird, und verwaltet einen Verlaufsdatensatz von Warnungen, die an bestimmte Systeme gebunden sind.

In IT Operations Management, Die Beziehung zwischen Warnungen und CIs spielt eine entscheidende Rolle bei der effektiven Verwaltung von Services und Infrastruktur. Ein CI stellt eine Komponente in Ihrer IT-Umgebung dar, z. B. einen Server, eine Anwendung oder eine Datenbank. Durch die Verknüpfung von Warnungen mit CIs wird sichergestellt, dass Warnungen und Incidents direkt mit der betroffenen Komponente verknüpft sind, was eine genaue Auswirkungsanalyse und eine schnellere Lösung ermöglicht.

In dynamischen und großen Umgebungen ist es oft schwierig zu bestimmen, welches CI für die Auslösung einer Warnung verantwortlich ist. Warnungen werden aus Rohereignisdaten generiert, die über mehrere Quellen hinweg erfasst wurden, diese Daten verweisen jedoch möglicherweise nicht explizit auf ein CI. Ohne eine zuverlässige Methode zum Binden von Warnungen an CIs stehen IT-Teams vor dem Risiko:

- Schlechter Einblick in die Serviceauswirkung.
- Längere durchschnittliche Zeit bis zur Lösung (MTTR).
- Ineffiziente Warnungsverwaltungsprozesse.

Ereignisregeln bieten eine strukturierte Möglichkeit, eingehende Ereignisdaten zu analysieren, mit zusätzlichem Kontext zu ergänzen und dem richtigen CI zuzuordnen. Diese Regeln fungieren als Brücke und wandeln Rohereignisdaten in umsetzbare Warnungen um, die mit CIs verknüpft sind. Ereignisregeln können beispielsweise:

- Eingehende Ereignisdaten analysieren: Der Prozess umfasst die Aufgliederung von Rohereignisdaten, um wichtige Details wie Hostnamen, IP-Adressen oder Service-Tags zu extrahieren. Diese Details werden dann verwendet, um das Ereignis zu analysieren – Quelle, Typ und Auswirkung zu identifizieren – und um die Warnung durch Hinzufügen relevanter Kontexte wie betroffene Services, Prioritäten oder Lösungsschritte zu bereichern, um sicherzustellen, dass es für IT-Teams umsetzbar ist.
- Übereinstimmungsmuster: Hier werden die extrahierten Ereignisdetails wie Hostnamen, IP-Adressen oder Service-Tags mit Einträgen in verglichen CMDB Dient zur Identifizierung des entsprechenden Konfigurationselements (Configuration Item, CI) basierend auf vordefinierten Regeln oder Logik. Nach dem Abgleich wird die Warnung mit dem CI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verknüpft und bietet Kontext zur betroffenen IT-Komponente, um die Transparenz zu verbessern und die Lösung zu beschleunigen.

- Binden Sie das CI an die Warnung: An diesem Punkt wird die Warnung automatisch dem identifizierten CI zugeordnet. Es stellt sicher, dass die Warnung mit der richtigen IT-Komponente im System verbunden ist, was die Nachverfolgung und Verwaltung erleichtert und Teams hilft, das Problem schnell zu beheben.

Typen der CI-Bindung

Bindungstyp	Beschreibung
Implizite Knotenbindung (Standardbindung)	Bindet Warnungen an Host-CIs, indem sie mit übereinstimmen **Knoten** Feld im Ereignis mit Attributen wie Name, FQDN, IP oder MAC-Adresse.
CI-Feld, das der Bindung entspricht	Bindet Warnungen mit **CI-Bezeichner** Feld, eine JSON-Struktur mit Spaltennamen und -Werten (z. B. Name, FQDN, IP oder MAC-Adresse).
CI-Identifizierungsbindung	Bindet Warnungen mithilfe von Ereignisregeln an bestimmte Anwendungen auf Hosts.
Bindung auf Prozessebene	Bindet Warnungen an Anwendungs-CIs, indem prozessbezogene Attribute abgeglichen werden.
Bindung auf Geräteebene	Bindet Warnungen an Geräte-CIs, indem Ereignisdaten mit Attributen wie Hostname, IP-Adresse oder MAC-Adresse abgeglichen werden.

Hauptvorteile

- Verbesserte Servicetransparenz: Mit CIs verknüpfte Warnungen bieten ein klares Bild davon, welche IT-Komponenten betroffen sind.
- Verbesserte Automatisierung: Automatisierte CI-Bindung reduziert den manuellen Aufwand und stellt Konsistenz sicher.
- Schnellere Lösung: Teams können Probleme schnell diagnostizieren und lösen, indem sie sich auf das betroffene CI konzentrieren.

Beispiel für einen Anwendungsfall

Szenario: Der E-Mail-Server eines Unternehmens mit dem Namen MailServer-01 fällt aus.

Prozess:

1. Warnungsgenerierung: Eine Warnung wird ausgelöst, wenn MailServer-01 nicht mehr reagiert.
2. CI-Bindung: Ereignismanagement sucht automatisch nach MailServer-01 in der CMDB (Configuration Management Database).
   - Wenn gefunden, wird die Warnung mit diesem bestimmten Server (CI) verknüpft.
   - Wenn nicht gefunden, bleibt die Verknüpfung der Warnung aufgehoben, bis weitere Informationen bereitgestellt werden.

Ergebnis: Die Warnung zeigt jetzt an, dass MailServer-01 das betroffene System ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Auswirkung: IT-Teams wissen sofort, welcher Server untersucht werden soll.
- Effizienz: Sie müssen keine anderen Infrastrukturkomponenten oder -Systeme überprüfen, was Zeit und Aufwand spart.

Dieser direkte Link hilft, die Problembehandlung zu optimieren, indem er auf die genaue Problemquelle verweist.

Zugehörige Informationen

Ereignisverarbeitung simulieren

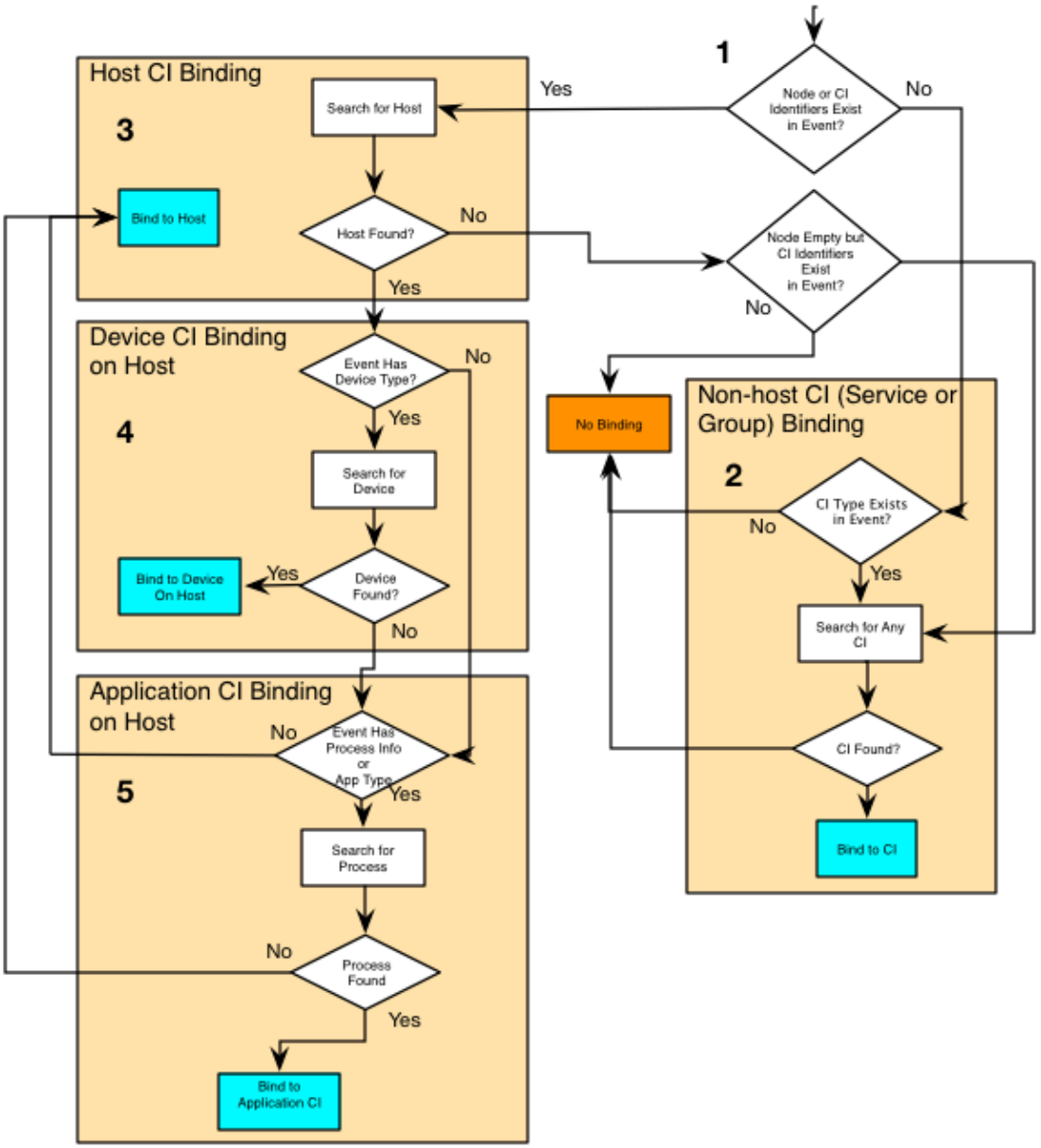
Bindungsprozess-Flow

Erfahren Sie mehr über den Prozess der Bindung von Konfigurationselementen (Configuration Items, CIs) an Warnungen. Dies umfasst die Verarbeitung der Ereignisanmeldung, die Bindung von Warnungen mithilfe verfügbarer Felder, wenn kein Knoten vorhanden ist, und die Suche nach CMDB Für übereinstimmende Hosts. Außerdem wird die Verknüpfung von Warnungen mit CIs basierend auf der Host- und CI-Typerkennung erläutert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Bindung an Warnungen: Flow-Diagramm



Prozess der Verknüpfung von CIs mit Warnungen

1. Ereignis-Ankunft: Wenn ein Ereignis empfangen wird, Ereignismanagement Sucht nach Knoten- oder CI-Bezeichnern.
2. Ist Knotenwert Vorhanden?
   - Ja: Wenn ein Knotenwert angegeben wird, Ereignismanagement Durchsucht CMDB Für einen übereinstimmenden Host.
   - Nein: Wenn kein Knoten gefunden wird, versucht das System, die Warnung anhand anderer verfügbarer Details zu binden, z. B.:
     - Warntyp
     - Zusätzliche Informationen
     - CI-Identifier

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Host- und CI-Typerkennung:
   - Beide gefunden: Wenn sowohl ein Host als auch ein CI-Typ identifiziert werden, wird die Warnung mit dem entsprechenden Geräte-CI verknüpft.
   - Nur gefundener Host: Wenn nur ein Host identifiziert wird, verknüpft das System die Warnung mit einem Anwendungs-CI.

Zusätzliche Überlegungen

- Ereignisverarbeitungsnotizen: Das Ereignis kann den Bindungsprozess-Flow in enthalten **Verarbeitungsnotizen** Feld, das Einblicke in die Bindungsaktionen bietet.
- Bindung an stillgelegte CIs: Standardmäßig werden Ereignisse nicht an CIs mit dem Status „stillgelegt“ gebunden. Um die Bindung an diese CIs zu aktivieren, legen Sie fest *evt_mgmt.ignore_retired_cis_in_binding*Eigenschaft auf „falsch“.
- CI-Status für die Bindung angeben: Sie können konfigurieren *evt_mgmt.install_status_list_to_ignore_in_binding*Eigenschaft, indem CI-Statusnummern angegeben werden, um zu steuern, welche CIs für die Bindung berücksichtigt werden. Zum Beispiel:

CI-Status

Statusnummer	Status
1	Installiert
2	OnOrder
3	InMaintenance
4	PendingInstall
5	PendingRepair
6	InStock
7	Retired
8	Gestohlen
100	Abwesend

Hinweis: Um mehrere Status anzugeben, trennen Sie jede Statusnummer durch ein Komma.

Warnungen an ein bestimmtes Host-CI binden (Standardbindung)

Binden von Warnungen an Konfigurationselemente (Configuration Items, CIs) mithilfe von **Knoten** Feld oder **CI-Bezeichner** Das Feld stellt eine genaue Ereigniszuordnung sicher. Durch Vergleich von Ereignisdatensätzen **Knoten** Oder **CI-Bezeichner** Wert, Warnungen sind mit dem richtigen System verknüpft. Dies verbessert die Reaktion, die Ursachenanalyse und die Auswirkungsbewertung, indem klare Einblicke in betroffene Assets gewährt werden.

Funktionsweise der Standardbindung

Das System kann die Standardbindung mit durchführen **Knoten** Feld oder **CI-Bezeichner** Feld aus dem Ereignisdatensatz.

Wenn ein Ereignis in das System eintritt, wird ein Schlüsselfeld wie **Knoten** Ist im Ereignisdatensatz verfügbar. Es gibt jedoch keine **Knoten** Feld im CI. Stattdessen wird der Knotenwert aus dem Ereignis mit verschiedenen Attributen im Host-CI verglichen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

z. B. Name, Fully Qualified Domain Name (FQDN), IP oder MAC-Adresse. Wenn eine Übereinstimmung gefunden wird, wird die Warnung mit dem entsprechenden CI verknüpft. Dies ist die Standardmethode zum Binden von Warnungen an CIs.

Hinweis: In diesem Bindungsprozess muss das CI ein Host sein. Host-CIs umfassen Computer, Betriebssysteme (OS), Switches, Router oder alle CI-Typen/-Klassen, die die Tabelle [cmdb_ci_Hardware] erweitern, was bedeutet, dass der CI-Typ oder die CI-Klasse eine Hardwarekomponente sein muss.

Wenn mit dem Knoten keine Übereinstimmung gefunden wird, sucht das System nach **CI-Bezeichner** Feld im Ereignisdatensatz. Die **CI-Bezeichner** Ist eine JSON-Struktur, die Spaltennamen und -Werte für den Vergleich enthält (z. B. Name, vollqualifizierter Domänenname, IP oder MAC-Adresse). Die JSON ist: {"column_Name":"<column_value>"}. Zum Beispiel, wenn wir eine Bindung an ein von identifiziertes CI vornehmen möchten **Serial_number** Dessen Wert ist **Dell Latitude 7420-Laptop** , Die JSON ist: `{"Serial_number":"Dell Latitude 7420 Laptop"}` . Wenn eine Übereinstimmung gefunden wird, wird die Warnung mit dem entsprechenden CI verknüpft.

Unterschied zwischen Bindung mit Knoten und . CI-Identifier

In der Standardbindung berücksichtigt das System alle Felder in **Zusätzliche Informationen** Feld und versucht, ihre Werte mit der CI-Tabelle abzugleichen. Die **CI-Bezeichner** Das Feld ermöglicht die Angabe bestimmter Felder für den Abgleich, auch wenn sie in nicht vorhanden sind **Zusätzliche Informationen** . Dieser Prozess verwendet eine vordefinierte JSON-Struktur und Gilt nur, wenn das CI ein Host ist.

Hinweis: Auch wenn **Knoten** Oder **CI-Bezeichner** Bindet die Warnung erfolgreich mit dem CI. Ereignisregeln bestimmen weiter, wie die Bindung mithilfe von erfolgt **Standardbindung überschreiben** Kontrollkästchen in Ereignisregeln verfügbar. Dadurch wird sichergestellt, dass Warnungen ordnungsgemäß basierend auf der Geschäftslogik gebunden werden, nicht nur auf direkten Übereinstimmungen. Dadurch wird sichergestellt, dass Warnungen ordnungsgemäß basierend auf der Geschäftslogik gebunden werden, nicht nur auf direkten Übereinstimmungen.

Beispiel: CI mithilfe von Knoten- und Ereignisregeln auflösen

Stellen Sie sich vor, ein Server (Server-123) in Ihrem Netzwerk generiert ein Ereignis. Der Ereignisdatensatz enthält einen **Knoten** Feld mit dem Wert „Server-123.example.com“.

1. Übereinstimmung mit CI-Attributen:
   a. Das System überprüft den Knotenwert anhand der CMDB.
   b. Sie vergleicht „Server-123.example.com“ mit dem FQDN, der IP, der MAC-Adresse oder dem Namen vorhandener Host-CIs.
   c. Wenn eine Übereinstimmung gefunden wird (z. B. ist FQDN in der CMDB auch „Server-123.example.com“), wird die Warnung mit diesem CI verknüpft.
2. Ereignisregeln werden angewendet: Auch wenn der Knoten in Server-123 aufgelöst wird, können zusätzliche Ereignisregeln bestimmen, ob die Warnung unterschiedlich verknüpft werden soll. Beispielsweise kann eine Ereignisregel festlegen, dass Warnungen von Server-123 mit einem übergeordneten CI (z. B. einem Cluster) und nicht mit dem einzelnen Server verknüpft werden sollen.

Standardbindung wird überschrieben

Das Überschreiben der Standardbindung ermöglicht Flexibilität beim Verknüpfen von Warnungen mit CIs über den standardmäßigen knotenbasierten Abgleich hinaus. Dies hilft, die Warnungsbindung an die Geschäftsanforderungen anzupassen, genaue Zuordnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sicherzustellen und falsch verknüpfte Warnungen zu verhindern, das Incident-Management und die Ursachenanalyse zu verbessern.

Standardmäßig werden Warnungen an CIs gebunden, indem der Knotenwert in der Warnung mit Attributen wie Name, FQDN, IP oder MAC-Adresse im CI abgeglichen wird. Wenn Sie dieses Verhalten jedoch ändern möchten, indem Sie zusätzliche Kriterien verwenden oder den Knoten vollständig ignorieren, können Sie verwenden **Standardbindung Überschreiben** Kontrollkästchen.

Dies ermöglicht zwei Szenarien:

1. Wenn Bindetyp = CI-Feldübereinstimmung
   - Wenn das CI ein Host ist, ist der Knoten für die Bindung erforderlich. Weitere Informationen finden Sie unter Binden Sie Host-CIs mithilfe der CI-Feldübereinstimmung.
   - Wenn das CI kein Host ist, muss der Knoten leer sein. Weitere Informationen finden Sie unter Binden Sie nicht-Host-CIs mithilfe der CI-Feldübereinstimmung.
2. Wenn Bindetyp = CI-Identifikation. Weitere Informationen finden Sie unter Binden Sie Warnungen mithilfe der CI-Identifizierung an CIs.

Diese Flexibilität stellt sicher, dass Warnungen basierend auf bestimmten Geschäftsanforderungen korrekt verknüpft werden.

Hinweis: Sie können auch verwenden Service Operations-Arbeitsbereich Zum Definieren von Bindungsregeln. Weitere Informationen finden Sie unter Erstellen Sie eine Anreicherungsautomatisierung.

Binden Sie Host-CIs mithilfe der CI-Feldübereinstimmung

Wenn die CI-Feldübereinstimmung verwendet wird und das CI ein Host ist, wird der Knotenwert aus der Warnung für die Bindung verwendet. Das System vergleicht den Knoten mit Attributen wie Name, FQDN, IP oder MAC-Adresse in der CMDB, um eine Übereinstimmung zu finden. Dadurch wird sichergestellt, dass Warnungen korrekt mit dem entsprechenden Host-CI verknüpft sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Ereignis in das System eintritt, Schlüsselfeld wie **Knoten** Ist im Ereignisdatensatz verfügbar. Die **Knoten** Das Feld stellt im Allgemeinen den Namen des Servers dar.Im CI gibt es kein Feld wie **Knoten** . Der Wert von jedoch **Knoten** Aus dem Ereignis wird mit verschiedenen Werten im Host-CI verglichen, z. B. Name, vollqualifizierter Domänenname (FQDN), IP oder MAC-Adresse. Wenn eine Übereinstimmung gefunden wird, wird die Warnung mit dem entsprechenden CI verknüpft. Dies ist die Standardbindung von Warnungen an CIs. In dieser Bindung muss das CI ein Host sein. Host-CIs umfassen Computer, BS, Switches, Router – im Wesentlichen alle CI-Typen oder -Klassen, die die Tabelle [cmdb_ci_Hardware] erweitern.

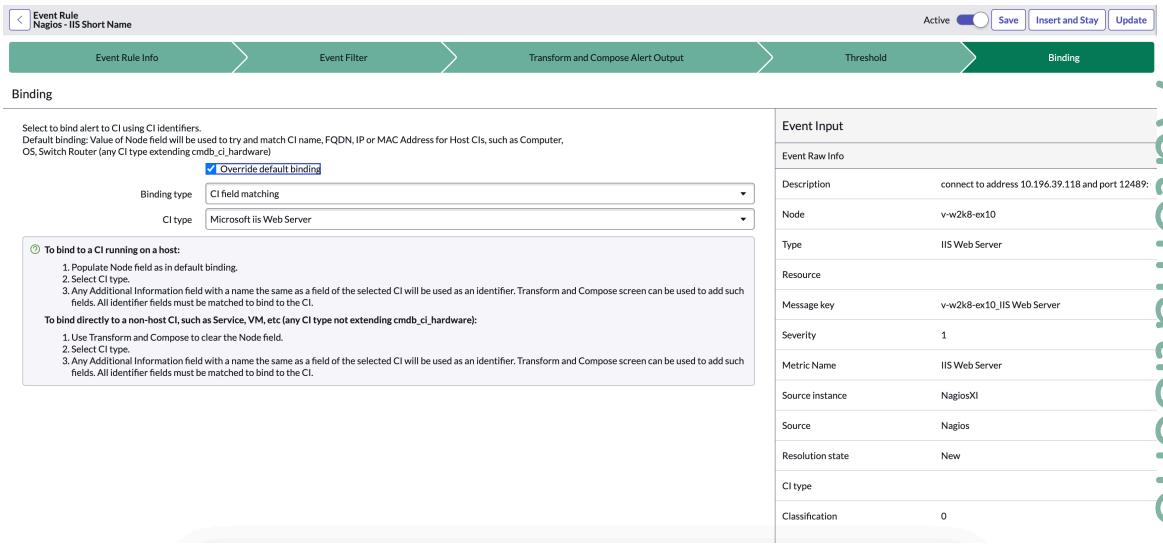
Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, der der Tabellenspalte entspricht, um sicherzustellen, dass der Abgleichprozess erfolgreich fortgesetzt wird. Informationen zum Erstellen eines manuellen Felds finden Sie unter Binden Sie CIs mithilfe von CI-Feldübereinstimmung und Verarbeitung von Spaltennamenunterschieden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Auch wenn der Knoten die Warnung erfolgreich an das CI bindet, bestimmen Ereignisregeln weiter, wie die Bindung erfolgt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie Aus **Neu** Und füllen Sie die erforderlichen Felder der Ereignisregel aus.
3. Wählen Sie aus **Bindung** Registerkarte.
4. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.
5. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.



6. In **CI-Typ** Feld den entsprechenden Typ der Hardwarekomponente (z. B. Server, Router oder Speichergerät) auswählen, die der CI-Typ darstellt.
   Die **CI-Typ** Bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht. Beispiel: Wenn **CI-Typ** Ist **Netzwerkadapter** , Sucht das System in der Tabelle [cmdb_ci_Network_Adapter].
7. Wählen Sie **Absenden**.

Hinweis: Sie können auch verwenden Service Operations-Arbeitsbereich Zum Definieren von Bindungsregeln. Weitere Informationen finden Sie unter Erstellen Sie eine Anreicherungsautomatisierung.

Zugehörige Informationen

Binden Sie nicht-Host-CIs mithilfe der CI-Feldübereinstimmung

Binden Sie Warnungen an ein bestimmtes Gerät

Binden Sie jede Warnung direkt an das Ursprungsgerät, um eine eindeutige Auswirkungsquelle zu ermitteln. Dies stellt eine genaue Fehlerbehebung sicher, reduziert das Rauschen durch nicht zugehörige Warnungen und hilft Teams, sich auf die schnellere Lösung des richtigen Problems zu konzentrieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

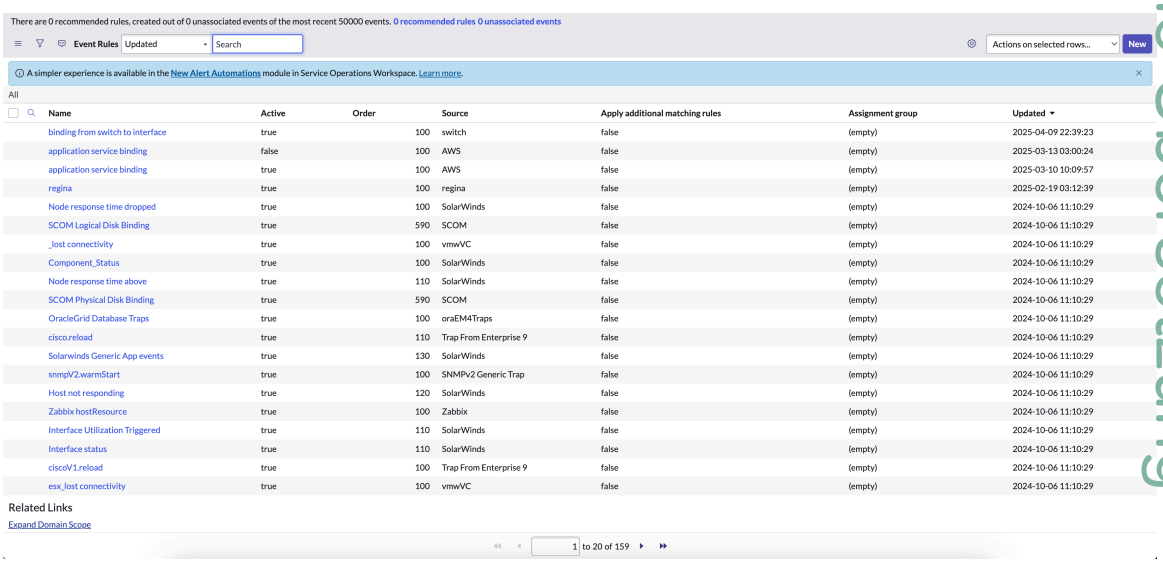
Warum und wann dieser Vorgang ausgeführt wird

In IT-Umgebungen haben mehrere Geräte wie Switches viele kleinere Komponenten, z. B. Ports. Wenn etwas schief geht, reicht es nicht aus, nur zu sagen, dass der Switch ein Problem hat – das System muss genau bestimmen, welcher Port das Problem verursacht. Durch die Bindung von Warnungen an den spezifischen Port, der das Problem ausgelöst hat, können Teams schneller handeln und das tatsächliche Problem beheben, ohne Zeit mit der Überprüfung des gesamten Switches oder nicht zugehöriger Komponenten zu verschwenden.

Das folgende Beispielverfahren zeigt die Konfiguration der Warnungsbindung für einen Switch mit dem Namen IP-Switch-1, um sicherzustellen, dass Warnungen auf den richtigen Port abzielen. Das Setup der Ereignisregel beginnt mit der Aktivierung von **Standardbindung überschreiben** Option und Auswahl **CI-Feldübereinstimmung** Als **Bindungstyp** . Auswahl **Switchport** Als **CI-Typ** Weist das System an, Warnungen an einzelne Ports zu binden. Die Bindungsgerätezuordnung definiert, wie das System den Switch (cmdb_ci_ip_Switch) mithilfe des Referenzfelds cmdb_ci mit seinen Ports (dscy_switchport) verknüpft. Diese Zuordnung leitet die Bindungslogik. Unter **Konfiguration** > **Netzwerk** > **Switches**, Auswahl **IP-Switch-1** Zeigt die Switchports und Schnittstellennamen an. Wenn ein eingehendes Ereignis einen übereinstimmenden Schnittstellennamen in enthält **Zusätzliche Informationen** Feld bindet das System die Warnung direkt an den richtigen Port, um einen präzisen und aussagekräftigen Warnungskontext sicherzustellen.

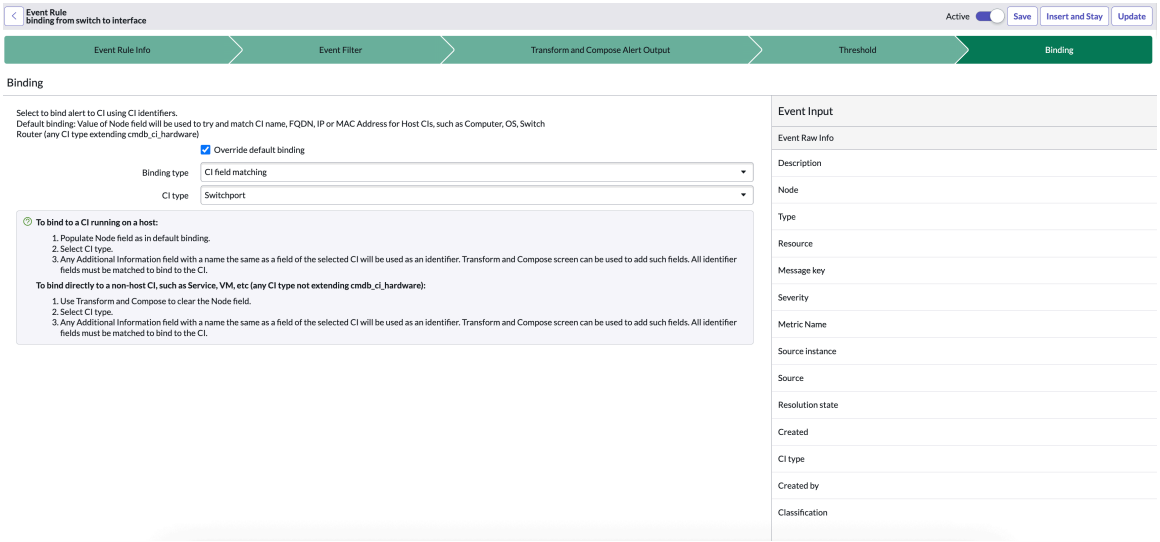
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie **Neu**.

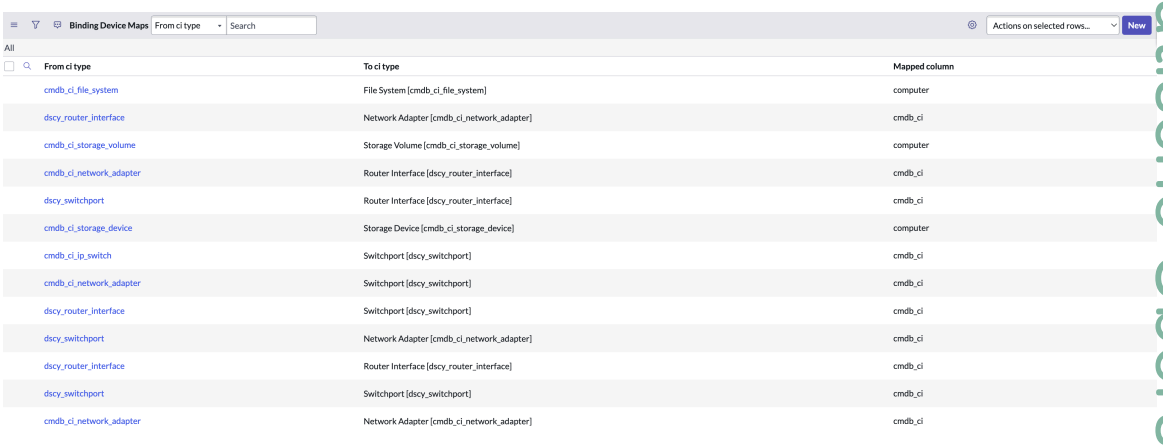


3. Wählen Sie aus **Bindung** Registerkarte.
4. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.
5. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.
6. In **CI-Typ** Feld auswählen **Switchport** .
   Die **CI-Typ** Bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

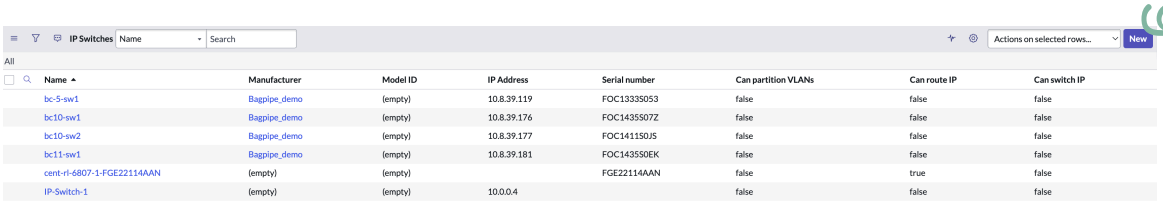


7. Navigieren Sie zu **Alle** Und suchen EM_Binding_device_Map.list .
   Die Seite „Bindungsgerätezuordnungen“ wird geöffnet. Hier die Spaltenwerte **Von ci-Typ** Ist zugeordnet zu **An ci-Typ** Mit **Zugeordnete Spalte** . Beispiel: **cmdb_ci_ip_Switch** Wird der Switchport-Tabelle [dscy_switchport] mithilfe des Referenzfelds zugeordnet **cmdb_ci** .



From ci type	To ci type	Mapped column
cmdb_ci_file_system	File System [cmdb_ci_file_system]	computer
dscy_router_interface	Network Adapter [cmdb_ci_network_adapter]	cmdb_ci
cmdb_ci_storage_volume	Storage Volume [cmdb_ci_storage_volume]	computer
cmdb_ci_network_adapter	Router Interface [dscy_router_interface]	cmdb_ci
dscy_switchport	Router Interface [dscy_router_interface]	cmdb_ci
cmdb_ci_storage_device	Storage Device [cmdb_ci_storage_device]	computer
cmdb_ci_ip_switch	Switchport [dscy_switchport]	cmdb_ci
cmdb_ci_network_adapter	Switchport [dscy_switchport]	cmdb_ci
dscy_router_interface	Switchport [dscy_switchport]	cmdb_ci
dscy_switchport	Network Adapter [cmdb_ci_network_adapter]	cmdb_ci
dscy_router_interface	Router Interface [dscy_router_interface]	cmdb_ci
dscy_switchport	Switchport [dscy_switchport]	cmdb_ci
cmdb_ci_network_adapter	Network Adapter [cmdb_ci_network_adapter]	cmdb_ci

8. Navigieren Sie zu **Alle** Und suchen Wechselt Und wählen Sie aus **Konfiguration** > **Netzwerk** > **Switches**an.
   Die Seite IP-Switches wird geöffnet.

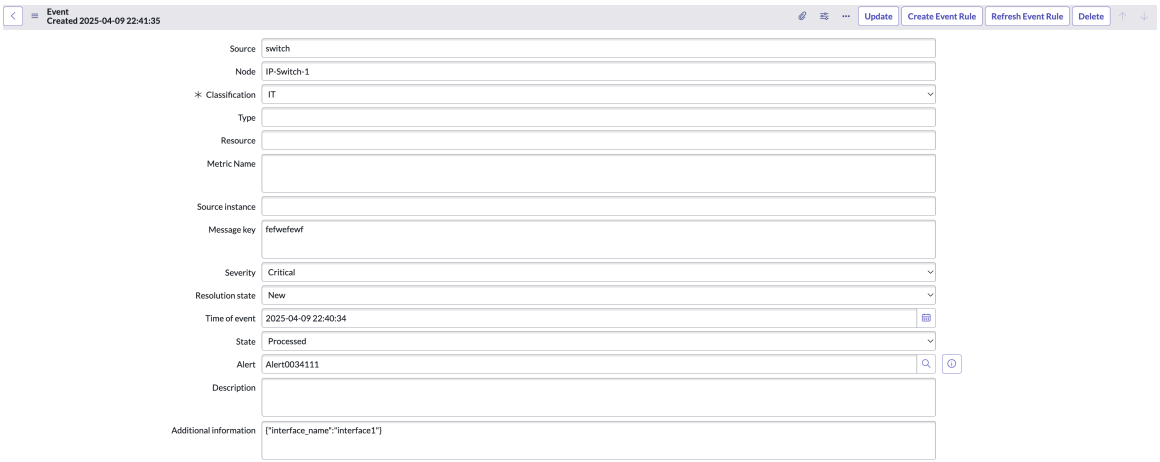


Name	Manufacturer	Model ID	IP Address	Serial number	Can partition VLANs	Can route IP	Can switch IP
bc-5-sw1	Bagpipe_demo	(empty)	10.8.39.119	FOC13335053	false	false	false
bc10-sw1	Bagpipe_demo	(empty)	10.8.39.176	FOC14355072	false	false	false
bc10-sw2	Bagpipe_demo	(empty)	10.8.39.177	FOC14115QJ5	false	false	false
bc11-sw1	Bagpipe_demo	(empty)	10.8.39.181	FOC14355QEK	false	false	false
cent-rl-6807-1-FGE22114AAN	(empty)	(empty)		FGE22114AAN	false	true	false
IP-Switch-1	(empty)	(empty)	10.0.0.4		false	false	false

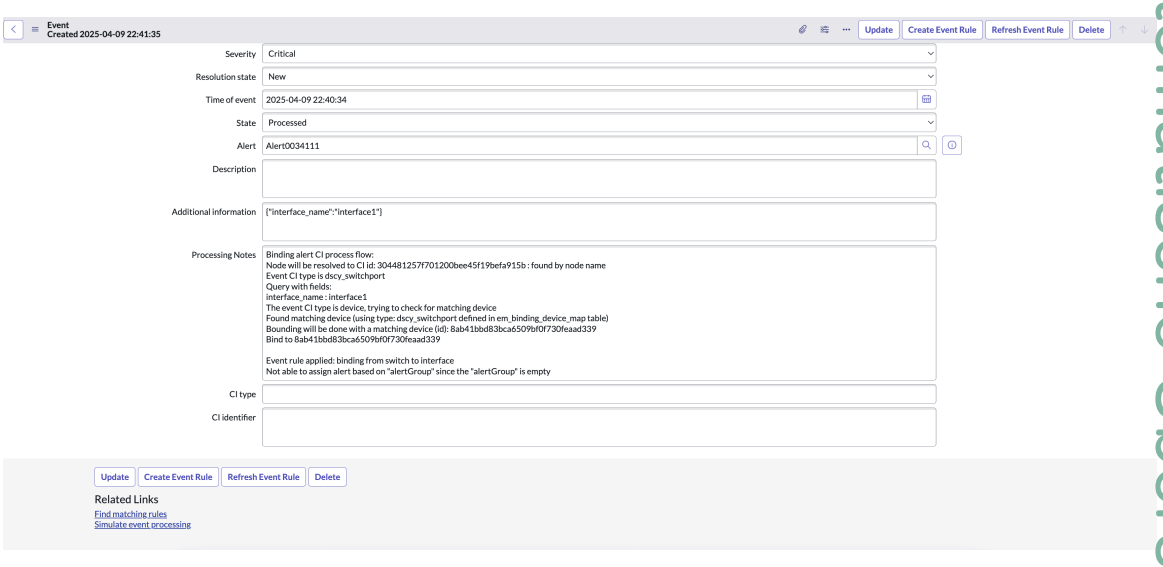
9. Wählen Sie Aus **IP-Switch-1** Zum Anzeigen der Detailseite.
10. Wählen Sie aus **Switchports** Registerkarte.
11. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
12. Wählen Sie das Ereignis mit aus **Knoten** Wert als **IP-Switch-1** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In der folgenden Abbildung sehen Sie die Verarbeitungsnotizen, die darauf hinweisen, dass die Bindung zwischen der Warnung und dem übereinstimmenden Gerät aufgetreten ist.



Binden Sie Warnungen an einen bestimmten Prozess

Binden Sie bestimmte Serverprozesse an die entsprechenden Konfigurationselemente (Configuration Items, CIs) in der CMDB, um eine genaue Zuordnung und Sichtbarkeit sicherzustellen. Diese Bindung ist entscheidend, um Serviceabhängigkeiten zu identifizieren, Mehrdeutigkeiten von generischen Prozessnamen zu reduzieren und eine effektive Überwachung zu ermöglichen. Es unterstützt eine schnellere Warnungslösung, Auswirkungsanalyse und eine bessere Ausrichtung zwischen Infrastruktur- und Anwendungskomponenten in dynamischen Umgebungen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Warnung (oder ein Ereignis) in das System eingeht, muss sie manchmal mit einem Konfigurationselement (CI) in der CMDB verbunden oder „gebunden“ werden. Standardmäßig bindet das System Warnungen an den in angegebenen Host **Knoten** Feld des Ereignisses. Stellen Sie sich eine Situation vor, in der ein Windows-Server mehrere Prozesse ausführt, z. B. MSFT SQL-Instanzen und SQL Server Analysis Services. Die Herausforderung besteht darin, ein Ereignis an die spezifische Prozessinstanz und nicht nur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

an den Hostserver zu binden, da mehrere Prozesse denselben generischen Namen haben können, z. B. MSSQLSERVER, was zu Mehrdeutigkeiten führen kann.

Das folgende Beispielverfahren verwendet einen Windows-Server als Host, MSFT SQL-Instanzen als CI-Klasse des Prozesses und MSSQLSERVER als Prozessname. Die folgenden Schritte basieren auf der Annahme, dass das Ereignis **Knoten** Das Feld des Ereignisses enthält den Hostnamen und **Zusätzliche Informationen** Feld enthält bestimmte Prozessdetails, die für die Bindung erforderlich sind.

Alert-to-CI-Bindung über Prozesszuordnung

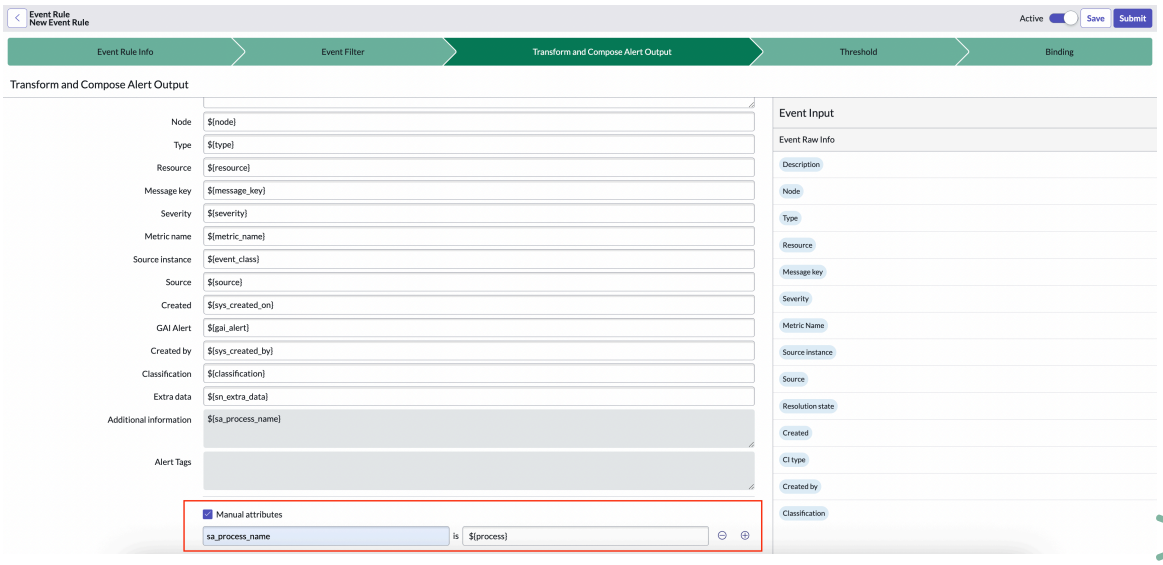
Aktion	Schritte
Ereignisregel festlegen: Prozessnamen hinzufügen	Fügen Sie den Prozessnamen hinzu `sa_Process_Name` In der Ereignisregel.
Ereignisregel festlegen: CI-Typ definieren	Wählen Sie den Ziel-CI-Typ in der Ereignisregel aus. Beispiel: MSFT SQL-Instanzen.
Definieren Sie die Prozesszuordnung	Navigieren Sie zur Tabelle „Prozess-zu-CI-Typzuordnung“ [em_Binding_Process_Map], und fügen Sie einen Eintrag hinzu, der einen CI-Typ (z. B. MSFT SQL-Instanzen) einem Prozessnamen (z. B. MSSQLSERVER) zuordnet.
CI an Warnung binden	Wenn ein Ereignis ausgelöst wird, führt das System folgende Schritte aus: **1.** Wendet die Standardbindung an, um den Host zu identifizieren. **2.** Überprüft den in der Ereignisregel angegebenen CI-Typ. **3.** Sucht in der Tabelle „Prozess-zu-CI-Typzuordnungen“ [em_Binding_Process_Map] nach einem übereinstimmenden Prozessnamen und CI-Typ. **4.** Durchsucht die Tabelle „CI-Beziehungen“ [cmdb_rel_ci.list] nach einer „wird ausgeführt am::ausgeführt“-Beziehung zwischen dem Prozess und dem Host-CI. **5.** Bindet an einen Prozess, wenn Werte aus dem **CI-Typ** Spalte stimmt mit den entsprechenden Einträgen in überein **Prozess** Spalte in der Tabelle „Zuordnungen von Prozess zu CI-Typ“ [em_Binding_Process_Map].

Automatische Übersetzung

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie **Neu**.
3. Wählen Sie aus **Warnungsausgabe umwandeln und verfassen** Registerkarte und führen Sie die folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Wählen Sie aus **Manuelle Attribute** Kontrollkästchen.

b. Geben Sie Ein sa_Process_Name Ist ${Process} .

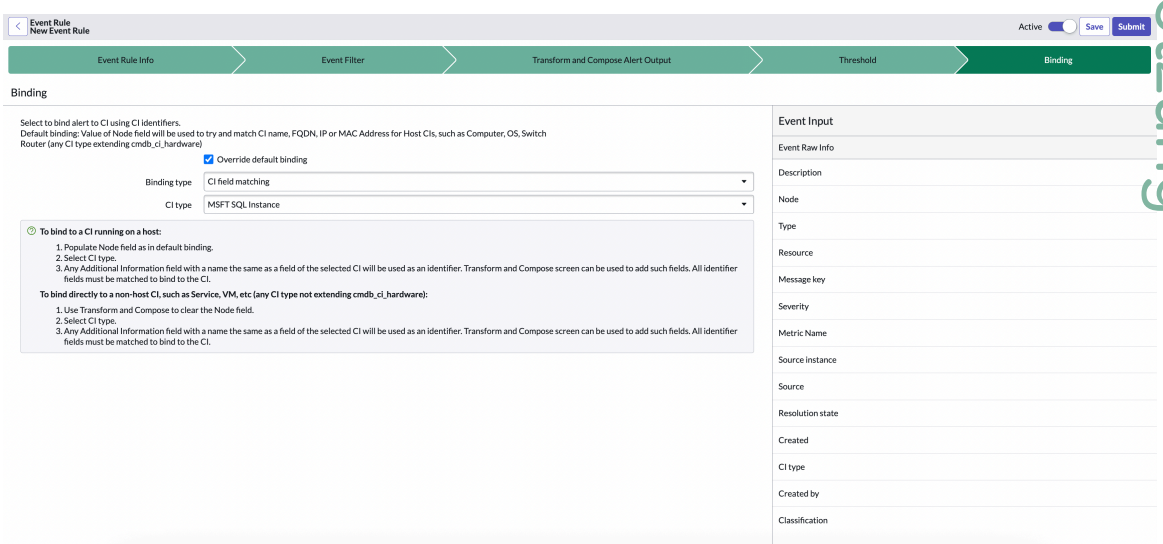
sa_Process_Name ist ein spezieller Variablenname, der verwendet wird, um den Namen des zu suchenden Prozesses anzugeben. ${sa_Process_Name} wird in angezeigt **Zusätzliche Informationen** Feld des Ereignisses. Anstelle von ${Process} , Sie können einen beliebigen anderen Feldnamen eingeben, aus dem die Variable stammt sa_Process_Name Leitet seinen Wert ab.

4. Wählen Sie aus **Bindung** Registerkarte.

5. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.

6. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.

7. In **CI-Typ** Feld auswählen **MSFT SQL-Instanzen** .
Die **CI-Typ** Bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht.

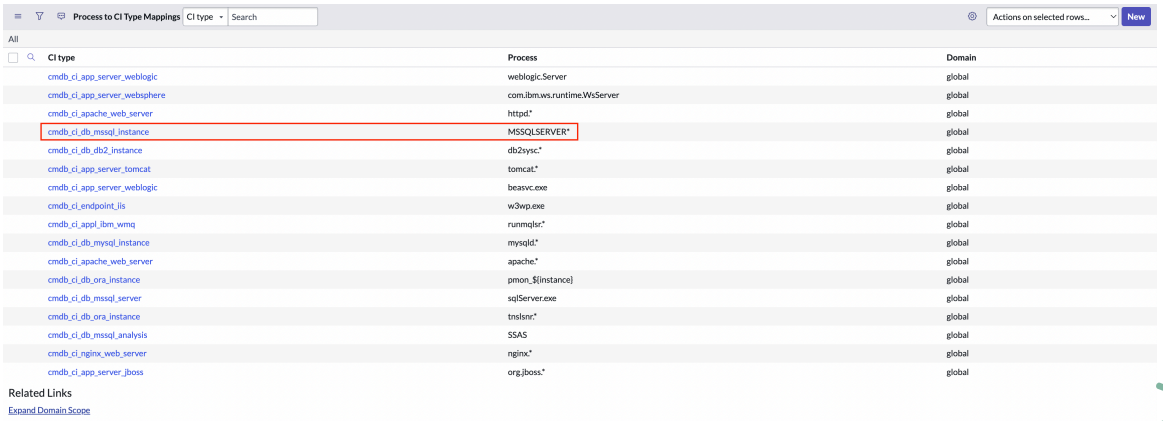


8. Navigieren Sie zu **Alle** Und suchen EM_Binding_Process_Map.list .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

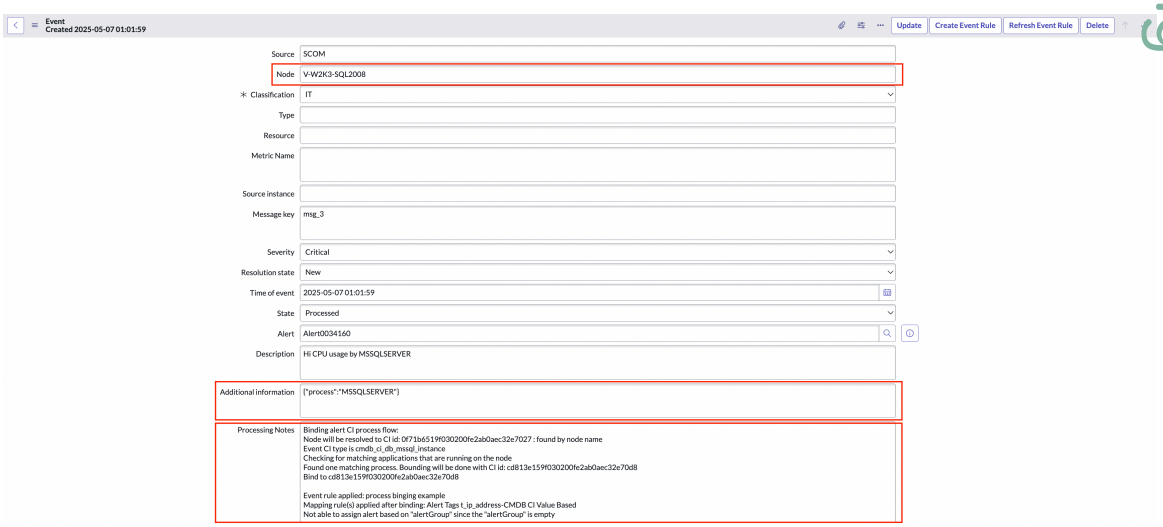
Die Seite „Zuordnungen von Prozess zu CI-Typ“ wird geöffnet. Hier die Werte aus dem **CI-Typ** Spalten werden Einträgen in zugeordnet **Prozess** Spalte. Beispiel: **cmdb_ci_DB_mssql_instance** Ist dem zugeordnet **MSSQLSERVER** Prozess.



9. **Wahlweise:** Navigieren Sie zu **Alle** Und suchen `cmdb_rel_ci.list` .
   Die Seite „CI-Beziehungen“ wird geöffnet.
10. **Wahlweise:** Überprüfen Sie, ob sich der Knoten in einer Beziehung „Ausführungen auf::Ausführungen“ mit dem entsprechenden Prozess befindet.

11. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
12. Erstellen Sie ein Ereignis mit **Knoten** Wert als Name des Hosts, z. B. Windows Server (V-W2K3-SQL2008).
    Die **Zusätzliche Informationen** Das Feld im Ereignis hat einen Schlüssel namens **Prozess** Dessen Wert ist **MSSQLSERVER** .

    In der folgenden Abbildung sehen Sie die Verarbeitungsnotizen, die darauf hinweisen, dass die Bindung zwischen der Warnung und dem Übereinstimmungsprozess aufgetreten ist.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Binden Sie nicht-Host-CIs mithilfe der CI-Feldübereinstimmung

Wenn keine Übereinstimmung mit gefunden wird **Knoten** Feld verwendet das System **CI-Bezeichner** Feld zum Abgleichen von Warnungen mit nicht-Host-CIs basierend auf Attributen wie Name, FQDN, IP oder MAC. Dies stellt eine genaue Warnungszuordnung sicher, verbessert die Transparenz, die Fehlerbehebung und die Ursachenanalyse für verschiedene Infrastrukturkomponenten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

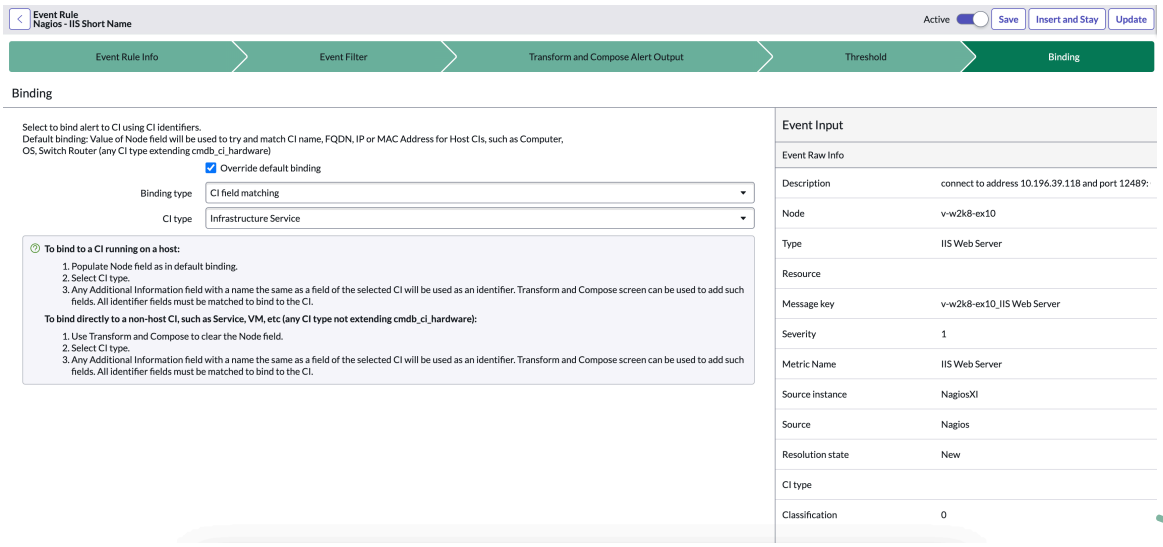
Wenn keine Übereinstimmung mit gefunden wird **Knoten** Feld betrachtet das System **Zusätzliche Informationen** Feld der Warnung. Wenn Sie einen CI-Typ auswählen, z. B. „Dateisystem“, sucht das System automatisch nach einem übereinstimmenden Datensatz in der Tabelle [cmdb_ci_file_System]. Es werden die Details verwendet, die im Ereignisregeldatensatz angegeben sind, insbesondere in **Zusätzliche Informationen** Feld, um die Suche zu verfeinern. Beispiel: Wenn **Zusätzliche Informationen** Feld enthält Werte wie `{"Mount_Point": "/SNAP/amazon-ssm-Agent/9565", "Name": "/dev/loop0"}` , Sucht das System nach einem Datensatz in der Tabelle [cmdb_ci_file_System], der diesen Werten entspricht. Wenn eine Übereinstimmung gefunden wird, bindet das System das CI an die Warnung, um eine genaue Identifizierung und Zuordnung sicherzustellen. Ähnlich, wenn **CI-Typ** Ist **Netzwerkadapter** , Sucht das System in der Tabelle [cmdb_ci_Network_Adapter].

Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, der der Tabellenspalte entspricht, um sicherzustellen, dass der Abgleichprozess erfolgreich fortgesetzt wird. Informationen zum Erstellen eines manuellen Felds finden Sie unter Binden Sie CIs mithilfe von CI-Feldübereinstimmung und Verarbeitung von Spaltennamenunterschieden.

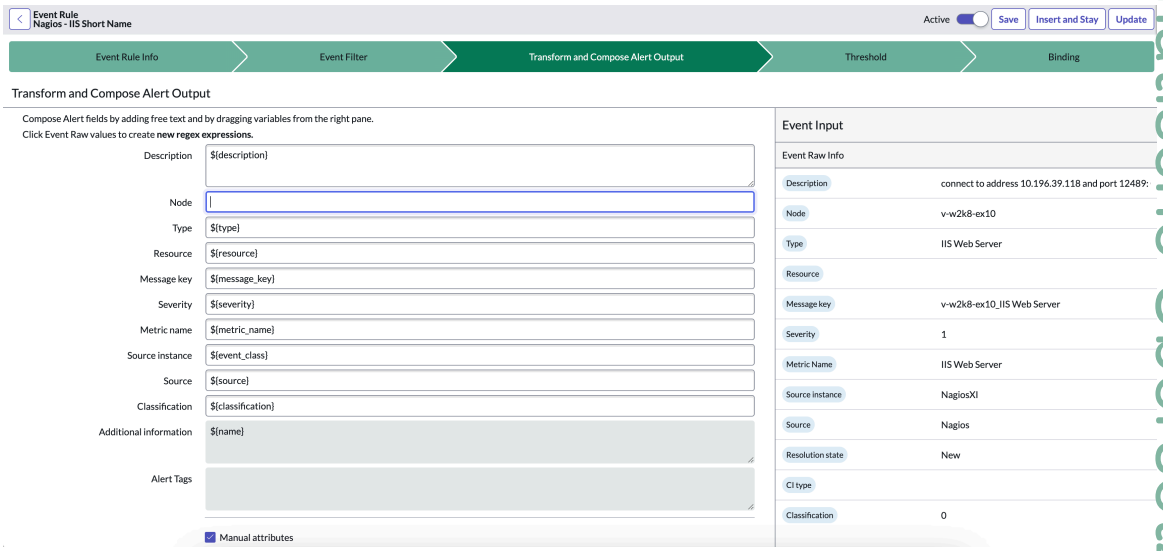
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie Aus **Neu** Und füllen Sie die erforderlichen Felder der Ereignisregel aus.
3. Wählen Sie aus **Bindung** Registerkarte.
4. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.
5. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie aus **Warnungsausgabe umwandeln und verfassen** Registerkarte.
7. Löschen Sie **Knoten** Feldwert.



8. In **CI-Typ** Feld das nicht-Host-CI auswählen.

   Ein nicht-Host-CI-Typ ist ein beliebiger CI-Typ, der die Tabelle [cmdb_ci_Hardware] nicht erweitert, z. B. ein Service oder eine VM. Die **CI-Typ** Bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht.

9. Wählen Sie **Speichern**.

Binden Sie CIs mithilfe von CI-Feldübereinstimmung und Verarbeitung von Spaltennamenunterschieden

Binden Sie CIs nach übereinstimmendem Ereignis **Zusätzliche Informationen** Felder mit CI-Attributen. Wenn sich die Spaltennamen unterscheiden, erstellen Sie manuell ein zusätzliches Schlüssel-Wert-Paar, das an der CI-Tabelle ausgerichtet ist, um eine genaue CI-Zuordnung sicherzustellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

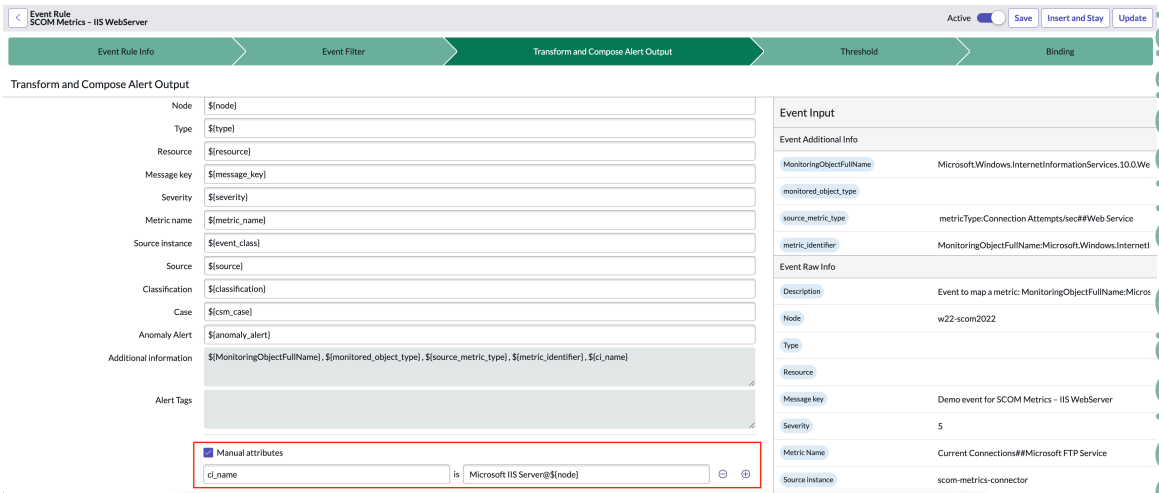
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn keine Übereinstimmung mit gefunden wird **Knoten** Feld betrachtet das System **Zusätzliche Informationen** Feld im Ereignisdatensatz. Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, der der Tabellenspalte entspricht, und es der hinzufügen **Zusätzliche Informationen** Feld, das sicherstellt, dass der Übereinstimmungsprozess erfolgreich fortgesetzt wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie Aus **Neu** Und füllen Sie die erforderlichen Felder aus, oder öffnen Sie einen vorhandenen Ereignisregeldatensatz, um ihn zu ändern.
3. Wählen Sie aus **Warnungsausgabe umwandeln und verfassen** Registerkarte.
4. Wählen Sie aus **Manuelle Attribute** Kontrollkästchen.
5. In **Feldname** Und **Feldwert** Felder den entsprechenden Feldnamen eingeben und das Quellfeld angeben, aus dem der Wert ausgefüllt werden soll.



Verwenden Sie das Hinzufügen-Symbol (⊕) Symbol zum Hinzufügen mehrerer Felder nach Bedarf.

6. Wählen Sie **Speichern**.
   Die Felder werden im Ereignisregeldatensatz erstellt. Wenn jedoch eine Warnung aus einem Ereignis mithilfe der Ereignisregel generiert wird, werden die manuell hinzugefügten Felder im angezeigt **Zusätzliche Informationen** Feld der Warnung.

Binden Sie Warnungen mithilfe der CI-Identifizierung an CIs

Binden Sie Warnungen mithilfe von Ereignisregeln an bestimmte Anwendungen auf Hosts, um eine genaue Nachverfolgung zu gewährleisten und die Geschwindigkeit der Problemlösung zu verbessern. Dies führt zu einer effizienten Korrektur und einer besseren Ausrichtung von Warnungen an den richtigen Ressourcen.

Vorbereitungen

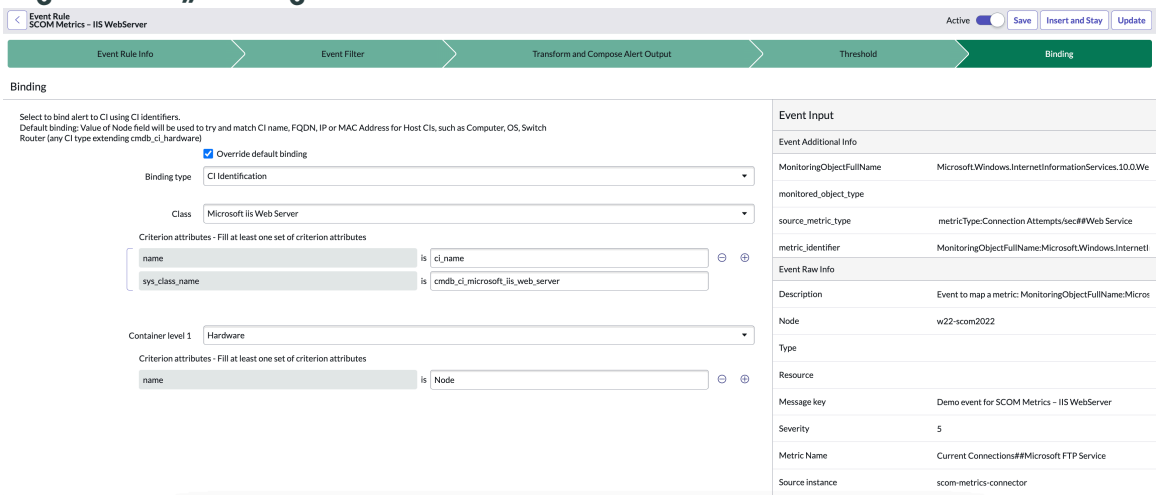
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Bevor wir das Verfahren durchlaufen, lassen Sie uns zunächst anhand eines Beispiels verstehen, wie diese Bindung funktioniert. Angenommen, eine sofort einsatzbereite Ereignisregel, SCOM Metrics – IIS Webserver, generiert eine Warnung für einen Microsoft IIS Webserver, der auf einem Host ausgeführt wird. Anstatt die Warnung nur an den Hostcomputer zu binden, soll sie der spezifischen Anwendung (IIS-Webserver) zugeordnet werden, bei der das Problem aufgetreten ist. So stellt das System eine genaue Bindung sicher.

Sagen wir in **Bindung** Registerkarte, die **Klasse** Und **Containerebene 1** Werden zusammen mit ihren jeweiligen Attributen definiert, wie in der Abbildung gezeigt.

Registerkarte „Bindung“



Das Bindungsverfahren führt die folgenden Schritte aus:

1. Identifizieren des Hosts (Containerebene 1)

   Da der Microsoft IIS-Webserver auf einem Host (in diesem Fall Hardware) ausgeführt wird, sucht das System zuerst den Host, der als definiert ist **Containerebene 1** . Das Namensfeld wird verwendet, um den Host zu identifizieren, und sein Wert wird aus dem übernommen **Knoten** Feld des Ereignisses. Mit diesem Namen durchsucht das System die CMDB, um ein übereinstimmendes Host-CI zu finden.

2. Identifizieren des Microsoft IIS-Webserver-CI auf dem Host

   Sobald der Host identifiziert wurde, sucht das System unter diesem Host nach einem Microsoft IIS-Webserver-CI mit den folgenden Attributen:

   - Name = ci_Name
   - sys_class_Name = cmdb_ci_microsoft_iis_Web_Server

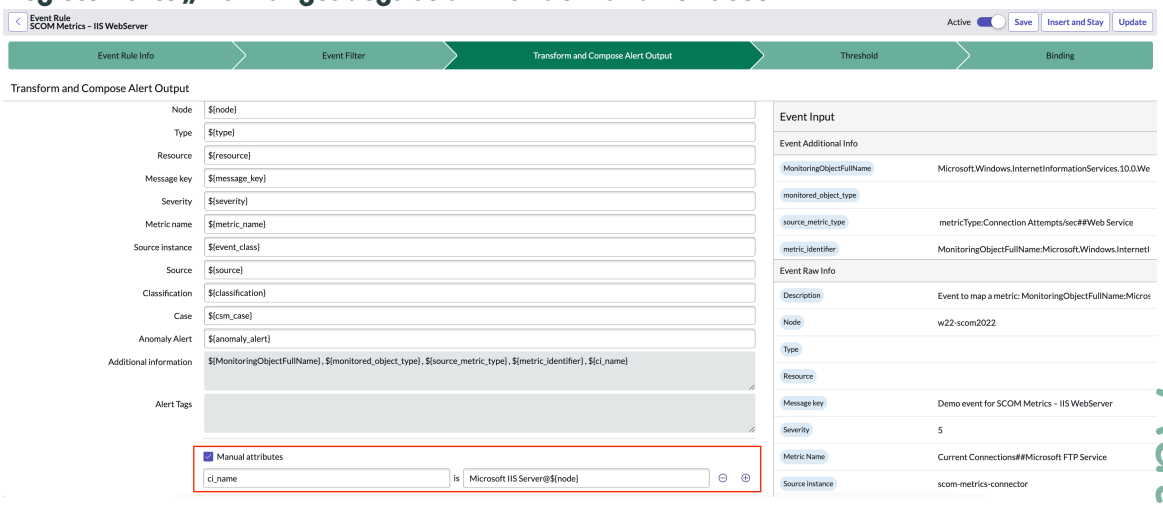
   Hier wird ci_Name aus dem in definierten Schlüssel-Wert-Paar abgeleitet **Warnungsausgabe umwandeln und verfassen** Registerkarte der Ereignisregel. Nehmen Sie dies in an **Warnungsausgabe umwandeln und verfassen** Registerkarte der Ereignisregel, der **Manuelle Attribute** Das Kontrollkästchen ist aktiviert, und das folgende Schlüssel-Wert-Paar wurde bereits hinzugefügt:

   - **Feldname** : `ci_Name`
   - **Feldwert** : `Microsoft IIS-Server@${node}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies stellt sicher ci_Name Wird in angezeigt **Zusätzliche Informationen** Feld der Warnung und wird beim Konfigurieren des Attributfelds der CI-Klasse verwendet.

Registerkarte „Warnungsausgabe umwandeln und verfassen“



Wenn auf dem identifizierten Host ein übereinstimmendes Microsoft IIS-Webserver-CI gefunden wird, wird die Warnung an das richtige Anwendungs-CI und nicht nur an den Host gebunden. Dies stellt eine genauere Nachverfolgung und Lösung von Incidents sicher, indem die Warnung mit dem tatsächlich betroffenen Service verknüpft wird, anstatt nur mit dem Computer, auf dem sie ausgeführt wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Wählen Sie Aus **Neu** Und füllen Sie die erforderlichen Felder der Ereignisregel aus.
3. Wählen Sie aus **Bindung** Registerkarte.
4. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.
5. In **Bindungstyp** Feld auswählen **CI-Identifizierung** .
6. In **Klasse** Feld eine CI-Klasse auswählen.
7. In **Wählen Sie einen Bezeichner aus** Feld einen Bezeichner für die Klasse auswählen.

   Ein Bezeichner für eine Klasse ist ein Satz von Regeln, mit denen das System CIs richtig erkennen und abgleichen kann. Stellen Sie sich dies wie einen Fingerabdruck für jeden CI-Typ (z. B. Server, Router oder Anwendung) vor. Der Bezeichner verwendet Schlüsselattribute wie eine Seriennummer, einen Hostnamen oder eine IP-Adresse, um sicherzustellen, dass neue Daten mit dem richtigen CI verknüpft werden, anstatt Duplikate zu erstellen. Weitere Informationen zur CI-Identifizierungsregel finden Sie unter Erstellen Sie eine CI-Identifizierungsregel .
8. In **Wert hinzufügen** Feld den genauen Wert hinzufügen oder das Quellfeld angeben, aus dem der Wert für das Feld ausgefüllt werden muss.

   Fügen Sie Felder mit dem Hinzufügen (hinzu ⊕) Und löschen (⊖) Symbole.

   Hinweis: Wenn Sie beim Ausfüllen der CI-Klassenattribute das gewünschte Attribut nicht finden, können Sie verwenden **Warnungsausgabe umwandeln und verfassen** Registerkarte der Ereignisregel, um das erforderliche Schlüssel-Wert-Paar hinzuzufügen. Weitere Informationen finden Sie unter Event-Regel konfigurieren, um den Warnungsinhalt anzupassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Transformation und Zusammensetzung der Ereignisregel ist nützlich, wenn relevante Informationen in einem anderen Feld vorhanden sind, aber extrahiert oder neu zugewiesen werden müssen, um eine ordnungsgemäße Warnungsverarbeitung zu gewährleisten. Dies ist besonders wichtig, wenn das erforderliche Attribut nicht direkt verfügbar ist und manuell definiert werden muss.

Nehmen Sie beispielsweise an **Zusätzliche Informationen** Das Feld einer Warnung enthält den Warnungsnamen unter **Knoten** Feld. Für eine korrekte Verarbeitung muss dieser Wert jedoch unter angezeigt werden **Name** Stattdessen Feld. Da das Ereignis kein Namensattribut enthält, können wir eines manuell mit erstellen **Warnungsausgabe umwandeln und verfassen** Registerkarte in der Ereignisregel. So geht's:

a. Wählen Sie aus **Warnungsausgabe umwandeln und verfassen** Registerkarte.

b. Wählen Sie aus **Manuelle Attribute** Kontrollkästchen.

c. Fügen Sie das folgende Schlüssel-Wert-Paar hinzu:

- **Feld** : Name
- **Feldwert** : Knoten

Diese Konfiguration stellt sicher, dass das System extrahiert **Knoten** Wert eingeben und dem Namensfeld zuordnen, sodass es für die CI-Bindung und Warnungskorrelation verfügbar ist.

9. In *`Container level 1`*Bereich, geben Sie den Host an.

10. In **Wählen Sie einen Bezeichner aus** Feld einen Bezeichner für den Container auswählen.

11. In **Wert hinzufügen** Feld den genauen Wert oder das Feld hinzufügen, das die Quelle für ist **Wählen Sie einen Bezeichner aus** Feld des Containers.

Fügen Sie Felder mit dem Hinzufügen (hinzu ⊕) Und löschen (⊖) Symbole.

12. Wählen Sie **Speichern**.

Beispiel: Binden von Warnungen an nicht-Host-CIs

Binden Sie Warnungen mithilfe von Ereignisregeln und Ereignisfeldzuordnungen an einen Anwendungsservice (ein nicht-Host-CI). Dieses Beispiel zeigt, wie dies durch Nutzung der IP-Adresse erreicht werden kann, die dem Service zugeordnet ist.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

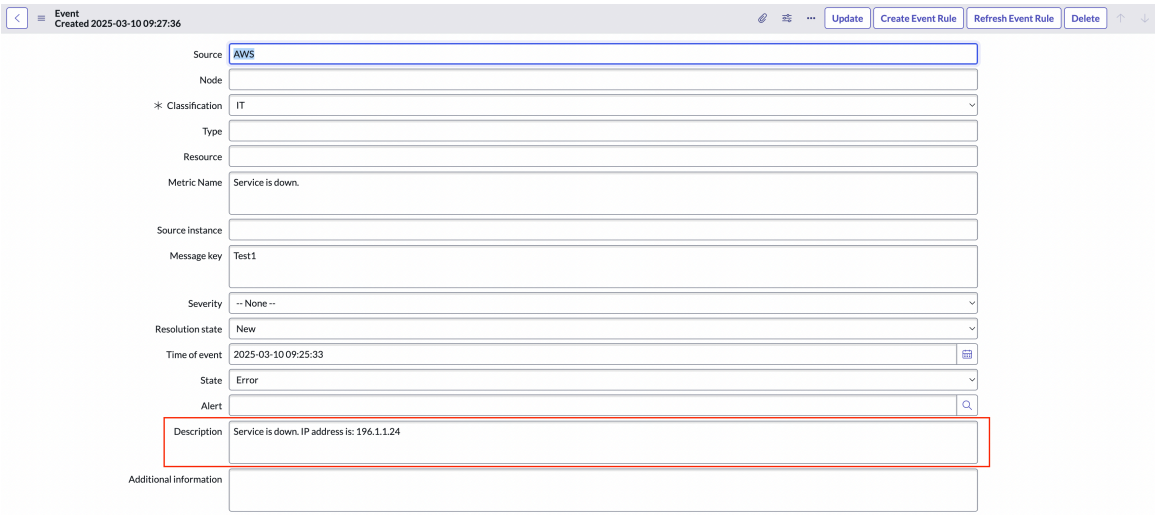
Wenn ein Ereignis generiert wird, enthält es möglicherweise nicht immer den genauen Namen des betroffenen Anwendungsservice. Stattdessen können Details wie eine IP-Adresse bereitgestellt werden. Angenommen, Anwendungsservices werden in diesem Beispiel durch IP-Adressen identifiziert. Da das Ziel darin besteht, die Warnung an einen Anwendungsservice zu binden, müssen Sie bestimmen, welcher Servicename der angegebenen IP-Adresse entspricht.

Führen Sie die folgenden Schritte aus, um dies zu erreichen:

1. Stimmen Sie mit dem richtigen Anwendungsservice überein: Überschreiben Sie die Standardbindung, und wählen Sie aus **Bindungstyp** Als **CI-Feldübereinstimmung** . Der Bindungsprozess muss die Warnung einem Anwendungsservice zuordnen, nicht einem Host. Legen Sie in der Ereignisregel fest **CI-Typ** Bis **Anwendungsservice** Damit das System in der Tabelle „Anwendungsservice“ (cmdb_ci_Service_Auto) nach dem Service sucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Extrahieren Sie die IP-Adresse aus der Ereignisbeschreibung: Das Ereignis enthält möglicherweise eine Nachricht wie Service ist ausgefallen. IP-Adresse ist: 196.1.1.24 . Sie müssen die IP-Adresse zur weiteren Verarbeitung aus dieser Beschreibung extrahieren.

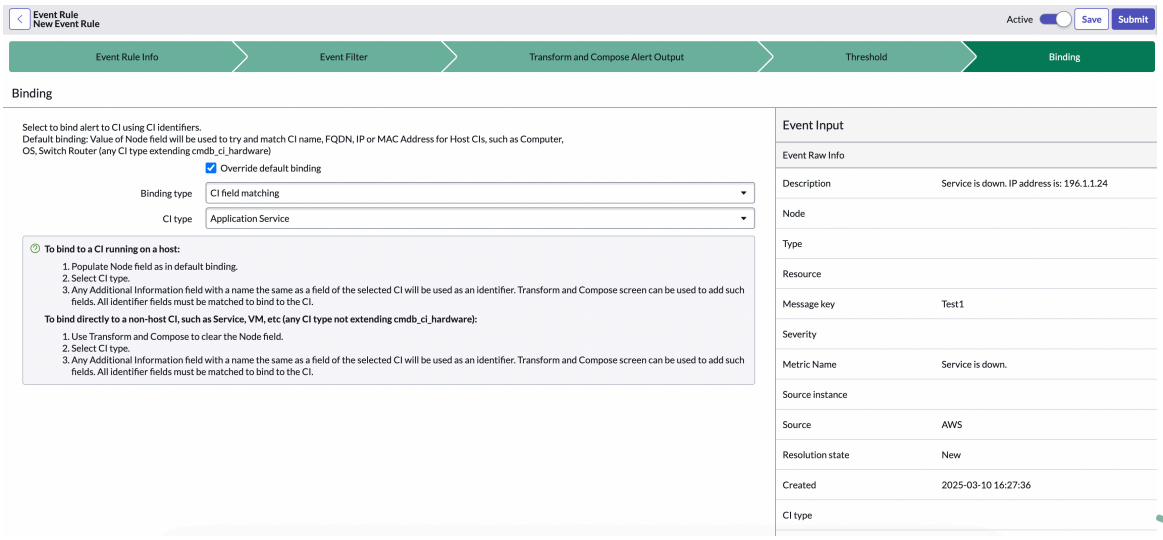


3. Übersetzen Sie die IP-Adresse mithilfe von Ereignisfeldzuordnung in einen Servicenamen: Verwenden Sie die Ereignisfeldzuordnung, um die extrahierte IP-Adresse in der CMDB zu suchen und den zugehörigen Anwendungsservice zu finden. Sobald ein übereinstimmender Service gefunden wurde, wird sein Name in gespeichert **Name** Feld des Ereignisses.
4. Binden Sie die Warnung an den richtigen Anwendungsservice: Wenn der Servicename identifiziert wird, wird das CI der Warnung mit diesem Service ausgefüllt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
2. Öffnen Sie das spezifische Ereignis, für das Sie eine Ereignisregel erstellen möchten.
3. Wählen Sie Aus **Erstellen Sie Eine Ereignisregel** .
   Die neue Ereignisregelseite wird geöffnet. Einige Felder in der Ereignisregel werden basierend auf den Ereignisdatensatzdaten ausgefüllt, z. B. dem Quellfeldwert.
4. In **Ereignisregelinformationen** Registerkarte im **Name** Feld eingeben `Anwendungsservice-Bindung` .
5. Wählen Sie aus **Bindung** Registerkarte.
   Auf dieser Registerkarte wählen Sie den CI-Typ als Service (nicht-Host) anstelle eines Hosts aus, da das Ziel darin besteht, Warnungen an einen Anwendungsservice und nicht an einen physischen oder virtuellen Computer zu binden.
6. Führen Sie die nachfolgenden Schritte durch:
   a. Wählen Sie aus **Standardbindung überschreiben** Kontrollkästchen.
   b. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.
   c. Von **CI-Typ** Liste, wählen Sie aus **Anwendungsservice** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



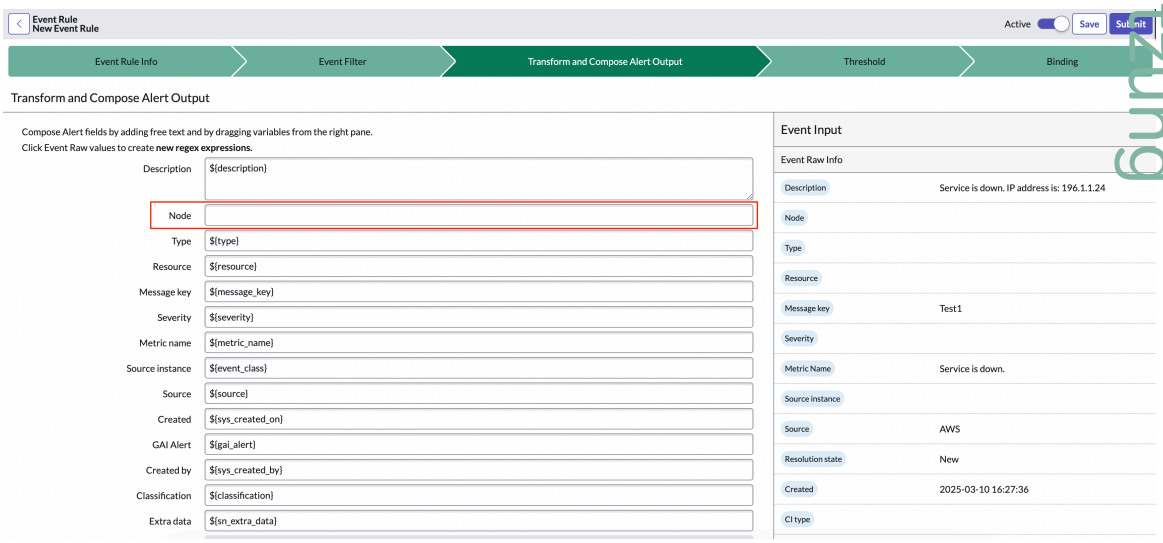
7. Wählen Sie aus **Warnungsausgabe umwandeln und verfassen** Registerkarte.

Auf dieser Registerkarte extrahieren Sie die IP-Adresse des Anwendungsservice in ein manuell erstelltes Feld. Durch das Extrahieren der IP kann das System den entsprechenden Service in der Tabelle „Anwendungsservice“ (cmdb_ci_Service_Auto) suchen. Ohne Extraktion der IP kann das System nicht bestimmen, zu welchem Anwendungsservice das Ereignis gehört, was das korrekte Binden der Warnung erschwert.

8. Führen Sie die nachfolgenden Schritte durch:

a. Löschen Sie **Knoten** Feld.

Wenn ein Ereignis verarbeitet wird, enthält es häufig mehrere Informationsfelder. Die **Knoten** Das Feld enthält normalerweise den Host- oder Gerätenamen. Da das Ziel jedoch darin besteht, die Warnung an einen Anwendungsservice anstatt an einen Host zu binden, wird gelöscht **Knoten** Das Feld stellt sicher, dass sich das System darauf konzentriert, den richtigen Service zu identifizieren, anstatt die Warnung versehentlich einem Host-CI zuzuordnen.



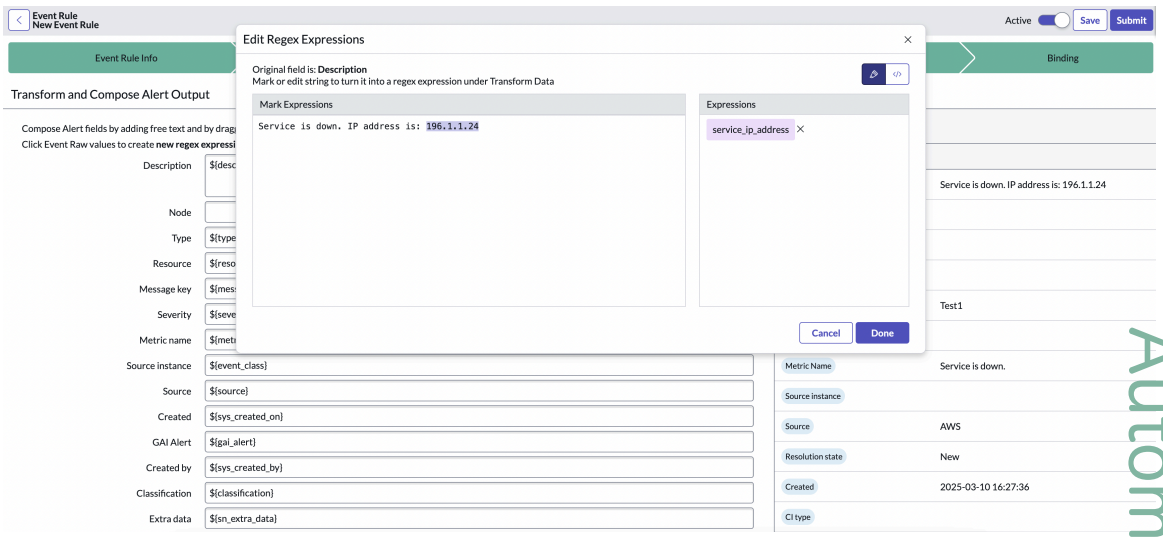
b. Unter **Ereigniseingabe** > **Rohinformationen zum Ereignis**, Wählen Sie aus **Beschreibung** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fenster „reguläre Ausdrücke bearbeiten“ wird geöffnet.

c. Wählen Sie im Abschnitt Ausdrücke markieren die IP-Adresse aus, geben Sie manuell einen Feldnamen (z. B. Service_ip_address) ein, und drücken Sie die Eingabetaste, um ihn zu speichern.



d. Wählen Sie **Fertig**.

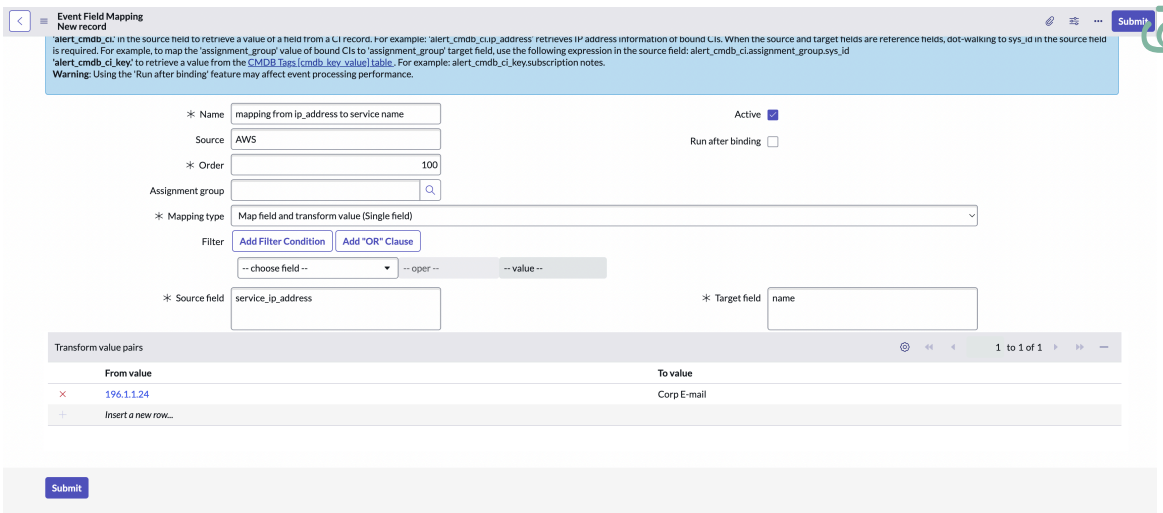
Die IP-Adresse wird in neu erstellte extrahiert **Service_ip_address** Feld, das dem hinzugefügt wird **Zusätzliche Informationen** Feld der Warnung. Dadurch kann er später verwendet werden, um den entsprechenden Anwendungsservice zu identifizieren.

9. Wählen Sie Aus **Übermitteln** In der Ereignisregel, um Ihre Änderungen zu speichern.

10. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisfeldzuordnung**an. Konfigurieren Sie in Ereignisfeldzuordnung die extrahierte IP-Adresse so, dass sie dem entsprechenden Servicenamen zugeordnet wird. Das Ereignis stellt nur eine IP-Adresse bereit, Warnungen müssen jedoch einem Servicenamen (nicht nur einer IP) zugeordnet werden. Das System muss diese IP dem entsprechenden Anwendungsservice zuordnen, damit Teams den betroffenen Service leicht identifizieren können.

11. Wählen Sie **Neu**.
Das Fenster „Ereignisfeldzuordnung“ wird geöffnet.

12. Führen Sie Folgendes aus:



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

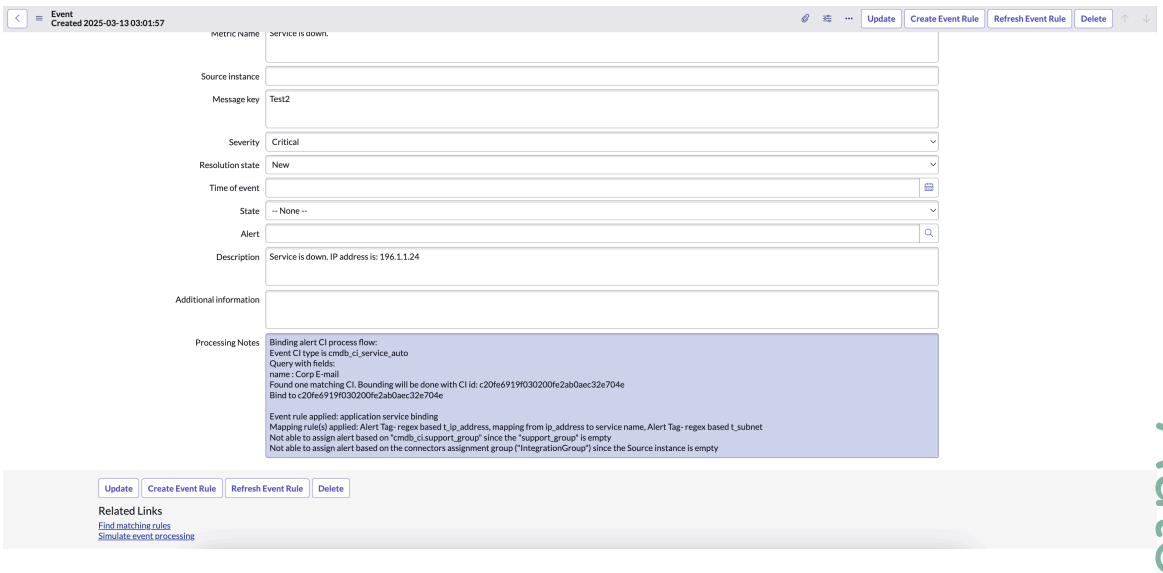
Feld	Aktion
Name	Geben Sie den Namen der Zuordnung ein. Beispiel: Zuordnung von ip_address zu Servicename.
Quelle	Geben Sie Ein `AWS` . **Hinweis:** Die Quelle ist mit der im Ereignisdatensatz identisch.
Zuordnungstyp	Wählen Sie Aus **Feld zuordnen und Wert umwandeln (einzelnes Feld)**
Quellenfeld	Geben Sie Ein `Service_ip_address` .
Zielfeld	Geben Sie Ein `Name` . Der Zielfeldwert ist der Spaltenname in der Tabelle „Anwendungsservice“ (cmdb_ci_Service_Auto), in der der Quellfeldwert durchsucht wird.
Wertepaare transformieren	
Ab Wert	196.1.1.24
Bis Wert	Unternehmens-E-Mail

13. Wählen Sie **Absenden**.

Das System extrahiert die IP-Adresse des Service aus dem Ereignis und speichert sie im **Service_ip_address** Feld. Da die Tabelle „Anwendungsservice“ (cmdb_ci_Service_Auto) keine Spalte für die Suche nach IP-Adresse enthält, wird die Funktion „Wertepaare umwandeln“ verwendet, um die IP-Adresse einem Namen zuzuordnen – in diesem Fall Corp E-Mail und und speichert sie im **Name** Feld in **Zusätzliche Informationen** Feld der Warnung. Die **Zielfeld** Gibt an, wo in der Tabelle „Anwendungsservice“ nach der Unternehmens-E-Mail gesucht werden soll. Das System sucht in nach Unternehmens-E-Mail **Name** Spalte der Anwendungsservice-Tabelle (cmdb_ci_Service_Auto). Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Übereinstimmung gefunden wird, wird die Warnung an den entsprechenden Anwendungsservice gebunden.



Beispiel: Binden Sie Warnungen mit dynamischen CI-Typen an CIs

Verwenden Sie die Ereignisfeldzuordnung, um Warnungen basierend auf Ereignisattributen dynamisch an die entsprechenden CIs zu binden, sodass keine separaten Ereignisregeln für jeden CI-Typ (auch als CI-Klasse bezeichnet) erforderlich sind. Dieser Ansatz vereinfacht die Konfiguration, verbessert die Genauigkeit und verbessert die Bindung von Warnungen zu CI.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

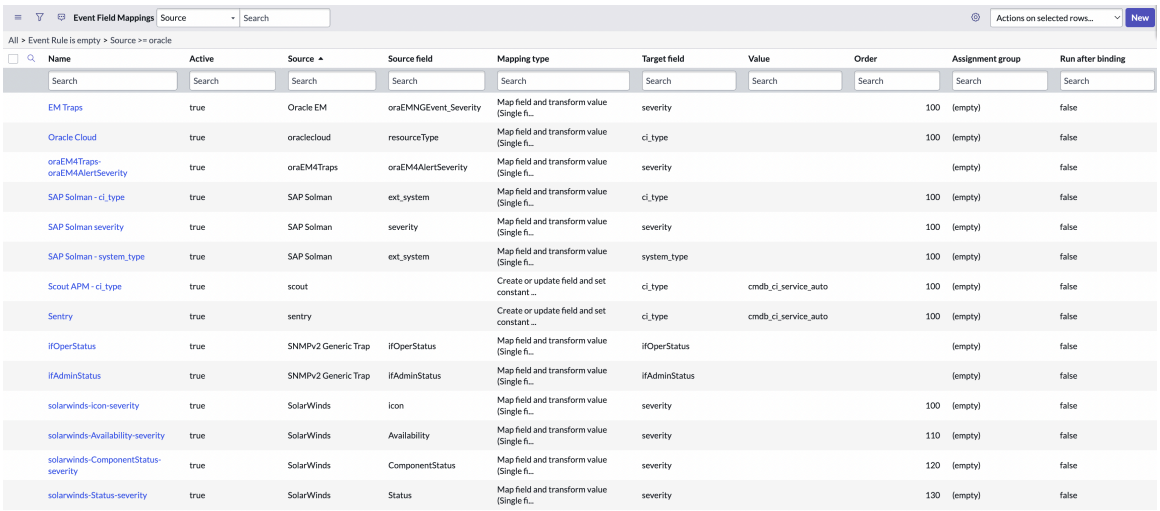
Im Allgemeinen für ein Ereignis, das aus einer bestimmten Quelle generiert wurde, die in erwähnt wird **Quelle** Feld wendet das System die entsprechende Ereignisregel an. Die Option Standardbindung überschreiben in einer Ereignisregel gibt eine bestimmte CI-Klasse für die Bindung an. In einem dynamischeren Anwendungsfall ist die CI-Klasse jedoch nicht vordefiniert und kann sich basierend auf Ereignisattributen ändern. Angenommen, ein Kunde hat mehrere CIs mit demselben Namen, aber jedes CI gehört zu einer anderen CI-Klasse. Bei der traditionellen Ereignisregelmethode ist die Zuordnung falsch, da die CI-Klasse (oder die CMDB-Tabelle) für ein CI definiert ist, da das System in derselben CI-Klasse nach allen CIs mit demselben Namen und denselben Attributen sucht, anstatt in der spezifischen CMDB-Tabelle zu suchen, die für jede CI-Klasse definiert ist.

Um dies zu beheben, also die richtige CI-Klasse für die Suche zu bestimmen, verwendet das System **CI-Typ** Feld aus dem Ereignis zur Identifizierung der CI-Klasse. Durch die Verwendung einer Ereignisfeldzuordnung, die Ereignisattribute dem CI-Typ zuordnet, kann ermittelt werden, welche CMDB-Tabelle gesucht werden soll, um sicherzustellen, dass das CI dem Ereignis korrekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

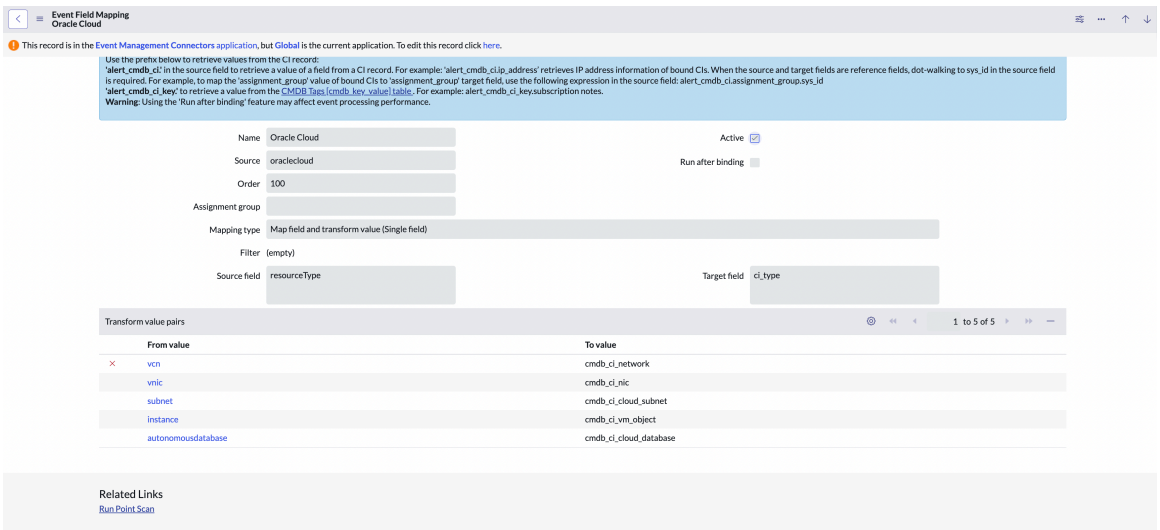
1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisfeldzuordnung**an.



Name	Active	Source	Source field	Mapping type	Target field	Value	Order	Assignment group	Run after binding
EM Traps	true	Oracle EM	oraEMNGEvent_Severity	Map field and transform value (Single fi...	severity		100	(empty)	false
Oracle Cloud	true	oraclecloud	resourceType	Map field and transform value (Single fi...	ci_type		100	(empty)	false
oraEM4Traps-oraEM4AlertSeverity	true	oraEM4Traps	oraEM4AlertSeverity	Map field and transform value (Single fi...	severity			(empty)	false
SAP Solman - ci_type	true	SAP Solman	ext_system	Map field and transform value (Single fi...	ci_type		100	(empty)	false
SAP Solman severity	true	SAP Solman	severity	Map field and transform value (Single fi...	severity		100	(empty)	false
SAP Solman - system_type	true	SAP Solman	ext_system	Map field and transform value (Single fi...	system_type		100	(empty)	false
Scout APM - ci_type	true	scout		Create or update field and set constant ...	ci_type	cmdb_ci_service_auto	100	(empty)	false
Sentry	true	sentry		Create or update field and set constant ...	ci_type	cmdb_ci_service_auto	100	(empty)	false
ifOperStatus	true	SNMPv2 Generic Trap	ifOperStatus	Map field and transform value (Single fi...	ifOperStatus			(empty)	false
ifAdminStatus	true	SNMPv2 Generic Trap	ifAdminStatus	Map field and transform value (Single fi...	ifAdminStatus			(empty)	false
solarwinds-icon-severity	true	SolarWinds	icon	Map field and transform value (Single fi...	severity		100	(empty)	false
solarwinds-Availability-severity	true	SolarWinds	Availability	Map field and transform value (Single fi...	severity		110	(empty)	false
solarwinds-ComponentStatus-severity	true	SolarWinds	ComponentStatus	Map field and transform value (Single fi...	severity		120	(empty)	false
solarwinds-Status-severity	true	SolarWinds	Status	Map field and transform value (Single fi...	severity		130	(empty)	false

2. Wählen Sie Aus **Oracle Cloud** .

   Dies ist eine vorhandene Ereignisfeldzuordnung, die als Beispiel verwendet wird. Die Detailseite der Ereignisfeldzuordnung wird geöffnet.



3. Überprüfen Sie die Detailseite der Ereignisfeldzuordnung, und verstehen Sie die relevanten Felder und die entsprechenden Werte.

Ereignisfeldzuordnungsfelder

Feld	Beschreibung
Name	Name der Ereignisfeldzuordnung.
Quelle	Ereignisüberwachungssoftware, die das Ereignis generiert hat. In diesem Fall oraclecloud.
Reihenfolge	Zahl zur Festlegung der Reihenfolge, in der diese Aktion verarbeitet werden soll. Aktionen mit niedrigeren Nummern werden zuerst verarbeitet.
Zuordnungstyp	Wählen Sie Aus **Feld zuordnen und Wert umwandeln (einzelnes Feld)** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quellenfeld	**ResourceType** Ist ein Feld, das in definiert ist **Zusätzliche Informationen** Feld des vom Oracle Cloud-System definierten Ereignisses. Die möglichen Werte von **ResourceType** Sind in aufgeführt **Von-Wert** Spalte, während die entsprechenden CMDB-Tabellen für diese Werte in angegeben sind **Bis Wert** Spalte im Abschnitt „Wertepaare transformieren“. Wenn **ResourceType** Ist **Instanz** , Sucht das System in der Tabelle [cmdb_ci_vm_object] nach CI-Bindung.
Zielfeld	Die **CI-Typ** Feld (**ci_type**) In einem Ereignis ist ein spezielles Feld, das den CI-Klassennamen bereitstellt, der angibt, welche CMDB-Tabelle gesucht werden soll. Die **CI-Typ** Feldwerte werden in aufgeführt **Bis Wert** Spalte im Abschnitt „Wertepaare transformieren“.
Wertepaare transformieren	
Ab Wert	Listet die möglichen Werte des Ereignisfelds auf (z. B. `ResourceType`), die aus den Ereignisdaten abgeleitet sind.
Bis Wert	Gibt die entsprechende CMDB-Tabelle an, die jedem in aufgeführten Wert zugeordnet ist **Von-Wert** Spalte. Gibt den CI-Typ an, an den die Warnung gebunden werden soll.

Muster für die Event-Gruppenerstellung anzeigen

Event-Gruppen sind Event-Sätze, die keine übereinstimmende Event-Regel haben. Sie können die Muster in einer Gruppe von Events anzeigen, um die Auswirkungen der Erstellung einer Regel basierend auf der Event-Quelle und den Beschreibungsmustern zu erfahren.

Vorbereitungen

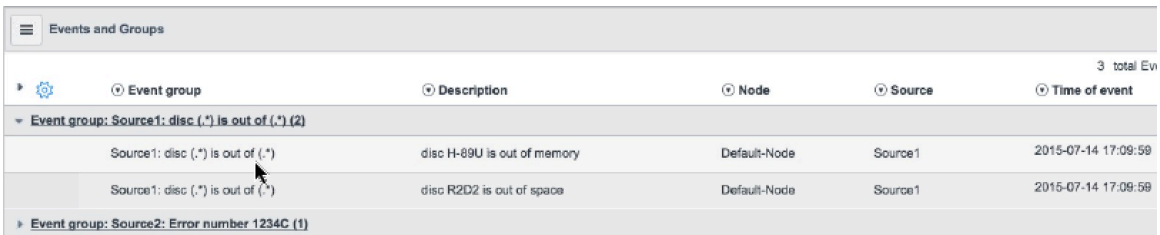
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Events werden entsprechend ihrer Quelle und Beschreibung gruppiert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln**an.
2. Warten Sie, bis die Gruppenberechnung abgeschlossen ist, und klicken Sie dann auf den erstellten Link. Wenn nicht genügend Ereignisse vorhanden sind, werden bei der Berechnung keine Gruppen erstellt.
3. Wählen Sie in der Liste der Ereignisse ein Ereignis aus.
4. Um das Muster eines Events zu ändern, doppelklicken Sie auf das Muster, nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Aktualisieren**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisieren Sie Ereignisregeln

Aktualisieren Sie Ereignisregeln manuell, um die aktuellen Ereignisinformationen widerzuspiegeln, da nach der Erstellung einer Ereignisregel die verwendet wird **Zusätzliche Ereignisinformationen** Und **Ereignis-Rohinformationen** Felder werden nicht automatisch aktualisiert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
2. Wählen Sie das Ereignis aus.
3. Wählen Sie Aus **Aktualisieren Sie Die Ereignisregel** .
4. Wählen Sie die zu aktualisierenden Ereignisregeln aus.
5. Wählen Sie Aus **Ausgewählte Aktualisieren** .

Wenn Sie mehrere Ereignisregeln ausgewählt haben, wird das zuletzt ausgewählte Element in der Liste im Ereignisregel-Designer geöffnet.

Hinweis: Wenn die Ausdrücke des regulären Ausdrucks der aktuellen Ereignisregel nach der Aktualisierung nicht mit dem ausgewählten Ereignis übereinstimmen, schlägt das Update fehl, und eine Fehlermeldung mit den problematischen Feldern wird angezeigt. Dieser Schutz stellt sicher, dass Ihre zuvor definierten regulären Ausdrücke der Ereignisregel aufgrund der Aktualisierung nicht beschädigt werden.

Suchen Sie nach Regeln, die auf ein Ereignis angewendet werden

Zeigen Sie die Regeln an, die auf ein Ereignis angewendet werden, um zu bestimmen, wie dieses Ereignis verarbeitet wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Ereignismanagement** > **Alle Ereignisse**, Und klicken Sie dann auf eine Ereignisnummer.
2. Klicken Sie unter **Zugehörige Links** auf **Übereinstimmungsregeln finden**.
3. Überprüfen Sie die Informationen, die im blauen Feld oben auf der Seite angezeigt werden, und überprüfen Sie alle **Verarbeitungsnotizen** Um Regeln zu finden, die für ein Ereignis gelten.

Zugehörige Informationen

Events anzeigen

Ereignisverarbeitung simulieren

Sie können Ereignisverarbeitungslogik für Ereignisse simulieren und die resultierende Warnung anzeigen, um besser zu verstehen, welche Regeln für ein bestimmtes Ereignis ausgeführt werden und wie sich die Ereignisfelder nach der Ausführung der Regel ändern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
2. Öffnen Sie das Ereignis, das Sie simulieren möchten.
3. In **Zugehörige Links** Abschnitt auswählen **Simulieren Sie die Ereignisverarbeitung.**
4. Wählen Sie in der Infonachricht, die oben auf dem Bildschirm angezeigt wird, den Link zur erstellten simulierten Warnung aus.
5. **Wahlweise:** Zeigen Sie an, welche Ereignisregeln und Ereignisfeldzuordnungsregeln angewendet wurden, und wählen Sie die Ereignisfeldwerte aus **Aktivitäten** Registerkarte.

Konfiguration der Event-Feldzuordnung

Verwenden Sie Zuordnungsregeln für Event-Felder, um Werte aus bestimmten Feldern Werten in anderen Feldern zuzuordnen.

Ereignismanagement speichert Event-Feldzuordnungen in der Tabelle Event-Feldzuordnung [em_mapping_rule]. Die Zuordnungen gelten nach der Verarbeitung der Event-Regel und vor der Warnungsgenerierung. Die Zuordnungswerte aus der Tabelle Event-Zuordnungspaar [em_mapping_pair] gelten für die Warnung. Der ursprüngliche Schweregrad des Events bleibt unverändert.

Beispiel: Wenn Ereignisse mit dem Feld „ **Org_severity** „ Mit den Werten “ `Low`, `Medium`, `High`„ Und Sie möchten die Warnung **Schweregrad** Um diesen Wert beizubehalten, erstellen Sie eine Ereignisfeldzuordnungsregel, die das Feld zuordnet **Org_severity** Bis **Schweregrad** , Mit diesen Werten:

Beispiel für org_severity, das dem Schweregrad zugeordnet ist

Ursprünglicher Wert für org_severity	Wird dem Warnungs-Schweregradwert zugeordnet
Niedrig	Warnung
Mittel	Schwerwiegend
Hoch	Kritisch

Standardmäßige Event-Feldzuordnungen

Ereignismanagement bietet Standard-Event-Feldzuordnungen für häufig verwendete Systemüberwachungstools. Die Feldzuordnungen „Wertepaare aus Ereignis umwandeln“ formatieren die eingehenden Ereignisdaten für Ereignismanagement.

Sie können die standardmäßigen Ereignisfeldzuordnungen und Zuordnungspaare anzeigen, indem Sie zu navigieren **Ereignismanagement** > **Bedingungen** > **Ereignisfeldzuordnungen** Und Doppelklick **Name** .

Event-Feldzuordnungen erstellen

Verwenden Sie Ereignisfeldzuordnungen, um Werte aus bestimmten Ereignisfeldern Werten in anderen Feldern zuzuordnen, um umfassendere Informationen in einer Warnung bereitzustellen. Verwenden Sie teambasierte Integrationen in Ereignisregeln, um sicherzustellen, dass Connector-Besitz und -Ausführung globalen Regeln Vorrang geben. Teams können Konsistenz und Hierarchie beibehalten und gleichzeitig Flexibilität und Anpassungsoptionen bieten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die Regel, um das Event anhand seiner Klasse und der ursprünglichen Werte abzugleichen. Geben Sie außerdem die neuen Werte an, um die ursprünglichen Werte im Ereignis zu ersetzen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisfeldzuordnung**an.
2. Wählen Sie Aus **Neu** Oder öffnen Sie eine vorhandene Regel, um die Felder zu bearbeiten und auszufüllen.

Formular Event-Feldzuordnung

Feld	Beschreibung
Name	Name der Event-Feldzuordnung.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Reihenfolge	Zahl zur Festlegung der Reihenfolge, in der diese Aktion verarbeitet werden soll. Aktionen mit niedrigeren Nummern werden zuerst verarbeitet.
Zuweisungsgruppe	Wählen Sie für teambasierte Integrationen eine Zuweisungsgruppe aus. Wenn in der Ereignisfeldzuordnungsregel keine Zuweisungsgruppe definiert ist, wird diese Regel als global betrachtet. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln und dann die Regeln ausgeführt, die zur Zuweisungsgruppe gehören, zu der die Quellinstanz des Ereignisses gehört.
Zuordnungstyp	Zuordnungsmechanismus, der zum Ändern eines Event-Feldwerts verwendet wird. ○ **Feld zuordnen und Wert umwandeln (einzelnes Feld)** : Ordnet zu **Quellfeld** Wert zum übereinstimmenden Wert in Transformieren Sie Wertpaare [Em_Mapping_pair] Tabelle und Ausfüllen S Die **Zielfeld** . Quell- und Zielfelder können Ereignisfelder, Felder mit zusätzlichen Informationen oder Warnungs-Tags sein. ○ **Feld erstellen oder aktualisieren und konstanten Wert festlegen (Konstante)** : Legt einen konstanten Wert auf ein fest **Zielfeld** . Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein. ○ **Feld zuordnen (Feld kopieren)** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Kopiert den genauen Wert von Quellfeld Zum angegebenen Zielfeld. Die Felder „Quelle“ und „Ziel“ können E sein Vent-Feld, Feld mit zusätzlichen Informationen , Oder Warnungs-Tags. ○ **Feld zuordnen und Wert mithilfe des regulären Ausdrucks transformieren** : Ordnet den Wert aus dem Feld Quelle dem übereinstimmenden Wert in der Tabelle „Wertpaare transformieren“ zu, und füllen Sie aus **Zielfeld** . Quell- und Zielfelder können Ereignis-, zusätzliche Informationen- oder Warnungs-Tags-Felder sein. ○ **Feld mit regulärem Ausdruck zuordnen** : Kopiert den Wert aus einem generisch definierten **Quellfeld** Zu **Zielfeld** . Das Feld „Quelle“ muss ein Feld aus dem Feld „zusätzliche Informationen zum Ereignis“ sein. Das Zielfeld kann das Feld des Ereignisses, der zusätzlichen Informationen oder des Warnungs-Tags sein. Mit diesem Typ können Sie den Namen des Quellfelds generisch mithilfe eines regulären Ausdrucks (regulärer Ausdruck) finden. ○ **Feld zuordnen und Wert aus Gruppe des regulären Ausdrucks kopieren** : Kopiert einen Teil des Quellfeldwerts in das Feld Ziel. Quell- und Zielfelder können Ereignisfelder, Felder mit zusätzlichen Informationen oder Warnungs-Tags sein. Definieren Sie einen regulären Ausdruck, um anzugeben, welcher Teil von **Quellfeld** Muss kopiert werden. ○ **Erweiterte Zuordnung mit Skript** : Implementieren S Ihre eigene Logik für die Transformation von Ereigniswerten mithilfe eines Skripts. Wenn das Kontrollkästchen „nach Bindung ausführen“ aktiviert ist, wird die Regel nach der CI-Bindungsphase ausgeführt und verwendet das dedizierte Skript, das auch die sys_ID des CI in den Eingabeparametern enthält. **Warnung:** Komplexe Skripts können sich auf die Leistung der Ereignisverarbeitung auswirken. ○ **Feld aus Referenztabelle zuordnen** Verwenden Sie diesen Regeltyp, um einen zu extrahieren **Quellfeld** Wert aus dem ausgewählten **Referenztabelle** Durch Abgleich von **Abzugleichendes Feld** Wert für **Übereinstimmendes Warnungsfeld** Wert und dann Zuordnung von **Quellfeld** Wert für **Zielfeld** . Die **Übereinstimmendes Warnungsfeld** Und **Zielfeld** Kann Ereignisfelder, zusätzliche Informationsfelder oder Warnungs-Tags sein.
Filter	Eine Bedingung für die Ereignisfeldzuordnung. Wählen Sie **Filterbedingung hinzufügen** oder **„ODER“-Klausel hinzufügen** aus, um mehrere Bedingungen zu konfigurieren. **Hinweis:** Beim Filter wird zwischen Groß- und Kleinschreibung unterschieden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktiviert oder deaktiviert die Ereignisfeldzuordnung. Wenn möglich, suchen Sie nach einer anderen Event-Feldzuordnungsregel, und wenden Sie diese an.
Nach Bindung ausführen	○ Wenn diese Option ausgewählt ist, wird die Regel nach der CI-Bindungsphase ausgeführt. ○ Verwenden Sie das entsprechende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** Dient zum Abrufen eines Felds aus dem CI-Datensatz. Beispiel: Verwenden Sie „Alert_cmdb_ci.assignment_Group“, um ein Warnungsfeld „assignment_Group“ mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Dot-Walk zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise Alert_cmdb_ci.Asset.model ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken. **Hinweis:** Dieses Kontrollkästchen wird nur für die folgenden Zuordnungstypen angezeigt: **Feld zuordnen und Wert umwandeln (einzelnes Feld)** , **Feld zuordnen (Feld kopieren)** , **Feld zuordnen und Wert mithilfe des regulären Ausdrucks transformieren** , **Feld zuordnen und Wert aus Gruppe des regulären Ausdrucks kopieren** , Und **Feld aus Referenztabelle zuordnen** .

○ Wenn Sie ausgewählt haben **Feld zuordnen und Wert umwandeln (einzelnes Feld)** Füllen Sie die Felder entsprechend aus.

Feld zuordnen und Wertfelder umwandeln (einzelnes Feld)

Feld	Beschreibung
Quellenfeld	Zuzuordnendes Ereignisfeld: Enthält alle Ereignisfelder und Felder mit zusätzlichen Informationen. Hinweis: Verwenden Sie für Felder mit zusätzlichen Informationen: „Additional_info.<field name>“. Wenn das Kontrollkästchen „nach Bindung ausführen“ aktiviert ist, können Sie verwenden **Alert_cmdb_ci** Und **Alert_cmdb_ci_key** Präfixe zum Empfangen von CI-bezogenen Daten.
Zielfeld	Event-Feld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Wenn dieses Feld mit identisch ist **Quellfeld** , Die Zuordnungsregel aktualisiert den Wert im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Arbeitsspeicher des Ereignisfelds. Warnungs-Tags können auch mit definiert werden <t_>Präfix.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das folgende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** Dient zum Abrufen eines Felds aus dem CI-Datensatz. Verwenden Sie beispielsweise „Alert_cmdb_ci.assignment_Group“, um ein Warnungsfeld „Assignation_Group“ mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Dot-Walk zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise Alert_cmdb_ci.Asset.model ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken.

Schlüsselfelder (Abschnitt „Wertpaare umwandeln“)

Feld	Beschreibung
Schlüssel	Wert, nach dem von der Zuordnungsregel gesucht wird. Immer wenn das Ereignisfeld diesen Wert hat, fügt die Zuordnungsregel den in aufgeführten Wert hinzu **Quellfeld** Feld zu dem Feld, das in aufgeführt ist **Zielfeld** . Dieses Feld wird angezeigt, wenn **Zuordnungstyp** Ist **Feld zuordnen und Wert umwandeln (einzelnes Feld)** . Wählen Sie Aus **+** Um weitere hinzuzufügen **Schlüssel** Felder, nach Bedarf.

Typischer Anwendungsfall: Um das Feld „event_severity“ im Feld „zusätzliche Informationen“ mit möglichen Werten [z. B. „WARNUNG“, „GERING“, „KRITISCH“, „LÖSCHEN“, „SCHWERWIEGEND“] dem Feld „Schweregrad“ zuzuordnen, konfigurieren Sie Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Quellfeld: „Event_severity“
- Zielfeld: „Schweregrad“
- Wertpaare transformieren:
  - Von-Wert: „WARNUNG“, bis-Wert: „4“
  - Von-Wert: „GERINGFÜGIG“, bis-Wert: „3“
  - Und so weiter...

○ Wenn Sie ausgewählt haben **Feld erstellen oder aktualisieren und konstanten Wert festlegen (Konstante)** Füllen Sie die Felder entsprechend aus.

Erstellen oder aktualisieren Sie ein Feld, und legen Sie Felder für konstanten Wert (Konstante) fest

Feld	Beschreibung
Zielfeld	Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein. Typischer Anwendungsfall: Legen Sie den Warnungsschweregrad für alle Ereignisse, die dem Filter entsprechen, auf 1 fest.
Wert	Wert zur Verwendung für das **An-Feld**. Dieses Feld wird angezeigt, wenn **Zuordnungstyp** Ist **Konstant** .

Typischer Anwendungsfall: Legen Sie den Warnungsschweregrad für alle Ereignisse, die dem Filter entsprechen, auf 1 fest.

○ Wenn Sie ausgewählt haben **Feld zuordnen (Feld kopieren)** Füllen Sie die Felder entsprechend aus.

Felder für Kartenfeld (Feld kopieren)

Feld	Beschreibung
Quellenfeld	**Quellfeld** Wert, der in kopiert werden soll **Zielfeld** Feld. Die **Quellfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das entsprechende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** Dient zum Abrufen eines Felds aus dem CI-Datensatz. Verwenden Sie beispielsweise „Alert_cmdb_ci.assignment_Group“, um ein Warnungsfeld „Assignation_Group“ mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Dot-Walk zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise Alert_cmdb_ci.Asset.model ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken.

Typischer Anwendungsfall: Dient zum Kopieren des IP-Felds aus dem Feld „zusätzliche Ereignisinformationen“ in den Warnungsfeldknoten , Verwenden Sie Folgendes:

- „Quellfeld“: ip
- „Zielfeld“: Knoten

○ Wenn Sie ausgewählt haben **Feld zuordnen und Wert mithilfe des regulären Ausdrucks transformieren** Füllen Sie die Felder entsprechend aus.

Feld zuordnen und Wert mit regulärem Ausdruck transformieren

Feld	Beschreibung
Quellenfeld	Quellfeldwert, der in kopiert werden soll **Zielfeld** Feld. Die **Quellfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das entsprechende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** Dient zum Abrufen eines Felds aus dem CI-Datensatz. Verwenden Sie beispielsweise „Alert_cmdb_ci.assignment_Group“, um ein Warnungsfeld „Assignation_Group“ mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Dot-Walk zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise Alert_cmdb_ci.Asset.model ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken.

Typischer Anwendungsfall: Um den Schweregrad aus der Feldfarbe im Feld „zusätzliche Informationen“ dem Feld „Schweregrad“ zuzuordnen, verwenden Sie:

- Quellfeld: „Farbe“
- Zielfeld: „Schweregrad“
- Wertpaare transformieren:
  - Von-Wert: „.*red“, bis-Wert: „1“. Dies deckt sowohl „dunkelrot“ als auch „hellrot“ und andere Werte mit „rot“ ab und ordnet sie alle „1“ zu.
  - Und so weiter...

Schlüsselfelder (Abschnitt „Wertpaare umwandeln“)

Feld	Beschreibung
Schlüssel	Wert, nach dem von der Zuordnungsregel gesucht wird. Immer wenn das Ereignisfeld diesen Wert hat, fügt die Zuordnungsregel den in aufgeführten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wert hinzu **Quellfeld** Feld zu dem Feld, das in aufgeführt ist **Zielfeld** . Dieses Feld wird angezeigt, wenn **Zuordnungstyp** Ist **Feld zuordnen und Wert umwandeln (einzelnes Feld)** . Wählen Sie Aus **+** Um weitere hinzuzufügen **Schlüssel** Felder, nach Bedarf.

- Wenn Sie ausgewählt haben **Feld mit regulärem Ausdruck zuordnen** Füllen Sie die Felder entsprechend aus.

Feld mithilfe von Feldern des regulären Ausdrucks zuordnen

Feld	Beschreibung
Quellenfeld	Generisch definierter Quellfeldwert, der in kopiert werden soll **Zielfeld** Feld. Die **Quellfeld** Muss ein Feld aus dem Feld „zusätzliche Informationen zum Ereignis“ sein. Mit diesem Typ können Sie den Namen des Quellfelds generisch mithilfe eines regulären Ausdrucks (regulärer Ausdruck) finden.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.

Typischer Anwendungsfall: Um das Feld „Region“ aus dem Feld „additional_info“, das als „Tags.Region“ oder „Tags|Region“ oder „Cloud.Region“ angezeigt wird, einem Warnungs-Tag zuzuordnen `t_region`, Verwenden:

- „Quellfeld“: *Region
- „Zielfeld“: t_Region

- Wenn Sie ausgewählt haben **Feld zuordnen und Wert aus Gruppe des regulären Ausdrucks kopieren** Füllen Sie die Felder entsprechend aus.

Feld zuordnen und Wert aus Gruppenfeldern des regulären Ausdrucks kopieren

Feld	Beschreibung
Quellenfeld	Generisch definierter Quellfeldwert, der in kopiert werden soll **Zielfeld** Feld. Das Feld „Quelle“ muss ein Feld aus dem Feld „zusätzliche Informationen zum Ereignis“ sein. Mit diesem Typ können Sie den Namen des Quellfelds generisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	mithilfe eines regulären Ausdrucks (regulärer Ausdruck) finden.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das entsprechende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** Dient zum Abrufen eines Felds aus dem CI-Datensatz. Verwenden Sie beispielsweise „Alert_cmdb_ci.assignment_Group“, um ein Warnungsfeld „Assignation_Group“ mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Dot-Walk zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise Alert_cmdb_ci.Asset.model ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken.
Gruppenausdruck des regulären Ausdrucks	.*_.*_(.*)_.*

Typischer Anwendungsfall: Um das dritte Oktet aus der IP zu extrahieren und in den zusätzlichen Informationen zu speichern *`third_octet`*Feld , Verwenden:

- „Quellfeld“: ip
- „Zielfeld“: Third_octet
- „Regulärer Ausdruck der Gruppe“: .*_.*_(.*)_.*.*

○ Wenn Sie ausgewählt haben **Erweiterte Zuordnung mit Skript** Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Zuordnung mithilfe von Skriptfeldern

Feld	Beschreibung
Skript	Der Code-Editor bietet Texteditor-Unterstützung für Inline-Skripts. Der Code-Editor verfügt über diese Funktionen für die unterstützten Sprachservices und Inline-Skripts: Syntaxfärbung, Einrückung, Zeilennummern und automatische Erstellung von schließenden Klammern und Anführungszeichen, automatische Vorschläge und automatische Vervollständigungen. Tipps zum Bearbeiten : ▪ Um einen festen Platz an einer beliebigen Stelle in Ihrem Code einzufügen, drücken Sie die Registerkarte Schlüssel. ▪ Um eine einzelne Codezeile einzurücken, wählen Sie im führenden Leerzeichen der Zeile aus, und drücken Sie dann die Tabulatortaste. ▪ Um eine oder mehrere Codezeilen einzuziehen, markieren Sie den Code, und drücken Sie die Tabulatortaste. ▪ Um den Einzug zu verringern, drücken Sie Umschalt+Tab. ▪ Um eine Registerkarte vom Anfang einer Codezeile zu entfernen, wählen Sie in der Zeile aus, und drücken Sie Umschalt+Tab. ▪ Um Variablen zu deklarieren, verwenden Sie das Stichwort var, damit sie innerhalb des richtigen JavaScript-Bereichs bleiben.
Nach Bindung ausführen	Wenn das Kontrollkästchen „nach Bindung ausführen“ aktiviert ist, wird die Regel nach der CI-Bindungsphase ausgeführt und verwendet das dedizierte Skript, das auch die sys_ID des CI in den Eingabeparametern enthält. **Warnung:** Komplexe Skripts können sich auf die Leistung der Ereignisverarbeitung auswirken.

- Wenn Sie ausgewählt haben **Feld aus Referenztabelle zuordnen** Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld aus Referenztabellenfeldern zuordnen

Feld	Beschreibung
Referenztabelle	Die Referenztabelle. Wählen Sie die Tabelle aus, aus der das Feld dem Zielfeld im Ereignis zugeordnet werden soll.
Abzugleichendes Feld	Das Feld aus der Referenztabelle, das mit dem übereinstimmenden Warnungsfeld aus dem Ereignis abgeglichen werden soll. Wird verwendet, um die Referenztabellendatensätze herauszufiltern.
Quellenfeld	**Quellfeld** Wert, der in kopiert werden soll **Zielfeld** Feld. Die **Quellfeld** Ist das Feld der Tabelle, die als Referenztabelle ausgewählt wurde.
Übereinstimmendes Warnungsfeld	Ereignisfeld, um übereinstimmende Referenztabellendatensätze zu finden. Die **Übereinstimmendes Warnungsfeld** Ist mit abgeglichen **Abzugleichendes Feld** Feld. Das übereinstimmende Warnungsfeld kann das Ereignisfeld, das Feld „zusätzliche Informationen“ oder das Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Die **Zielfeld** Kann ein Ereignisfeld, ein Feld mit zusätzlichen Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das entsprechende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **Alert_cmdb_ci.** In **Übereinstimmendes Warnungsfeld** , Um einen Wert eines Felds aus einem CI-Datensatz abzurufen. Beispiel: „Alert_cmdb_ci.ip_address“ ruft IP-Adressinformationen von gebundenen CIs ab. Wenn **Übereinstimmendes Warnungsfeld** Und **Abzugleichendes Feld** Felder sind Referenzfelder, DOT-Walking zur sys_ID im **Übereinstimmendes Warnungsfeld** Ist erforderlich. Beispiel: Um den Wert „assignment_Group“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	von gebundenen CIs für den Abgleich mit zu verwenden **Abzugleichendes Feld** Feld verwenden Sie den folgenden Ausdruck in **Übereinstimmendes Warnungsfeld** : Alert_cmdb_ci.assignment_Group.sys_ID ▪ **Alert_cmdb_ci_key.** Dient zum Abrufen eines Werts aus der Tabelle „CMDB-Tags“. Beispiel: Alert_cmdb_ci_key.Subscription Notes. **Warnung** : Die Verwendung der Funktion „nach Bindung ausführen“ kann sich auf die Leistung der Ereignisverarbeitung auswirken.

Typischer Anwendungsfall: Extrahieren Sie „short_description“ aus den Datensätzen „pc_Vendor_Cat_item“, die dem Feld „Name“ mit dem Feld „Cat_item_Name“ im Feld „zusätzliche Informationen“ des Ereignisses übereinstimmen, und ordnen Sie es dem Feld „description“ des Ereignisses in den folgenden Feldern zu:

- „Referenztabelle“: pc_Vendor_Cat_item
- „Abzugleichendes Feld“: Name
- „Quellfeld“: Short_description
- „Übereinstimmendes Warnungsfeld“: Cat_item_Name
- „Zielfeld“: Beschreibung

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
4. Wählen Sie **Absenden**.

Example:
Die folgenden Werte enthalten eine vordefinierte Regel, die auf Ereignisse in angewendet wird `Trap Von Enterprise 9` Klasse. Wenn die Ereignisse enthalten SnmpTrapOID Element mit einem Wert von iso.org.dod.internet.private.enterprises.cisco.0.0 , Die Zuordnungsregel ändert den Wert in Neu laden In den Warnungen. Wenn die Ereignisse enthalten SnmpTrapOID Element, ein Wert von iso.org.dod.internet.private.enterprises.cisco.0.1 , Die Zuordnungsregel ändert den Wert in TcpConnectionSchließen In den Warnungen.

Feld	Werte
Name	cisco.snmpTrapOID
Quelle	Trap From Enterprise 9
Zuordnungstyp	Feld zuordnen und Wert umwandeln (einzelnes Feld).
Quellenfeld	snmpTrapOID
Zielfeld	snmpTrapOID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Werte
Wertpaare Transformieren	• Paar 1 ○ **Schlüssel**: iso.org.dod.internet.private.enterprises.cisc ○ **Wert**: reload • Paar 2 ○ **Schlüssel**: iso.org.dod.internet.private.enterprises.cisc ○ **Wert**: tcpConnectionClose

Nächste Maßnahme

Testen Sie eine Ereignisfeldzuordnung, indem Sie ein Ereignis senden, das ein Feld enthält, das in der Ereignisfeldzuordnung vorhanden ist.

Event-Bezeichner

Event-Felder identifizieren jedes Event eindeutig. Ereignismanagement verwendet diese Informationen, um zu bestimmen, ob eine neue Warnung erstellt oder eine vorhandene aktualisiert werden soll.

- Standardmäßig wird jedes Event durch den **Nachrichtenschlüssel**eindeutig identifiziert.
- Wenn der **Nachrichtenschlüssel** nicht eingetragen ist, werden die Felder **Quelle**, **Typ**, **Knoten**, **Ressource** und **Metrikname** verkettet, um das Feld **Nachrichtenschlüssel** zu füllen.
- Wenn im Event keine Bezeichner angegeben werden, können Sie sie mit Event-Regeln hinzufügen.

Warnungstags

Warnungs-Tags ermöglichen die Konsolidierung aller normalisierten Felder und verbessern die Administrator-Experience, um Warnungsfelder (Schlüssel/Wert) umzuwandeln und zu normalisieren, wodurch normalisierte Felder in verschiedenen Quellen wiederverwendet werden können. Dies verbessert die Warnungsqualität für die Korrelation und bietet mehr sofort einsatzbereite TBAC-Definitionen (Tag Based Automatic Correlation).

Beispiel: Feldnormalisierung in Warnungsmanagement

In einigen Fällen können dieselben Informationen unter verschiedenen Feldnamen in Datenquellen vorhanden sein. Beispielsweise wird bei einem eingehenden Ereignis aus einer Quelle der Standort unter dem Feld gespeichert **Region** , Aber in einer anderen Quelle werden dieselben Informationen unter erfasst **Impact_Region** . Um Verwirrung zu vermeiden und eine konsistente Gruppierung, Filterung oder Automatisierung zu ermöglichen, normalisieren wir diese Felder, indem wir ein einheitliches Feld erstellen, z. B. **t_Region** . Dieses Feld ruft den Wert aus ab **Region** Oder von **Impact_Region** Abhängig davon, welches Feld im Ereignis vorhanden ist. Auf diese Weise das normalisierte Feld **t_Region** Enthält den Standortwert immer konsistent, unabhängig vom ursprünglichen Quellfeld.

Das Feld Warnungs-Tags wird im Formular Warnungen angezeigt. Diese Tags werden von Ereignisregeln und in der Ereigniszuordnung erstellt und in der Tabelle der Warnungs-Tags gespeichert [Em_Alert_Tags] . Die Namenskonvention zum Erstellen von Schlüssel-Wert-Paaren ist t_<tag name>. Dies ermöglicht die Wiederverwendung von Tags in den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisregeln, indem Anwender Tags auswählen können, die zuvor definiert wurden. Wenn neue Warnungs-Tags definiert werden, werden automatisch TBAC-Tags (Tag-basiertes Warnungs-Clustering) erstellt. Mit diesen TBAC-Tags können Sie neue TBAC-Warnungs-Clustering-Definitionen aus der neuen Quelle von Tags erstellen☒

Event-Feldformat für die Event-Erfassung

Ereignismanagement erfordert, dass alle Events ein Standardformular verwenden, unabhängig davon, wie sie bei der Instanz ankommen.

Geben Sie im Anwendungsnavigationsfilter `em_event.list` ein.

Event-Formular

Name	Beschreibung
em_event.source [Quelle]	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
em_event.node [Knoten]	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
em_event_type [Typ]	Optional. Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen
em_event.resource [Ressource]	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen
metric_name [Metrikname]	Der Name der Metrik, die gemessen wurde, wie `Freier Speicher DB-Festplatte (MB)`, `Festplatten-Schreibvorgänge/s` oder `Geschriebene Bytes auf Festplatte/s`.
em_event.event_class [Quellinstanz]	Wenn das Feld em_event.node nicht angegeben ist, müssen Warnungen automatisch erstellt werden. Werte für das Feld „em_event.event_class“ stammen entweder von der Quelle, die die Events generiert, oder von der Event-Regel. Name des Computers oder der Software, von dem/der das Event generiert wurde. Beispiel: SolarWinds auf 10.22.33.44. Der entsprechende Feldanzeigename ist **Quellinstanz**.
em_event.message_key [Nachrichtenschlüssel]	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
em_event.ci_type [CI-Typ]	Zeichenfolge mit Informationen zum CI-Typ. Maximale Länge: 100 Zeichen
em_event.severity [Schweregrad]	Optionen für den Event-Schweregrad sind: • **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. • **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Formular (Fortsetzung)

Name	Beschreibung
	• **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. • **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. • **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. • **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
em_event.resolution_state [Auflösungsstatus]	Optional. Wenn das Feld leer ist, steht die Auflösung der entsprechenden Warnungen noch aus. Der Event-Status aus der Event-Quelle ist entweder **Neu** oder **Wird geschlossen**. • **Neu** , Die Lösung für entsprechende Warnungen ist offen. • **Wird Geschlossen** Der Ereignisstatus schließt entsprechende Warnungen.
em_event.time_of_event [Zeit des Events]	Uhrzeit, zu der das Event im Quellsystem aufgetreten ist. Dieses Feld ist ein GlideDateTime-Feld im Format „UTC“ oder „GMT“. Maximale Länge: 40 Zeichen
em_event.state [Status]	Aktueller Verarbeitungsstatus des Events: • **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. • **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. • **Ignoriert** : Dieser Wert wird nicht verwendet. • **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer.
em_event.alert [Warnung]	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
em_event.description [Beschreibung]	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen
em_event.additional_info [Zusätzliche Informationen]	Optional. Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed. Error 0x80070490"}. Diese Informationen können für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Formular (Fortsetzung)

Name	Beschreibung
	Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-Format, das die Daten enthält: {“additional_content”: “Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).
processing_notes [Verarbeitungshinweise]	Anzeige des Event-Verarbeitungsprotokolls.

Benutzerdefinierte Warnungsfelder

Sie können benutzerdefinierte Warnungsfelder mit Daten aus dem Feld **Zusätzliche Informationen** des Events befüllen.

Wertvolle Daten, die in den Feldern für **Zusätzliche Informationen** von Events enthalten sind, können beispielsweise für Berichte nützlich sein. Warnungsfelder werden automatisch aus Feldern befüllt, die im Event denselben Namen haben. Dieses Verhalten gilt für die Event-Felder **Zusätzliche Informationen** und für die Felder **Zusätzliche Informationen**, die von der Event-Regel hinzugefügt werden. Verwenden Sie daher den benutzerdefinierten Feldnamen im Feld **Zusätzliche Informationen**, um ein benutzerdefiniertes Warnungsfeld mit dem Wert in den Feldern für **Zusätzliche Informationen** auszufüllen. Sie können zu diesem Zweck auch Event-Regeln verwenden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Format normalisiert, wenn das Event verarbeitet wird. Weitere Informationen finden Sie unter Event-Regel konfigurieren, um den Warnungsinhalt anzupassen.

Das Feld „Kurzbeschreibung“ einer Warnung wird automatisch anhand des Typs, Knotens und der Beschreibung der Warnung geschrieben. Um zu verhindern, dass das Feld „Kurzbeschreibung“ überschrieben wird, öffnen Sie die Tabelle *sys_properties*, suchen die Eigenschaft *evt_mgmt.override_alert_short_description*, ändern den Wert in false und klicken dann auf **Aktualisieren**.

Abhängig von den Berechtigungen können Sie möglicherweise nur Felder mit dem Präfix **user_** erstellen. Wenn dies der Fall ist, erstellen Sie mithilfe der Event-Regeln ein Feld mit **Zusätzlichen Informationen** mit demselben Namen. Um zu verhindern, dass einige Felder in das Warnungsfeld kopiert werden, verwenden Sie die Eigenschaft *evt_mgmt.alert_black_list_fields* und fügen die Feldnamen hinzu, die ausgeschlossen werden müssen. Standardmäßig werden die folgenden Felder nicht kopiert:

- message_key
- category
- additional_info
- sys_updated_on

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sys_updated_by
- sys_created_by
- sys_created_on
- sys_mod_count
- sys_id

Ereignisse werden getestet und gesendet

Sie können Ereignisse manuell testen und senden, um dies zu bestätigen Ereignismanagement Verwaltet Ereignisse ordnungsgemäß und generiert Warnungen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Beispielsweise können Sie Events manuell senden, um:

- zu bestätigen, dass der MID Server eine Event-Connector-Definition und Instanz zum Senden von Events verwendet.
- zu bestätigen, dass Event-Regeln, Event-Feldzuordnungen und andere Konfigurationen Warnungen generieren.
- einen Vorgang oder eine Aktion, der/die kein Event generiert hat, zu verfolgen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**an.
2. Klicken Sie auf **Neu**, und füllen Sie anschließend die Felder aus.

Event-Formular

Name	Beschreibung
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen
Ressource	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
Metrikname	Der Name der Metrik, die gemessen wurde, wie `Freier Speicher DB-Festplatte (MB)`, `Festplatten-Schreibvorgänge/s` oder `Geschriebene Bytes auf Festplatte/s`.
Quellinstanz	Name des Computers oder der Software, von dem/der das Event generiert wurde. Beispiel: SolarWinds auf 10.22.33.44. Der entsprechende Feldanzeigename ist **Quellinstanz**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
Schweregrad	Der Schweregrad des Events. Die Optionen werden normalerweise wie folgt interpretiert: ○ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ○ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ○ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen. ○ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.
Auflösungsstatus	Optional. Wenn das Feld leer ist, steht die Auflösung der entsprechenden Warnungen noch aus. Der Event-Status aus der Event-Quelle ist entweder **Neu** oder **Wird geschlossen**. ○ **Neu** , Die Lösung für entsprechende Warnungen ist offen. ○ **Wird Geschlossen** Der Ereignisstatus schließt entsprechende Warnungen.
Zeit des Events	Uhrzeit, zu der das Event im Quellsystem aufgetreten ist. Dieses Feld ist ein GlideDateTime-Feld im Format „UTC“ oder „GMT“. Maximale Länge: 40 Zeichen
Status	Der aktuelle Verarbeitungsstatus des Events: ○ **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. ○ **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. ○ **Ignoriert**: Dieser Wert wird nicht verwendet. ○ **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer.
Warnung	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
Beschreibung	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen
Zusätzliche Informationen	Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Error 0x80070490"}. Diese Informationen können für die Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-Format, das die Daten enthält: {“additional_content”: “Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).

3. Klicken Sie auf **Absenden**.

Event-Verarbeitungsstatistiken anzeigen

Extrahieren Sie Statistiken aus Ihrer Instanz, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird, und extrahieren Sie Metriken im Zusammenhang mit Eventprozessen, um den Status der Eventverarbeitung zu überwachen.

Vorbereitungen

Stellen Sie sicher, dass die Aufgabe *`Event Management - Collect xmlstats`* aktiv ist. Konfigurieren Sie diese geplante Aufgabe, indem Sie zu navigieren **Systemdefinition** > **Geplante Aufgaben**an.

Sie können die Verarbeitung von Event-Statistiken mithilfe dieser Eigenschaften steuern:

- *`evt_mgmt.enable_event_processing_stats`*. Informationen zur Verwendung dieser Eigenschaft finden Sie unter Verarbeitung von Event-Verarbeitungsstatistiken aktivieren.
- *`evt_mgmt.event_processing_stats_period`*. Informationen zur Verwendung dieser Eigenschaft finden Sie unter Konfigurieren Sie den Statistikverarbeitungszeitraum.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Schlüsselmetriken der Instanz anzeigen, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird, und um den Status der Verarbeitung von Events zu überwachen. Weitere Informationen zum Anzeigen von Statistiken zur Eigensystemüberwachung finden Sie unter Statistiken der Eigensystemüberwachung für Metric Intelligence anzeigen.

Prozedur

1. Führen Sie in einem Browser, in dem die Instanz ausgeführt wird, das XML-Statistikskript aus, indem Sie den folgenden Text an die Instanz-URL anhängen: `xmlstats.do?include=XMLStatsEm`
2. Drücken Sie die **Eingabetaste**.
3. Überwachen Sie die gemeldeten Event-Verarbeitungsmetriken, um sicherzustellen, dass Events gemäß akzeptierten Benchmark-Werten verarbeitet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Example: Beispielausgabe nach dem Ausführen des XML-Statistikskripts

```
<xmlstats created="Tue Oct 23 04:01:25 PDT 2018" includes="XMLStatsEm" version="2">
<itom_event_management>
<event_processing>
<processed count="47" max_process_time="10" mean_process_time="5"
 record_time="2018-10-23 11:00:41"/>
<ready count="7" oldest_ready_event="37" record_time="2018-10-23 11:00:41"/>
<error count="5" record_time="2018-10-23 11:00:41"/>
<total_created count="5" record_time="2018-10-23 11:00:41"/>
</event_processing>
</itom_event_management>
</xmlstats>
```

Die Metriken zur Event-Verarbeitung im Bericht werden in der folgenden Tabelle beschrieben.

Hinweis: Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in letzter Minute aktualisiert wurden.

Event-Verarbeitungsstatistiken

Metrik	Beschreibung
Event-Verarbeitungsstatistiken	
verarbeitete Anzahl = n	Anzahl der von der Instanz verarbeiteten Events.
max_process_time = n	Längste Zeit, die die Instanz für die Verarbeitung eines Events benötigt.
mean_process_time = n	Durchschnittliche Zeit, die die Instanz zur Verarbeitung der Events in diesem Zyklus benötigt.
Event-fähige Statistiken	
Bereitschaftsanzahl = n	Anzahl der Events, die sich im Status „Bereit“ befinden und zur Verarbeitung verfügbar sind. Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in der letzten Minute aktualisiert wurden.
oldest_ready_event=n	Die längste Zeit, die ein Event benötigt, um im Status „Bereit“ zu bleiben. Wenn diese Metrik einen Wert aufweist, der größer ist als Ihre Benchmarkzahl, untersuchen Sie das Event weiter, um festzustellen, was die Verarbeitung behindert. Der Standardverarbeitungszyklus: Events, die in der letzten Stunde erstellt wurden.
Sonstige Verarbeitungsstatistiken	
Fehleranzahl = n	Anzahl der Events, für die Fehler gemeldet wurden. Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in der letzten Minute aktualisiert wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Verarbeitungsstatistiken (Fortsetzung)

Metrik	Beschreibung
total_created Anzahl = n	Gesamtanzahl der Events, die während dieses Event-Verarbeitungszyklus verarbeitet wurden. Der Standardverarbeitungszyklus: Events, die in der letzten Stunde erstellt wurden.

Verarbeitung von Event-Verarbeitungsstatistiken aktivieren

Aktivieren Sie die Verarbeitung von Event-Verarbeitungsstatistiken.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Eigenschaft `evt_mgmt.enable_event_processing_stats`, um das XMLStatsEm-Skript zum Ausführen und Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren. Sie können die Ausführung des XMLStatsEm-Skripts deaktivieren, um z. B. ein Leistungsproblem zu beheben.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach der Eigenschaft `evt_mgmt.enable_event_processing_stats`.
3. Konfigurieren Sie entweder den Wert einer vorhandenen `evt_mgmt.enable_event_processing_stats`-Eigenschaft, damit das XMLStatsEm-Skript ausgeführt werden kann, oder erstellen Sie eine neue Eigenschaft, wenn sie noch nicht vorhanden ist.
   - Wenn die Eigenschaft vorhanden ist, setzen Sie die Eigenschaft auf **Aktivieren**, um das XMLStatsEm-Skript zum Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren, und klicken Sie auf **Aktualisieren**.
   - Wenn die Eigenschaft nicht vorhanden ist, klicken Sie auf **Neu**, füllen Sie das Formular aus, und klicken Sie auf **Aktualisieren**.

Feld „Systemeigenschaft“

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen.
Beschreibung	Text, der die Eigenschaft und ihre Funktion beschreibt.
Auswahlmöglichkeiten	Durch Kommas getrennte Werte für eine Auswahlliste. Wenn Sie eine andere Auswahllistenbezeichnung und einen anderen Wert benötigen, verwenden Sie ein Gleichheitszeichen (=), um die Bezeichnung vom Wert zu trennen. Beispiel: Blau = 0000FF, Rot = FF0000, Grün = 00FF00 zeigt Blau, Rot und Grün in der Liste an und speichert den entsprechenden Hex-Wert im Eigenschaftswertfeld.
Typ	Datentyp, der aus einer Liste ausgewählt wird (z. B. Ganzzahl, Zeichenfolge oder true | false).
Wert	Gewünschter Wert für die Eigenschaft. Wenn Sie Eigenschaften mit der Methode `gs.getProperty()` abrufen, behandeln Sie die Ergebnisse als Zeichenfolgen. Beispielsweise gibt eine Wahr|Falsch-Eigenschaft „true“ oder „false“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Leserollen	Rollen, die über Lesezugriff auf diese Eigenschaft verfügen.
Schreibrollen	Rollen, die über Schreibzugriff auf diese Eigenschaft verfügen.

Zugehörige Informationen

Systemeigenschaft hinzufügen

Konfigurieren Sie den Statistikverarbeitungszeitraum

Legen Sie den Zeitraum (in Sekunden) für die Erfassung von Statistiken zur Event-Verarbeitung fest. Beispielsweise können Sie einen Zeitraum festlegen, der doppelt so lang ist wie der Standardwert von 60 Sekunden, um weitere Statistiken zu erfassen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Eigenschaft *`evt_mgmt.event_processing_stats_period`*, um die XMLStatsEm-Skriptzeit zum Sammeln von Statistiken zur Event-Verarbeitung zu konfigurieren. Der Standardwert dieser Eigenschaft ist 60, und die Einheit ist Sekunde. Legen Sie die Eigenschaftswerte fest, um das Skript über einen längeren oder kürzeren Zeitraum auszuführen. Legen Sie beispielsweise einen kürzeren Zeitraum für die Statistikerfassung fest, damit weniger CPU-Ressourcen verwendet werden.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach der Eigenschaft *`evt_mgmt.event_processing_stats_period`*.
   Konfigurieren Sie entweder den Wert einer vorhandenen *`evt_mgmt.event_processing_stats_period`* Eigenschaft, um das XMLStatsEm-Skript über einen kürzeren oder längeren Zeitraum auszuführen, oder erstellen Sie eine neue Eigenschaft, wenn sie noch nicht vorhanden ist.
   - Wenn die Eigenschaft vorhanden ist, setzen Sie die Eigenschaft auf den erforderlichen Zeitraum fest, um das XMLStatsEm-Skript zum Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren, und klicken Sie auf **Aktualisieren**.
   - Wenn die Eigenschaft nicht vorhanden ist, klicken Sie auf **Neu** , Füllen Sie das Formular aus, und klicken Sie auf **Übermitteln** .

Zugehörige Informationen

Systemeigenschaft hinzufügen

Warnungen verwalten und überwachen

Eine Warnung ist eine Benachrichtigung für ausgewählte Events, die als wichtig eingestuft werden und die der Aufmerksamkeit bedürfen. Ereignismanagement generiert Warnungen basierend auf Event-Regeln.

Die Art und Weise, wie Sie Warnungen überwachen und lösen können, basiert auf den Berechnungen der Warnungsauswirkungen sowie den Konfigurations- und Eigenschafteneinstellungen der Warnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsverwaltungsregeln zum Auflösen von Warnungen

Sie können konfigurieren Ereignismanagement Um automatisch auf Warnungen zu reagieren. Eine Warnungsverwaltungsregel bestimmt die erforderliche Warnungsantwort, z. B. zum Öffnen eines Incident, eines Knowledge Base-artikels, zum Öffnen einer Aufgabe oder zum Starten einer Korrekturaktion.

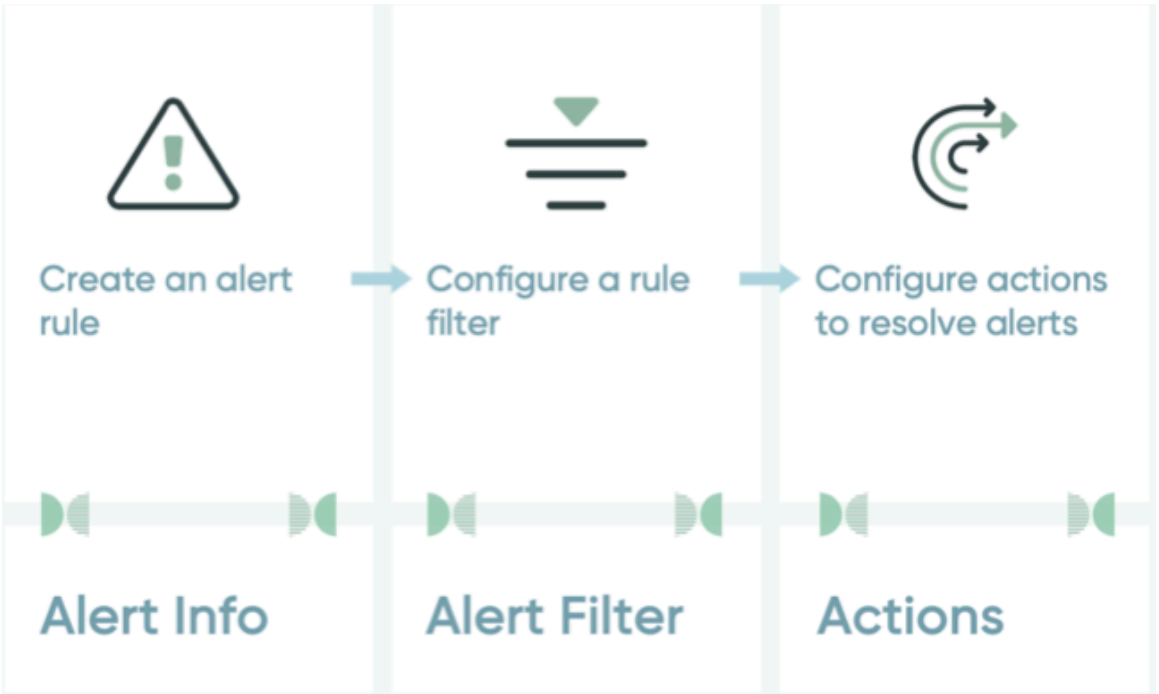
Warnungsverwaltungsregeln, die mit bereitgestellt werden Basissystem Als Store-Anwendung (Warnungsregelverwaltung [sn_em_Arm]), um Sie bei der Reaktion auf Warnungen zu unterstützen. Sie können Filter erstellen, um Bedingungen für die Regel anzugeben, sodass die in der Regel angegebene Nachbesserungsaktion nur wirksam wird, wenn die Bedingungen erfüllt sind. Beispiele sind Starten des erforderlichen Subflow oder Öffnen eines Incident auf Grundlage einer Warnung. Der Ausführungsverlauf der Warnung wird automatisch aktualisiert und gibt die aufgerufenen Aktionen an.

Benutzer mit der Rolle „evt_mgmt_admin“ können den Warnungsverwaltungsregel-Designer verwenden, um Warnungsverwaltungsregeln für spezifische Warnungen zu erstellen und anzupassen. Definieren Sie Regeln mit Filtern, um zu bestimmen, für welche Warnungen die Regel gilt. Sie können Regeln erstellen, um Anwendungen, URLs, Subflows, Nachbesserungsaktionen oder andere Aktionen auszuführen, z. B. um einen Incident zu öffnen. Weitere Informationen finden Sie unter Warnungsverwaltungsregel erstellen.

Benutzer mit der Rolle „evt_mgmt_operator“ können Warnungsverwaltungsregeln manuell ausführen.

Warnungsverwaltungsregel-Flow

Der Flow zum Erstellen und Ausführen einer Warnungsverwaltungsregel lautet:



Komponenten von Warnungsverwaltungsregeln

Komponente	Beschreibung
Warnungsinformationen	Konfigurieren Sie einen Namen und allgemeine Informationen für die Regel.
Warnungsfilter	Geben Sie einen Filter an, um zu bestimmen, für welche Warnungen die Regel gilt. Sie können die zugehörigen Listenbedingungen angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten von Warnungsverwaltungsregeln (Fortsetzung)

Komponente	Beschreibung
	Hinweis: Die Felder, die für die Warnungsfilterung nicht unterstützt werden, sind: Gesamtereignisanzahl, Priorität, Prioritätsgruppe, Prioritätsaufgliederung, Tags, und betroffene Services.
Aktionen	Geben Sie die Antwort auf die Warnung an, z. B. um einen Subflow auszuführen, eine Fehlerkorrektur durchzuführen, eine Anwendung zu starten oder eine URL in einem Browser zu starten.

Wie Regeln auf aktualisierte Warnungen angewendet werden

Warnungsverwaltungsregeln werden für alle aktualisierten offenen Warnungen ausgeführt. Regeln werden für geschlossene Warnungen nicht ausgeführt, auch wenn sie aktualisiert wurden. Die Filter bestimmen, ob die Aktionen der Regel für die Warnung gelten. Beispiel: Wenn die Bedingung einer Regel angibt, dass eine E-Mail-Nachricht gesendet wird, wenn sich der Schweregrad der Warnung in „Schwerwiegend“ ändert, gilt die Regel für eine Warnung, die durch eine Änderung des Schweregrads von „Warnung“ in „Schwerwiegend“ aktualisiert wird.

Filter und andere Aktionen verwenden

Filter stellen sicher, dass die Regel nur aufgerufen wird, wenn die konfigurierte Bedingung auftritt, und nicht bei jeder Aktualisierung der Warnung. Sie können beispielsweise eine Regel so konfigurieren, dass Updates, die nicht relevant sind (z. B. **Arbeitsnotizen** Feldaktualisierung) veranlassen Sie nicht, dass die Regel ausgeführt wird. Ein weiteres Beispiel ist eine Filterbedingung, die angibt, dass die Warnungsverwaltungsregel nur ausgeführt wird, wenn der Warnungsschweregrad „Kritisch“ lautet.

Sie können die folgenden Aktionen ausführen:

- Geben Sie einen Filter an, um zu bestimmen, für welche Warnungen die Regel gilt.
- Konfigurieren Sie im Abschnitt „Zugehörige Listenbedingungen“ des Formulars zusätzliche Bedingungen, z. B. mit einer *`Alert > Parent`*-Beziehung, um nach Warnungen zu filtern, die heute empfangen wurden.
- Auf Warnungen reagieren. Erstellen Sie beispielsweise mithilfe von Subflows und Workflows Incidents für primäre Warnungen mit kritischem Schweregrad, oder öffnen Sie eine Suchmaschine in einem Browser, um nach Daten gemäß dem Beschreibungsfeld der Warnung zu suchen.
- Fehlerkorrekturmaßnahmen anwenden. Die Fehlerkorrektur basiert auf Orchestrierungs-Workflows, die zur Ausführung von Fehlerkorrekturmaßnahmen wie dem Erfassen von Systeminformationen oder dem Neustart eines Servers geskriptet werden können.

Hinweis: Für verbesserte Leistung von *`Event Management - Evaluate Scoped Alert Rules Management`*Geplante Aufgaben. Verwenden Sie Subflows anstelle von Workflows.

Geplante Aufgaben, die Warnungsverwaltungsregeln überprüfen

Warnungsverwaltungsregeln werden alle 11 Sekunden durch den standardmäßigen geplanten Auftrag *`Event Management - Evaluate Scoped Alert Rules Management0`* überprüft. Der Auftrag führt dann die erforderlichen Aktionen aus. Für große Umgebungen können Sie mehr als einen Auftrag hinzufügen. Wenden Sie sich an Kundenservice und Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Nur neue Anwender ab Vancouver erhalten zwei geplante Aufgaben: *Event Management - Evaluate Scoped Alert Rules Management0*Und *Event Management - Evaluate Scoped Alert Rules Management1*. Benutzer, die ein Upgrade von vorherigen Familien-Releases durchführen, verbleiben bei einer einzelnen geplanten Aufgabe *Event Management - Evaluate Scoped Alert Rules Management0*.

Ändern Sie nicht *sn_em_arm.alert_management.num_of_jobs*Eigenschaft.

Standardmäßig wird der Warnungsgruppierungsauftrag (**Service Analytics gruppiert Warnungen mit RCA/Warnungszusammenfassung**) Und das Warnungsmanagement (**Ereignismanagement: Management0 Für Bereichsbezogene Warnungsregeln Auswerten**) Aufträge werden unabhängig voneinander ausgeführt. Weitere Informationen zur Koordination der Warnungsantwort und der automatisierten Warnungsgruppierung finden Sie unter Warnungsantwort wird mit automatisierter Warnungsgruppierung synchronisiert.

Vorhandene Warnungsaktionsregeln migrieren

Vorhandene Warnungsaktionsregeln aus einem früheren Release können zu Warnungsverwaltungsregeln migriert werden. Sie können eine Warnungsaktionsregel nur ändern, nachdem sie zu einer Warnungsverwaltungsregel migriert wurde. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Warnungsverwaltungsregel erstellen

Erstellen Sie eine Warnungsverwaltungsregel, um Warnungen nachzuverfolgen und zu lösen, indem Sie die erforderliche Antwort bestimmen, z. B. um einen Incident zu öffnen oder eine Fehlerkorrekturmaßnahme zu starten.

Vorbereitungen

Zum Aktivieren der Fehlerkorrektur mit einem Subflow können Sie einen Subflow verwenden, der mit dem Basissystem verfügbar ist, oder Sie können Ihren eigenen Subflow erstellen. Details finden Sie unter Erstellen Sie einen anwenderdefinierten Subflow für Warnungen.

Erforderliche Rolle: evt_mgmt_admin, flow_designer

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Warnungsverwaltungsregeln zum Nachverfolgen und Beheben von Warnungen.
Während Sie im Warnungsverwaltungsregel-Designer arbeiten, können Sie in mehreren Abschnitten arbeiten, ohne Informationen in einem beliebigen Abschnitt zu verlieren.

Hinweis:

- Warnungsverwaltungsregeln, die nicht für die Ausführung einer Aktion konfiguriert sind, werden übersprungen, und die Regel wird automatisch auf inaktiv festgelegt.
- Wenn eine Warnung durch eine Benutzeraktion (z. B. eine Warnungsverwaltungsregel) an ein CI gebunden ist und sich das CI im Wartungsstatus befindet, müssen Sie das CI manuell an die Warnung binden und es mit dem Status **In Wartung** markieren.

Warnungsverwaltungsregel erstellen, die:

- Nach weiteren Warnungsverwaltungsregeln suchen, die für die ausgewählte Warnung relevant sind.
- Bestimmen, wann die Regel ausgeführt wird.

Warnungsverwaltungsregeln werden nicht unbedingt in der Reihenfolge abgeschlossen, in der sie aufgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Warnungsverwaltungsregeln so konfigurieren, dass sie:

- Automatisch Incidents, Aufgaben oder Wissensartikel generieren und mit Warnungen verknüpfen
- Automatisch Fehlerkorrektur-Workflows anwenden oder Benutzern ermöglichen, Fehlerkorrekturmaßnahmen manuell vorzunehmen
- Automatisch eine URL entsprechend dem Wert der in der Warnung angegebenen Felder generieren

Zu Ihrer Unterstützung stellt das Basissystem mehrere Warnungsverwaltungsregeln bereit. Sie können sie wie dargestellt verwenden oder als Beispiele verwenden, um benutzerdefinierte Warnungsverwaltungsregeln zu erstellen.

Mit dem Basissystem bereitgestellte Warnungsverwaltungsregeln

Regel	Beschreibung	Aktiv
Sensor-Dashboard in PRTG öffnen	Das Sensor-Dashboard in der Applikation „Paessler PRTG Network Monitor“ (PRTG) wird geöffnet.	Ja
Oracle EM Launch – Zielstatus und Events anzeigen	Starten Sie Oracle Enterprise Manager, um Folgendes anzuzeigen: • Zielstatus • Event für Warnungen von Oracle EM-Quelle	Ja
Drilldown zu OMI	Drilldown zur HP Operations Manager i (OMi)-Anwendung.	Ja
Incident für die primäre kritische Warnung erstellen	Erstellt einen Incident für primäre kritische Warnungen. Der Incident kann automatisch oder manuell erstellt werden.	Nein
Google-Suche nach „Beschreibung“.	Öffnet die Google-Suche in einem Browser, um anhand der Beschreibung, die in der Warnung angezeigt wird, nach Daten zu suchen.	Ja
Incident erstellen	Erstellt einen Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden. Die Regel wird bei selektiver Aktualisierung automatisch ausgeführt.	Nein
Incident manuell erstellen	Erstellt manuell einen Incident für Warnungen, die sich nicht im Wartungsstatus befinden.	Ja
Kandidat für schwerwiegenden Incident erstellen	Erstellt einen Kandidaten für einen schwerwiegenden Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden und keine sekundären Warnungen sind. Ein Kandidat für einen schwerwiegenden Incident kann zu einem schwerwiegenden Incident befördert werden.	Nein
Major Incident erstellen	Erstellt einen schwerwiegenden Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden und keine sekundären Warnungen sind.	Nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach einem Upgrade Ihrer Instanz von Kingston stehen Ihnen die Warnungsaktionsregeln zur Verfügung, die mit dem Kingston Basissystem bereitgestellt wurden. Wenn Sie jedoch eine der Regeln geändert haben, werden die vorgenommenen Änderungen nicht übertragen.

Warnungsverwaltungsregeln werden 5 Sekunden nach der Aktualisierung einer Warnung ausgeführt. Der Timer wird zurückgesetzt, wenn Aktualisierungen innerhalb dieses Fensters erfolgen. Diese Verzögerung stellt sicher, dass Korrekturaktionen wie die Erstellung von Incidents nur ausgelöst werden, wenn das Problem klar und stabil ist, wodurch Duplikate und unnötiges Rauschen reduziert werden. Um die standardmäßige Verzögerung von 5 Sekunden zu ändern, erstellen Sie *evt_mgmt.alert_rule_delay*Eigenschaft auf **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** Und ändern Sie den Wert. Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Prozedur

1. Navigieren zu **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln**an.
2. Klicken Sie auf **Neu**, und füllen Sie anschließend die Felder aus.

Formular Warnungsverwaltungsregel

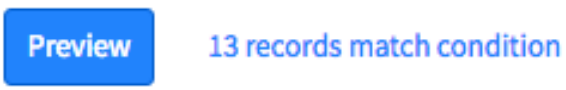
Feld	Beschreibung
Name	Eindeutiger Name für die Regel.
Aktiv	Checkbox zum Aktivieren der Regel. Wenn dieses Kontrollkästchen aktiviert ist, müssen Sie Folgendes angeben: ○ Im Abschnitt **Warnungsfilter** einen Warnungsfilter ○ im Abschnitt **Aktionen** mindestens eine dieser Aktionen: ▪ Aktiver Subflow ▪ Workflow ▪ Schnelle Antwort
Reihenfolge	Reihenfolge, in der Regeln ausgewertet werden, wenn mehrere Regeln für dieselbe Warnung definiert sind. Warnungsverwaltungsregeln werden in aufsteigender Reihenfolge ausgewertet. Der Standardwert ist 100.
Mehrere Warnungsregeln	Anweisung, ob nach zusätzlichen Regeln gesucht werden soll: ○ **Nach zusätzlichen Regeln suchen**: Führen Sie die aktuelle Regel aus, fahren Sie dann fort, und führen Sie andere übereinstimmende Regeln in der Reihenfolge der Regelpriorität aus, wobei die niedrigere Zahl die höhere Priorität hat. ○ **Suche nach zusätzlichen Regeln beenden**: Führen Sie nur die aktuelle Regel für die Warnung aus, die dem Filter entspricht. Wenn Sie diese Option auswählen, wird möglicherweise eine Regel ausgeführt, die in einer Regelhierarchie als zweite konfiguriert wird, bevor die Ergebnisse der ersten Regel wirksam werden.
Beschreibung	Beschreibender Text für die Regel
Zuweisungsgruppe	Zuweisungsgruppe, die an der Warnung arbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn in der Warnungsregel keine Zuweisungsgruppe definiert ist, wird diese Warnungsregel als globale Regel betrachtet. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln und dann die Regeln ausgeführt, die zur Zuweisungsgruppe der Warnung gehören.

3. Klicken Sie auf **Warnungsfilter** und geben Sie Bedingungen für Warnungen an, auf die diese Regel angewendet wird.

Warnungsfilterphase

Feld	Beschreibung
Regel ist aktiviert, wenn	Die Regel wird ausgeführt, wenn: ○ **Warnungsänderungen zu Filter**: Änderungen des Inhalts der Warnung bewirken, dass die Warnung dem Filter angepasst wird. Wenn der Filter bei der folgenden Aktualisierung der Warnung abgeglichen wird, wird die Regel nicht angewendet. Wenn die Warnung geschlossen wurde und dann erneut geöffnet wird, wird die Regel beim nächsten Update der Warnung angewendet, und der Filter wird abgeglichen. Danach, wenn die Warnung aktualisiert wird, wird die Regel nicht mehr angewendet. ○ **Warnung entspricht Filter**: der Inhalt der Warnung entspricht dem Filter. Folgend der Aktualisierung der Warnung und wenn der Filter abgeglichen ist, wird die Regel ausgeführt und auf die Warnung angewendet. Die Regel wird für jede übereinstimmende Aktualisierung angewendet.
Warnungsfilter	
Vorschau	Funktion zum Anzeigen einer Vorschau der Warnungen, die der angegebenen Bedingung entsprechen. Ein Hyperlink zeigt an, wie viele Warnungen dem Filter entsprechen.  Wenn Sie auf den Hyperlink klicken, öffnet der Browser eine weitere Registerkarte, die Warnungen in der Tabelle Warnungen [em_alert_list] auflistet. Die Liste zeigt, welche Warnungen der Regel entsprechen, einschließlich geschlossener Warnungen. Warnungen, die bereits von der Regel ausgeführt wurden, werden nicht markiert. Sie können auf eine Warnung klicken, um weitere Details anzuzeigen.
Bedingungen	Bedingungen, die bei Erfüllung den Filter anwenden. Weitere Informationen zu Gebäudebedingungen finden Sie unter Mit dem Bedingungsgenerator . Zum Hinzufügen einer weiteren Bedingung klicken Sie auf **Neue Kriterien**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Bedingung **Erstellt am** wird nicht aufgerufen, wenn der Job **Event Management – Warnungsverwaltungsregeln evaluieren** ausgeführt wird. Verwenden Sie stattdessen die Bedingung **Aktualisiert am**, da der Auftrag Warnungen basierend auf dem Zeitpunkt erkennt, zu dem sie aktualisiert wurden, nicht auf dem Zeitpunkt, zu dem sie erstellt wurden.
Zugehörige Listenbedingungen	Bedingungen, um eine Beziehung zu einer anderen Tabelle in den Filter aufzunehmen. **a.** Klicken Sie auf **Tabelle**, und wählen Sie die erforderliche Tabelle aus. **b.** Geben Sie die Bedingungen für diesen Filter an. Weitere Informationen zum Erstellen zugehöriger Listen finden Sie unter Fügen Sie zugehörige Listenbedingungen hinzu .

4. Klicken Sie auf **Aktionen**.
   In diesem Abschnitt können Sie die folgenden Aktionstypen als Antwort auf Warnungen oder zur Behebung von Warnungen konfigurieren:
   - Fehlerkorrektur-Subflows: Führen Sie einen mit dem Basissystem bereitgestellten Subflow aus.
   - Anwendungen starten: Öffnen Sie Anwendungen und Browser, die Sie konfigurieren.

   Hinweis: Die Option „Nachbesserungs-Subflows“ ist veraltet. Verwenden Sie den Flow Designer, um das Auslösen von Flows durch Warnungen zu ermöglichen.

5. **Wahlweise:** Befolgen Sie im Abschnitt „Nachbesserungs-Subflows“ die folgenden Anweisungen, um Subflows hinzuzufügen:

   a. Doppelklicken Sie unter **Subflow** auf die Zelle.

   b. Klicken Sie auf das Suchsymbol .
   Die Liste der mit dem Basissystem bereitgestellten Subflows wird angezeigt. Weitere Informationen finden Sie unter Ereignismanagement-Subflows im Basissystem.

   c. Wählen Sie in der Subflow-Liste einen Subflow aus.

   d. Wiederholen Sie den Vorgang, und fügen Sie so viele Subflows wie erforderlich hinzu.

   (Optional)

Remediation Subflows

	Subflow	Execution	Automatic executions limit	Active
	Create Incident	Automatic	1	true
	Close Alert	Automatic	1	true

   e. Um anzugeben, wann der Subflow ausgeführt werden muss, doppelklicken Sie unter **Ausführung** in die Zelle.

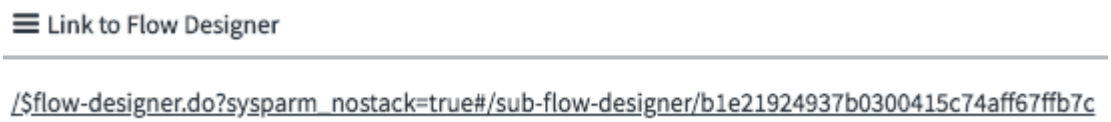
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflow-Ausführungsoptionen

Name	Beschreibung
Automatisch	Der Subflow wird automatisch ausgeführt, wenn die Regel abgeglichen wird.
Manuell	Subflow bei Bedarf ausführen, wenn die Regel abgeglichen wird.
Beides	Wenn die Regel erfüllt ist, wird der Subflow automatisch ausgeführt, und Sie können den Subflow optional erneut manuell ausführen.

f. Doppelklicken Sie in die Zelle unter **Grenzwert für automatische Ausführungen**, und geben Sie mit einer ganzen Zahl an, wie oft der Subflow ausgeführt werden soll.
Nachdem der Subflow die angegebene Anzahl von Malen ausgeführt wurde, wird er nicht mehr ausgeführt.

g. Um den auszuführenden Subflow zu aktivieren, doppelklicken Sie in die Zelle unter **Aktiv**, und wählen Sie `true` aus.
Ein Link in der Zelle unter **Link zum Flow Designer** wird erst angezeigt, nachdem ein Subflow ausgewählt und die Regel gespeichert wurde.



6. Zum Hinzufügen von Anweisungen zum Starten von Anwendungen oder zum Öffnen von Browserfenstern im Bereich „Anwendungen starten“:

a. Doppelklicken Sie unter **Anzeigenname** auf die Zelle.
Geben Sie einen Namen für den Link an.

b. Erstellen Sie im **URL**-Feld die URL anhand der Daten der Warnung im folgenden Format:`http://${source}.com:${port}/${cmdb_ci.name}`
Das Feld **Aktiv** wird automatisch aktualisiert.

Jede URL-basierte Aktion kann die Warnungsparameter verwenden, und die URLs können auf Wikis, Messaging-Services, REST APIs usw. verweisen.

7. Klicken Sie auf **Absenden**.

Ergebnis

Die Warnungsverwaltungsregel wird der Liste der verfügbaren Regeln hinzugefügt, die zum Lösen von Warnungen verwendet werden können.

Zugehörige Informationen

Schnelle Antworten in einer Warnung anwenden

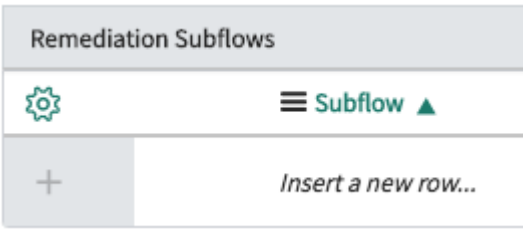
Ereignismanagement-Subflows im Basissystem

Die mit dem Basissystem bereitgestellten Subflows werden im Bereich „Nachbesserungs-Subflows“ der Warnungsverwaltungsregeln angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf Subflows zugreifen

Navigieren zu **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln** Und klicken Sie auf **Neu** . Klicken Sie auf die Registerkarte **Aktionen**. Doppelklicken Sie im Bereich „Nachbesserungs-Subflows“ auf das Feld **Neue Zeile einfügen**.



Klicken Sie auf das Suchsymbol , um Subflows hinzuzufügen. Die Liste der mit dem Basissystem bereitgestellten Subflows wird angezeigt.

Subflows im Basissystem

Name	Beschreibung
Warnung bestätigen	Subflow, um die Warnung als bestätigt zu markieren. Bestätigen Sie eine Warnung, um anzuzeigen, dass weitere Aufmerksamkeit erforderlich ist.
Wissensartikel anhängen (veraltet)	Subflow zum Anhängen eines Wissensartikels an die Warnung. Dieser Subflow wird für Instanzen bereitgestellt, die aus veralteten Releases (vor dem London-Release) migriert werden. **Hinweis:** Fügen Sie die **Wissensartikelspalte** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_rule] hinzu und wählen Sie einen Artikel aus, der bei Ausführung der Regel an eine Warnung angehängt werden soll.
Warnung in den Wartungsmodus setzen	Subflow, um den Alarm als in Wartung befindlich zu markieren.
Warnung schließen	Subflow, um die Warnung als geschlossen zu markieren.
Incident erstellen	Subflow zum Erstellen eines Incidents. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem (Fortsetzung)

Name	Beschreibung
	Hinweis: • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Nachdem ein bestimmter Zeitrahmen verstrichen ist, wird der Warnungsverwaltungsauftrag auch dann ausgeführt, wenn der Auftrag zur Warnungsgruppierung nicht abgeschlossen ist. In diesem Fall können Sie durch Aktivieren der Regel *`Avoid INTs on secondary alerts`* verhindern, dass Incidents für sekundäre Warnungen erstellt werden (dazu muss Eigenschaft *`evt_mgmt.avoid_int_enabled`* aktiviert sein), da für die primäre Warnung bereits ein Incident vorhanden ist.
Kandidat für schwerwiegenden Incident erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen. Ein Kandidat für einen schwerwiegenden Incident kann auf einen schwerwiegenden Incident aktualisiert werden. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Kandidat für schwerwiegenden Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Schwerwiegenden Incident aus Warnung erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents aus einer Warnung Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten schwerwiegenden Incident auszufüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem (Fortsetzung)

Name	Beschreibung
	Hinweis: • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Schwerwiegenden Incident mit Auswirkung erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents aus einer Warnung, in der auch das Feld **Auswirkung** als Eingabe verwendet wird. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten schwerwiegenden Incident auszufüllen. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Kandidat für schwerwiegenden Incident mit Auswirkung erstellen	Subflow zum Erstellen eines Kandidaten für schwerwiegenden Incident, in dem auch das Feld **Auswirkung** als Eingabe verwendet wird. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen. Ein Kandidat für einen schwerwiegenden Incident kann auf einen schwerwiegenden Incident aktualisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

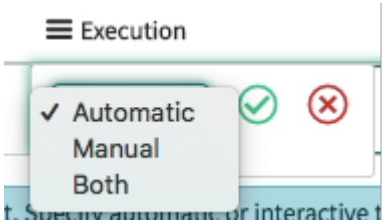
Subflows im Basissystem (Fortsetzung)

Name	Beschreibung
	Hinweis: • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Kandidat für schwerwiegenden Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Aufgabe erstellen (veraltet)	Dieser Subflow verwendet, sofern vorhanden, eine Aufgabenvorlage oder das `EventMgmtCustomIncidentPopulator`Skript für Instanzen, die aus veralteten Releases (vor dem London-Release) migriert werden. Falls konfiguriert, wenden Sie die Aufgabenvorlage an. **Hinweis:** Fügen Sie die Spalte **Aufgabenvorlage** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_rule] hinzu und wählen Sie eine Aufgabenvorlage und eine Aufgabe aus, die bei Ausführung der Regel angewendet werden sollen.
Warnvorlage überschreiben (veraltet)	Dieser Subflow wendet die Alarmvorlage an. Dieser Subflow wird für Instanzen bereitgestellt, die aus veralteten Releases (vor dem London-Release) migriert werden. **Hinweis:** Fügen Sie die Spalte **Aufgabentyp** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_rule] hinzu und wählen Sie eine Aufgabenvorlage aus, die bei Ausführung der Regel angewendet werden soll.

1. Wählen Sie den von Ihnen benötigten Subflow aus.
2. Informationen zum Anpassen eines Subflows finden Sie unter Erstellen Sie einen anwenderdefinierten Subflow für Warnungen. Dieses Thema beschreibt auch die Eingabeparameter in einem Subflow.
3. Wenn Sie angeben möchten, wann der Workflow ausgeführt werden muss, doppelklicken Sie auf die Zelle unter **Ausführung**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



.

Erstellen Sie einen anwenderdefinierten Subflow für Warnungen

Sie können einen Subflow gemäß Ihren Anforderungen erstellen. Sie können beispielsweise Warnungen lösen, Teams benachrichtigen oder Korrekturaktionen ausführen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, flow_designer

Warum und wann dieser Vorgang ausgeführt wird

Kopieren Sie einen vorhandenen Subflow, und passen Sie ihn an. Veröffentlichen Sie den benutzerdefinierten Subflow, damit er zur Lösung von Warnungen verwendet werden kann. Weitere Informationen finden Sie unter Erstellen Sie einen Subflow .

Hinweis: Wenn Ihre Instanz ServiceNow Domänentrennung verwendet, müssen Sie sicherstellen, dass der neue benutzerdefinierte Subflow, den Sie erstellt haben, nur auf die Daten der angegebenen Domäne angewendet wird.

Prozedur

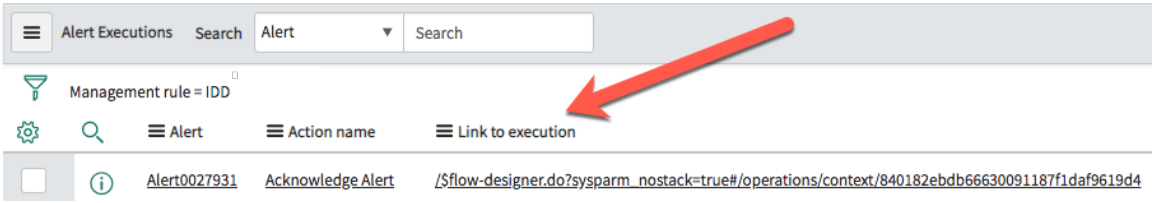
1. Navigieren zu **Alle** > **Prozessautomatisierung** > **Flow Designer**an.
2. Klicken Sie im Fenster „Flow Designer“ auf **Subflows**.
3. Klicken Sie auf **Incident erstellen**.
   Der Subflow „Incident erstellen“ wird im Flow Designer im schreibgeschützten Format geöffnet. Die Eingaben im Subflow „Incident erstellen“ werden in der folgenden Tabelle beschrieben.

Incident-Eingabeparameter erstellen

Wert	Beschreibung
alertRuleName	Der Name der Warnungsverwaltungsregel, die diesen Subflow angibt, z. B. `IDD`.
alertRuleId	Die sys_id der Warnungsverwaltungsregel, z. B. `1ae122e84f5f1300b28392918110c71e`.
alertGR	Der Warnungsdatensatz, der dem Filter entspricht, der in der Warnungsverwaltungsregel definiert ist, z. B. `Alert0027931`
executionId	Die ID der abzurufenden Ausführung, z. B. `000182ebdb66630091187f1daf9619d4`
userName	Der Name des aktuellen Anwenders, z. B. `Administrator` .
userDisplayName	Der Name, den der aktuelle Anwender für die Anzeige angegeben hat, z. B. `Systemadministrator` .

Beispiel: In einer Warnungsverwaltungsregel, die Warnungen verarbeitet hat, klicken Sie im Bereich „Warnungsausführungen“ auf den **Link zur Ausführung** der erforderlichen Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Flow Designer wird geöffnet. Klicken Sie auf **Subfloweingaben und -ausgaben**. Die Namen der Eingabevariablen des Subflows werden mit ihren jeweiligen Werten angezeigt.

Subflow Input

VARIABLE NAME	TYPE	RUNTIME VALUE
alertGR	Reference	Alert0027931
alertRuleId	String	1ae122e84f5f1300b28392918110c71e
alertRuleName	String	IDD
executionId	String	000182ebdb66630091187f1daf9619d4
userDisplayName	String	System Administrator
userName	String	admin

4. Klicken Sie im Header des Subflows auf „Weitere Aktionen“ , und wählen Sie **Subflow kopieren**.
5. Im Feld **Neuer Subflow-Name** geben Sie den Namen des neuen Subflows ein.
6. Um den Anwendungsbereich des Subflows zu beschränken, wählen Sie im Feld **Anwendung** die erforderliche Anwendung aus, andernfalls wählen Sie Global.
7. Klicken Sie auf **Kopieren**.
   Der neue Subflow wird erstellt und als Registerkarte im Subflow-Designer-Editor geöffnet. Die von der Vorlage bereitgestellten Eingaben werden angezeigt.

   Eingaben sind fest und es kann nichts hinzugefügt werden.

   Im Editor können Sie Subflow-Eingaben oder -Ausgaben je nach Bedarf löschen.
8. Zum Löschen einer Eingabe klicken Sie auf das .
   Eingaben sind fest und es kann nichts hinzugefügt werden.
9. Erstellen Sie Subflow-Ausgaben, indem Sie die Namen und Datentypen definieren.
   a. Klicken Sie auf das , um eine Ausgabe hinzuzufügen.
   b. Definieren Sie den Namen und den Datentyp.
10. Klicken Sie auf **Speichern**, um den Subflow im Entwurfsstatus zu speichern.
11. Um den Subflow zu speichern und zu veröffentlichen, sodass er im Regel-Designer der Warnungsverwaltung verwendet werden kann, klicken Sie auf **Veröffentlichen**.

Ergebnis

Schließen Sie den geänderten Subflow in eine Warnungsverwaltungsregel ein, um Warnungen gemäß Ihren benutzerdefinierten Anforderungen aufzulösen.

Zugehörige Informationen

Subflows

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zur Warnungsausführung

Warnungsausführungsinformationen bieten einen Verweis auf die durchgeführten Warnungsverwaltungsregelaktionen. Diese Informationen werden nur dann im Datensatz der Warnungsverwaltungsregel angezeigt, wenn eine Warnung dem Filter in der Regel entspricht und eine Aktion ausgeführt wurde. Sie können auf einen beliebigen Link in der Liste Warnungsausführungen klicken, um das referenzierte Element zu öffnen.

Warnungsausführungen

Im Datensatz der Warnungsverwaltungsregel zeigt die Liste „Warnungsausführungen“ wichtige zugehörige Datensätze für die Regel an.

Hinweis: Die Liste „Warnungsausführungen“ im Datensatz „Warnungsverwaltungsregeln“ zeigt Warnungsausführungsinformationen und eine Liste der Warnungsverwaltungsregeln an, mit denen die ausgewählte Warnung übereinstimmt.

Warnungsausführungsliste

Informationen in der Warnungsausführungsliste

Die Spalten in der Warnungsausführungsliste werden mit Details der Warnungen gefüllt, die der Warnungsverwaltungsregel und den ausgeführten Aktionen entsprechen. Die aufgelisteten Warnungen entsprechen dem Filter der Regel.

Informationen zur Warnungsausführung anzeigen

Sie können auf einen beliebigen Link in der Warnungsausführungsliste klicken, um die Warnungsausführungsinformationen des referenzierten Elements zu öffnen. Diese Informationen werden nur dann im Datensatz der Warnungsverwaltungsregel angezeigt, wenn eine Warnung dem Filter in der Regel entspricht und eine Aktion ausgeführt wurde.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zu den Informationen in der Warnungsausführungsliste zählen:

- Die Liste der Warnungen, die dem Filter der Regel entsprechen.
- Die Aufgaben, einschließlich Incidents, die geöffnet wurden.
- Welche Nachbesserungs-Workflows und welche Subflows ausgeführt wurden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln**an.
2. Klicken Sie in der Liste der Warnungsverwaltungsregeln auf die Regel.
   Wenn eine Warnung mit dem Filter in der Regel übereinstimmt und eine Aktion ausgeführt wurde, wird im Datensatz der Warnungsverwaltungsregeln die Liste der Warnungsausführungen angezeigt. Die Liste wird unabhängig von der Phase der ausgewählten Warnungsverwaltungsregel angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsausführungsliste

Spalte	Beschreibung
Warnung	Warnungsnummer der Warnungen, die der Warnungsverwaltungsregel entsprechen
Aktionsname	Name der Aktion, die ausgeführt wurde, um die Warnung zu lösen (Subflow oder Workflow).
Link zur Ausführung	Link zu dem Aktionsausführungsprotokoll, das bei Ausführung der Aktion erstellt wurde.
Zugehörige Aufgabe	Link zu der Aufgabe, die erstellt wurde, als die Warnung gelöst wurde. Beispiel: Wenn die Aktion für eine Regel das Erstellen eines Incidents ist, enthält dieses Feld die Incident-Nummer mit einem Link zum Öffnen des Incidents. Es wird ein Link zur Workflow-Nachbesserungsaufgabe bereitgestellt, die zur Überwachung der Nachbesserung erstellt wird.
Log	Hinweis oder Information, die das Ergebnis der Ausführungsaktion anzeigt, z. B. wie die Ausführung erfolgte, „1 von 2 Ausführungen“. Wenn die Warnung geschlossen wird, wird die Anzahl der Ausführungen (die erste Zahl) auf 0 zurückgesetzt. Diese Informationen geben nicht an, dass der Subflow erfolgreich ausgeführt wurde, sondern dass der Aufruf des Subflows erfolgreich war und der Subflow ordnungsgemäß konfiguriert ist.
Automatische Ausführung	Angabe, wie die Aktion ausgeführt wurde: automatisch (true) oder manuell (false).
Erstellt	Datum und Uhrzeit der Erstellung des Eintrags.

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

Vorhandene Warnungsaktionsregeln aus einem früheren Release können zwar ausgeführt, aber nicht geändert werden. Migrierte Warnungsaktionsregeln werden zu Warnungsverwaltungsregeln, und alle Definitionen der Warnungsaktionsregeln werden in das Warnungsverwaltungsregelformat migriert. Migrierte Regeln können geändert werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

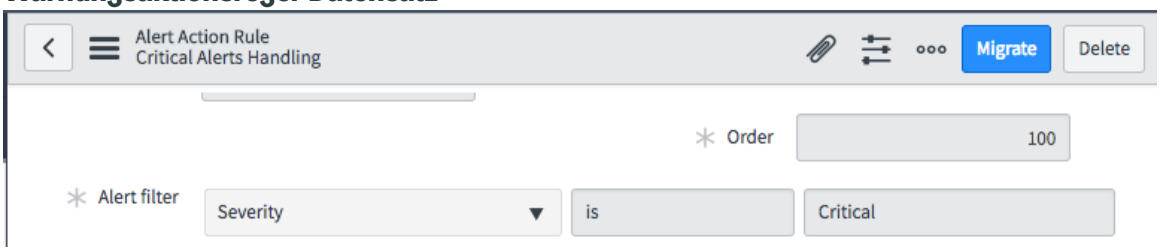
Vorhandene Warnungsaktionsregeln sind aktive, schreibgeschützte Regeln. Eine Warnungsaktionsregel kann nur geändert werden, nachdem sie in eine Warnungsverwaltungsregel migriert wurde.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Warnungsaktionsregeln**an.
2. Wählen Sie eine Warnungsaktionsregel zum Migrieren oder Löschen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsaktionsregel-Datensatz



3. Klicken Sie auf **Migrieren**.
   Wenn Sie auf geklickt haben **Migrieren** , Die Liste der migrierten Regeln kann zusammen mit neuen Warnungsverwaltungsregeln gefunden werden, indem Sie zu navigieren **Ereignismanagement** > **Bedingungen** > **Warnungs-Management**an.

   Nach einer erfolgreichen Migration werden alle Definitionen der Warnungsaktionsregeln in das Warnungsverwaltungsregelformat migriert.

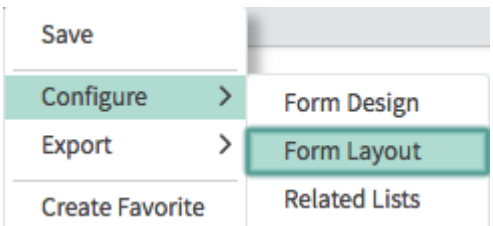
Ergebnis

Wenn eine Alarmaktionsregel erfolgreich migriert wurde, kann die Alarmaktionsregel nicht mehr geändert werden. Die neue Warnungsverwaltungsregel kann jedoch geändert werden.

Nächste Maßnahme

Wenn die migrierte Alarmaktionsregel über eine Aufgabenvorlage verfügt, können Sie den Designer der Alarmverwaltungsregel so anpassen, dass der Name der Aufgabenvorlage angezeigt wird.

1. Klicken Sie im Header der Warnungsverwaltungsregel auf **Zusätzliche Aktionen** .
2. Auswahlvorgang **Konfigurieren** > **Formularlayout**an.



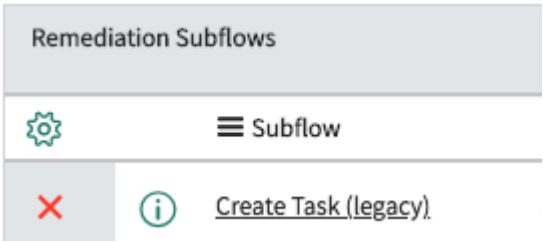
3. Wählen Sie im Bereich **Verfügbar Aufgabenvorlage**, und verschieben Sie sie in den Bereich **Ausgewählt**. Positionieren Sie sie wie erforderlich.

4. Wählen Sie im Feld **Aufgabenvorlage** die zu verwendende Vorlage aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie auf der Registerkarte „Aktionen“ im Bereich „Nachbesserungs-Subflows“ den (veralteten) Subflow „Aufgabe erstellen“ (veraltet) aus, um die Aufgabenvorlage auszuführen.



Zugehörige Informationen

Schnelle Antworten in einer Warnung anwenden

Warnungsantwort wird mit automatisierter Warnungsgruppierung synchronisiert

Synchronisieren Sie die Warnungsantwort mit der Gruppierung, indem Sie sicherstellen, dass Warnungsverwaltungsaufträge nach Warnungsgruppierungsaufträgen ausgeführt werden. Dadurch werden doppelte Aktionen wie die Incident-Erstellung für sekundäre Warnungen verhindert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird der Warnungsgruppierungsauftrag (**Service Analytics gruppiert Warnungen mit RCA/Warnungszusammenfassung**) Und den Warnungsverwaltungsauftrag (**Ereignismanagement: Management0 Für Bereichsbezogene Warnungsregeln Auswerten**) Wird unabhängig voneinander ausgeführt. Um die Warnungsantwort mit der automatisierten Warnungsgruppierung zu synchronisieren (z. B. um die Erstellung eines Incidents für eine sekundäre Warnung zu vermeiden), müssen Sie die Eigenschaft aktivieren `evt_mgmt.avoid_int_enabled`Um sicherzustellen, dass der Warnungsverwaltungsauftrag ausgeführt wird, nachdem der Warnungsgruppierungsauftrag abgeschlossen wurde. Diese Eigenschaft ist über zugänglich Ereignismanagement Eigenschaftenseite (**Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**) an. Darüber hinaus müssen Sie die entsprechende Warnungsverwaltungsregel konfigurieren (z. B. für die Incident-Erstellung), um alle sekundären Warnungen herauszufiltern.

Hinweis: Wenn bei der Ausführung des Warnungsverwaltungsauftrags nur eine Warnung vorhanden ist, wird ein Incident erstellt. Wenn später eine zweite Warnung eingeht, bildet der nächste Warnungsgruppierungsauftrag eine Gruppe, macht die neue Warnung als sekundär und erstellt einen neuen Incident.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**an.
2. Wenn Sie Incidents bei sekundären Warnungen vermeiden möchten, wählen Sie aus **Aktivieren Sie „Incidents bei sekundären Warnungen vermeiden“, und warten Sie, bis der Gruppierungsauftrag ausgeführt wird** Kontrollkästchen.
3. Wählen Sie **Speichern**.
4. Um sekundäre Warnungen herauszufiltern, navigieren Sie zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln**an.
5. Wählen Sie die entsprechende Regel aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie im Formular Warnungsverwaltungsregel die aus **Warnungsfilter** Registerkarte.
7. Wählen Sie im Bedingungsbereich aus **Und** .
8. Bedingung hinzufügen:
   - **Rolle in Gruppe**
   - **ist nicht**
   - **Sekundär**
9. Wählen Sie **Aktualisieren**.

Aktionen zum Beheben von Warnungen konfigurieren

Führen Sie Befehle zum Beheben von Warnungen für CIs von Linux- und Windows-Remote-Systemen aus.

Vorbereitungen

Installieren Sie die folgenden Plugins:

- IntegrationHub Enterprise Spokes-Plugin
- ServiceNow IntegrationHub-Aktionsschritt – PowerShell
- ServiceNow IntegrationHub-Aktionsschritt – SSH

Unter Linux: Vergewissern Sie sich, dass der Remote-Linux-Host über die MID-Server-IP-Adresse erreichbar ist, über die Aktionsskripts ausgeführt werden.

Für Windows:

- Stellen Sie sicher, dass Powershell v3.0 bis 5,0 unterstützt und auf installiert sind Windows Zielserver.
- Aktivieren Sie Powershell-Remoting auf der Remote Windows Zielserver.
- Stellen Sie sicher, dass Remote Windows Der Zielserver ist über den FQDN von erreichbar MID-Server Das Aktionsskripts ausführt.

Fügen Sie den Aliassen für Anmeldeinformationen, die mit dem Basissystem bereitgestellt werden, Anmeldeinformationen hinzu:

- linuxAdmin
- windowsAdmin

Erforderliche Rolle: evt_mgmt_admin oder flow_designer

Prozedur

1. Greifen Sie auf eine der folgenden Arten auf Korrekturaktionen zu:
   - Über Schnellaktionen in einer Warnung, wie in Schnelle Antworten in einer Warnung anwenden beschrieben.
   - Die Registerkarte Playbook in Service Operations-Arbeitsbereich, Wie in beschrieben Führen Sie Aktionen aus, um Warnungsprobleme zu lösen .
2. Konfigurieren Sie zusätzliche Eingaben im Feld **Zusätzliche Information** der Warnung, und verwenden Sie dazu folgendes Format:

```
{"remediation_action_resource":"<mandatory input>"}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Pflichteingabe pro Aktion wird in der folgenden Tabelle beschrieben.

Aktionsname	Pflichteingabe im Feld „Zusätzliche Information“
Windows-Prozess beenden	Prozess-ID
Linux-Service neu starten	Servicename
Linux-Prozess beenden	Prozess-ID
Windows-Prozesse abrufen	N/V
Windows-Dienst beenden	Anzeigename für Service
Windows-Dienst neu starten	Anzeigename für Service
Windows-Dienste abrufen	N/V
Linux-Service beenden	Servicename
Windows-Dienst starten	Anzeigename für Service
Windows-Dienst anhalten	Anzeigename für Service
Linux-Services abrufen	N/V
Linux Top-Befehl für Arbeitsspeicher ausführen	N/V
Verwendeten Speicherplatz anzeigen	N/V
Linux Top-Befehl ausführen	N/V
Linux-Service starten	Servicename
Verwendeten Speicherplatz anzeigen	N/V

Ergebnis

Nach der Ausführung einer Warnungsaktion werden die Ergebnisse im Feld `Work Notes` der Warnung vermerkt.

Zugehörige Informationen

- Fehlerbehebung bei WMI-/Powershell-Problemen auf dem Remotecomputer
- WMI, PowerShell und Windows Firewalls
- MID-Server: Fehlerbehebung bei WMI-/Powershell-Problemen – Anmeldeinformationen
- So aktivieren/testen Sie PowerShell-Remoting auf Windows-Host

CI-Fehlerkorrektur

Warnungs- und Configuration Item (CI)-Fehlerkorrekturen helfen bei der Behebung von zugrunde liegenden Problemen, die Warnungen generieren. Die Fehlerkorrektur basiert auf Orchestrierungs-Workflows, die zur Ausführung von Fehlerkorrekturmaßnahmen wie dem Erfassen von Systeminformationen oder dem Neustart eines Servers geskriptet werden können.

Ereignismanagement bietet einen Rahmen für die Konfiguration und Implementierung eines systemweiten Fehlerkorrekturplans zur Lösung, Minimierung oder Verhinderung von Problemen, die Events und Warnungen generieren. Konfigurieren Sie Warnungsverwaltungsregeln für die Fehlerkorrektur von Warnungen und CI-Fehlerkorrekturregeln für die Fehlerkorrektur einer Reihe von CIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungs-Fehlerkorrektur

Verwenden Sie Warnungsverwaltungsregeln, um bestimmte Warnungen einem Fehlerkorrektur-Workflow zuzuordnen. Sie können einen Workflow manuell auf Warnungen anwenden. Alternativ können Sie die Warnungsverwaltungsregel konfigurieren, die einen Workflow automatisch für Warnungen ausführt, die den Regelkriterien entsprechen. Der Workflow kann auch geskriptet werden, um eine Benutzergenehmigung anzufordern, bevor nachfolgende Workflow-Aufgaben ausgeführt werden. Der Workflow wird zur Benutzergenehmigung angehalten, auch wenn er automatisch ausgelöst wurde.

CI-Fehlerkorrektur

Konfigurieren Sie die Fehlerkorrektur umfassender, indem Sie CI-Fehlerkorrekturregeln erstellen, um die Fehlerkorrektur manuell auf bestimmte CIs anzuwenden.

Nachbesserungsaufgaben

Wenn ein Fehlerkorrektur-Workflow ausgeführt wird, wird eine Fehlerkorrekturaufgabe erstellt, um Details zu erfassen, wie z. B. die Zeit, zu der der Workflow gestartet wurde, die Warnung, die den Fehlerkorrektur-Workflow ausgelöst hat (falls relevant) und das CI, das korrigiert wurde. Zeigen Sie diese Aufgaben an, um Korrekturaktivitäten in der Organisation nachzuverfolgen.

Zugehörige Informationen

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

CI-Fehlerkorrektur erstellen oder bearbeiten

Erstellen Sie eine CI-Fehlerkorrekturregel, mit der Benutzer manuell einen Orchestration Workflow zur Lösung von Problemen mit bestimmten CIs anwenden können, die Warnungen zugeordnet sind. Definieren Sie diese CIs in den CI-Filterbedingungen der Regel.

Vorbereitungen

Erstellen Sie den Workflow, um CIs zu beheben. Wählen Sie in den Workflow-Einstellungen **Fehlerkorrektur-Aufgabe [em_remediation_task]** im Feld **Tabelle** aus.

Senden Sie dann die Workflow-Definition, und fügen Sie den Workflow-Eigenschaften die folgenden Bedingungen hinzu:

- **[Fehlerkorrektur ausführen] [ist] [true]**
- **[Workflow-] [Liste] [<Name des neuen Workflows, den Sie erstellt haben>]**

  Beispiel: Wenn der Name des Workflows `CI-Fehlerkorrektur` ist, fügen Sie diese Bedingung hinzu:

  [Workflow] [ist] [CI-Fehlerkorrektur]

Nachdem Sie den Workflow konfiguriert haben, stellen Sie sicher, dass Sie ihn veröffentlichen. Weitere Informationen finden Sie unter Erstellen Sie einen Workflow .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine CI-Fehlerkorrekturregel ordnet eine Reihe von CIs zu, bei denen Probleme mit einem Fehlerkorrektur-Workflow auftreten können. Der Fehlerkorrektur-Workflow kann entweder das zugrunde liegende Problem lösen oder zur Behebung des Problems beitragen, das die Warnung generiert hat. Beispielsweise können Sie proaktiv einen Workflow mit den entsprechenden Antwortaktionen für vorhersehbare Warnungen konfigurieren. Weitere Informationen finden Sie in unserem kurzen Video Event Management-Fehlerkorrektur .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **CI-Fehlerkorrekturen**an.
2. Klicken Sie auf **Neu**, oder wählen Sie eine CI-Fehlerkorrektur zur Bearbeitung aus.
3. Füllen Sie die Felder aus, und klicken Sie auf **Senden** oder **Aktualisieren**.

CI-Fehlerkorrekturformular

Kontrolldiagramm	Beschreibung
CI-Filter	Bedingungen, die den CIs entsprechen, auf die Sie diese Fehlerkorrektur anwenden möchten.
Orchestrierungs-Workflow	Der Fehlerkorrektur-Workflow, der auf CIs angewendet werden soll, die den Filterbedingungen entsprechen.

Ergebnis

In Servicezuordnungen, die über das Dashboard Ereignismanagement geöffnet werden, kann diese Fehlerkorrektur auf alle CIs angewendet werden, die den Filterbedingungen entsprechen.

Fehlerkorrekturaufgaben anzeigen

Ereignismanagement erstellt automatisch eine Fehlerkorrekturaufgabe, um jede Fehlerkorrektur zu erfassen, die auf ein CI oder eine Warnung angewendet wurde. Sie erhalten damit eine Gesamtansicht der Fehlerkorrekturaktivitäten in der Organisation.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Korrekturaufgaben**an.

Spalte	Beschreibung
Zahl	Nummer, die der Aufgabe zugewiesen ist.
Konfigurationselement	Element oder Service, der von dieser Aufgabe betroffen ist.
Priorität	Priorität, die dieser Aufgabe zugewiesen wurde, basierend auf Auswirkung und Dringlichkeit.
Status	Status der Aufgabe, der offen oder geschlossen sein kann.
Zugewiesen an	Person, der diese Aufgabe zugewiesen wurde.
Kurzbeschreibung	Beschreibung der Aufgabe
Aufgabentyp	Dieser Aufgabentyp ist eine Fehlerkorrekturaufgabe.

Funktionsweise von Warnungen mit CIs in der Wartung

Wenn sich ein CI in der Wartung befindet, werden die Auswirkungsstruktur, die Servicezuordnung und die Registerkarte „Warnungen“ basierend auf verschiedenen Faktoren aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement Teil 2 | Auswirkungsstruktur Sehen Sie sich dieses kurze Video an, um mehr darüber zu erfahren, wie Warnungen mit CIs funktionieren.

Ein CI wird in folgenden Fällen gewartet:

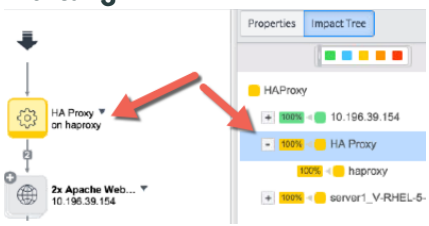
- Eine Change-Anforderung ist für das CI geplant.
- Die **Installationsstatus** Feld im CI-Datensatz ist auf festgelegt **In Wartung** .

Hinweis: Informationen zum Anpassen der Funktionsweise von Warnungen mit CIs in der Wartung finden Sie unter Wartungsregeln erstellen.

Darstellung von CIs in der Wartung in Event Management	Beschreibung und der optimale Zeitpunkt für die Lösung der Warnung
CI mit einer aktiven Change-Anforderung Ob eine aktive Change-Anforderung für das CI geplant ist oder ob **Installationsstatus** Des CI ist **In Wartung** , Alle Warnungen für das betroffene CI werden von der Berechnung der Auswirkung ausgeschlossen. Auf der Registerkarte „Warnungen“ werden alle entsprechenden Warnungen vorübergehend ebenfalls ausgeblendet. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. Die Auswirkungsstruktur und die Servicezuordnung zeigen CIs vorübergehend grün an. Für einen Service werden alle Warnungen bezüglich CIs im Service auch auf der Registerkarte „Warnungen“ ausgeblendet. Der gesamte Service wird im Auswirkungsbaum in Grün angezeigt. Für einen Host mit einer aktiven Change-Anforderung werden die Host-Applikationen als eine Einheit betrachtet. Alle untergeordneten Anwendungen werden, bis die Change-Anforderung nicht mehr aktiv ist, so behandelt wie der Host.	Eine aktive Change-Anforderung hat die folgenden Werte: • Der **Status** ist **Geplant** oder **Implementieren**. • Die aktuelle Zeit liegt zwischen geplantem Startdatum und geplantem Enddatum der Change-Anforderung. ODER • Die aktuelle Zeit liegt zwischen tatsächlichem Startdatum und tatsächlichem Enddatum der Change-Anforderung. Sie können den Fortschritt der Change-Anforderung überwachen. Warten Sie, bis die Change-Anforderung in den Status **Überprüfen** oder **Geschlossen** verschoben wird. Anschließend können Sie alle Warnungen für das betroffene CI und alle Warnungen behandeln, die zwischen Start- und Enddatum generiert wurden. Verwenden Sie die Auswirkungsstruktur, die Topologie und die Registerkarte „Warnungen“, um den berechneten Auswirkungsschweregrad anzuzeigen. **Hinweis:** Die **Wartung** Kontrollkästchen für eine Warnung ist aktiviert, wenn **Installationsstatus** Feld im CI-Datensatz ist **In Wartung** . Dies **Wartung** Das Kontrollkästchen gibt an, dass die Warnung in ausgeblendet werden muss **Warnungen** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darstellung von CIs in der Wartung in Event Management	Beschreibung und der optimale Zeitpunkt für die Lösung der Warnung
CI ohne aktive Change-Anforderung und nicht in der Wartung  Wenn keine aktive Change-Anforderung für ein CI vorhanden ist und sich das CI nicht in der Wartung befindet, wird die Auswirkungsberechnung fortgesetzt. Die Auswirkungsstruktur, die Servicezuordnung und die Registerkarte „Warnungen“ zeigen den berechneten Auswirkungsschweregrad für Warnungen an.	Eine inaktive Change-Anforderung hat die folgenden Werte: • Der **Status** ist **Neu**, **Bewerten**, **Autorisieren**, **Prüfen**, **Schließen** oder hat überhaupt keine Änderungen. • Der **Status** ist **Geplant** oder **Implementieren**. Die aktuelle Zeit liegt jedoch vor oder nach dem geplanten oder tatsächlichen Datumsbereich in der Change-Anforderung. Sie können den Fortschritt der Change-Anforderung überwachen. Wenn ein CI eine inaktive Change-Anforderung aufweist, können Sie die entsprechenden Warnungen nach Bedarf bearbeiten.
CI ohne aktive Change-Anforderung und in Wartung Wenn für das CI keine aktive Change-Anforderung geplant ist und wenn **Installationsstatus** Des CI ist **In Wartung** , Alle Warnungen für dieses CI sind von der Auswirkungsberechnung ausgeschlossen. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. Die Auswirkungsstruktur und die Servicezuordnung zeigen CIs vorübergehend grün an.	Alle Warnungen für ein CI mit einer inaktiven Change-Anforderung und **In Wartung** Hat keine Auswirkungsberechnung.

Zugehörige Informationen

Wartungsregeln erstellen

SLAs für Anwendungsservices und CIs

Ereignismanagement unterstützt die Erstellung von SLAs für Anwendungsservices und CIs.

Sie können die Qualität der von Ihrer Organisation angebotenen Services überwachen und verwalten. Beispielsweise können Sie eine SLA einrichten, die ausgelöst wird, wenn der maximale Warnungsschweregrad eines Anwendungsservice oder CI **kritisch** ist, und die Zeit messen, die erforderlich ist, um den Anwendungsservice oder das CI wieder in den Status **OK** zu versetzen , wenn die Bedingungen erfüllt sind, die die Warnung verursacht haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLAs und die Aufgabentabelle

Sie können SLAs nur für Tabellen erstellen, die die Aufgabentabelle erweitern. Die Anwendung Ereignismanagement stellt eine Tabelle mit dem Namen Ereignismanagement-SLA [em_ci_severity_task] bereit, die die Aufgabentabelle erweitert. Verwenden Sie diese Tabelle in Ihren SLAs, um den Schweregrad anzugeben, der die SLA auslösen und stoppen soll. Während der Berechnung der Warnungsauswirkung werden Änderungen im Schweregrad von Anwendungsservices und CIs automatisch in der SLA-Tabelle Ereignismanagement aktualisiert. Scheduled Jobs halten die Informationen in dieser Tabelle auf dem neuesten Stand.

Wie die Ereignismanagement-SLA-Tabelle ausgefüllt wird

Die SLA-Tabelle Ereignismanagement wird für Anwendungsservices und CIs unterschiedlich ausgefüllt:

- Bei Anwendungsservices füllt das System die SLA-Tabelle Ereignismanagement automatisch aus, wenn ein Anwendungsservice erstellt oder der maximale Schweregrad geändert wird.
- Für CIs müssen Sie zuerst identifizieren, welche CIs für SLAs verfügbar gemacht werden können, indem Sie einen SLA-Konfigurationsdatensatz erstellen. Das System füllt dann automatisch die SLA-Tabelle Ereignismanagement mit dem CI-Schweregrad „geändert“ aus.

Hinweis: Doppelte CIs werden der SLA-Tabelle Ereignismanagement nicht hinzugefügt, auch wenn dasselbe CI mehr als einem SLA-Konfigurationsfilter entspricht.

Erstellen Sie eine SLA-Konfiguration für CIs

Erstellen Sie eine SLA-Konfiguration in der Anwendung Ereignismanagement, um zu bestimmen, welche CIs für SLAs verfügbar sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Der SLA-Konfigurationsdatensatz ist ein Filter für eine Tabelle im System. Wählen Sie eine Tabelle mit den CIs aus, für die Sie eine SLA erstellen möchten.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **SLA-Konfiguration**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

SLA-Konfigurationsformularfelder

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Tabelle	Wählen Sie eine Tabelle mit den CIs aus, für die Sie eine SLA erstellen möchten. Sie können auch die Tabelle „Konfigurationselement für Host-Ansicht“ [query_based_Service_Basic_View] verwenden, die von verwendet wird Dynamische CI-Gruppen .
Filter	Konfigurieren Sie den Filter für die Datensätze.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example:
Hier ein Beispiel:

Wenn Sie eine SLA auf allen Linux-Servern für schwerwiegende und kritische Warnungen ausführen möchten, erstellen Sie zuerst eine SLA-Konfiguration in der Linux-Server-Tabelle [cmdb_ci_linux_server]. Erstellen Sie dann die SLA-Definition mit diesem Filter:

- CI.class ist ein Linux-Server
- Der Schweregrad ist „Schwerwiegend“ oder „Kritisch“

Nächste Maßnahme
Erstellen Sie eine SLA-Definition für die CIs, die dieser SLA-Konfiguration entsprechen.

Beschränken Sie die Datensätze für den SLA-Konfigurationsfilter

Wenn der SLA-Konfigurationsfilter zu viele Datensätze zurückgibt, können Sie eine Eigenschaft hinzufügen, um die maximale Anzahl von Datensätzen festzulegen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig ist die Größe von Datensätzen für dynamische CI-Gruppen auf 10.000 Elemente beschränkt. Das Überschreiten dieses Grenzwerts kann die Systemstabilität beeinträchtigen. Wenn die Filterkonfiguration für eine angegebene dynamische CI-Gruppe zu viele Datensätze zurückgibt, können Sie die Anzahl der zurückgegebenen Datensätze beschränken, indem Sie den Wert der Eigenschaft „sa.qbs.max_num_of_cis“ festlegen. Weitere Informationen finden Sie unter Erstellen Sie eine dynamische CI-Gruppe .

Prozedur

1. Geben Sie sys_properties.list im Anwendungsnavigator ein.
2. Fügen Sie die folgenden Eigenschaften hinzu:
   sa.qbs.max_num_of_cis
3. Legen Sie den Wert auf eine ganze Zahl fest, die die maximale Anzahl zurückzugebender Datensätze darstellt.

Erstellen Sie eine SLA-Definition für ein CI oder einen Anwendungsservice

Sie können SLAs für CIs und Anwendungsservices genau wie für andere Aufgabendatensätze in der Instanz erstellen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Service-Level-Management** > **SLA** > **SLA-Definitionen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „SLA-Definition“ aus.
   Eine Beschreibung der einzelnen Felder finden Sie unter Erstellen Sie eine SLA-Definition für ein CI oder einen Anwendungsservice.
4. Wählen Sie für das Feld **Tabelle** die Option **Event Management SLA [em_ci_severity_task]** aus .
5. Konfigurieren Sie den **Startbedingungsfilter,** indem Sie Bedingungen hinzufügen, z. B .:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLA-Filterbedingungen

Für alle CIs mit **kritischem Schweregrad**		
Typ	**ist**	**CI** **Hinweis:** Ereignismanagement-SLAs funktionieren nur für CI-Klassen aus der Serviceinstanz [cmdb_ci_Service_Auto].
Schweregrad	**ist**	**Kritisch**
Für einen bestimmten Service, z. B. E-Mail, wenn der **Schweregrad kritisch** ist		
Anwendungsservice	**ist**	**E-Mail**
Schweregrad	**ist**	**Kritisch**

6. Konfigurieren Sie Bedingungen für Pause, Stopp und Zurücksetzen.
7. Klicken Sie auf **Absenden**.

Warnungslebenszyklus-Konfiguration

Ereignismanagement bietet verschiedene Module, Vorlagen und Eigenschaften für die Konfiguration von Warnungen und die Aktionen, die für diese Warnungen ausgeführt werden.

Konfigurieren des aktiven Alarmintervalls

Die aktive Intervalleigenschaft (**evt_mgmt.Active_interval**) Bestimmt, wie Ereignismanagement Verarbeitet ein neues Ereignis, das Ereignissen ähnelt, die in einer vorhandenen geschlossenen Warnung angezeigt werden. Basierend auf dem aktiven Intervall, dem Ereignis und den vorhandenen geschlossenen Warnungsinformationen wird die Warnung erneut geöffnet, und die Ereignisinformationen werden der vorhandenen Warnung hinzugefügt, oder eine neue Warnung wird erstellt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das neue Ereignis empfangen wird und die Warnung bereits geschlossen ist, Ereignismanagement Vergleicht die Zeit seit der letzten Warnungsaktualisierung (**sys_updated_on**) Und den Wert der aktiven Intervalleigenschaft. Anschließend aktualisiert das System entweder die vorhandene Warnung oder erstellt eine neue Warnung (wenn die ursprüngliche Warnung geschlossen wird), wie in der folgenden Tabelle erläutert. Wenn die Warnung offen ist, Ereignismanagement Aktualisiert es automatisch, ohne den Wert der aktiven Intervalleigenschaft zu überprüfen.

Szenario	Ergebnis
Das neue Ereignis tritt ein, bevor das aktive Intervall für die vorhandene geschlossene Warnung verstrichen ist.	Das Ereignis wird als Wiederholung eines vorhandenen Problems identifiziert. Die Warnung wird mit den Ereignisinformationen aktualisiert, und die Warnung wird erneut geöffnet.
Das neue Ereignis tritt auf, nachdem das aktive Intervall für die vorhandene geschlossene Warnung verstrichen ist.	Eine neue Warnung wird erstellt, da das Ereignis als neues Problem identifiziert wird. Die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Ergebnis
	Ereignisinformationen werden der neuen Warnung hinzugefügt.

Ändern Sie das aktive Intervall, indem Sie das **aktive Intervall (in Sekunden)** bearbeiten , innerhalb dessen ein neues Ereignis einen Eigenschaftswert der geschlossenen Warnung erneut öffnet .

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**an.
2. Ändern Sie die Anzahl der Sekunden für die Eigenschaft **Aktivintervall (Zeitintervall in Sekunden, innerhalb dessen von einem neuen Ereignis ein geschlossener Alarm erneut geöffnet wird)**.
3. Klicken Sie auf **Speichern**.

Fluktuierende Warnungen konfigurieren

Legen Sie Fluktuationseigenschaften fest, um zu bestimmen, wann eine Warnung in den Status „Fluktuierend“ übergeht oder diesen verlässt. Flattern kann auf Konfigurationsprobleme (d. h. zu niedrig festgelegte Schwellenwerte), störende Services oder tatsächliche Netzwerkprobleme hinweisen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Flattern tritt auf, wenn von der Event-Quelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Flattern bewirkt, dass der Status der Ressource wiederholt zwischen dem Schweregrad `OK` und einem Schweregrad schwankt, der Aufmerksamkeit erfordert, z. B. `Critical`.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**an.
2. Bearbeiten Sie die folgenden Eigenschaften nach Bedarf.

Eigenschaft	Beschreibung
evt_mgmt.update_alert_restricted_fields_elapsed_time	Wenn das System Ereignisse empfängt, die keine Warnungen aktualisieren – da die Ereignisdaten nicht neu sind und mit der vorhandenen Warnung identisch sind, werden Systemfelder standardmäßig nicht aktualisiert. Dies trägt zur Reduzierung von Rauschen bei. Beispielsweise kann alle paar Minuten ein Keep-Alive-Ereignis von einem Server gesendet werden, um zu bestätigen, dass ein Gerät noch verbunden ist, auch wenn keine neuen Daten ausgetauscht werden. Diese Eigenschaft definiert das Mindestzeitintervall (in Sekunden), das vergehen muss, bevor eine Warnung basierend auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	identischen Ereignissen aktualisiert werden kann. Wenn innerhalb dieses Intervalls ein identisches Ereignis empfangen wird, wird das Update unterdrückt, um häufige, redundante Benachrichtigungen zu vermeiden. Standardmäßig ist das Intervall auf 86.400 Sekunden (24 Stunden) festgelegt.
evt_mgmt.flap_interval	Fluktuationsintervall in Sekunden, das der Zeitraum ist, innerhalb dessen eine Warnung in den Fluktuationsstatus übergeht. Eine Warnung tritt in den Status „Fluktuierend“ ein, wenn seine aktuelle **Anzahl der Fluktuationen** den gegebenen *`evt_mgmt.flap_frequency`* Eigenschaftswert innerhalb der von der angegebenen Eigenschaft *`evt_mgmt.flap_interval`* festgelegten Zeit erreicht oder überschreitet.
evt_mgmt.flap_frequency	Fluktuationshäufigkeit (die zum Übergehen in den Status „Fluktuierend“ erforderliche Warnungshäufigkeit).
evt_mgmt.flap_quiet_interval	Intervall für Verlassen des Fluktuationsstatus (Zeit in Sekunden, die vergehen muss, bis eine Warnung den Status „Fluktuierend“ verlässt). Eine Warnung verlässt den Status „Fluktuierend“, wenn das Zeitintervall zwischen dem letzten Auftreten des Events und der **letzten Aktualisierungszeit** der Warnung den Eigenschaftswert *`evt_mgmt.flap_quiet_interval`* erreicht oder überschreitet. Eine Warnung kann den Status „Fluktuierend“ auch unter folgenden Bedingungen verlassen: ○ Wenn ein eingehendes Event nach Ablauf der Zeit *`flap_quiet_interval`* eintritt. Die neue Warnung wird generiert, und ihr Statuswert hängt vom Schweregrad des eingehenden Events ab. ○ Nach einem Hintergrundauftrag, der alle fünf Minuten ausgeführt wird, wird sichergestellt, dass keine Warnungsaktualisierungen stattgefunden haben und die Zeit *`flap_quiet_interval`* verstrichen ist. Wenn keine Updates vorhanden sind,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	zeigt die Warnung den vorherigen Sta–tuswert vor der Ausführung des Hinter–grundauftrags an.

3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Sie können überwachen **Ereignismanagement** > **Alle Warnungen** Liste für Warnungen, die sich im Fluktuationsstatus befinden. Details finden Sie unter Warnungen im Status „Fluktuierend“ anzeigen.

Zugehörige Informationen

Mit fluktuierenden Warnungen arbeiten

Warnungen im Status „Fluktuierend“ anzeigen

Warnungspriorität

Bestimmen Sie die Reihenfolge, in der Warnungen behandelt werden, anhand der Punktzahl der Warnungspriorität. Mehrere Faktoren bestimmen die Priorität der Warnung, und dieser Wert ändert sich mit Änderungen an den zugrunde liegenden Faktoren.

Multifaktor-Entscheidungen

Der Wert der Warnungsprioritätspunktzahl setzt sich aus dem Wert der Kategorie und ihrer relativen Gewichtung zusammen. Sie können die Faktoren, aus denen die Punktzahl besteht, wie in den folgenden Abschnitten beschrieben, gemäß `Category order`, `Category value mapping` und `CI type weight factor mapping` konfigurieren. Die Kategorien sind:

- `Accumulated categories` - Diese Kategorien kumulieren Elemente mit verschiedenen Untertypen, die möglicherweise einen anderen Status oder Gewichtsfaktor haben. Beispielsweise Services, die nach unterschiedlicher Relevanz berücksichtigt werden, oder Services, die nach Kosten berücksichtigt werden.
- `Choice-list categories` - Eine Liste von Elementen Sie können jedes Element einem anderen Wert zuordnen, wodurch die Priorität für dieses Element geändert wird. Beispielsweise kann der kritische Schweregrad, der standardmäßig den Wert 1 hat, 4 zugeordnet werden, um ihm eine höhere Gewichtung in der berechneten Warnungspriorität zu geben.

Kategorienliste

Kategorie	Beschreibung
Kumulierte Kategorien	
Anzahl der betroffenen Business Services	Diese Kategorie wird von der Geschäftsrelevanz des Services berücksichtigt. Eine Warnung, die sich auf einen Service auswirkt, hat eine niedrigere Priorität als eine Warnung, die sich auf viele Services auswirkt. Wenn beispielsweise ein Router ausgefallen ist, kann dies Auswirkungen auf viele Services haben, und eine höhere Priorität stellt sicher, dass diese Warnung vor einer anderen behandelt wird, die sich auf weniger Services auswirkt. Eine Warnung, die sich auf viele nicht kritische Services auswirkt, muss mit Priorität behandelt werden. Wenn sich eine Warnung jedoch nur auf einige wenige Services auswirkt, dies aber wichtige Services sind, hat diese Warnung eine höhere Priorität.
CI-Typ	Diese Kategorie unterscheidet verschiedene CI-Typen. Beispielsweise kann eine Warnung auf einem CI-Typ, der ein Router oder Switch ist, eine höhere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorienliste (Fortsetzung)

Kategorie	Beschreibung
	Priorität haben als eine Warnung auf einem anderen CI-Typ, z. B. einem Server oder einer Anwendung.
Anzahl sekundärer Warnungen	Warnungen, die ähnliche Eigenschaften wie andere Warnungen aufweisen, werden normalerweise gruppiert, z. B. Warnungen mit demselben Nachrichtenschlüssel. Eine übergeordnete Warnung mit vielen sekundären Warnungen hat eine höhere Priorität als eine übergeordnete Warnung mit nur wenigen sekundären Warnungen. Alle sekundären Warnungen einer übergeordneten Warnung werden gezählt. Wenn eine sekundäre Warnung geschlossen wird, ist sie nicht mehr mit der übergeordneten Warnung korreliert. Wenn eine übergeordnete Warnung geschlossen wird, sind alle sekundären Warnungen nicht mehr korreliert, und ihr Prioritätswert wird entsprechend berechnet.
Auswahllisten-Kategorien	
Warnungsstatus	Für eine Warnung im Status `Closed` wird keine Prioritätspunktzahl berechnet. Die verfügbaren Status mit ihren Standardwerten sind: • Offen = Zuordnungswert 1 • Erneut öffnen = Zuordnungswert 2 • Flattern = Zuordnungswert 3
Warnungsschweregrad	Die Prioritätspunktzahl spiegelt den Schweregrad der zugrunde liegenden Warnung wider, z. B. hat eine Warnung mit dem Schweregrad `Critical` einen höheren gewichteten Wert als eine Warnung mit dem Schweregrad `Minor`. Für eine Warnung mit dem Schweregrad `OK` wird keine Priorität berechnet. Die verfügbaren Stufen sind: • Kritisch • Hoher • Geringer • Warnung
Rolle	Die Prioritätspunktzahl spiegelt die Rolle der Warnung wider. Die Prioritätspunktzahl ist höher für eine Warnung mit der Rolle `Parent` hat, darauf folgt Rolle `None`, und das geringste Gewicht hat eine Warnung mit Rolle `Secondary`. Eine übergeordnete Warnung mit vielen sekundären Warnungen hat einen höheren Wert als eine übergeordnete Warnung mit weniger sekundären Warnungen. Die verfügbaren Rollen sind: • Übergeordnet • Keine • Sekundär

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Struktur der Warnungsprioritätspunktzahl

Gewichteter Wert für jede Kategorie

Jede Kategorie verfügt über eine eigene Platzierung in der Alarmprioritätspunktzahl, entsprechend ihrer Reihenfolge und ihrem Limit. Wie nachfolgend unter Warnungsprioritätspunktzahl ändern beschrieben, können Sie Reihenfolge und Grenzwert konfigurieren. Es gibt nur positive Zahlen.

Mit Ausnahme der folgenden werden alle Kategoriewerte aus der Tabelle *em_alert_priority_category_mapping* zugeordnet:

- CI-Typ: Aus der Tabelle *em_alert_priority_ci_type* zugeordnet
- Sekundär: Der Wert entspricht der Anzahl der sekundären Warnungen und wird aus keiner Tabelle zugeordnet.

Hinweis: Um einen optimalen Arbeitsspeicherschutz zu gewährleisten, haben Warnungsgruppen mit mehr als 1000 Warnungen möglicherweise keine genaue Prioritätspunktzahl.

Beispielkomponenten für die Warnungsprioritätspunktzahl 7302020.003

Kategorie	Punktzahl
Services	(7,0, 1000000,0) Beispiel: Es gibt 2 betroffene Services, deren geschäftliche Relevanz wie folgt bewertet wird: • Service1: Geschäftsrelevanz-Prioritätspunktzahl = **3** • Service2: Geschäftsrelevanz-Prioritätspunktzahl = **4** Die Summe der geschäftlichen Relevanzprioritätspunktzahlen ist **7**, daher beträgt der berechnete Prioritätswert 7.000.000 (7 * 1.000.000). **Hinweis:** Die Prioritätspunktzahl der Geschäftsrelevanz ist der zugeordnete Wert (**Wert nach Zuordnung**) In den Anwendungsservices-Einträgen der Tabelle „Zuordnungen der Warnungsprioritätskategorie“ (em_Alert_Priority_category_Mapping).
Schweregrad	(3,0, 100000,0)
CI-Typ	(20,0, 100,0)
Rolle	(2,0, 10,0)
Sekundär	(0, 0,01)
Status	(3,0, 0,001)

Mit den Punktzahlen aus der vorherigen Tabelle wird die Warnungsprioritätspunktzahl wie folgt berechnet:

```
(Services value * 1,000,000) + (Severity value * 100,000) + (CI type value
* 100) + (Role value * 10) + (Secondary value) + (State value * 0.001)
```

Durch Ersetzen der Werte der Kategorien aus der vorherigen Tabelle in der Formel ergibt sich:

```
(7 * 1,000,000) + (3 * 100,000) + (20 * 100) + (2 * 10) + (0 * 0.001) + (3
* 0.001) = 7,302,020.003
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Bereich **Prioritätsaufgliederung** der Registerkarte **Weitere Informationen** wird als Warnungsprioritätswert 7302020.003 angezeigt. In der Liste „Warnungen“ wird dieser Wert als 7302 (Anzahl der Tausender) angezeigt.

Hinweis: Wenn Sie anwenderdefinierte Geschäftskritikalitätswerte haben, die sich von den vordefinierten Werten unterscheiden, fügen Sie der Tabelle „Zuordnungen der Warnungsprioritätskategorie“ [em_Alert_Priority_category_Mapping] einen Eintrag hinzu.

Auswirkung von Kategoriebegrenzungen

Durch Grenzwerte für Kategorien können sich Überlaufwerte auf die nächste Kategorie auswirken, die in der Prioritätsreihenfolge höher angeordnet ist. Jede aufgelaufene Kategorie hat ein vordefiniertes Limit. Wenn die Anzahl diesen Grenzwert überschreitet, wird 1 zur nächsthöheren Kategorie addiert. Wenn beispielsweise die Anzahl der CI-Typen den Grenzwert überschreitet, wird 1 zur nächsten Kategorie (Schweregrad) addiert, die eine höhere Priorität hat: `yyy-zzz` wird zu `yy (y + 1) - 000`.

In Liste „Alle Warnungen“ anzeigen

In der Liste **Alle Warnungen** wird die Warnungsprioritätspunktzahl in der Spalte **Priorität** angezeigt. Nur zu Anzeigezwecken wird die tatsächlich berechnete Warnungsprioritätspunktzahl durch 1000 geteilt, während in der Datenbank für Berechnungs- und Sortierzwecke der vollständige berechnete Wert verwendet wird.

Die detaillierte Berechnung der Warnungspriorität der ausgewählten Warnung wird auf der Registerkarte **Weitere Informationen** im Bereich **Prioritätsaufgliederung** angezeigt.

Berechnung der Warnungsprioritätspunktzahl

Die Berechnung der Warnungspriorität basiert auf allen Warnungen einer Gruppe und nicht nur auf der primären Warnung der Gruppe. Die Priorität wird für Warnungen berechnet, die diese Bedingungen erfüllen:

- Status ungleich **Geschlossen**
- Schweregrad ungleich **OK**

Warnungen, die zur Prioritätsberechnung in der Warteschlange stehen, werden in der Tabelle `em_alert_trigger_queue` aufgelistet. In der Tabelle „Geplante Aufgaben“ sind zwei Jobs für `Event Management - Warteschlangenpriorität Warnungen` vorhanden. Diese beiden Jobs können parallel ausgeführt werden. Sie können `Einfügen und bleiben` verwenden, um einen anderen Job zu erstellen. Der Job `Event Management - Warnungspriorität` wird einmal pro Minute ausgeführt und berechnet Prioritäten in Batches von 1000 offenen Warnungen. Es gibt mehrere Faktoren, die den Wert der Priorität einer Warnung bestimmen. Eine Änderung des Schweregrads löst eine sofortige Aktualisierung der Warnungsprioritätspunktzahl aus. In diesem Fall wird nur der Schweregradteil der Priorität geändert, zusammen mit den Schweregradinformationen im Bereich **Prioritätsaufgliederung** der Registerkarte **Weitere Informationen**.

Auslöser, die eine Neuberechnung auslösen

Auslöser, die eine Neuberechnung der Warnungsprioritätspunktzahl bewirken können, sind:

Liste der Auslöser für die Neuberechnung

Wiederholung	Auswirkung auf die Warnungsprioritätspunktzahl
Neue Warnung	Die Generierung einer neuen Warnung ist ein Auslöser für die Berechnung der Warnungsprioritätspunktzahl.
Vorhandene Warnung, die von „Geschlossen“ in einen anderen Status übergeht	Die Priorität wird für eine geschlossene Warnung nicht berechnet. Wenn der Warnungsstatus also von „Geschlossen“ in „Offen“, „Erneut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Auslöser für die Neuberechnung (Fortsetzung)

Wiederholung	Auswirkung auf die Warnungsprioritätspunktzahl
	öffnen“ oder „Fluktuierend“ geändert wird, ist diese Änderung ein Ausler fösür die Neuberechnung der Warnungsprioritätspunktzahl.
Rollenänderung zwischen primär, sekundär oder keine	Änderungen an der Rolle sind ein Auslöser für die Neuberechnung der Warnungsprioritätspunktzahl. Beispiel: • Eine Warnung, deren Typ in Primärgeändert wurde, löst eine Neuberechnung der Warnungsprioritätspunktzahl aus. • Eine Warnung, deren Typ in Keine geändert wurde, löst die Neuberechnung der Warnungsprioritätspunktzahl aus. • Eine Warnung, deren Typ in Sekundärgeändert wurde, löst eine Neuberechnung der Warnungsprioritätspunktzahl aus.
CI-Typ	Wenn ein CI an einen Alarm gebunden wird, ist diese Änderung ein Auslöser für die Neuberechnung der Alarmprioritätspunktzahl. Dieser Auslöser zur Neuberechnung der Priorität erfolgt nur einmal, wenn das CI an den Alarm gebunden ist.
Änderung der Anzahl sekundärer Warnungen	Eine Änderung der Anzahl sekundärer Warnungen löst eine Neuberechnung der Warnungsprioritätspunktzahl aus.
Schweregrad	Eine Änderung des Schweregrads löst eine Neuberechnung der Warnungsprioritätspunktzahl aus. Zum Beispiel löst die Änderung von OK zu Schwerwiegend eine Neuberechnung der Punktzahl aus. Im Gegensatz zu den anderen oben aufgeführten Auslösern löst eine Änderung des Schweregrads eine sofortige Aktualisierung des Schweregrads der Berechnung der Warnungsprioritätspunktzahl aus.

Warnungsprioritätspunktzahl ändern

Sie können die Wichtigkeit einiger Kategorien der Warnungspriorität ändern, indem Sie deren Reihenfolge und/oder Gewichtung wie unten beschrieben ändern. Beispiel: Wenn der CI-Typ eine höhere Bedeutung hat als die Anzahl der betroffenen Services, können Sie deren Reihenfolge ändern. Infolgedessen wird die Anzahl der Services jetzt mit 100 multipliziert, während der CI-Typ jetzt mit 1000000 multipliziert wird.

Hinweis: Durch die Änderungen, die Sie mit diesem erweiterten Verfahren vornehmen, ändert sich die Standardmethode zur Berechnung der Warnungsprioritätspunktzahl. Wenn diese konfigurierbaren Werte geändert werden, ändert sich bei Warnungen, die andernfalls möglicherweise keine hohe Punktzahl haben würden, möglicherweise die Reihenfolge, in der die Warnungen abgearbeitet werden.

Kategoriereihenfolge ändern

Navigieren Sie zur Tabelle *em_alert_priority_category_order*. In der Spalte **Reihenfolge** können Sie die Reihenfolge der erforderlichen Kategorie ändern.

Kategoriewertzuordnung

Die Tabelle *em_alert_priority_category_mapping* zeigt den Konfigurationswert für jede Kategorieauswahl. Jeder Wert in einer Dropdown-Liste von Kategorien kann durch Konfigurieren dieser Tabelle einem anderen Wert zugeordnet werden.

CI-Typ-Gewichtsfaktorzuordnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zur Tabelle *em_alert_priority_ci_type*. Sie können einen neuen CI zum Beispiel DualCoreCPU hinzufügen und in der Spalte **Priorität** die Priorität der gewünschten Kategorie ändern. Darüber hinaus können Sie den vorhandenen Typ bearbeiten und seinen Prioritätswert ändern. Diese Tabelle wird dazu verwendet, den Wert jedes CI-Typs zuzuordnen. Beispielsweise kann ein Mainframe mit CI_type: cmdb_ci_mainframe eine Priorität von 80 haben, während ein Server mit CI_type: cmdb_ci_server eine Priorität von 60 aufweisen könnte. Mit der Zuordnung können Sie die Priorität der verschiedenen CI-Typen anpassen.

Warnungszuweisungsgruppen für Teams

Warnungszuweisungsgruppen weisen den richtigen Teams schnell und automatisch Warnungen zu, wodurch die Incident-Management-Fähigkeiten insgesamt verbessert werden.

Administratoren bestimmen die Priorität der Warnungszuweisungsgruppe und stellen sicher, dass Warnungen an die entsprechenden Teammitglieder weitergeleitet werden.

Die Warnungszuweisungsgruppe wird durch bestimmt *evt_mgmt.alert_auto_assignment_field*Eigenschaftswert. Als Administrator können Sie die Zuweisungsgruppe basierend auf den Warnungsfeldern mithilfe des Eigenschaftswerts und der Reihenfolge der kommagetrennten Felder festlegen, indem Sie den Eigenschaftswert bearbeiten.

Zugehörige Informationen

Zuweisen der Priorität der Warnungszuweisungsgruppe

Teambasierte Integrationseigenschaften

Event-Regel erstellen oder bearbeiten

Event-Feldzuordnungen erstellen

Zuweisen der Priorität der Warnungszuweisungsgruppe

Weisen Sie Warnungszuweisungsgruppenvorrang zu, um sicherzustellen, dass Warnungen an die entsprechenden Teammitglieder weitergeleitet werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu **Alle** Und suchen Sie nach sys_properties.list .
2. In **Suchen** Feld eingeben evt_mgmt.Alert_Auto_assignment_field Und wählen Sie den Eigenschaftsdatensatz aus.
   Weitere Informationen zur Eigenschaft finden Sie unter Teambasierte Integrationseigenschaften.
3. In **Wert** Geben Sie die Priorität der Zuweisungsgruppe ein.
   Legen Sie den Vorrang der Zuweisungsgruppe gemäß der Reihenfolge der kommagetrennten Felder fest, z. B. cmdb_ci.Support_Group, IntegrationGroup.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Teambasierte Integrationseigenschaften

Wird Konfiguriert Express-Liste Ansichten für Anwender und Anwendergruppen

Steuern Sie zentral, was Anwender überwachen, indem Sie Ansichten in vordefinieren Express-Liste Und weisen Sie sie Anwendern und Anwendergruppen zu.

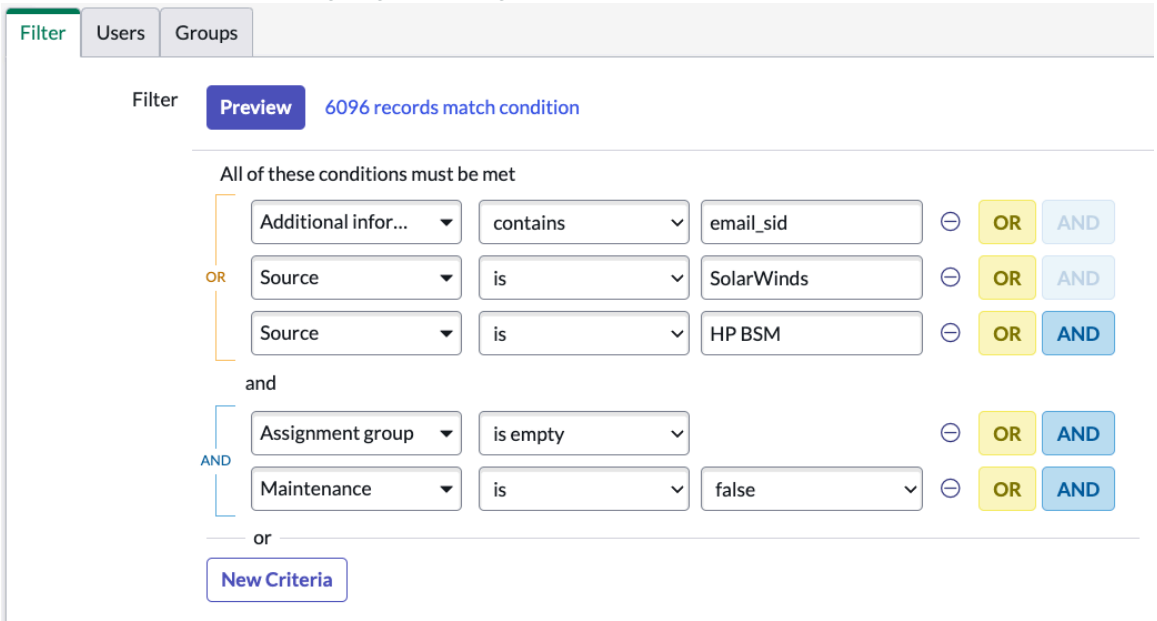
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Ereignismanagement administrator, können Sie erstellen Express-Liste Ansichten, um sicherzustellen, dass sich Anwender auf bestimmte Services, Prioritäten oder Warnungen konzentrieren. Mit Ereignismanagement können Sie die Filter, die Spaltenreihenfolge und die Filterattribute für definieren Express-Liste Zeigen Sie die Ansicht an, und weisen Sie sie einzelnen Anwendern und Anwendergruppen zu.

Anwender, die einer Gruppe angehören, können nur die vordefinierten Ansichten sehen, die Sie dieser Gruppe zugewiesen haben, und ihre eigenen gespeicherten Ansichten. Wenn ein Anwender mehreren Gruppen angehört, kann er die Ansichten sehen, die Sie allen diesen Gruppen zugewiesen haben. Anwender können zwischen Ansichten wechseln und alle Ansichten mit Ausnahme der zugewiesenen Standardansicht ändern und speichern. Sie können jedoch Einstellungen in keiner ihrer zugewiesenen Ansichten überschreiben und ihre Standardansicht ändern oder freigeben.

Mit dem Filterbedingungs-Generator können Sie UND und ODER Bedingungen zwischen Attributen konfigurieren.

Express-Liste Filterbedingungen anzeigen



Beispielsweise kann der Administrator Bedingungen konfigurieren, die es dem Anwender ermöglichen, nur Warnungen anzuzeigen, die keiner Zuweisungsgruppe zugewiesen sind oder in Wartung sind. Im Beispiel müssen die Warnungen auch den Wert email_sid enthalten und aus einer der angegebenen Quellen stammen.

Zugehörige Informationen

Erstellen Sie eine vordefinierte Express-Liste Ansicht für Anwender

Verwenden Sie einen zugewiesenen Express-Liste Anzeigen

Erstellen Sie eine vordefinierte Express-Liste Ansicht für Anwender

Konfigurieren Sie einen Express-Liste Zeigen Sie diese Ansicht an, damit Anwender sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren können. Sie können die Filter, die Spaltenreihenfolge und die Filterattribute für diese Ansicht festlegen und sie einzelnen Anwendern oder Anwendergruppen zuweisen.

Vorbereitungen

Für weitere Informationen zu vordefinierten Elementen Express-Liste Ansichten, siehe Wird Konfiguriert Express-Liste Ansichten für Anwender und Anwendergruppen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Express-Listenansichten**an.
2. Wählen Sie **Neu**.
3. Auf der **Express-Listenansicht** Füllen Sie die Felder aus.

Express-Liste Tabelle anzeigen

Feld	Beschreibung
Name	Eindeutiger Name von Express-Liste Anzeigen.
Primäres Feld „Sortieren nach“	Das Feld, nach dem sortiert werden soll Express-Liste. Standard: Generierungszeit des ersten Ereignisses.
Sekundäres Feld „Sortieren nach“	Das Feld, nach dem die Ergebnisse des primären Sortierfelds sortiert werden sollen. Dieses Feld ist optional.
Reihenfolge	Die Reihenfolge davon Express-Liste Anzeigen, wenn mehrere Ansichten vorhanden sind.
Reihenfolge des primären Felds „Sortieren nach“	Die Sortierreihenfolge des Felds „Primäres Sortieren nach“: Aufsteigend oder Absteigend.
Reihenfolge des sekundären Felds „Sortieren nach“	Die Sortierreihenfolge des Felds „Sekundär sortieren nach“, wenn festgelegt: Aufsteigend oder Absteigend.
Standard	Option zum Festlegen Express-Liste Ansicht als Standardansicht für den zugewiesenen Anwender oder die zugewiesene Gruppe. Wenn mehrere Standardansichten vorhanden sind, bestimmt der im Feld Reihenfolge festgelegte Wert deren Reihenfolge.

4. Legen Sie Filterbedingungen für fest Express-Liste Anzeigen.

Hinweis: Wenn Sie sogar einen einzelnen nicht unterstützten Filter in Ihren einschließen Express-Liste Anzeigen, wird verhindert Ereignismanagement Der Operator kann die Einstellungen aller Filter in dieser Ansicht ändern, einschließlich der unterstützten. Wenn Sie Operatoren erlauben möchten, ihre persönliche Ansicht anzupassen, achten Sie darauf, nur unterstützte Filter einzubeziehen.

a. In **Filter** Wählen Sie ein Feld, einen Operator und einen oder mehrere Werte für eine Bedingung aus.

Hinweis: Das Standardfeld ist Status.

b. **Wahlweise:** Führen Sie die folgenden Aufgaben aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Prozedur
Fügen Sie eine Filterbedingung hinzu	**i.** Wählen Sie entweder den Operator UND ODER ODER aus. **ii.** Wählen Sie ein Feld, einen Operator und einen oder mehrere Werte für die Bedingung aus.
Fügen Sie eine Warnungs-Tag-Filterbedingung hinzu	**i.** Wählen Sie im Abschnitt Filter für Warnungs-Tags die Option aus **Neue Zeile einfügen...** . **ii.** Wählen Sie das erforderliche Tag, den Operator und den Wert für jeden Tag-Filter aus.
Fügen Sie einen zusätzlichen Satz von Warnungs-Tag-Filterbedingungen hinzu	**i.** Wählen Sie im Abschnitt Filter für Warnungs-Tags die Option aus **Neue Kriterien** . **ii.** Fügen Sie die erforderlichen Tag-Filterbedingungen hinzu.
Zeigen Sie die Anzahl der Ergebnisse an, die eine Abfrage mit den konfigurierten Bedingungen zurückgeben würde	Wählen Sie **Vorschau**.

5. Weisen Sie Anwendern und Gruppen zu zu Express-Liste Anzeigen.

Aufgabe	Prozedur
Weisen Sie dem ausgewählten einen Anwender zu Express-Liste Anzeigen	**a.** In **Anwender** Wählen Sie die Registerkar–te aus **Neue Zeile einfügen...** . **b.** Wählen Sie das Suchsymbol ( ) Und suchen Sie im nach dem relevanten An–wender **Anwender** Tabelle. **c.** Wählen Sie den Anwender aus, und wäh–len Sie dann das Speichersymbol ( ).
Weisen Sie dem ausgewählten eine Anwender-gruppe zu Express-Liste Anzeigen	**a.** In **Gruppen** Wählen Sie die Registerkarte aus **Neue Zeile einfügen...** . **b.** Wählen Sie das Suchsymbol ( ) Und suchen Sie in nach der entsprechenden Gruppe **Gruppen** Tabelle. **c.** Wählen Sie die Gruppe aus, und wählen Sie dann das Speichersymbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Prozedur
	Hinweis: Anwender, die einer Gruppe angehören, können nur die Ansichten anzeigen, die Sie dieser Gruppe zugewiesen haben. Wenn ein Anwender mehreren Gruppen angehört, kann er die Ansichten sehen, die Sie für alle diese Gruppen konfiguriert haben.

6. Wählen Sie im Formularmenü die Option aus **Speichern** .
   Die folgenden Registerkarten werden angezeigt:
   - Die **Express-Listentabellenfelder** Auf der Registerkarte werden die Felder angezeigt, die als Tabellenspalten in angezeigt werden sollen Express-Liste.
   - Die **Feldattribute Der Express-Listenansicht** Auf der Registerkarte werden die Filterattribute für die offenen Warnungen in angezeigt Express-Liste.
7. **Wahlweise:** Fügen Sie Tabellenfelder und Feldattribute zu hinzu Express-Liste Anzeigen.

Aufgabe	Prozedur
Fügen Sie eine Spalte zu hinzu Express-Liste Tabelle	**a.** In **Express-Listentabellenfelder** Wählen Sie die Registerkarte aus **Neu** . **b.** Füllen Sie die Felder des Formulars aus. ▪ Feld: Die hinzuzufügende Spalte. ▪ Express-Liste Ansicht: Der Name der Ansicht, der die Spalte hinzugefügt werden soll. ▪ Mindestbreite: Mindestbreite der Spalte . ▪ Reihenfolge: Die Position der Spalte in der Tabelle. ▪ Aktiv: Option zum Aktivieren der Spalte. **c.** Wählen Sie **Absenden**.
Fügen Sie dem Filterbereich in ein Attribut hinzu Express-Liste	**a.** In **Feldattribute Der Express-Listenansicht** Wählen Sie die Registerkarte aus **Neu** . **b.** Füllen Sie die Felder des Formulars aus. **i.** Feld: Das Attribut, das dem Filterbereich hinzugefügt werden soll. **ii.** Express-Liste Ansicht: Der Name der Ansicht, der das Attribut hinzugefügt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Prozedur
	iii. Reihenfolge: Die Position des Attributs im Bereich. **iv.** Aktiv: Option zum Aktivieren des Attributs. **c.** Wählen Sie **Absenden**.

8. **Wahlweise:** Felder oder Feldattribute aus dem ausschließen Express-Liste Zeigen Sie an, indem Sie sie deaktivieren.

Aufgabe	Prozedur
Deaktivieren Sie ein Feld	**a.** In **Express-Listentabellenfelder** Wählen Sie das Informationssymbol (ⓘ) Links neben einem Felddatensatz. **b.** Löschen Sie im Feldformular **Aktiv** . **c.** Wählen Sie **Aktualisieren**.
Deaktivieren Sie ein Feldattribut	**a.** In **Feldattribute Der Express-Listenansicht** Wählen Sie das Informationssymbol (ⓘ) Links neben einem Feldattribut-Datensatz. **b.** Löschen Sie im Feldformular **Aktiv** . **c.** Wählen Sie **Aktualisieren**.

Hinweis: Sie können den aktualisierten Status eines Felds oder eines Feldattributs in der Tabelle anzeigen, indem Sie das Symbol für Listensteuerungen (≡) Und dann auswählen **Aktualisieren Sie Die Liste** .

9. Wenn Sie mit zufrieden sind Express-Liste Anzeigen, auswählen **Aktualisieren** .

Weisen Sie vordefinierten Anwendern und Gruppen zu Express-Liste Ansichten

Weisen Sie einzelne Anwender und Anwendergruppen vorkonfiguriert zu Express-Liste Ansichten, um sicherzustellen, dass sie sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren.

Vorbereitungen

Für weitere Informationen zu vordefinierten Elementen Express-Liste Ansichten, siehe Wird Konfiguriert Express-Liste Ansichten für Anwender und Anwendergruppen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Express-Listenansichten**an.
2. Wählen Sie die vordefinierte aus Express-Liste Ansicht, die Sie einem Anwender oder einer Gruppe zuweisen möchten.
3. Weisen Sie dem ausgewählten Anwender oder Gruppen zu Express-Liste Anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Prozedur
Weisen Sie dem ausgewählten einen Anwender zu Express-Liste Anzeigen	**a.** In **Anwender** Wählen Sie die Registerkarte aus **Neue Zeile einfügen...** . **b.** Wählen Sie das Suchsymbol ( ) Und suchen Sie im nach dem relevanten Anwender **Anwender** Tabelle. **c.** Wählen Sie den Anwender aus, und wählen Sie dann das Speichersymbol ( ).
Weisen Sie dem ausgewählten eine Anwendergruppe zu Express-Liste Anzeigen	**a.** In **Gruppen** Wählen Sie die Registerkarte aus **Neue Zeile einfügen...** . **b.** Wählen Sie das Suchsymbol ( ) Und suchen Sie in nach der entsprechenden Gruppe **Gruppen** Tabelle. **c.** Wählen Sie die Gruppe aus, und wählen Sie dann das Speichersymbol ( ). **Hinweis:** Anwender, die einer Gruppe angehören, können nur die vordefinierten Ansichten sehen, die Sie dieser Gruppe zugewiesen haben, und ihre eigenen gespeicherten Ansichten. Wenn Anwender mehreren Gruppen angehören, können sie die Ansichten sehen, die Sie allen diesen Gruppen zugewiesen haben.

4. Wählen Sie **Aktualisieren**.

Warnungsauswirkungsberechnung

Die Auswirkungsberechnung zeigt das Ausmaß eines Ausfalls von CIs, Services, Warnungen und Warnungsgruppen an. Vom System werden Faktoren wie Auswirkungsregeln und CI-Beziehungen zur Berechnung des Schweregrads einer generierten Warnung verwendet. Der Schweregrad wird in der Auswirkungsstruktur, den Anwendungsservices-Zuordnungen und Dashboards angezeigt.

Auswirkungsberechnungen sind für Anwendungsservices-Warnungsgruppen verfügbar. Die folgenden Faktoren werden zur Berechnung der Gesamtauswirkung eines Ausfalls verwendet.

- Auswirkungsregeln
- Anzahl der zugehörigen aktiven Warnungen.
- Vergangener Verlauf des betroffenen CI.
- Beziehungen zwischen CIs für einen bestimmten Anwendungsservice oder Anwendungsservices.
- Wenn das CI-Element ein Netzwerk oder Speichergeräte enthält.
- Warnungen zu CIs in der Wartungsphase werden aus der Auswirkungsberechnung ausgeschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

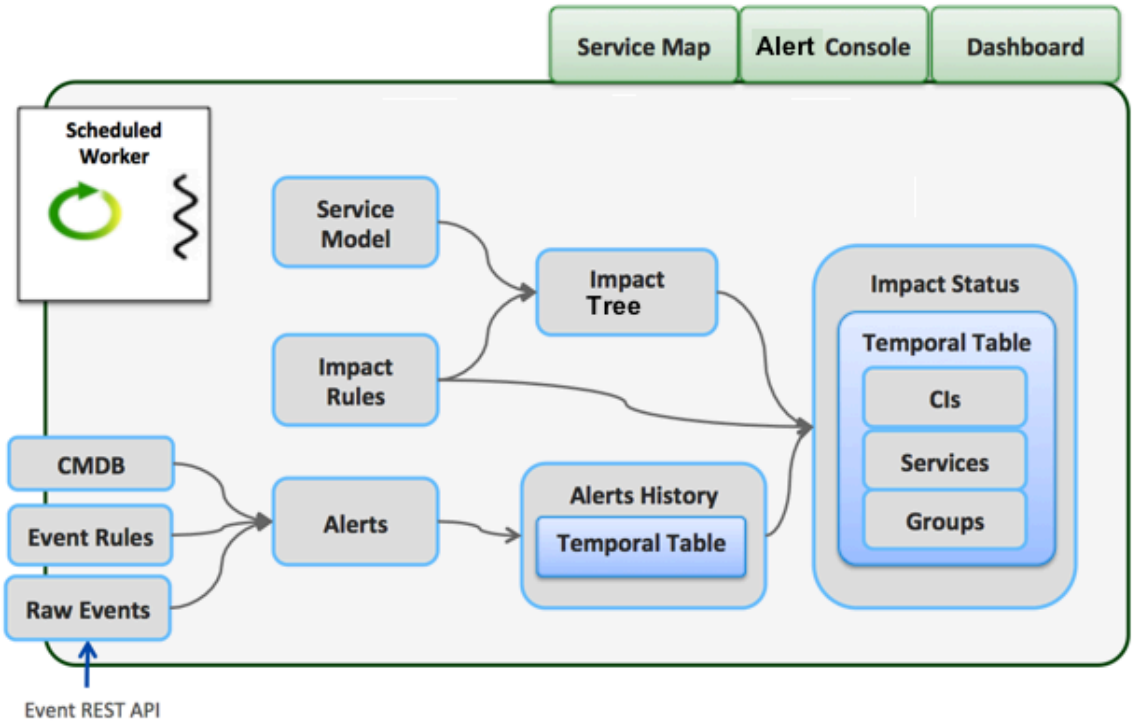
Hinweis:

- CIs gelten nicht nur dann als in Wartung, wenn eine aktive Change-Anforderung geplant ist, sondern auch, wenn das **Statusfeld** des CIs auf **In Wartung** gesetzt ist.
- Wenn ein untergeordnetes CI in Wartung gesetzt wird, wird auch das übergeordnete CI in Wartung gesetzt.

- Standardmäßig wird die Auswirkung für alle operativen Anwendungsservices berechnet. Mit dem System können Sie jedoch die Auswirkungsberechnung nach Serviceklasse oder einzelnen Anwendungsservice filtern. Weitere Informationen finden Sie unter Hinzufügen CMDB Tabellen oder Klassen für die Berechnung der Auswirkung und Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

Wenn eine Verbindung zwischen Services besteht, werden auch die Auswirkungen eines Services auf den anderen berechnet.

Auswirkungsberechnungen verwenden Informationen aus verschiedenen Quellen, um den Schweregrad der Warnung festzulegen.



Berechnung der Auswirkung

Die Berechnung der Auswirkung hängt von den CI-Beziehungen für einen Anwendungsservice oder Anwendungsservices ab. Zusätzliche Faktoren wie Change-Anforderungen, Netzwerkpfade, Speicherpfade und zugehörige CIs wirken sich auf die Auswirkungsberechnung aus.

Services

Der folgende Flow für die Auswirkungsberechnung wird für Warnungen ausgeführt, bei denen der Ausfall kein Netzwerk oder keinen Netzwerkspeicher betrifft. Ereignismanagement führt die folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Erstellen einer Servicezuordnung Verwenden Sie die Tabellen „Zuordnungen von Servicekonfigurationselementen“ [svc_ci_assoc] und „CI-Beziehungen“ [cmdb_rel_ci], um untergeordnete und übergeordnete Beziehungen im Anwendungsservice oder den Anwendungsservices zu erstellen.
2. Wenn kein CMDB-Pfad vom Service zum CI vorhanden ist, aber in der Tabelle „svc_ci_assoc“ eine Zuordnung angezeigt wird, zeigen Sie eine Abhängigkeitsbeziehung zwischen dem Anwendungsservice und dem CI an. Andernfalls zeigen Sie keine Verbindung an.
3. Wenn für Anwendungsservices die dem Service zugewiesenen CIs auch mit dem Service in der CMDB verbunden sind, behält die Zuordnung die Hierarchie zwischen CIs so bei, wie sie in der CMDB angezeigt werden. Die CI-Servicezuweisungen werden im Abschnitt Anwendungsservice für Servicekonfigurationselemente angezeigt. Wenn in der CMDB keine Verbindung zum Service besteht, werden die CIs direkt unter den Anwendungsservices in der Zuordnung angezeigt.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Change-Anforderungen und der Status „In Wartung“

Ob eine aktive Change-Anforderung für das CI geplant ist oder ob **Installationsstatus** Des CI ist **In Wartung** , Alle Warnungen für das betroffene CI werden von der Berechnung der Auswirkung ausgeschlossen. Auf der Registerkarte „Warnungen“ werden alle entsprechenden Warnungen vorübergehend ebenfalls ausgeblendet. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. Die Auswirkungsstruktur und die Servicezuordnung zeigen CIs vorübergehend grün an.

Hinweis:

- CIs gelten nicht nur dann als in Wartung, wenn eine aktive Change-Anforderung geplant ist, sondern auch, wenn das **Statusfeld** des CIs auf **In Wartung** gesetzt ist.
- Wenn ein untergeordnetes CI in Wartung gesetzt wird, wird auch das übergeordnete CI in Wartung gesetzt.

Für einen Service werden alle Warnungen bezüglich CIs im Service auch auf der Registerkarte „Warnungen“ ausgeblendet. Der gesamte Service wird im Auswirkungsbaum in Grün angezeigt. Für einen Host mit einer aktiven Change-Anforderung werden die Host-Applikationen als eine Einheit betrachtet. Alle untergeordneten Anwendungen werden, bis die Change-Anforderung nicht mehr aktiv ist, so behandelt wie der Host. Weitere Informationen finden Sie unter Funktionsweise von Warnungen mit CIs in der Wartung.

Netzwerkpfade

Zur Berücksichtigung der Netzwerkredundanz verwendet Ereignismanagement eine separate Auswirkungsberechnung. Sie können Netzwerktopologie oder Pfadänderungen im Anwendungsservice anzeigen. Der folgende Flow für die Auswirkungsberechnung wird für Warnungen ausgeführt, bei denen der Ausfall einen Netzwerkpfad betrifft. Ereignismanagement führt die folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Erstellen Sie eine Anwendungsservicezuordnung für das betroffene Netzwerk.
   - Verwenden Sie die Host-ID und die Ziel-IP-Informationen aus der Warnung und den Netzwerkpfad aus der Tabelle „Netzwerkpfade“ [sa_network_paths].
   - Verwenden Sie die Elemente im Netzwerkpfad, die von der Configuration Item-Tabelle [cmdb_ci] abgeleitet sind. Verwenden Sie auch die Elemente, die dem Pfad zugeordnet sind, aus der Tabelle „Infra-Pfad zu Elementen“ [sa_infra_path_assoc].
   - Legen Sie Beziehungen fest. Das Anwendungs-CI weist die Beziehung „Abhängig von::Verwendet von“ für ein Element im Pfad auf, das in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] definiert ist. In der Beziehung ist das Anwendungs-CI das übergeordnete Element und das Element im Netzwerkpfad das untergeordnete Element.
2. Berechnen Sie einen separaten Schweregrad für jedes reguläre Element im Pfad. Jedes reguläre Element im Pfad fügt seinen eigenen Schweregrad zu seinen Vorfahren bis zum Anwendungs-CI hinzu, von dem der Pfad stammt.
3. Berechnen Sie alle redundanten Elemente im Pfad mit der Redundanzregel, indem Sie den Schweregrad der betroffenen CIs um eine Ebene reduzieren. Beispiel: Wenn der Schweregrad `Critical` ist, verringert die Redundanzregel den Schweregrad um eine Ebene auf `Major`.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Speicherpfade

Zur Berücksichtigung der Netzwerkredundanz verwendet Ereignismanagement eine separate Auswirkungsberechnung. Sie können Aktualisierungen der Auswirkungsstruktur anzeigen, wenn sich die Netzwerkspeichertopologie vom Anwendungsservice ändert. Ereignismanagement Führt die folgenden Schritte für Warnungen aus, die Speicher-CIs enthalten:

1. Erstellen Sie eine Anwendungsservicezuordnung für das betroffene Speichergerät:
   - Verwenden Sie das Speichergerät in der Tabelle „sa_fs_to_storage_path“. Die Speichergerätedefinition verwendet die Dateisysteminformationen im Pfad.
   - Verwenden Sie die Elemente im Netzwerkpfad, die von der Configuration Item-Tabelle [cmdb_ci] abgeleitet sind. Verwenden Sie auch die Elemente, die dem Pfad aus der Tabelle „Infra-Pfad zu Elementen“ [sa_infra_path_assoc] zugeordnet sind.
   - Legen Sie Beziehungen fest. Das Anwendungs-CI weist die Beziehung „Abhängig von::Verwendet von“ für ein Element im Pfad auf, das in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] definiert ist. In der Beziehung ist das Anwendungs-CI das übergeordnete Element und das Element im Speicherpfad das untergeordnete Element.
2. Berechnen Sie einen separaten Schweregrad für jedes reguläre Element im Pfad. Jedes reguläre Element im Pfad fügt seinen eigenen Schweregrad zu seinen Vorfahren bis zum Original-Anwendungs-CI des Pfads hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Berechnen Sie redundante Elemente im Pfad mit der Redundanzregel, indem Sie den Schweregrad der betroffenen CIs um eine Ebene reduzieren. Beispiel: Wenn der Schweregrad `Critical` ist, verringert die Redundanzregel den Schweregrad um eine Ebene auf `Major`.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Zugehörige CIs

Während Warnungen für ein CI generiert werden, werden zusätzliche Auswirkungsberechnungen für zugehörige CIs ausgeführt. Beispielsweise werden zusätzliche Auswirkungsberechnungen für eine Abhängigkeit des Anwendungsservice von einem CI ausgeführt, das nicht tatsächlich Teil des Anwendungsservice ist. Diese zugehörigen CIs werden nicht als Teil des Services erkannt. Stattdessen werden die zugehörigen CIs durch Definition einer Infrastrukturbeziehung angegeben.

Der folgende Flow zur Auswirkungsberechnung wird für Warnungen mit CIs ausgeführt, die eine Abhängigkeit von zugehörigen CIs haben, die außerhalb des Anwendungsservice betrachtet werden. Ereignismanagement Führt die folgenden Schritte aus:

1. Leiten Sie Beziehungen zwischen den Anwendungsservice-CIs und zugehörigen CIs ab. Verwenden Sie Beziehungen, Auswirkungsregeln und andere Daten aus der Tabelle „Infrastrukturbeziehungen“ [em_impact_infra_rel_def].
2. Fügen Sie der Auswirkungsstruktur und der Warnungsliste im Dashboard Ereignismanagement zugehörige CIs hinzu.
   - Verwenden Sie Daten aus der Tabelle „Infrastrukturbeziehung“ [em_impact_infra_rel_def], um Containment-Links zum Host anzuzeigen.
   - Verwenden Sie die Tabellen „Auswirkungsstatus“ [em_impact_status] und „Warnungsverlauf“ [em_alert_history], um den Status zu bestimmen.

Auswirkungsregeln

Auswirkungsregeln, die für die Auswirkungsberechnung verwendet werden, schätzen den Umfang oder den Schweregrad eines Ausfalls basierend auf betroffenen CIs.

Die Tabelle „Auswirkungsregel“ [em_Impact_rule] enthält Auswirkungsregeln, die die anwendbaren CIs, Anwendungsservices und Einstellungen für Impact anzeigen. Die folgenden Standardauswirkungsregeln sind verfügbar.

Mitglied in Anwendungscluster

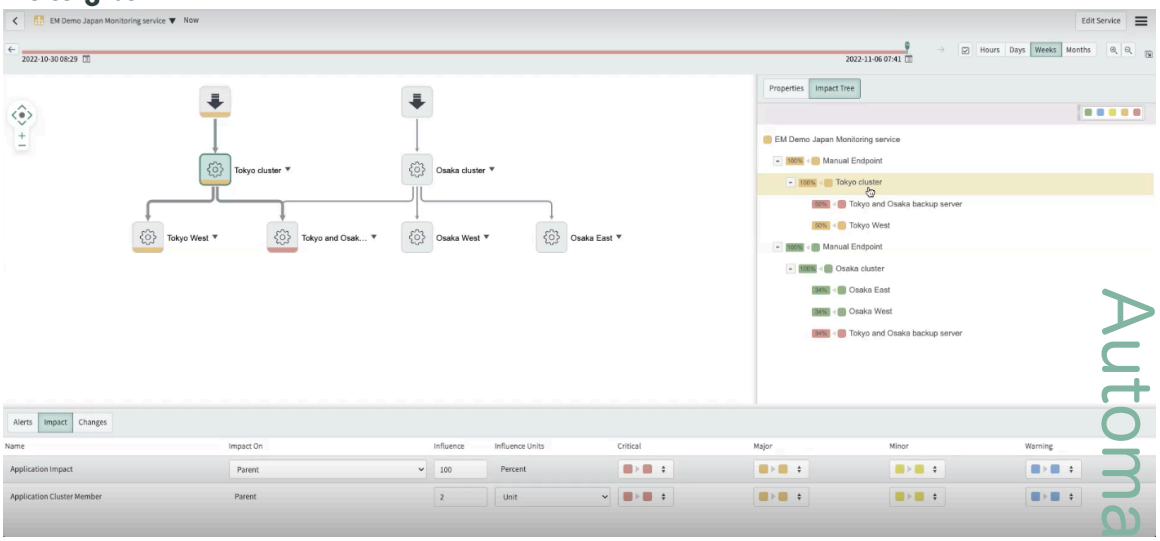
Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Mitgliedern erfordert **90 % Einfluss** Um den Schweregrad für den gesamten Cluster auf festzulegen **Schwerwiegend** , Hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen.

Sie können verschiedene Auswirkungsregeln pro Cluster konfigurieren, sodass die Weitergabe der Auswirkungen des untergeordneten CI an das übergeordnete CI (für dasselbe untergeordnete CI) unterschiedlich ist. Daher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie manuell Gruppen von CIs (auch als manuelle Cluster bezeichnet) erstellen und die Auswirkungsregel auf Clusterebene für nachgelagerte untergeordnete Cluster-Elemente konfigurieren.

Beispiel, in dem dasselbe untergeordnete CI seine Auswirkung auf seinen übergeordneten Cluster für jeden Cluster unterschiedlich weitergibt



Im obigen Beispiel gibt es zwei Einstiegspunkte. Der Osaka-Cluster auf der rechten Seite hat drei CIs. Der Tokyo-Cluster auf der linken Seite hat zwei CIs. Der Sicherungsserver Tokio und Osaka hat gemeinsam genutzte übergeordnete Elemente – Tokyo-Cluster und Osaka-Cluster. Im rechten Bereich sehen Sie die Auswirkungsstruktur, in der der Tokyo-Cluster zwei Anwendungsclustermitglieder mit jeweils 50 % Einfluss und der Osaka-Cluster drei mit jeweils 34 % Einfluss hat.

Für die manuelle Clusterkonfiguration gibt es zwei Zeilen: Anwendungsauswirkung und Anwendungsclustermitglied. Die untergeordneten Elemente werden angezeigt, da das Feld Auswirkung auf als übergeordnetes Element und nicht als Anwendungsservice ausgewählt wurde. In der Zeile Anwendungsclustermitglied ist das Feld Einfluss auf zwei konfiguriert. Dies bedeutet, dass die Mindestanzahl der fehlgeschlagenen untergeordneten Elemente (und dass sie den Fehler an ihre übergeordneten Elemente weitergeben) zwei sind. Der Osaka-Cluster ist auf drei konfiguriert. Der Prozentsatz unterscheidet sich für den Sicherungsserver Tokio und Osaka für jeden Cluster (50 % und 34 %). Wie Sie sehen, wirkt sich der Ausfall des Sicherungsservers in Tokio und Osaka auf die übergeordneten Elemente unterschiedlich aus. Der Osaka-Cluster bleibt grün, auch wenn der Tokio-Clusterfehler Orange schwerwiegend ist.

Klicken Sie auf einen Service oder ein CI, um die zugehörigen Warnungen anzuzeigen. Wenn Sie beispielsweise auf den allgemeinen Anwendungsservice klicken, werden die ihm zugeordneten Warnungen im Warnungsbereich unter der Kartenansicht angezeigt, wenn Sie auswählen **Warnungen** . Die aufgeführten Warnungen beziehen sich auf den ausgewählten Service. Warnungen von untergeordneten Services werden aufgelistet, wenn diese Services ausgewählt werden.

Die folgenden Auswirkungsfelder werden angezeigt, wenn Sie auswählen **Auswirkung** .

Einschluss

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt.

Infrastrukturabhängigkeiten

Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen.

CI-Anwendungsservice

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Anwendungsservices sind.

CI-Auswirkung

Gilt für Anwendungsservices. Bestimmung der Beziehung zwischen Servicemitgliedern. Die Auswirkung von untergeordneten auf übergeordnete CIs ist immer 100 %. Zum Beispiel wird der Schweregrad der Auswirkungen auf die übergeordnete Ebene vom untergeordneten CI mit dem höchsten Schweregrad abgeleitet.

Übergeordnetes CI in Anwendung

Auswirkungen werden nur für die übergeordnete Entität festgelegt.

Netzwerkpfad

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind.

Mitglied in OS-Cluster

Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Hosts erfordert **60 % Einfluss** Zum Festlegen des Schweregrads von **Schwerwiegend** , Hat jedes Mitglied **20 % Einfluss** (60 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv.

Speicherpfad

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind.

Eigenschaften

Neben Auswirkungsregeln können Sie Eigenschaften für die Auswirkungsberechnung konfigurieren.

Konfigurieren Sie diese Eigenschaften nach Bedarf:

Eigenschaften der Auswirkungsberechnung

Eigenschaftsname	Beschreibung
evt_mgmt.impact_calculation.alert_group_support	Aktiviert die Unterstützung von Warnungsgruppen
evt_mgmt.impact_maintenance.sleep_time_sec	Mindestzeit in Sekunden für die Überprüfung der CI-Wartung: überprüft sowohl das Feld „Status“ des CI als auch alle Change-Anforderungszeitpläne für das CI
evt_mgmt.impact_calculation.alert_copy_delay	Die Verzögerung nach dem Erstellen oder Aktualisieren einer Warnung, bevor sie für die Auswirkungsberechnung und -gruppierung verwendet wird. Wird dazu verwendet, verspätete Eingänge oder langsame Geschäftsregeln zu kompensieren, die in der Tabelle em_alert definiert sind. Standard = 2000 ms.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Auswirkungsberechnung (Fortsetzung)

Eigenschaftsname	Beschreibung
	Wird verwendet, wenn Warnungen und Events nacheinander verarbeitet werden (wenn die Eigenschaft evt_mgmt.max_objs_in_alert_query nicht definiert oder auf **1** festgelegt ist)
evt_mgmt.impact_calculation.alert_copy_delay_when_alerts_are_processed_in_batch	Die Verzögerung, nachdem Ereignisse in Batches Aktualisieren einer Warnung, bevor sie für die Auswirkungsberechnung und -gruppierung verwendet wird. Wird dazu verwendet, verspätete Eingänge oder langsame Geschäftsregeln zu kompensieren, die in der Tabelle em_alert definiert sind. Standard = 30000 ms. Wird in großen Kundenumgebungen mit hohem Datenverkehr verwendet, wenn Warnungen und Ereignisse in Batches verarbeitet werden (wenn) evt_mgmt.max_objs_in_Alert_query Eigenschaft ist auf einen Wert größer als festgelegt **1**).

Weitere Informationen finden Sie unter Ereignismanagement – Auswirkungsberechnung [KB1157218] .

Servicezuordnungen verstehen

Servicezuordnungen zeigen aktive Warnungen für CIs und die Beziehungen zwischen CIs an. Durch das Anzeigen dieser Informationen können Sie die Quelle von Warnungen besser verstehen und Abhilfemaßnahmen ergreifen. Die Servicezuordnung ist für alle Anwendungsservices verfügbar.

Über Servicezuordnungen

Eine Servicezuordnung zeigt Warnungen mit betroffenen CIs und CI-Abhängigkeiten an. Beispielsweise werden Änderungen an einer Verbindung zwischen einem Host und einem Hypervisor auf der Servicezuordnung angezeigt. Wenn sich Definitionen von Servicezuordnungen ändern, werden Servicezuordnung, Warnung und Auswirkungsinformationen entsprechend aktualisiert. Seit Release Quebec wurde die Transparenz erhöht. Wenn die Warnung an den Einstiegspunkt gebunden ist, identifiziert die Servicezuordnung ein Problem am Einstiegspunkt.

Hinweis: Warnungen werden für die Einstiegspunkte in der Servicezuordnung nicht angezeigt.

Sie können eine Servicezuordnung über diese Orte öffnen:

- In der Liste Anwendungsservices können Sie Servicezuordnungen für Anwendungsservices anzeigen.
- In der Liste „Überwachte Services“ können Sie Servicezuordnungen für überwachte Services anzeigen.

Die folgenden Symbole werden in Servicezuordnungen verwendet. Die Symbolformen unterscheiden sich für Anwendungsservices geringfügig.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbole der Servicezuordnung

Symbol	Beschreibung
( )	Stellt Anwendungen wie Microsoft IIS- oder SQL-Server dar
( )	Stellt physische sowie virtuelle VM-Computer und -Server dar
( )	Stellt den Startpunkt des Netzwerks dar. Beispielsweise werden Layer-3-Geräte oben auf der Zuordnung angezeigt, und verbundene Software und Services werden am Ende der Zuordnung angezeigt.
( )	Zeigt die Anzahl der redundanten CIs an
( )	Zeigt die Arbeitsauslastung zwischen Computern an.
( )	Der graue Connector zeigt eine Beziehung zwischen CIs an.
()	Jedes CI ohne aktives Warnungsfeld stellt ein Netzwerk-CI dar. Ein graues Feld stellt ein CI ohne aktive Warnungen dar. Informationen zum CI sind ausgeblendet.
( )	Blendet mehrere CIs aus, die als redundant gekennzeichnet sind
( )	Ein betroffenes CI zeigt die Farbe an, die den Schweregrad des dem CI zugeordneten Alarms darstellt. • **Kritisch (rot)**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. • **Schwerwiegend (orange)**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. • **Geringfügig (gelb)**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. • **Warnung (blau)**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. • **OK (grün)**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. • **Keine Farbe**: Keine aktiven Warnungen.
( )	Stellt Fiber Channel, Festplatten oder andere Datenspeichergeräte dar
( )	Stellt zugehörige Webservices für das Netzwerk dar, z. B. NGINX- oder JBoss-Webserver.

Hinweis: Einstellungen für Sitzungszeitüberschreitungen gelten nicht für diesen Bildschirm. Die Sitzung bleibt verbunden, auch wenn keine menschliche Interaktion stattfindet. Wenn diese Einstellung ein Problem darstellt, melden Sie sich entweder ab oder schließen die aktive Registerkarte im Browser.

Zugehörige Informationen

Warnungsauswirkungsberechnung

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen der Auswirkungsstruktur

Die Auswirkungsstruktur zeigt die Beziehungen zwischen CIs und die relative prozentuale Auswirkung für jedes untergeordnete CI an. Diese Informationen sind sowohl für erkannte Services als auch für Anwendungsservices verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

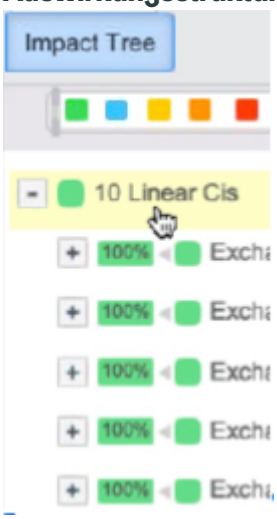
Die Auswirkungsstruktur zeigt das Ergebnis von Auswirkungsregeln für über- und untergeordnete CI-Beziehungen. Die Struktur stellt eine Servicezuordnung mit CIs aus der Zuordnung von Servicekonfigurationselementen [svc_ci_assoc] dar. Wenn zugehörige CIs verbunden, aber nicht Teil der Servicezuordnung sind, kann die Auswirkung für die zugehörigen CIs auch in der Auswirkungsstruktur angezeigt werden.

Die Zahlen oder Prozentsätze in einem übergeordneten CI fassen den Gesamtschweregrad basierend auf Warnungen von untergeordneten CIs zusammen. Der übergeordnete Schweregrad basiert auf Auswirkungsregelberechnungen.

Im folgenden Video-Tutorial erfahren Sie mehr über Auswirkungsstrukturen.

Ereignismanagement Teil 2 | Auswirkungsstruktur

Auswirkungsstruktur



Prozedur

1. Öffnen Sie die Servicezuordnung für den Service aus der Liste Anwendungsservice.
   a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**an.
   b. Klicken Sie Auf **Service anzeigen** Neben dem Service.
2. Klicken Sie auf der Servicezuordnung auf ein CI mit einer Farbe des Schweregrads.
3. Klicken Sie auf die Registerkarte **Auswirkung**.
4. Erweitern Sie auf der Registerkarte **Auswirkungsstruktur** im Seitenbereich das übergeordnete CI, und klicken Sie auf das CI, das Warnungen generiert hat.
5. Verwenden Sie die Farbe des Schweregrads, um CIs zu finden, die Warnungen enthalten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kritisch (rot)**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.
- **Schwerwiegend (orange)**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.
- **Geringfügig (gelb)**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten.
- **Warnung (blau)**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist.
- **OK (grün)**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.

6. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Bezeichnung
Anpassen der Auswirkungsregeln	**a.** Klicken Sie auf die Registerkarte **Auswirkung**. **b.** Überprüfen Sie die Auswirkungsregeln, und passen Sie sie bei Bedarf an.
Nachbesserung einer Warnung	**a.** Klicken Sie auf die **Warnungen**. **b.** Klicken Sie mit der rechten Maustaste auf die Warnung, und wählen Sie **Korrektur ausführen** aus.

Netzwerkpfade, die in der Auswirkungsstruktur angezeigt werden, können eine große Menge an Ressourcen verbrauchen, was die Systemleistung beeinträchtigt. Um zu deaktivieren, dass Netzwerkpfade in der Auswirkungsstruktur angezeigt werden, navigieren Sie zu **Systemeigenschaften** > **Alle Eigenschaften** Und legen Sie fest *evt_mgmt.network_path_excluded*Eigenschaft bis **Wahr** .

Dient zum Anzeigen der Auswirkungsstruktur mit Service Operations-Arbeitsbereich, Siehe Zeigen Sie die Auswirkungsstruktur mit an Service Operations-Arbeitsbereichan.

Anpassen der Auswirkungsregeln für ein CI

Konfigurieren Sie Auswirkungsregeln, um die Auswirkungsberechnung anzupassen Für Discovery-Services und manuelle Services . Die Auswirkungsregeln aktualisieren die allgemeine Warnung und zeigen die Auswirkung auf zugehörige CIs an. Wenn Sie Auswirkungsregeln ändern, gelten die Updates für den Schweregrad von Warnungen an Stellen wie dem Dashboard Ereignismanagement und dem Betreiber-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Auswirkungsregeln von CIs über anzeigen und anpassen Anwendungsservice Zuordnung eines Service.

Hinweis: Das Ereignismanagement-Dashboard wird für neue Instanzen im Paris-Release nicht unterstützt. Instanzen, die von einem Release vor Orlando aktualisiert wurden und das Ereignismanagement Dashboard verwenden, können dies jedoch weiterhin tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Anwendungsservicezuordnung entweder über das Dashboard Ereignismanagement oder über die Liste Anwendungsservice.

Option	Bezeichnung
Über das Ereignismanagement-Dashboard	**a.** Navigieren zu **Ereignismanagement** > **Dashboard**an. **b.** Doppelklicken Sie auf die Kachel der Anwendungsservices.
Über die Liste Anwendungsservice	**a.** Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**an. **b.** Klicken Sie Auf **Karte Anzeigen** Neben den Anwendungsservices.

2. Klicken Sie in der Anwendungsservicezuordnung auf ein CI.
3. Klicken Sie unterhalb der Karte auf die Registerkarte **Auswirkung**, und passen Sie dann die Auswirkungsregeln entsprechend an.

Auswirkungsregeln

Feld	Beschreibung
Name	Der Name der Auswirkungsregel. ○ **Anwendungsclustermitglied**: Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Mitgliedern erfordert **90 % Einfluss** Um den Schweregrad für den gesamten Cluster auf festzulegen **Schwerwiegend** , Hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen. **Hinweis:** Informationen zum Konfigurieren eines manuellen Clusters finden Sie unter Konfigurieren Sie einen manuellen Cluster ○ **Auswirkung Auf Die Anwendung** : Bestimmt, wie die Auswirkung auf ein bestimmtes CI, den allgemeinen Anwendungsservice oder übergeordnete/untergeordnete Entitäten innerhalb eines Anwendungsservice angewendet wird. Für die Anwendungsauswirkungsregel können Sie aus den folgenden Auswirkungsoptionen auswählen: **Anwendungsservice** Oder **Übergeordnet** . ▪ Wenn kein CI ausgewählt ist, gilt die Warnungsregel für den gesamten Anwendungsservice. ▪ Wenn Sie ein bestimmtes CI auswählen, können Sie definieren, ob die Regel für den Service oder sein übergeordnetes Element gilt. ○ **Übergeordnetes CI in Anwendung**: Auswirkungen werden nur für die übergeordnete Entität festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Inclusion**: Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt. ○ **Infrastrukturabhängigkeiten**: Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen. ○ **Netzwerkpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind. ○ **Mitglied in OS-Cluster**: Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Hosts erfordert **60 % Einfluss** Zum Festlegen des Schweregrads von **Schwerwiegend** , Hat jedes Mitglied **20 % Einfluss** (60 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv. ○ **Speicherpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind.
Auswirkung auf	Der gültige Servicetyp für diese Auswirkungsregel. ○ **Anwendungsservice** : Die Auswirkungsregel gilt für Anwendungsservice . ○ **Übergeordnet**: Die Auswirkungsregel gilt für das übergeordnete CI.
Einfluss	Der Wert, der die Festlegung der Auswirkungsregel für das übergeordnete Element zulässt. Legen Sie einen Wert für das übergeordnete Element fest. Dieses Feld arbeitet mit dem Feld **Einflusseinheiten** zusammen.
Einflusseinheiten	Die Maßeinheit, die die Auswirkung auf das übergeordnete Element anzeigt. Legen Sie den höchsten Wert für das übergeordnete CI fest. Legen Sie niedrigere Werte für jedes untergeordnete CI fest. Wenn Warnungen für mehrere untergeordnete CIs auftreten, berechnet Ereignismanagement die Summe der **Einflusseinheiten** für jedes untergeordnete Element. Wenn die Summe den übergeordneten **Einflusseinheitswert** überschreitet, erhält das übergeordnete Element den höchsten Schweregrad im Satz. Dieses Feld arbeitet mit dem Feld **Einfluss** zusammen. ○ **Prozent**: Wenn der Prozentsatz den **Einflusswert** überschreitet, wenden Sie die Auswirkung auf das übergeordnete Element an. ○ **Nummer**: Wenn die Nummer den **Einflusswert** überschreitet, wenden Sie die Auswirkung auf das übergeordnete Element an. Beispielsweise können Sie die übergeordneten **Einflusseinheiten** auf **100 %** und die untergeordneten CIs auf diese Werte festlegen: ▪ Kind 1: 34 % ▪ Kind 2: 34 % ▪ Kind 3: 34 % ▪ Untergeordnet 4 : 70 % Wenn Warnungen für untergeordnetes Element 3 und untergeordnetes Element 5 den Schweregrad Kritisch haben, wird der Schweregrad des übergeordneten Elements auf Kritisch festgelegt, da die Summe größer als 100 % ist (34 % + 70 % = 1 04 %).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auswirkung wenn kritisch	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad „Kritisch“ ist. Wenn die Spalte rechts von **Auswirkung, wenn kritisch** einen höheren Schweregrad aufweist, aktualisieren Sie alle Spalten ganz rechts mit dem gleichen oder einem niedrigeren Schweregrad als **Auswirkung, wenn kritisch**. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ○ **Kritisch**: Rot (höchster Schweregrad). ○ **Schwerwiegend**: Orange. ○ **Geringfügig**: Gelb. ○ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung wenn größer	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Schwerwiegend** ist. Wenn die Spalte rechts von **Auswirkung, wenn schwerwiegend** einen höheren Schweregrad aufweist, aktualisieren Sie alle Spalten ganz rechts mit dem gleichen oder einem niedrigeren Schweregrad als **Auswirkung, wenn schwerwiegend**. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ○ **Kritisch**: Rot (höchster Schweregrad). ○ **Schwerwiegend**: Orange. ○ **Geringfügig**: Gelb. ○ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung, wenn geringfügig	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Geringfügig** ist. Steuert die Feldwerte rechts von diesem Feld. Wenn die Spalte **Auswirkung, wenn Warnung** einen höheren Schweregrad aufweist, verwenden Sie den Wert **Auswirkung, wenn geringfügig** für beide Felder. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ○ **Kritisch**: Rot (höchster Schweregrad). ○ **Schwerwiegend**: Orange. ○ **Geringfügig**: Gelb. ○ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung, wenn Warnung	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Warnung** ist. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, müssen die Spalten auf der linken Seite höhere Schweregrade aufweisen. ○ **Kritisch**: Rot (höchster Schweregrad). ○ **Schwerwiegend**: Orange. ○ **Geringfügig**: Gelb. ○ **Warnung**: Blau (niedrigster Schweregrad).

Nächste Maßnahme

Überprüfen Sie die Änderungen in der Auswirkungsstruktur. Wenn Sie beispielsweise eine Zahl oder einen Prozentsatz für den Einfluss von untergeordneten CIs geändert haben, überprüfen Sie die Aktualisierungen der Auswirkungsstruktur entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Sie können Servicezuordnungen anzeigen, um aktive Warnungen für CIs und die Beziehungen zwischen CIs anzuzeigen. Durch das Anzeigen dieser Informationen können Sie die Quelle von Warnungen besser verstehen und Abhilfemaßnahmen ergreifen. Die Servicezuordnung ist für alle Anwendungsservices verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Servicezuordnung über diese Orte öffnen:

- In der Liste Anwendungsservices können Sie Servicezuordnungen für Anwendungsservices anzeigen.
- In der Liste „Überwachte Services“ können Sie Servicezuordnungen für überwachte Services anzeigen.

Prozedur

1. Öffnen Sie eine Anwendungsservice-Zuordnung:
   a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**an.
   b. Klicken Sie neben dem Service auf **Zuordnung anzeigen**.
2. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Aktion
Anzeige von Warnungen für ein CI nach Typ und Schweregrad	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Karte auf die Registerkarte **Warnungen**, und überprüfen Sie die aufgelisteten Warnungen.
Anzeige von Änderungen an einem CI in einem erkannten Service	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Zuordnung auf die Registerkarte **Änderungen**.
Warnungsbindungen an CIs anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie auf das Menüsymbol für zusätzliche Aktionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	, um den Indikator **Betroffene CIs** anzuzeigen. **c.** Klicken Sie unterhalb der Zuordnung auf die Registerkarte **Betroffene CIs**.
Anzeige von Dateieigenschaften	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie im Seitenbereich auf die Registerkarte **Eigenschaften**, und überprüfen Sie Informationen zum CI. **c.** Wenn Sie detailliertere Informationen anzeigen möchten, scrollen Sie zum Ende des Bereichs, und klicken Sie auf **Detaillierte Eigenschaften**.
Auswirkungsregeln für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf ein CI mit einem Schweregrad. **b.** Klicken Sie unterhalb der Servicezuordnung auf die Registerkarte **Auswirkung**, und überprüfen Sie die aufgeführten Auswirkungsregeln.
Anzeigen von Warnungsdetails für Netzwerke oder Speicher für einen Service	In der Servicezuordnung: **a.** Klicken Sie mit der rechten Maustaste auf einen Pfad zwischen CIs. **b.** Wählen Sie **Netzwerkpfad anzeigen** oder **Speicherpfad anzeigen**.
Anzeigen weiterer Informationen für CIs	Im Header der Servicezuordnung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	a. Klicken Sie auf das Menüsym–bol für zusätzliche Aktionen **b.** Um auf Wunsch weitere Informationen anzuzeigen, können Sie die **Zuordnungsin dikatoren** auswählen.
Nachbessern eines CIs	Klicken Sie in der Topologie mit der rechten Maus-taste auf das CI, und wählen Sie dann **Optionen für die Fehlerkorrektur**.

Zugehörige Informationen

Warnungsauswirkungsberechnung

Servicezuordnungen verstehen

Erstellen einer Infrastrukturbeziehung für zugehörige CIs

Infrastrukturbeziehungen zeigen CIs, die mit einem Anwendungsservice verbunden sind, aber keine erforderlichen Teile des Services sind. Infrastrukturbeziehungen sind nur für Anwendungsservices verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine CI-Infrastrukturbeziehung erstellen, werden die Informationen in der Tabelle „Infrastrukturbeziehungen“ [em_impact_infra_rel_def] gespeichert. Wenn Warnungen generiert werden, begleitet das zugehörige CI die Anwendungsservice-Informationen im Dashboard Ereignismanagement und in der Auswirkungsstruktur. Zusätzliche Informationen für die zugehörigen CIs werden nur in einer zugehörigen Abhängigkeitsansichtszuordnung für den Anwendungsservice angezeigt. Die folgenden Standard-Infrastrukturbeziehungen sind verfügbar.

Standard-Infrastrukturbeziehungen

Infrastrukturbeziehung	Auswirkungsregel	Beschreibung
cmdb_ci_appl	Mitglied in OS-Cluster	Zeigt die Auswirkung von Warnungen zwischen Hardware- und Softwareanwendungen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Infrastrukturbeziehungen (Fortsetzung)

Infrastrukturbeziehung	Auswirkungsregel	Beschreibung
cmdb_ci_esx_server	Infrastrukturabhängigkeiten	Zeigt die Auswirkung von Warnungen zwischen VCenter und ESX-Clustern an.
cmdb_ci_kvm	Infrastrukturabhängigkeiten	Zeigt die Auswirkung der Warnung auf die Linux-Kernel-basierte Virtual Machine-Konnektivität (KVM) an.
cmdb_ci_vm_zones	Infrastrukturabhängigkeiten	Zeigt die Auswirkung von Warnungen auf die Solaris-VM-Zonen an.

Beispielsweise fügt Ereignismanagement basierend auf der Infrastruktur-Beziehungsdefinition cmdb_ci_vm_zones ZoneServer@mmp1 dem Anwendungsservice hinzu. Die Containment-Regel verwaltet den Schweregrad der Auswirkung auf Warnungen.

Zugehörige CIs werden im BSM angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Infrastrukturbeziehungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Formular Infrastrukturbeziehungen

Feld	Beschreibung
Untergeordneter Typ	Die Tabelle, die Daten zur untergeordneten Entität enthält.
Übergeordneter Typ	Die Tabelle, die Daten zur übergeordneten Entität enthält.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beziehungstyp	Die Beziehung zwischen den untergeordneten und übergeordneten Entitäten.
Auswirkungsrichtung	Die Auswirkungsrichtung, die in der Anwendungsservicezuordnung angezeigt werden soll. ○ **Vom untergeordneten zum übergeordneten Element**: Wenn sich eine Warnung auf ein untergeordnetes Element bezieht, die Auswirkung auf das übergeordnete Element anzeigen. ○ **Vom übergeordneten zum untergeordneten Element**: Wenn sich eine Warnung auf ein untergeordnetes Element bezieht, die Auswirkung auf das übergeordnete Element anzeigen.
Auswirkungsregel	Die Auswirkungsregel zum Berechnen von Infrastrukturbeziehungen: ○ **BS-Clustermitglied** : Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Hosts erfordert **60 % Einfluss** Zum Festlegen des Schweregrads von **Schwerwiegend** , Hat jedes Mitglied **20 % Einfluss** (60 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv. ○ **Mitglied Des Anwendungsclusters** : Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Beispiel: Wenn ein Cluster mit drei Mitgliedern erfordert **90 % Einfluss** Um den Schweregrad für den gesamten Cluster auf festzulegen **Schwerwiegend** , Hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen. ○ **Infrastrukturabhängigkeiten** : Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen. ○ **CI-Anwendungsservice**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Anwendungsservices sind. ○ **Übergeordnetes CI in Anwendung**: Auswirkungen werden nur für die übergeordnete Entität festgelegt. ○ **Inclusion**: Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt. ○ **Netzwerkpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind. ○ **Speicherpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind. ○ **CI-Auswirkung** : Gilt für Anwendungsservices. Bestimmung der Beziehung zwischen Servicemitgliedern. Die Auswirkung von untergeordneten auf übergeordnete CIs ist immer 100 %. Zum Beispiel wird der Schweregrad der Auswirkungen auf die übergeordnete Ebene vom untergeordneten CI mit dem höchsten Schweregrad abgeleitet.

4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkung des untergeordneten Services auf den übergeordneten Service anzeigen

In der Zuordnungsansicht eines Anwendungsservices wird der Schweregrad eines untergeordneten Services an den übergeordneten Service weitergegeben.

Vorbereitungen

Erforderliche Rolle:

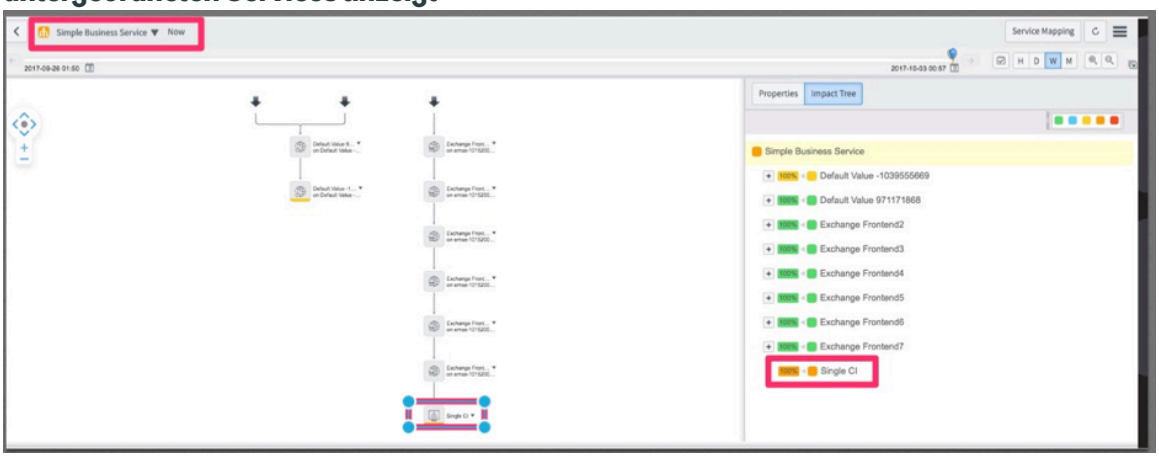
- für Anwendungsservices, evt_mgmt_admin
- Für erkannte Services Service_Mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In der Zuordnungsansicht eines Anwendungsservices können Sie sehen, dass der Schweregrad eines untergeordneten Services an den übergeordneten Service weitergegeben wird.

Ein Anwendungsservice wird durch den Schweregrad von Warnungen beeinflusst, die ihm direkt zugeordnet sind, und von Warnungen auf den CIs, die sich im Service befinden. Wenn der Schweregrad eines untergeordneten Services höher als der des übergeordneten Services ist, wird für den übergeordneten Service in der Zuordnungsansicht der Schweregrad des untergeordneten Services angezeigt. In der Kartenansicht werden die CIs in der Liste **Auswirkungsstruktur** angezeigt. Die Farbe der CIs zeigt den Schweregrad der Warnung an. Der untergeordnete Service ist auch von Anwendungsservices betroffen, die sich unter ihm befinden.

Beispiel, in dem der übergeordnete Service den Schweregrad des untergeordneten Services anzeigt



Wenn eine Schleife entsteht, z. B. durch Verbindung eines übergeordneten Services mit einem untergeordneten Service, kann diese Beziehung in der Zuordnungsansicht angezeigt werden. Die Auswirkung dieser Schleife wird nicht berechnet, und die Beziehung wird in der Auswirkungsstruktur nicht angezeigt. Beispiel: Es gibt drei CIs, A, B und C, wobei C ein Subservice von B und B ein Subservice von A ist. Die Beziehung des mit C verbundenen Services von A wird in der Zuordnungsansicht angezeigt. Diese Beziehung wird jedoch nicht in der Auswirkungsstruktur angezeigt.

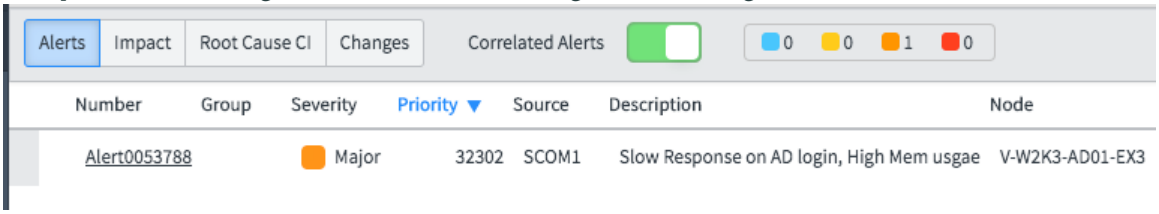
Hinweis: Eine Nachricht wird im Systemfehlerprotokoll im folgenden Format angezeigt, wobei sich die sys_id des Services und der Knoten entsprechend ändern: Schleife in Service-ID: [sysId] und Knoten: [sysId] gefunden. Diese Beziehung wird entfernt, um Auswirkungsschleifen zu vermeiden.

Beispiel: Schleife gefunden in Service-ID: 409d4fd59f030200fe2ab0aec32e705c und Knoten: df5cf6159f030200fe2ab0aec32e70a2. Diese Beziehung wird entfernt, um Auswirkungsschleifen zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf einen Service oder ein CI, um die zugehörigen Warnungen anzuzeigen. Wenn Sie beispielsweise auf den allgemeinen Anwendungsservice klicken, werden die zugehörigen Warnungen im Warnungsbereich unter der Zuordnungsansicht angezeigt. Die aufgeführten Warnungen beziehen sich auf den ausgewählten Service. Warnungen von untergeordneten Services werden aufgelistet, wenn diese Services ausgewählt werden.

Beispiel für Warnungen, die in der Zuordnungsansicht aufgelistet sind



Prozedur

Öffnen Sie eine Anwendungsservice-Zuordnung:

a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**an.

b. Wählen Sie Aus **Service Anzeigen** Neben dem Service.

c. Wählen Sie im rechten Bereich aus **Auswirkungsstruktur** .

d. Wählen Sie im unteren Bereich aus **Auswirkung** .

Ergebnis

In der Servicezuordnung können Sie visuell überprüfen, ob für die Serviceintegrität des untergeordneten Service ein Rollup zum übergeordneten Service durchgeführt wird. Unten von Jeweils Das Symbol eines betroffenen CI ist ein farbiger Balken, der den Schweregrad der Warnung darstellt. Diese Farbleiste wird auch in der unteren Leiste des übergeordneten Services angezeigt. Für die manuelle Clusterkonfiguration können Sie Anwendungsauswirkung und Anwendungsclustermitglied ändern.

Zugehörige Informationen

Zuordnungssegmente auf andere Anwendungsservices übertragen

Konfigurieren Sie einen manuellen Cluster

Warnungsauswirkungen bei der Selektierung von Warnungen anpassen

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Hinzufügen CMDB Tabellen oder Klassen für die Berechnung der Auswirkung

Fügen Sie hinzu CMDB Tabellen, die Anwendungsservices enthalten, die bei der Auswirkungsberechnung berücksichtigt werden sollen, um genaue und relevante Auswirkungsergebnisse sicherzustellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Organisationen können eine große Anzahl von haben CMDB Tabellen oder Klassen wie cmdb_ci_Service_by_Tags, cmdb_ci_Service_Auto und viele andere. Für die Berechnung der Auswirkung sind jedoch nicht alle erforderlich. Um die Analyse zu optimieren und die Verarbeitung irrelevanter Daten zu vermeiden, können Sie selektiv nur diese hinzufügen oder entfernen CMDB Klassen, die kritische Infrastruktur oder Komponenten darstellen. Das folgende Verfahren zeigt, wie Sie einen hinzufügen CMDB Klasse. Wenn Sie eines

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

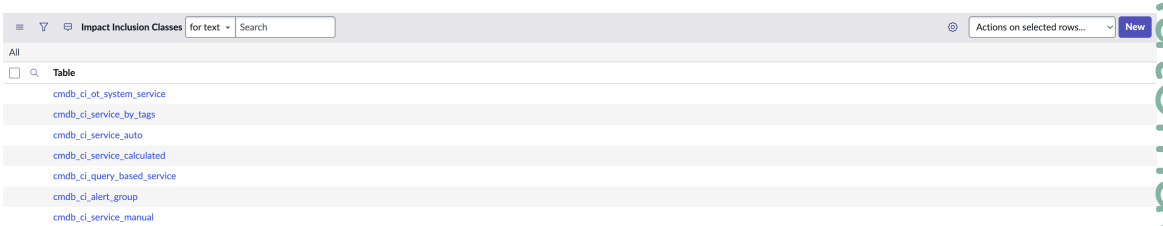
entfernen möchten CMDB Tabelle aus der Liste siehe Entfernen CMDB Tabellen oder Klassen aus der Auswirkungsberechnung.

Wenn Sie hinzufügen CMDB Klasse, werden alle Anwendungsservices im Zusammenhang mit dieser Klasse für die Berechnung der Auswirkung berücksichtigt. Wenn Sie jedoch nicht alle Services einer bestimmten Klasse einschließen und nur bestimmte auswählen möchten, können Sie dies auf der Seite „Impact Filterservices“ tun. Weitere Informationen zum ein- oder Ausschließen eines Service finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

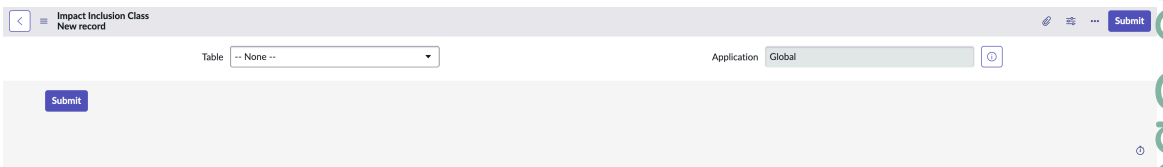
Prozedur

1. Navigieren Sie zu **Alle** Und suchen Sie nach `EM_Impact_Inclusion_class.list` .

   Die Seite Impact Inclusion-Klassen wird geöffnet und zeigt eine Liste von an CMDB Klassen, die in der Auswirkungsberechnung enthalten sind.

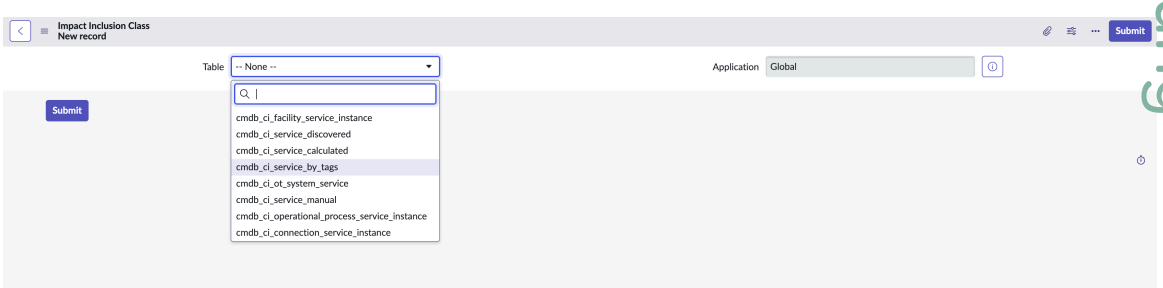


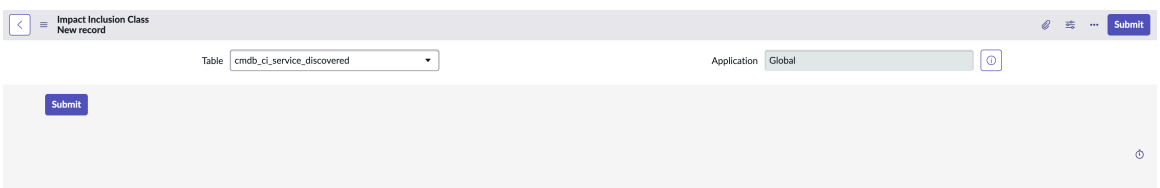
2. Wählen Sie **Neu**.



3. Von **Tabelle** Wählen Sie ein aus CMDB Tabelle.

   Hinweis: Die Liste enthält nur die CMDB Tabellen, die für die Berechnung der Auswirkung unterstützt werden, nicht alle CMDB Tabellen.



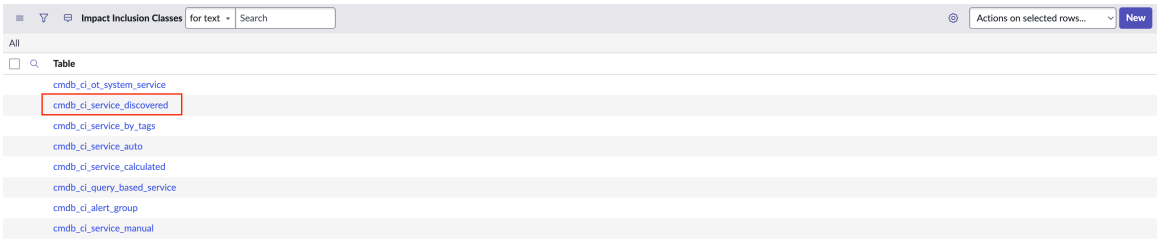


4. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die CMDB Tabelle wird der Liste der Impact-Aufnahmeleklassen hinzugefügt.



Entfernen CMDB Tabellen oder Klassen aus der Auswirkungsberechnung

Unnötige ausschließen CMDB Tabellen oder Klassen aus der Auswirkungsberechnung, um die Leistung zu verbessern und sich auf relevante Daten zu konzentrieren.

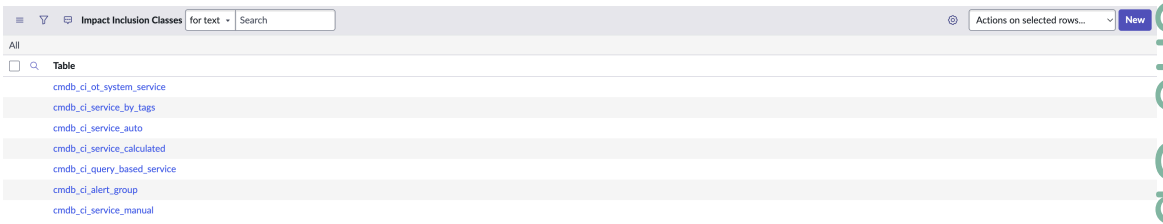
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren Sie zu **Alle** Und suchen Sie nach EM_Impact_Inclusion_class.list .

   Die Seite Impact Inclusion-Klassen wird geöffnet und zeigt eine Liste von an CMDB Klassen, die in der Auswirkungsberechnung enthalten sind.



2. Wählen Sie aus CMDB Tabelle, die Sie entfernen möchten.
3. Wählen Sie das Menü Aktionen für ausgewählte Zeilen aus, und wählen Sie dann aus **Löschen** .
4. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die CMDB Tabelle wird aus der Liste entfernt.

Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu

Geben Sie die Anwendungsservices an, die bei der Auswirkungsberechnung berücksichtigt werden müssen, um eine genaue Serviceauswirkungsbewertung sicherzustellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Organisationen können Tausende – oder sogar Hunderttausende – von Anwendungsservices haben. Wenn ein CMDB Klasse wird der Tabelle em_Impact_Inclusion_class.list hinzugefügt, dann werden alle Anwendungsservices, die sich auf diese Klasse beziehen, in die Auswirkungsberechnung einbezogen. Es gibt jedoch zwei mögliche Szenarien:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Szenario 1: CMDB Klasse wird der Liste „em_Impact_Inclusion_class.list“ hinzugefügt, Sie möchten jedoch, dass nur bestimmte Services für die Berechnung der Auswirkung berücksichtigt werden. Sie können entweder:
  - Entfernen Sie die unerwünschten Services aus der Liste em_Impact_Filter_Service.list, oder
  - Legen Sie ihren Status in der Liste em_Impact_Filter_Service.list auf „falsch“ fest.

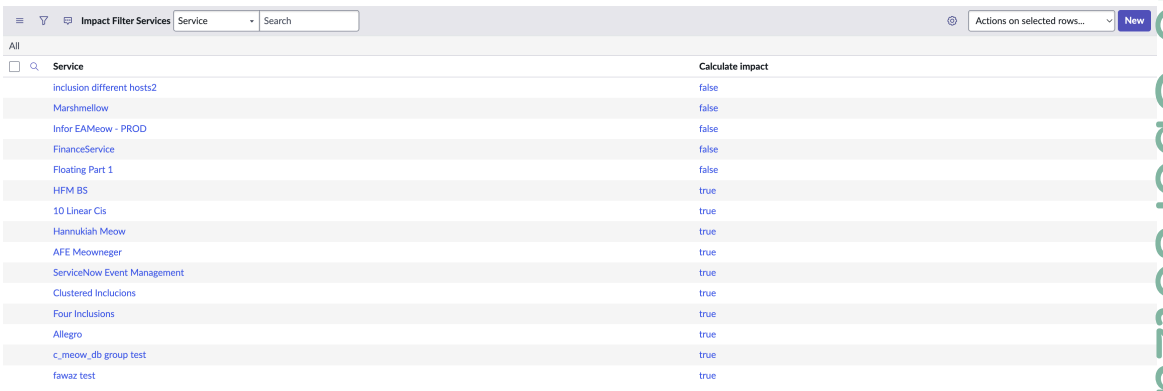
  Informationen zum Entfernen des Anwendungsservice aus der Liste finden Sie unter Entfernen Sie Anwendungsservices aus der Auswirkungsberechnung.
- Szenario 2: CMDB Klasse wird nicht zu em_Impact_Inclusion_class.list hinzugefügt. Daher wird keiner der Anwendungsservices im Zusammenhang mit dieser Klasse für die Berechnung der Auswirkung berücksichtigt. Sie möchten jedoch nur bestimmte Anwendungsservices aus dieser Klasse einschließen. Sie können diese Services direkt der Tabelle „em_Impact_Filter_Service.list“ hinzufügen und ihren Status auf „wahr“ festlegen, ohne dass hinzugefügt wird CMDB Klasse in die Tabelle „em_Impact_Inclusion_class.list“.

Das folgende Verfahren zeigt, wie ein Anwendungsservice direkt der Tabelle „em_Impact_Filter_Service.list“ hinzugefügt wird, damit er für die Berechnung der Auswirkung berücksichtigt wird.

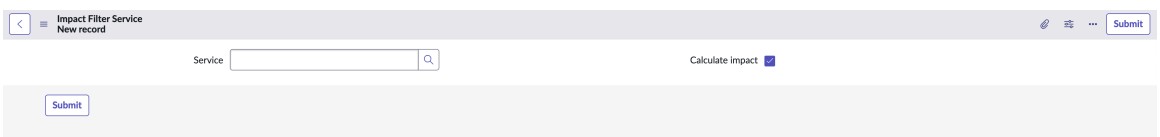
Prozedur

1. Navigieren Sie zu **Alle** Und suchen Sie nach EM_Impact_Filter_Service.list .

   Die Seite Impact Filterservices wird geöffnet.



2. Wählen Sie **Neu**.



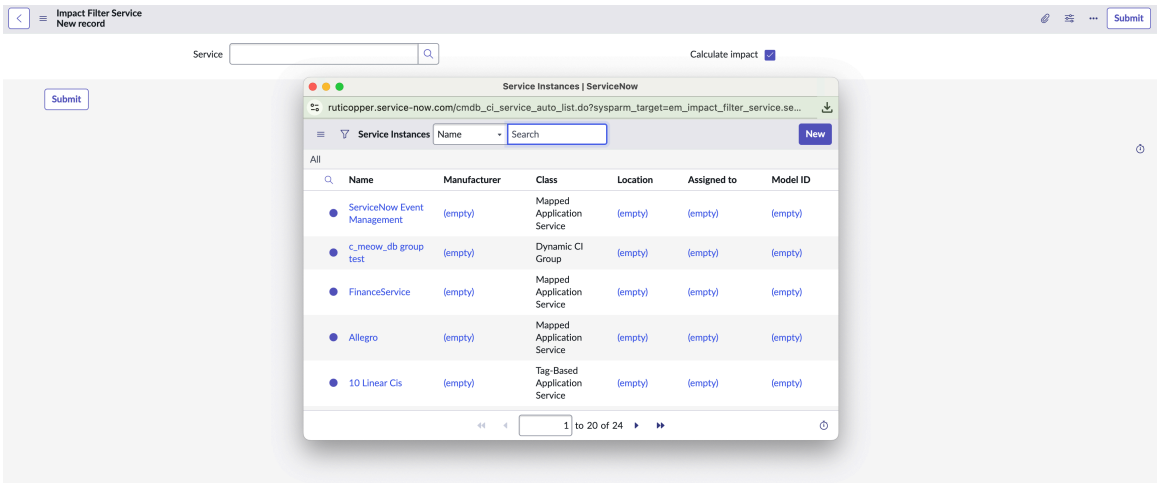
3. In **Service** Wählen Sie das Suchsymbol ( ).

   Hinweis: Standardmäßig ist **Berechnen Sie die Auswirkung** Das Kontrollkästchen ist aktiviert.

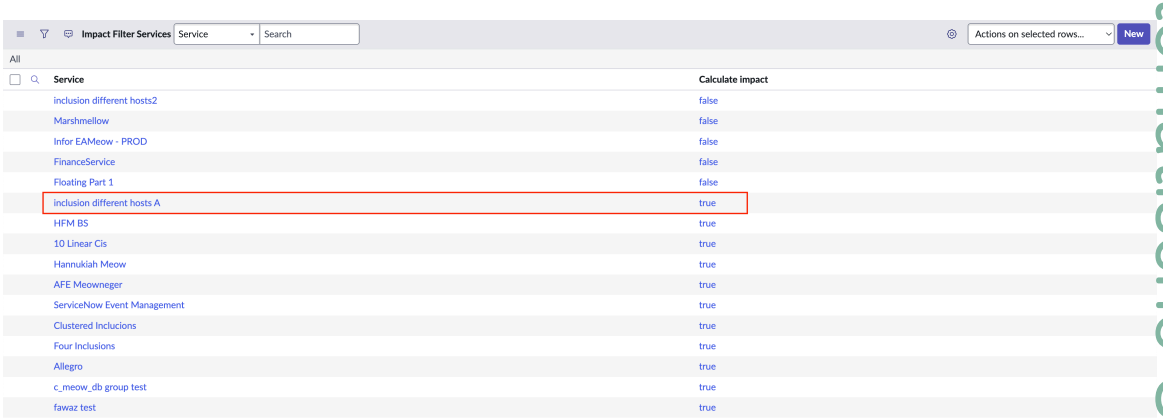
4. Wählen Sie auf der Seite „Serviceinstanzen“ den Service aus, den Sie für die Auswirkungsberechnung hinzufügen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie **Absenden**.
Der Anwendungsservice wird der Liste der Auswirkungsfilterservices hinzugefügt.



Hinweis: Nur die Anwendungsservices, die der Liste „Impact Filterservices“ hinzugefügt wurden, werden im angezeigt Service-Dashboard .

Entfernen Sie Anwendungsservices aus der Auswirkungsberechnung

Schließen Sie bestimmte Anwendungsservices von der Auswirkungsberechnung aus, um Rauschen zu reduzieren und sich auf kritische Komponenten zu konzentrieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Durch das Entfernen oder Löschen eines Datensatzes aus der Liste wird der Anwendungsservice nicht unbedingt von der Auswirkungsberechnung ausgeschlossen, wenn dies der Fall ist CMDB Klasse ist noch in em_Impact_Inclusion_class.list vorhanden. Selbst wenn die Klasse jedoch in em_impact_Inclusion_class.list vorhanden ist, wird der Anwendungsservice für die Auswirkungsberechnung nicht berücksichtigt, wenn sein Status auf festgelegt ist **Berechnen Sie Die Auswirkung** = **Falsch** In em_Impact_Filter_Service.list.

Fügen Sie für den Anwendungsservice, den Sie aus der Auswirkungsberechnung ausschließen möchten, den Anwendungsservice mit hinzu **Berechnen Sie Die Auswirkung** = **Falsch** , Oder ändern **Berechnen Sie Die Auswirkung** = **Falsch** , Wenn dieser Datensatz bereits vorhanden ist. Das Verfahren zeigt, wie diese Einstellung konfiguriert wird.

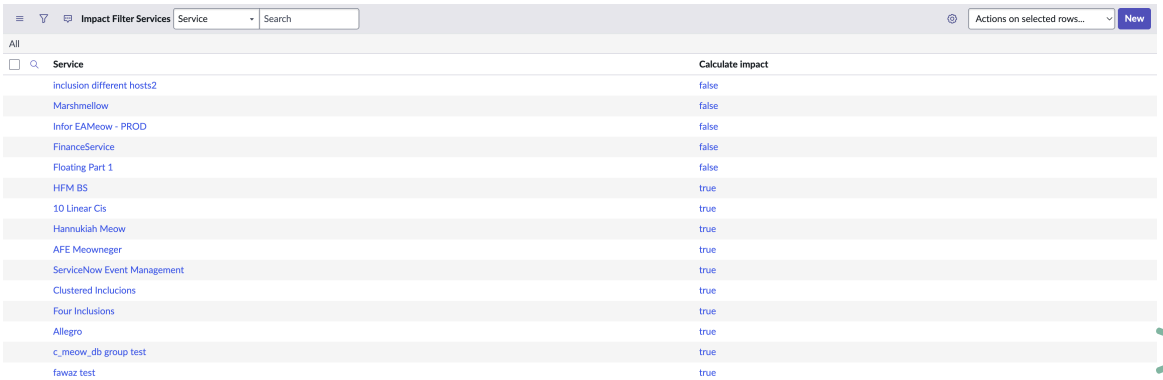
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu **Alle** Und suchen Sie nach EM_Impact_Filter_Service.list .

   Die Seite Impact Filterservices wird geöffnet.



2. Ändern Sie für den Anwendungsservice, den Sie aus der Auswirkungsberechnung ausschließen möchten **Berechnen Sie die Auswirkung** Status des Anwendungsservice an **Falsch** .
   Dadurch wird der Anwendungsservice-Datensatz in der Liste beibehalten, aber von der Auswirkungsberechnung ausgeschlossen.

Ursachenanalyse (RCA)

Verkürzen Sie die durchschnittliche Zeit bis zur Reparatur (MTTR), indem Sie die Ursache einer Warnung ermitteln.

Die Ursachenanalyse (RCA) bietet eine Liste der wahrscheinlichen Ursachen für Warnungen. Diese Funktion verwendet vorhandene Daten in IT Service Management, um die Ursache eines Problems zu ermitteln.

RCA berücksichtigt drei Faktoren: Warnungen, Configuration Item (CI)-Topologie und Change-Anforderungen auf den CIs. Sie extrahiert CIs aus Warnungen oder Warnungsgruppen und analysiert die CI-Beziehungen in der CMDB. Anschließend werden verschiedene konfigurierbare Filter verwendet, um relevante Change-Anforderungen in den CIs als mögliche Ursachen zu berücksichtigen.

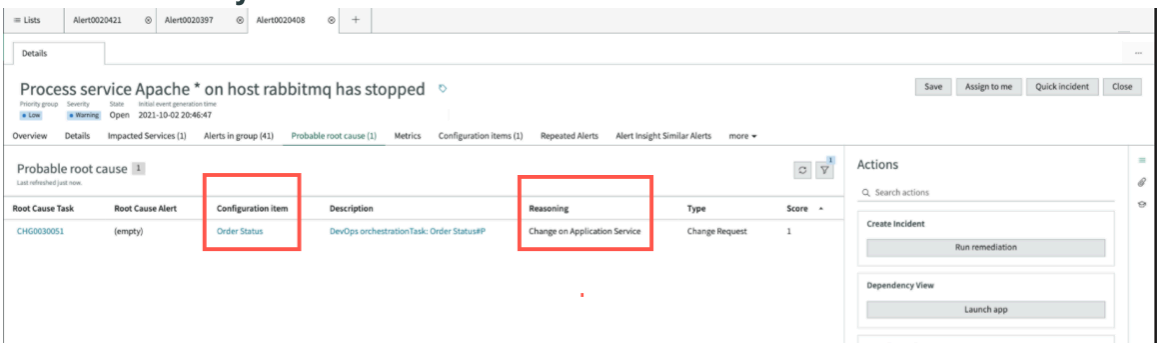
Change-Anforderungen können sich auf einen Zeitrahmen oder ein CI, den zugehörigen Anwendungsservice oder die darauf installierte Software beziehen. Beispielsweise muss ein CI aktualisiert oder ein Sicherheitspatch installiert werden. Eine Change-Anforderung für ein CI kann sich auf andere CIs auswirken.

RCA ordnet die Warnungen und Change-Anforderungen den CIs zu. Anschließend wird die Ursachenpunktzahl berechnet, eine logische Punktzahl, die zum Sortieren wahrscheinlicher Ursachen verwendet wird. Die Berechnung dieser Punktzahl basiert auf Change-Anforderungen für CIs und auf Warnungen für ein wichtiges CI, das als Topologieursprungs-CI bezeichnet wird. Die Punktzahl der Ursache bestimmt, wie RCA die Liste der wahrscheinlichen Ursachen ausfüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Analyse wahrscheinlicher Ursachen



Standardmäßig zeigt die Liste die fünf wahrscheinlichsten Ursachen mit der höchsten Punktzahl an. Sie listet die mit den einzelnen Warnungen verbundenen CIs und den Grund auf, aus dem sie von RCA als mögliche Ursachen identifiziert wurden.

Die Bewertung für wahrscheinliche Ursachen wird durch die folgenden Kriterien in der angegebenen Reihenfolge bestimmt (niedrigere Nummer = höhere Priorität):

1. Change für ein CI, das aus einer Topologie stammt
2. Change für ein zugehöriges CI, das aus einer Topologie stammt
3. Change für ein CI
4. Change für ein zugehöriges CI/Change für einen Anwendungsservice/Change für Software
5. Warnung für das CI, das aus einer Topologie stammt

Um die Funktion „Analyse wahrscheinlicher Ursachen“ zu deaktivieren, müssen Sie die Eigenschaft erstellen *sa_analytics.disable_prc*Und legen Sie den Wert auf fest Wahr . Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

RCA-Einstellungen anpassen

Ändern Sie die Standardeinstellungen, die das RCA-Verhalten bestimmen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardfiltereinstellungen steuern, welche Change-Anforderungen von RCA als mögliche Ursachen angesehen werden. Sie können bestimmte Standardeinstellungen ändern, um z. B. RCA Standard-Change-Anforderungen zu ignorieren.

Sie können auch die Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen ändern. Standardmäßig zeigt die Liste die fünf wahrscheinlichsten Ursachen mit der höchsten Punktzahl für die Ursache an.

Standardmäßig ist die RCA-Berechnung aktiviert. Sie können sie deaktivieren, indem Sie den Standard ändern *sa_analytics.disable_prc*Wert auf „wahr“.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Führen Sie je nach Bedarf eine oder beide der folgenden Aktionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie die Standardfiltereinstellungen:

  a. Wählen Sie Aus **Neu** .

  b. Geben Sie im Feld **Name** den Namen der Eigenschaft an, für die Sie die Standardeinstellung ändern möchten.

  Die neue Eigenschaft muss denselben Namen haben wie die zugehörige Eigenschaft in der Tabelle.

Eigenschaft	Beschreibung	Typ	Standardwert
sa_analytics.rca.filter_category	Die Kategorien von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	" "
sa_analytics.rca.filter_type	Die Typen von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	„Standard, Normal, Notfall“
sa_analytics.rca.filter_status	Die Status von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	„-1,0,3,7,8,157“
sa_analytics.rca.filter_interval_in_hours	Der Zeitrahmen in Stunden, in dem Change-Anforderungen aufgetreten sind, die RCA als mögliche Ursache betrachtet.	Integer	168

  c. Geben Sie einen gültigen Wert für die Eigenschaft ein.

  Hinweis: Der Wert, den Sie für die neue Eigenschaft festlegen, überschreibt den Standardwert für die zugehörige Eigenschaft.

- Ändern Sie die Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen:

  a. Suchen Sie die Eigenschaft *sa_analytics.rca_task_table_max_records*.

Name der Eigenschaft	Beschreibung	Typ	Standardwert
sa_analytics.rca_task_table_max_records	Die maximale Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen:	Integer	5

  b. Ersetzen Sie den Standardwert durch einen neuen gültigen Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Deaktivieren Sie RCA, indem Sie erstellen *sa_analytics.disable_prc*Eigenschaft.

  a. Wählen Sie **Neu**.

  b. Füllen Sie das Formular mit den folgenden Werten aus.

Eigenschaftsname	Beschreibung	Typ	Wert
sa_analytics.disable_prc	Die wahrscheinliche Ursache wird deaktiviert.	Boolean	True

3. Klicken Sie auf **Absenden**.

Warnungsähnlichkeit

Das Finden von Warnungen, die der von Ihnen untersuchten Warnung ähnlich sind, kann helfen, Zeit bei der Fehlerbehebung zu sparen, indem Sie sehen, wie ähnliche Warnungen gelöst wurden.

Ähnliche Warnungen suchen

Warnungsähnlichkeit gilt für Natural Language Processing (NLP) basierend auf ServiceNow AI Platform Maschinelles Lernen (ML) wie in implementiert Predictive Intelligence .

Die ML-Logik filtert irrelevante Informationen heraus und bietet weitere Informationen zum Verständnis der Ursache von Warnungen. Sie können Lösungen zur Lösung ähnlicher Warnungen und die wahrscheinliche Ursache anzeigen.

ML hilft bei der Suche nach ähnlichen Warnungen basierend auf dem Text in diesen Warnungsdatensatzfeldern:

- Konfigurationselement.Klasse
- Metrikname
- Beschreibung

Zusätzliche Warnungsinformationen

Wählen Sie im Warnungsarbeitsbereich die erforderliche Warnung aus, und klicken Sie auf **Insight**, um zusätzliche Informationen zur Warnung anzuzeigen.

Wählen Sie in der Liste Warnungen die erforderliche Warnung aus, und verwenden Sie die Registerkarten „Warnungseinblick“ auf der rechten Seite des Warnungsdatensatzes, um zusätzliche Informationen zur Warnung anzuzeigen. Zum Beispiel können Sie die letzten Warnungen für das aktuelle CI und ähnliche CIs anzeigen, um die beste Lösung für das Nachbessern und Lösen dieser Warnung zu finden.

Die Registerkarten für Warnungseinblick sind:

- Betroffene Services
- Flatternd
- Verlauf
- Aktivitäten
- Weitere Informationen
- Wiederholte Warnungen
- Ähnliche Warnungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CI-Incidents
- CI-Change Requests
- CI-Probleme
- Zugehörige Incidents
- Zugehörige Change Requests
- Zugehörige Probleme

Weitere Informationen zu den Registerkarten für Warnungseinblick finden Sie unter Informationen zu Warnungseinblick.

Ähnliche Warnungen suchen

Sie können Warnungen finden, die der derzeit untersuchten Warnung ähnlich sind. Sparen Sie Zeit bei der Fehlerbehebung, indem Sie ähnliche Warnungen überprüfen, um zu sehen, wie sie gelöst wurden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Predictive Intelligence aktiv ist. Informationen zum Aktivieren dieses Plugins finden Sie unter Aktivieren Sie ein Plugin .

Stellen Sie sicher, dass die Eigenschaft `evt_mgmt.similarity_use_ml` auf `true` festgelegt ist.

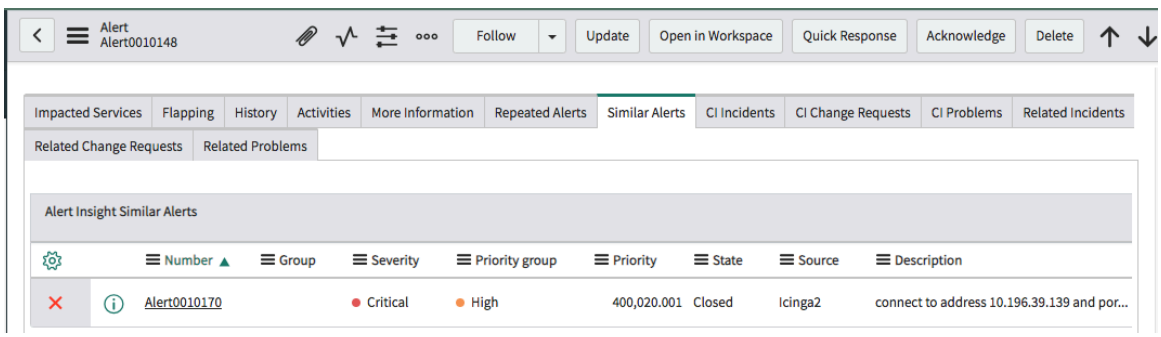
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sparen Sie Zeit beim Lösen der aktuellen Warnung, indem Sie überprüfen, wie ähnliche Warnungen gelöst wurden. Stellen Sie eine Lösungskonsistenz bereit, indem Sie ähnliche Warnungen auf dieselbe Weise lösen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie in der Liste der Warnungen auf den Warnungsdatensatz, den Sie untersuchen möchten.
3. Klicken Sie im Warnungsdatensatz auf die Registerkarte **Ähnliche Warnungen**.
   Warnungen, die der untersuchten Warnung ähnlich sind, werden aufgelistet.



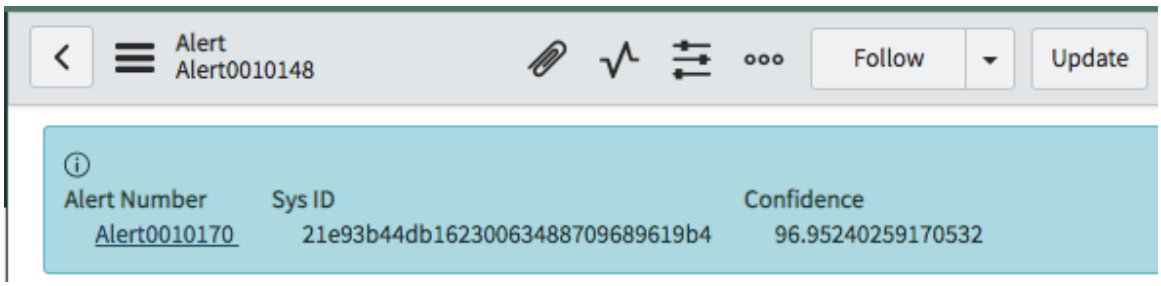
   Standardmäßig werden bis zu 10 ähnliche Warnungen aufgelistet. Sie können diesen Wert ändern, indem Sie die Eigenschaft `evt_mgmt.similarity_max_similar_alerts_shown` festlegen.

4. Wenn Sie einen Schwellenwert konfiguriert haben, klicken Sie im Bereich „Zugehörige Links“ auf **Ähnlichkeitsdetails anzeigen**.
   Die Sys-ID und das Confidence-Level jeder ähnlichen Warnung werden angezeigt. Das Confidence-Level zeigt an, wie die ähnliche Warnung mit den von Ihnen festgelegten Parametern übereinstimmt. Beispielsweise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zeigt ein hoher Confidence-Prozentwert eine höhere Wahrscheinlichkeit einer Ähnlichkeit der Warnungen mit den von Ihnen festgelegten Werten an.



Sie können den Wert des Schwellenwerts ändern, indem Sie die Eigenschaft evt_mgmt.similarity_use_threshold festlegen.

Ähnlichkeitslösungen

Mithilfe von Ähnlichkeitslösungen können Sie Machine Learning (ML) verwenden, um den Text in einem Datensatz für gelöste Warnungen mit einem Datensatz für offene Warnungen zu vergleichen, um den Lösungsansatz erneut zu verwenden.

Ähnlichkeitslösung trainieren

Zum Trainieren einer Ähnlichkeitslösung sammeln Sie Wörter, um eine Sammlung zu erstellen, die Machine Learning (ML) verwenden kann, um Text in den Feldern **Kurzbeschreibung**, **Beschreibung**, **Quelle**, **Typ**, **Ressource** und **Metrikname** in einer gelösten Warnung zu vergleichen, um zu sehen, ob die Wörter in der festgelegten Übereinstimmung mit den Wörtern in einer offenen Warnung übereinstimmen. Die gelöste Warnung, die einer offenen Warnung ähnelt, ist ein Beispiel dafür, wie die offene Warnung gelöst werden kann.

Um eine Lösung zu trainieren, muss der Filter mindestens einen Datensatz zurückgeben. Wenn Ihr Filter keine Datensätze zurückgibt, aktualisieren Sie ihn.

Hinweis: Die bevorzugte Anzahl von Datensätzen für das Trainieren einer Lösung besteht aus 30.000 bis 300.000 Datensätzen. Wenn Sie mehr als 300.000 Datensätze einreichen, werden die neuesten 300.000 Datensätze zum Trainieren der Lösung verwendet. Verwenden Sie nur authentische Datensätze aus der Datenbank.

- Stellen Sie sicher, dass die Datensätze, die Sie trainieren, nicht zu alt und relevant für Ihren Geschäftbedarf sind. Sorgen Sie dafür, dass die Wörter in der Sammlung stets aktuell sind.
- Verwenden Sie keine hartcodierten Datumsangaben als Filter, da diese Filter nicht aktualisiert werden, wenn die Lösungen neu trainiert werden, es sei denn, Sie aktualisieren sie vor jedem neuen Training manuell. Verwenden Sie stattdessen relative Datumsfilter, wie z. B. letzte 3 Monate, letzte 6 Monate oder letzte 12 Monate.
- Führen Sie nach Bedarf Trainings durch, bis eine akzeptable Ähnlichkeitslösung bereitgestellt wird. Diese Praxis bietet Ihnen Zeit zum Überprüfen und Aktualisieren Ihrer Lösungsdefinition.

Felder, die in die Lösung einbezogen werden sollen

Notieren Sie sich Felder, die wahrscheinlich Wörter und Ausdrücke enthalten, die dem System helfen, ähnliche Datensätze für Ihre Lösung zu identifizieren.

Die Ähnlichkeitsfelder, die Sie auswählen, sollten eine Teilmenge Ihres Eingabefelds „Auswahlen“ sein. Beispiel: Wenn Sie „Felder“ aus Incident-Datensätzen auswählen, die sich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

im Status „Offen“ befinden, wählen Sie **Hinweis schließen** nicht als Ähnlichkeitsfeld aus. Da offene Datensätze keine **Hinweis schließen**-Felder enthalten, kann der Text nicht ähnlich sein.

Die Ähnlichkeitsfelder stehen Benutzern beim Erstellen von Datensätzen zur Verfügung.

Über die Ähnlichkeitspunktzahl

Die Ähnlichkeitspunktzahl ist ein Maß für den Ähnlichkeitsgrad zwischen zwei Warnungsdatensätzen von 0 bis 100. Warnungsdatensätze, deren Ähnlichkeitspunktzahl über dem von Ihnen angegebenen Schwellenwert liegt, werden von der Lösung zurückgegeben.

Überprüfen Sie Ähnlichkeitsbeispiele und ihre Punktzahlen mithilfe der Funktion **Schulungsfortschritt anzeigen**, um zu bestimmen, ob der Lösungsschwellenwert erhöht oder verringert werden soll. Sie können den Schwellenwert im Feld **Threshold for Similarity Score** (Schwellenwert für Ähnlichkeitspunktzahl) ändern.

Fortschritt der Trainingslösung anzeigen

Die Trainingsdauer variiert je nach Anzahl der Datensätze und Klassen innerhalb des Trainingssatzes. Je mehr Datensätze und Klassen Sie verwenden, desto länger dauert das Training. Zum Beispiel kann das Trainieren eines Satzes mit 100.000 Datensätzen und mehreren hundert Klassen ungefähr fünf Stunden dauern.

Um den Fortschritt der Trainingslösung zu zeigen, führt die ML-Lösung automatisch die folgenden Tätigkeiten aus, wenn Sie **Trainingsfortschritt anzeigen** auf der Seite „Lösungen“ wählen. Weitere Informationen finden Sie unter Zeigen Sie den Fortschritt des Lösungstrainings an .

Lösungstrainingsaktivitäten

Aktivität	Beschreibung
Dateien zum Trainieren abrufen.	Das System lädt die Trainingsdatensätze herunter und sendet sie an den nächstgelegenen Trainingsservice.
Daten vorbereiten.	Das System entfernt doppelte Datensätze aus dem Trainingssatz.
Lösung trainieren.	Der Trainingsservice trainiert die Lösung.
Trainierte Lösung hochladen.	Der Trainingsservice lädt die Lösung als Anhangsdatensätze hoch.

Eine Ereignismanagement Ähnlichkeitslösung erstellen

Erstellen und trainieren Sie eine Lösung, die maschinelles Lernen auf eine Sammlung von Wörtern anwendet und ähnliche Warnungen in Ihrem Instanzdatensatz vorschlägt. Sie können beispielsweise den Text in einer gelösten Warnung mit einer offenen Warnung vergleichen, um die Lösung wiederzuverwenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Das von Ihnen verwendete Verschlüsselungsschema kann sich darauf auswirken, ob Sie Lösungen trainieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Ihre Daten durch Full Disc Encryption (FDE) verschlüsselt sind, können Sie Lösungen trainieren.
- Wenn das Feld, das Sie für das Training verwenden, mit verschlüsselt ist Feldverschlüsselung Stellen Sie sicher, dass der Benutzer des gemeinsam genutzten Service Worker über die richtige Verschlüsselungsmodulrolle verfügt, die für die Verschlüsselung verwendet wurde.
- Wenn Sie Edge Encryption verwenden, wird das Trainieren nicht unterstützt.

Hinweis: Diese Funktion unterstützt nur die englischsprachige Verarbeitung.

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungsdefinitionen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

ML-Lösungsdefinitionsformular

Feld	Beschreibung
Lösungsvorlage	Verwendung zum Definieren einer Wortsammlung.
Bezeichnung	Eindeutiger Name für die Ähnlichkeitslösung.
Name	Feld, das automatisch mit einem vom System zugewiesenen Namen gefüllt wird, der dem Bezeichnungsnamen beim Erstellen der Lösung ähnlich ist.
Tabelle	Tabelle, die die Datensätze enthält, die für die Wortsammlung verwendet werden sollen, z. B. Incident-Tabelle oder Asset-Tabelle. Wenn Sie einen Tabellenwert zuweisen, erscheint ein Link, der die Anzahl der Datensätze zeigt, die mit Ihren aktuellen Bedingungen übereinstimmen.
Filter	Bedingungen, die Sie auf die Trainingsdatensätze anwenden möchten. Um eine Lösung zu trainieren, muss der Filter mindestens einen Datensatz zurückgeben. Wenn Ihr Filter keine Datensätze zurückgibt, aktualisieren Sie ihn.
Eingabefelder	Notieren Sie sich Felder, die den Text und Kontext enthalten, die Sie in Ihre Wortsammlung aufnehmen möchten. Der Felddatentyp kann eine Zeichenfolge, Referenz, Auswahl oder HTML sein, z. B. **Kurzbeschreibung** und **Beschreibung**. **Hinweis:** **Journaltyp** ist kein unterstützter Datentyp. Gute Kandidaten für Ihre Eingabefelder enthalten Text, der für die Lösung relevant ist. Wenn Sie zum Beispiel eine Lösung konfigurieren, um ähnliche Incident-Datensätze zu finden, können Sie die Felder **Kurzbeschreibung**, **Beschreibung**, **Lösungsnotizen** und **Notizen schließen** auswählen.
Schulungshäufigkeit	Trainings werden standardmäßig einmal vom System durchgeführt. Da Ihre Daten mit der Zeit altern können, wodurch die Genauigkeit Ihres Vorhersagemodells beeinträchtigt wird, sollten Sie regelmäßige Trainings in Betracht ziehen, wenn Ihre Lösungsdefinition relativ stabil ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Domäne	Wählen Sie in Instanzen mit aktiver Domänentrennung die Domäne aus, deren Zieldatensätze Sie für Ihre Wortsammlung verwenden möchten. Erstellen Sie einen separaten Datensatz für die Ähnlichkeitslösungsdefinition für jede Domäne, deren Feldwerte Sie für Ihre Wortsammlung verwenden möchten.
Ähnlichkeitsfelder	Notieren Sie sich Felder, die wahrscheinlich Wörter und Ausdrücke enthalten, die dem System helfen, ähnliche Datensätze für Ihre Lösung zu identifizieren. Wenn Sie Ihre **Ähnlichkeitsfeldauswahl** ändern möchten, klicken Sie auf das Schlosssymbol ( ), um es zu öffnen, und nehmen Sie Aktualisierungen vor. Klicken Sie erneut auf das Symbol, um das Feld zu schließen und die Aktualisierungen zu speichern.
Ähnlichkeitsfenster	Der Zeitraum, in dem Sie nach ähnlichen Datensätzen suchen möchten. Wenn Sie eine kleinere Zahl an insgesamt eingehenden Datensätzen haben, ist möglicherweise ein größeres Fenster am besten. Wenn das Fenster jedoch zu groß ist, rufen Sie möglicherweise Datensätze ab, die nicht nützlich sind. Wenn das Fenster zu klein ist, können Sie möglicherweise nicht genügend ähnliche Datensätze abrufen. Wenn Sie beispielsweise nach ähnlichen Incident-Datensätzen suchen, die geöffnet sind, können Sie **Letzter Tag** auswählen. Diese Auswahl bezieht sich auf die neuesten Datensätze, von denen viele noch offen sein könnten.
Ähnlichkeitsfensterfilter	Filterbedingungen für Ihr Ähnlichkeitsfenster. Diese Filter definieren die Datensatz-Bedingungen, unter denen Ihre Ähnlichkeitsergebnisse ermittelt werden. Wenn Sie zum Beispiel nach ähnlichen Incident-Datensätzen suchen, die offen sind, können Sie Ihre Suche filtern, indem Sie Bedingungen erstellen wie: **[Incident-Status] [ist] [In Bearbeitung]** Diese Filter werden zusätzlich zu den **Eingabefeld**-Filtern angewendet.
Aktualisierungshäufigkeit für Fenster	Aktualisierungshäufigkeit des Ähnlichkeitsfensters. Beispiel: Wenn Ihr Fenster offene Incident-Datensätze enthält, können Sie die Aktualisierungshäufigkeit **Alle 15 Minuten**auswählen. Neue Incidents treten häufig im Laufe des Tages auf, sodass diese Häufigkeit die Wahrscheinlichkeit erhöht, dass neu geöffnete Datensätze in die Aktualisierung einbezogen werden. **Hinweis:** Wenn das Ähnlichkeitsfenster aus Datensätzen besteht, z. B. Wissensartikel-Datensätze, die in der Regel nicht häufig erstellt werden, können Sie eine höhere Aktualisierungshäufigkeit wählen, z. B. **Jeden Tag**.

4. Klicken Sie auf **Speichern**, um den Lösungsdefinitionsdatensatz zu speichern, damit Sie später darauf zurückgreifen können, oder auf **Senden und trainieren**, um den Lösungsdefinitionsdatensatz zu erstellen und zu trainieren.
5. Wenn Sie die Lösung zum Trainieren übermittelt haben, klicken Sie im Fenster **Trainingsaktivierung** zur Bestätigung auf **OK**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Das System plant das Trainieren der Lösung beim nächstgelegenen Trainingsservice. Sie und andere Benutzer, die die Kategorie „Predictive Intelligence-Benachrichtigungen“ abonniert haben, erhalten eine Benachrichtigung, wenn das Training abgeschlossen ist, einschließlich aller Fehler, die im Training aufgetreten sind. Nach Abschluss des Trainings lädt das System die Lösung als Anhangsdatensatz hoch.

Nächste Maßnahme

Schauen Sie sich die Beispiele der trainierten Ähnlichkeitslösung im zugehörigen Link **Ähnlichkeitsbeispiele** des Formulars „ML-Lösungsdefinition“ an.

Fortschritt des Lösungstrainings Ereignismanagement anzeigen

Zeigen Sie den Fortschritt oder Statistiken des Lösungstrainings an, um zu bestimmen, ob eine Lösung verfügbar ist oder wie lange der nächste Trainingszyklus vermutlich dauert.

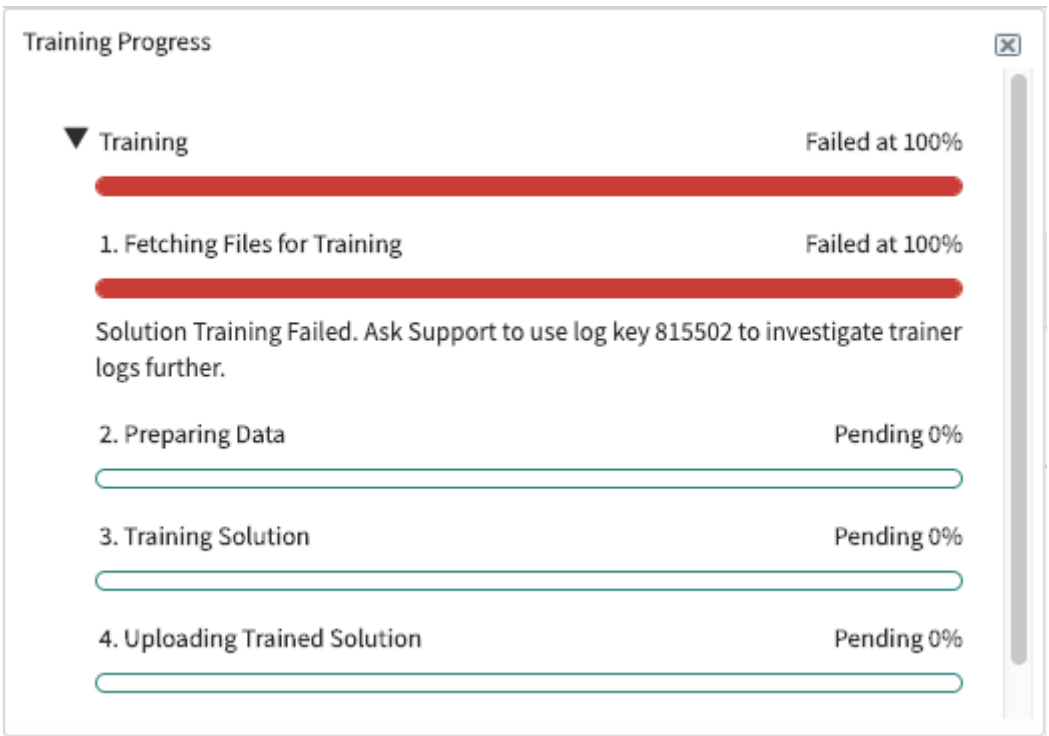
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**an.
2. Wählen Sie in der Liste der ML-Lösungen die Lösung aus, deren Fortschritt oder Statistiken Sie anzeigen möchten.
3. Klicken Sie auf den zugehörigen Link **Trainingsfortschritt anzeigen**.
   Die ML-Lösung führt automatisch Aktivitäten aus, die im Popup-Fenster „Trainingsfortschritt“ angezeigt werden.

   Das System zeigt ein Popup-Fenster mit dem Trainingsfortschritt an. Im folgenden Beispiel ist der Fortschritt fehlgeschlagen.



   Bei einem erfolgreichen Training wären alle Balken vollständig blau und der Fortschritt für jeden Schritt würde 100 % betragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Weitere Informationen finden Sie unter Ereignismanagement Ähnlichkeitsbeispiele prüfen.

Ereignismanagement Ähnlichkeitsbeispiele prüfen

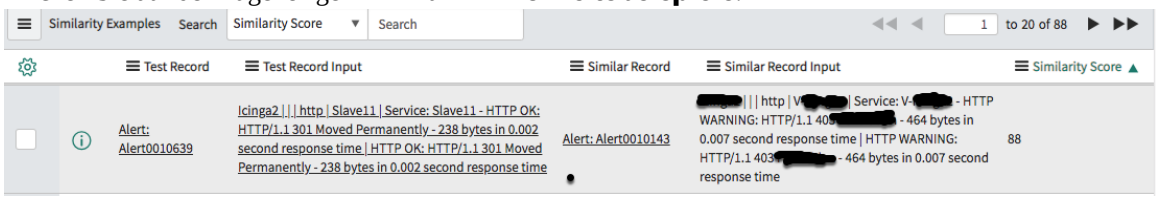
Überprüfen Sie die Ähnlichkeitsbeispiele und Punktzahlen, die das System während der Lösungsschulung bereitstellt, um den Vergleich des ausgewählten Warnungsdatensatzes mit vorhandenen Warnungsdatensätzen zu überprüfen. Beispielsweise können Sie den Schwellenwert der Ähnlichkeitspunktzahl ändern, um die Genauigkeit Ihrer Ähnlichkeitsempfehlungen zu erhöhen.

Vorbereitungen
Ähnlichkeitslösung in einem ServiceNow Rechenzentrum trainieren Weitere Informationen finden Sie unter Eine Ereignismanagement Ähnlichkeitslösung erstellen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Passen Sie den aktuellen Schwellenwert an, um nützliche Ergebnisse zu erhalten. Beispielsweise hat eine niedrige Ähnlichkeitspunktzahl mehr Abdeckung, aber weniger Genauigkeit.

Prozedur
1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**an.
2. Suchen Sie Ihre Lösung in der Liste der ML-Lösungen, und klicken Sie auf das Informationssymbol ( ).
3. Klicken Sie auf **Datensatz öffnen**.
4. Klicken Sie auf den zugehörigen Link für **Ähnlichkeitsbeispiele**.



5. Überprüfen Sie die Ähnlichkeitsbeispiele und ihre Schwellenwert-Punktzahlen, um das Niveau der Genauigkeit und Abdeckung zu bestimmen, die auf die Ergebnisse der Lösungsähnlichkeit angewendet werden sollen.
   Je höher die Ähnlichkeitspunktzahl ist, desto präziser ist sie und desto weniger Abdeckung bietet sie. Je niedriger die Ähnlichkeitspunktzahl ist, desto mehr Abdeckung und desto weniger Präzision bietet sie.
6. Bestimmen Sie abhängig von Ihrer Überprüfung, ob der Schwellenwert für die Ähnlichkeitslösung erhöht oder verringert werden soll.

   Die Lösung gibt nur Ähnlichkeitsergebnisse zurück, deren Punktzahl über dem Schwellenwert liegt. Wenn der aktuelle Schwellenwert keine nützlichen Ergebnisse liefert, passen Sie den Schwellenwert an.

7. Navigieren zu **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**an.
8. Suchen Sie in der Liste der ML-Lösungen Ihre Lösung, und klicken Sie auf das Referenzsymbol ( ).
9. Klicken Sie auf **Datensatz öffnen**.
10. Geben Sie im Abschnitt „Lösungsstatistiken“ im Feld **Schwellenwert für Ähnlichkeitspunktzahl** einen neuen Wert ein.
    Angenommen, die aktuelle Punktzahl beträgt 80. Basierend auf Ihrer Ähnlichkeitsbeispielüberprüfung möchten Sie das Feld möglicherweise aktualisieren, indem Sie eine höhere Punktzahl von 90 eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch werden weniger Ergebnisse zurückgegeben, aber diese sind dem geprüften Warnungsdatensatz ähnlicher. Eine niedrige Ähnlichkeitspunktzahl hat mehr Abdeckung, aber weniger Genauigkeit.

11. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
Ihre Lösung verwendet den neuen Ähnlichkeitsschwellenwert. In dem Beispiel gibt die Lösung nur Ähnlichkeitsergebnisse zurück, deren Punktzahl über 90 liegt.

Lösungsversion Ereignismanagement aktivieren

Das System aktiviert die neueste Version der Lösung, Sie können jedoch auch eine zuvor trainierte Lösungsversion von Ereignismanagement aktivieren, wenn sie angemessener ist.

Vorbereitungen

Da Sie möglicherweise mehrere Lösungen erstellt haben, können Sie die Lösung aktivieren, die am besten geeignet ist.
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**an.
2. Klicken Sie in der Liste der ML-Lösungen auf das Referenzsymbol (ⓘ) für die trainierte Lösung, die Sie aktivieren möchten.
3. Klicken Sie auf **Datensatz öffnen**.
Sie können der Lösung mithilfe der Eigenschaft `evt_mgmt_similarity_solution_title` einen Titel zuweisen. Der Standardwert ist `ml_x_global_alert_similarity`. Diese Eigenschaft ändert den Wert im Feld **Lösungsname**.
4. Klicken Sie im Lösungsdatensatz auf **Aktivieren**.
Das System aktiviert diese Lösungsversion und deaktiviert jede andere Lösungsversion.

Eigensystemüberwachung für Ereignismanagement

Verwenden Sie die Ereignismanagement Eigensystemüberwachung zur Nachverfolgung von Ereignismanagement Merkmalen und Problembehebung.

Überwachen Sie Ereignismanagement, um Probleme zu erkennen und zu beheben

Aktivieren Sie die Eigensystemüberwachung, um Systemprobleme Ereignismanagement zu erkennen und zu beheben. Einige Konfigurationen sind erforderlich, damit die Eigensystemüberwachung aussagekräftige Daten anzeigen kann. Nach der Konfiguration und Aktivierung der Aufgaben zeigt Service Operations-Arbeitsbereich Daten an, die nach einem wiederkehrenden Zeitplan automatisch erfasst und berechnet werden.

Hinweis: Ereignismanagement Dashboard wird für neue Instanzen im Paris Release nicht unterstützt. Instanzen, die von einem Release vor Orlando aktualisiert wurden und das Ereignismanagement Dashboard verwenden, können dies jedoch weiterhin tun.

Die Funktion „Eigensystemüberwachung“ erstellt CIs in der CMDB zur Darstellung der Komponenten der Eigensystemüberwachung. Verwenden Sie die bereitgestellten Überwachungen, um den Status von Services und Ereignismanagement Funktionen zu überwachen und nachzuverfolgen.

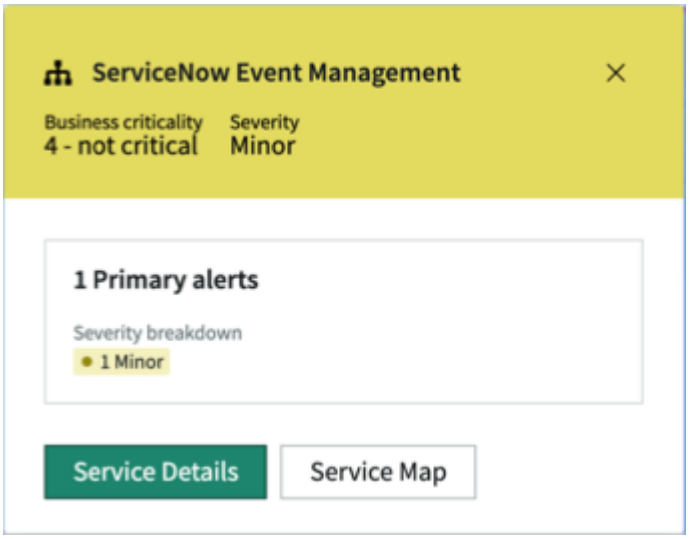
Ereignismanagement Eigensystemüberwachung kann:

- Warnungen auslösen, wenn ein Problem mit Ereignismanagement auftritt
- Zeigen Sie an **ServiceNow-Ereignismanagement** Anwendungsservices in Service Operations-Arbeitsbereich. Verwenden Sie Service Operations-Arbeitsbereich, um Warnungen nach

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservice, technischem Service und Warnungsgruppen anzuzeigen. Sie können auf eine Kachel doppelklicken, um allgemeine Informationen zum Service anzuzeigen.



- Klicken Sie auf **Servicedetails**, um Details des Services anzuzeigen.
- Klicken Sie Auf **Servicezuordnung** Dient zum Anzeigen einer Kartendarstellung von **ServiceNow-Ereignismanagement** Anwendungsservices, um die Beziehungen zwischen CIs in anzuzeigen **ServiceNow-Ereignismanagement** Anwendungsservices.

Prozess-Workflow Eigensystemüberwachung

Wenn die Eigenschaft *`Event Management – self-health monitoring`* aktiviert ist:

1. Die **ServiceNow-Ereignismanagement** Anwendungsservices werden automatisch erstellt.
2. Aufträge werden automatisch zur Ausführung von Skripts geplant, die konfigurieren, was überwacht werden muss.
3. Die Tabelle „Überwachungsstatus [em_monitor_state]“ wird nach jeder Event-Ausführung aktualisiert, die von den Konfigurationsskripts ausgelöst wird.
4. Die generierten Warnungen werden überwacht.

   Der Service zeigt den Status der überwachten Entität an. Beispielsweise werden Warnungen in angezeigt Ereignismanagement Dashboard, Service Operations-Arbeitsbereich Oder Liste aller Warnungen.

Sie können mit **Quick Response** auf der Standard-Plattform-Schnittstelle die Warnungen nach dem zugrunde liegenden Problem beheben. Details finden Sie unter Schnelle Antworten in einer Warnung anwenden.

Geplante Aufträge zur Verarbeitung von Skripts

Die standardmäßig geplanten Aufgaben, nachdem die Eigenschaft *`Event Management – self-health monitoring`* aktiviert wurde, sind:

- Die `Ereignismanagement– Integritätsüberwachung Einfügen` Geplante Aufgabe, die die Skripts ausführt.
- Die `Ereignismanagement– Integritätsüberwachung Aktualisieren` Geplante Aufgabe, die die Update-Skripts ausführt. Dieser Auftrag wird einmal pro Minute ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemüberwachung starten oder anhalten

Sie können das Starten oder Anhalten der Eigensystemüberwachung steuern, indem Sie die Eigenschaft der Eigensystemüberwachung konfigurieren. Wenn die Eigenschaft zur Selbstintegritätsüberwachung zum ersten Mal aktiviert wird, wird ServiceNow automatisch erstellt Ereignismanagement Anwendungsservices.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Eigenschaft zur Selbstintegritätsüberwachung, um Anwendungsservices und zu überwachen und nachzuverfolgen Ereignismanagement.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignismanagement-Eigenschaften**an.
2. Suchen Sie die Eigenschaft *`Enable Event Management self-health monitoring`* (*`evt_mgmt.self_health_active`*).
   Wählen Sie einen dieser Werte aus:

Aktivieren Sie die Eigenschaft Event Management-Eigensystemüberwachung

Feld	Beschreibung
Aktiviert	ServiceNow Ereignismanagement Anwendungsservices werden erstellt und so festgelegt, dass die Selbstintegrität überwacht wird. Events werden empfangen und Warnungen werden generiert.
Nur Warnungen	ServiceNow Ereignismanagement Anwendungsservices und die zugehörigen CIs werden nicht erstellt. Warnungen werden erstellt, sind jedoch nicht an ein CI gebunden.
Deaktiviert	ServiceNow Ereignismanagement Anwendungsservices sind nicht funktionsfähig. Events werden nicht empfangen, und es werden keine Warnungen generiert.

3. Klicken Sie auf **Speichern**.

Ergebnis

ServiceNow Ereignismanagement Anwendungsservices werden gemäß dem für ausgewählten Wert festgelegt *`evt_mgmt.self_health_active`*Eigenschaft.

Konfigurieren Sie Ereignismanagement– Geplante Integritätsüberwachung-Aufgabe einfügen

Bestimmen Sie, was der ist Ereignismanagement– Die geplante Aufgabe „Integritätsüberwachung einfügen“ soll überwacht werden. Nachdem der Auftrag ausgeführt wurde, können Sie anzeigen **ServiceNow-Ereignismanagement** Anwendungsservices.

Vorbereitungen

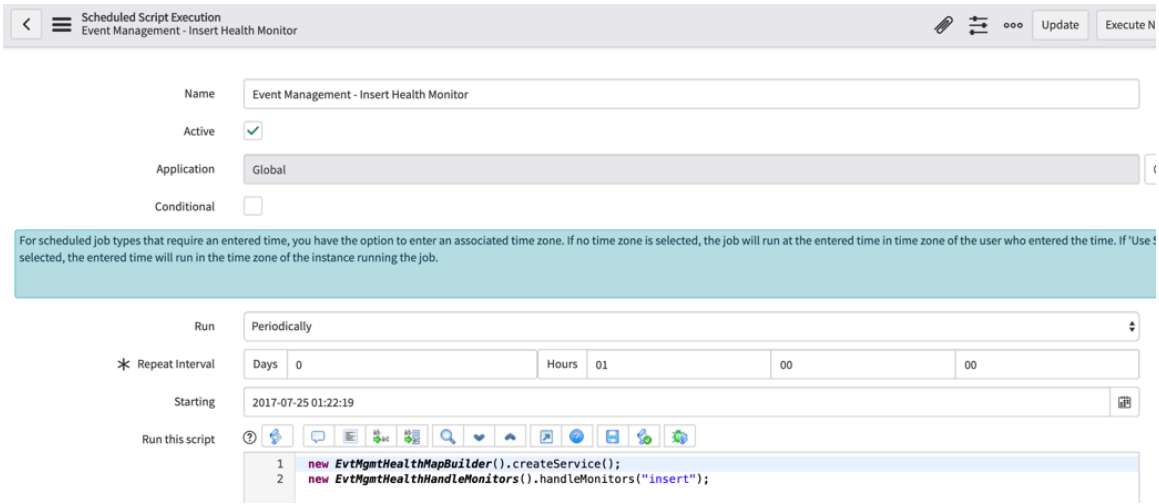
Stellen Sie sicher, dass *`Enable Event Management – self-health monitoring`*Die Eigenschaft ist auf der Seite „Ereignismanagement-Eigenschaften“ aktiviert (**Ereignismanagement** > **Ereignismanagement-Eigenschaften**) an.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**an.
2. Suchen und wählen Sie den Auftrag **Event Management - Systemüberwachung einfügen**.



3. Ändern Sie die im Feld **Dieses Skript ausführen** angegebenen Skripts , um zu festzulegen, welche Skripts überwacht werden sollen.

Eigensystemüberwachung mit Domänentrennung

Verwenden Sie die Domänentrennung, um die Anzeige der Selbstintegrität zu aktivieren Ereignismanagement Integritätsprobleme, die auf Daten, Regeln und Einstellungen aus der angemeldeten Anwenderdomäne basieren. Die ausgewählte Domäne darf keine untergeordneten Domänen enthalten.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Domänenunterstützung – Domänenerweiterungs-Installationsprogramm“ (com.glide.domain.msp_extensions.installer) aktiviert ist und dass der aktiviert ist MID-Server Sie stellen eine Verbindung zu her, ist für konfiguriert Ereignismanagement.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Eigensystemüberwachung ist domänenbezogen. Wenn das Plugin „Domänenunterstützung – Domänenerweiterungs-Installationsprogramm“ (com.glide.domain.msp_extensions.installer) aktiviert wurde, zeigt die Selbstintegrität Integritätsprobleme basierend auf Daten, Regeln und Einstellungen aus der angemeldeten Anwenderdomäne an. Wenn für eine untergeordnete Domäne keine Regeln und Einstellungen definiert sind, werden die Einstellungen des übergeordneten Elements rekursiv angewendet.

Hinweis: Um Ereignisse zur Selbstintegritätsüberwachung in der domänengetrennten Instanz zu generieren, müssen Sie die Domäne dieser generierten Ereignisse angeben. Dies erfolgt durch Angabe von sys_ID Der erforderlichen Domäne in *evt_mgmt.domain_self_monitoring*Eigenschaft.

Wenn das Plugin „Domänenunterstützung – Domänenerweiterungs-Installationsprogramm“ (com.glide.domain.msp_extensions.installer) nicht aktiviert ist, wird ein Connector oder hinzugefügt oder entfernt MID-Server Wird sofort in der Karte angezeigt.

Wenn das Plugin „Domänensupport - Domänenerweiterungs-Installer“ (com.glide.domain.msp_extensions.installer) aktiviert ist, werden die

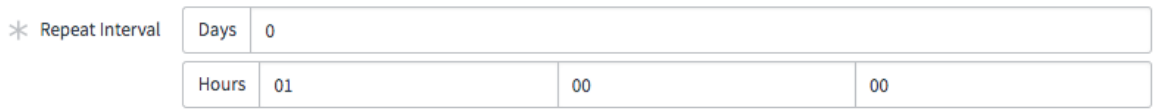
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Updates regelmäßig gemäß den Intervallspezifikationen des geplanten Auftrags Ereignismanagement„Systemüberwachung einfügen“ durchgeführt.

Prozedur

1. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**an.
2. Suchen und wählen Sie in der Liste **Zeitplan** den Auftrag Ereignismanagement„Systemüberwachung einfügen“ aus.
3. In Ereignismanagement— Integritätsüberwachungsauftrag einfügen, wählen Sie unter zugehörige Links die Option aus **Konfigurieren Sie Die Auftragsdefinition** .
4. Legen Sie die erforderliche regelmäßige Aktualisierungszeit im Feld **Wiederholungsintervall** fest, indem Sie die erforderlichen Werte angeben.
   Der Standardwert ist 1 Stunde.

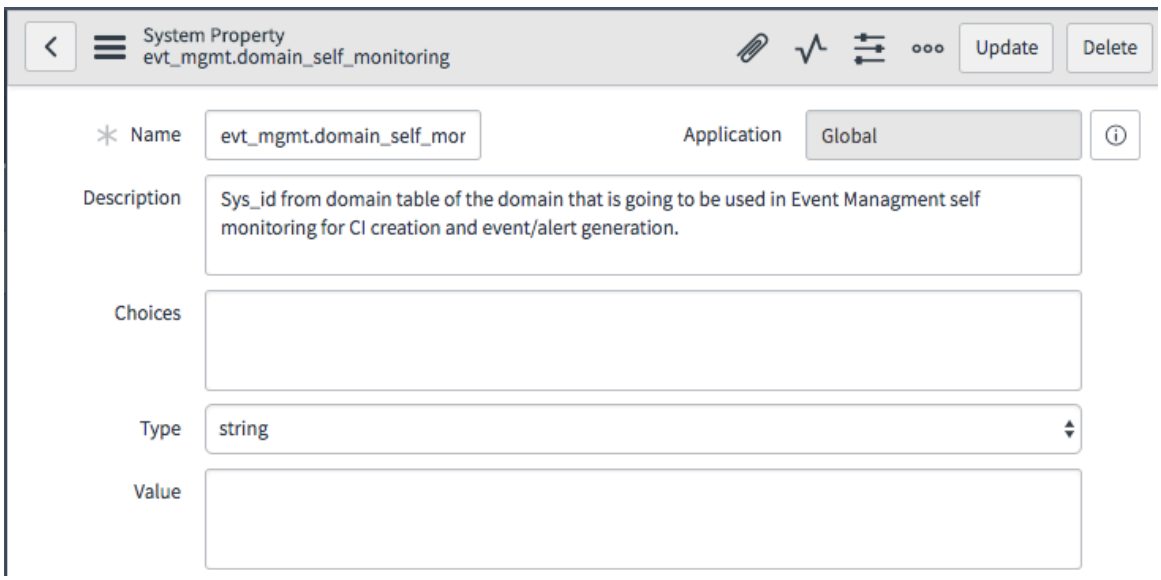


5. Wählen Sie **Aktualisieren**.

Ergebnis

Weitere Konfiguration ist für die CI-Erstellung, den Empfang von Events und die Generierung von Warnungen erforderlich. Die sys_id der Domäne muss im Feld **Wert** der Eigenschaft *evt_mgmt.domain_self_monitoring* angegeben werden.

1. Navigieren Sie zu **Systemeigenschaften** **Alle Eigenschaften** .
2. Suchen Sie nach der Eigenschaft *evt_mgmt.domain_self_monitoring*, und wählen Sie sie aus.



3. Geben Sie im Feld **Wert** die sys_id der Domäne an.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Einrichtung der Domänentrennung und grundlegende Verwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigensystemüberwachung konfigurieren

Sie können eine Eigensystemüberwachung konfigurieren, um Ereignismanagement Komponenten nachzuverfolgen und um sicherzustellen, dass sie den angegebenen Schwellenwert nicht überschreiten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „Überwachungskonfigurationen [em_monitor_conf]“ enthält die Datensätze, die bestimmen, welche Ereignismanagement Komponenten überwacht werden. Jeder Datensatz enthält das Skript für die Systemüberwachung, das für Ihre Überwachung relevant ist. Wenn Sie beabsichtigen, ein neues Systemüberwachungsskript zu erstellen, müssen Sie eine Überwachung konfigurieren, die dem Zweck des benutzerdefinierten Skripts entspricht. Sie können die Überwachungskonfigurationsdatensätze so konfigurieren, dass sie die für Sie wichtigen Elemente nachverfolgen. Beispielsweise können Sie den Schwellenwertaspekt im Datensatz `Connector's Idle state monitoring` ändern, indem Sie angeben, dass die Häufigkeit des Überwachungsauftrags 90 Sekunden anstatt 120 Sekunden beträgt.

Hinweis: Jeder der Überwachungskonfigurationsdatensätze kann deaktiviert werden.

Wenn eine Überwachungskonfiguration einen Schwellenwert angibt, bestimmt der Konfigurationswert, welcher Warnungsschweregrad angezeigt werden soll. Schwellenwerte geben die Verzögerungszeitwerte in Minuteneinheiten an.

Nach Aktivierung der Eigenschaft `Event Management - self-health monitoring` werden Aufträge automatisch zur Ausführung von Skripts geplant, die konfigurieren, was überwacht werden muss:

- Die Ereignismanagement– Integritätsüberwachung Einfügen Die geplante Aufgabe führt die Skripts aus. Bestimmen Sie, was überwacht werden muss, indem Sie das Skript in diesem Auftrag hinzufügen oder ändern, der einmal pro Stunde ausgeführt wird.
- Die Ereignismanagement– Integritätsüberwachung Aktualisieren Die geplante Aufgabe führt die Update-Skripts aus. Dieser Auftrag wird einmal pro Minute ausgeführt.

Verwenden Sie das folgende Verfahren, um zu konfigurieren, ob eine Überwachungskonfiguration ausgeführt werden kann, und die Häufigkeit der Überwachungsaufgabe festzulegen. Sie können die Schwellenwerte angeben, die bei Überschreitung eine Warnung auslösen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Eigensystemüberwachung**an.
2. Wählen Sie in der Liste „Überwachungskonfigurationen“ einen Überwachungskonfigurationsdatensatz aus, und ändern Sie das erforderliche Feld.
   Füllen Sie die Felder des Formulars aus.

Überwachungskonfigurationsformular

Feld	Beschreibung
Aktiv	Kontrollkästchen zum Aktivieren der Überwachungskonfiguration.
Überwachungsauftragshäufigkeit [Sekunden]	Häufigkeit, mit der der Überwachungsauftrag ausgeführt wird.
Schwellenwert für „Kritisch“	Jeder Punkt über dem Wert gilt als kritische Konsequenz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schwellenwert für „Schwerwiegend“	Jeder Punkt über dem Wert, jedoch unter dem Wert des **kritischen Schwellenwerts**, gilt als schwerwiegende Konsequenz.
Schwellenwert für „Gering“	Bei Überschreitung gilt der Wert als geringfügige Konsequenz.
Warnungsschwellenwert	Wenn der Wert überschritten wird, wird eine Warnung ausgegeben.

3. Klicken Sie auf **Aktualisieren**.

Ergebnis

Die Werte im geänderten Datensatz der Überwachungskonfiguration werden mit den tatsächlichen Werten verglichen, wie sie in empfangenen Events auftreten. Warnungen werden gemäß den Konfigurationseinstellungen erstellt.

Example:

Beispiel 1: Verwenden Sie das folgende Verfahren, um das Feld **Kritischer Schwellenwert** der **Überwachung des Ruhezustands des Connectors** von 30 Sekunden auf 35 Sekunden zu ändern. Dieses Feld bestimmt die Anzahl der Sekunden, die vergehen, bevor eine Warnung generiert wird, wenn der Leerlaufstatuswert eines **kritischen Schwellenwerts** eines Connectors überschritten wird. In diesem Beispiel wird das Feld **Kritischer Schwellenwert** von 30 Sekunden auf 35 Sekunden geändert.

1. Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration**an.
2. Wählen Sie in der Liste „Überwachungskonfigurationen“ die **Connector-Leerlaufüberwachung** aus.
3. Ändern Sie im Feld **Kritischer Schwellenwert** den Wert auf 35.
4. Klicken Sie auf **Aktualisieren**.

Ergebnis Der Schwellenwert des Felds **Kritischer Schwellenwert** wurde von 30 auf 35erhöht. Dadurch wird die Anzahl der Sekunden erhöht, die vergehen, bevor eine Warnung für diesen Schwellenwert generiert wird.

Beispiel 2: Dieses Beispiel beschreibt die Konfiguration des Schweregradschwellenwerts bei Verwendung der **Connectors-Statusüberwachung**. Die **Connector-Statusüberwachung** hat eine Konfiguration „true“ (= Wert 1) oder „false“ (= Wert 0) für den Schweregradschwellenwert. Für diese Überwachung wird für einen Schwellenwert mit dem Wert 1 dieser Schweregrad angezeigt. Nur ein Schweregradschwellenwert kann den Wert 1 haben. Dieses Beispiel geht davon aus, dass der angezeigte erforderliche Schweregrad Geringfügig ist.

1. Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration**an.
2. Wählen Sie in der Liste „Überwachungskonfigurationsliste“ **Connector-Status** aus.
3. Geben Sie im Feld **Schwellenwert für „Gering“**den Wert 1 ein.
4. Klicken Sie auf **Aktualisieren**.

Ergebnis Die Überwachung gibt eine Warnung aus, wenn der Schwellenwert des Felds **Schwellenwert für „Gering“** überschritten wird.

Nächste Maßnahme

Erstellen Sie eine benutzerdefinierte Überwachung. Eine Vorlage wird bereitgestellt, die Sie bei der Erstellung eines Skripts unterstützt, das die angegebenen Komponenten überwachen kann. Weitere Informationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Erstellen Sie eine Eigensystemüberwachung, um ein benutzerdefiniertes Skript für die Systemüberwachung zu verwenden.

Erstellen Sie eine Eigensystemüberwachung, um ein benutzerdefiniertes Skript für die Systemüberwachung zu verwenden

Sie können eine Eigensystemüberwachung erstellen, um ein benutzerdefiniertes Skript für die Systemüberwachung zur Überwachung spezifischer Ereignismanagement Komponenten zu verwenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zur Erweiterung der Eigensystemüberwachungen, die im Basissystem enthalten sind, können Sie eine Eigensystemüberwachung erstellen, um die von Ihnen angegebenen Komponenten zu überwachen. Die mit dem Basissystem bereitgestellten Eigensystemüberwachungsskripts sind in der folgenden Tabelle aufgelistet.

Eigensystemüberwachungsskripts, die mit dem Basissystem bereitgestellt werden

Systemüberwachungsskript	Verwendet von einer Überwachung für folgende Zwecke:
Verzögerung bei der Event-Verarbeitung überprüfen	Die Dauer [in Minuten] von Events überwachen, die im Status „Bereit“ blieben und nicht verarbeitet wurden.
Connector-Überwachung	Überwachung: • Gibt an, ob die Zeit, die ein Connector im Leerlauf war, den konfigurierten Schwellenwert [in Minuten] überschritten hat. • Der aktive Status von Connectors.
Status der Event-Verarbeitung abrufen	Überwachung der Zeit, in der sich die Events im Status „Bereit“ befinden. Warnungen werden gesendet, wenn diese Zeit den Schwellenwert überschreitet.
MID-Server-Schwellenwertwarnungen	MID Serverzustand überwachen. Wenn Änderungen am MID-Server-Status erkannt werden, werden Events gesendet.

Sie können Warnungsverwaltungsregeln erstellen, um auf die von der Eigensystemüberwachung erkannten Probleme zu reagieren und sie zu beheben. Warnungen werden basierend auf dem angegebenen Schweregrad und Schwellenwert generiert. Navigieren zu **Ereignismanagement** > **Administration** > **Eigensystemüberwachung** Für die Monitore, die mit der Basisinstanz bereitgestellt werden, um die durch die Selbstintegrität erkannten Probleme zu überwachen, die:

Monitor	Beschreibung
Überwachung des Connectors im Ruhezustand	Überwachung, um zu überprüfen, ob sich einer der Connectors im Ruhezustand befand und den konfigurierten Schwellenwert [in Minuten] überschritten hat. Ausgewähltes Eigensystemüberwachungsskript: Connector-Überwachung.
Connectors-Status	Überwachung zur Nachverfolgung des aktiven Status der Connectors. Wählen Sie nur einen Schwellenwert aus, um zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Monitor	Beschreibung
	konfigurieren, welcher Schweregrad aufgerufen werden soll. Verwenden Sie 1 zum Auswählen des Schwellenwertfelds oder 0, um das Schwellenwertfeld zu ignorieren. Weitere Informationen finden Sie unter Connector-Statusbeispiel. Ausgewähltes Eigensystemüberwachungsskript: Connector-Überwachung.
Verzögerung bei der Event-Verarbeitung	Die Dauer [in Minuten] von Events überwachen, die im Status „Bereit“ blieben und nicht verarbeitet wurden, Dieser Zeitraum initiiert eine Warnung für das Event, das das CI verarbeitet, mit Schweregrad gemäß den konfigurierten Schwellenwerten [Minuten]. Ausgewähltes Systemüberwachungsskript: Verzögerung bei der Event-Verarbeitung überprüfen.
Event-Verarbeitungsauftrag	Überwachung des Status der Event-Verarbeitungsaufgaben. Eine Warnung wird generiert, wenn die Leerlaufzeit eines Auftrags den konfigurierten Schwellenwert überschreitet. Ausgewähltes Systemüberwachungsskript: Event-Verarbeitungsstatus überprüfen.
MID-Server MID-Server Schwellenwertwarnungen	Überwachen MID-Server MID-Server Integrität. Events werden gesendet, wenn Probleme mit der MID-Server-Verfügbarkeit und Ressourcenschwellenwerten erkannt werden. Systemüberwachungsskript ausgewählt: MID Server-Schwellenwertwarnungen.

Hinweis: Um zu verhindern, dass eine Eigensystemüberwachung den Connector-Status erkennt, können Sie das Kontrollkästchen **Aktiv** der Überwachung jederzeit deaktivieren und dann auf **Aktualisieren** klicken.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Administration** > **Eigensystemüberwachung**, Und klicken Sie auf **Neu** .
2. Füllen Sie im Formular die Felder aus.

Überwachungskonfigurationsformular

Feld	Beschreibung
Name	Beschreibender und aussagekräftiger Name für die Überwachung.
Beschreibung	Textbeschreibung, die die Überwachung beschreibt.
Aktiv	Kontrollkästchen, um die Überwachung zu aktivieren.
Überwachungsauftragshäufigkeit [Sekunden]	Häufigkeit, mit der der Überwachungsauftrag ausgeführt werden soll. Standardwert: 120 Sekunden
Letzte Ausführung	Datum und Uhrzeit der letzten Ausführung Diese Werte werden automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Skript	Überwachungsskript. Klicken Sie auf das Suchsymbol. Die vorhandenen Skripts werden auf dem Bildschirm „Systemüberwachungsskripts“ aufgelistet, oder klicken Sie auf **Neu**, um ein benutzerdefiniertes Skript für die Systemüberwachung zu erstellen. Weitere Informationen zum Erstellen eines benutzerdefinierten Systemüberwachungsskripts finden Sie unter Schritt 3.
Hinweis: Zu allen folgenden Schwellenwertkonfigurationsfeldern: Alle überwachten Werte werden mit den Schwellenwerten verglichen. Wenn ein überwachter Wert einen Schwellenwert überschreitet, wird eine Warnung mit dem entsprechenden Schweregrad ausgegeben.	
Schwellenwert für „Kritisch“	Jeder Punkt über dem Wert gilt als kritische Konsequenz.
Schwellenwert für „Schwerwiegend“	Jeder Punkt über dem Wert, jedoch unter dem Wert des kritischen Schwellenwerts, gilt als schwerwiegende Konsequenz.
Schwellenwert für „Gering“	Bei Überschreitung gilt der Wert als geringfügige Konsequenz.
Warnungsschwellenwert	Wenn der Wert überschritten wird, wird eine Warnung ausgegeben.
Zusätzliche Informationen	Weitere Informationen zur Überwachung.

3. Zum Erstellen eines benutzerdefinierten Systemüberwachungsskripts klicken Sie im Formular „Überwachungskonfiguration“ neben dem Feld **Skript** auf das Suchsymbol, um das Skript Systemüberwachung zu öffnen, und klicken Sie auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Systemüberwachungsskript“

Feld	Beschreibung
Aktiv	Kontrollkästchen, um die Überwachung zu aktivieren.
Beschreibung	Textbeschreibung, die das benutzerdefinierte Skript beschreibt.
Name	Beschreibender und aussagekräftiger Name für das benutzerdefinierte Skript.
Skript	Benutzerdefiniertes Skript, das bei Aufruf von einer Überwachung ausgeführt wird. Eine Skriptvorlage wird als Leitfaden bereitgestellt. Sie können verwenden Eigensystemüberwachungsskripts, die mit dem Basissystem bereitgestellt werden Als Beispiele für die Erstellung des Skripts und die Verwendung von Skripteditor-Tools . Stellen Sie sicher, dass das benutzerdefinierte Skript Folgendes enthält: Führen Sie die Überwachungsfunktion aus, die entsprechend der Einstellung „Häufigkeit der Überwachungsaufträge“ `runUpdateHealthMonitorScripts(scriptId)` aufgerufen wird. Fügen Sie diese Funktion hinzu, um die Überwachungslogik auszuführen. Geben Sie die Konfigurationsfunktion an, die stündlich `runInsertHealthMonitorScripts(scriptId)` aufgerufen wird. Fügen Sie die Konfigurationslogik hinzu, und fügen Sie bei Bedarf ein CI hinzu. Geben Sie im Suchfeld des Navigationsbereichs em_monitor_state.list ein . Geben Sie in der Tabelle „Überwachungsstatus“ [em_monitor_state] die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Initialisierung des Überwachungsdatensatzes im erforderlichen Datensatz an. Verwenden Sie die Hilfsfunktionen, die in den Skripteinbindungen *`EvtMgmtHealthMonitorCommon`* und *`EvtMgmtEventAlertGenerator`* definiert sind: ○ EvtMgmtHealthMonitorCommon ○ healthMonitorCommon.shouldRun ○ healthMonitorCommon.calculateSeverity ○ EvtMgmtEventAlertGenerato ○ openAlert ○ closeAlert

Sie können die Tabelle „Überwachungskonfigurationen“ [em_monitor_conf] für die Konfiguration der Systemüberwachung, die Tabelle „Systemüberwachungsskripts“ [em_monitor_scripts] für Skripts und die Tabelle „Überwachungsstatus“ [em_monitor_state] für die Anzeige der Ergebnisse der Überwachung verwenden, wie in *`runInsertHealthMonitorScripts`* initialisiert.

Weitere Informationen zu Skripteinbindungen und APIs finden Sie unter Skripteinbindungen, die sind Mit Ereignismanagement installiert

5. Klicken Sie auf **Absenden**.

Ergebnis
Sie können eine Eigensystemüberwachung erstellen, um ein benutzerdefiniertes Skript für die Systemüberwachung zur Überwachung spezifischer Ereignismanagement Komponenten zu verwenden.

Zeigen Sie an Ereignismanagement Zuordnung von Anwendungsservices für die Selbstintegrität

Sie können anzeigen Ereignismanagement Anwendungsservices-Zuordnungen, um eine Visualisierung der Daten zu Konfigurationselementen (Configuration Items, CIs) zu erhalten, die diesen Service umfassen, sowie der Beziehungen und Verbindungen zwischen diesen CIs.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Die Ereignismanagement Die Topologiezuordnung der Anwendungsservices zeigt nur MID-Server an, die die Validierung bestanden haben, und aktive Connectors.

Warum und wann dieser Vorgang ausgeführt wird
Die Ereignismanagement Komponenten, die von den Self-Health-Anwendungsservices überwacht werden, sind in der folgenden Tabelle aufgeführt:

Komponenten, die vom Anwendungsservice Eigensystemüberwachung überwacht werden

Komponente	Was wird überwacht
Event-Connectors	Für jeden Connector:

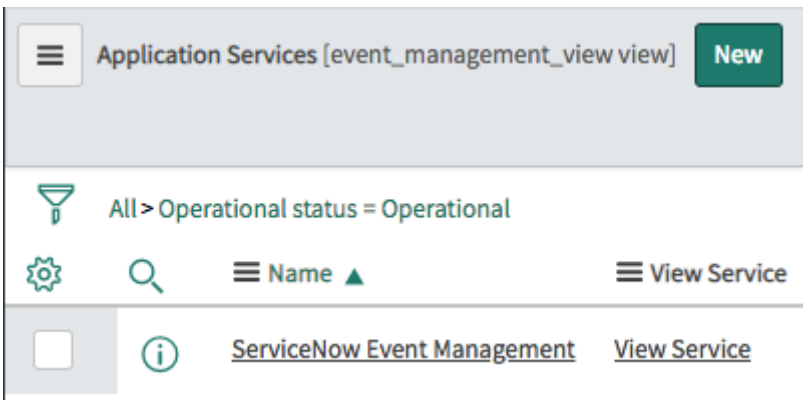
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten, die vom Anwendungsservice Eigensystemüberwachung überwacht werden (Fortsetzung)

Komponente	Was wird überwacht
	• Status: „Erfolg“ oder „Fehler“ • Verzögerung: Verstrichene Zeit seit „letzter Laufzeit“ (über dem Schwellenwert)
Event-Verarbeitungsaufträge	Für jeden Event-Verarbeitungsauftrag • Anzahl der tatsächlich ausgeführten Aufträge im Vergleich zur Anzahl der zur Ausführung konfigurierten Aufträge. • Verzögerung einer der Event-Verarbeitungsaufträge über die als Schwellenwert festgelegte Zeit. • Dauer von Events im Status „Bereit“ im Vergleich zum angegebenen Schwellenwert. • Verzögerung einer Event-Regelverarbeitung über den festgelegten Schwellenwert hinaus. Bei einer Verzögerung wird eine Warnung generiert und die Event-Regel deaktiviert.
MID-Server	MID Server, die validiert wurden, werden angezeigt. Der MID Serverstatus und die Tabelle `Ecc_agent_issue` werden überwacht. Ein Event wird ausgelöst, wenn diese Tabelle aktualisiert wird. Der MID Serverstatus wird entweder **Nach oben** oder **Nach unten** angezeigt. Informationen zur Integrität des MID-Servers finden Sie unter MID-Server-Heartbeat

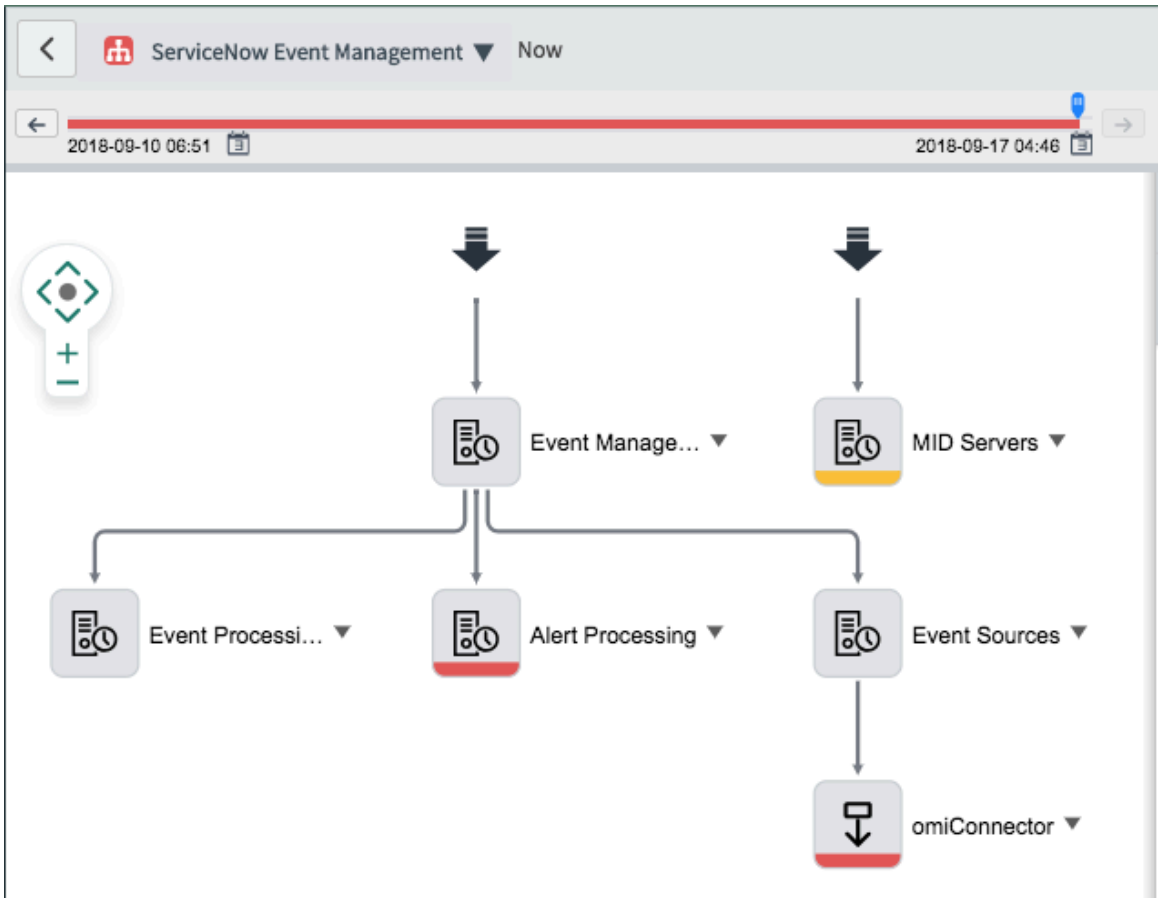
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**an.
2. Klicken Sie auf **ServiceNow-Ereignismanagement** Anwendungsservices.
3. Suchen Sie auf der Seite **Anwendungsservices** nach **ServiceNow Event Management**, und klicken Sie auf **Service anzeigen**.



Auf der Karte werden die zugehörigen MID Server und das Objekt Ereignismanagement angezeigt, wie im folgenden Bild dargestellt; diese MID Server haben den Status **NACH OBEN**. MID Server werden aktualisiert, wenn sie erstellt oder deaktiviert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Unter dem Objekt Ereignismanagement befinden sich Event-Verarbeitung, Warnungsverarbeitung und Event-Quellen (z. B. Connectors). Nur **aktive** Connectors werden angezeigt. Wenn ein Connector erstellt wird, wird der Connector erst angezeigt, nachdem er aktiviert wurde. Der Status aktiver Connectors wird aktualisiert, und der Status nicht aktiver Connectors wird nicht angezeigt.

Im vorherigen Bild wird die Integrität der Ereignismanagement Komponenten angezeigt. Die Komponente „omniConnector“ weist einen roten Balken auf, der angibt, dass eine kritische Warnung aufgetreten ist, die diesen Connector betrifft. Darüber hinaus wirkt sich diese kritische Warnung auf das übergeordnete Warnungsverarbeitungsobjekt aus, das daher einen roten Balken aufweist.

Ergebnis

Sie können das Konfigurationselement mit einer kritischen Warnung auswählen und die Auswirkung vom übergeordneten Element zum Anwendungsservice ändern.

Wartungsregeln erstellen

Verwenden Sie Wartungsregeln, um CIs im Wartungsstatus zu kennzeichnen. Im Wartungsstatus werden diese CIs von der Auswirkungsberechnung ausgeschlossen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Regeln definieren, um CIs, die den angegebenen Kriterien entsprechen, als Wartungsstatus zu kennzeichnen. Die markierten CIs füllen die Tabelle „Auswirkungswartungs-CIs“ [em_impact_maint_ci].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Beim Ausführen von Wartungsregeln wird der Status „cmdb_ci“ übereinstimmender CIs nicht geändert. Übereinstimmende CIs werden jedoch in der Tabelle „em_impact_maint_ci“ von diesen Regeln gekennzeichnet, und dieser Status wird für Auswirkungs- und Warnungsberechnungen berücksichtigt.

Das Feld, das von dieser Regel als im Wartungsstatus gekennzeichnet ist, ist das CMDB-Statusfeld.

Hinweis: Zum Aktivieren einer Wartungsregel wählen Sie das Feld **Aktiv** in der Wartungsregel aus. Deaktivieren Sie das Feld **Aktiv**, um eine Wartungsregel zu deaktivieren.

Die mit der Wartungsregeln bereitgestellten Skripts sind:

Standard-Wartungsregel	Beschreibung
CI im Change-Zeitfenster	Wenn das CI ein aktives Change-Zeitfenster hat, werden die übereinstimmenden CIs als im Wartungsstatus gekennzeichnet. Die Regel führt eine Abfrage für die Change-Anforderungstabelle [change_request] aus, um zu bestimmen, ob die Regel angewendet wird. Alle diese Bedingungen in der Tabelle „change_request“ müssen erfüllt sein: • **Status** ist eine der folgenden Optionen: Geplant, Implementieren, In Bearbeitung oder Offen/Neu (Status in (-2, -1, 1, 2)). • **Genehmigung** ist „Genehmigt“ (genehmigung = „genehmigt“). • Das Change-Anforderungsfenster ist aktiv, d. h. die aktuelle Zeit liegt zwischen dem **Geplanten Startdatum** und dem **Geplanten Enddatum**, oder die aktuelle Zeit liegt zwischen dem **Tatsächlichen Startdatum** und dem **Tatsächlichen Enddatum**. • Der Change-Anforderungsdatensatz ist kein Wartungsdatensatz (on_hold = „false“). **Hinweis:** Alle diese Bedingungen müssen vorhanden sein, damit das CI von dieser Regel in den Wartungsstatus versetzt wird. Beispiel: Wenn der **Status** des Change-Anforderungsgenehmigung Change wartet auf Genehmigung ist, wird die Änderung der Tabelle „em_impact_maint_ci“ hinzugefügt.
Wartungsstatus des CIs	CIs, deren CMDB-Statusfeld **In Wartung** ist, werden von dieser Regel als im Wartungsstatus gekennzeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Wartungsregel	Beschreibung
	Standardmäßig sind stillgelegte CIs nicht in CIs enthalten, die sich **In Wartung** befinden. So schließen Sie stillgelegte CIs ein: **1.** Navigieren Sie zu **Alle Eigenschaften**. **2.** Wählen Sie **Neu**. **3.** Konfigurieren Sie die *evt_mgmt.maintenance_rule_include_retired*Eigensc mit **Wert = true**. **Hinweis:** Das Einbeziehen von Tausenden stillgelegter CIs kann die Systemleistung beeinträchtigen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Wartungsregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Spaltenüberschrift	Beschreibung
Name	Der Name der Wartungsregel.
Aktiv	Wählen Sie diese Option, um die Wartungsregel zu aktivieren.
Erweitert	Wählen Sie diese Option, um die Anzeige des optionalen Skriptabschnitts zu aktivieren.
Beschreibung	Informationen, die diese Wartungsregel beschreiben.
CIs kennzeichnen, die auf diesem Host ausgeführt werden	Wählen Sie diese Option, um alle Anwendungen, die auf dem erkannten Host ausgeführt werden, als in Wartung befindlich zu kennzeichnen.
Tabelle	Wählen Sie die Tabelle aus, die das erforderliche CI enthält.
Filter	Legen Sie fest, wie die Daten ausgewählt werden.
CI-Feldname	Wählen Sie das CI aus der Liste aus. Die Liste wird entsprechend Ihrer Auswahl im Feld **Tabelle** ausgefüllt. Wenn eine CMDB-Tabelle oder eine von CMDB abgeleitete Tabelle ausgewählt wurde, geben Sie sys_id für den **CI-Feldnamen** an. Andernfalls geben Sie das erforderliche CI-Feld an, das Sie verwenden möchten. Siehe Beispiele.

4. Klicken Sie auf **Absenden**.

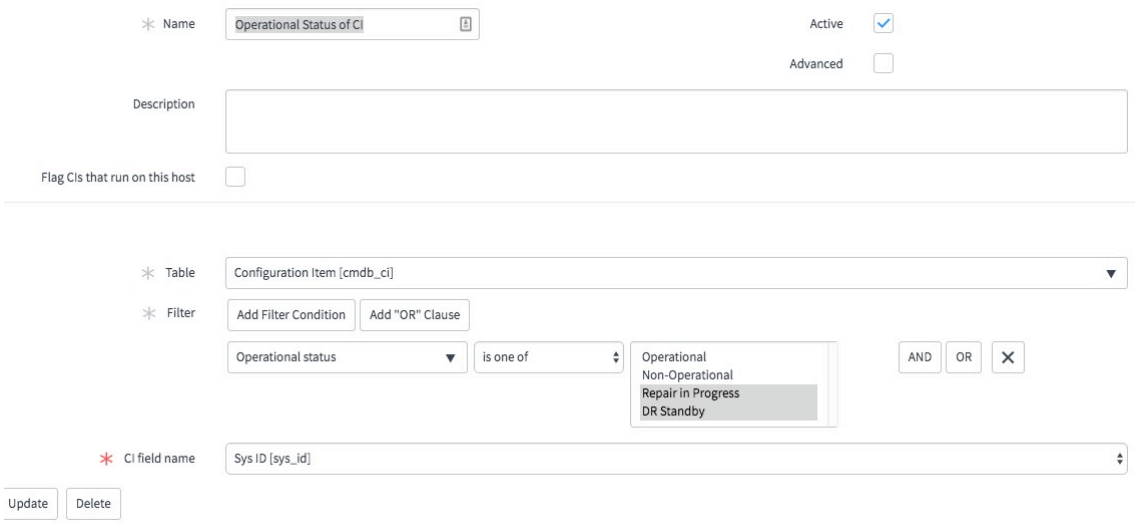
Example:

Beispiel für eine Wartungsregel, die eine CMDB-Tabelle verwendet.

Automatische Übersetzung

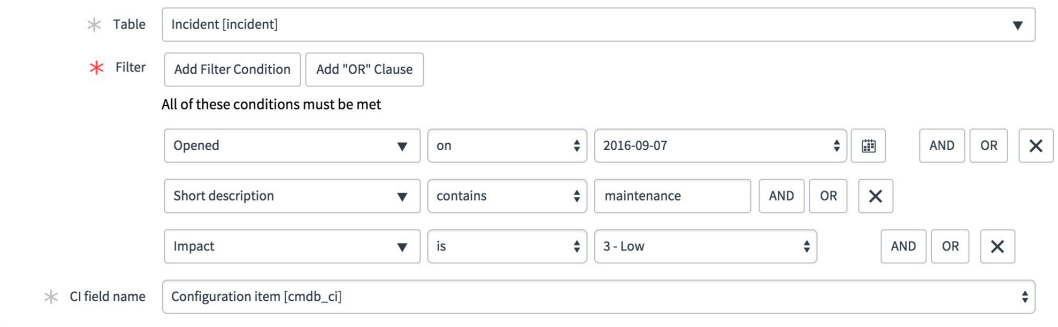
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angenommen, ein Unternehmen definiert ein CI als in Wartung, wenn der Betriebsstatus des CIs entweder **Reparatur in Bearbeitung** oder **DR-Standby** lautet.



Beispiel für eine Wartungsregel, die eine andere als eine CMDB-Tabelle verwendet.

Angenommen, ein Unternehmen verwendet Incident-Datensätze zur Nachverfolgung der Wartung. Jede Wartungsanforderung wird in einen Incident übersetzt, wenn sie eine Beschreibung hat, die mit „CI-Wartung wird durchgeführt“ beginnt. Solange der Status eines solchen Incidents offen ist, gibt dieser Status an, dass die Wartung in Bearbeitung ist. Geben Sie für das Feld **CI-Feldname** einen CI-Namen aus der ausgewählten Tabelle an, in diesem Fall **Incident**.



Beispiel für eine Wartungsregel, die die erweiterte Skriptfunktion verwendet.

Wählen Sie auf der Seite „Wartungsregel“ die Option **Erweitert**. Passen Sie das bereitgestellte Beispielskript an:

```
var now_GR = new GlideRecord('cmdb_ci');
gr.addQuery('name', 'your_name_here');
gr.query();
while (gr.next()){
 result.push(gr.sys_id +'');}
```

Der Rückgabewert für dieses Beispielskript ist eine Textzeichenfolge, die ein Array von CI-IDs darstellt, z. B. [„sys_id1“, „sys_id2“, „sys_id3“].

Sie können dieses Skript als Beispiel verwenden, um Ihr eigenes benutzerdefiniertes Skript vorzubereiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
(function findCisInMaint(){
var result = [];


//Your code goes here, this is an example of setting CIs in maintenance
var gr = new GlideRecord('cmdb_ci');
gr.addQuery('name', 'your_name_here');
gr.query();
while (gr.next()){
 result.push(gr.sys_id +''); //The array should be a string array, make sure to add strings
}


//Make sure to create a string representation of the array
return JSON.stringify(result);

})();
```

Zugehörige Informationen

Funktionsweise von Warnungen mit CIs in der Wartung

Warnung in Wartung setzen

Incidents im Zusammenhang mit einer Warnung lösen

Wenn Sie einen Incident lösen, der einer Warnung zugeordnet ist, wird gemäß der Eigenschaft `evt_mgmt.incident_closes_alert` ggf. auch die Warnung geschlossen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Öffnen Sie einen Incident.
2. Klicken Sie Auf **Incident Lösen** .

   Die entsprechende Warnung wird geschlossen, gelöst oder unverändert gelassen, wie von angegeben `evt_mgmt.incident_closes_alert`Systemeigenschaft.

   Die Warnung wird möglicherweise nicht sofort geschlossen, wenn der Incident geschlossen wird. Abhängig vom Wert von `evt_mgmt.alert_rule_close_delay`Parameter, kann die Warnung 5 Sekunden nach der letzten Warnungsaktualisierung schließen. Dieser Wert (in Sekunden) wird im Parameter definiert. Um die Eigenschaft zu verwenden, müssen Sie die Eigenschaft mit demselben Namen erstellen und ihr den erforderlichen Wert zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Warnungen schließen

Schließen Sie eine Warnung durch ein Event oder eine Benutzeraktion. Beim Schließen der Warnung werden auch alle zugehörigen Incidents geschlossen, die nicht bereits gelöst oder geschlossen sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Eine Warnung kann manuell, automatisch durch ein Ereignis „Schließen“ oder „Löschen“ oder wenn ein zugehöriger Incident gelöst wird geschlossen werden. Ob die Warnung geschlossen wird, wenn der Incident geschlossen wird, wird von bestimmt `evt_mgmt.incident_closes_alert`Eigenschaft.

Wenn ein Löschereignis für eine offene Warnung ausgelöst wird, wird die entsprechende Warnung auf den Status „Geschlossen“ gesetzt. Beim Schließen der Warnung werden auch alle zugehörigen Incidents geschlossen, die nicht bereits gelöst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder geschlossen sind. Dieses Standardverhalten kann mit konfiguriert werden `evt_mgmt.alert_closes_incident`Eigenschaft.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Alle Warnungen**an.
2. Wählen Sie die Warnung aus, die Sie schließen möchten.
3. Wählen Sie im Warnungsformular aus **Schließen** .
   Die Warnung wird ohne Bestätigung geschlossen. Weist die Warnung gelöste oder geschlossene Incidents auf, dann wird dem Incident eine Arbeitsnotiz darüber hinzugefügt, dass die zugehörige Warnung geschlossen wurde.

   Wenn eine Warnung einen offenen Incident hat, der nicht mit anderen offenen Warnungen verknüpft ist, wird der Incident basierend auf entweder geschlossen, gelöst oder unverändert gelassen `evt_mgmt.alert_closes_incident`Eigenschaft.

Warnungen erneut öffnen

Weitere Events können zum erneuten Öffnen von Warnungen führen; außerdem können Sie eine Warnung erneut öffnen, indem Sie ihren Status ändern. Wenn eine Warnung erneut geöffnet wird, werden zugeordnete Incidents gemäß ihrem Status und der Eigenschaft `evt_mgmt.alert_reopens_incident` ggf. ebenfalls aktualisiert oder erneut geöffnet.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Warnung erneut geöffnet wird, wird der zugehörige Incident wie folgt verarbeitet:

- Wenn der Incident nicht `Resolved` oder `Closed` ist, wird eine Arbeitsnotiz darüber hinzugefügt, dass die zugehörige Warnung erneut geöffnet wurde.
- Wenn es sich bei dem Incident um `Resolved` oder `Closed` handelt, wird abhängig vom Wert der Eigenschaft `evt_mgmt.alert_reopens_incident` entweder der Incident erneut geöffnet, ein neuer Incident erstellt oder es wird nichts unternommen.
  - Falls er erneut geöffnet wird, werden dem Incident Arbeitsnotizen hinzugefügt.
  - Wenn ein neuer Incident erstellt wird, werden alle entsprechenden Warnungsverwaltungsregeln, Warnungsaktionsregeln und Aufgabenvorlagen auf den Incident angewendet. Wenn keine übereinstimmende Warnungsaktionsregel oder Vorlage vorhanden ist, werden Felder aus dem vorhandenen Incident in einen neuen Incident kopiert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Suchen Sie anhand der Warnungsnummer.
3. Klicken Sie im Feld **Status** auf **Erneut öffnen**.
4. Klicken Sie auf **Aktualisieren**.

Warnungseinblick-Eigenschaften

Wählen Sie diese Eigenschaften, um Warnungseinblick zu konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Die folgenden alert_insight-Eigenschaften befinden sich unter „sys_properties“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
Zeitrahmen	
evt_mgmt.alert_insight_alert_history_min	Legen Sie den Zeitrahmen (in Minuten) fest, um wiederholte und ähnliche Warnungsdaten abzurufen. Standard: 43200 (30 Tage) **Hinweis:** Warnungen werden unabhängig von ihrem Status (offen/erneut geöffnet/ fluktuierend/geschlossen) abgerufen.
evt_mgmt.alert_insight_closed_alert_window	Legen Sie den Zeitrahmen (in Minuten) fest, um bereits geschlossene Warnungen abzurufen. Es ist die Zeit nach dem Datum der letzten Aktualisierung der Warnung. Standard: 4320 (3 Tage)
Ähnlichkeit	
evt_mgmt.alert_insight_alert_same_as_filter	Diese Eigenschaft ist eine kommagetrennte Zeichenfolge, die definiert, welches der Warnungsfelder verwendet wird, um Warnungen als ähnlich zu betrachten. Standard: source,type,resource,metric_name
Zugehörige CIs	
evt_mgmt.alert_insight_related_cis_topology_levels Die Beziehungstypen sind: • CMDB-basiert (Metadatenregeln und vorgeschlagene Beziehungen) • In Anwendungsservices • Innerhalb von Warnungsgruppen	Für den Beziehungstyp „innerhalb des Anwendungsservice“ legt diese Eigenschaft die Tiefe oder die maximale Ebene der Beziehung der abgerufenen CIs fest. Standard: 3
Punktzahl	
evt_mgmt.alert_insight_group_mapping	Diese Eigenschaft legt die Punktzahl für Warnungsgruppenbeziehungen fest. Standardwert: 2
evt_mgmt.alert_insight_level_1_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 1 fest. Standard: 3
evt_mgmt.alert_insight_level_2_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 2 fest. Standardwert: 2
evt_mgmt.alert_insight_level_3_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 3 fest. Standard: 1
Maximale Anzahl zugehöriger Aufgaben	
evt_mgmt.alert_insight_max_tasks	Maximale Anzahl zugehörige Aufgaben, die für Warnungseinblick abgerufen werden sollen. Standard: 10.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berücksichtigung von Metadatenregeln

Die über- und untergeordnete Beziehung von CIs wird berücksichtigt. Abhängige Beziehungsregeln bestehen aus Hosting- und Containment-Regeln, wobei jeder Typ die Daten aus einer anderen Perspektive des CIs modelliert.

Abhängige Beziehungsregeln verwalten:

- Um auf Regeln auf Klassenebene zuzugreifen, verwenden Sie den CI-Klassenmanager. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**an.
- Verwenden Sie den Metadaten-Editor, um auf gruppierte Regeln zuzugreifen. Navigieren zu **Alle** > **Konfiguration** > **Identifikation/Ausgleich** > **Metadaten-Editor**an.

Containment-Regeln stellen die Konfigurationshierarchie der CIs dar und beschreiben, welches CI welche anderen CIs enthält.

Hosting-Regeln repräsentieren die Platzierung von CIs in einer Unternehmensdefinition und beschreiben, worauf CIs ausgeführt werden.

Ändern Sie die Warnungseinblick-Eigenschaften, um die Anzeige von Warnungsinformationen und -analysen im Bereich „Warnungseinblick“ zu konfigurieren.

Konfiguration zugehöriger CIs

Die folgenden Eigenschaften steuern, welche CMDB-Beziehungen für zugehörige CIs berücksichtigt werden sollen. Die CMDB-Beziehungen umfassen reguläre CMDB-Beziehungsregeln, Metadatenregeln (Containment-Regeln und Hosting-Regeln) und vorgeschlagene Beziehungen.

Eigenschaft	Verwendung
evt_mgmt.related_cis_get_all_relation_types	Abrufen aller Beziehungstypen, außer Metadatenregeln. Standardwert: `false`
evt_mgmt.related_cis_use_containment_rules	Verwendung von Metadaten-Containment-Regeln. Standardwert: `true`
evt_mgmt.related_cis_use_hosting_rules	Verwendung von Metadaten-Hosting-Regeln. Standardwert: `true`
evt_mgmt.related_cis_use_suggested_relations_rules	Verwendung von Regeln für vorgeschlagene Beziehungen. Standardwert: `false`
evt_mgmt.related_cis_validate_relation_rules	Diese Eigenschaft steuert, ob die Beziehung des CIs gemäß Metadatenregeln validiert werden soll. Standardwert: `true`

Punktzahl

Punktzahlen werden nach Beziehungstyp oder -tiefe konfiguriert. Punktzahlen werden kumuliert. Je höher die Punktzahl, desto relevanter ist das zugehörige CI zum aktuellen CI.

Beispiel: Für ein CI, das auf Ebene gefunden wurde `2` Im gleichen Anwendungsservice des aktuellen CI beträgt die Punktzahl `2` . Das gleiche CI befindet sich in der gleichen Warnungsgruppe, daher gibt es eine zusätzliche Punktzahl von 3. Die kumulierte Punktzahl ist daher `2 + 3 = 5`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörigkeitstyp

Die Spalte Zugehörigkeitstyp in den Registerkarten **Zugehörige Incidents**, **Zugehörige Change-Anforderungen** und **Zugehörige Probleme** zeigen den Beziehungstyp an, über den das CI der ausgewählten Warnung und das zugehörige CI verfügen.

Navigieren Sie zu , um Beziehungen zum Zugehörigkeitstyp anzuzeigen **Alle** > **Konfiguration** > **Identifikation/Ausgleich** > **Metadaten-Editor**an.

Die Beziehung zwischen über- und untergeordneten Elementen zwischen Konfigurationselementen wird berücksichtigt:

Rotieren Sie die Ereignis- und Warnungstabelle für die Bereinigung

Das Wachstum von Datentabellen beeinträchtigt die Leistung. Behalten Sie die Instanzleistung durch Rotieren der Event-Tabellen und Bereinigen der Warnungstabellen für die Beibehaltung von Status- und Warnungsverlauf bei.

Wachstum von Event-Tabellen kontrollieren

Standardmäßig verwendet die Ereignismanagement-Event-Tabelle [em_event] die Tabellenrotation. Der Zeitplan für die Tabellenrotation stellt sicher, dass neue Daten in eine der Tabellen in der Rotationsgruppe geschrieben werden. Entsprechend dem Wert der Einstellung **Basisrotation bereinigen** wird die Basistabelle gelöscht, und dann beginnt eine neue Schreibrunde für die Tabellen in einer täglichen Rotation. Standardmäßig erfolgt diese Tabellenlöschung nach sieben Rotationen.

Informationen zum Sichern von Events in einer benutzerdefinierten Tabelle finden Sie unter Ereignismanagement-Konfigurationspräferenzen.

Wachstum von Warnungstabellen kontrollieren

Standardmäßig bereinigt ein Scheduled Job die Warnungstabelle [em_alert]. Die Tabellenbereinigung wird auch für die Tabelle „Auswirkungsstatus“ und „Warnungsverlauf“ durchgeführt.

Zugehörige Informationen

Auswirkungsstatus und Warnungsverlauf löschen

Bereinigung der Warnungstabelle

Tabellenrotation

Ändern Sie die Rotation der Ereignistabelle

Tabellenrotation wird standardmäßig von Ereignismanagement verwendet, um das Wachstum von Event-Tabellen [em_event] innerhalb der Rotationstabellengruppe zu kontrollieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabellenrotation stellt sicher, dass die Ereignistabellen eine angemessene Größe erreichen.
Gemäß dem Zeitplan für jede Tabellenrotation werden neue Daten in eine der Tabellen in der Rotationsgruppe geschrieben. Eine Tabellenrotationsgruppe enthält die ursprüngliche Tabelle sowie mehrere zusätzliche Tabellen. Nachdem im Rotationsverfahren die letzte Tabelle einer Rotation geschrieben wurde, überschreibt die Rotation die erste Tabelle der Rotation. Standardmäßig ist die Tabellenrotation für Ereignismanagement das Rotieren von em_table in eine Offload-Tabelle, und die Basistabellenbereinigung erfolgt nach sieben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenrotationen. Informationen zum Sichern von Events in einer benutzerdefinierten Tabelle finden Sie unter Ereignismanagement-Konfigurationspräferenzen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Tabellenrotationen**an.
2. Wählen Sie die zu ändernde Tabellenrotationsgruppe [em_event] aus.
3. Bearbeiten Sie die erforderlichen Felder.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Tabellenrotation

Tabellenrotation anwenden

Rotieren Sie die Ereignis- und Warnungstabelle für die Bereinigung

Auswirkungsstatus und Warnungsverlauf löschen

Bereinigt automatisch veraltete Auswirkungsstatus und Warnungsverlauf aus der Datenbank, um Speicherplatz freizugeben, die Systemleistung zu verbessern und sicherzustellen, dass nur relevante Daten gespeichert werden.

Vorbereitungen

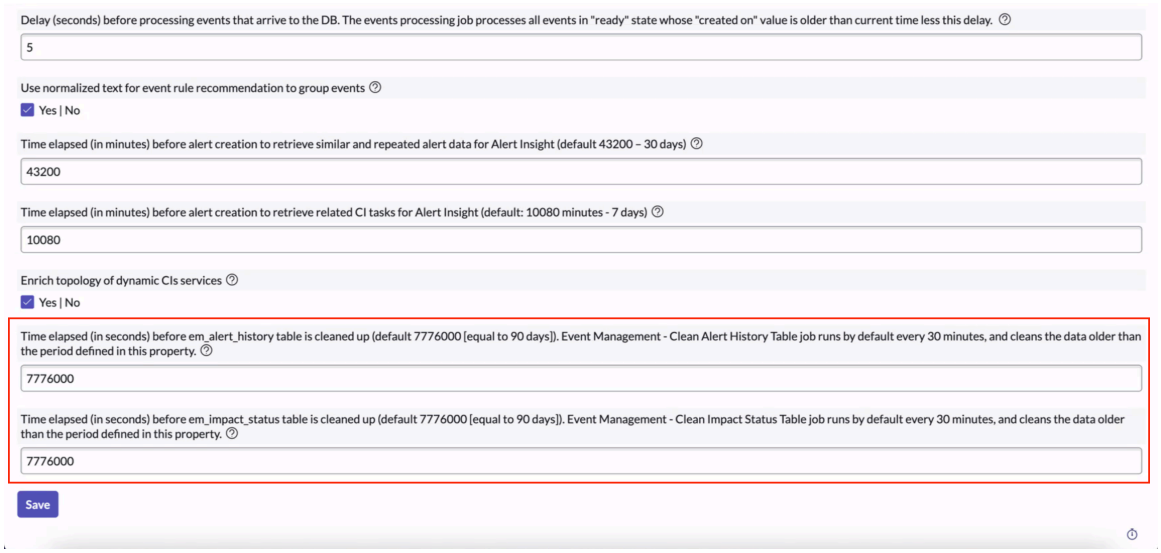
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Datensätze älter als 90 Tage sind, werden sie standardmäßig gelöscht. Wenn Datensätze für einen längeren Zeitraum aufbewahrt werden, werden größere Datenmengen gespeichert, und die Leistung kann beeinträchtigt werden. Die Datenbereinigung erfolgt durch zwei Aufgaben: Ereignismanagement – Warnungsverlaufstabelle bereinigen und Ereignismanagement – Auswirkungsstatustabelle bereinigen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**an.
2. Um den Aufbewahrungszeitraum zu verkürzen, verwenden Sie die hervorgehobenen Eigenschaften.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Rotieren Sie die Ereignis- und Warnungstabelle für die Bereinigung

Ändern Sie die Rotation der Ereignistabelle

Tabellen „Warnungsverlauf“ und „Auswirkungsstatus“ bereinigen

Bereinigung der Warnungstabelle

Tabellen „Warnungsverlauf“ und „Auswirkungsstatus“ bereinigen

Planen Sie Aufträge, um alte Warnungsdatensätze in den Tabellen „Warnungsverlauf“ [em_alert_history] und „Auswirkungsstatus“ [em_impact_status] zu markieren und zu entfernen und so zu verhindern, dass die Tabellen mit Daten überladen werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Planen Sie die folgenden Aufträge, um alte Warnungsdatensätze zu entfernen:

- **Auffüllen**: Bestimmt, wann Warnungen zum Löschen markiert werden sollen
- **Clean**: Löscht die Warnungen

Hinweis: Die Datensätze in den Tabellen [em_Alert_history] und [em_Impact_Status] werden standardmäßig nach drei Monaten gelöscht. Dies wird durch die Eigenschaften gesteuert `evt_mgmt.impact_calculation.cleanup_age_seconds.em_alert_history`Und `evt_mgmt.impact_calculation.cleanup_age_seconds.em_impact_status`. Der Standardwert ist 7.776.000 Sekunden (entspricht 90 Tagen).

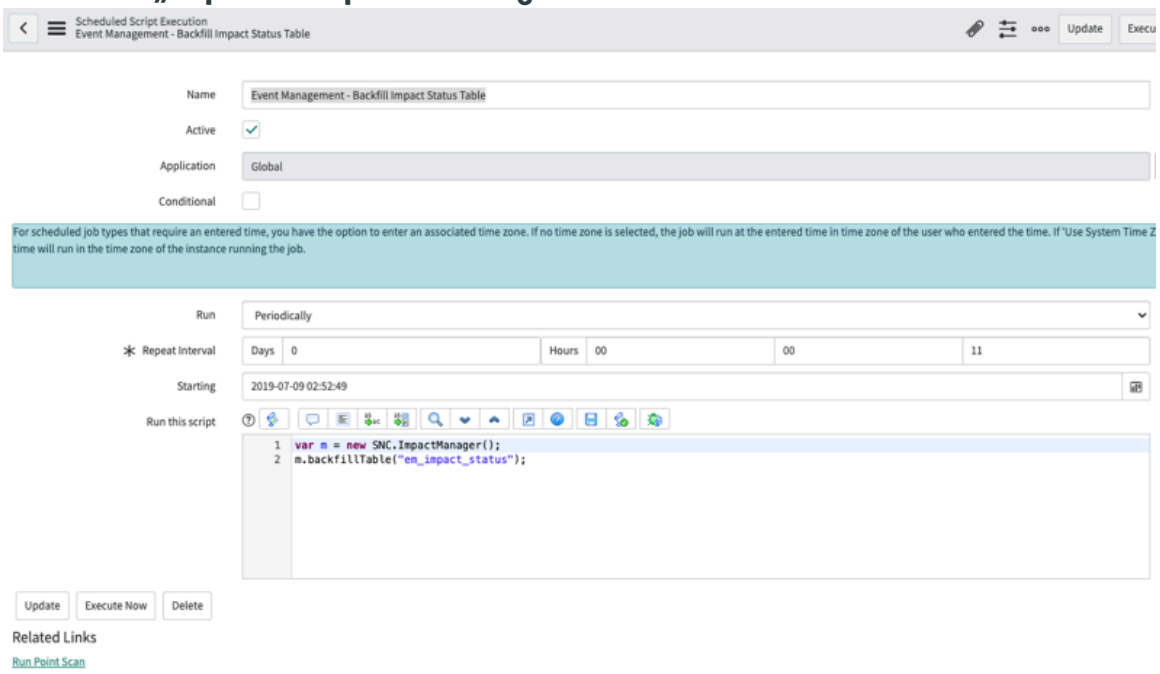
Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
   Die Seite **Scheduled Jobs** wird angezeigt.
2. So bestimmen Sie, wie oft Warnungen in der Tabelle **Auswirkungsstatus** zum Löschen markiert werden:

   a. Suchen Sie nach der Aufgabe **Event Management – Auswirkungsstatustabelle für Auffüllung** und wählen Sie sie aus.
   Die Seite **Geplante Skript-Ausführung** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Geplante Skript-Ausführung“

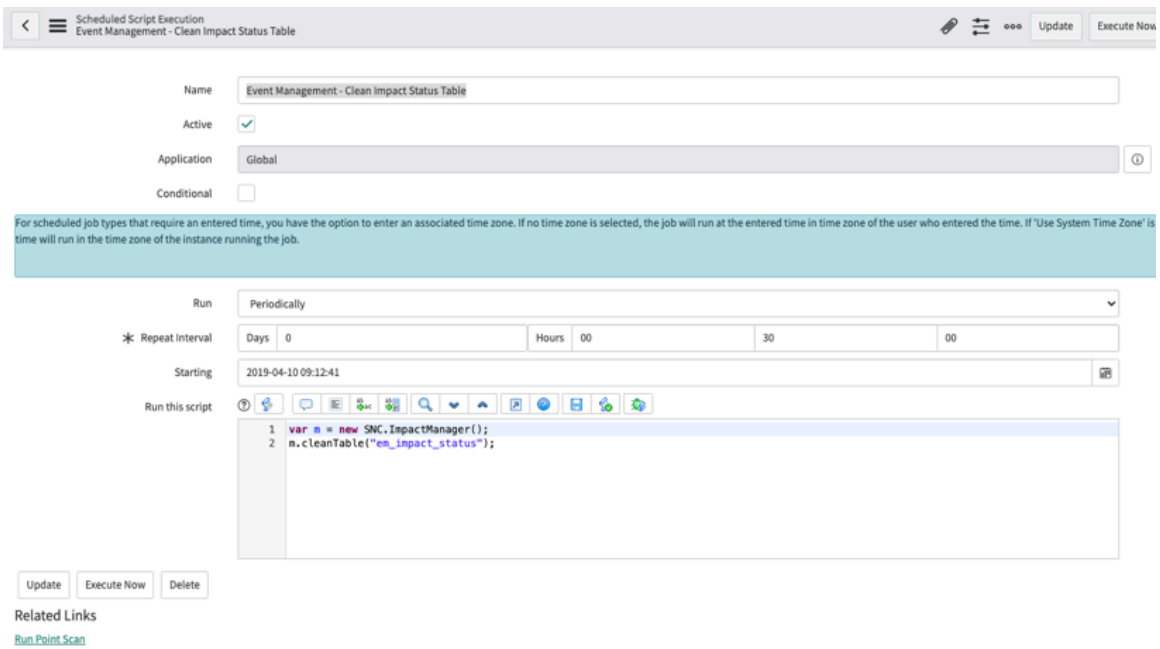


b. Konfigurieren Sie im Feld **Wiederholungsintervall**, wie oft der Auftrag ausgeführt werden soll. Um den Auftrag sofort auszuführen, wählen Sie **Jetzt ausführen** aus.

c. Wählen Sie **Aktualisieren**.

3. So entfernen Sie alte Warnungen aus der Tabelle **Auswirkungsstatus**:

a. Suchen Sie nach der Aufgabe **Event Management – Tabelle mit Auswirkungsstatus bereinigen** und wählen Sie sie aus.
Die Seite **Geplante Skript-Ausführung** wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Konfigurieren Sie im Feld **Wiederholungsintervall**, wie oft der Auftrag ausgeführt werden soll. Um den Auftrag sofort auszuführen, wählen Sie **Jetzt ausführen** aus.

c. Wählen Sie **Aktualisieren**.

4. Wiederholen Sie die Schritte 2 und 3, um die Auffüll- und Bereinigungsaufträge für die **Tabelle „Warnungsverlauf“** auszuführen.

Bereinigung der Warnungstabelle

Die Funktion „geplante Aufgaben“ führt ein Skript aus, um Warnungen in der Tabelle „Warnungen“ [em_Alert] automatisch zu schließen, die bestimmte Bedingungen erfüllen, wodurch das Warnungsrauschen reduziert und das System sauber und effizient gehalten wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Event Management-Plugin aktiviert ist, wird standardmäßig ein Job zur Ausführung des Skripts `Event Management – Warnungen automatisch schließen` geplant, um Warnungen in der Warnungstabelle, die die angegebenen Bedingungen erfüllen, automatisch zu schließen. Die standardmäßige Aufbewahrungsrichtlinie für geschlossene Warnungen lautet, dass das System geschlossene Warnungen löscht, wenn sie 90 Tage lang nicht aktualisiert wurde. Weitere Informationen zur geplanten Aufgabe finden Sie unter Tabellenbereinigung .

Aufgrund des hohen Datenverkehrs zur Tabelle können Sie die Warnungstabelle [em_alert] nicht als Ganzes prüfen. Prüfen Sie stattdessen ausgewählte Felder von Interesse in der Tabelle.

Prozedur

1. Legen Sie die Tabelle auf `audit = true` fest.
2. Legen Sie `audit = true` für die relevanten Felder fest.
   Um übermäßig viele Audit-Datensätze zu vermeiden, prüfen Sie nur die Felder, die für die Prüfung erforderlich sind.

Ergebnis

Das Skript `Event Management – Warnungen automatisch schließen` wird automatisch ausgeführt und zu geplanten Zeiten wiederholt. Dabei schließt es Warnungen, die die angegebenen Bedingungen erfüllen.

Zugehörige Informationen

Rotieren Sie die Ereignis- und Warnungstabelle für die Bereinigung

Ändern Sie die Rotation der Ereignistabelle

Auswirkungsstatus und Warnungsverlauf löschen

Warnungsgruppierung

Warnungsgruppierung ist der Prozess der Organisation und Konsolidierung zugehöriger Warnungen in Sätzen basierend auf allgemeinen Merkmalen oder Kriterien. Dies hilft bei der Vereinfachung des Warnungsmanagements, indem das Rauschen reduziert wird, wodurch es einfacher wird, Probleme effizient zu priorisieren, nachzuverfolgen und zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppierte Warnungen bieten einen klareren Überblick über zugehörige Incidents und erleichtern so eine schnellere Ursachenanalyse und -Behebung.

Warnungsgruppierung verstehen

Sehen Sie sich dieses kurze Video an, um zu erfahren, wie die Warnungsgruppierung Warnungen basierend auf bestimmten Kriterien in Cluster organisiert.

Video, in dem erläutert wird, wie die Warnungsgruppierung Warnungen basierend auf bestimmten Kriterien in Cluster organisiert.

Funktionsweise der Warnungsgruppierung

Die Warnungsgruppierung verbessert die betriebliche Effizienz und optimiert das Warnungsmanagement durch Kategorisierung von Warnungen. So funktioniert es:

1. Ereigniskonsolidierung: Ereignismanagement Sammelt Warnungen aus mehreren Quellen und bietet eine zentrale Ansicht von Benachrichtigungen und Warnungen. Diese Konsolidierung ermöglicht es Teams, Warnungen effizienter zu verwalten und kritische Probleme einfacher zu erkennen.
2. Kontextbezogene Anreicherung: Warnungen werden mit Daten aus der Konfigurationsmanagement-Datenbank (CMDB), die detaillierte Informationen zu Anwendungen und Infrastrukturkomponenten enthält. Dieser Kontext ermöglicht es Teams, die Bedeutung von Warnungen besser zu verstehen und Antworten basierend auf ihren Auswirkungen zu priorisieren.
3. Intelligente Korrelation: Ereignismanagement Verwendet verschiedene Arten von Algorithmen für maschinelles Lernen, um zugehörige Warnungen automatisch zu gruppieren. Diese intelligente Gruppierung reduziert Warnungsrauschen durch die Kombination ähnlicher Warnungen, sodass Teams sich auf wichtige Probleme konzentrieren können, anstatt mit mehreren Benachrichtigungen überschwemmt zu werden.

Vorteile der Warnungsgruppierung

- Wird Erstellt Automatisierte Warnungsgruppen Durch Zusammenfassen von Warnungen basierend auf vordefinierten Mustern.
- Korrelation von Warnungen mithilfe von Zeitstempeln und CI-Identifizierung, um automatisierte Warnungsgruppen zu bilden.
- Wird Gebildet CMDB Basierte Warnungsgruppierung Durch Korrelation von Warnungen basierend auf CI-Beziehungen in der CMDB.
- Korrelation von Warnungen basierend auf der Textähnlichkeit von Warnungen mithilfe von NLP (Natural Language Processing).

Zugehörige Informationen

Warnungsantwort wird mit automatisierter Warnungsgruppierung synchronisiert

Warnungsgruppierung und Anwendungsfälle

Warnungsgruppierungsmethoden reichen von anwenderdefinierten Ansätzen wie Manuell Und regelbasiert bis zu erweiterten, feinoptimierbaren Algorithmen, einschließlich automatisch, gemischt, textbasiert, Log Analytics und auf Netzwerkdatenverkehr basierende Gruppierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle

Typ	Beschreibung	Anwendungsfall
Log Analytics-Gruppierung	Warnungen werden basierend auf der Analyse der Protokolldaten gruppiert. Dies umfasst die Korrelation von Protokolleinträgen, um zugehörige Warnungen und Probleme zu identifizieren. Durch die Nutzung von Protokollmustern und -Sequenzen kann diese Methode komplexe, mehrstufige Probleme in der gesamten IT-Umgebung erkennen.	Ein Online-Gaming-Unternehmen verbessert die Serverstabilität durch die Implementierung proaktiver Protokoll-Analytics. Sie überwachen Protokolle von Spieleservern in Echtzeit und verwenden Analysetools, um Muster von Fehlern zu erkennen, die vor Abstürzen auftreten. Beispielsweise zeigt die Analyse, dass bestimmte Fehlermuster etwa 30 Minuten vor Serverabstürzen angezeigt werden. Durch die Einrichtung automatisierter Warnungen für diese Muster kann das Unternehmen Korrekturaktionen initiieren, z. B. das Neustarten von Services oder die Neuzuweisung von Ressourcen, bevor ein Absturz auftritt. Dieser proaktive Ansatz verhindert Unterbrechungen, minimiert Ausfallzeiten und verbessert die Gaming-Experience, indem Probleme behoben werden, bevor sie sich auf die Spieler auswirken.
Regelbasierte Gruppierung	Warnungen werden gemäß vordefinierten Regeln und Kriterien gruppiert, die von Anwendern festgelegt werden. Diese Regeln können bestimmte Bedingungen enthalten, z. B. Schwellenwerte oder Ereignistypen. Diese Methode ist effektiv für konsistente und wiederholbare Muster, erfordert jedoch die Wartung der Regeln.	In einem Rechenzentrum, das eine E-Commerce-Website verwaltet, hilft die regelbasierte Warnungsgruppierung bei hohem Datenverkehr bei Ereignissen wie Flash-Vertrieb. Warnungen zu Serverproblemen, z. B. zu hoher CPU-Auslastung, werden als übergeordnete Warnungen festgelegt. Diese übergeordneten Warnungen sind mit untergeordneten Warnungen verknüpft, die zugehörige Probleme

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
		melden, z. B. langsame Datenbankabfragen. Die Regeln stellen sicher, dass serverbezogene Warnungen mit ihren Symptomen gruppiert werden, sodass das IT-Team Probleme mit Serverüberlastung schnell identifizieren und beheben kann. Dieser Ansatz verbessert die Effizienz der Problemlösung und minimiert Ausfallzeiten.
Automatisierte Gruppierung	Erweiterte Algorithmen identifizieren und gruppieren zugehörige Warnungen automatisch basierend auf Mustern und Ähnlichkeiten in den Warnungsdaten. Diese Methode nutzt maschinelles Lernen und KI, um sich an neue und unbekannte Probleme anzupassen und proaktives Warnungsmanagement zu bieten. Ereignismanagement Gruppiert Warnungen, die ähnlich, aber nicht unbedingt identisch sind, basierend auf der Nähe zum Zeitpunkt der letzten Ereignisgenerierung. Warnungen mit demselben CI und demselben Musterbezeichner werden gruppiert. Die automatische Warnungsgruppierung besteht aus den folgenden Komponenten. • Lerner Für Warnungszusammenfassung (**Service Analytics – Warnungszusammenfassung – Lerner – Täglich**): Dieser Offline-Auftrag wird täglich ausgeführt, um	Ein großes Finanzinstitut verwendet maschinelles Lernen, um Warnungen von zahlreichen Servern und Anwendungen zu verwalten. Das System analysiert historische Warnungsdaten, um Muster zu erkennen, z. B. Datenbankserverfehler, die häufig von Client-Verbindungsfehlern begleitet werden. Dann werden zugehörige Warnungen automatisch zusammen gruppiert. Wenn beispielsweise eine neue Datenbankserverfehlerwarnung erkannt wird, wird sie mit vorherigen Verbindungsfehlerwarnungen gruppiert. Diese automatisierte Gruppierung hilft IT- und Sicherheitsteams, Probleme schnell zu identifizieren und zu beheben, die Reaktionszeiten zu verbessern und Ausfallzeiten zu reduzieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
	vergangene Warnungen zu verarbeiten und statistische Analysen durchzuführen, um Warnungsmuster zu erstellen. Details finden Sie unter Konfigurieren Sie die musterbasierte Warnungsgruppierung. • Auftrag zur Zusammenfassung von Warnungen in Echtzeit (**Service Analytics gruppiert Warnungen mit RCA/ Warnungszusammenfassung**): Dieser Auftrag wird jede Minute ausgeführt, um Warnungszusammenfassungsgruppen basierend auf Warnungsmustern, CMDB-Beziehungen, Textähnlichkeit, anwenderdefinierten Warnungs-Clustering-Tags und Netzwerkverkehrsverbindung zwischen Prozessen zu generieren.	
Gemischte Gruppierung	Die gemischte Gruppierungsmethode kombiniert Warnungen mit mehreren Gruppierungsstrategien, z. B. CMDB-basierte Gruppierung und Tag-basierte Gruppierung, in einer einzigen, zusammenhängenden Gruppe. Sie nutzt die Stärken jeder Strategie, um Warnungsrauschen zu reduzieren, die Warnungskorrelation zu verbessern und die wahre Ursache von Incidents hervorzuheben. • CMDB-basierte Gruppierung: Warnungen werden basierend auf CI-Beziehungen (Configuration Item) und Abhängigkeiten aus der Configuration Management Database (CMDB) gruppiert. Dieser Ansatz stellt	Anwendungsfall für CMDB-basierte Gruppierung: Ein Telekommunikationsunternehmen verwendet CMDB-Daten, um Warnungen im Zusammenhang mit seiner Netzwerkinfrastruktur zu verwalten. Warnungen im Zusammenhang mit einem bestimmten Netzwerkrouter und seinen verbundenen Geräten werden basierend auf ihren CMDB-Beziehungen gruppiert, sodass das Netzwerkteam alle zugehörigen Probleme sehen und die Ursache effizient beheben kann. Anwendungsfall für Tag-Cluster-Gruppierung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
	sicher, dass Warnungen im Zusammenhang mit bestimmten Infrastrukturkomponenten oder -Services gruppiert werden, was ein kontextbezogenes Warnungsmanagement bietet. • Tag-Clustergruppierung: Warnungen werden kategorisiert und mithilfe von Tags oder Bezeichnungen gruppiert, die allgemeine Attribute darstellen, z. B. Anwendung, Servertyp oder geografischer Standort. Diese Methode ermöglicht eine flexible und dynamische Gruppierung basierend auf sich entwickelnden Tagging-Strategien.	Eine Organisation ohne CMDB verwaltet einen Linux-Server, auf dem verschiedene Services ausgeführt werden. Das IT-Team verwendet einen **Knoten** Feld in jeder Warnung, um den Server zu identifizieren, und sie gruppieren alle Ereignisse im Zusammenhang mit Services auf demselben Server basierend auf diesem Knotenwert. Beispielsweise gruppieren sie Warnungen wie Service A ausgefallen und Service B hohe CPU-Auslastung zusammen, wenn sie denselben Knotenwert haben. Dieser Ansatz hilft dem IT-Team, serverbezogene Probleme effizienter zu beheben. Durch Clustering von Warnungen für denselben Knoten, dieselbe Anwendung oder dieselbe IP-Adresse optimiert das Team seine Antwortbemühungen und löst Probleme effektiver, auch ohne CMDB.
Netzwerkdatenverkehr-basierte Gruppierung	Die netzwerkbasierte Warnungsgruppierung analysiert Netzwerkverbindungen zwischen Prozessen auf Hosts, um zugehörige Warnungen zu identifizieren. Diese Methode nutzt Servicekandidaten, die durch ML Service Mapping erkannt wurden, und stellt sicher, dass Warnungen im Zusammenhang mit Netzwerkdatenverkehrsproblemen gruppiert werden, um einen besseren Kontext und eine schnellere Lösung von Warnungen zu gewährleisten.	Eine cloudbasierte E-Commerce-Plattform erlebt Transaktionsverlangsamungen, was zu Verzögerungen bei der Zahlungsverarbeitung führt. Herkömmliche Warnungen generieren separate Warnungen für API-Zeitüberschreitungen, Datenbankverzögerungen und Netzwerkprobleme, was die Identifizierung der Ursache erschwert. Bei der auf Netzwerkverkehr basierenden Gruppierung werden Warnungen automatisch basierend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
		auf Prozess-zu-Prozess-Verbindungen gruppiert, die durch ML Service Mapping identifiziert wurden. Das System erkennt, dass Zahlungs-Gateway-Services, Betrugserkennung und Auftragsverarbeitung Teil desselben Servicekandidaten sind. Dies zeigt, dass ein überlasteter Betrugserkennungsprozess Transaktionsengpässe verursacht. Durch die Skalierung des Service löst das Team das Problem schnell, minimiert Ausfallzeiten und verbessert die Kunden-Experience.
Textbasierte Gruppierung	Warnungen werden gruppiert, indem der Textinhalt von Warnungen analysiert wird, um Ähnlichkeiten und zugehörige Probleme zu identifizieren. NLP-Techniken (Natural Language Processing) werden verwendet, um Gemeinsamkeiten in Warnungsbeschreibung, Metrikname und ci-Klasse zu finden, wodurch diese Methode für unstrukturierte Daten effektiv ist.	In einer Organisation, die Zoom Rooms für virtuelle Besprechungen verwendet, erhält das IT-Team zahlreiche Warnungen, wenn der Zoom Room-Server einen Ausfall aufweist. Jede Warnung kann darauf hinweisen, dass ein anderer Zoom-Raum ausgefallen ist, z. B. Zoom-Raum Nr. 10 ist ausgefallen, Zoom-Raum Nr. 11 ist ausgefallen usw. der einzige Unterschied ist die Raumnummer. Für Organisationen mit einer CMDB können diese Warnungen mithilfe von CMDB-Beziehungen gruppiert werden, da das System die Warnungen basierend auf den Auswirkungen des Servers auf alle zugehörigen Zoom-Räume korrelieren kann. Für Organisationen ohne CMDB jedoch textbasierte Gruppierung Kann sein Verwendet. Das System wendet die Verarbeitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
		in natürlicher Sprache an, um Warnungen mit ähnlichen Beschreibungen zu gruppieren, sodass das IT-Team schnell erkennen kann, dass mehrere Zoom-Räume von demselben zugrunde liegenden Serverproblem betroffen sind. Dieser Ansatz ermöglicht es dem IT-Team, die Ursache des Problems effizient zu beheben, Ausfallzeiten zu reduzieren und die Reaktionszeiten zu verbessern.
Manuelle Gruppierung	Anwender wählen zugehörige Warnungen manuell aus und gruppieren sie basierend auf ihrer Kompetenz und ihrem Verständnis des Systems. Dieser Ansatz ermöglicht eine präzise Steuerung, kann jedoch zeitaufwändig sein und automatisierte Korrelationen möglicherweise verfehlen.	Ein Systemadministrator erhält mehrere Warnungen über verschiedene Services, die auf einem einzelnen Server fehlschlagen. Der Administrator gruppiert diese Warnungen manuell, wobei er erkennt, dass sie alle mit einem einzelnen Hardwarefehler auf diesem Server zusammenhängen, und priorisiert die Behebung des Hardwareproblems, um alle Services wiederherzustellen.

Die manuelle und regelbasierte Warnungsgruppierung unterscheidet sich von der algorithmusbasierten Gruppierung hauptsächlich dadurch, wie die übergeordnete Warnung ausgewählt wird. Bei der manuellen, regelbasierten oder Protokoll-Analytics-Gruppierung wird eine der echten Warnungen als übergeordnete Warnung festgelegt. In den Modi „automatisch“, „CMDB“, „textbasiert“, „Tag-Cluster“ und „Netzwerkverkehr“ eine virtuelle Warnung, die die älteste und schwerste Warnung in der Gruppe darstellt, wird als übergeordnete Warnung erstellt.

Hinweis: In domänengetrennten Umgebungen werden Warnungsgruppen nur für Warnungen innerhalb derselben Domäne erstellt.

Informationen zu geplanten Aufgaben und Parametern finden Sie unter Geplante Aufgaben und Parameter für die Warnungsgruppierung. Detaillierte Informationen zu verschiedenen Gruppierungstypen finden Sie unter Warnungsgruppierungstypen und Erstellungsmethoden.

Geplante Aufgaben und Parameter für die Warnungsgruppierung

Automatisieren Sie die Warnungsorganisation, indem Sie Aufträge konfigurieren, um Warnungen basierend auf vordefinierten Kriterien und Parametern zu gruppieren.

Zum Gruppieren von Warnungen in den Gruppen „automatisiert“, „CMDB“, „textbasiert“, „Tag-Cluster“ und „Netzwerkverkehrskorrelation“ wird die geplante Aufgabe benannt **Service Analytics gruppiert Warnungen mit RCA/Warnungszusammenfassung** Wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

normalerweise einmal pro Minute ausgeführt. Dieser Auftrag verarbeitet die Gruppierung von Warnungen basierend auf der angegebenen Methode. Darüber hinaus können Sie mehrere geplante Aufgaben parallel ausführen, um die Warnungsgruppierung effizienter zu verwalten. Weitere Informationen finden Sie unter Führen Sie mehrere geplante Aufgaben für die Warnungsgruppierung aus.

Um zu definieren, welche Warnungen gruppiert werden, werden die folgenden Parameter verwendet:

- *sa_analytics.aggregation_enabled*: Dieser Parameter aktiviert die von der geplanten Aufgabe erstellte Warnungsgruppierung. Legen Sie die Eigenschaft fest *Enable alert aggregation for Automated, CMDB, and Text-Based groups*Bis Wahr Zum Aktivieren dieser Funktion.

  Hinweis: Diese Eigenschaft gilt auch für die Gruppierung von Tag-Clustern und Netzwerkverkehr-Korrelation.

- *sa_analytics.agg.query_dynamic_window*: Standardmäßig ist dies auf 10 Minuten (600 Sekunden) festgelegt. Definiert die maximal zulässige Zeitdifferenz zwischen den Zeiten der letzten Ereignisgenerierung von zwei Warnungen, die gruppiert werden kann.
- *sa_analytics.agg.query_max_group_lifetime*: Dieser Parameter gibt den maximalen Zeitraum von der Generierung der ersten Warnung bis zur letzten Warnung in einer Gruppe an, mit einem Standardwert von 30 Minuten (1800 Sekunden). Wenn Ereignisse mit einer Verzögerung eintreffen, die diesen Zeitraum überschreitet, wird die angezeigt *sa_analytics.agg.group_expiration_time*Der Parameter kann verwendet werden, um die Gruppierungszeit über 30 Minuten zu verlängern.

Hinweis: Einige Parameter, z. B. **sa_Analytics.agg.query_Dynamic_window** , **sa_Analytics.agg.query_max_Group_Lifetime** , Und **sa_analytics.agg.group_expiration_time** , Sind Nicht Sofort einsatzbereit bereitgestellt. Um diese Eigenschaften zu verwenden, müssen Sie Eigenschaften mit denselben Namen erstellen und ihnen die erforderlichen Werte zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Beispiel: Wie Warnungen gruppiert werden

Für die Tag-Cluster-Gruppierung werden Warnungen basierend auf dem Zeitrahmen-Parameter hinzugefügt, der in den Einstellungen für das Warnungs-Tag-Clustering definiert ist. Für die automatisierte, CMDB- und textbasierte Gruppierung des Netzwerkverkehrs werden Warnungen wie folgt zusammengefasst.

Berücksichtigen Sie die folgenden Warnungen mit demselben CI. (Alle können derselben CMDB-Gruppe hinzugefügt werden.)

- Alert1: Erste Ereignisgenerierung um 01:00:00 UHR
- Alert2: Erste Ereignisgenerierung um 01:11:00 UHR
- Alert3: Erste Ereignisgenerierung um 01:13:00 UHR
- Alert4: Erste Ereignisgenerierung um 01:16:00 UHR
- Alert5: Erste Ereignisgenerierung um 01:25:00 UHR
- Warnung 6: Erste Ereignisgenerierung um 01:34:00 UHR
- Alert7: Erste Ereignisgenerierung um 01:43:00 UHR

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alert1 und Alert2 sind aufgrund des Zeitabstands von mehr als 10 Minuten nicht gruppiert. Alert2 und Alert3 erstellen um 01:13:00 UHR eine Gruppe. Das dynamische 10-Minuten-Fenster beginnt um 01:13:00 UHR mit folgendem Vorgang:

- Alert4 wird der Gruppe um 01:16:00 UHR hinzugefügt, wodurch das 10-Minuten-Fenster neu gestartet wird.
- Alert5 und Alert6 werden der Gruppe hinzugefügt, da ihre Ereigniszeiten innerhalb des 10-Minuten-Fensters liegen.
- Alert7 wird der Gruppe nicht hinzugefügt, da er 9 Minuten nach Alert6 eintrifft und überschreitet *sa_analytics.agg.query_max_group_lifetime*Grenzwert der maximalen Gruppenlebensdauer von 30 Minuten ab der ersten Gruppenerstellung (01:13:00 UHR + 30 Minuten = 01:43:00 UHR).

Hinweis: Nachdem eine Warnung erstellt wurde, wird die Korrelationslogik nur einmal angewendet. Änderungen an der Warnung nach ihrer Erstellung werden nicht erneut auf Korrelation ausgewertet. Wenn die Korrelation anfänglich nicht hergestellt wird, kann die Warnung später noch einer Gruppe hinzugefügt werden, aber nur, wenn eine neue eingehende Warnung übereinstimmt und die Gruppierungslogik auslöst.

Konfigurieren Sie die auf geplanten Aufgaben basierende Warnungsgruppierung

Richten Sie Regeln und Parameter ein, um zugehörige Warnungen automatisch zu gruppieren, um das Warnungsmanagement zu optimieren und das Warnungsrauschen zu reduzieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die geplante Aufgabe „Service Analytics: Warnungen mit RCA/Warnungszusammenfassung gruppieren“ hilft beim Gruppieren von Warnungen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**an.
2. Aktivieren Sie auf der Seite „Warnungskorrelationseigenschaften“ die relevanten Eigenschaften.
   - CMDB-Korrelation aktivieren (*sa_analytics.agg.query_cmdb_correlation_enabled*).
   - Korrelation des Netzwerkverkehrs aktivieren (*sa_analytics.agg.query_network_traffic_correlation_enabled*).
   - ML-basierte Automatisierungskorrelation aktivieren (*sa_analytics.specific_patterns_enabled*).
   - Textbasierte Korrelation aktivieren (*sa_analytics.text_based_group_enabled*).
   - Eigenschaft „Gruppieren nach“ mit kommagetrennter Liste von Feldnamen, die übereinstimmende Werte für Warnungen aufweisen müssen, damit Warnungen gruppiert werden können. Die Eigenschaft kann Warnungsfeldnamen (z. B. Assignation_Group), CI-Feldnamen (z. B. Alert_cmdb_ci.location), Feldnamen für zusätzliche Warnungsinformationen (z. B. additional_info.State) oder Warnungs-Tags (z. B. t_Data_Center) enthalten. Wenn die angegebenen Feldwerte zwischen Warnungen übereinstimmen, können diese Warnungen gruppiert werden (*sa_analytics.agg.group_alert_with_same_group_by_fields*).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Maximale Anzahl von Beziehungen zwischen CIs in einer Topologie, die eine CMDB-Gruppe bilden (*sa_analytics.agg.query_cmdb_graph_walk_nodes*).
- Alle CMDB-Beziehungen für CMDB-Gruppenkorrelation verwenden (*evt_mgmt.related_cis_get_all_relation_types*).

3. Wählen Sie **Speichern**.

   Um Warnungen ohne CI als textbasierte oder ML-basierte Gruppen zu gruppieren, legen Sie fest *sa_analytics.enable_no_ci_grouping*Bis `Wahr` . Stellen Sie sicher, dass der Funktionsbezeichner sowohl den Knoten als auch den Metriknamen enthält. Weitere Informationen zum Konfigurieren des Feature-Bezeichners finden Sie unter Geben Sie Musterbezeichnerattribute für die Warnungsgruppierung an, und verwalten Sie sie.

4. **Wahlweise:** Festlegen *evt_mgmt.alert_groups_reasoning.enable_worknotes*Bis `Keine` Um zu verhindern, dass Arbeitsnotizen zur Gruppenbegründung angezeigt werden.

   (Optional) Standardmäßig wird im eine Arbeitsnotiz angezeigt **Aktivitäten** Registerkarte, wenn eine Gruppe erstellt oder aktualisiert wird, mit dem Gruppierungsgrund.

Zugehörige Informationen

Automatisierte Warnungsgruppierung

CMDB Basierte Warnungsgruppierung

Textbasierte Warnungsgruppierung

Warnungsgruppierung des Tag-Clusters

Führen Sie mehrere geplante Aufgaben für die Warnungsgruppierung aus

Führen Sie mehrere geplante Aufgaben parallel zu Gruppenwarnungen aus. Dies trägt dazu bei, eine Überlastung des Systems bei Überspannungen (Warnungsstürme) zu verhindern.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die aktuelle geplante Aufgabe wird mit einem einzelnen Thread ausgeführt. Bei Warnungsstößen (Warnungsstürme) dauert die Verarbeitung erheblich länger. Um diese Auswirkung zu beheben, können jetzt mehrere Aufgaben Warnungen innerhalb der geplanten Aufgabe verarbeiten. Dies verbessert die Skalierbarkeit und verbessert die Gesamtleistung in Zeiten mit hohem Volumen.

Die Anzahl der Aufträge, die in der Warnungsverarbeitung ausgeführt werden sollen, wird in einer neuen Eigenschaft definiert *sa_analytics.agg.alert_grouping.num_of_jobs*. Die Auftragsnummer wird als Parameter an die entsprechende Methode gesendet.

Hinweis: In diesem Szenario wird das Verfahren zum Erhöhen der Skalierung von „keine Skalierung“ (einzelner Auftrag) auf 2 Aufträge angezeigt.

Sie können mithilfe bestimmter Eigenschaften mehrere geplante Aufgaben effizient verwalten und parallel zur Gruppe von Warnungen ausführen. Mit diesen Eigenschaften können Sie die Gruppierungskriterien an Ihre Anforderungen anpassen und sicherstellen, dass Warnungen basierend auf Zuweisungsgruppen, Domänentrennung oder Gruppierung nach Feldern verarbeitet werden. Die verfügbaren Eigenschaften sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *sa_analytics.agg.group_alert_with_same_assignment_group_only*: Gruppiert Warnungen, die dieselbe Zuweisungsgruppe teilen. Standardmäßig ist der Wert auf „falsch“ festgelegt. Wenn Sie diese Eigenschaft auf „wahr“ festlegen möchten, erstellen Sie eine Eigenschaft mit demselben Namen, und legen Sie den Wert auf „wahr“ fest.
- *sa_analytics.agg.group_alert_with_same_domain_only*: Gruppiert Warnungen, die zu derselben Domäne gehören. Standardmäßig ist der Wert auf „wahr“ festgelegt.
- *sa_analytics.agg.group_alert_with_same_group_by_fields*: Eigenschaft „Gruppieren nach“ mit kommagetrennter Liste von Feldnamen, die übereinstimmende Werte für Warnungen aufweisen müssen, damit Warnungen gruppiert werden können. Die Eigenschaft kann Warnungsfeldnamen (z. B. Assignation_Group), CI-Feldnamen (z. B. Alert_cmdb_ci.location), Feldnamen für zusätzliche Warnungsinformationen (z. B. additional_info.State) oder Warnungs-Tags (z. B. t_Data_Center) enthalten. Wenn die angegebenen Feldwerte zwischen Warnungen übereinstimmen, können diese Warnungen gruppiert werden.

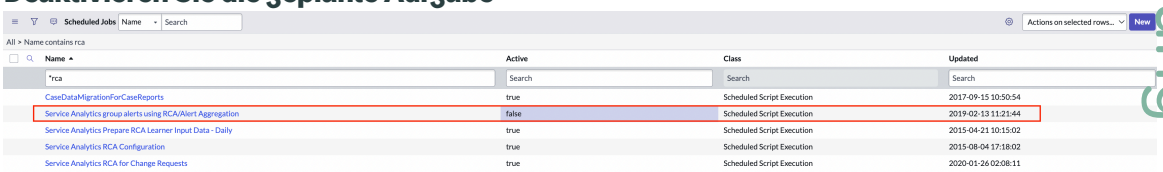
Hinweis: Um eine effiziente Skalierung zu gewährleisten, muss mindestens eine dieser Eigenschaften definiert werden, um eine Form von Trennungs- oder Gruppierungslogik festzulegen. Dies ist erforderlich, um sicherzustellen, dass alle Warnungen, die zu derselben Gruppe gehören, von bestimmten Aufträgen korrekt verarbeitet werden, wodurch eine logische Aufteilung von Warnungen erstellt wird.

Wenn nicht mindestens eine dieser Eigenschaften auf „wahr“ festgelegt wird, werden die Warnungen nicht ordnungsgemäß getrennt. Wenn Sie beispielsweise keine Gruppierungslogik definieren (beliebige Eigenschaft auf „wahr“ festlegen) und sowohl die Zuweisungsgruppe als auch die Domänentrennung auf „falsch“ festgelegt sind, funktioniert die Skalierung nicht, und alle Warnungen werden von einer einzigen geplanten Aufgabe verarbeitet.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Suchen Sie die geplante Aufgabe: Service Analytics gruppieren Sie Warnungen mithilfe von RCA/ Warnungszusammenfassung.
3. Legen Sie für alle vorhandenen geplanten Aufgaben von Service Analytics-Gruppenwarnungen mit RCA/ Warnungszusammenfassung den Wert in fest **Aktiv** Spalte bis **Falsch** .

Deaktivieren Sie die geplante Aufgabe



4. Erstellen Sie eine neue Eigenschaft *sa_analytics.agg.alert_grouping.num_of_jobs*Oder aktualisieren Sie die Eigenschaft, falls sie bereits vorhanden ist, auf die gewünschte Anzahl mehrerer geplanter Aufgaben für die Warnungsgruppierung, z. B. 2 oder 4.
5. Klonen Sie die Definition der geplanten Aufgabe aus der Tabelle „geplante Aufgaben“ [sys_Auto] auf die gewünschte Anzahl mehrerer geplanter Aufgaben für die Warnungsgruppierung.
6. Rufen Sie in den neuen Aufträgen im Abschnitt dieses Skript ausführen die neue JS-Funktion queryS0 auf (anstelle der alten Abfragefunktion ())), und übertragen Sie die Auftragsnummer als Eingabeparameter.

Hinweis: Auftragsnummern müssen bei 0 beginnen und nacheinander folgen: 0, 1, 2, 3, 4...

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Beheben Sie Hashes in den Tabellen [sa_Analytics_Status] und [sa_hash], indem Sie den frühesten Hash mit demselben Präfix auswählen, klonen und das Hash-Namenssuffix hinzufügen, z. B. „_groupingX“, wobei X die Auftragsnummer ist.

   Im Falle der Skalierung von „keine Skalierung“ (einzelner Auftrag) auf 2 Aufträge und für den Hash-Namen `Last_Alert_Process_time` , Klonen Sie es, um denselben Wert wie in beizubehalten `Last_Alert_Process_time` :

   - `Last_Alert_Process_time_grouping0`
   - `Last_Alert_Process_time_grouping1`

   Im Falle der Skalierung von „keine Skalierung“ (einzelner Auftrag) auf 4 Aufträge und für den Hash-Namen `Last_Alert_Process_time` , Klonen Sie es, um denselben Wert wie in beizubehalten `Last_Alert_Process_time` :

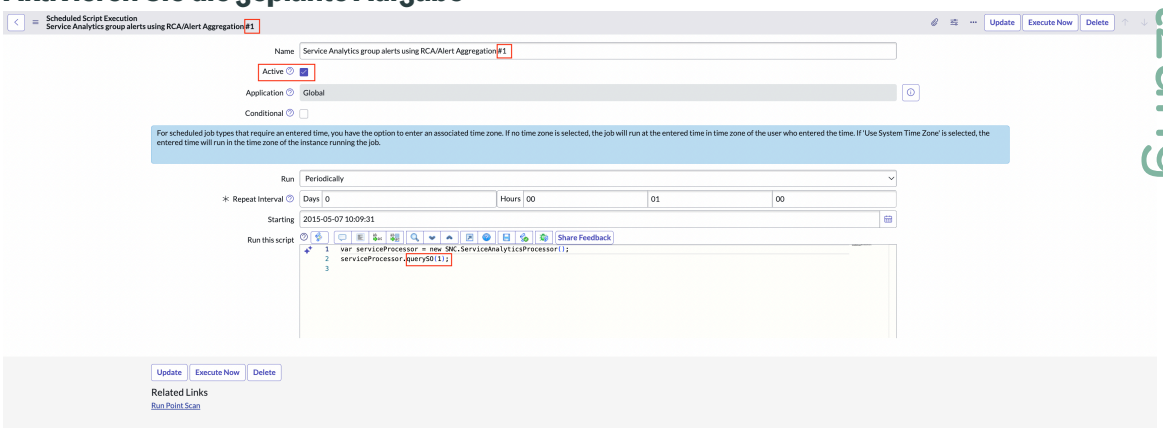
   - `Last_Alert_Process_time_grouping0`
   - `Last_Alert_Process_time_grouping1`
   - `Last_Alert_Process_time_grouping2`
   - `Last_Alert_Process_time_grouping3`

Zu klonende Hashes

Hash-Name	Tabelle
Query_Job_Last_Run	sa_Hash
Last_Alert_Process_time	sa_Analytics_Status
Last_Staging_table_Update_time	sa_Analytics_Status
Last_Staging_table_truncate_time	sa_Analytics_Status
analytics_Trigger_g1	sa_Hash

8. Aktivieren Sie die neuen Aufträge, indem Sie auswählen **Aktiv** Kontrollkästchen für jeden Auftrag.

Aktivieren Sie die geplante Aufgabe



Ergebnis

Die geplante Aufgabe „Service Analytics-Gruppenwarnungen mithilfe von RCA/ Warnungszusammenfassung“ ist so eingerichtet, dass mehrere Aufgaben gleichzeitig für die Warnungsgruppierung ausgeführt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die logische Reihenfolge der Warnungskorrelation

Verbessern Sie das Warnungsmanagement, indem Sie Anwendern die Korrelationslogik-Reihenfolge anpassen können. Mit dieser Funktion können Sie Korrelationsmethoden an ihre spezifischen Anforderungen anpassen und so die Priorisierung von Warnungen und die Effizienz der Reaktion verbessern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach der Eigenschaft *sa_analytics.agg.query.group_logic_order*.

   Der Standardwert ist „CMDB,NETWORK_TRAFFIC,TAG_BASED,PATTERN,TEXTBASE“. Dies ist eine kommagetrennte Liste der Gruppierungstypen in der Reihenfolge ihrer Ausführung.

   Hinweis: Wenn einer der Gruppierungstypen in der Eigenschaft nicht angegeben ist, muss er manuell hinzugefügt werden. Warnungskorrelationsregeln sind auslöserbasiert und werden sofort angewendet, wenn eine Warnung erstellt oder aktualisiert wird, bevor andere Gruppierungsalgorithmen verwendet werden.

   - CMDB: CMDB-Gruppierung
   - NETWORK_TRAFFIC: Gruppierung des Netzwerkverkehrs
   - TAG_BASED: Tag-Cluster-Gruppierung
   - MUSTER: Automatisierte CI-basierte Mustergruppierung
   - TEXTBASE: Textbasierte Gruppierung
3. Verwenden Sie die Eigenschaft *sa_analytics.agg.query.group_logic_order*Zum Definieren oder Ändern der Reihenfolge von Korrelationsmethoden basierend auf Ihren Einstellungen.

Zugehörige Informationen

Warnungsgruppierung und Anwendungsfälle

Filter für automatische Warnungsgruppen konfigurieren

Filtern Sie Warnungen und Warnungsgruppen, um Warnungsrauschen zu reduzieren. Nur Warnungen, die dem Filter entsprechen, werden in die Gruppe des ausgewählten Gruppentyps (Automatisiert, CMDB oder Text) aufgenommen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihr Filter Warnungen angibt, deren Konfigurationselementklasse nicht Linux ist, werden nur Warnungen mit nicht-Linux-Konfigurationselementen in der Gruppe des ausgewählten Gruppentyps eingeschlossen.

Hinweis: Nachdem der Filter erstellt wurde, gilt er nur für neue Warnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Automatischer Gruppenfilter**an.
2. Wählen Sie auf der Seite „Automatische Gruppenfilter“ entweder einen vorhandenen Gruppenfilter aus oder erstellen Sie einen neuen Filter.
3. Wenn Sie einen neuen Filter erstellen:
   a. Wählen Sie **Neu**.
   b. Geben Sie im Feld **Name** einen Namen für den Filter ein.
   c. Wählen Sie den Warnungsgruppentyp aus:
      - Automatisiert
      - Test
      - CMDB

      Sie können mehr als einen Gruppentyp mit einer einzelnen Filterbedingung zuweisen.

      Jeder Gruppentyp kann nur einen einzigen aktiven Filter aufweisen.
4. Erstellen Sie im Abschnitt **Warnungsfilter** Bedingungen, die eine Warnung erfüllen muss, damit sie in die Gruppe aufgenommen wird.
5. Speichern Sie den Warnungsgruppenfilter.
   - Wählen Sie für einen vorhandenen Warnungsgruppenfilter **Absenden** aus.
   - Wählen Sie für einen neuen Warnungsgruppenfilter **Aktualisieren** aus.

Ergebnis

Die Filterbedingung wird auf der Seite „SA-gruppierte Warnungsfilter“ in der Spalte **Warnungsfilter** angezeigt.

Warnungsgruppenfilter auf zusammengefasste Gruppen anwenden

Reduzieren Sie Rauschen, indem Sie nur zusammengefasste Warnungsgruppen suchen, die einem konfigurierten Filter entsprechen. Zusammengefasste Gruppen sind Gruppen, die für Warnungen mit identischen CIs und Musterbezeichnern erstellt wurden.

Vorbereitungen

Hinweis: Dieses Verfahren ist nur für die erweiterte Konfiguration relevant.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Automatische Gruppenfilter**an.
2. Fügen Sie auf der Seite Automatische Gruppenfilter hinzu **Aggregiert** Spalte.
   a. Wählen Sie das Symbol Liste personalisieren ( ) In der oberen rechten Ecke.
   b. Verschieben Sie **Aggregiert** Eintrag aus **Verfügbar** Liste zu **Ausgewählt** Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie die Aufwärts-/Abwärtspfeile aus, um festzulegen, wo der Eintrag **Zusammengefasst** im Formular angezeigt werden soll.

d. Wählen Sie **OK**.

3. Doppelklicken Sie auf der Seite Automatische Gruppenfilter auf den Wert in **Aggregiert** Spalte.

Zusammengefasste Gruppen gelten nur für automatisierte Warnungsgruppen. Wenn die Option „Zusammengefasst“ angezeigt wird, wurde sie automatisch für eine automatisierte Warnungsgruppe aktiviert.

Hinweis: Wenn der Wert von **Automatisiert** Feldänderungen, der Wert von **Aggregiert** Das Feld ändert sich auch. Sie können den Wert von ändern **Aggregiert** Feld nur, wenn der Wert von **Automatisiert** Feld ist „wahr“.

4. Wählen Sie Aus **Wahr** Damit der angegebene Filter auf Gruppen mit identischen CIs und Musterbezeichnern angewendet wird, oder wählen Sie aus **Falsch** Um den Filter zu ignorieren und zusammengefasste Gruppen für alle Warnungen im System zu erstellen.

Zugehörige Informationen

Geben Sie Musterbezeichnerattribute für die Warnungsgruppierung an, und verwalten Sie sie

Warnungsgruppierungstypen und Erstellungsmethoden

Erkunden Sie verschiedene Warnungsgruppierungstypen, verstehen Sie ihre Beschreibungen, und erfahren Sie mehr über ihre Erstellungsmethoden, um die Problemidentifizierung zu verbessern und das Warnungsmanagement zu optimieren.

Warnungsgruppen anzeigen und verwalten

Navigieren zu **Ereignismanagement** > **Alle Warnungen** Zum Anzeigen aller Warnungsgruppen. Das Symbol in **Gruppe** Spalte gibt den Warnungsgruppentyp an, während Warnungen, die keiner Gruppe zugeordnet sind, keinen Eintrag in haben **Gruppe** Spalte. Doppelklicken Sie auf **Gruppe** Spalte zum Öffnen des Dialogfelds „gruppierte Warnungen“, in dem Sie alle Warnungen in der Gruppe anzeigen und Warnungen manuell hinzufügen oder entfernen können.

Hinweis: Eine Warnung kann jeweils nur zu einer Warnungsgruppe gehören.

Typen der Warnungsgruppierung

Warnungsgruppierungstypen

Typ	Symbol	Beschreibung	Erstellungsmethode	Zusätzliche Information
Log Analytics	L	Log Analytics Gruppen werden gebildet, wenn das System mehrere zugehörige identifiziert Log Analytics Warnungen, gruppieren sie basierend auf ihren wichtigen Verbindungen.	Erstellt als Teil der Log Analytics-Ereignisverarbeitung.	Arten von Health Log Analytics-Warnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen (Fortsetzung)

Typ	Symbol	Beschreibung	Erstellungsmethode	Zusätzliche Information
Regelbasiert	R	Regelbasierte Gruppen bestehen aus zugehörigen Warnungen, die basierend auf der Compliance mit Warnungskorrelationsregeln organisiert sind, die bestimmen, wie Warnungen gemäß ihren Beziehungen gruppiert werden.	Erstellt über Business-Regel (Korrelationsregel berechnen) in der Tabelle „em_Alert“, wenn eine Warnung erstellt oder aktualisiert wird.	• Regelbasierte Warnungsgruppierung • Warnungskorrelationsregel erstellen
Automatisiert	A	Automatisierte Gruppen werden durch Warnungszusammenfassung gebildet und enthalten eine virtuelle Warnung als primäre Warnung der Gruppe. Eine aggregierte automatisierte Gruppe wird erstellt, wenn mindestens zwei Warnungen denselben CI-Typ und Metriknamen verwenden.	Erstellt über geplante Aufgabe.	Automatisierte Warnungsgruppierung
CMDB	C	CMDB-Gruppen werden basierend auf CI-Beziehungen in der CMDB gebildet, insbesondere für CIs, die nicht in regelbasierten oder automatisierten Gruppen enthalten sind.	Erstellt über geplante Aufgabe.	CMDB Basierte Warnungsgruppierung
Basierend auf Netzwerkdatenverkehr	N	Warnungsgruppen für Netzwerkverkehr werden durch die Analyse von Netzwerkverkehrsverbindungen zwischen Prozessen auf Hosts gebildet. Diese Methode nutzt Servicekandidaten, die durch ML Service Mapping identifiziert wurden, um Warnungen im Zusammenhang mit Netzwerkdatenverkehrsproblemen zu gruppieren.	Erstellt über geplante Aufgabe.	Auf Netzwerkdatenverkehr basierende Warnungsgruppierung
Text	T	Textgruppen werden gebildet, indem Warnungen basierend auf ähnlichem Text aus häufig verwendeten Wörtern in den folgenden Feldern gruppiert werden. • Beschreibung • Metrikname • CI-Klasse	Erstellt über geplante Aufgabe.	Textbasierte Warnungsgruppierung
Tag-Cluster	Tag	Tag-Clustergruppen werden gebildet, indem Warnungen gemäß anwenderdefinierten Tag-basierten	Erstellt über geplante Aufgabe.	Warnungsgruppierung des Tag-Clusters

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen (Fortsetzung)

Typ	Symbol	Beschreibung	Erstellungsmethode	Zusätzliche Information
		Warnungs-Clustering-Definitionen gruppiert werden.		
Manuell	M	Warnungen, die manuell nach Anwendern gruppiert werden, um zugehörige Probleme zu organisieren.	Manuell vom Anwender erstellt.	Manuelle Warnungsgruppierung

Informationen zu geplanten Aufgaben und Parametern finden Sie unter Geplante Aufgaben und Parameter für die Warnungsgruppierung. Detaillierte Informationen zum Konfigurieren der Logikreihenfolge für Warnungskorrelationen finden Sie unter Konfigurieren Sie die logische Reihenfolge der Warnungskorrelation.

Protokollanalysen-Warnungsgruppierung

ServiceNow Health Log Analytics Identifiziert Muster in Protokolldaten und lernt das Musterverhalten. Wenn die Engine für künstliche Intelligenz anomales Verhalten erkennt, sendet sie ein Ereignis an den ServiceNow Ereignismanagement Anwendung.

Protokollanalysen-Warnungsgruppen werden von erstellt Health Log Analytics Anwendung. Weitere Informationen finden Sie unter Typen von Health Log Analytics Warnungen.

Regelbasierte Warnungsgruppierung

Die regelbasierte Warnungsgruppierung wird durch Warnungskorrelationsregeln erstellt. Mit diesen Regeln können Sie Warnungen manuell als primär oder sekundär klassifizieren und eine Beziehung zwischen ihnen herstellen. Verwenden Sie Warnungskorrelationsregeln, um zugehörige Warnungen zu gruppieren. Die Regel wird nur für neue Warnungen oder Warnungen ausgeführt, deren Status sich von „Schließen/Fluktuation“ in „Öffnen/erneut öffnen“ geändert hat.

Beispiel: Wenn eine regelbasierte Warnungsgruppierung angewendet wird, werden sekundäre Warnungen, die darauf hinweisen, dass virtuelle Maschinen oder Anwendungen auf dem Offline-Server ebenfalls ausgefallen sind, und unter der primären Warnung gruppiert, die die Stammwarnung für den Server ist, der offline ist. Sie können die regelbasierte Warnungsgruppierung in anzeigen Express-Liste Von Service Operations-Arbeitsbereich(ITOM). Weitere Informationen finden Sie unter Anzeigen von Links zwischen Warnungen in regelbasierten Warnungsgruppen.

Primäre und sekundäre Warnungen

- Primäre Warnung: Identifiziert die Ursache einer Warnungsgruppe und stellt ihre sekundären Warnungen dar.
- Sekundäre Warnung: Im Zusammenhang mit demselben Problem werden sie unter der primären Warnung gruppiert. Der Zweck von sekundären Warnungen besteht darin, zu bestimmen, welche Warnungen unterdrückt werden sollen, um Warnungsrauschen zu reduzieren und Ihnen zu ermöglichen, sich auf die primäre Warnung zu konzentrieren.

Wie primäre und sekundäre Warnungen interagieren

In der regelbasierten Warnungsgruppierung wird eine der echten Warnungen als primäre Warnung festgelegt. Primäre und sekundäre Warnungsfilterbedingungen geben an, welche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen als primär und welche als sekundär klassifiziert werden. Die Filterkriterien werden auf die Tabelle „Warnung“ [em_Alert] angewendet.

In dieser Warnungsgruppierung sind sowohl primäre als auch sekundäre Warnungen sichtbar, aber sekundäre Warnungen werden unter der primären Warnung gruppiert. Die Eigenschaft **Lassen Sie die sekundäre Warnung offen, auch wenn die primäre Warnung geschlossen wurde. Für manuell oder regelbasiert** (`evt_mgmt.rule_based_manual_closure`) Steuert, ob sekundäre Warnungen offen bleiben oder geschlossen werden, wenn die primäre Warnung geschlossen wird.

Wenn die Eigenschaft nicht ausgewählt ist (d. h. auf „Nein“ festgelegt), wird nach dem Schließen der primären Warnung die übergeordnete Referenz aus den sekundären Warnungen entfernt (die Gruppierung wird aufgelöst), und die sekundären Warnungen werden geschlossen und eigenständig. Wenn Sie das Kontrollkästchen für die Eigenschaft aktivieren (d. h. auf „Ja“ festlegen) und die primäre Warnung geschlossen wird, wird die übergeordnete Referenz aus den sekundären Warnungen entfernt (die Gruppierung wird aufgelöst), wodurch sie zu eigenständigen offenen Warnungen werden.

Warnungshierarchie

Nur eine Ebene sekundärer Warnungen ist zulässig. In Situationen, in denen eine Sekundärwarnung über eine eigene Sekundärwarnung verfügt, wird die Hierarchie von der Event Management-Anwendung abgeflacht, damit es weiterhin nur zwei Ebenen gibt.

Ein Beispiel: Nehmen wir an, Warnung A ist die primäre Warnung und Warnung B ist die sekundäre Warnung. Wenn Warnung C zu einer sekundären Warnung von Warnung B wird, wird die Hierarchie von der Anwendung abgeflacht: A bleibt die primäre Warnung, B und C werden zu sekundären Warnungen (eine Ebene unter A).

Als weiteres Beispiel nehmen wir an, dass drei Korrelationsregeln vorhanden sind, was zu den folgenden Ergebnissen führt:

- Regel 1 (mit Reihenfolgenwert 1): B wird zur primären Warnung für A.
- Regel 2 (mit Reihenfolgenwert 2): A wird zur primären Warnung für C und D.
- Regel 3 (mit Reihenfolgenwert 3): E wird zur primären Warnung für A.

Wenn die Warnungen B, C, D und E ausgelöst werden, erscheinen sie alle getrennt in der Warnungsliste, da keine Korrelationen zwischen ihnen bestehen.

Wenn Warnung A ausgelöst wird:

1. Durch Regel 1 wird A zu einer sekundären Warnung unter Warnung B.
2. Regel 2 macht sowohl C als auch D sekundäre Warnungen unter Warnung A, und die Hierarchie wird reduziert, sodass A, C und D zu sekundären Warnungen zur primären Warnung B werden
3. Regel 3 wird nicht angewendet, da mehrere übergeordnete Elemente nicht zulässig sind – A hat bereits B als primäres Element.

Wenn daher alle Warnungen ausgelöst werden, wird nur B als primäre Warnung für A, D und C angezeigt, während E eine eigenständige Warnung bleibt.

Warnungskorrelationsregel erstellen

Erstellen Sie eine Warnungskorrelationsregel, um primäre und sekundäre Warnungen zu definieren. Die primäre Warnung wird als Ursache der Warnungsgruppe identifiziert, und die sekundären Warnungen werden unter der primären Warnung gruppiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Warnungskorrelationsregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Formular für Warnungskorrelationsregel.
4. Wählen Sie **Absenden**.

Ergebnis
Eine regelbasierte Warnungsgruppe wird erstellt, wenn eine neue Warnung generiert wird oder wenn sich der Status einer vorhandenen Warnung von „Geschlossen“ oder „flüchtig“ in „Offen“ oder „erneut geöffnet“ ändert, sofern die Filterkriterien erfüllt sind.

Automatisierte Warnungsgruppierung

Die automatisierte Warnungsgruppierung ist ein Prozess, der Verlaufsdaten verwendet, um ähnliche Warnungen automatisch in Gruppen zu organisieren. Diese Warnungen können Systemprobleme wie Serverfehler oder Netzwerkausfälle sein. Durch die Gruppierung zugehöriger Warnungen können Teams Muster schnell identifizieren, wiederkehrende Probleme verwalten und das Rauschen durch zu viele einzelne Warnungen reduzieren.

Stellen Sie sich vor, Sie überwachen das Verkehrssystem einer Stadt. Sie erhalten viele Warnungen, z. B. Berichte über Unfälle, Staus und Straßensperrungen. Die automatisierte Warnungsgruppierung funktioniert wie ein intelligenter Assistent, der diese Warnungen basierend auf Mustern organisiert, damit Sie zugehörige Probleme zusammen sehen und effizienter reagieren können. Diese automatisierten Warnungsgruppen werden in angezeigt Express-Liste Innerhalb von Service Operations-Arbeitsbereich.

Wie aktivieren Sie diese Gruppierung

Legen Sie die Eigenschaft fest, um die auf maschinellem Lernen basierende Automatisierung für die Warnungskorrelation zu aktivieren **Aktivieren Sie DIE ML-basierte Automatisierungskorrelation** (sa_Analytics.specific_patterns_enabled) auf „wahr“.

Wenn das Installationsprogramm „Domänenunterstützung – Domänenerweiterungen“ aktiviert ist, werden Warnungszusammenfassungsmuster basierend auf der Domänenebene erstellt, die in der Eigenschaft „sa_Analytics.agg.learner_Domain_level“ definiert ist. Standardmäßig ist diese Domänenebene auf zwei festgelegt, was der zweiten Ebene in der Domänenhierarchie entspricht. Beispielsweise kann Ebene 1 in einem Unternehmen das Unternehmen selbst darstellen, während Ebene 2 Abteilungen oder Teams innerhalb des Unternehmens darstellen könnte. Warnungen werden basierend auf dieser zweiten Ebene gruppiert, z. B. nach Abteilung oder Team.Weitere Details finden Sie unter . Domain Separation und Ereignismanagement.

Wie funktioniert es

Die automatisierte Warnungsgruppierung verwendet maschinelles Lernen (ML) und Verlaufsdaten, um Muster zwischen Warnungen zu identifizieren. Es werden bestimmte Merkmale untersucht, die als Musterbezeichner bezeichnet werden – z. B. die Art des Problems, das betroffene System, das CI oder die Metrik, die mehrmals innerhalb eines ähnlichen Zeitraums aufgetreten sind –, um zu bestimmen, ob Warnungen zusammenhängen. Der Lerner für Warnungszusammenfassung verwendet Algorithmen, um Warnungen basierend auf Mustern zu gruppieren. Insbesondere werden musterbasierte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Algorithmen und probabilistische Methoden verwendet, um eingehende Warnungen zu analysieren und zugehörige zu identifizieren.

Stellen Sie sich vor, als würden Sie bemerken, dass Unfälle häufig an einer bestimmten Kreuzung zur Hauptverkehrszeit passieren. Das System gruppiert ähnliche Warnungen (z. B. wiederkehrende Datenverkehrsstaus an derselben Stelle) basierend auf bestimmten Bezeichnern (z. B. Standort oder Typ des Problems). Das System befolgt diese wichtigen Schritte, um Warnungen effektiv zu gruppieren:

- Historische Daten analysieren: Das System untersucht vergangene Warnungen, um Muster und Beziehungen zu lernen.
- Maschinelles Lernen anwenden: ML-Algorithmen analysieren historische Warnungsdaten, um Muster und Beziehungen zwischen Warnungen zu identifizieren. Dadurch kann das System aus früheren Incidents lernen und seine Fähigkeit verbessern, ähnliche Warnungen im Laufe der Zeit zusammenzufassen.
- Ähnliche Warnungen gruppieren: Warnungen mit übereinstimmenden Mustern werden automatisch gruppiert.

Stellen Sie sich vor, Sie verwalten das Verkehrssystem einer Stadt und erhalten mehrere Warnungen:

- 8:00 UHR: Unfall auf der Hauptstraße
- 8:05 UHR: Stau in der Nähe der Main Street
- 8:10 UHR: Straßenschließung auf der Hauptstraße

Die automatisierte Warnungsgruppierung funktioniert wie ein intelligenter Assistent, indem diese Warnungen analysiert und ein Muster erkannt wird. Sie werden gruppiert, da sie sich alle auf die Main Street beziehen, die wahrscheinlich auf denselben Unfall zurückzuführen ist. Dies hilft Ihnen, das Gesamtbild schnell zu sehen und sich auf die Lösung der Ursache (des Unfalls) zu konzentrieren, anstatt jede Warnung separat zu behandeln.

Vorteile

- Wiederkehrende Probleme finden: Muster schnell erkennen (z. B. ein Server, der ständig überhitzt).
- Zeit sparen: Verarbeiten Sie Gruppen zugehöriger Warnungen anstelle einzelner Warnungen.
- Antwort verbessern: Konzentrieren Sie sich auf die Behebung der Ursache, anstatt sich mit vereinzelten Problemen zu befassen.

Musterbezeichner verstehen

Ein Musterbezeichner ist eine Reihe von Kriterien oder Attributen (z. B. Warnungstyp, betroffenes System usw.), die zum Gruppieren ähnlicher Warnungen verwendet werden. Es hilft, wiederkehrende Probleme zu identifizieren, sodass Teams leichter reagieren und laufende Probleme beheben können.

Wie Musterbezeichner Warnungen gruppieren

Betrachten Sie ein Netzwerküberwachungssystem, das Warnungen für verschiedene Probleme generiert, z. B. hohe CPU-Auslastung, Speicherlecks oder Verbindungszeitüberschreitungen.

Musterbezeichner: Metrikname und CI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Warnung 1: Hohe CPU-Auslastung auf Server A um 10:00 UHR
- Warnung 2: Hohe CPU-Auslastung auf Server A um 10:05 UHR
- Warnung 3: Speicherleck auf Server B um 10:10 UHR
- Warnung 4: Hohe CPU-Auslastung auf Server A um 10:15 UHR

In diesem Fall könnte der Musterbezeichner auf den Metriknamen (z. B. hohe CPU-Auslastung) in Kombination mit dem Konfigurationselement (CI) (z. B. Server A) festgelegt werden. Warnungen 1, 2 und 4 werden gruppiert, da sie dieselbe Metrik (hohe CPU-Auslastung) und dasselbe CI (Server A) verwenden, was auf ein wiederkehrendes Problem hinweist, das möglicherweise weitere Untersuchungen erfordert. Warnung 3 wird jedoch nicht in diese Gruppe aufgenommen, da sie eine andere Metrik (Speicherverlust) und ein anderes CI (Server B) aufweist.

Hinweis: Die Gruppe von Warnungsfeldern, die für den Musterbezeichner verwendet werden, wird auch als Funktionsbezeichnerattribute oder einfach als Attribute bezeichnet.

So konfigurieren Sie effektive Musterbezeichner

Um effektive Musterbezeichner für die Warnungsgruppierung zu konfigurieren, befolgen Sie diese drei wichtigen Schritte, um eine genaue und aussagekräftige Analyse von Warnungen sicherzustellen.

Schritt	Aktion	Beschreibung
Event-Regel erstellen	Definieren Sie eine Ereignisregel. Informationen zum Erstellen einer Ereignisregel finden Sie unter Event-Regel erstellen oder bearbeiten.	Richten Sie eine Ereignisregel ein, um die relevanten Warnungsfelder für den Musterbezeichner auszufüllen.
Verwalten Sie den Musterbezeichner	Fügen Sie dem Musterbezeichner ein relevantes Warnungsfeld hinzu. Informationen zum Hinzufügen von Feldern zum Musterbezeichner finden Sie unter Geben Sie Musterbezeichnerattribute für die Warnungsgruppierung an, und verwalten Sie sie.	Wählen Sie nach dem Hinzufügen der relevanten Warnungsfelder aus **Bereitstellen** Zum Aktivieren des Musterbezeichners.
Wählen Sie relevante Bezeichner aus	Wählen Sie Warnungsfelder aus, die das Problem eindeutig identifizieren. Wenn das Problem beispielsweise darin besteht, dass ein Service offline ist oder keine Verbindung zur Datenbank besteht, suchen Sie in der Warnung nach	• Vermeiden Sie zu eindeutige Felder (z. B. Datum), die die Musteridentifizierung erschweren. • Vermeiden Sie zu häufige Felder, die dazu führen, dass zu viele Warnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Aktion	Beschreibung
	bestimmten Werten, die darauf hinweisen. Fügen Sie diese Feldtypen dem Musterbezeichner hinzu. Standardmäßig stellen wir bereit **Metrikname** Feld als Musterbezeichner.	gruppiert werden, wodurch Muster nicht unterscheidbar sind.

Warnungsgruppierung und gelernte Muster

Erfahren Sie, wie Warnungsmuster im System erkannt, gruppiert und angezeigt werden.

Konzept	Beschreibung
Muster-Discovery	Wenn eine Reihe von Warnungsfeldern übereinstimmt, werden die Warnungen in einem „Gelerntes Muster“ gruppiert. Beispielsweise werden Warnungen mit derselben Prioritätsgruppe und Ressource in einem Muster gruppiert.
Musterberichterstellung	Diese Muster werden im Bericht „Gelernte Muster“ unter angezeigt **Ereignismanagement** > **Administration** > **Erlernte Muster**an.

Verwalten von Musterattributen und Zeitrahmen

Erfahren Sie, wie Sie Musterbezeichnerattribute verwalten, neue Sätze bereitstellen und wie das System Probleme identifiziert.

Konzept	Beschreibung
Aktive Musterbezeichner-Attribute	Es kann jeweils nur ein Satz von Attributen aktiv sein. **Hinweis:** Der neue Satz ersetzt den aktuellen nach der Bereitstellung.
Zweck und Zeitrahmen	Die Mustergruppierung identifiziert Probleme innerhalb der letzten 30 Tage, die von gesteuert werden **sa_Analytics.agg.learner_period_days** Eigenschaft.
Problem-Identifizierung	Um ein Problem zu identifizieren, verwendet das System eine Kombination aus Konfigurationselementen (Configuration Items, CIs) und Musterbezeichnern (manchmal als Funktionsbezeichner bezeichnet). Standardmäßig ist ein Musterbezeichner als Metrikname definiert, dieser kann jedoch geändert werden. Zwei Warnungen werden als ähnlich betrachtet, wenn sie dasselbe CI und denselben Musterbezeichner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konzept	Beschreibung
	verwenden. Felder wie Quelle, Schweregrad, Beschreibung und andere können sich jedoch unterscheiden. Weitere Informationen finden Sie unter Geben Sie Musterbezeichnerattribute für die Warnungsgruppierung an, und verwalten Sie sie. **Hinweis:** Der Lerner für Warnungszusammenfassung identifiziert auch Muster von Warnungen innerhalb manueller Warnungsgruppen. In einigen Fällen können Sie Muster aus Warnungen erstellen, bei denen die CIs denselben Wert in einem angegebenen Feld teilen. Beispiel: Um Muster aus Warnungen mit demselben CI zu erstellen **Standort** Feld eingeben Standort In `sa_analytics.agg.learner_group_by_property` Eigensch Weitere Informationen finden Sie unter Konfigurieren Sie die auf geplanten Aufgaben basierende Warnungsgruppierung. Stellen Sie bei der Arbeit mit CI-basierten Gruppen sicher, dass der Musterbezeichner sowohl den Knoten als auch den Metriknamen enthält. Weitere Informationen zum Konfigurieren des Funktionsbezeichners finden Sie unter Bericht zu erlernten Mustern. **Hinweis:** Warnungen ohne CI können weiterhin als textbasierte oder CI-basierte Warnungsgruppen gruppiert werden, wobei ein Knoten als CI behandelt wird. Um diese Funktionalität zu aktivieren, legen Sie die Eigenschaft „sa_Analytics.enable_no_ci_grouping“ auf „wahr“ fest.

Automatische Übersetzung

Konfigurieren Sie die musterbasierte Warnungsgruppierung

Konfigurieren Sie den Lerner für Warnungszusammenfassung (Service Analytics Alert Aggregation Learner – Daily), einen Offline-Auftrag, der täglich ausgeführt wird, um vergangene Warnungen zu verarbeiten. Es identifiziert Muster zugehöriger Warnungen mithilfe einer Kombination aus musterbasierten und probabilistischen Techniken, wodurch wiederkehrende Probleme schneller erkannt und gelöst werden können.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Der Learner der Warnungszusammenfassung verfolgt das manuelle Hinzufügen und Entfernen von Warnungen aus automatisierten Warnungsgruppen. Wenn Sie vorherige Hinzufügungen oder Entfernungen von Warnungen rückgängig machen, wird der automatische Prozess entsprechend angepasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Anwenderhinzufügungen und -Entfernungen aus automatisierten Warnungsgruppen überprüfen und Aktionen rückgängig machen, um zu verhindern, dass sie automatisch wiederholt werden. Der Warnungszusammenfassungssucher identifiziert auch Muster in manuellen Warnungsgruppen und ermöglicht die automatische Bildung neuer Warnungsgruppen basierend auf diesen Mustern, wenn neue Warnungsströme ankommen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrektureigenschaften**an.
2. Aktivieren Sie die folgenden Eigenschaften.
   - Warnungszusammenfassung für automatisierte, CMDB- und textbasierte Gruppen aktivieren (*sa_analytics.aggregation_enabled*).

     Hinweis: Wenn diese Option deaktiviert ist, werden alle anderen Gruppen deaktiviert.

   - ML-basierte Automatisierungskorrelation aktivieren (*sa_analytics.specific_patterns_enabled*).
3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um den Zeitraum zu konfigurieren, in dem der Lerner für die Warnungszusammenfassung Warnungen verarbeiten soll:
   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
   b. Wählen Sie auf der Seite Systemeigenschaften die aus *sa_analytics.agg.learner_period_days*Eigenschaft.

      Wenn die Eigenschaft nicht vorhanden ist, müssen Sie sie definieren.
   c. Legen Sie die Eigenschaft fest **Wert** Bis zur Anzahl der Tage, bis zu denen der Lernauftrag für die Warnungszusammenfassung verarbeitet werden soll.

      Hinweis: Werte, die größer als 30 Tage sind, erhöhen die Auftragsverarbeitungszeit. Um eine optimale Leistung zu erzielen, verwenden Sie Werte von maximal 30 Tagen.

Geben Sie Musterbezeichnerattribute für die Warnungsgruppierung an, und verwalten Sie sie

Der Warnungszusammenfassungssucher analysiert Warnungen und identifiziert Muster mithilfe eines definierten Satzes von Warnungs- und Konfigurationselementattributen (CI). Indem Sie diese Attribute als Musterbezeichner konfigurieren, können Sie steuern, welche Merkmale zum Gruppieren von Warnungen verwendet werden. Diese Anpassung erstellt aussagekräftige Warnungsgruppen, verbessert das Warnungsmanagement und die Antwortzeit, indem das Rauschen reduziert und der Fokus auf kritische Probleme ermöglicht wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Ereignismanagement** > **Administration** > **Muster-Identifier verwalten**an.
2. Wählen Sie auf der Seite „SA-Warnungszusammenfassungsmuster-Attribute“ die Option aus **Neu** Um einen neuen Musterbezeichner zu erstellen oder einen vorhandenen Musterbezeichner zu öffnen.
   Die Seite „Attribut des SA-Warnungszusammenfassungsmusters“ wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie das Symbol „Funktionsbezeichner-Attribute entsperren“ aus ( ) Und verschieben Sie Attribute aus **Verfügbar** Liste zu **Ausgewählt** Liste.

   Hinweis: Eigenschaften von CMDB-CI über Dot-Walking werden nicht ausgefüllt.

   Die **Konfigurationselement** Attribut wird automatisch als Bezeichner betrachtet und darf nicht explizit dem Abschnitt „Funktionsbezeichnerattribute“ hinzugefügt werden. Das Muster ist als eine Kombination aus dem Konfigurationselement und den ausgewählten Attributen des Funktionsbezeichners definiert.

4. Auswählen des Symbols „Funktionsbezeichner-Attribute sperren“ ( ).
5. Wählen Sie Aus **Übermitteln** Für einen neuen Musterbezeichner oder **Aktualisieren** Für einen vorhandenen Musterbezeichner.
6. Navigieren Sie zurück zur Seite „SA-Warnungszusammenfassungsmuster-Attribut“, indem Sie den Musterbezeichner öffnen.
7. Aktivieren Sie die Attribute des Musterbezeichners, indem Sie auswählen **Bereitstellen** .

Nächste Maßnahme

- Stellen Sie sicher, dass eine entsprechende Ereignisregel vorhanden ist: Stellen Sie sicher, dass eine Ereignisregel eingerichtet ist, um den eingehenden Warnungen die neu definierten Musterbezeichnerattribute zuzuweisen oder auszufüllen. Ereignisregeln definieren, wie Attribute Warnungen basierend auf bestimmten Bedingungen zugewiesen werden.
- Führen Sie den Service Analytics-Attributausfüller für historische Warnungen aus: Nachdem die neue Ereignisregel vorhanden ist, wird dieser Auftrag verwendet, um die Musterbezeichnerattribute für vorhandene Warnungen rückwirkend auszufüllen, die erstellt wurden, bevor die neuen Attribute definiert wurden. Es stellt sicher, dass auch vergangene Warnungen (Verlaufswarnungen) über die erforderlichen Attribute verfügen, um sie ordnungsgemäß zu gruppieren.

Bericht zu erlernten Mustern

Der Bericht „Gelernte Muster“ hilft, die Effizienz der Warnungszusammenfassung zu bewerten und wiederkehrende Warnungsmuster zu identifizieren. Es ermöglicht eine proaktive Problemlösung und verbessert die Gesamtsystemleistung, indem Einblicke in häufige Warnungen bereitgestellt werden.

Navigieren und Sortieren des Berichts

Um auf den Bericht zu erlernten Mustern zuzugreifen, navigieren Sie zu **Ereignismanagement** > **Bericht** > **Erlernte Muster**an.

Sortieroptionen: Sie können Muster nach Musterpunktzahl, Häufigkeit und Größe sortieren, um zu priorisieren, welche Warnungen zuerst behandelt werden sollen.

Metriken und Daten im Bericht

Der Bericht zeigt Schlüsselmetriken an, die mit gelernten Mustern verknüpft sind, einschließlich:

- Häufigkeit: Die Anzahl der Vorkommen von Musterbezeichnerattributen (CI/MetricName).
- Musterbezeichnerattribute: Beschreibt, wie die Warnungsgruppierung relevante Musterattribute kombiniert, um ein gelerntes Muster zu erstellen. Diese Muster können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in mehreren Warnungen erneut angezeigt werden, was häufig auf dasselbe zugrunde liegende Problem hinweist.

- Präsentationsformat: Metriken werden in einem Tabellenformat angezeigt, das nach gelernten Mustern organisiert ist.

Mit diesem Bericht können Sie:

- Fokus auf Warnungen mit höherer Häufigkeit: Weisen Sie Ressourcen Warnungen mit höherer Häufigkeit zu, um die Lösung zahlreicher Warnungen zu beschleunigen.
- Größere Muster mit niedrigerer Häufigkeit anvisieren: Ordnen Sie Ressourcen größeren gelernten Mustern mit niedrigerer Häufigkeit zu, um gezielte Analysen zu ermöglichen.

Mustergruppendetails und Bezeichnerattribute

- Erweitern Sie eine Mustergruppe, um Details zu allen Bezeichnerattributen anzuzeigen, die dem Muster zugeordnet sind.
- Sortieren Sie die Einträge in jedem Muster nach Konfigurationselement und Funktionsbezeichner.

Spalte	Beschreibung
Konfigurationselement	CI, das den Attributen des kombinierten Musterbezeichners zugeordnet ist.
Funktionsbezeichner	Funktionsbezeichner, der für die Attribute des kombinierten Musterbezeichners verwendet wird.
Häufigkeit	Gibt an, wie oft die Attribute des kombinierten Musterbezeichners im Datensatz angezeigt werden.
Größe	Anzahl der Vorkommen der kombinierten Musterbezeichnerattribute (z. B. Konfigurationselement und Funktionsbezeichner) in einem gelernten Muster.
Punktzahl	Berechnete Punktzahl, die die Häufigkeit und Größe des gelernten Musters kombiniert. Die Formel für diese Punktzahl lautet: `Punktzahl = Häufigkeit X (Größe + 1)` . Diese Punktzahl hilft bei der Priorisierung von Mustern basierend auf ihrer Wiederholung und Größe, wodurch sich die Fokussierung auf Muster mit hoher Priorität erleichtert.
CI-Link	Link in **Konfigurationselement** Spalte zum Anzeigen von Details der CI-Informationen.

Schließen Sie Muster aus gelernten Mustern aus

Schließen Sie CI-basierte oder CI-klassenbasierte Warnungen und Muster aus, wenn Sie auf Warnungen stoßen, die einem erlernten Muster durch den Auftrag „Erlernte Muster“ falsch hinzugefügt wurden. Ein Muster kann beispielsweise eine Warnung enthalten, die gleichzeitig mit anderen Warnungen aufgetreten ist, aber nicht tatsächlich damit verbunden ist. Dadurch wird die Genauigkeit beibehalten, wodurch eine bessere Warnungsgruppierung und eine effizientere Verwaltung sichergestellt werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

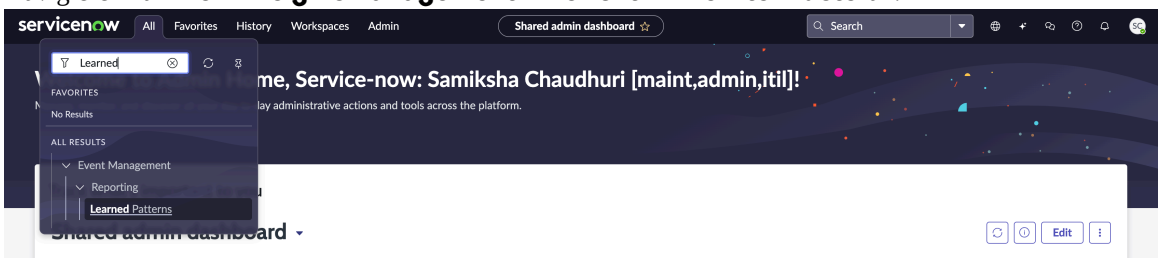
Warum und wann dieser Vorgang ausgeführt wird

Sie wählen die falsche Warnung in einem Muster aus, um das gesamte Muster auszuschließen, zu dem sie gehört.

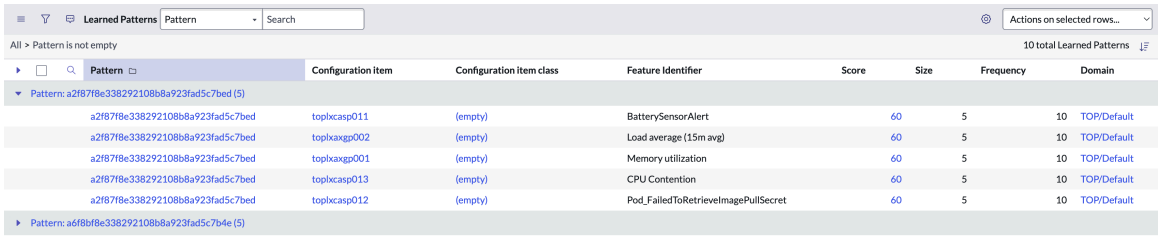
Hinweis: Wenn Sie eine falsche Warnung ausschließen, werden alle anderen Muster, die diese Warnung enthalten, ebenfalls ausgeschlossen.

Prozedur

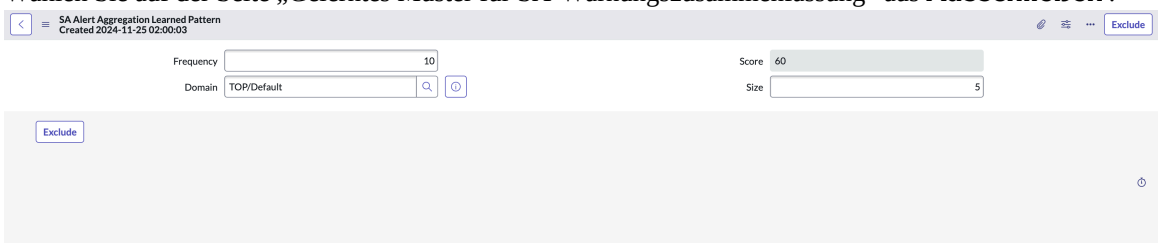
1. Navigieren zu **Alle** > **Ereignismanagement** > **Bericht** > **Erlernte Muster**an.



2. Erweitern Sie auf der Seite „Erlernte Muster“ das anomale Muster.



3. Wählen Sie den Musternamen aus, um ihn zum Ausschließen zu öffnen.
4. Wählen Sie auf der Seite „Gelerntes Muster für SA-Warnungszusammenfassung“ aus **Ausschließen** .



Ergebnis

Das gesamte Muster wird aus dem Bericht „Gelernte Muster“ entfernt und auf der Seite „Ausgeschlossene Muster“ unter aufgeführt **Ereignismanagement** > **Administration** > **Ausgeschlossene Muster**an.

Wenn das Muster andere Warnungen enthält, können Sie es wiederherstellen, indem Sie diese Warnungen als gelerntes Muster zurückfordern. Weitere Informationen finden Sie unter Ausgeschlossene Muster wiederherstellen.

Ausgeschlossene Muster wiederherstellen

Durch das Wiederherstellen ausgeschlossener Muster im Bericht „Gelernte Muster“ können Sie wertvolle Einblicke, die aufgrund falscher Warnungen verloren wurden, erneut integrieren. Diese Flexibilität sorgt für eine genaue Warnungszusammenfassung und verbessert die Überwachung. Wenn Sie beispielsweise ein Muster aufgrund einer falschen Warnung ausgeschlossen haben, können Sie es ohne diese Warnung wiederherstellen, um sicherzustellen, dass relevante Daten für Analysen und Entscheidungen zugänglich bleiben.

Automatische Übersetzung

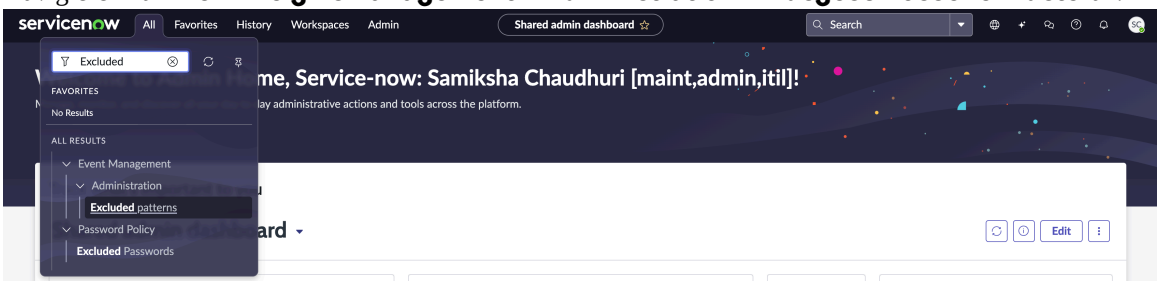
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

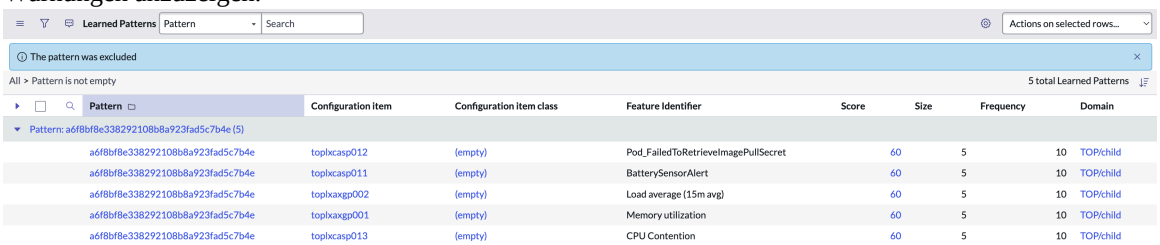
Erforderliche Rolle: evt_mgmt_admin

Prozedur

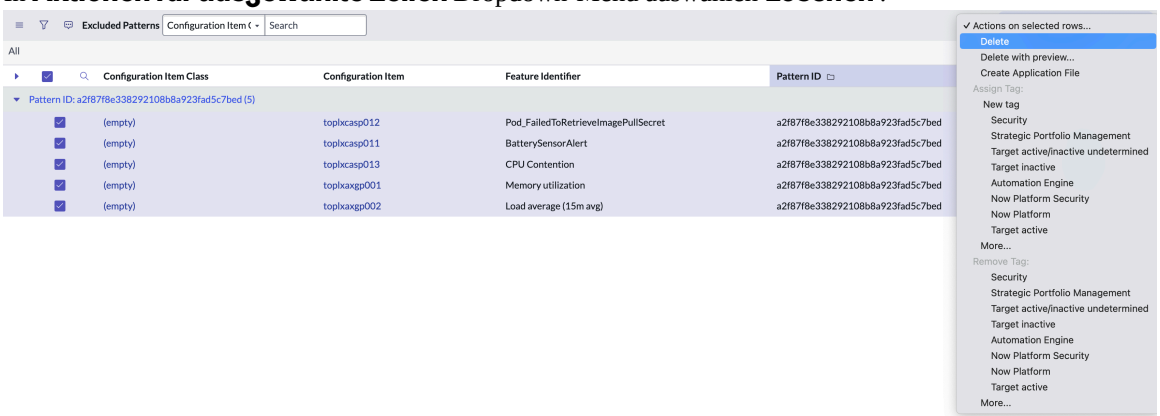
1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ausgeschlossene Muster**an.



2. Erweitern Sie auf der Seite „Ausgeschlossene Muster“ ein Muster oder wählen Sie eins aus, um seine Warnungen anzuzeigen.



3. Wählen Sie die Muster aus, die Sie wiederherstellen möchten.
4. In **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Löschen** .



5. Wählen Sie im Bestätigungsfenster **Löschen**.
6. Führen Sie die regelmäßige Aufgabe „Erlernte Muster“ aus.

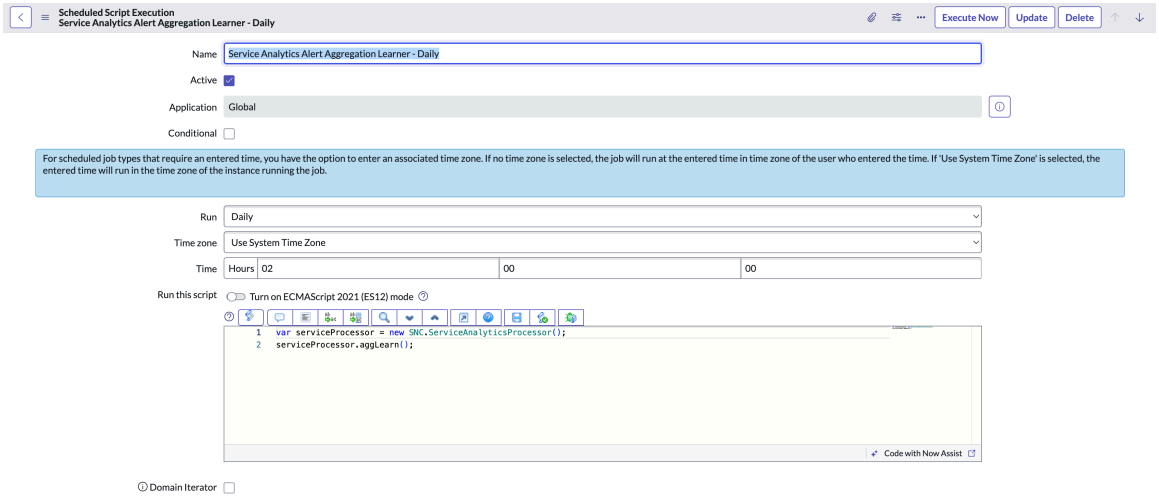
   a. Auswahlvorgang **Systemdefinition** > **Geplante Aufgabe**an.

   b. Suchen Sie auf der Seite „geplante Aufgaben“ nach der Aufgabe „Service Analytics – Warnungszusammenfassung – Learner – täglich“.

   c. Öffnen Sie die Aufgabe Service Analytics-Warnungszusammenfassung – Learner – Daily.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Wählen Sie **Jetzt ausführen**.

Ergebnis

Das Muster wird mit seinen wiederhergestellten Warnungen auf der Berichtsseite „Erlernte Muster“ angezeigt. Um auf diese Seite zuzugreifen, navigieren Sie zu **Ereignismanagement** > **Bericht** > **Erlernte Muster**an.

Auf Netzwerkdatenverkehr basierende Warnungsgruppierung

Die auf Netzwerkverkehr basierte Warnungsgruppierungsmethode gruppiert Warnungen, indem Netzwerkverkehrsverbindungen zwischen Prozessen auf Hosts analysiert werden. Es nutzt Servicekandidaten, die von ML Service Mapping identifiziert wurden, um Warnungen im Zusammenhang mit Netzwerkdatenverkehrsproblemen zu gruppieren. Dadurch wird sichergestellt, dass Warnungen von direkt verbundenen Prozessen innerhalb desselben Servicekandidaten gruppiert werden, was eine kontextbezogene Ansicht von Netzwerk-Incidents bietet.

Servicekandidaten sind potenzielle Sammlungen von Prozessen in Ihrer IT-Umgebung, die basierend auf ihren Netzwerkverbindungen und Interaktionen identifiziert werden. Sie stellen verschiedene Services oder Funktionen dar, die Ihre IT-Systeme bereitstellen, auch wenn sie in der Konfigurationsdatenbank Ihres Systems nicht vollständig detailliert sind. Beispielsweise können Servicekandidaten alle Prozesse gruppieren, die an der E-Mail-Zustellung beteiligt sind, auch wenn die Konfigurationsdetails unvollständig sind.

ML Service Mapping verwendet maschinelles Lernen, um diese Servicekandidaten automatisch zu erkennen und zuzuordnen. Sie identifiziert, wie verschiedene Prozesse und Komponenten basierend auf ihrem Netzwerkverkehr und ihren Interaktionen verbunden und gruppiert werden. Dies hilft beim Verständnis und Organisieren der IT-Services und ihrer Komponenten und erleichtert die Verwaltung und Behebung von Problemen. Beispielsweise kann ML Service Mapping die Verbindungen zwischen E-Mail-Servern und E-Mail-Clients basierend auf ihren Netzwerkinteraktionen automatisch identifizieren und zuordnen.

Hinweis: Die auf Netzwerkverkehr basierte Warnungsgruppierung ist für neue Kunden ab aktiviert Zurich Release. Bestandskunden müssen die Eigenschaft Netzwerkverkehrskorrelation aktivieren (`sa_analytics.agg.query_network_traffic_correlation_enabled`) Manuell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise

- Host-Identifizierung: Warnungen im Zusammenhang mit Netzwerkproblemen werden aus verschiedenen Quellen generiert.
- Netzwerkkontextidentifizierung: Der Korrelationsprozess verwendet horizontale Discovery-Ergebnisse und ML Service Mapping, um die relevantesten Servicekandidaten und Netzwerkverbindungen zu identifizieren.

  Dieser Prozess verwendet die Ergebnisse der geplanten Aufgabe **Ereignismanagement – Servicekandidaten-Prozess zu Prozesszuordnung ausfüllen – täglich** , Der einmal täglich ausgeführt wird und zum Speichern von Prozess-zu-Prozess-Verbindungen für Host-CIs in dem vom Warnungsgruppierungsalgorithmus erforderlichen Format verwendet wird.
- Warnungsgruppierung: Warnungen werden basierend auf direkten Prozess-zu-Prozess-Verbindungen im Kontext desselben Servicekandidaten gruppiert. Die Gruppierung wird in Echtzeit aktualisiert, wenn neue Warnungen empfangen werden.

Vorteile

- Verbesserte Genauigkeit: Durch die Nutzung von Netzwerkdatenverkehrsverbindungen und Servicekandidaten bietet diese Methode eine hohe Genauigkeit bei der Gruppierung von Warnungen, wodurch falsch positive Ergebnisse minimiert werden.
- Erweiterte Abdeckung: Warnungen werden auch in Umgebungen mit niedriger CMDB-Reife effektiv gruppiert und decken ein breiteres Spektrum von Warnungen und Problemen ab.
- Optimierte Lösung: IT-Teams können zugehörige Probleme schnell in großen Mengen identifizieren und lösen, wodurch das Volumen der zu verwaltenden Warnungen reduziert und die betriebliche Effizienz verbessert wird.

Aktivieren Sie die auf dem Netzwerkverkehr basierte Warnungsgruppierung

Aktivieren Sie die auf Netzwerkverkehr basierte Warnungsgruppierung, um Warnungsrauschen automatisch zu korrelieren und zu reduzieren, indem zugehörige Ereignisse basierend auf Netzwerkverkehrsmustern gruppiert werden. Dies trägt zur Verbesserung der Effizienz der Warnungsantwort bei und optimiert das Warnungsmanagement.

Vorbereitungen
Stellen Sie sicher, dass die Anwendung Service Mapping Plus (sn_sm_scoped_App) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**an.
2. Stellen Sie sicher, dass die Eigenschaft Netzwerkverkehrskorrelation aktivieren (`sa_analytics.agg.query_network_traffic_correlation_enabled`) Ist ausgewählt.

Deaktivieren Sie die auf dem Netzwerkverkehr basierte Warnungsgruppierung

Deaktivieren Sie die auf dem Netzwerkverkehr basierte Warnungsgruppierung, um zu verhindern, dass Warnungen nur nach Netzwerkaktivität gruppiert werden, reduzieren Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das Rauschen bei Datenverkehrsspitzen und stellen Sie sicher, dass kritische Probleme für eine schnellere Lösung von Bedeutung sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**an.
2. Deaktivieren Sie dieses Kontrollkästchen für die Eigenschaft Korrelation des Netzwerkverkehrs aktivieren (*sa_analytics.agg.query_network_traffic_correlation_enabled*).
3. Legen Sie die Eigenschaft fest *sa_analytics.enable_process_mapping_calculation*Auf „falsch“.

Verfolgen Sie Arbeitsnotizen, und überprüfen Sie den Servicekandidaten

Verfolgen Sie Arbeitsnotizen nach, und verfolgen Sie sie, während Sie den Servicekandidaten überprüfen, um sicherzustellen, dass alle Aktionen und Updates erfasst werden. Dies trägt dazu bei, Klarheit und Kontinuität im Überprüfungsprozess zu erhalten, wodurch die Wahrscheinlichkeit verringert wird, dass Details verpasst werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin und sm_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.

   Hinweis: Scrollen Sie mit nach unten zu einer Warnung **Netzwerkverkehr** Als Gruppe und in der **Gruppe** Spalte, klicken Sie mit der rechten Maustaste, und wählen Sie aus **Übereinstimmungen Anzeigen** . Dadurch werden alle Warnungen angezeigt, die sich auf beziehen **Netzwerkverkehr** .

2. Wählen Sie für die Warnung, deren Arbeitsnotizen Sie sehen möchten, die Warnungsnummer aus.
3. Scrollen Sie auf der Seite „Warnung“ nach unten, und wählen Sie aus **Aktivitäten** Registerkarte.
   Sie können die Arbeitsnotizen für die ausgewählte Warnung anzeigen.
4. Wählen Sie in den Arbeitsnotizen den Servicekandidaten aus, um Details anzuzeigen.
   Die Seite „Anwendungsservice-Candidate“ wird geöffnet.
5. Wählen Sie Aus **Vorschau Des Kartendiagramms Anzeigen** Dient zum Anzeigen der Zuordnung von Servicekandidaten in Form eines Diagramms.
   Die Zuordnung von Servicekandidaten bietet eine visuelle Darstellung, wie verschiedene Servicekandidaten miteinander verbunden sind, wodurch Beziehungen leichter verstanden, potenzielle Probleme identifiziert und Abhängigkeiten effektiver analysiert werden können.

Gemischte Warnungsgruppierung

Die gemischte Warnungsgruppierung kombiniert mehrere Strategien – derzeit CMDB-basierte und Tag-basierte Gruppierung –, um eine einzelne, zusammenhängende Warnungsgruppe zu bilden. Es reduziert das Rauschen, schließt Lücken, wenn eine Methode nicht ausreicht, und bietet eine klarere End-to-End-Ansicht von Incidents. Dieser Ansatz hilft Betreibern, Ursachen schneller zu identifizieren und fundierte Maßnahmen zu ergreifen, auch in komplexen oder unvollständigen Datenumgebungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um zu verstehen, wie die gemischte Gruppierung in der Praxis funktioniert, ist es wichtig, sich die einzelnen Strategien anzusehen, die derzeit unterstützt werden. In dieser Phase umfasst die gemischte Gruppierung zwei Kernmethoden: CMDB Basierte Warnungsgruppierung, Der in der CMDB definierte Servicebeziehungen nutzt, und Warnungsgruppierung des Tag-Clusters, Der freigegebene Metadaten für Warnungen verwendet. Jede spielt eine unterschiedliche Rolle bei der effektiven Korrelation zugehöriger Warnungen.

Informationen zum Gruppieren von Warnungen finden Sie unter Gruppenautomatisierung erstellen.

CMDB Basierte Warnungsgruppierung

CMDB Die basierte Warnungsgruppierung hilft Organisationen, Warnungen zu verwalten, indem sie sie gemäß ihren zugehörigen Konfigurationselementen (Configuration Items, CIs) in der Configuration Management Database (organisiert CMDB). Diese Methode gruppiert Warnungen basierend auf CI-Beziehungen in Anwendungen oder Infrastrukturkomponenten, sodass Teams die Auswirkungen von Problemen besser verstehen, effektiver auf Warnungen reagieren und die Serviceverfügbarkeit aufrechterhalten können.

CMDB Warnungsgruppen werden basierend auf den aktuellen Beziehungen zwischen CIs in einer Organisation erstellt. Dies bedeutet, dass Warnungen basierend auf CI-Beziehungen gruppiert werden, wenn mehrere Warnungen für verschiedene CIs ausgelöst werden (z. B. wenn bei einem Server Probleme auftreten).

Standardmäßig werden alle vorhandenen Verbindungen zwischen CIs zum Gruppieren von Warnungen verwendet. Angesichts der Komplexität von IT-Systemen gibt es jedoch viele Arten von Beziehungen, und Organisationen können filtern, welche bei der Zusammenfassung von Warnungen berücksichtigt werden sollen. Sie können beispielsweise Beziehungstypen nach vorgeschlagenen Beziehungen filtern, die in der Tabelle „CMDB-Gruppen-CI-Beziehungen“ [em_proposed_Relation_type] angezeigt werden. Sie können auch mithilfe der Hosting- und Containment-Regeln (abhängige Beziehungsregeln) filtern.

Wenn beispielsweise ein Server mehrere Anwendungen hostet und ein Problem mit diesem Server besteht, können alle Warnungen im Zusammenhang mit dem Server und den Anwendungen, die er hostet, gruppiert werden. Dies hilft dem IT-Team, die Ursache des Problems schnell zu identifizieren und zu beheben, anstatt jede Warnung isoliert zu bearbeiten. Wenn auf einem Server verschiedene Prozesse ausgeführt werden, können Teams durch die Gruppierung von Warnungen basierend auf diesen Prozessen sehen, wie sich Probleme in einem Bereich auf andere auswirken können, was zu einem umfassenderen Verständnis der Situation führt.

Die CMDB Warnungsgruppen werden effektiv in angezeigt Express-Liste Innerhalb von Service Operations-Arbeitsbereich, Wodurch Teams zugehörige Warnungen einfach überwachen und verwalten können. Diese Funktion verbessert die betriebliche Effizienz, indem sie einen klaren Überblick über Warnungen bietet, die basierend auf den aktuellen Beziehungen zwischen Konfigurationselementen (Configuration Items, CIs) miteinander verbunden sind.

Anwendungsfälle für CMDB Basierte Warnungsgruppierung

Anwendungsfälle für CMDB Gruppierung verbessert das Warnungsmanagement, indem Warnungen basierend auf Konfigurationselementbeziehungen korreliert werden, die Transparenz verbessert und eine effizientere Fehlerbehebung ermöglicht wird.

Allgemein CMDB Gruppieren von Anwendungsfällen

Im Kontext von CMDB Bei der Gruppierung stehen Organisationen bei der Verwaltung von Warnungen im Zusammenhang mit Konfigurationselementen (Configuration Items, CIs) vor mehreren Herausforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anwendungsfälle

Anwendungsfall	Herausforderungen	Lösungen
Freigegebenes Konfigurationselement (CI) Szenario: Eine Organisation überwacht einen Datenbankserver, bei dem mehrere Probleme auftreten, was zu zahlreichen Warnungen im Zusammenhang mit verschiedenen Anwendungen führt, die diese Datenbank verwenden.	• Verzögerte Antwort: Teams reagieren möglicherweise isoliert auf Warnungen und übersehen möglicherweise zugehörige Warnungen, was zu verzögerten Lösungen führt. • Ineffiziente Ressourcenzuteilung: Zeit und Ressourcen können für die Untersuchung separater Warnungen verschwendet werden, die tatsächlich zusammenhängen. • Fehlender Kontext: Warnungen, die sich auf dasselbe CI beziehen, können auf verschiedene Warnungsgruppen verteilt sein, was es schwierig macht, das vollständige Bild zu sehen.	• Aggregieren Sie Warnungen im Zusammenhang mit demselben CI in einer einzigen Gruppe, um eine einheitliche Ansicht zu erhalten. • Erleichtern Sie eine schnellere Warnungslösung, indem Sie alle zugehörigen Warnungen zusammen behandeln.
Hosting-/Containment-Beziehungen Szenario: Ein physischer Server hostet mehrere virtuelle Computer (VMs), und es wird eine Warnung für einen Hardwarefehler auf dem Server generiert. Aufgrund ihrer Abhängigkeit vom Server werden auch mehrere Warnungen für die VMs ausgegeben.	• Transparenz in Abhängigkeiten: Teams mangelt möglicherweise nicht Einblick in die Art und Weise, wie CIs miteinander verbunden sind, was zu ineffizienten Problembehebungsprozessen führt. • Komplexe Warnungslösung: Das Verständnis, welche CIs betroffen sind und wie sie zusammenhängen, kann kompliziert sein, was zu längeren Lösungszeiten führt. • Ressourcenabfluss: Die falsche Verwaltung von Warnungen kann zu doppelten Anstrengungen	• Warnungen mit gruppieren CMDB Hosting-/Containment-Regeln zum Zusammenfassen von Warnungen im Zusammenhang mit dem physischen Server und seinen gehosteten VMs in einer einzigen Warnungsgruppe. • Bieten Sie eine umfassende Ansicht aller Warnungen im Zusammenhang mit dem Ausfall des physischen Servers. • Konzentrieren Sie Korrekturmaßnahmen auf den physischen Server, während Sie die VMs überwachen, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anwendungsfälle (Fortsetzung)

Anwendungsfall	Herausforderungen	Lösungen
	in Teams führen, was Zeit und Ressourcen verschwendet.	sicherzustellen, dass alle Aspekte effizient behandelt werden.
Anwendbare Beziehungen Szenario: Eine Enterprise-Anwendung basiert auf mehreren Micro-Services, und bei einem dieser Services tritt ein Problem auf, das Warnungen für mehrere Komponenten generiert, was die Diagnose erschwert.	• Anwendungsabhängigkeiten verstehen: Teams finden es möglicherweise schwierig, nachzuverfolgen, wie Anwendungskomponenten interagieren, was es schwierig macht, Probleme in komplexen Systemen zu erkennen. • Langsame Incident-Lösung: Ohne ein klares Verständnis des anwendbaren Flows kann die Lösung von Warnungen langsam und arbeitsintensiv sein. • Inkonsistente Überwachung: Warnungen im Zusammenhang mit Anwendungen werden möglicherweise nicht einheitlich überwacht oder priorisiert, was zu potenziellen Übersichten führt.	• Implementieren Sie eine Gruppierung basierend auf anwendbaren Flow-Beziehungen, um Warnungen im Zusammenhang mit dem betroffenen Microservice und seinen abhängigen Komponenten zusammenzufassen. • Verwenden Sie Abhängigkeitszuordnungen, um zu visualisieren, wie verschiedene Services interagieren. • Optimieren Sie den Lösungsprozess, indem Sie gruppierte Warnungen im Zusammenhang mit der Anwendung behandeln und die Antwortzeiten verbessern.

CMDB Warnungsgruppierung – Eigenschaften und Funktionalität

Erfahren Sie mehr über die wichtigsten Eigenschaften und Funktionen von CMDB Warnungsgruppierung, die eine effiziente Warnungsorganisation basierend auf Beziehungen erleichtert und die Gesamteffektivität des Warnungsmanagements verbessert.

Eigenschaften für die Verwaltung CMDB Warnungsgruppenerstellung

Verwenden Sie zur Steuerung die in den folgenden Tabellen aufgeführten Eigenschaften CMDB Warnungsgruppenerstellung. Weitere Informationen finden Sie unter Konfigurieren Sie die auf geplanten Aufgaben basierende Warnungsgruppierung.

Eigenschaft	Einstellung
CMDB-Korrelation aktivieren `sa_analytics.agg.query_cmdb_correlation_enabled`	Aktivieren Sie diese Eigenschaft, um CI-Beziehungen automatisch für die Warnungszusammenfassung, die Korrelation von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Einstellung
	Warnungen und die Erstellung zu verwenden CMDB Warnungsgruppen.
Maximale Anzahl von Beziehungen zwischen CIs in einer Topologie, die einen bilden CMDB Gruppe *sa_analytics.agg.query_cmdb_graph_walk_nodes*	Legen Sie die maximale Anzahl aktivierter Beziehungen zwischen CIs in einer Topologie fest, die eine bilden CMDB Gruppe. Wenn Sie diese Eigenschaft beispielsweise auf 3 festlegen, wird ein CI, das einer Warnung zugeordnet ist, automatisch mit ähnlichen CIs innerhalb von maximal drei Hops gruppiert. **Hinweis:** Diese Eigenschaftseinstellung wirkt sich auf alle Arten von Beziehungen aus, die für die Warnungszusammenfassung verwendet werden. Die Verwendung eines Werts größer als 4 kann sich negativ auf die Leistung des Warnungszusammenfassungsauftrags auswirken.
Alle verwenden CMDB Beziehungen für CMDB Gruppenkorrelation *evt_mgmt.related_cis_get_all_relation_types*	Legen Sie diese Option auf „wahr“ fest, wenn Sie alle Beziehungstypen für verwenden möchten CMDB Gruppierung. Die Standardeinstellung für neue Anwender ist, dass die Option auf „wahr“ festgelegt ist, d. h. alle Beziehungstypen werden für die Gruppierung verwendet. Legen Sie die Eigenschaft auf „falsch“ fest, um die Beziehungen zu filtern.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB Warnungsgruppen für erweiterte Anwendungsfälle

In einigen Anwendungsfällen müssen Sie möglicherweise bestimmte CI-Beziehungen ignorieren oder von der automatischen Erstellung von Warnungsgruppen ausschließen. In diesem Fall wird *evt_mgmt.related_cis_get_all_relation_types*Eigenschaft muss auf „falsch“ festgelegt werden, und die Eigenschaften in der folgenden Tabelle müssen ebenfalls konfiguriert werden.

Hinweis: Wenn *evt_mgmt.related_cis_get_all_relation_types*Eigenschaft ist auf „falsch“ festgelegt, und die Beziehung ist nicht in der Tabelle [em_proposed_Relation_type] angegeben. Die Beziehung wird für die Warnungszusammenfassung nicht berücksichtigt.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB Warnungsgruppen für erweiterte Anwendungsfälle

Eigenschaft	Einstellung
Aktivieren Sie vorgeschlagene Beziehungen für CMDB Korrelation	Lassen Sie diese Eigenschaft aktiviert, um alle vorgeschlagenen Beziehungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB Warnungsgruppen für erweiterte Anwendungsfälle (Fortsetzung)

Eigenschaft	Einstellung
sa_analytics.agg.query_cmdb_suggested_relationships	zu verwendende, die in der CMDB Tabelle „CI-Beziehungen gruppieren“ [em_proposed_Relation_type] beim Erstellen CMDB Warnungsgruppen. Um eine neue Beziehung einzubeziehen, fügen Sie sie dieser Tabelle hinzu. Diese Eigenschaft ist standardmäßig aktiviert.
Verwenden CMDB Beziehung basierend auf Host-Containment-Metadatenregeln *evt_mgmt.related_cis_use_containment_rules*	Containment-Regeln geben an, welche Konfigurationselementklassen beim Erstellen einer Servicevorlage durch eine bestimmte Beziehung in einem anderen Element enthalten sein können. Lassen Sie diese Eigenschaft beim Erstellen aktiviert CMDB Warnungsgruppen zur Verwendung von Host-Containment-Regeln, die im Metadaten-Editor definiert sind. Weitere Einzelheiten finden Sie unter Abhängige CMDB-Beziehungsregeln . Diese Eigenschaft ist standardmäßig aktiviert.
Aktivieren Sie die Filterung nach abhängigen Beziehungsregeln *evt_mgmt.related_cis_use_hosting_rules*	Hosting-Regeln definieren, welche Klassen von Konfigurationselementen in anderen Klassen von Konfigurationselementen gehostet werden. Lassen Sie diese Eigenschaft beim Erstellen aktiviert CMDB Warnungsgruppen zum Anwenden von Hosting-Regeln, die definieren, welche Klassen von Konfigurationselementen auf anderen Klassen gehostet werden. Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert. **Hinweis:** Wenn Sie den Standardwert ändern müssen, fügen Sie die Eigenschaft hinzu, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .
Ignorieren CMDB Warnungsgruppen werden aufgrund von CI-Flow-Beziehungen nicht gebildet *sa_analytics.agg.ignore_cmdb_applicative_flow*	Legen Sie diese Eigenschaft auf „wahr“ fest, um dies zu verhindern CMDB Gruppen aus der Bildung basierend auf anwendbaren Flow-Beziehungen für CI-Beziehungen in Anwendungsservices.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB Warnungsgruppen für erweiterte Anwendungsfälle (Fortsetzung)

Eigenschaft	Einstellung
	Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert. **Hinweis:** Wenn Sie den Standardwert ändern müssen, fügen Sie die Eigenschaft hinzu, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .
`sa_analytics.applicative_flow_rc_enable`	Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert.

Ereignismanagement Speichert eine Zuordnung zugehöriger CIs in Ereignismanagement Tabelle „CI-Graph-Wiederverwendung“ [em_ci_Graph_Reuse] für jedes verarbeitete CI. Sie können den Speicherzeitraum anpassen, indem Sie ändern `sa_analytics.agg.query_cmdb_graph_reuse_period`Eigenschaft, bei der der Standardwert auf einen Tag (86.400 Sekunden) festgelegt ist. Dieser Prozess verbessert die Suchleistung von Beziehungen in CMDB. Um den Speicherprozess während erweiterter Anwendungsfallkonfigurationen zu deaktivieren, legen Sie den Eigenschaftswert auf null fest.

Hinweis: Wenn Sie den Standardwert ändern müssen, fügen Sie hinzu `sa_analytics.agg.query_cmdb_graph_reuse_period`Eigenschaft, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Zeigen Sie die Abhängigkeitszuordnung für an CMDB Warnungen

Die Abhängigkeitszuordnung veranschaulicht, wie und warum Warnungen gruppiert werden, was die Fehlerbehebung und das Problemmanagement vereinfacht. Zeigt Verbindungen zwischen CIs in einem an CMDB Warnungsgruppe, die die Transparenz ihrer Beziehungen verbessert. Wenn ein CI nicht Teil der Gruppe ist, aber eine Verbindung zu anderen Warnungs-CIs herstellt, bleibt es außerdem auf der Karte sichtbar, was die Lösung von Warnungen und die proaktive Verwaltung unterstützt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_Operator

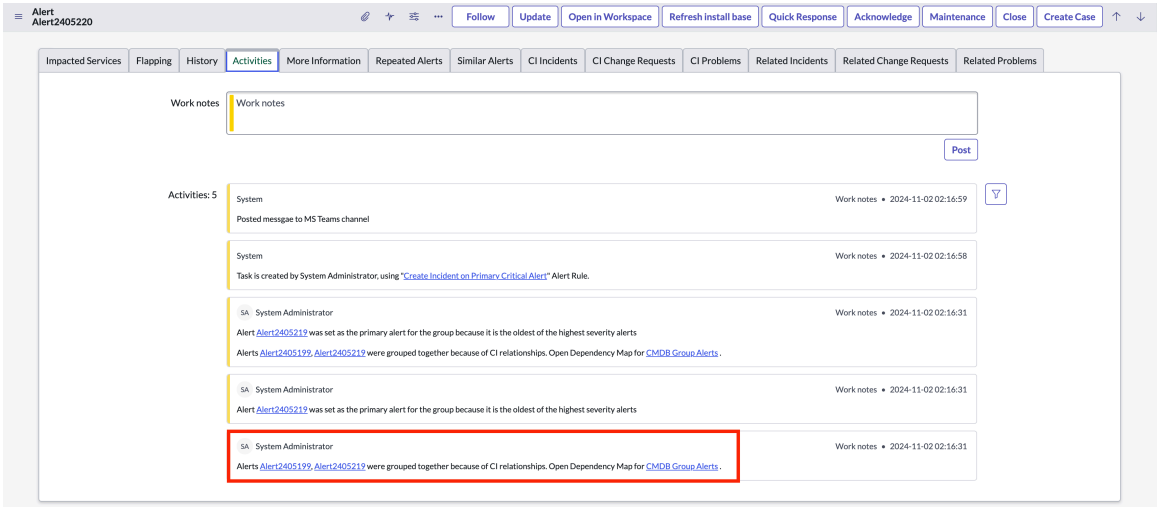
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Suchen Sie nach CMDB Gruppe.
3. Öffnen Sie ein CMDB Gruppenwarnung.
4. Scrollen Sie nach unten, und wählen Sie aus **Aktivitäten** Registerkarte.

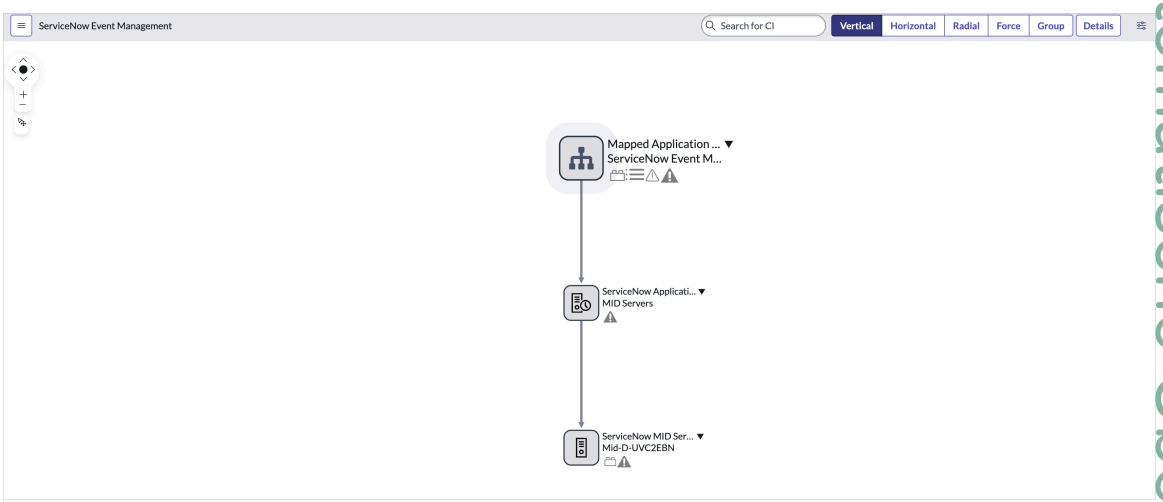
Möglicherweise wird eine Nachricht ähnlich der folgenden angezeigt:

Alert2405199 und Alert2405219 wurden aufgrund von CI-Beziehungen gruppiert. Öffnen Sie die Abhängigkeitszuordnung für CMDB-Gruppenwarnungen. Öffnen Sie die Abhängigkeitszuordnung für CMDB-Gruppenwarnungen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie den Link aus, um die Abhängigkeitsansicht von anzuzeigen CMDB Warnungen.



Fügen Sie eine CI-Beziehung zu hinzu CMDB Gruppen-CI-Beziehungen

Fügen Sie ein hinzu CMDB Gruppen-CI-Beziehung für eine CI-Klasse, um eine genaue Generierung von Warnungsgruppen zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie *sa_analytics.agg.query_cmdb_suggested_relationship_enabled*Eigenschaft zur weiteren Verbesserung der Warnungsgruppierung durch Verwendung vorgeschlagener Beziehungen. Weitere Informationen zu Eigenschaften finden Sie unter CMDB Warnungsgruppierung – Eigenschaften und Funktionalität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **CMDB-Gruppe – CI-Beziehungen**an.

   a. Klicken Sie auf **Neu**.

   b. Füllen Sie das Formular aus.

Felder „Vorgeschlagene Beziehungen“

Feld	Beschreibung
Basisklasse	Die Basisklasse in der Beziehung dient je nach Typ der hergestellten Beziehung entweder als übergeordnetes oder als untergeordnetes Element.
Beziehung	Der Typ der Beziehung, der definiert, wie zwei oder mehr Entitäten verbunden sind.
Abhängige Klasse	Die Klasse, die auf einer anderen Klasse in der Beziehung basiert und je nach Beziehungstyp entweder als übergeordnetes oder untergeordnetes Element dient.

2. Klicken Sie auf **Absenden**.

Example: CMDB Gruppen-CI-Beziehung

Basisklasse	Beziehung	Abhängige Klasse/Zielklasse
Oracle	Ist gehostet auf	Linux-Server
Oracle	Ist gehostet auf	Solaris-Server

Hinweis: Dieselbe übergeordnete Klasse und Beziehung können mehr als einmal angezeigt werden.

Löschen Sie eine CI-Beziehung aus CMDB Gruppen-CI-Beziehungen

Löschen Sie einen CMDB Gruppen-CI-Beziehung, für die verfügbare Beziehungen begrenzt werden sollen CMDB Warnungsgruppierung, die zur Reduzierung von Lärm und zur Verbesserung der Warnungsrelevanz beiträgt.

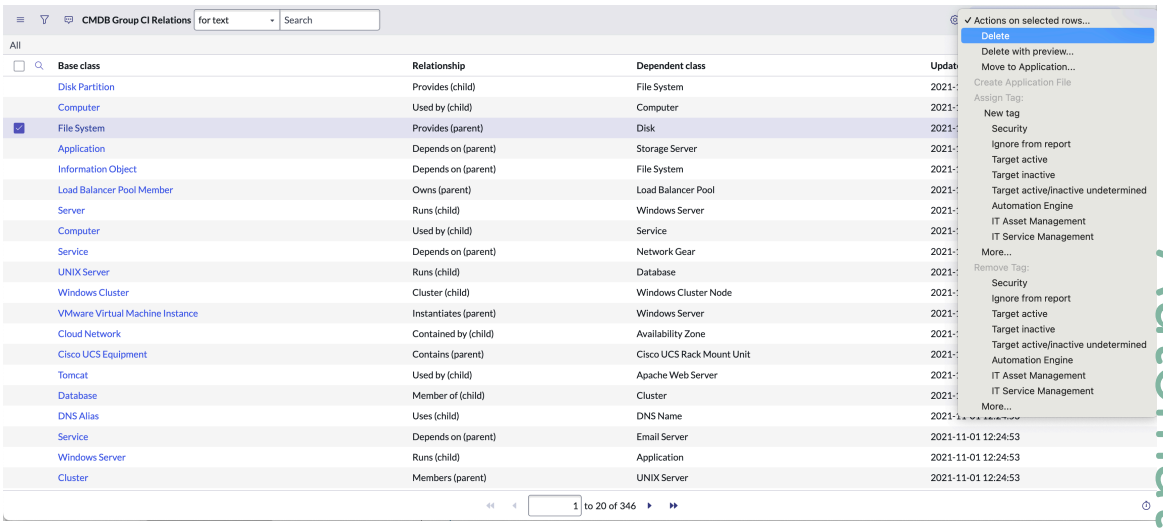
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **CMDB-Gruppe – CI-Beziehungen**an.
2. Aktivieren Sie das Kontrollkästchen neben der CI-Beziehung, die Sie löschen möchten.
3. Wählen Sie das Menü Aktionen und dann aus **Löschen** .



4. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die CI-Beziehung wird gelöscht.

Warnungsgruppierung des Tag-Clusters

Mit der Tag-Cluster-Warnungsgruppierung können Sie einfach Gruppen von Warnungen erstellen. Es handelt sich um eine Methode der Warnungsgruppierung ohne Code, bei der Warnungen korreliert werden, ohne die CMDB oder Modelltraining verwenden zu müssen. Diese einfachere Art der Gruppierung ähnlicher Warnungen reduziert das allgemeine Rauschen einer großen Menge von Warnungen.

Die Warnungsgruppierung des Tag-Clusters wird unmittelbar nach der Aktivierung der Anwendung „Tag-basierte Warnungs-Clustering-Engine“ aktiviert, die in verfügbar ist ServiceNow Store. Diese Gruppierung wird gemäß der Korrelationslogikreihenfolge angewendet, die in angegeben ist Konfigurieren Sie die logische Reihenfolge der Warnungskorrelation. Warnungsgruppierungs-Tags werden an Definitionen auf M2M-Basis angehängt. Mehrere Tags können mit einer einzelnen Definition verknüpft werden, und ein Tag kann Teil mehrerer Definitionen sein. Gruppen, die aus Warnungsgruppierungsdefinitionen des Tag-Clusters gebildet werden, werden als Tag-Clustergruppentyp klassifiziert.

Die Warnungsgruppierung des Tag-Clusters unterstützt die Domänentrennung, sodass verschiedene Domänen über eigene Konfigurationen und Logik für die Warnungsgruppierung verfügen können.

Erstellen Sie zuerst Warnungsgruppierungs-Tags, um die Kriterien für die Gruppierung von Warnungen zu definieren. Sie können die Tags so festlegen, dass eine genaue Übereinstimmung, eine ungefähre Übereinstimmung („Fuzzy“) oder eine Zeichenmusterübereinstimmung erforderlich sind.

Sie können auch vorkonfigurierte Tags verwenden, um das Warnungs-Clustering zu beschleunigen. Diese vordefinierten Tags werden aus Warnungen zugeordnet und basieren auf Informationen aus Quellen wie dem Warnungsfeld, Warnungs-Tags oder zusätzlichen Warnungsinformationen. Wenn die erforderlichen Daten fehlen und die ausgewählte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Quelle Warnungs-CI oder Warnungs-CI-Schlüssel ist, wird das Tag mit dem Wert Configuration Item (CI) aus dem ausgefüllt Configuration Management Database (CMDB). Vordefinierte Tags werden leicht anhand ihrer Beschreibung identifiziert, die sofort einsatzbereit ist.

Sie können ein oder mehrere Tags an eine Warnungs-Clustering-Definition anhängen, die die Bedingungen für die Warnungskorrelation angibt. Sie können entweder eine eigene Warnungs-Clustering-Definition erstellen oder eine von der Anwendung bereitgestellte vordefinierte Definition verwenden. Vordefinierte Definitionen enthalten zugeordnete Tags.

Wichtig: Stellen Sie sicher, dass Sie vordefinierte Definitionen vor der Verwendung aktivieren. In neuen Systemen sind standardmäßig mehrere Definitionen aktiv. Die verbleibenden müssen aktiviert werden. Weitere Informationen finden Sie unter Aktivieren Sie eine vordefinierte Warnungs-Clustering-Definition.

Sobald ein oder mehrere Warnungs-Clustering-Tags an eine Definition angehängt wurden, erfasst das System Warnungen und überprüft, ob ihre Tags allen in der Definition angegebenen Tag-Werten entsprechen. Warnungen mit übereinstimmenden oder ähnlichen Tag-Werten werden gruppiert. Neue eingehende Warnungen treten einer vorhandenen Gruppe bei, wenn ihre Tags mit den Tags in der zum Erstellen der Gruppe verwendeten Definition übereinstimmen.

Für die Tag-Cluster-Gruppierung werden Warnungen basierend auf dem in den Warnungs-Clustering-Einstellungen definierten Zeitrahmen einer Gruppe hinzugefügt. Die Zeit zwischen der ersten Warnung (virtuelle Warnung) und nachfolgenden Warnungen wird ausgewertet. Wenn zwei neue Warnungen empfangen werden und ihre Zeitdifferenz innerhalb des definierten Zeitrahmens liegt, werden sie der Gruppe hinzugefügt. Die Generierungszeit des ersten Ereignisses wird verwendet, um die Relevanz des Zeitrahmens zu bestimmen.

Zugehörige Informationen

- Alarm-Clustering-Tags erstellen
- Alarm-Clustering-Definitionen erstellen
- Aktivieren Sie eine vordefinierte Warnungs-Clustering-Definition
- Hängen Sie ein vordefiniertes Tag an eine Tag-basierte Warnungsgruppierungsdefinition an
- Event-Regel konfigurieren, um den Warnungsinhalt anzupassen
- Warnungstags

Alarm-Clustering-Tags erstellen

Erstellen Sie optimierte Warnungskorrelationen mit Warnungs-Clustering-Tags, indem Sie Warnungen gruppieren, die identische oder ähnliche Tags verwenden, basierend auf Ihrer konfigurierten Übereinstimmungsmethode. Dies reduziert das Rauschen, verbessert die Priorisierung von Incidents und verbessert die betriebliche Effizienz, wodurch die Problemlösung und Reaktionszeiten beschleunigt werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Tags für Warnungs-Clustering**an.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie die Werte im Ereignismanagement-Formular „Tag-basiertes Warnungs-Clustering-Tag“ ein.
4. Wählen Sie **Absenden**.

Ergebnis
Das Tag wird in der Tabelle Tag-basiertes Warnungs-Clustering-Tags angezeigt.

Alarm-Clustering-Definitionen erstellen

Definieren Sie Bedingungen für Warnungs-Clustering, um ein oder mehrere Warnungs-Clustering-Tags auszulösen, die helfen, Warnungsgruppen aus weniger Warnungen zu erstellen. Das Erstellen von Warnungsgruppen aus weniger Warnungen reduziert das Rauschen, wodurch es einfacher wird, kritische Incidents zu identifizieren, Antworten zu priorisieren und Probleme effektiv zu verwalten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Um eine Tag-definition zu erstellen, müssen Anwender Filter verwenden, um zu definieren, für welche Warnungen die Definition gilt, und Gruppierungskriterien zu definieren, indem sie angeben, welche Feldwerte verglichen werden sollen, um eine Gruppe zu erstellen.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Warnungs-Clustering-Definitionen**an.
2. Wählen Sie **Neu**.
3. Konfigurieren Sie die Felder im Ereignismanagement Formular zur Definition der Tag-basierten Warnungsgruppierung.
4. Wählen Sie **Speichern**.

Ergebnis
Die Definition wird in der Tabelle „Tag-basierte Warnungs-Clustering-Definitionen“ und „Service Operations-Arbeitsbereich (ITOM) > Gruppierungsautomatisierung“ angezeigt. Von dieser Definition erstellte Warnungsgruppen werden als Tag-Cluster-Gruppen kategorisiert.

Aktivieren Sie eine vordefinierte Warnungs-Clustering-Definition

Aktivieren Sie vor der Verwendung die vordefinierten Warnungs-Clustering-Definitionen, die mit der Anwendung Tag-basierte Warnungs-Clustering-Engine bereitgestellt werden. Die Verwendung dieser vorkonfigurierten Definitionen minimiert die Setup-Zeit und stellt einen effizienteren Konfigurationsprozess sicher, was eine schnellere Implementierung und ein optimiertes Warnungsmanagement ermöglicht.

Vorbereitungen

Wichtig: Wenn Sie die Anwendung „Tag-basierte Warnungs-Clustering-Engine“ bereits verwenden, sind alle vordefinierten Definitionen inaktiv und müssen aktiviert werden. Im Gegensatz dazu finden neue Kunden standardmäßig mehrere Definitionen aktiv, was eine sofortige Nutzung der Warnungs-Clustering-Funktionen ohne zusätzliches Setup ermöglicht.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **#Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Clustering-Definitionen**an.
2. Wählen Sie eine vordefinierte Definition aus.

   Hinweis: Eine vollständige Liste der verfügbaren vordefinierten Definitionen finden Sie unter Liste der vordefinierten Tag-basierten Warnungsgruppierungsdefinitionen.

3. Wählen Sie im Formular „Tag-basierte Warnungs-Clustering-Definition“ die aus **Aktiv** Kontrollkästchen.
4. Wählen Sie **Speichern**.

Ergebnis

In der Tabelle „Tag-basierte Warnungs-Clustering-Definitionen“ die **Aktiv** Das Feld für die aktivierte Definition zeigt den Wert an **Wahr** . Sie können dieser Definition jetzt ein Warnungs-Clustering-Tag zuordnen, um eine effektive Gruppierung von Warnungen basierend auf den definierten Kriterien zu ermöglichen.

Hängen Sie ein vordefiniertes Tag an eine Tag-basierte Warnungsgruppierungsdefinition an

Beginnen Sie mit Warnungs-Clustering schneller, indem Sie ein vordefiniertes Warnungs-Clustering-Tag an eine Tag-basierte Warnungs-Clustering-Definition in anhängen Ereignismanagement. Durch die Zuordnung eines vordefinierten Tags stellen Sie sicher, dass Warnungen, die die angegebenen Kriterien erfüllen, effektiv gruppiert werden, was die Identifizierung und Reaktion auf zugehörige Incidents erleichtert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Anwendung „Tag-basierte Warnungs-Clustering-Engine“ enthält eine Reihe vordefinierter Warnungs-Clustering-Tags. Hängen Sie ein Tag an eine Tag-basierte Warnungs-Clustering-Definition an, um die Bedingungen anzugeben, die für die Warnungskorrelation erfüllt sein müssen. Dies ermöglicht eine effektive Gruppierung von Warnungen basierend auf gemeinsam genutzten Merkmalen und verbessert die Genauigkeit und Effizienz der Reaktion auf Incidents und des Managements.

Prozedur

1. Navigieren zu **Alle** > **#Ereignismanagement** > **Tag-Basierte Warnungs-Clustering-Engine** > **Warnungs-Clustering-Definitionen**an.
2. Wählen Sie eine Definition aus.
3. Wählen Sie im Abschnitt Tag-basierte Warnungs-Clustering-Definitionen Tags M2M die Option aus **Fügen Sie eine neue Zeile ein** .
4. Verwenden Sie das Suchfeld, um ein vordefiniertes Warnungs-Clustering-Tag zu suchen, und wählen Sie dann das grüne Häkchen aus, um Ihre Auswahl zu bestätigen.

   Hinweis: Vordefinierte Tags sind an ihrer Beschreibung erkennbar, die „sofort einsatzbereit“ enthält. Eine vollständige Liste der verfügbaren vordefinierten Tags finden Sie unter Liste der vordefinierten Warnungsgruppierungs-Tags.

5. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Das vordefinierte Warnungs-Clustering-Tag ist jetzt an die Tag-basierte Warnungs-Clustering-Definition angehängt. Diese Zuordnung ermöglicht die effektive Gruppierung von Warnungen basierend auf den angegebenen Kriterien, wodurch das Warnungsmanagement und die Effizienz der Reaktion verbessert werden.

Textbasierte Warnungsgruppierung

Bei der textbasierten Warnungsgruppierung werden Warnungen basierend auf bestimmten Textmustern oder Stichwörtern innerhalb des Warnungsinhalts organisiert und korreliert. Dieser Ansatz gruppiert Warnungen dynamisch, die ähnliche Textmerkmale aufweisen, z. B. Fehlermeldungen oder Ereignisbeschreibungen, um eine flexiblere und adaptive Verwaltung von Warnungen zu ermöglichen.

Die EM-Warnungs-Clustering-Lösung ist eine Methode, mit der Warnungen basierend auf Ähnlichkeiten in bestimmten Feldern und Formularclustern oder -Gruppen korreliert werden. In ServiceNow Ereignismanagement, Erstellt Cluster basierend auf den Feldern Beschreibung, Metrikname und Konfigurationselement.Klasse. Diese Lösung organisiert Warnungen in textbasierte Gruppen. Wenn eine neue Warnung eingeht, identifiziert die ML-Vorhersage den entsprechenden Cluster und gruppiert Warnungen innerhalb desselben Clusters.

Hinweis: Der ML-Vorhersageauftrag ist asynchron und weist Clustern Echtzeitwarnungen zu, was zu leichten Verzögerungen führen kann. Diese Verzögerung kann dazu führen, dass textbasierte Gruppen einige Minuten später erstellt werden, da der Warnungsgruppierungsauftrag einmal pro Minute ausgeführt wird. Wenn Vorhersageergebnisse während einer Ausführung nicht verfügbar sind, werden sie im nächsten Gruppierungsauftrag erneut überprüft.

Damit die textbasierte Logik ausgeführt werden kann, müssen Sie über verfügen Predictive Intelligence Plugin (com.glide.platform_ml) installiert und die Definition der EM Alert Clustering-Lösung aktiviert.

Es gibt bestimmte Einstellungen oder Grenzwerte, die verwendet werden, um das Verhalten der textbasierten Warnungsgruppierung zu steuern. Diese Schwellenwerte definieren die Kriterien dafür, wie Warnungen basierend auf Textmustern oder Attributen gruppiert werden. Die textbasierten Schwellenwerte sind:

- Cluster-Qualitätsschwellenwert: Der Cluster-Qualitätsschwellenwert (*`sa_analytics.alert_grouping_tb_cluster_quality_threshold`*) Bestimmt die Mindestqualität, die erforderlich ist, damit ein Warnungscluster als gültig betrachtet wird. Dieser Schwellenwert stellt sicher, dass nur Cluster mit einem Mindestmaß an Ähnlichkeit und Zuverlässigkeit verwendet werden. Cluster, die diesen Schwellenwert erfüllen, gelten als gültig, wodurch die Genauigkeit der Gruppierungen verbessert und das Rauschen durch irrelevante oder qualitativ mindernde Cluster reduziert wird. Der Bereich des Schwellenwerts liegt zwischen 1 und 100, und der Standardwert ist 70.
- Warnungsrang-Schwellenwert: Der Warnungsrang-Schwellenwert (*`sa_analytics.alert_grouping_tb_alert_rank_threshold`*) Definiert den Mindestrang, der erforderlich ist, damit eine Warnung in eine Gruppe aufgenommen werden kann. Dieser Schwellenwert stellt sicher, dass nur Warnungen mit einem bestimmten Ähnlichkeitsgrad gruppiert werden, wodurch Warnungen mit niedrigerem Rang herausgefiltert werden, um die Qualität der Warnungsgruppe beizubehalten. Der Standardwert ist 0,3, wobei kleinere Werte auf eine bessere Ähnlichkeit hinweisen.

Hinweis: Um diese Eigenschaften zu verwenden, müssen Sie Eigenschaften mit denselben Namen erstellen und ihnen die erforderlichen Werte zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Definition der EM-Warnungs-Clustering-Lösung befindet sich in der Tabelle [ml_Capability_Definition_Clustering]. Um darauf zuzugreifen, navigieren Sie zu **Predictive Intelligence** > **Clustering** > **Lösungsdefinitionen**an.

Informationen zum Überprüfen, ob die Lösungsdefinition aktiv ist, finden Sie unter Überprüfen Sie die textbasierte Clustering-Lösung. Um die Definition der EM-Warnungs-Clustering-Lösung zu deaktivieren, deaktivieren Sie die textbasierte Warnungsgruppierung, indem Sie die Eigenschaft festlegen *sa_analytics.text_based_group_enabled*Bis Falsch Und löschen **Aktiv** Kontrollkästchen in der Definition der EM-Warnungs-Clustering-Lösung.

Beispiel für textbasierte Warnungsgruppierung

Szenario	Beispiel
Netzwerkkonnektivitätsprobleme: Es gibt weit verbreitete Netzwerkkonnektivitätsprobleme, die mehrere Abteilungen betreffen.	Warnungen von verschiedenen Netzwerküberwachungstools können Probleme wie „Netzwerksegment ausgefallen“, „hoher Paketverlust“ oder „Konnektivitätsprobleme im Subnetz“ melden. Die textbasierte Warnungsgruppierung verwendet die EM-Warnungs-Clustering-Lösung und ML Predictor, um das Warnungsmanagement zu optimieren. Die EM-Warnungs-Clustering-Lösung verwendet Natural Language Processing (NLP)-Algorithmen, um allgemeine Textmuster in Warnungen wie „Netzwerksegment ausgefallen“ oder „hoher Paketverlust“ zu analysieren und zu identifizieren. Anschließend werden diese Warnungen basierend auf ihrer Textähnlichkeit gruppiert und zugehörige Probleme gruppiert. Die ML-Vorhersage verbessert diesen Prozess weiter, indem neue Warnungen in Echtzeit ausgewertet und basierend auf ihren Textmustern den entsprechenden vorhandenen Clustern zugewiesen werden. Diese dynamische Gruppierung bietet eine konsolidierte Ansicht der Konnektivitätsprobleme, sodass Netzwerktechniker die Ursache der Probleme schneller diagnostizieren und effizienter beheben können.

Überprüfen Sie die textbasierte Clustering-Lösung

Ereignismanagement Verwendet Natural Language Processing (NLP)-Algorithmen, um allgemeine Textmuster in Warnungen zu identifizieren und Warnungsgruppen durch Clustering zu erstellen. Dieser Ansatz organisiert nicht nur ähnliche Warnungen effizient, sondern reduziert auch Rauschen und hilft, sich auf wichtige Probleme zu konzentrieren, wodurch das allgemeine Warnungsmanagement verbessert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Predictive Intelligence Plugin (com.glide.platform_ml) Ist installiert.

Stellen Sie den Parameter sicher *sa_analytics.text_based_group_enabled*Ist auf festgelegt Wahr .

Hinweis: Wenn Predictive Intelligence Plugin ist nicht installiert, die textbasierte Logik wird nicht ausgeführt, auch wenn *sa_analytics.text_based_group_enabled*Ist auf „wahr“ festgelegt. Dies liegt daran, dass die textbasierte Gruppierung auf Clustering-Warnungen basierend auf der Beschreibung, dem Metriknamen und der CI-Klasse basiert. Ohne das Plugin kann kein Clustering durchgeführt werden, und daher werden keine textbasierten Gruppen erstellt, unabhängig vom aktiven Status.

Stellen Sie sicher, dass die Tabelle „Warnungen“ [em_Alerts] mindestens 100 Warnungen enthält.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Predictive Intelligence** > **Clustering** > **Lösungsdefinitionen**an.
   Die Seite Clustering-Definitionen wird geöffnet.
2. Wählen Sie EM aus Warnung Clustering-Lösung.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.
4. Wählen Sie Aus **Aktualisieren Und Erneut Trainieren** .
   Weitere Informationen zu ML-Lösungen finden Sie unter Überprüfen Sie Ihre ML-Lösungsschulungsaufträge .

Manuelle Warnungsgruppierung

Die manuelle Warnungsgruppierung umfasst die Organisation und Kategorisierung von Warnungen basierend auf anwenderdefinierten Kriterien und direkten Eingriffen.

Sie können Warnungen manuell auswählen und gruppieren, um Incidents besser zu verwalten und zu lösen, indem Sie die Gruppierung an bestimmte Anforderungen, Relevanz oder Kontext anpassen. Dieser Ansatz stellt sicher, dass Warnungen effektiv kategorisiert werden, wodurch das Incident-Management und die Reaktionseffizienz insgesamt verbessert werden.

Erstellen Sie eine Warnungsgruppe manuell

Erstellen Sie manuell eine Warnungsgruppe, um zugehörige Warnungen zu organisieren und zu verwalten, wenn Sie keine geplanten Aufgaben verwenden. Dies bietet Flexibilität, Warnungen bei Bedarf zu gruppieren, um eine effektive Lösung zu gewährleisten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

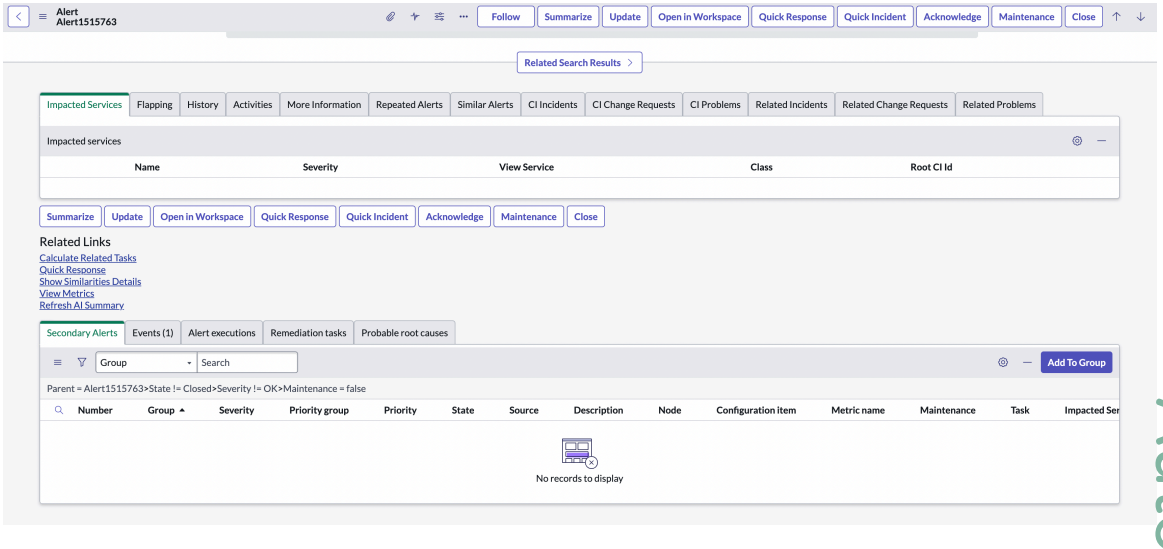
1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Wählen Sie die Warnungsnummer aus, um die Warnung zu öffnen.

   Die Warnung wird verwendet, um eine Warnungsgruppe zu erstellen, die als primäre Warnung festgelegt ist und der Sie sekundäre Warnungen hinzufügen können.

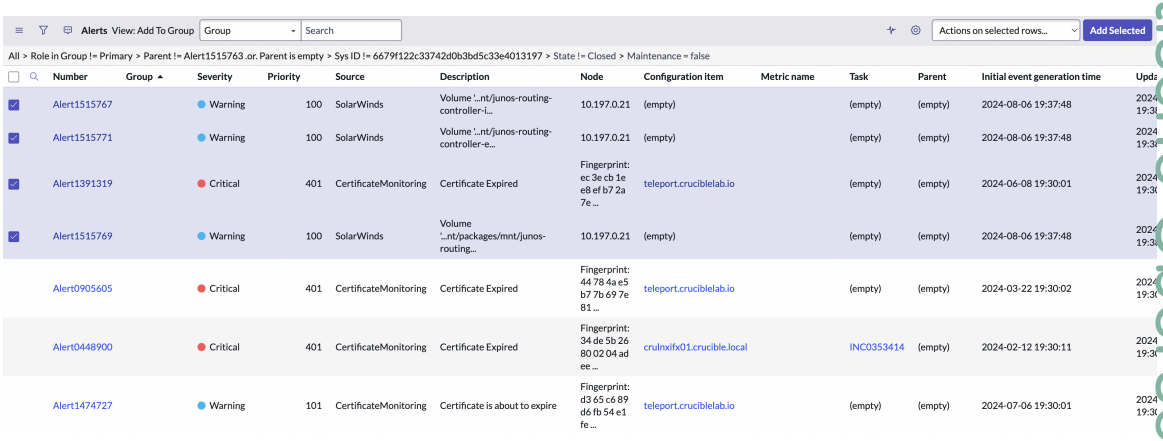
   Hinweis: Eine geschlossene Warnung kann nicht als übergeordnete Warnung zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

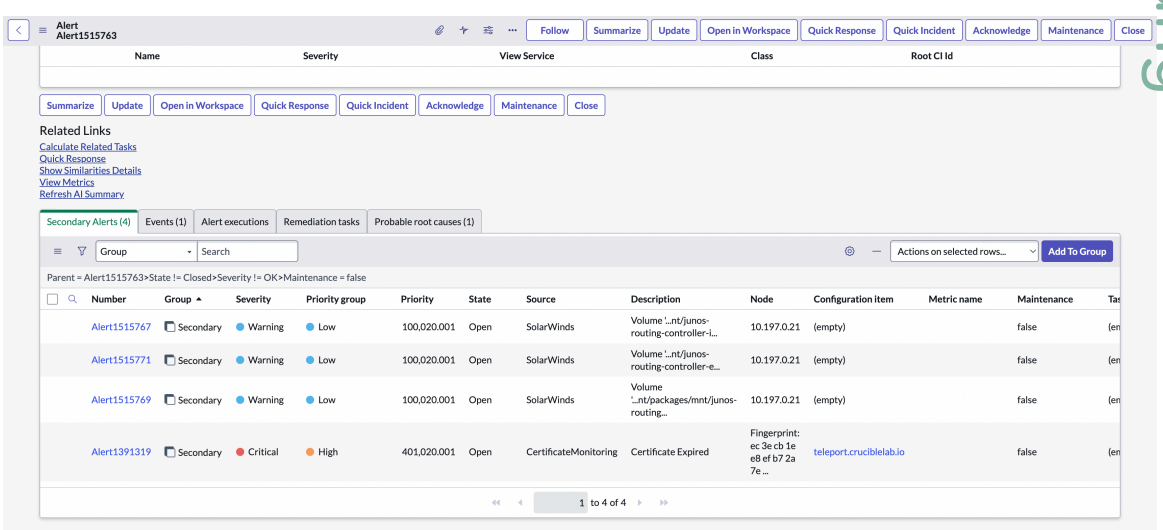
3. Scrollen Sie nach unten und in **Sekundäre Warnungen** Wählen Sie die Registerkarte aus **Zu Gruppe Hinzufügen** .



4. Aktivieren Sie die Kontrollkästchen für alle Warnungen, die Sie der Gruppe als sekundäre Warnungen hinzufügen möchten, und wählen Sie aus **Auswahl Hinzufügen** .



5. In **Sekundäre Warnungen** Registerkarte die Warnungen anzeigen, die als sekundär hinzugefügt wurden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einer vorhandenen Warnungsgruppe manuell eine sekundäre Warnung hinzu

Fügen Sie alle relevanten Warnungen, die während der Überprüfung einer automatisierten Warnungsgruppe erkannt wurden, als sekundäre Warnung hinzu, um die Vollständigkeit und das Dienstprogramm der Gruppe für die Fehlerbehebung bei Incidents zu verbessern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

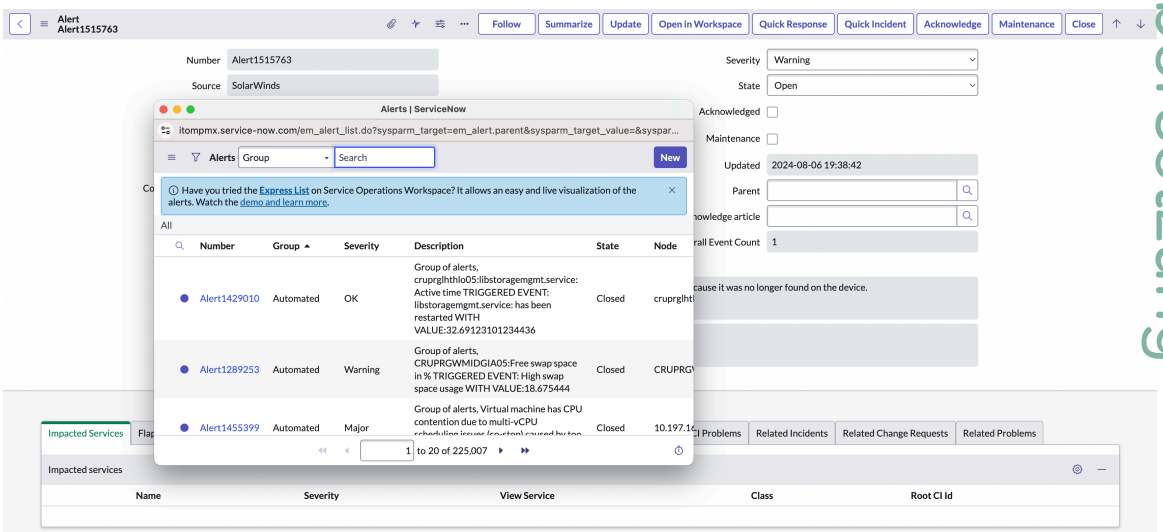
Warum und wann dieser Vorgang ausgeführt wird

Die Warnung, die Sie einer neuen Gruppe hinzufügen möchten, ist möglicherweise bereits Teil einer anderen Gruppe. Wenn Sie sie der neuen Gruppe hinzufügen, wird sie automatisch aus der aktuellen Gruppe entfernt, wodurch die Gruppenzuordnung geändert wird. Alternativ können Sie das übergeordnete Element der Warnung aktualisieren, um sie in eine andere Gruppe zu verschieben. Durch Angabe eines neuen übergeordneten Elements wird die Warnung an die Gruppe des neuen übergeordneten Elements übertragen und aus der vorherigen entfernt. Dies kann durch Aktualisieren von erreicht werden **Übergeordnet** Feld im Warnungsformular oder durch Ändern von **Übergeordnet** Spalte in der Warnungsliste.

Hinweis: Wenn Sie einer Gruppe eine Warnung hinzufügen, wird diese Aktion als Feedback für die Warnungsgruppierung als Teil des Prozesses protokolliert. Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus. Zukünftige Erweiterungen dieser Funktion werden in Betracht gezogen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Wählen Sie die Warnungsnummer aus, um die Warnung zu öffnen.
3. In **Übergeordnet** Feld nach der Warnung suchen, die Sie als übergeordnete Warnung für die ausgewählte Warnung zuweisen möchten.



4. Wählen Sie die Nummer der übergeordneten Warnung aus.
5. Wählen Sie **Aktualisieren**.

Ergebnis

Die Warnung wird der ausgewählten übergeordneten Warnung als sekundäre Warnung hinzugefügt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

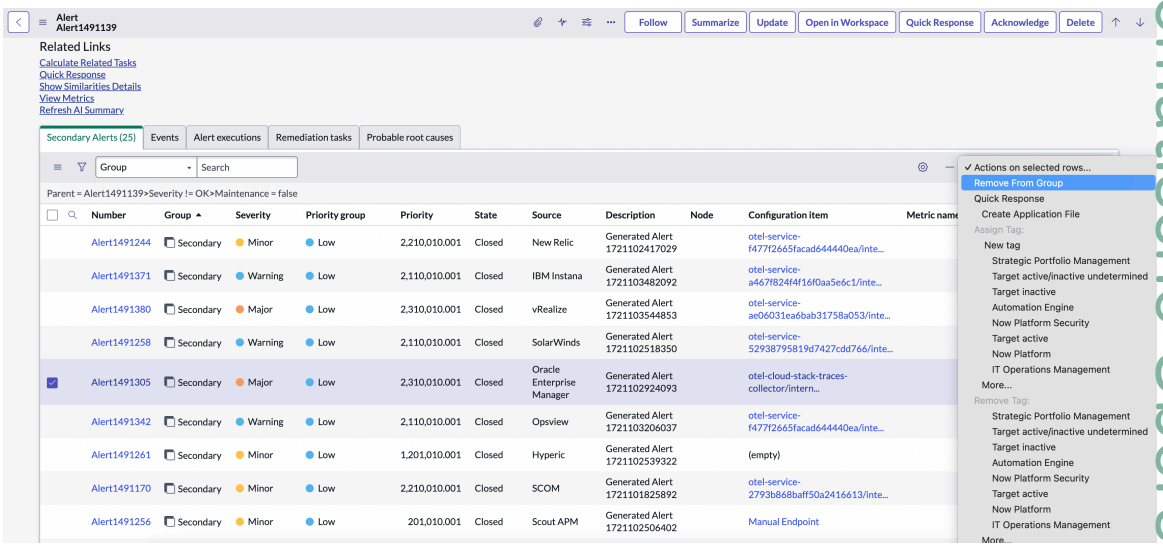
Warnungen aus einer Warnungsgruppe entfernen

Entfernen Sie eine Warnung, wenn Sie die Genauigkeit und den Nutzen der Gruppe bei der Behebung eines Incident verbessern möchten. Wenn diese Aktion die Gruppe mit einer oder keiner Warnung verlässt, wird die Gruppe gelöscht und nicht mehr als Warnungsgruppe angezeigt.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Wählen Sie die Warnungsnummer aus, um die Warnungsgruppe zu öffnen.
3. Scrollen Sie nach unten, um anzuzeigen **Sekundäre Warnungen** Registerkarte.
4. Aktivieren Sie das Kontrollkästchen neben der Warnung, die Sie aus der Gruppe entfernen möchten.
5. Wählen Sie im Menü Aktionen für ausgewählte Zeile die Option aus **Aus Gruppe Entfernen** .



Ergebnis
Die Warnung wird aus der Gruppe entfernt.

Konfigurieren Sie Arbeitsnotizen, um Begründungen der Warnungsgruppierung zu erfassen

Wenn Warnungen zu einer Gruppe hinzugefügt werden, wird im Feld „Arbeitsnotizen“ der Warnung eine Nachricht aufgezeichnet, um zu erklären, warum die Warnung in die Gruppe aufgenommen wurde. Definieren Sie Warnungstypen zum Erstellen dieser Arbeitsnotizen im Zusammenhang mit der Begründung der Warnungsgruppe.

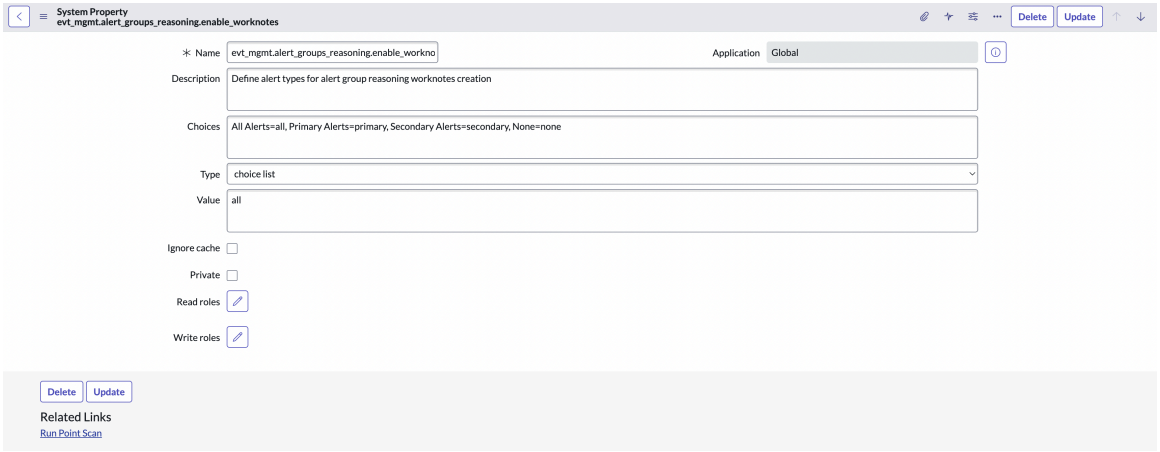
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie nach der Eigenschaft `evt_mgmt.alert_groups_reasoning.enable_worknotes`.
3. Öffnen Sie die Eigenschaft.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. In **Auswahlmöglichkeiten** Feld, definieren Sie Warnungstypen zum Erstellen von Arbeitsnotizen im Zusammenhang mit der Begründung der Warnungsgruppe.

Eigenschaftswerte

Wert	Beschreibung
Alle Warnungen	Arbeitsnotizinformationen werden für jede Warnung generiert.
Primäre Warnungen	Arbeitsnotizdaten werden nur für primäre Warnungen generiert.
Sekundäre Warnungen	Arbeitsnotizdaten werden nur für sekundäre Warnungen generiert.
Keine	Es werden keine Arbeitsnotizdaten generiert.

5. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Warnungsgruppierungstypen und Erstellungsmethoden

Anwendungsservice in Ereignismanagement

Ein Anwendungsservice ist eine Reihe untereinander verbundener Anwendungen und Hosts, die so konfiguriert sind, dass sie einer Organisation einen Service bereitstellen.

Allgemeine Informationen zu Anwendungsservices finden Sie unter Anwendungsservices .

Erstellen Sie in manuell einen Anwendungsservice Ereignismanagement

Sie können Anwendungsservices manuell erstellen. Ereignismanagement Kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Anwendungsservice ist ein Satz verbundener Anwendungen und Hosts, die so konfiguriert sind, dass sie der Organisation einen Service anbieten. Anwendungsservices können intern sein, beispielsweise ein E-Mail-System einer Organisation, oder auf Kunden ausgerichtet sein, z. B. die Website einer Organisation. Verwenden Sie Anwendungsservices, um Services in Ihrer Organisation zu organisieren, zu verwalten und zu überwachen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservices unterstützen diese CI-Typen nicht:

- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Erstellen Sie ein Serviceformular

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Anwendungsservicenamen ein.
Eigentum von	Geben Sie einen Inhaber an, der für diesen Anwendungsservice im Unternehmen verantwortlich ist.
Einstiegspunkte hinzufügen:	
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. cmdb_ci_appl für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus.

Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Details zum Gruppieren von Anwendungsservices finden Sie unter Gruppieren Sie Anwendungsservices .

Details zur Steuerung des Anwenderzugriffs auf Anwendungsservices finden Sie unter Steuern Sie den Anwenderzugriff auf Anwendungsservices .

Konvertieren Sie manuelle Services in Anwendungsservices

Sie können vorhandene manuelle Services in Anwendungsservices konvertieren. Ereignismanagement Kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Manuelle Services werden nicht mehr unterstützt, und dieser Servicetyp sowie erkannte Services wurden durch Anwendungsservices ersetzt. Alle vorhandenen manuellen Services müssen in Anwendungsservices konvertiert werden.

Während des Konvertierungsvorgangs:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der manuelle Serviceeintrag wird von der Tabelle für manuelle Services [cmdb_ci_service_manual] in die Tabelle für zugeordnete Anwendungsservices [cmdb_ci_service_discovered] durch Änderung der Datensatzklasse verschoben.
- Alle ursprünglichen manuellen Serviceattribute, z. B. Name, Besitzer und Betriebsstatus, werden in den Anwendungsservices beibehalten.
- Die Konfigurationselemente (Configuration Items, CIs) des manuellen Service werden nach der Konvertierung in den Anwendungsservices beibehalten.
- Das System fragt die CMDB nach den neuesten CI-Changes ab und wendet die CI-Auswirkungsregeln an.

Anwendungsservice Unterstützt diese CI-Typen nicht:

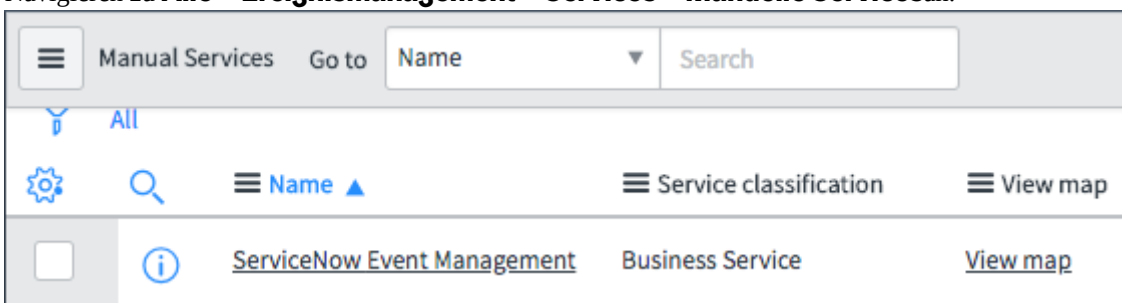
- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Wenn die vorherigen CI-Typen im manuellen Service verwendet werden, den Sie konvertieren möchten, schlägt die Konvertierung fehl. CIs dieses Typs sollten vor der Konvertierung entfernt werden. Sie können ersetzt werden, indem den Anwendungsservices nach der Konvertierung neue CIs hinzugefügt werden.

Wenn Ihre Instanz ServiceNow Domain Separation verwendet, schlägt die Konvertierung fehl, wenn sich CIs aus mehreren Domänen im gleichen Service befinden. Ersetzen oder entfernen Sie relevante CIs vor der Konvertierung. Die konvertierten Anwendungsservices enthalten nur CIs, die derselben Domäne wie die Anwendungsservices zugewiesen sind.

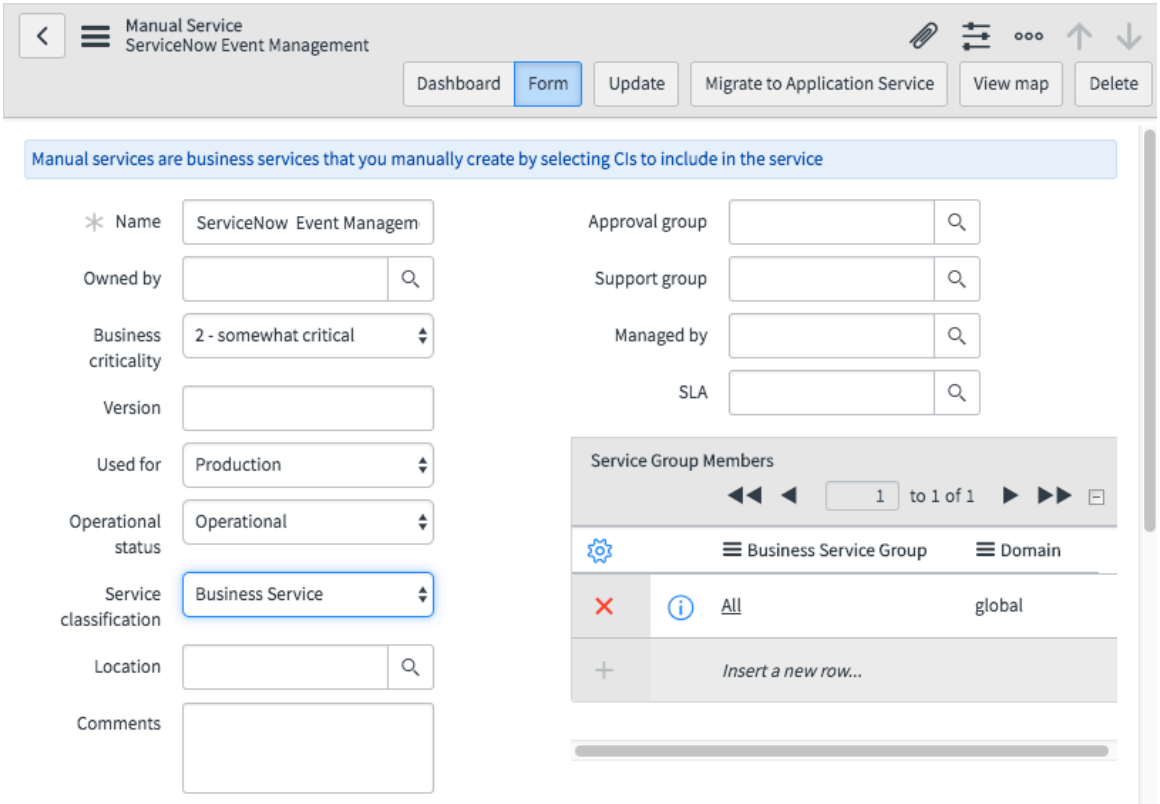
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Manuelle Services**an.



2. Wählen Sie den manuellen Service aus, den Sie in Anwendungsservices konvertieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Zu Anwendungsservice migrieren**.
4. Klicken Sie auf **OK**.

Ergebnis

- Die CIs aus dem manuellen Service werden den konvertierten Anwendungsservices hinzugefügt.
- Nachdem der Konvertierungsprozess abgeschlossen ist, wird das Formular „Anwendungsservices“ geöffnet.

Konvertieren Sie manuelle Services mithilfe der API in Anwendungsservices

Sie können eine JavaScript-API verwenden, um vorhandene manuelle Services in Anwendungsservices zu konvertieren. Ereignismanagement Kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Manuelle Services werden nicht mehr unterstützt, und dieser Servicetyp sowie erkannte Services wurden durch Anwendungsservices ersetzt. Alle vorhandenen manuellen Services müssen in Anwendungsservices konvertiert werden. Stellen Sie sicher, dass jede Automatisierung manueller Services (wie Geschäftsregeln und regelmäßige Aufgaben) erstellt und getestet wird, bevor Sie sie in Anwendungsservices konvertieren.

Hinweis: Manuelle Services sind statisch und behalten ihre ursprüngliche Struktur nach der Konvertierung in Anwendungsservices bei. Um importierte manuelle Services mit dem vorhandenen CMDB-Status zu aktualisieren, füllen Sie entweder die ursprünglichen manuellen Services, um sicherzustellen, dass alle CIs dem richtigen Service zugewiesen sind, oder führen Sie nach der Konvertierung die Option zum **Mit CMDB-Changes aktualisieren** aus.

Während des Konvertierungsvorgangs:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der manuelle Serviceeintrag wird von der Tabelle für manuelle Services [cmdb_ci_service_manual] in die Tabelle für zugeordnete Anwendungsservices [cmdb_ci_service_discovered] durch Änderung der Datensatzklasse verschoben.
- Alle ursprünglichen manuellen Serviceattribute, z. B. Name, Besitzer und Betriebsstatus, werden in den Anwendungsservices beibehalten.
- Die Konfigurationselemente (Configuration Items, CIs) des manuellen Service werden nach der Konvertierung in den Anwendungsservices beibehalten.
- Das System fragt die CMDB nach den neuesten CI-Changes ab und wendet die CI-Auswirkungsregeln an.

Die maximale Anzahl von CI-Verbindungen, die Anwendungsservices während dieses Vorgangs hinzugefügt werden, wird von gesteuert sa.service.max_ci_service_population Eigenschaft. Standardmäßig ist der Wert 1000 festgelegt (1000 Verbindungen). Eine höhere Anzahl von CI-Verbindungen kann zu Leistungsproblemen führen. Um die maximale Anzahl der hinzugefügten CI-Verbindungen anzupassen, fügen Sie die Eigenschaft sa.service.max_ci_service_population hinzu, wie in beschrieben Fügen Sie eine Systemeigenschaft hinzu .

Wenn versucht wird, mehr CIs zu verarbeiten als der in der Eigenschaft „sa.service.max_ci_service_population angegebene Wert, schlägt der Vorgang fehl.

Führen Sie den Konvertierungsprozess in kleinen Blöcken von jeweils ungefähr 10 aus, um den problematischen Service im Falle eines Konvertierungsproblems leichter zu lokalisieren.

Anwendungsservices Diese CI-Typen werden nicht unterstützt:

- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Wenn die vorherigen CI-Typen im manuellen Service verwendet werden, den Sie konvertieren möchten, schlägt die Konvertierung fehl. CIs dieses Typs sollten vor der Konvertierung entfernt werden. Sie können ersetzt werden, indem den Anwendungsservices nach der Konvertierung neue CIs hinzugefügt werden.

Wenn Ihre Instanz ServiceNow Domain Separation verwendet, schlägt die Konvertierung fehl, wenn sich CIs aus mehreren Domänen im gleichen Service befinden. Ersetzen oder entfernen Sie relevante CIs vor der Konvertierung. Die konvertierten Anwendungsservices enthalten nur CIs, die derselben Domäne wie die Anwendungsservices zugewiesen sind.

Die JavaScript-API lautet:

```
BusinessServiceManager.migrateManualToApplicationService(String service_id)
```

Parameter

Name	Typ	Beschreibung
service_id	Zeichenfolge	Sys-ID des zu konvertierenden manuellen Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Typ	Beschreibung
Boolescher Wert	„true“ für eine erfolgreiche Konvertierung, „false“ für eine fehlgeschlagene Konvertierung

Wobei sys_ID Eines vorhandenen manuellen Service ist 451047c6c0a8016400de0ae6df9b9d76 , Führen Sie die folgende API aus, um sie in Anwendungsservices zu konvertieren:

```
var bsManager = new SNC.BusinessServiceManager();
var res =
 bsManager.migrateManualToApplicationService("451047c6c0a8016400de0ae6df9b9d76");
```

Zugehörige Informationen

BusinessServiceManager – Global

Konfigurieren von CIs in einem manuellen Service als manueller Cluster

Konfigurieren oder ändern Sie ein CI als bestimmtes CI oder eine generische CI-Klasse in einem manuellen Service (der nicht automatisch erkannt wurde) als manuell definiertes Cluster. Ein manueller Cluster stellt Redundanzfähigkeiten im Cluster bereit und bietet kontinuierliche Vorgänge oder Services des gesamten Clusters, wenn ein oder mehrere CIs in diesem Cluster ausfallen.

Mit dem manuellen Cluster können Sie CIs in einem Service unter einem logischen Cluster gruppieren. In der Auswirkungsstruktur können Sie die relative Auswirkung eines Clustermitglieds auf den Cluster festlegen.

Hinweis: Die Erstellung geschachtelter manueller Cluster (Cluster innerhalb des Clusters) wird derzeit nicht unterstützt.

Sobald das CI als manueller Cluster definiert ist, zeigt seine Auswirkungsberechnung das Ausmaß eines Ausfalls für seine untergeordneten CIs an. Die Auswirkungsberechnung verwendet Faktoren wie Auswirkungsregeln und CI-Beziehungen, um den Schweregrad einer generierten Warnung zu berechnen. Auswirkungsregeln, die für die Berechnung der Auswirkung verwendet werden, schätzen den Umfang oder Schweregrad eines Ausfalls basierend auf betroffenen CIs und bestimmen, wie die Auswirkung auf übergeordnete oder untergeordnete Entitäten gilt, die Teil eines Anwendungsservice sind.

Das Ausmaß eines Ausfalls kann 100 % niedriger, 60 % betroffen, 40 % beeinträchtigt oder 20 % beeinträchtigt sein.

Redundanz ist in Auswirkungsregeln definiert. Sie können beispielsweise definieren, dass das übergeordnete CI kritisch ist, wenn mindestens zwei untergeordnete CIs kritisch sind. Die Auswirkung von untergeordneten CIs auf übergeordnete CIs beträgt nicht immer 100 %. Wenn die CIs aller drei untergeordneten Elemente betroffen sind, ist die Auswirkung um 100 % geringer.

In einer Servicezuordnung können Sie ein bestimmtes CI oder eine generische CI-Klasse in einem manuellen Service als manuell definiertes Cluster konfigurieren oder ändern. Bei der Konfiguration als generische CI-Klasse werden alle CIs der ausgewählten Klasse in diesem Service gleich konfiguriert.

Zugehörige Informationen

Warnungsauswirkungsberechnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen manuellen Cluster

Stellen Sie Redundanzfähigkeiten eines gesamten Clusters bereit, wenn ein oder mehrere CIs in diesem Cluster ausfallen. Indem Sie die relativen Auswirkungen eines Clustermitglieds auf die Clusterinformationen anzeigen, können Sie die Quelle von Warnungen besser verstehen und Korrekturmaßnahmen ergreifen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
In einem manuellen Service, der nicht automatisch erkannt wurde, können Sie ein bestimmtes CI oder eine generische CI-Klasse manuell unter einem logischen Cluster gruppieren. Die relative Auswirkung eines Clustermitglieds auf den Cluster kann in der Auswirkungsstruktur konfiguriert werden.

Weitere Informationen finden Sie unter Warnungsauswirkungsberechnung.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Manuelle Cluster**an.
2. Wählen Sie **Neu**.
3. In **Wählen Sie einen Service aus, der diesen manuellen Cluster enthält** Wählen Sie einen Anwendungsservice aus, um den neuen manuellen Cluster basierend auf einem bestimmten CI oder einer allgemeinen CI-Klasse aufzunehmen.
   Die Clusternummer wird automatisch generiert und in angezeigt **Nummer** Feld.

   a. Wählen Sie das Symbol „Suchen mit Liste“ ( ) In **Service** Feld.

   b. Wählen Sie in der Tabelle „CMDB CI-Service“ [cmdb_ci_Service_detected] einen manuell erstellten Service aus.
   Informationen zum Definieren eines neuen Anwendungsservice finden Sie unter Erstellen Sie in manuell einen Anwendungsservice Ereignismanagement.

   c. **Wahlweise:** Zeigen Sie eine Vorschau des Datensatzes an, indem Sie auf das Symbol Vorschau dieses Datensatzes anzeigen ( ).

4. In **Wählen Sie ein bestimmtes CI oder eine generische CI-Klasse aus** Abschnitt im **Definiert Als** Feld auswählen, ob der manuelle Cluster als bestimmtes CI eines manuellen Clusters oder als generische CI-Klasse eines manuellen Clusters definiert werden soll, der auf alle CIs dieser Klasse angewendet wird.
   - Spezifisches CI: In **Konfigurationselement** Wählen Sie das Symbol „Suche mit Liste“ ( ) Und wählen Sie das Konfigurationselement aus.
   - Generische CI-Klasse – in **Konfigurationselementklasse** Wählen Sie die Konfigurationselementklasse aus.
5. In **Geben Sie eine Beschreibung an** Geben Sie im Abschnitt entweder eine Beschreibung an **Beschreibung** Feld oder lassen Sie es leer, um eine automatisch generierte Beschreibung zu enthalten, wenn Sie auswählen **Speichern** Oder **Übermitteln** .

   Die **Beschreibung** Das Feld wird automatisch aktualisiert, wenn Sie auswählen **Speichern** Oder **Übermitteln** . Die automatisch generierte Beschreibung besteht aus dem Konfigurationselementnamen und dem Servicenamen. Beispiel: `CI-<Alert Processing> in Service-<linuxApplService> (*** automatisch generiert ***)` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine automatische Aktualisierung des Felds Beschreibung zu verhindern und Ihre Änderungen beizubehalten, löschen Sie das Suffix (*** automatisch generiert ***), das als Teil der Beschreibung angezeigt wird.

6. Aktivieren Sie den Cluster, indem Sie auswählen **Aktivieren** Kontrollkästchen.
7. Wählen Sie **Absenden**.

Ergebnis

Der manuelle Cluster wird in der Tabelle „Manueller EM-Impact-Cluster“ [em_Impact_Manual_Cluster] gespeichert. Die Auswirkungsberechnung wird automatisch neu berechnet.

Zugehörige Informationen

Konfigurieren von CIs in einem manuellen Service als manueller Cluster

Ändern Sie einen manuellen Cluster

Ändern Sie einen vorhandenen manuellen Cluster, indem Sie den Service, das spezifische CI, die generische CI-Klasse oder die Beschreibung im Falle einer falschen Erstkonfiguration, Änderungen im Netzwerk oder anderer Probleme ändern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Manuelle Cluster**an.
2. Wählen Sie in der Liste einen manuellen Cluster aus.
3. Ändern Sie den Service, der den manuellen Cluster enthält, indem Sie einen anderen im auswählen **Wählen Sie einen Service aus, der diesen manuellen Cluster enthält** Abschnitt.
   Die Clusternummer wird in angezeigt **Nummer** Feld.
   a. Wählen Sie das Symbol „Suchen mit Liste“ ( ) In **Service** Feld.
   b. Wählen Sie in der Tabelle „CMDB CI-Service“ [cmdb_ci_Service_detected] einen manuell erstellten Service aus.
   c. **Wahlweise:** Zeigen Sie eine Vorschau des Datensatzes an, indem Sie auf das Symbol Vorschau dieses Datensatzes anzeigen ( ).
4. In **Wählen Sie ein bestimmtes CI oder eine generische CI-Klasse aus** Abschnitt in **Definiert Als** Ändern Sie den manuellen Cluster entweder als bestimmtes CI eines manuellen Clusters oder als generische CI-Klasse eines manuellen Clusters, die auf alle CIs dieser Klasse angewendet wird.
   - Spezifisches CI: In **Konfigurationselement** Wählen Sie das Symbol „Suche mit Liste“ ( ) Und wählen Sie das Konfigurationselement aus.
   - Generische CI-Klasse – in **Konfigurationselementklasse** Wählen Sie die Konfigurationselementklasse aus.
5. **Wahlweise:** In **Geben Sie eine Beschreibung an** Ändern Sie die Beschreibung in **Beschreibung** Feld.

   (Optional) Die **Beschreibung** Das Feld wird automatisch aktualisiert, wenn Sie auswählen **Speichern** Oder **Übermitteln** . Die automatisch generierte Beschreibung besteht aus dem Konfigurationselementnamen und dem Servicenamen. Beispiel: `CI-<Alert Processing> in Service-<linuxApplService> (*** automatisch generiert ***)` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine automatische Aktualisierung des Felds Beschreibung zu verhindern und Ihre Änderungen beizubehalten, löschen Sie das Suffix (*** automatisch generiert ***), das als Teil der Beschreibung angezeigt wird.

6. Aktivieren oder deaktivieren Sie den Cluster, indem Sie auswählen oder deaktivieren **Aktivieren** Kontrollkästchen.
7. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Ergebnis

Der manuelle Cluster wird in der Tabelle „Manueller EM-Impact-Cluster“ [em_Impact_Manual_Cluster] gespeichert. Die Auswirkungsberechnung wird automatisch neu berechnet.

Zugehörige Informationen

Konfigurieren von CIs in einem manuellen Service als manueller Cluster

Erstellen Sie eine Warnungsabfrage

Eine Warnungsabfrage ist ein Satz von Warnungen, die bestimmte Kriterien für einen bestimmten Service erfüllen.

Vorbereitungen

Navigieren zu **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften** Und stellen Sie sicher, dass die **Aktivieren Sie die Unterstützung von Warnungsabfragen** (*`evt_mgmt.impact_calulation.alert_group_support`* Eigenschaft) ist auf festgelegt **Ja** .

Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Die Hauptmotivation für die Verwendung von Warnungsabfragen ist eine Modellierungslösung basierend auf Daten, die in der Warnung selbst enthalten sind, als Alternative zur Verwendung von erkannten, Anwendungs- oder technischen Services.
Erstellen Sie eine Warnungsabfrage, um ähnliche Warnungen zu kombinieren, die die spezifischen Kriterien erfüllen.

Sie können mehr über erfahren Ereignismanagement Grundlagen, einschließlich Warnungsabfragen, aus diesem Video:

Erste Schritte mit Ereignismanagement

Prozedur

1. Navigieren zu **Ereignismanagement** > **Services** > **Warnungsabfragen**an.
2. Wählen Sie **Neu**.
3. Auf der **Warnungsabfrage** Formular, f Krank in den Feldern .

   Eine Beschreibung der Feldwerte finden Sie unter Warnungsabfrageformular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Im Feld **Filter**:

- Wenn Sie einen Warnungsabfragefilter definieren, beziehen Sie nur Felder ein, die in der Tabelle „Warnungsverläufe“ [em_Alert_history] angezeigt werden. Die Auswirkungsberechnung basiert auf Warnungsverlaufsdaten und Feldern wie Gesamtereignisanzahl, Priorität und Prioritätsgruppe werden nicht in die Tabelle „Warnungsverläufe“ [em_Alert_history] kopiert.
- Geben Sie keine dynamische Zeitbedingung an. Geben Sie beispielsweise im Filter nicht an Erstellt Bedingung von Letzte 45 MinutenDa die Auswirkungsberechnung durch eine Änderung der Warnung oder Warnungsabfrage ausgelöst wird. Für die dynamische Zeitbedingung hat sich jedoch keine dieser Bedingungen geändert.

- Einige Filter können die Auswirkungsberechnung verlangsamen. Um dieses Problem zu lösen, passen Sie Ihre Warnungsabfrage an, indem Sie einen entsprechenden Index hinzufügen, wie in beschrieben Indizieren Sie Vorschläge für langsame Abfragen .

4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Erstellen Sie eine Warnungsgruppe manuell

Erstellen Sie eine Anwendungsservicegruppe

Erstellen Sie Servicegruppen, um ähnliche Services zu kombinieren. Organisieren Sie Services nach Gruppen, um Aktionen für mehrere Services gleichzeitig auszuführen und den Benutzerzugriff auf Services zu steuern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Servicegruppen sind eine Möglichkeit, Services basierend auf den Anwendungsservices oder technischen Services zu organisieren und zu gruppieren, die sich auf sie auswirken. Anstatt einzelne Services aus verschiedenen Infrastrukturkomponenten (z. B. Servern, Datenbanken oder Anwendungen) zu betrachten, helfen Servicegruppen, sie unter dem Dach einer Servicegruppe zu konsolidieren. Anwendungsservicegruppen ermöglichen eine schnellere Identifizierung von Warnungsauswirkungen. Servicegruppen werden in angezeigt **Gruppieren nach** Option auf Service Operations-Arbeitsbereich Dashboard.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Servicegruppen**an.
   Die Seite „Anwendungsservicegruppe“ wird geöffnet.
2. Wählen Sie **Neu**.
3. Im Feld **Name** geben Sie den Namen der neuen Servicegruppe ein.
4. **Wahlweise:** Um die neue Gruppe in eine andere Gruppe einzubetten, geben Sie den Namen der anderen Gruppe im Feld **Übergeordnete Gruppe** ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer mit Zugriff auf eine übergeordnete Servicegruppe haben automatisch Zugriff auf alle untergeordneten Gruppen.

5. Wählen Sie **Absenden**.

Zugehörige Informationen

Einer Servicegruppe eine Rolle zuweisen

Gruppen-Anwendungsservices

Einer Servicegruppe eine Rolle zuweisen

Weisen Sie einen zu Ereignismanagement Rolle für die Anwendungsservicegruppe, um sicherzustellen, dass Gruppenmitglieder Warnungen verwalten und bearbeiten können.

Vorbereitungen

Konfigurieren Sie eine Servicegruppe, damit Anwender Anwendungsservices oder Warnungsgruppen verwalten können.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Zuständigkeiten der Servicegruppe**an.
2. Klicken Sie auf **Neu**.
3. In **Anwendungsservicegruppe** Wählen Sie den Namen der Servicegruppe aus.
4. Wählen Sie im Feld **Rolle** eine Ereignismanagement-Rolle aus:
   - evt_mgmt_admin
   - evt_mgmt_integration
   - evt_mgmt_operator
   - evt_mgmt_user
5. Klicken Sie auf **Absenden**.
6. Um Anwender zu finden, die der Rolle zugewiesen sind, navigieren Sie zu **Anwenderadministration** > **Anwender** > **Rollen** Und suchen Sie nach der Rolle.

Zugehörige Informationen

Mit Ereignismanagement installierte Rollen

Service-Mapping aktivieren und für die Erkennung von oben nach unten konfigurieren

Eine Discovery von oben nach unten bietet eine Liste von CIs und ihren Beziehungen. Diese Informationen sind nützlich für die Verwaltung von Softwarediensten und Hardwareproblemen, die mit Warnungen verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

In Ereignismanagement werden Service-Mapping-Beziehungen in Warnungen angezeigt. Sie können das zugehörige CI und andere Informationen im Dashboard Ereignismanagement anzeigen. Die Zuordnungsbeziehungen werden in einer Servicezuordnung mit der generierten Warnung, allen an die Warnung gebundenen CIs und allen zugehörigen CIs angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Verwenden Service-Mapping Zum Abrufen von Top Down-Discovery-Informationen.
Service-Mapping, Die eng mit verbunden ist Ereignismanagement, Stellt Tools zur Erkennung der Beziehungen zwischen Netzwerk, Hardware, Software, Speicher und anderen Geräten bereit.

Zugehörige Informationen

Service-Mapping

Service-Mapping anfordern

E-Mail-Benachrichtigung bei Änderung des Anwendungsservice-Schweregrads konfigurieren

Konfigurieren Sie eine E-Mail-Benachrichtigung, um Benutzer über Änderungen des Anwendungsservice-Schweregrads zu informieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie eine E-Mail-Benachrichtigung, um Benutzer über Änderungen des Anwendungsservice-Schweregrads zu informieren. Dabei können Sie einstellen, wann die Benachrichtigung gesendet wird, wer sie empfängt und was sie enthält.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **E-Mail-Eigenschaften**an.
2. Wählen Sie im Abschnitt **Konfiguration für ausgehende E-Mails** unter **E-Mail-Versand aktiviert** die Option **Ja** aus, um das Senden von Schweregradinformationen per E-Mail zu ermöglichen.
3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**an.
5. Klicken Sie auf **Neu**.
   a. Geben Sie im Formular **E-Mail-Benachrichtigungsaktionen** diese Werte an.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein, z. B. *`Application Service severity change`*.
Tabelle	Wählen Sie den erforderlichen Servicetyp und die entsprechende Tabelle aus: Warnungsgruppe, erkannter Service, technischer Service oder Anwendungsservice.
Aktiv	Aktivieren Sie die Checkbox, um die E-Mail-Benachrichtigung zu aktivieren.

   b. Klicken Sie auf die Registerkarte **Empfänger**.
   Im Bereich **Benutzer** suchen und wählen Sie den erforderlichen Benutzer (der Benutzer benötigt keine Systemadministrator-Anmeldeinformationen). Wiederholen Sie diesen Schritt für alle Benutzer, die für den Empfang dieser Benachrichtigung erforderlich sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf **Zeitpunkt des Sendens** Registerkarte und in **Wählen Sie das Feld aus** Feld suchen und auswählen `Severity`.

d. Klicken Sie auf **Was wird enthalten** Registerkarte und in **Betreff** Feld aussagekräftigen Text eingeben, der dem Empfänger der E-Mail-Benachrichtigung deutlich macht, was der Inhalt der E-Mail ist.

e. Erstellen Sie im Nachrichtenbereich **Nachricht-HTML** mithilfe der Funktionen **Variablen auswählen** die Bedingungen, unter denen die E-Mail-Benachrichtigung gesendet werden soll.
Konfigurieren Sie beispielsweise diese Variablen, um den Schweregrad zu ändern:

```
severity changed
```

```
Severity: ${severity}
```

```
on application service
```

```
Name: ${name}
```

6. Klicken Sie auf **Absenden**.

Kontextbezogene Farben und Symbole konfigurieren

Verwenden Sie das Formular **Kontextbezogene Farben und Symbole**, um Farbe, Text und Symbole so zu konfigurieren, dass verschiedene Standardkontexte oder benutzerdefinierte Kontexte vorhanden sind, die durch eine Kontext-ID identifiziert werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Farben oder Symbole von Elementen im Formular **Kontextbezogene Farben und Symbole** anpassen, um die angezeigten Farben oder Symbole von Schweregraden in zugehörigen Ereignismanagement-Bildschirmen zu beeinflussen, entweder wenn der Eingabehilfemodus aktiviert oder deaktiviert ist. Weitere Informationen zur Barrierefreiheit finden Sie unter Barrierefreiheitsfunktionen .

In jedem Farbauswahlfeld haben Sie die Möglichkeit, den Wert der Farbe als eines der folgenden CSS-Formate (Cascading Style Sheet) einzugeben, die bestimmen, wie HTML-Elemente angezeigt werden sollen:

- Name: vordefinierte Farbnamen, z. B. Rot, Grün, Oliv, Blau, Dunkelblau oder Hellblau
- RGB-Dezimalzahl: RGB(102, 153, 204)
- RGB-Hex-Wert: #223344

Auf den folgenden Websites finden Sie Informationen zu CSS-Farbdeklarationen (einschließlich Hex- oder RGB-Schreibweise):

- HTML-Farben (W3CSchools) für weitere Informationen zu Hex-Wert und RGB Schreibweise.
- HTML-Farbnamen (W3CSchools) für gültige Farbnamen.

Die mit der Basisinstanz bereitgestellten Kontext-IDs sind:

- information_severity
- warning_severity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- minor_severity
- major_severity
- critical_severity
- topology_connection

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Kontextbezogene Farben und Symbole**an.
2. Klicken Sie auf **Neu** oder auf eine vorhandene Konfiguration.
3. Konfigurieren Sie die folgenden Felder.

Element	Beschreibung
Kontextdetails	
Kontext-ID	Geben Sie eine eindeutige ID für den Kontext ein, z. B. „clear_severity“.
Kontextname	Lesbarer Name für den Kontext. Dieser Text kann von Sprachausgabeprogrammen vorgelesen werden.
Batch	Batch, zu dem dieser Kontext gehört.
Beschreibung	Beschreibung der Verwendungen für den Kontext.
Farben **Hinweis:** Für jeden Eintrag in den Farbfeldern wird nach der Eingabe eines Farbcodes ein Block rechts vom Feld mit der angegebenen Farbe angezeigt. Die Verwendung ungültiger Farbcodes löst eine entsprechende Fehlermeldung aus.	
CSS-Farbe	Der entsprechende CSS-Farbcode für den Kontextfarbnamen.
CSS-Farbe bei Interaktion	CSS-Farbcode, der beim Daraufzeigen oder Fokussieren angezeigt wird.
Verfügbare CSS-Farbe	Verfügbarer CSS-Farbcode, der anzeigt, wenn der Eingabehilfemodus aktiviert ist.
Verfügbare CSS-Farbe bei Interaktion	Eingabehilfe-CSS-Farbcode, der beim Daraufzeigen oder Fokussieren angezeigt wird.
Symbole	
Symbol	Symbol, das anzeigt, ob der Kontext ein Symbol enthält.
Eingabehilfesymbol	Symbol, das anzeigt wird, wenn der Kontext ein Symbol enthält und wenn der Eingabehilfemodus aktiviert ist. Informationen zum Hinzufügen eines eigenen Symbols oder zum Anzeigen einer Liste der verfügbaren Symbole finden Sie unter Laden Sie mindestens ein Bild hoch .

4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lizenznutzung für Event Management anzeigen

Ereignismanagement wird basierend auf der Anzahl der CIs lizenziert, die im letzten Jahr an Warnungen gebunden wurden. Für Warnungen, die nicht an CIs gebunden sind, berechnet das System die Anzahl der Knoten (Server), die im letzten Jahr Ereignisse direkt oder über ein Überwachungstool einer Drittpartei an die Instanz senden können.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Die **Ereignismanagement: Knotenanzahl-Speicher** Der Auftrag berechnet die Anzahl der eindeutigen Knoten, die Ereignisinformationen entweder direkt oder über Drittparteien an senden Ereignismanagement Und sind im letzten Jahr für die Lizenzierung berechtigt. Die Informationen dieses Auftrags werden in der Tabelle Lizenznutzung [em_unique_nodes] gespeichert, um für alle Benutzer sichtbar zu sein. An Warnungen gebundene CIs werden bei der Lizenzierung berücksichtigt. Wenn keine CIs vorhanden sind, die an Warnungen gebunden sind, wird das Event-Knotenfeld verwendet. Knoten ist ein Verweis auf einen Server, nicht auf die Instanzen der darauf befindlichen Software. Ihre Knotenanzahl basiert auf der Menge der Infrastruktur (z. B. Server), die Ereignisse sendet.

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Bericht** > **Lizenznutzung**an.

Die Tabelle wird basierend auf den Warnungen im System automatisch ausgefüllt. Der Anwender hat keine Berechtigung zum Bearbeiten der Tabelle. Wird verwendet, um die Nutzung von zu berechnen Ereignismanagement Lizenzierung.

Spalte	Beschreibung
CMDB CI	Das CI, das an die Warnung gebunden ist, die aus dem Event generiert wird. Wenn für dieses Feld ein Wert vorhanden ist, ist das **Knotenfeld** leer.
Knoten	Der Zeichenfolgenwert des **Knotenfelds** des Events. Wenn für dieses Feld ein Wert vorhanden ist, ist das Feld **CMDB CI** leer.
Typ	Einer der folgenden Werte: • Unbekannt – Ein CI ist nicht an die gene–rierte Warnung gebunden. • Server – Die Quelle des Events war ein Server. • PaaS – Die Quelle des Events war „Plat–form as a Service“.
Ist lizenzierbar	Einer der folgenden Werte: • True – Das aufgelistete Event wird auf die Lizenznutzung angerechnet. • False – Das aufgelistete Event wird nicht auf die Lizenznutzung angerechnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement verwenden

Als Ereignismanagement Operator haben Sie die Aufgabe, Warnungen zu finden und zu analysieren sowie Aktionen zur Lösung des zugrunde liegenden Problems zu ergreifen.

Dieser Leitfaden kann Sie regelmäßig unterstützen.

Warnungsinformationen anzeigen

Zeigen Sie eine Liste aller Warnungen für Anwendungsservices an, und verwalten Sie dann nach Bedarf einzelne Warnungen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Mehrere zugehörige Events können zu einer einzigen Warnung korrelieren. Ereignismanagement erstellt Warnungen nur, wenn mindestens ein Event die Bedingungen erfüllt, die in Eventregeln, Warnungsaktionsregeln und Warnungskonfigurationseinstellungen definiert sind.

Beim Aktualisieren einer Warnung werden von leeren Feldwerten keine Werte überschrieben, die vom Ereignis der Warnung übernommen wurden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie auf die Warnungsnummer, um eine Warnung anzuzeigen oder zu verwalten.
3. Überprüfen Sie die Informationen im Warnungsformular.
   Sie können auf die Registerkarten im Formular klicken, um weitere Informationen zu erhalten.
   - Um Informationen zur Fluktuation anzuzeigen, klicken Sie auf die Registerkarte **Fluktuierend**.
   - Um den Warnungsverlauf anzuzeigen, klicken Sie auf die Registerkarte **Verlauf**.

Warnungsformular

Feld	Beschreibung
Nummer	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen
Ressource	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen
Konfigurationselement	JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: `{"name":"SAP ORA01","type":"Oracle"}` ({"Name": "SAP ORA01", "Typ": "Oracle"}). Der CI-Bezeichner, der das Event generiert hat, wird im Feld **Zusätzliche Informationen** angezeigt. Maximale Länge: 1.000 Zeichen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Referenz-Popups und Click-throughs sind für schreibgeschützte Felder standardmäßig ausgeblendet. Für **Konfigurationselement** und andere schreibgeschützte Felder können Sie die Einstellung „Schreibgeschützt“ optional ändern. Weitere Informationen finden Sie unter Popups für schreibgeschützte Felder konfigurieren . Klicken Sie auf das , um die Warnung in der Abhängigkeitsansicht zu öffnen.
Aufgabe	Die entsprechende Aufgabe für die Warnung, z. B. Incident, Change oder Problem.
Metrikname	Eindeutiger Name, der beschreibt, welche Metrikdaten erfasst werden.
Beschreibung	Eine Beschreibung der Warnung.
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
Schweregrad	Der Schweregrad des Events. Der Wert für dieses Feld wird aus dem Event kopiert, es sei denn, das Event schließt die Warnung. In diesem Fall wird der vorherige Schweregrad für die Berichterstellung beibehalten. ○ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ○ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ○ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ○ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Status	Der Status der Warnung. ○ **Öffnen**: Die Warnung erfordert eine Benutzeraktion. ○ **Erneut öffnen**: Die zuvor geschlossene Warnung erfordert eine Benutzeraktion. ○ **Flatternd**: Nachdem die Warnung geschlossen wurde, gehen sehr viele identische Events aus derselben Quelle ein, die zu zahlreichen erneuten Öffnungen der Warnung führen. Benutzeraktion ist erforderlich. ○ **Geschlossen**: Die Warnung ist geschlossen, und es ist keine weitere Benutzeraktion erforderlich.
Bestätigt	Wählen Sie **Bestätigt** aus, um anzugeben, dass ein Benutzer die Warnung bestätigt hat.
Reserviert	Ein Kontrollkästchen, mit dem angezeigt wird, ob sich die von der Warnung betroffene Ressource in Wartung befindet.
Aktualisiert	Der Zeitpunkt der letzten Aktualisierung der Informationen zur Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordnet	◦ Wenn dieses Feld leer ist, können Sie eine Warnungsnummer angeben. Die aktuelle Warnung wird zu einer sekundären Warnung zu dieser übergeordneten Warnung. ◦ Wenn eine Warnungsnummer angezeigt wird, ist die aktuelle Warnung bereits eine sekundäre Warnung zu dieser aktuellen Warnung, der übergeordneten Warnung.
Feedback	Dieses Feld wird in Warnungsformularen nur angezeigt, wenn die Warnung wird geändert Ist eine übergeordnete Warnung. Ihre Antwort bietet Feedback zur Genauigkeit und Nützlichkeit der Gruppe. Mögliche Werte sind: ◦ Kein – Es wurde kein Wert ausgewählt. ◦ Kein Feedback – Für diese Warnung gibt es kein Feedback. ◦ Ja – die Warnungsgruppe ist genau und nützlich. ◦ Nein – die Warnungsgruppe ist nicht genau und nützlich. **Hinweis:** Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus.
Wissensartikel	Der der Warnung zugeordnete Wissensartikel (sofern vorhanden).
Gesamtanzahl der Events	Der Zähler wird jedes Mal erhöht, wenn ein Event an die Warnung gebunden wird. Der Zählwert wird beibehalten, auch nachdem das tatsächliche Event gelöscht wurde. Primäre Warnungen (virtuelle Warnungen) werden basierend auf ihren sekundären Warnungen aktualisiert. Die tatsächliche Anzahl der Events, die sich auf die Warnung auswirken, wird angezeigt. **Hinweis:** Erstellen Sie keine Warnungsgruppe basierend auf der Event-Anzahl. Wenn eine Warnungsgruppe auf der Event-Anzahl basiert, wird die Auswirkung der Gruppe nicht ordnungsgemäß berechnet, da das Feld „Event-Anzahl“ nicht für die Auswirkungsberechnung in die Tabelle „em_alert_history“ kopiert wird.
Quellinstanz	Der Name des Computers oder der Software, die/der das Event generiert hat. Beispiel: SolarWinds auf 10.22.33.44.
Benutzername und Rolle	Der Benutzer und die Rolle der Person, die die neuesten Warnungsaktualisierungen vorgenommen hat.
Bestätigt	Das Kontrollkästchen **Bestätigt** nach dem neuesten Update mit den meisten Warnungen. ◦ *True*: **Bestätigt** ist ausgewählt. ◦ *False*: Das Kontrollkästchen **Bestätigt** wird deaktiviert.
Abschnitt **Korrelierte Warnungen**	Die sekundären Warnungen, die mit dieser Warnung korrelieren, wobei diese Warnung die primäre Warnung ist. Weitere Informationen finden Sie unter Regelbasierte Warnungsgruppierung.
Abschnitt **Primäre Warnungen**	Die primäre Warnung, die mit dieser Warnung korreliert, wobei diese Warnung eine sekundäre Warnung ist. Weitere Informationen finden Sie unter Regelbasierte Warnungsgruppierung.

Zusätzliche Registerkarten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Registerkarte „Betroffene Services“	
Betroffene Services	Die betroffenen Services, die zu dieser Warnung gehören, werden aufgelistet. Weitere Informationen finden Sie unter Anzeigen der Auswirkungsstruktur.
Registerkarte „Flatternd“	
Anzahl der Fluktuationen	Die Anzahl, wie oft es innerhalb des Flatterintervalls seit der Startzeit im **Flattern – Startfenster** zu Flatterbewegungen bei Warnungen gekommen ist, d. h. zwischen einem geschlossenen und einem nicht geschlossenen Zustand gewechselt wurde.
Flattern – Startfenster	Die anfängliche Startzeit zur Messung der Fluktuationsereignisse.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.
Registerkarte „Verlauf“	
Generierungszeit des ersten Events	Die Zeit, zu der das Event, von dem die Warnung zuerst generiert wurde, aufgetreten ist. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Generierungszeit des letzten Events	Das letzte Mal, dass das mit der Warnung verknüpfte Event aufgetreten ist. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Erstellt	Uhrzeit, zu der die Warnung erstellt wurde.
Arbeitsnotizen	Die zusätzlichen Notizen zur Warnung.
Registerkarte Aktivitäten	
Aktivität	Ein Datensatz der durchgeführten Arbeit. Der Text hat einen Datums- und Zeitstempel.
Registerkarte „Weitere Informationen“	
Prioritätsaufgliederung	Zeigt die Berechnung der Warnungsprioritätspunktzahl an.
Zusätzliche Informationen	Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed. Error 0x80070490"}. Diese Informationen können für die Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-Format, das die Daten enthält: {“additional_content”: “Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).

Nächste Maßnahme

Sie können auf eine Warnung wie folgt reagieren:

Optionen zur Reaktion auf Warnungen

Option	Beschreibung
Absenden	Speichern Sie die am Formular vorgenommenen Änderungen, und kehren Sie zur Liste der **Warnungen** zurück.
Bestätigen Sie die Warnung.	Klicken Sie auf **Bestätigen**. Wenn die Warnung erneut geöffnet wird, wird diese Schaltfläche erneut angezeigt, damit Sie die Warnung erneut bestätigen können.
Erstellen eines Incidents.	Klicken Sie auf **Incident erstellen**. Weitere Informationen finden Sie unter Erstellen Sie einen Incident oder Security Incident aus einer Warnung.
Wenn Security Incident Response aktiviert ist, erstellen Sie eine Reaktion auf einen Security Incident.	Klicken Sie auf **Security Incident erstellen**.
Legen Sie fest, dass sich die Warnung in Wartung befindet.	Klicken Sie auf das Kontrollkästchen **Wartung**. Weitere Informationen finden Sie unter Alle Warnungen nach Wartungsstatus anzeigen.
Schließen Sie die Warnung.	Klicken Sie auf **Schließen**. Weitere Informationen finden Sie unter Warnungen schließen.

Zugehörige Informationen

Aus Events und Warnungen erstellte Security Incidents

Prioritätsgruppe

Zur besseren Selektierung und Fokussierung werden Warnungen mit einer höheren Priorität an den Anfang der Warnungsliste gesetzt. Diese Platzierung macht Sie auf die Warnungen aufmerksam, die eine höhere Priorität als andere Warnungen haben.

Die Prioritätsgruppe gibt an, welche Warnungen zuerst Aufmerksamkeit erfordern. Die Priorität wird für alle offenen Warnungen berechnet, woraufhin diese einer von vier Prioritätskategorien zugeordnet werden.

Schwellenwerte

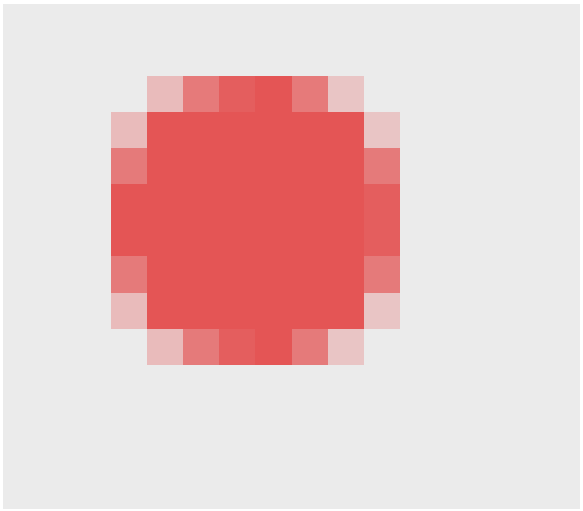
Schwellenwerte für die berechnete Priorität werden verwendet, um zu bestimmen, welcher Kategorie die Warnung zugeordnet wird. Warnungen mit einer Priorität, die über dem Wert der Eigenschaft `evt_mgmt.top_priority_group_threshold` liegt, werden als **Dringend**kategorisiert, was die höchste Priorität ist. Der Standardwert für den Schwellenwert ist 1M.

Prioritätsgruppenkategorien

Die Prioritätsgruppen, in die Warnungen fallen, sind in der folgenden Tabelle aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

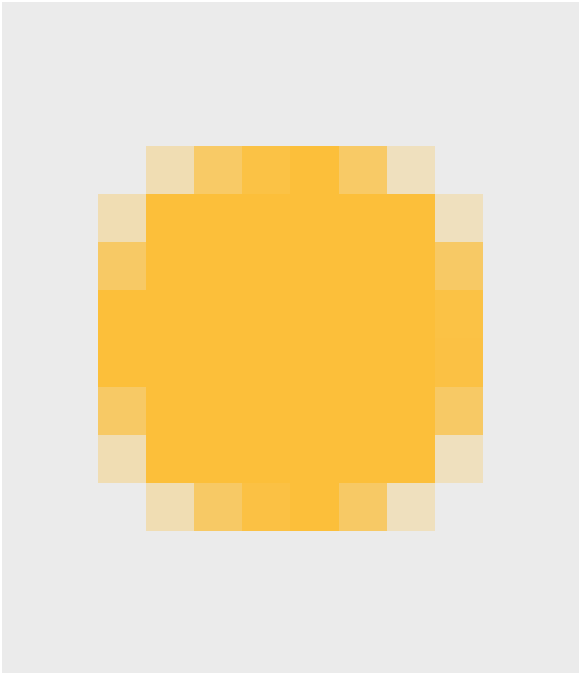
Warnungsprioritätsgruppen

Prioritätsgruppe	Symbol
Dringend	
Hoch	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsprioritätsgruppen (Fortsetzung)

Prioritätsgruppe	Symbol
Mittel	
Niedrig	

Der Wert der Warnungsprioritätsgruppe ist aussagekräftiger als der Warnungsschweregrad an sich. Beispiel: Eine Warnung mit dem Schweregrad „Schwerwiegend“ muss möglicherweise nicht vor einer Warnung gelöst werden, deren Priorität „Kritisch“ ist. Der kombinierte Gruppenprioritätswert berücksichtigt die Gewichtung jedes Faktors, sodass Sie besser wissen, welche Warnung zuerst bearbeitet werden muss.

Die Warnungsprioritätsgruppe ist in Warnungslisten auf der Seite „Dashboard“, „Alert Intelligence“ und „Alle Warnungen“ verfügbar. Beispielsweise wird in der Liste **Alle Warnungen** die Warnungsprioritätsgruppe wie in der folgenden Abbildung dargestellt angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Number	Group	Severity	Priority group	Priority
Demo0001011		Warning	Low	100
Demo0001006		Warning	Moderate	100
Alert0010004		Minor	High	200

Auslöser, die eine Neuberechnung auslösen

Änderungen an offenen Warnungen lösen die Neuberechnung der Priorität aus. Anschließend wird die Warnung erneut in die entsprechende Prioritätsgruppe eingeteilt. Geschlossene Warnungen werden bei der Berechnung der Warnungsprioritätsgruppe nicht berücksichtigt.

Zugehörige Informationen

Warnungspriorität

Informationen zur Warnungsausführung

Warnungsausführungsinformationen bieten einen Verweis auf die durchgeführten Aktionen in Bezug auf die Warnung. Zu den angezeigten Informationen gehören, welche Warnungsverwaltungsregeln für die Warnung ausgeführt wurden, Incidents, die geöffnet wurden, und welche Nachbesserungs-Workflows ausgeführt wurden.

Warnungsausführungen

In einem Warnungsformular zeigt die Registerkarte „Warnungsausführung“ wichtige zugehörige Datensätze für die Warnung an. Beispielsweise wird angezeigt, welche Aktionen ausgeführt wurden und welche Warnungsverwaltungsregeln ausgeführt wurden. Wenn ein Incident geöffnet wurde, werden die zugehörigen Aufgaben angezeigt.

Warnungsausführungen

Felder im Abschnitt „Warnungsausführungen“

Feld	Beschreibung
Warnung	Verweis auf die Warnung, die unter dieser Regel ausgeführt wurde.
Aktionsname	Gibt an, wie die Warnung gelöst wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder im Abschnitt „Warnungsausführungen“ (Fortsetzung)

Feld	Beschreibung
Link zur Ausführung	Verknüpfte Aktion, die zur Behebung der Warnung durchgeführt wurde.
Zugehörige Aufgabe	Link zu der Aufgabe, die erstellt wurde, als die Warnung gelöst wurde.
Protokoll	Link zu dem Protokoll, das die Aktionen zur Lösung der Warnung ausführlich beschreibt.
Automatische Ausführung	Gibt an, ob die Regel automatisch (true) oder manuell (false) war.

Aktionsname
Dies gibt an, was beispielsweise aufgetreten ist, wenn ein Incident erstellt wurde.

Protokoll
Das Protokoll zeigt, welche Warnungsverwaltungsregel die Aktion initiiert hat. Es zeigt z. B. die automatische Ausführung (1 von 3) oder die manuelle Ausführung (2 von 4) an.

Warnungen im Status „Fluktuierend“ anzeigen

Sie können Warnungen anzeigen, die sich im Status „Fluktuierend“ befinden.

Vorbereitungen
Bevor Sie mit diesem Verfahren beginnen, bitten Sie Ihren Administrator, Eigenschaften für fluktuierende Warnungen zu konfigurieren.
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Flattern tritt auf, wenn von der Event-Quelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Flattern bewirkt, dass der Status der Ressource wiederholt zwischen dem Schweregrad *OK* und einem Schweregrad schwankt, der Aufmerksamkeit erfordert, z. B. *Critical*.

Die Häufigkeit von Events aus einer identischen Quelle innerhalb eines bestimmten Zeitintervalls bestimmt, ob sich eine Warnung im Status „Fluktuierend“ befindet oder ob ein neues Problem aufgetreten ist. Basierend auf den Eigenschaftswerten *evt_mgmt.flap_frequency* und *evt_mgmt.flap_interval*:

- Wenn das gleiche Problem wiederholt auftritt, ordnet Ereignismanagement das neue Event der vorhandenen Warnung zu, und der Status der Warnung wird auf **Flatternd** festgelegt.
- Wenn das Problem nach Ablauf des Zeitintervalls auftritt, erstellt Ereignismanagement eine Warnung.

Beispielsweise können Sie auf eine Warnung reagieren, indem Sie einen problematischen Server neu starten. Nachdem mehrere Minuten lang keine Events generiert wurden, wird davon ausgegangen, dass das Problem behoben ist, und die Warnung wird geschlossen. Wenn das Problem durch den Neustart nicht behoben wurde, kann dieser Server später weitere Events generieren. Dann werden zusätzliche Warnungen für dasselbe Problem generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie auf die Nummer einer Warnung, die sich im Status **Flatternd** befindet.
3. Klicken Sie in der Warnung auf die Registerkarte **Flatternd**.

Registerkarte „Flatternd“ auf Warnungsformular

Feld	Beschreibung
Registerkarte **Flatternd**	
Anzahl der Fluktuationen	Die Anzahl, wie oft es innerhalb des Flatterintervalls seit der Startzeit im **Flattern – Startfenster** zu Flatterbewegungen bei Warnungen gekommen ist, d. h. zwischen einem geschlossenen und einem nicht geschlossenen Zustand gewechselt wurde.
Flattern – Startfenster	Die anfängliche Startzeit zur Messung der Fluktuationsereignisse.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.

4. Wenn das Feld **Übergeordnet** leer ist, behandeln Sie diese Warnung als neues Problem.

Zugehörige Informationen

Fluktuierende Warnungen konfigurieren

Alle Warnungen nach Wartungsstatus anzeigen

Der **Wartungsstatus** gibt an, dass das CI gewartet wird. Beispielsweise gibt es ein Software-Upgrade, und die Probleme können aus dieser Aktivität resultieren, daher werden alle Wartungswarnungen verworfen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Der Wartungsstatus der Warnung kann sich aus einem der folgenden Gründe ändern:

- Ein Benutzer hat das Kontrollkästchen **Wartung** in der Warnung aktiviert oder die Warnung in der Listenansicht ausgewählt und dann auf die UI-Aktion **Wartung** geklickt.
- Eine neue Warnung, die an ein CI gebunden war, das sich in der CMDB-Tabelle im Wartungsstatus befindet.
- Wenn alle vorherigen zugehörigen Events der Warnung in Wartung sind, kann das Warnungsfeld **Wartung** automatisch auf `true`„Wartung läuft “gesetzt werden. Wenn das Feld **Wartung für** Warnungen `false` ist, der zugehörige CI-Status jedoch in `In Maintenance` geändert wird, nachdem die Warnung erstellt wurde, wird die Warnung bei nachfolgenden Events nicht in den Wartungsmodus versetzt. Beispiel: Wenn für einen Router eine Warnung generiert wird und der Router später zur Wartung heruntergefahren wird, wird dennoch davon ausgegangen, dass ein Problem vor Beginn der Wartung aufgetreten ist, und das Problem darf nicht ignoriert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn für eine Warnung in Genf ein Wartungs-Flag festgelegt wurde, wirkt sich dies nach dem Upgrade in Helsinki auf die Auswirkung als reguläre Warnung aus.
- Wenn eine Warnung durch eine Benutzeraktion (z. B. eine Warnungsverwaltungsregel) an ein CI gebunden ist und sich das CI im Wartungsstatus befindet, müssen Sie das CI manuell an die Warnung binden und es mit dem Status **In Wartung** markieren.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Überprüfen Sie die Spalte **Wartung** für jede Warnung.
   Der Wert `true` gibt an, dass das CI gewartet wird.

Hinweis: Wenn das Feld **Wartung** auf dem Warnungsformular nicht angezeigt wird, personalisieren Sie die Liste, um das Feld hinzuzufügen. Weitere Informationen finden Sie unter Persönliche Listen .

Innerhalb einer Warnung zusammenarbeiten

Sie können mit Kollegen zusammenarbeiten und Arbeitsnotizen schreiben, während Sie in einer Warnung arbeiten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können in einer kompakten Ansicht von Connect arbeiten, die die Standardbenutzeroberfläche überlagert, oder in einem Vollbild-Arbeitsbereich. Die Konversationen werden nicht in die Warnung kopiert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie auf die gewünschte Warnung.
3. Klicken Sie im Warnungsbildschirm auf **Folgen**.
   Die Bezeichnung der Schaltfläche ändert sich in **Verfolgt** und zeigt die aktuelle Verbindung mit dem Status der Zusammenarbeit an.
4. Um die Connect-Seitenleiste als Vollbild anzuzeigen, klicken Sie auf der Schaltfläche **Folgen** auf den Abwärtspfeil, und wählen Sie **Connect Full öffnen**.
   Sie können Text im Feld **Arbeitsnotiz** eingeben. Dieser Text wird nicht in die Warnung kopiert.
5. Zur Zusammenarbeit mit Kollegen oder dem Support klicken Sie auf das Symbol **Benutzer hinzufügen**.
6. Um die Connect-Zusammenarbeitssitzung abzuschließen, klicken Sie auf **Verfolgt**.

Erstellen Sie einen Incident oder Security Incident aus einer Warnung

Wenn eine Warnung eskaliert und einer Person zugewiesen werden muss, die das zugrunde liegende Problem lösen kann, können Sie einen Incident öffnen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Wenn Security Incident Response aktiviert ist, können Sie einen Security Incident erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Incidents und Sicherheits-Incidents manuell über das Warnungsformular erstellen. Um doppelte Aufgaben zu vermeiden, überprüft das System die Bedingungen aller Aufgabenvorlagen, bevor ein Incident erstellt wird.

Sie können den erstellten Incident mithilfe der `EvtMgmtCustomIncidentPopulator.populateFieldsFromAlert`Skripteinbindung anpassen. Die Anpassung umfasst das Zuordnen von Feldern von der Warnung zum Incident oder das Abbrechen der Incident-Erstellung gemäß benutzerdefinierten Bedingungen. Weitere Informationen finden Sie unter Benutzerdefinierte Warnungsfelder.

Sie können Incident-Felder mithilfe von benutzerdefinierten Warnungsfeldwerten aus zusätzlichen Informationsfeldern ausfüllen. Verwenden Sie die Skripteinbindung `EvtMgmtCustomIncidentPopulator`, um die Werte nach dem Kopieren der Daten in die Warnung in den Incident zu kopieren. Weitere Informationen finden Sie unter Benutzerdefinierte Warnungsfelder.

Hinweis: Wenn Security Incident Response aktiviert ist, enthält das Basissystem eine Warnungsaktionsregel namens **Create security incidents for critical alerts** (Sicherheitsvorfälle für kritische Warnungen erstellen). Diese Warnungsaktionsregel erstellt Sicherheitsvorfälle, wenn kritische Sicherheitsereignisse gemeldet werden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie auf die **Nummer** der Warnung.
3. So erstellen Sie einen Incident:
   - Zum Erstellen eines Incidents klicken Sie auf **Quick Incident**.
   - Zum Erstellen von Security Incidents klicken Sie auf **Security Incident erstellen**. Sie müssen das Security-Plugin (SecOps) installieren, um diese Option zu aktivieren.
4. Klicken Sie auf **Aktualisieren**.

Ergebnis

Der erstellte Incident wird im Feld **Aufgaben** im Warnungsformular angezeigt.

Zugehörige Informationen

Aus Events und Warnungen erstellte Security Incidents

Warnung in Wartung setzen

Sie können Warnungen manuell in die Wartung setzen, um sie in der Warnungsliste und im Agent Workspace auszublenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Das Platzieren der Warnung in Wartung setzt nicht das CI in Wartung. Das **Statusfeld** im CI-Datensatz bleibt unverändert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Führen Sie eine der folgenden Aktionen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Um mehrere Warnungen in Wartung zu versetzen	Aktivieren Sie die Kontrollkästchen neben den einzelnen Warnungen, und klicken Sie dann oben in der Liste auf die UI-Aktion **Wartung**.
Um eine Warnung in Wartung zu versetzen	Öffnen Sie die Warnung, und aktivieren Sie entweder das Kontrollkästchen **Wartung**, und klicken Sie auf **Aktualisieren**, oder klicken Sie oben in der Liste auf die UI-Aktion **Wartung**.

Zugehörige Informationen

Wartungsregeln erstellen

Informationen zu Warnungseinblick

Warnungseinblick hilft bei der schnelleren Suche nach Warnungen, sodass eine Lösung schneller gefunden und die wahrscheinliche Ursache der ausgewählten Warnung offengelegt werden kann.

Warnungseinblick verwenden, um eine Lösung zu finden und die Ursache der Warnung zu finden

Ergebnisse der Datenanalyse liefern weitere Informationen über die Warnung, die über die Informationen im Warnungsformular hinausgehen. Dies hilft bei der schnelleren Suche nach Warnungen, sodass eine Lösung schneller gefunden und die wahrscheinliche Ursache der Warnung offengelegt werden kann.

Die angezeigten Informationen stammen aus wiederholten Warnungen, ähnlichen Warnungen, Incidents, Problemen und Change Requests für dasselbe CI, ähnliche CIs und andere CIs, die durch CMDB-Beziehungen oder Gruppierungen verbunden sind.

Schnelle Antworten in einer Warnung anwenden

In einer Warnung können Sie die Funktion *`Schnelle Antwort`* verwenden, um Fehlerkorrekturen auf die Warnung anzuwenden oder eine Webanwendung zu starten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

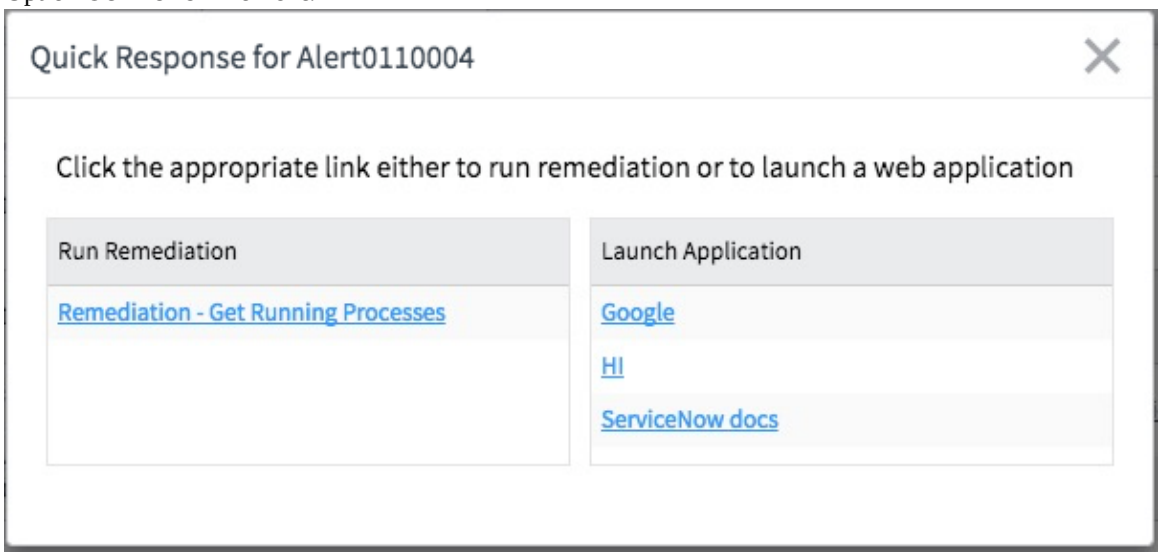
Mit der Funktion **Schnelle Antwort** können Sie schnelle Aktionen in der ausgewählten Warnung durchführen. Mit dieser Aktion können Sie Nachbesserungen anwenden oder Anwendungen starten. Wenn Sie ein Upgrade von Istanbul oder einer früheren Version durchgeführt haben, können Sie sich diese Funktion als Kombination aus den Funktionen **Fehlerkorrektur** und **Anwendung starten** vorstellen.

Wenn Sie beim Aufrufen einer schnellen Antwort einen Link für die Fehlerkorrektur auswählen, wird ein Workflow ausgeführt, und zwar anhand den in der Warnungsverwaltungsregel angegebenen Kriterien. Klicken Sie auf den entsprechenden Link vom Typ „Anwendung starten“, um die in der Warnungsverwaltungsregel festgelegte Webanwendung zu starten. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie mit der rechten Maustaste auf die jeweilige Warnung in der Warnungsliste und wählen Sie die Option **Schnelle Antwort**.



3. Klicken Sie auf der Seite „Schnelle Antwort“ auf den entsprechenden Link, um die gewünschte Aktion auszuführen.
   Wenn der gewünschte Link nicht verfügbar ist, führen Sie eine dieser Aktionen aus.

Option	Bezeichnung
Bei Fehlerkorrekturen definieren Sie eine Korrekturaufgabe, und zwar abhängig von einer Warnungsregel und basierend auf der ausgewählten Warnung	**a.** Navigieren Sie zu **Warnungsregeln**. **b.** Wählen Sie die gewünschte Warnungs–verwaltungsregel zur Bearbeitung aus. **c.** Klicken Sie auf **Fehlerkorrektur**. **d.** Klicken Sie auf **Fehlerkorrektur aktivieren**. **e.** Wählen Sie im Feld **Ausführung** entweder „automatisch“ oder „manuell“ aus. **f.** Geben Sie im Workflow-Feld **Orchestration** den gewünschten Workflow für die Fehlerkorrektur an. ▪ Bei **Orchestration** wählen Sie in den Workflow-Einstellungen die **Korrekturaufgabe [em_remediation_task]** im Feld **Tabelle** aus. ▪ Veröffentlichen Sie den Orchestration Workflow, wenn Sie ihn fertig konfigu–riert haben. **g.** Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.
Erstellen Sie bei „Anwendung starten“ einen Link auf eine Webanwendung, indem Sie basierend auf der ausgewählten Warnung eine Warnungsregel verwenden	**a.** Navigieren Sie zu **Warnungsregeln**. **b.** Wählen Sie die gewünschte Warnungsverwaltungsregel zur Bearbeitung aus. **c.** Klicken Sie auf **Startprogramm**. **d.** Klicken Sie auf **Aktivieren**. **e.** Geben Sie im Feld **Anzeigename** einen Namen für den Link ein. **f.** Im Feld **URL** erstellen Sie anhand von Daten aus der Warnung die URL, und zwar im folgenden Format: `${source}.com:${port}/${cmdb_ci.name}` **g.** Klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Nächste Maßnahme

Informationen dazu, wie Sie Korrekturaufgaben oder Links zu Webanwendungen erstellen, finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Zugehörige Informationen

Webanwendungen aus einer Warnung starten

Serviceintegritätüberwachung

Auf der Betreiber-Arbeitsbereich, Sie können Warnungen nach Anwendungsservices, technischem Service und Warnungsgruppe anzeigen. Für Services können Sie auch eine Servicezuordnung öffnen, um Beziehungen zwischen CIs im Service anzuzeigen.

Vorbereitungen

Bitten Sie einen Administrator, mindestens einen Anwendungsservice, einen technischen Service oder eine Warnungsgruppe zu erstellen, wenn keines dieser Elemente vorhanden ist.

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Die Kacheln Betreiber-Arbeitsbereich stellen einen Service, eine Warnungsgruppe oder ein CI dar. Die Kachelfarbe stellt den Gesamtschweregrad der Warnung dar.

Hinweis: Das Ereignismanagement-Dashboard wird für neue Instanzen im Paris-Release nicht unterstützt. Für Instanzen, die ausgehend von einem Release vor Orlando aktualisiert wurden und in denen das Ereignismanagement-Dashboard verwendet werden kann, ist dies jedoch weiterhin möglich.

Diese Kachelsymbole sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard-Kachelsymbole

Symbol	Bedeutung
	Stellt den Status eines zugeordneten Anwendungsservices dar.
	Stellt den Status einer Warnungsgruppe mit einer Reihe von entsprechenden offenen Warnungen dar.
	Stellt den Status einer dynamischen CI-Gruppe dar.

Jede Kachel stellt den höchsten Schweregrad einer Warnung für den Service, die Warnungsgruppe oder das CI dar. Beispielsweise wird eine Kachel rot angezeigt, wenn eine Warnung kritisch ist. Eine grüne Kachel zeigt entweder Informationswarnungen oder keine derzeit aktiven Warnungen an. Wenn sich die Warnungsschweregrade ändern, werden die Kachelfarben entsprechend aktualisiert. Die folgenden Schweregrade sind verfügbar:

- **Rot**: Schweregrad „Kritisch“ (höchster Schweregrad) Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.
- **Orange**: Schweregrad „Schwerwiegend“ Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.
- **Gelb**: Schweregrad „Gering“ Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten.
- **Blau**: Schweregrad „Warnung“ (niedrigster Schweregrad) Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist.
- **Frün**: Information. Kein Schweregrad Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.

Prozedur

Aktivieren Sie zur Integration mit Operational Intelligence das Plugin „Operational Intelligence“ (com.snc.sa.metric).
Befolgen Sie die Schritte im Erste Schritte mit Metrikdaten Thema. Metrikinformationen werden im angezeigt **Metriken** Registerkarte im Service Operations-Arbeitsbereich.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Erkannten Service-Verlauf anzeigen

Der Verlauf der erkannten Services zeigt die Häufigkeit der erkannten Services für einen bestimmten Zeitraum an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Der Verlauf der erkannten Services wird nur angezeigt, wenn mehrere erkannte Services innerhalb eines Zeitraums auftreten. Ein erkannter Service ist ein Service, der von Service-Mapping erkannt wird. Der Verlauf der erkannten Services ist für Anwendungsservices nicht verfügbar. Wenn für einen bestimmten Service keine erkannten Services generiert werden, wird der Verlauf der erkannten Services ausgeblendet.

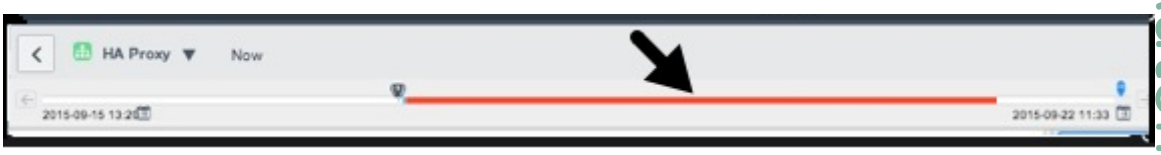
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Service Operations-Arbeitsbereich**an.
2. Klicken Sie auf eine Servicekachel, und klicken Sie auf **Servicezuordnung**.
3. Klicken Sie auf die Schaltfläche **Verlaufszuordnung**.

   Die Verlaufszeitleiste wird angezeigt. Änderungen am Service werden durch ein Uhrensymbol ( ) angezeigt.

4. Zum Anzeigen einer Zuordnung, die Änderungen am Schweregrad des Services darstellt, klicken Sie auf das Symbol „Mehr“ ( ), und wählen Sie **Erweiterte Zuordnung**.



   Die angezeigte Farbe entspricht dem Schweregrad der erkannten Services, und die Länge der Leiste in jeder Farbe entspricht der Dauer, die die erkannten Services diesen Schweregrad beibehalten haben.

   In der folgenden Tabelle werden die Schweregradfarben erläutert:

Farben des Serviceschweregrads

Schweregrad	Symbolfarbe
Kritisch	Rot
Schwerwiegend	Orange
Kleiner	Gelb
Warnung	Blau

5. Um die Informationen zu ändern, die auf der erweiterten Zuordnung des erkannten Serviceverlaufs angezeigt werden, klicken Sie auf ein Verlaufssymbol.

   - **Kalendersymbol**: Informationen für derzeit aktive erkannte Services anzeigen.
   - **Stunden**: Informationen zu erkannten Services anzeigen, die in der letzten Stunde aufgetreten sind.
   - **Tage**: Informationen zu erkannten Services anzeigen, die in den letzten 24 Stunden aufgetreten sind.
   - **Wochen**: Informationen zu erkannten Services anzeigen, die in der letzten Woche aufgetreten sind.
   - **Monate**: Informationen zu erkannten Services anzeigen, die im letzten Monat aufgetreten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie Warnungen für Anwendungsservices

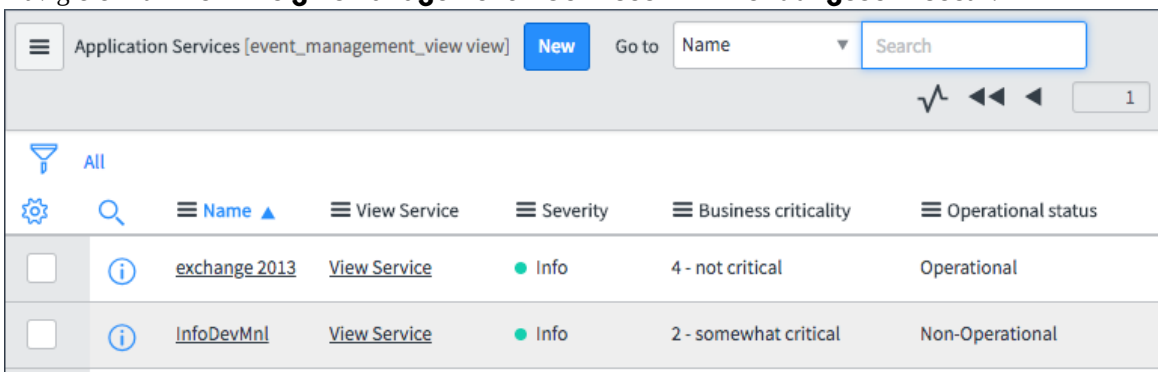
Um Informationen nur für Anwendungsservices anzuzeigen, navigieren Sie zur Liste Anwendungsservices. In dieser Liste können Sie Servicezuordnungen öffnen, um Warnungen für die CIs in jedem Service anzuzeigen und zu verwalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**an.



2. Klicken Sie in der Zeile der erforderlichen Anwendungsservices auf **Karte Anzeigen** .
3. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Aktion
Warnungsdetails für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Karte auf die Registerkarte **Warnungen**, und überprüfen Sie die aufgelisteten Warnungen.
Auswirkung auf übergeordnetes CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Servicezuordnung auf die Registerkarte **Auswirkung**, und überprüfen Sie die aufgeführten Auswirkungsregeln. **c.** Auswirkungsregeln bei Bedarf anpassen
Ändern Sie die Zuordnungsanzeige, das Zuordnungslayout oder die Zuordnungsindikatoren	Im Header der Servicezuordnung: **a.** Klicken Sie auf das Menüsymbol. **b.** Konfigurieren Sie die entsprechenden Einstellungen.
Navigieren Sie zu anderen Anwendungsservices	Im Header der Servicezuordnung: **a.** Klicken Sie auf den Abwärtspfeil neben dem Servicenamen oder das Ordnersymbol für alle Services. **b.** Suchen und wählen Sie andere Anwendungsservices aus ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Die Symbolfarbe stellt die höchste Auswirkung oder den höchsten Schweregrad für aktive Warnungen in den Anwendungsservices dar. ○ **Kritisch**: Rot (höchster Schweregrad). ○ **Schwerwiegend**: Orange. ○ **Geringfügig**: Gelb. ○ **Warnung**: Blau (niedrigster Schweregrad).
Eigenschaften für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie im Seitenbereich auf die Registerkarte **Eigenschaften**, und überprüfen Sie Informationen zum CI. **c.** Wenn Sie detailliertere Informationen anzeigen möchten, scrollen Sie zum Ende des Bereichs, und klicken Sie auf **Detaillierte Eigenschaften**.

Überwachte Services anzeigen

Zeigen Sie alle Services an, die Ereignismanagement Unterstützt z. B. Warnungsgruppen, erkannte Services, Anwendungsservices, und technische Services. Je nach Typ des Services können Sie Details zur Servicedefinition anzeigen oder einen Drilldown in den Service durchführen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

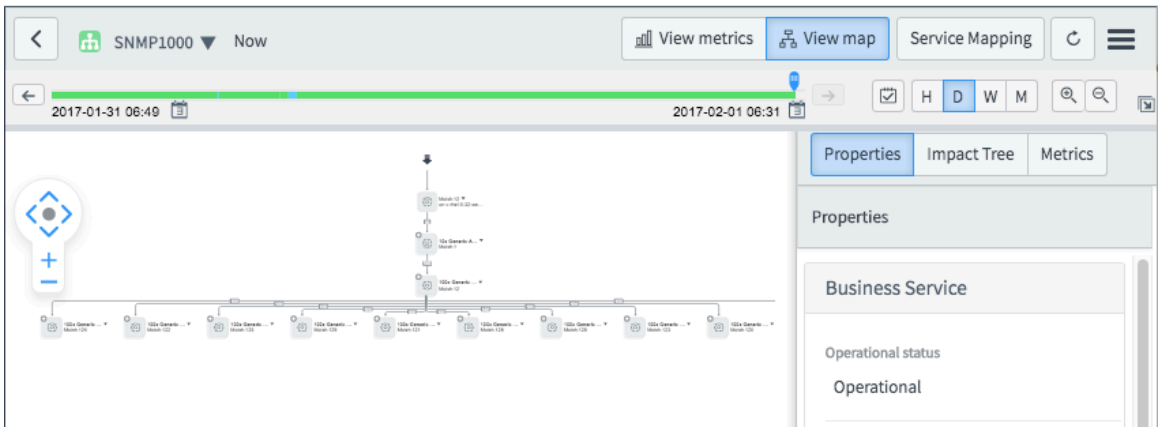
Hinweis: Anwendungsservices, die vor der Aktivierung des Plugins Ereignismanagement erstellt wurden, werden in der Spalte **Service anzeigen** der Liste „Überwachte Services“ nicht aufgeführt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Überwachte Services**an.
2. Klicken Sie auf **Service anzeigen**, um die für diesen Service relevante Ansicht zu öffnen.
   Wenn Sie einen Drilldown zum Inhalt des Services durchführen, wird je nach Service-Typ entweder eine Zuordnung, eine Warnungsliste oder eine CI-Liste angezeigt.

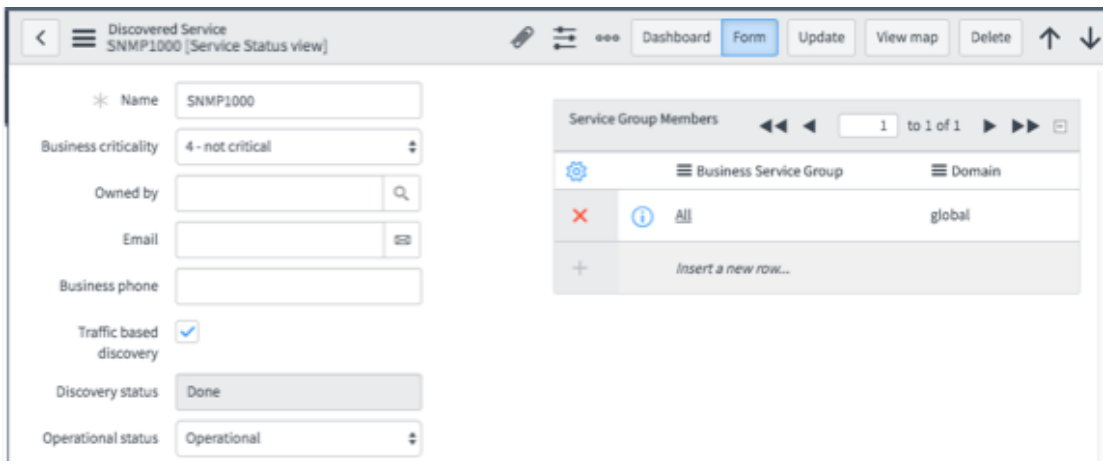
   Wenn Sie beispielsweise für SNMP1000 auf **Service anzeigen** klicken, können Sie einen Drilldown zum Inhalt des Services durchführen, und die zugehörige Topologiezuordnung wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Zum Anzeigen von Servicedefinitionsdetails eines Services klicken Sie auf den Namen des Services auf der Seite **Überwachte Services**.

   Beispiel: Klicken Sie in der Spalte **Name** auf SNMP1000 ( ).



Zugehörige Informationen

Serviceintegritätüberwachung

Übersichts-Dashboard „Event Management“ verwenden

Das Ereignismanagement Übersichtsmodul verwendet Performance Analytics zur Präsentation von Daten aus Ihrer Instanz, um Ihre Prozesse besser darzustellen und zu verstehen und kontinuierliche Verbesserungen zu erzielen.

Warum und wann dieser Vorgang ausgeführt wird

Ab dem Xanadu-Release wurde das Ereignismanagement-Übersichtsmodul veraltet und durch die AIOps-Dashboards ersetzt. Zu den veralteten Dashboards gehören:

- Ereignismanagement-Einblicke
- Ereignismanagement-Bewertungslisten
- Ereignismanagement – Übersicht

Die AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten. Sie können Leistungskennzahlen (Key Performance Indicators, KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontexte für die IT-Umgebung insgesamt gewinnen. Weitere Informationen finden Sie unter AIOps-Dashboards in Service Operations-Arbeitsbereich Für ITOM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Performance Analytics und Reporting

Webanwendungen aus einer Warnung starten

Sie können eine Webanwendung aus einer Warnung starten, wenn die in einer Warnungsaktionsregel festgelegten Bedingungen erfüllt sind.

Vorbereitungen

Erstellen und konfigurieren Sie eine Warnungsaktionsregel, damit sie eine URL vorbereitet, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Beispielsweise können Sie mit dieser Funktion abhängig von der Lösung der Warnungsparameter einen Artikel in der Knowledge Base öffnen oder eine URL erstellen.

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Klicken Sie mit der rechten Maustaste auf eine Warnung, und zwar unter „Alle Warnungen“ oder in der Liste der Warnungen im Dashboard Ereignismanagement (für Instanzen, die von einem Release vor Orlando aktualisiert wurden). Wählen Sie anschließend **Schnelle Antwort** aus. Klicken Sie auf den jeweiligen Link, um die in der Warnungsaktionsregel konfigurierte Webanwendung zu starten. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie mit der rechten Maustaste auf die jeweilige Warnung, und wählen Sie die Option **Schnelle Antwort**.
   Ein Fenster wird angezeigt, das eine Liste der verfügbaren, in der Warnungsaktionsregel konfigurierten Webanwendungen sowie den der Warnung entsprechenden Filter enthält. Zeigen Sie zum Anzeigen der Ziel-URL auf den Cursor über dem Namen der Anwendung.

   Hinweis: Kann mindestens ein Parameter der Warnungsaktionsregel nicht gelöst werden, wird der zugehörige Anwendungsname schwarz angezeigt. Nach Lösung der Warnungsparameter wird der Anwendungsname zu einem Link.

3. Klicken Sie auf den Namen einer Anwendung, um die URL in Ihrem Browser zu öffnen (in einer neuen Registerkarte oder einem neuen Fenster).

Example:

Ein häufiger Anwendungsfall ist der Start im Kontext des Quellverwaltungssystems.
Zu anderen Beispielen zählt die Suche in Knowledge Bases, ob innerhalb von ServiceNow oder extern. Jede URL-basierte Aktion kann die Warnungsparameter verwenden, und die URLs können auf Wikis, Messaging-Services, REST APIs usw. verweisen.

Zugehörige Informationen

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

Schnelle Antworten in einer Warnung anwenden

Ereignismanagement Operator-Tutorial

Als Ereignismanagement Operator haben Sie die Aufgabe, Warnungen zu finden und zu analysieren sowie Aktionen zur Lösung des zugrunde liegenden Problems zu ergreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Tutorial durchlaufen

Bevor Sie als Operator arbeiten können, sollten Sie sich anhand des Tutorials mit verschiedenen Konzepten von Ereignismanagement vertraut machen, um zu verstehen, was Operatoren bei der täglichen Arbeit tun.

Starten Sie das Tutorial, indem Sie auf die erste Lektion klicken:

Lektion 1	Übersicht über Events und Warnungen
Lektion 2	Übersicht über die Anwendungsservices
Lektion 3	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	Was Operatoren tun

Eine Übersicht zu Warnungen für Ereignismanagement Operatoren

Als Ereignismanagement Operator müssen Sie wissen, wie eine Warnung aus einem Event generiert wird, worauf Sie bei Warnungen achten müssen und wie Warnungen gruppiert werden können.

Dies ist die erste Lektion im Ereignismanagement Tutorial.

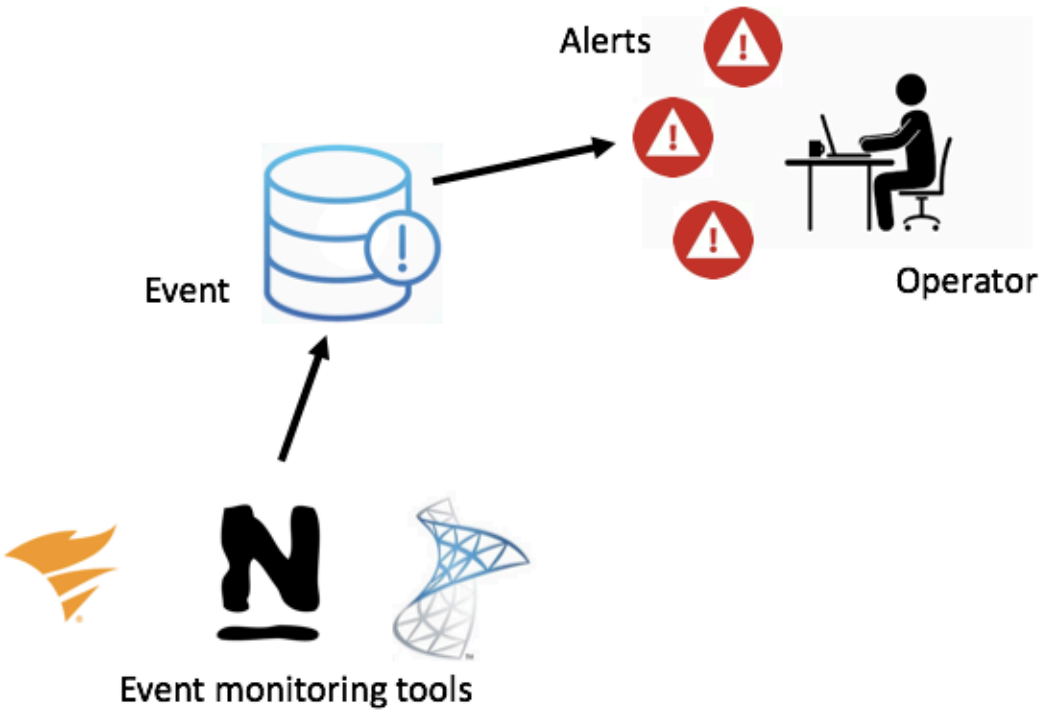
Lektion 1	○	**Übersicht über Events und Warnungen**
Lektion 2	○	Übersicht über die Anwendungsservices
Lektion 3	○	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	○	Was Operatoren tun

Ihre Organisation verfügt bereits über ein Tool für die Event-Überwachung, z. B. Microsoft System Center Operations Manager (SCOM), Nagios, SolarWinds usw. Wenn ein Problem in Ihrem Netzwerk auftritt, z. B. wenn ein Computer oder eine Datenbank ausfällt, senden die Event-Überwachungstools verschiedene *Events* an Ihre ServiceNow Instanz. Die Anwendung Ereignismanagement verarbeitet die *Events* gemäß den vom Administrator konfigurierten Einstellungen und generiert dann *Warnungen*. Eine Warnung ist ein Indikator dafür, dass Probleme eine Aktion erfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgenerierung



Als Ereignismanagement-Bediener besteht Ihre Rolle darin, Warnungen anzuzeigen und je nachdem, wie Ereignismanagement in Ihrer Organisation implementiert ist, eine Aktion zur Behebung des zugrunde liegenden Problems durchzuführen oder jemanden zu diesem Zweck zu benachrichtigen. Später in diesem Tutorial werden die Phasen eines typischen Warnungsverwaltungsprozesses erläutert.

Warnungspriorität und Schweregrad

Die zwei häufigsten Merkmale einer Warnung sind Priorität und Schweregrad.

- Die *Priorität* Einer Warnung ist eine Punktzahl, mit der Sie bestimmen können, wie wichtig die Auswirkung für Anwendungsservices ist. Mehrere Faktoren bestimmen die Prioritätspunktzahl der Warnung. Ihr Ereignismanagement Administrator kann den Algorithmus konfigurieren, den die Anwendung Ereignismanagement zur Berechnung der Priorität verwendet.
- Der *Schweregrad* einer Warnung ist ein Indikator dafür, wie schwerwiegend das zugrunde liegende Problem ist. Das Tool zur Event-Überwachung in Ihrer Organisation übermittelt normalerweise Schweregradwerte mit dem Event, die dann für die Warnung übernommen werden. Die folgenden standardmäßigen Typen von Schweregraden werden in diesem Tutorial vorgestellt:

Schweregrad	Beschreibung
Kritisch	Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad	Beschreibung
Schwerwiegend	Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert.
Geringfügig	Ein partieller, nicht kritischer Verlust der Funktionalität oder eine Leistungsverschlechterung ist aufgetreten.
Warnung	Aufmerksamkeit ist erforderlich, obwohl die Ressource noch funktionsfähig ist.
OK	Kein Schweregrad Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.
Löschen	Die Warnung benötigt keine Aktion mehr.

Korrelierte Warnungen

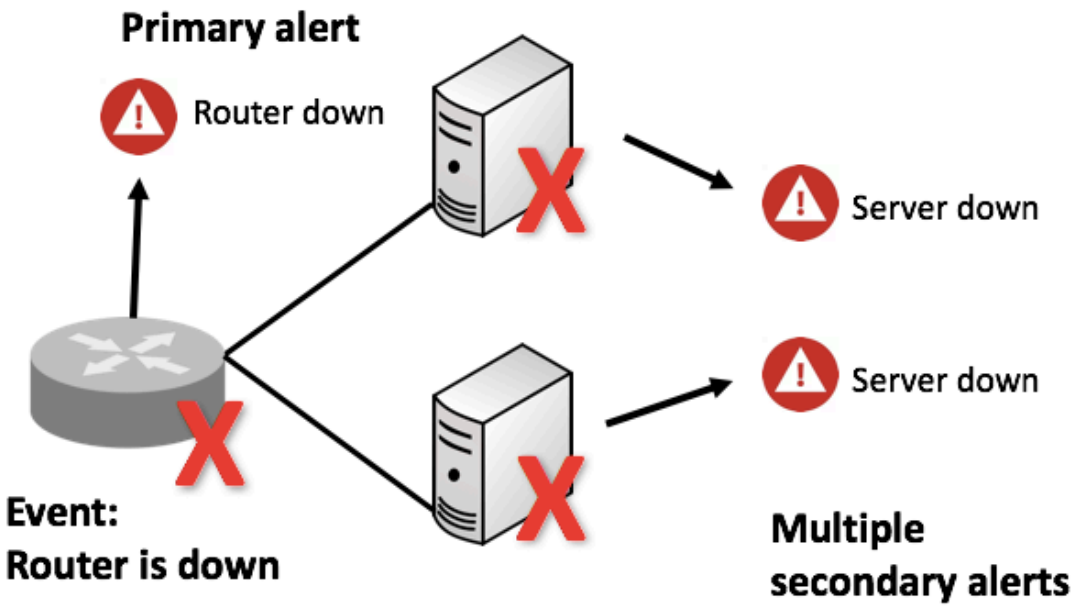
Einige Warnungen sind miteinander verknüpft. Wenn beispielsweise ein Router ausfällt, werden ggf. mehrere separate Warnungen generiert, eine für jeden mit dem Router verbundenen Server. Alle diese Warnungen sind miteinander verbunden oder *korreliert*. Um Sie bei der Verwaltung korrelierter Warnungen zu unterstützen, kann Ereignismanagement diese automatisch gruppieren. Dabei wird eine zweistufige Hierarchie eingerichtet, mit einer Stammwarnung, der so genannten *primären Warnung*, und anderen zugehörigen Warnungen, den sogenannten *sekundären Warnungen*. Wenn Sie Warnungen anzeigen, werden primäre Warnungen standardmäßig hervorgehoben. So wissen Sie immer sofort, auf welche Warnung Sie sich konzentrieren müssen, ohne von den sekundären Warnungen abgelenkt zu werden.

Wenn in unserem Beispiel ein Router in Ihrem Netzwerk ausfällt, ist die Netzwerkkommunikation auch für verbundene Server betroffen, vorausgesetzt, diese können keine anderen Router erreichen. Der Routerausfall wird zur primären Warnung, und die auf dem Server generierten Warnungen sind sekundäre Warnungen, die unter der Routerwarnung korreliert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sekundäre Warnungsgenerierung



Abhängig von der Ereignismanagement-Implementierung in Ihrer Organisation werden Warnungen ggf. automatisch gruppiert, und zwar abhängig von den vom Administrator eingerichteten Korrelationsregeln. Ihre Instanz kann auch lernen, wie Sie die Korrelation von Warnungen basierend auf diesen Regeln verbessern können. Als Operator sollten Sie dennoch stets die Genauigkeit der Korrelation verifizieren und bei Bedarf zusätzliche Warnungen manuell mit der primären Warnung korrelieren. Später im Tutorial erfahren Sie, wie Sie dies tun können.

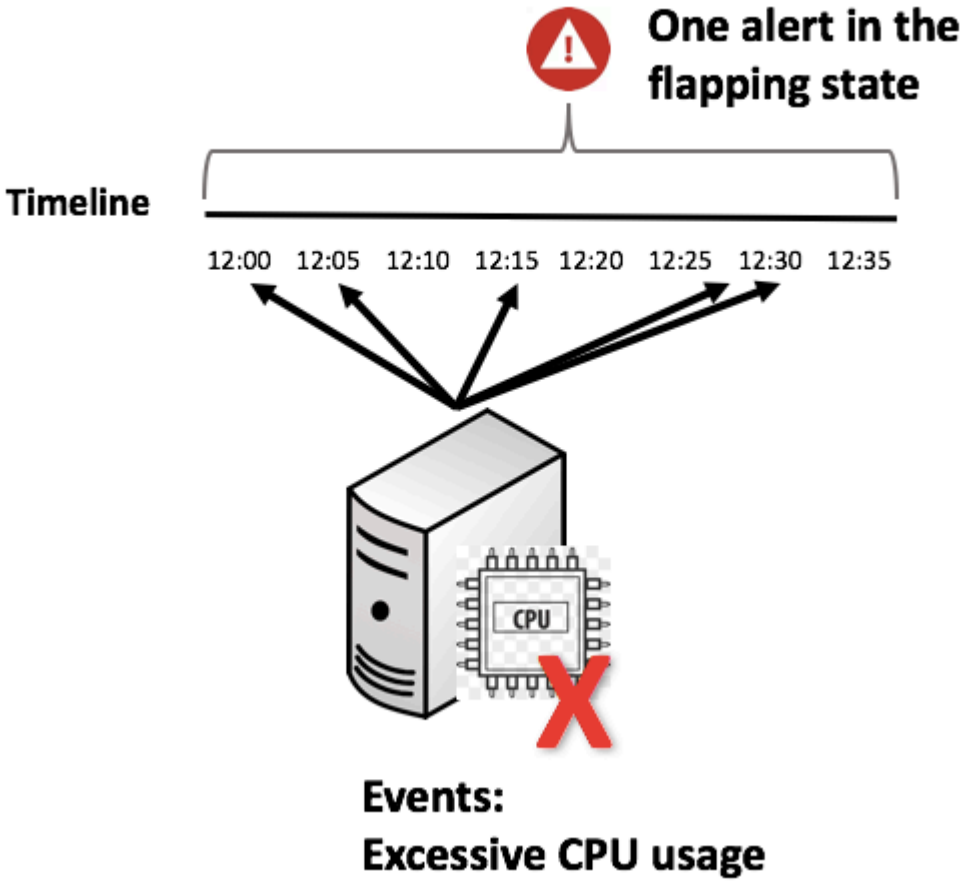
In diesem Tutorial erfahren Sie, wie Warnungen manuell korreliert werden.

Fluktuierende Warnung

Eine Warnung kann „flattern“, wobei sie in schneller Abfolge mehrere Ereignisse vom Typ „Öffnen“ / „Schließen“ erhält. Flattern weist darauf hin, dass Ereignismanagement nicht weiß, ob die zugrundeliegenden Events echt sind oder nicht. Die Events können auf kleine Probleme mit der CI-Konfiguration hindeuten, oder aber auf größere Probleme, z. B. einen Netzwerkausfall.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fluktuierende Warnung



Nehmen wir zum Beispiel einen Server an, der einen Webservice hostet. Wenn der Server zu viele aktive Prozesse aufweist, wird ggf. ein Event aufgrund übermäßiger CPU-Auslastung ausgelöst. Da die CPU-Auslastung je nach Web-Serviceanfragen schnell schwanken kann, werden eventuell mehrere Ereignisse ausgelöst, wodurch die Warnung in den Status „Fluktuierend“ versetzt wird. Als Operator müssen Sie möglicherweise einen Incident erstellen, um den Server neu zu starten; vielleicht muss auch die CPU neu konfiguriert oder eine Hardwareänderung am Gerät vorgenommen werden.

Ein weiteres Beispiel ist ein lockeres Netzwerkkabel, das vorübergehende, wiederholte Netzwerkausfälle verursacht. Die vom Administrator konfigurierten Schwellenwerte sind für diese Art von Warnung möglicherweise nicht optimal, daher geht Ereignismanagement von einer fluktuierenden Warnung aus.

Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Anwendungsservices für Ereignismanagement Operatoren.

Anwendungsservices für Ereignismanagement Operatoren

Als Ereignismanagement Operator, Sie müssen verstehen, was Anwendungsservices sind.

Dies ist die zweite Lektion im Ereignismanagement Tutorial.

Lektion 1	✓	Übersicht über Events und Warnungen

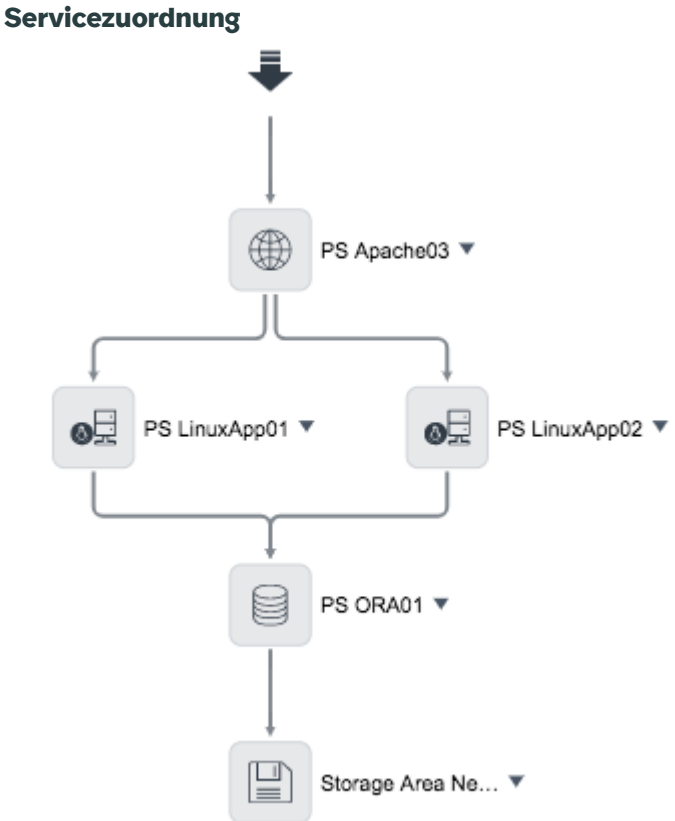
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lektion 2	○	**Übersicht über die Anwendungsservices**
Lektion 3	○	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	○	Was Operatoren tun

Ein Anwendungsservice ist eine Sammlung von Komponenten, z. B. Netzwerkgeräten, Computern und Anwendungen, die Ihrer Organisation einen Service bieten. Bei den Services kann es sich um ein E-Mail-System handeln, oder um eine Website, die Bestellungen oder Anforderungen in einer Datenbank nachverfolgt. Ihr Administrator sollte die Anwendungsservices bereits in angegeben haben ServiceNow Instanz.

Jede Komponente, aus der ein Anwendungsservice besteht, wird als *Konfigurationselement* oder *CI (Configuration Item)* bezeichnet. Diese Servicezuordnung bietet eine visuelle Darstellung für einen Anwendungsservice:



In diesem Beispiel sehen Sie einen Webportal Anwendungsservice mit diesen CIs:

- **PS Apache03**: Ein Apache-Webserver, der eine Unternehmenswebsite hostet.
- **PS LinuxApp01** und **PS LinuxApp02**: Zwei Linux-Server, welche sich die Arbeitsauslastung vom Webservers teilen.
- **PS ORA01**: Ein Datenbankserver, auf den beide Linux-Server zugreifen müssen.
- **Storage Area Network 001**: Massenspeichergerät, von dem andere CIs abhängen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können solche Servicezuordnungen auf dem Dashboard „Service Operations Workspace“ sehen. Später in diesem Tutorial erfahren Sie mehr über das Dashboard und darüber, wie ein Anwendungsservice aussieht, wenn eine Warnung einem CI zugeordnet ist.

Typen von Anwendungsservices

Ereignismanagement Klassifiziert Anwendungsservices in die folgenden Typen:

Technische Services

Ein technischer Service ist eine dynamische Gruppierung von CIs, die auf einigen allgemeinen Kriterien basiert. Beispielsweise kann ein technischer Service aus allen Webservern oder allen Oracle-Datenbanken für einen bestimmten Standort bestehen, z. B. Nordamerika.

Anwendungsservices

Ein Anwendungsservice kann aus erkannten Services, manuellen Services oder beidem bestehen. Ein erkannter Service ist ein Anwendungsservice, der Service-Mapping Anwendungsfindet (wenn Ihre Organisation verwendet Service-Mapping). Ein manueller Service ist ein Anwendungsservice, den Ihr Administrator konfiguriert, indem er CIs auswählt bzw. hinzufügt und die Beziehungen zwischen CIs angibt.

Warnungsgruppen

Warnungen, die entweder manuell oder automatisch gruppiert werden.

Warnungsauswirkung

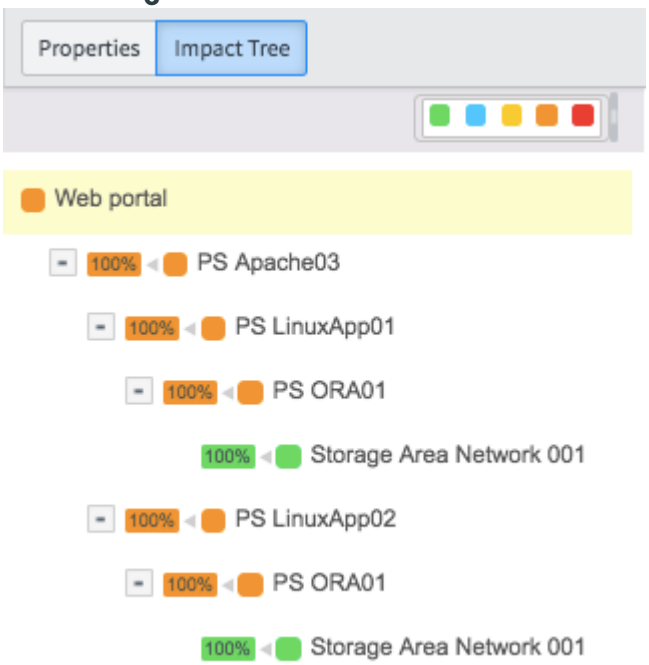
Anwendungsservices sind entscheidend für den Betrieb Ihrer Organisation. Wenn ein Problem bei einem CI auftritt, kann der gesamte Anwendungsservice betroffen sein. Ein Teil Ihrer Rolle als Operator besteht darin, Warnungen auf CIs zu analysieren und zu sehen, wie sie sich auf den Anwendungsservice als Ganzes auswirken. Dann ergreifen Sie eine Aktion, um das zugrunde liegende Problem zu korrigieren oder zu lösen. Ihr Administrator kann Auswirkungsregeln konfigurieren, welche in die Berechnungen zum *Schweregrad* einer Warnung einfließen.

Später erfahren Sie mehr darüber, wie Sie das Dashboard „Service Operations Workspace“ verwenden können. Dabei zeigen wir Ihnen, wie Sie eine *Auswirkungsstruktur* für einen Anwendungsservice anzeigen, um die Beziehung zwischen dem Schweregrad einer Warnung und dem gesamten Anwendungsservice zu verstehen.

In diesem Beispiel sehen Sie eine **schwerwiegende** Warnung zu einer Oracle-Datenbank (**PS ORA01**), die ebenfalls schwerwiegende Warnungen für die übergeordneten CIs und den Webportal Anwendungsservice auslöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkungsstruktur



Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Ereignismanagement Operator-Umgebung.

Ereignismanagement Operator-Umgebung

Als Ereignismanagement Operator, Ihre primäre Arbeitsumgebung ist der Dashboard „Service Operations Workspace“.

In dieser dritten Lektion im Ereignismanagement Tutorial erhalten Sie einen Überblick über Ihre Arbeitsbereiche, um immer schnell die benötigten Informationen finden zu können.

Tutorial-Lektionen

Lektion 1	✓	Übersicht über Events und Warnungen
Lektion 2	✓	Übersicht über die Anwendungsservices
Lektion 3	○	Ereignismanagement Operator-Umgebung
Lektion 4	○	Was Operatoren tun

Das Dashboard „Service Operations-Arbeitsbereich“

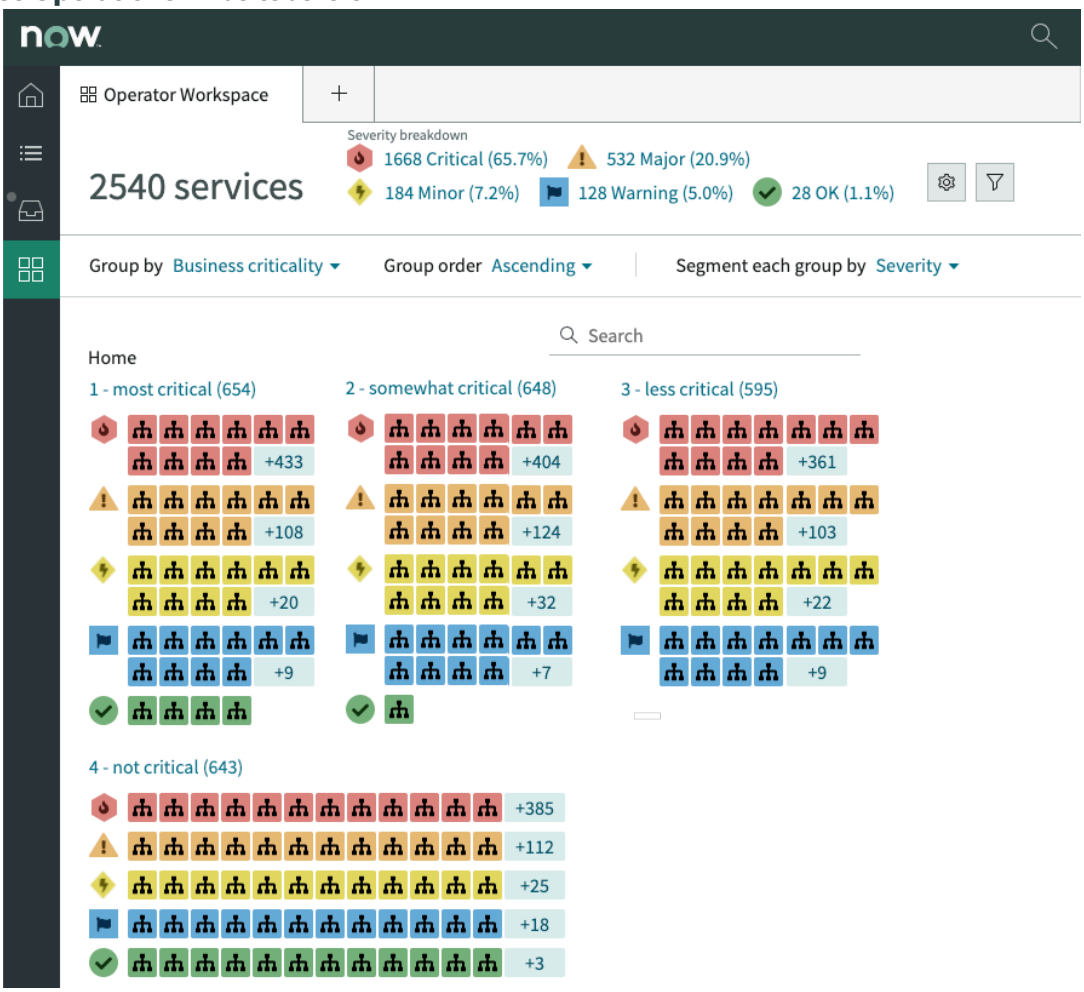
Ihr Hauptarbeitsbereich ist das Dashboard „Service Operations-Arbeitsbereich“, das eine Ansicht bietet, die sich darauf konzentriert, wie sich Warnungen auf Anwendungsservices beziehen. Von hier aus können Sie Detailinformationen zu den einzelnen Anwendungsservices anzeigen, um die betroffenen CIs anzuzeigen und ein Verständnis der Gesamtauswirkungen der Ursache der Warnung zu erhalten. Um das

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard zu öffnen, wechseln Sie zu: **Ereignismanagement** > **Service Operations-Arbeitsbereich**an.

Service Operations-Arbeitsbereich



Die Hauptbereiche des Dashboards sind:

Banner

Das Banner enthält Steuerungen, die Anwendungsservices basierend auf den von Ihnen ausgewählten Kriterien anzeigen oder ausblenden:

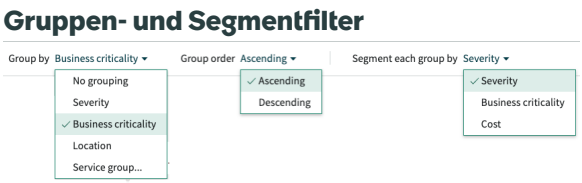
Klicken Sie auf einen Schweregrad, um Anwendungsservices basierend auf den zugehörigen Warnungen anzuzeigen oder auszublenden.

Verwenden Sie die Steuerungen **Gruppe** und **Segment**, um die Ansicht zu organisieren.

Hinweis: Ihr Administrator weist einer Anwendung die Relevanz und den Kostenwert zu.

Automatische Übersetzung

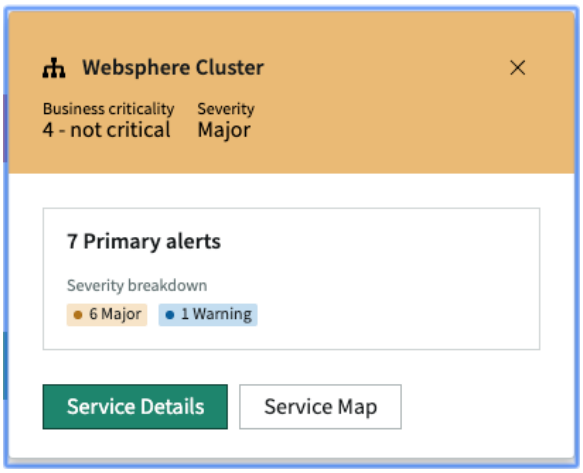
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Anwendungsservices

Die Dashboard „Service Operations Workspace“Zeigt Kacheln an, die Anwendungsservices darstellen. Die Farbe einer Kachel repräsentiert den *Schweregrad* der Warnungen, die dem Anwendungsservice zugeordnet sind.

Klicken Sie auf eine Kachel, um eine Zusammenfassung der Warnungen anzuzeigen, die mit dem Anwendungsservice verknüpft sind. Klicken Sie, um Details oder die Servicezuordnung anzuzeigen.



Warnungen

Klicken Sie auf das Listensymbol (List). Klicken Sie auf der Registerkarte „Listen“ auf die anzuzeigende Warnung.

Sie können die Liste filtern oder sortieren, um eine bestimmte Warnung zu finden. Sortieren Sie nach beliebigen Warnungsdetails, z. B. nach **Priorität**. Dabei werden mehrere Faktoren für den **Schweregrad** der Warnung berücksichtigt; dieser Wert wird vom Tool für die Event-Überwachung bereitgestellt.

Öffnen Sie eine beliebige Warnung, indem Sie auf die Nummer klicken.

Bei der Analyse einer Warnung erfahren Sie später, was die einzelnen Spalten bei einer Warnung bedeuten.

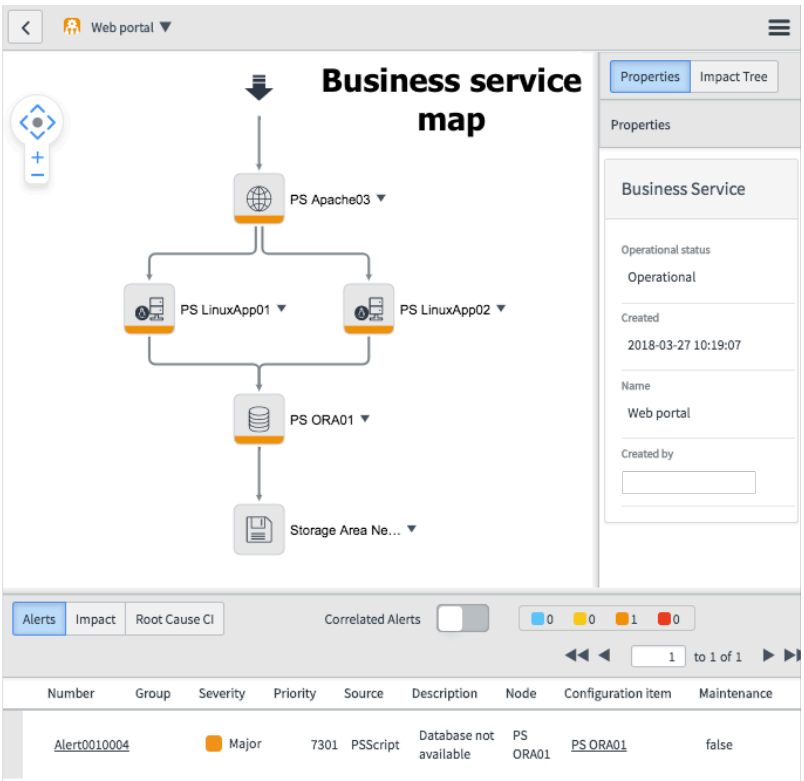
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservice-Zuordnungsansichten im Dashboard „Service Operations-Arbeitsbereich“

Doppelklicken Sie auf den Namen einer Anwendungsservice-Kachel, um eine der Anwendungsservice-Zuordnungsansichten zu öffnen. Welche Ansicht angezeigt wird, hängt vom Anwendungsservice-Typ ab.

Für einen Anwendungsservice vom Typ *manuell* oder *Standard* wird diese Ansicht angezeigt:

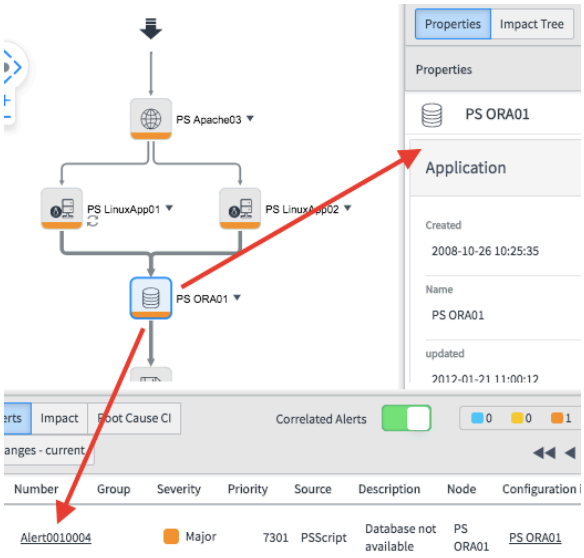


Die in einer vorherigen Lektion vorgestellte Anwendungsservicezuordnung wird im Hauptbereich angezeigt. Folgendes ist in dieser Ansicht möglich:

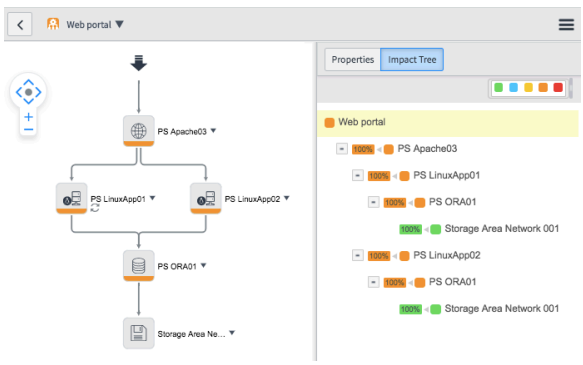
Klicken Sie auf eines der CIs, um nur Warnungen für dieses CI anzuzeigen, und die Details zu diesem CI im Bereich **Eigenschaften** anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



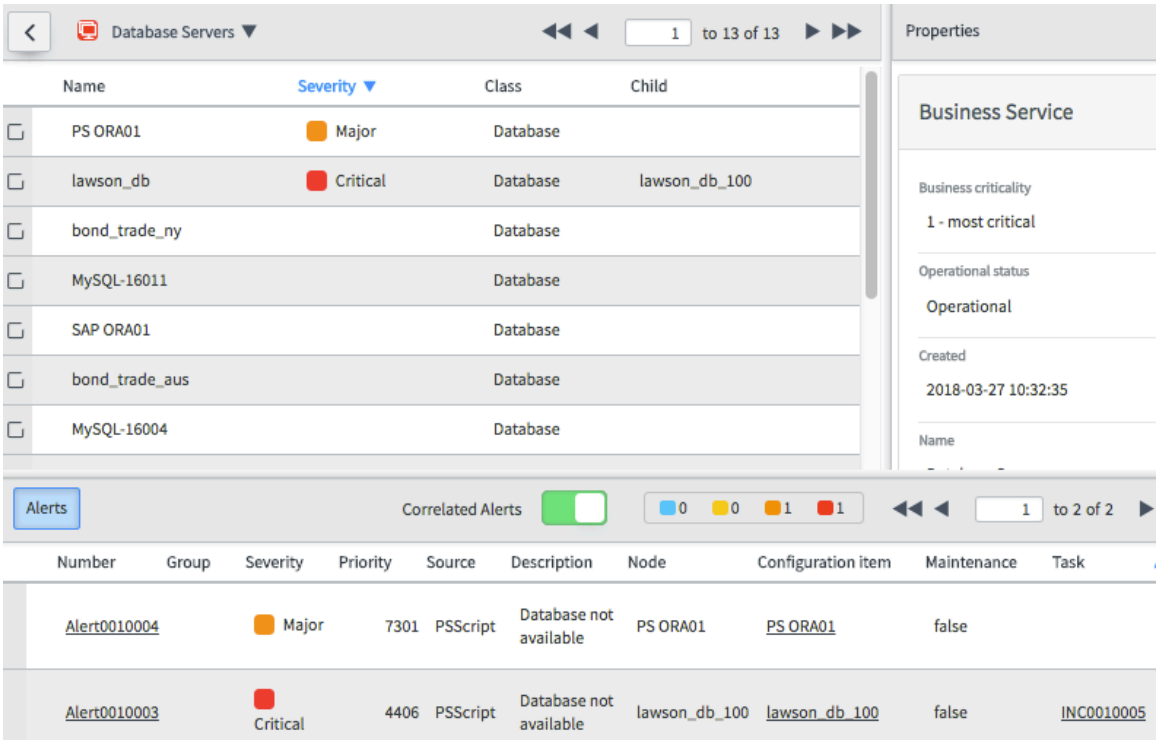
Klicken Sie auf **Auswirkungsstruktur**, um den Status aller CIs anzuzeigen sowie ihre Auswirkungen aufeinander beim Empfangen einer Warnung. Sie werden später im Tutorial mehr über die Auswirkungsstruktur erfahren.



Öffnen Sie eine beliebige Warnung aus der Liste **Warnungen** unten, indem Sie auf die Nummer klicken.

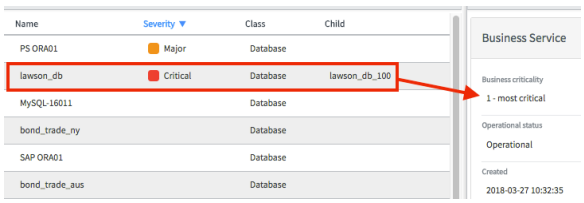
Für einen *technischen* Anwendungsservice wird diese Ansicht angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Folgendes ist in dieser Ansicht möglich:

Klicken Sie auf ein CI, um Details dazu anzuzeigen.



Öffnen Sie eine beliebige Warnung aus der Liste **Warnungen** unten, indem Sie auf die Nummer klicken.

Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Was Ereignismanagement Operatoren tun.

Was Ereignismanagement Operatoren tun

Als Ereignismanagement Operator, Ihr typischer Workflow umfasst drei Phasen: Analyse einer Warnung und ihrer Auswirkungen auf Anwendungsservices, Durchführung einer Art von Aktion und Sicherstellung, dass die Warnung endgültig geschlossen wird.

Dies ist die letzte Lektion im Ereignismanagement Tutorial. In dieser Lektion gehen wir die drei Phasen eines alltäglichen Operator-Workflows durch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lektion 1	✓	Übersicht über Events und Warnungen
Lektion 2	✓	Übersicht über die Anwendungsservices
Lektion 3	✓	Ereignismanagement Service Operations-Arbeitsbereich
Lektion 4	○	**Was Operatoren tun**

Ihre Organisation verfügt sicherlich über spezifische Richtlinien und Verfahren, die von den in diesem Thema beschriebenen Phasen abweichen können. Darüber hinaus hat Ihr Administrator möglicherweise die Anwendung Ereignismanagement angepasst, sodass einige dieser Phasen automatisiert sind, und von Ihnen keine Aktion erfordern.

Für die Zwecke dieses Tutorials führen wir Sie durch die einzelnen Phasen und ermöglichen Ihnen, die Aufgaben manuell auszuführen.

Phase 1	Warnungen analysieren und bestätigen	In dieser Phase finden Sie eine Warnung, die bearbeitet werden soll, analysieren die Details und bestätigen die Warnung, damit andere Operatoren wissen, dass es sich um eine gültige Warnung handelt.
Phase 2	Warnungen selektieren	In dieser Phase ergreifen Sie eine Aktion, um das Problem hinter der Warnung zu beheben. In den meisten Fällen werden Sie einen Incident erstellen und jemandem zuweisen, der das zugrunde liegende Problem lösen kann.
Phase 3	Warnungen schließen	In dieser Phase verifizieren Sie, ob die Warnung gelöst wurde, und schließen die Warnung anschließend.

Beginnen Sie hier

Lernen Sie zunächst, wie Sie Warnungen analysieren und bestätigen.

Operator-Phase 1: Warnungen analysieren und bestätigen

Als Ereignismanagement Operator sollten Sie zuerst auf Warnungen zugreifen und dann diejenigen suchen, auf die Sie sich konzentrieren möchten. Sie können das Warnungsformular öffnen, um Details zu analysieren, und dann die Warnung bestätigen. So teilen Sie anderen Operatoren mit, dass das Problem hinter der Warnung in irgendeiner Weise behoben werden muss.

Vorbereitungen

Phase 1	○	**Warnungen analysieren und bestätigen**
Phase 2	○	Warnungen selektieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phase 3	Warnungen schließen

Sie müssen beide Operatorumgebungen verstehen: Die Dashboard „Service Operations Workspace“Und Service Operations-Arbeitsbereich. Überprüfen Sie Ereignismanagement Operator-Umgebung, falls noch nicht geschehen. Dieses Tutorial verwendet das Dashboard „Service Operations Workspace“.

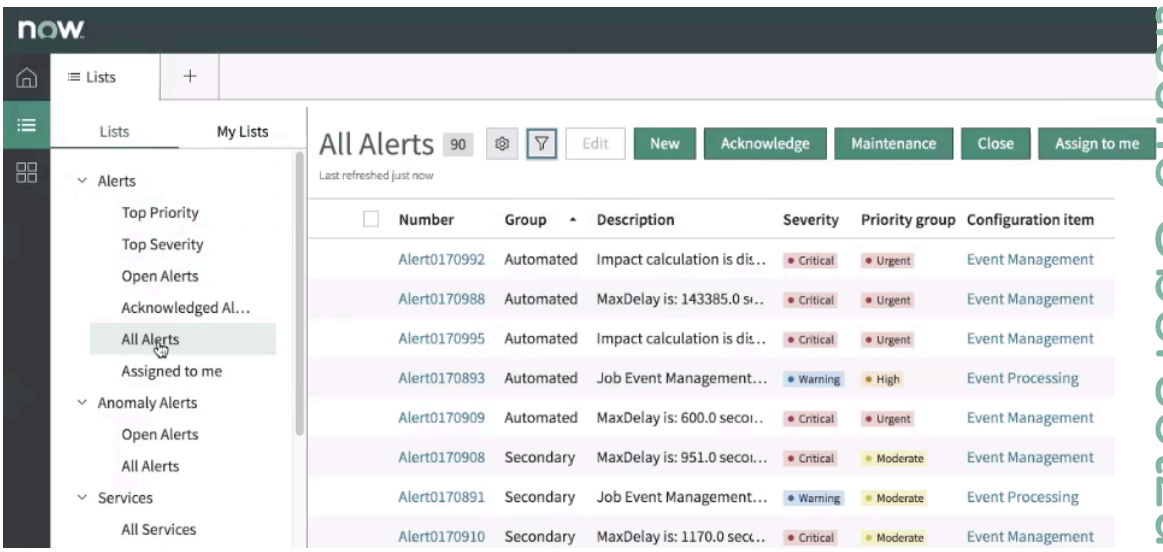
Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Ereignismanagement** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.

   Klicken Sie in der Liste auf **Alerts** > **Alle Warnungen**an. Standardmäßig werden alle Warnungen nach **Gruppe** sortiert in der Liste angezeigt. Klicken Sie auf eine beliebige Überschrift, um nach diesem Wert zu sortieren. Um die aktuellen Filtereinstellungen anzuzeigen, klicken Sie auf das Filtersymbol

   . Klicken Sie auf **Erweiterte Ansicht**, um die Filtereinstellungen zu ändern.

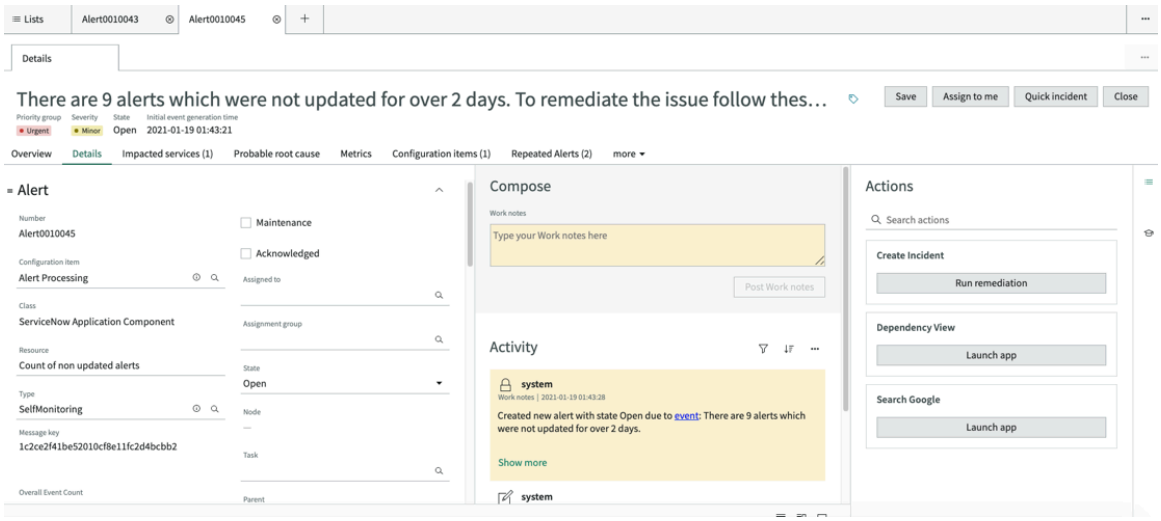


2. Suchen Sie die Warnungen, auf die Sie sich konzentrieren möchten, indem Sie auf klicken **Anwendungsservices** > **Services**, Oder mithilfe einer der Filter- und Sortieroptionen.
3. Klicken Sie auf einen Warnungsnamen, um die Registerkarte **Details** für diese Warnung zu öffnen.

   Example
   Die wichtigen Felder im Formular und zugehörige Elemente werden nach dem Screenshot beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Felder auf der Registerkarte „Warnungsdetails“ für eine Warnung, die einem einzelnen CI zugeordnet ist

Feld	Beschreibung
Anzahl	Die automatisch generierte Warnungsnummer, die Sie in der Liste der Warnungen auf der gesehen haben Dashboard „Service Operations Workspace“.
Knoten	Der Name für das CI, dem die Warnung zugeordnet ist. Das Event hinter der Warnung ist auf diesem CI aufgetreten. Möglicherweise wird ein Computername, eine IP-Adresse oder eine MAC-Adresse eines Geräts angezeigt.
Ressource	Das Objekt auf dem Knoten, welches das Event verursacht hat. Möglicherweise werden Werte angezeigt, wie der Name einer Festplatte, einer CPU oder eines Prozesses/Services. Bei Bedarf können Sie diesem Feld Informationen hinzufügen.
Konfigurationselement	Das CI in der CMDB, für das diese Warnung gilt Wenn dieses Feld leer ist, während das Feld **Knoten** ausgefüllt ist, und Sie wissen, welches CI der Knoten darstellt, können Sie das CI in dieses Feld eingeben, um die Warnung manuell zuzuordnen. **Hinweis:** Ihr Administrator kann Regeln konfigurieren, die CIs automatisch mit einer Warnung verknüpfen, für gewöhnlich basierend auf den Angaben im Feld **Knoten**. Unter Umständen findet das System aber nicht das richtige CI, an welches die Warnung gebunden werden soll. In diesem Fall müssen Sie möglicherweise manuell ein CI auswählen. Für die Zwecke dieses Tutorials gehen wir davon aus, dass das richtige CI mit der Warnung verknüpft ist. Wenn eine Warnung ein CI enthält, wird bei ihrer Auswahl die Registerkarte **Übersicht** geöffnet.
Aufgabe	Alle vorhandenen Aufgaben, die der Warnung zugeordnet sind, werden in diesem Feld angezeigt, z. B. Incidents, Change-Anforderungen oder Probleme. Wenn Sie eine Warnung zum ersten Mal betrachten, ist dieses Feld leer. Sie können eine Aufgabe zuordnen, wenn Sie die Warnung selektieren. Später in diesem Tutorial werden Sie einen Incident mit einer Warnung verknüpfen und den Incident jemandem zuweisen.

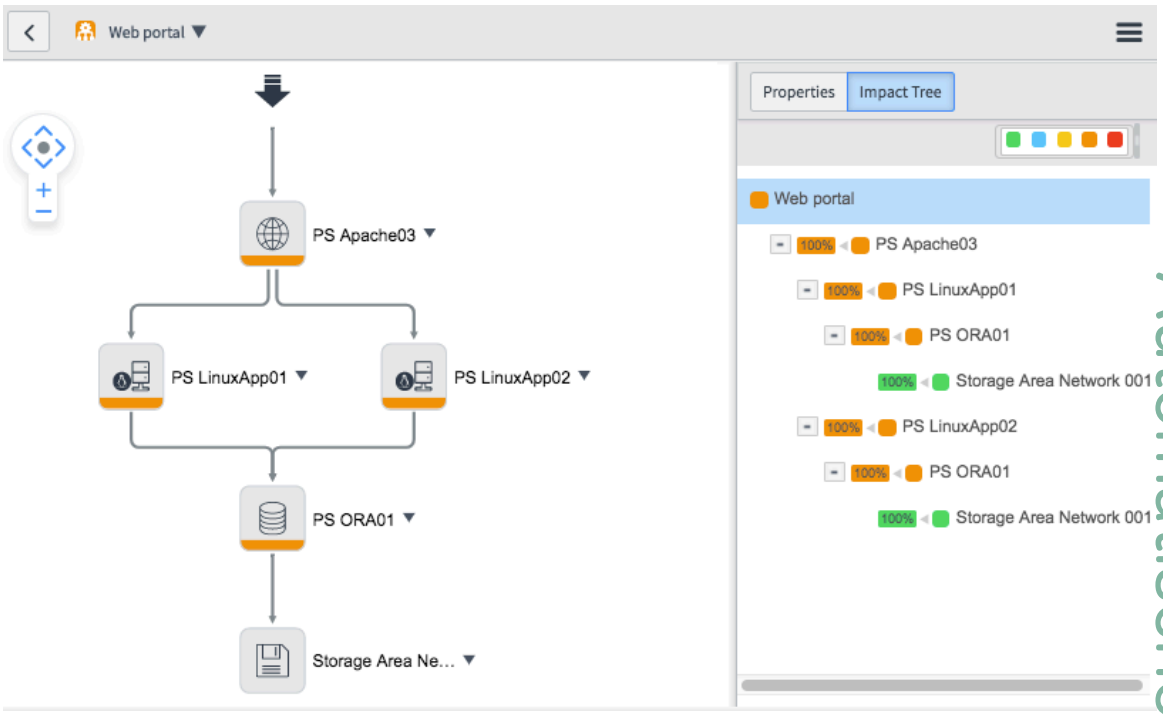
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Eine Beschreibung der Warnung, der von der Software für das Warnungsmonitoring in Ihrer Organisation stammt. Bei Bedarf können Sie Informationen hinzufügen.
Schweregrad	Schweregradwert für die Warnung: ○ Kritisch: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. ○ Schwerwiegend: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung wurde beeinträchtigt. ○ Gering: Es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor, oder die Leistung hat sich verschlechtert. ○ Warnung: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. ○ Info: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. ○ Löschen oder Gelöst: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Status	Der Verarbeitungsstatus, in dem sich die Warnung befindet. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status sind: ○ **Erneut öffnen** gibt an, dass eine zuvor geschlossene Warnung erneut geöffnet wurde und Ihre Aufmerksamkeit erfordert. ○ **Flatternd** gibt an, dass die Warnung häufig identische Events aus der gleichen Quelle erhält. Dadurch werden viele Warnungen erneut geöffnet, nachdem sie geschlossen wurden. ○ **Geschlossen** gibt an, dass die Warnung geschlossen wurde und keine weitere Aktion erfordert. In der letzten Phase dieses Tutorials werden Sie eine Warnung schließen.
Wartung	Gibt an, dass die Warnung nicht bearbeitet werden muss und in der Liste der Warnungen in ausgeblendet ist Dashboard „Service Operations Workspace“. In diesem Beispiel möchten wir die Warnung nicht in den Status „Wartung“ versetzen.
Bestätigt	Gibt an, dass ein Operator die Gültigkeit der Warnung verifiziert hat und sie derzeit selektiert. In einer späteren Phase in diesem Thema werden Sie eine Warnung bestätigen. Ihr Ereignismanagement Administrator kann Warnungen auch sofort automatisch bestätigen lassen, nachdem sie generiert wurden. In diesem Fall ist das Kontrollkästchen **Bestätigen** im Warnungsformular möglicherweise bereits aktiviert.
Übergeordnet	Zeigt nur für sekundäre Warnungen einen Wert an. Der Wert gibt die Warnungsnummer der übergeordneten Warnung an. Für primäre Warnungen (ohne übergeordnete Warnung) ist das Feld leer.
Wissensartikel	Alle vorhandenen Artikel in der Knowledge Base (KB), die der Warnung zugeordnet sind. Wenn Sie eine Warnung zum ersten Mal öffnen, ist dieses Feld leer. Sie können einen KB-Artikel zuordnen, wenn Sie die Warnung selektieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **Betroffene Services**, und klicken Sie dann auf den Servicenamen. Bevor Sie die Warnung bestätigen, möchten Sie ggf. mehr über die Services erfahren, die wegen dem Service hinter der Warnung betroffen sind.

   Der Service wird geöffnet und die Registerkarte **Details** wird angezeigt. Klicken Sie auf **Servicezuordnung**, um die Zuordnung der zugehörigen Anwendungsservices anzuzeigen.



   Beachten Sie, dass der Indikator für den Schweregrad „schwerwiegend“ für mehrere CIs in Orange angezeigt wird. Das beginnt mit der Oracle-Datenbank (**PS ORA01**) und wird an alle CIs weitergegeben, die von der Datenbank abhängen. Sie können also davon ausgehen, dass die Warnung mit dem höchsten Schweregrad in der Oracle-Datenbank die Ursache des Problems darstellt.

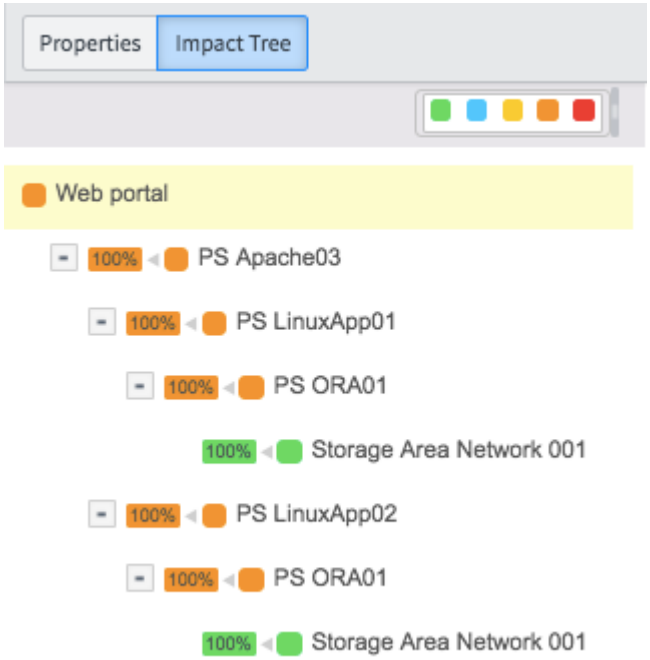
   Das System hat nicht unbedingt separate Warnungen für jedes CI generiert, aber die Möglichkeit besteht. Bei der Selektierung einer Warnung können Sie ermitteln, ob Warnungen über andere CIs unter einer primären Warnung korreliert werden müssen.

5. Klicken Sie auf die Registerkarte **Auswirkungsstruktur** und überprüfen Sie die Auswirkungen auf die CIs.

   Die Prozentsätze neben jedem CI in der Auswirkungsstruktur zeigen die Auswirkung auf die einzelnen CIs an. In diesem Beispiel ist jedes CI zu 100 % von der Warnung betroffen. Das der Warnung zugrunde liegende Problem ist also schwerwiegend genug, um die Funktionalität vom Anwendungsservice zu beeinträchtigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Bestätigen Sie die Warnung.

   Wenn Sie eine Warnung bestätigen, wird sie Ihnen nicht zugewiesen, und es wird keine Aufgabe erstellt (z. B. ein Incident oder eine Change-Anforderung). Durch die Bestätigung werden andere Operatoren darüber informiert, dass Sie von dem Problem wissen. Nachdem Sie eine Warnung bestätigt haben, ergreifen Sie während der Selektierungsphase weitere Aktionen.

Option	Bezeichnung
Einzelne Warnungen bestätigen	Mit diesem Prozess können Sie nur die Warnung bestätigen, die Sie gerade anzeigen. **a.** Öffnen Sie das Formular „Warnungsdetails“, wie zuvor beschrieben. **b.** Wählen Sie das Kontrollkästchen **Bestätigt** aus.
Eine oder mehrere Warnungen bestätigen	Mit diesem Prozess können Sie eine Warnung oder mehrere zugehörige Warnungen bestätigen. **a.** Öffnen Sie die Liste der Warnungen, wie zuvor beschrieben. **b.** Wählen Sie alle zu bestätigenden Warnungen aus. **c.** Klicken Sie auf **Bestätigen**.

7. Navigieren Sie zurück, und suchen Sie nach der Warnung, die Sie bestätigt haben.
   Wie Sie sehen, hat **Bestätigt** den Wert **true**.

Number	Group	Severity ▲	Priority	Source	Description	Node	Configuration item	Maintenance	Task	Acknowledged
Alert0010002		Major	3301	SolarWinds	Database issue	PS ORA01	PS ORA01	false		true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Gehen Sie zu Operator-Phase 2: Warnungen selektieren.

Operator-Phase 2: Warnungen selektieren

Nachdem Sie eine Warnung analysiert und bestätigt haben, müssen Sie diese selektieren. In der Selektierungsphase verifizieren Sie die Korrelation von Warnungen und ergreifen eine Aktion, um das Problem hinter der Warnung zu beheben. In diesem Thema wird die häufigste Selektierungsaufgabe behandelt: Wie Sie einen Incident aus einer Warnung erstellen.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Bevor Sie die Warnung bearbeiten, finden Sie heraus, ob andere Warnungen mit der überprüften Warnung verknüpft werden müssen:

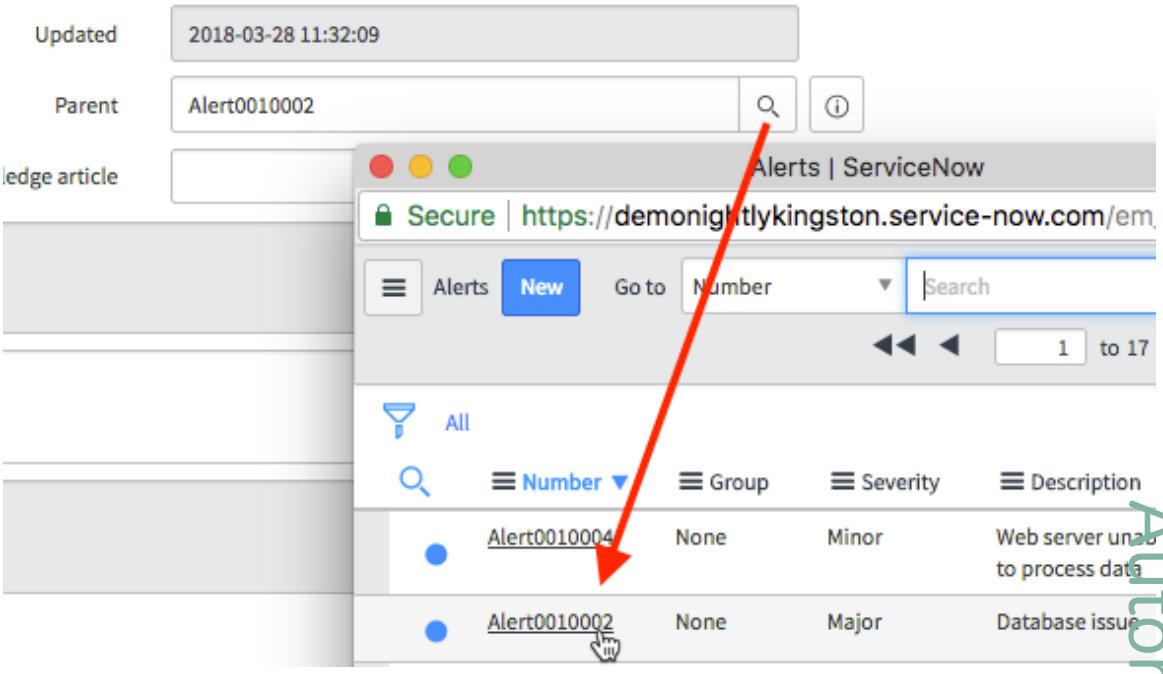
   a. Navigieren zu **Ereignismanagement** > **Service Operations-Arbeitsbereich**an.

   b. Klicken Sie auf dieselbe Anwendungsservice Kachel, und überprüfen Sie die Warnungen in der Liste **Warnungen**.

   c. Wenn mehrere Warnungen vorhanden sind, öffnen Sie eine davon. So können Sie bestimmen, ob sie mit der anderen Warnung verknüpft ist, oder ob das zugrunde liegende Problem in beiden Warnungen gleich ist.
   Nehmen wir zum Beispiel an, dass eine Warnung einem Webserver zugeordnet ist, und bereits eine Warnung für das Datenbankproblem vorliegt. Korrelieren Sie in diesem Fall die Webserver-Warnung als *sekundäre* Warnung mit der Datenbank-Warnung als *primäre* Warnung.

   d. Öffnen Sie die sekundäre Warnung, klicken Sie auf das Suchsymbol (🔍) im Feld **Übergeordnet**, und wählen Sie dann die primäre Warnung aus.
   Dadurch wird eine Beziehung vom Typ „primär (übergeordnet) / sekundär (untergeordnet)“ zwischen den beiden Warnungen erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wiederholen Sie diesen Vorgang, um so viele sekundäre Warnungen wie nötig zu korrelieren.

f. Navigieren Sie zurück zu Dashboard „Service Operations Workspace“, um zu verifizieren, dass für die primäre Warnung ein Symbol in der Spalte **Gruppe** angezeigt wird.

Hinweis: Ihr Administrator kann Regeln einrichten, mit denen das System automatisch Warnungen korrelieren kann, sodass Sie dies nicht manuell tun müssen. In diesem Fall wird im Warnungsformular das Feld **Feedback** angezeigt. Wählen Sie **Ja**, wenn das System die Warnung korrekt korreliert hat, andernfalls **Nein**. Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus.

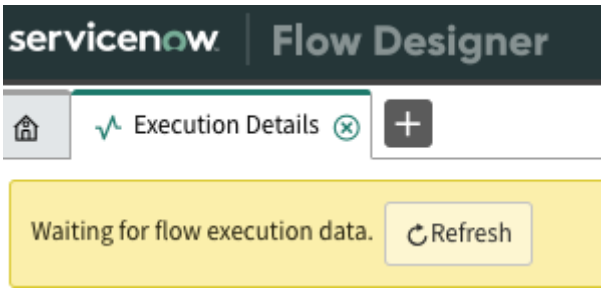
2. Öffnen Sie die primäre Warnung.

3. Klicken Sie im Warnungsformular auf **Aktionen** > **Incident erstellen**an.
Wenn Ihre Organisation Security Incident Response verwendet, ist die Schaltfläche stattdessen **Security Incident erstellen**.

Der Flow Designer wird geöffnet.

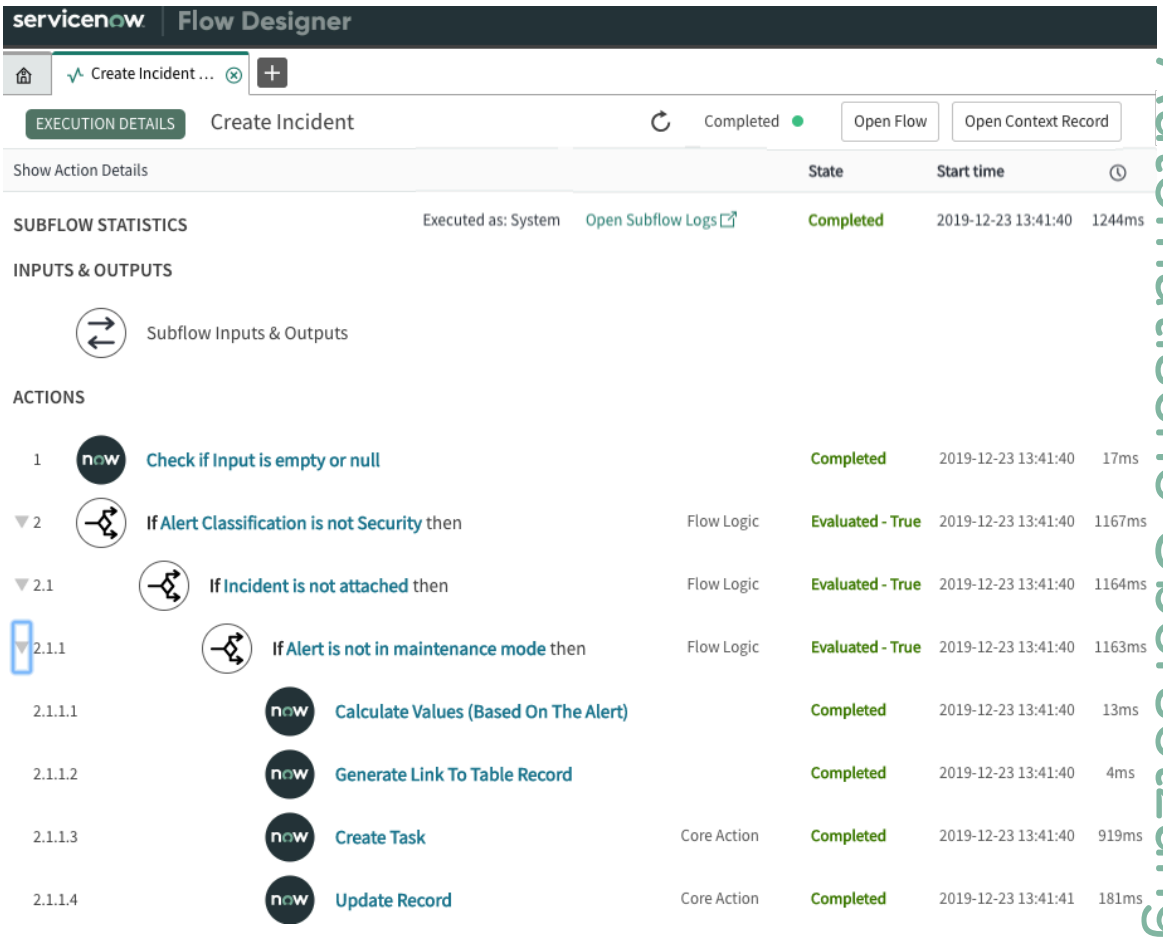
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Aktualisieren**.

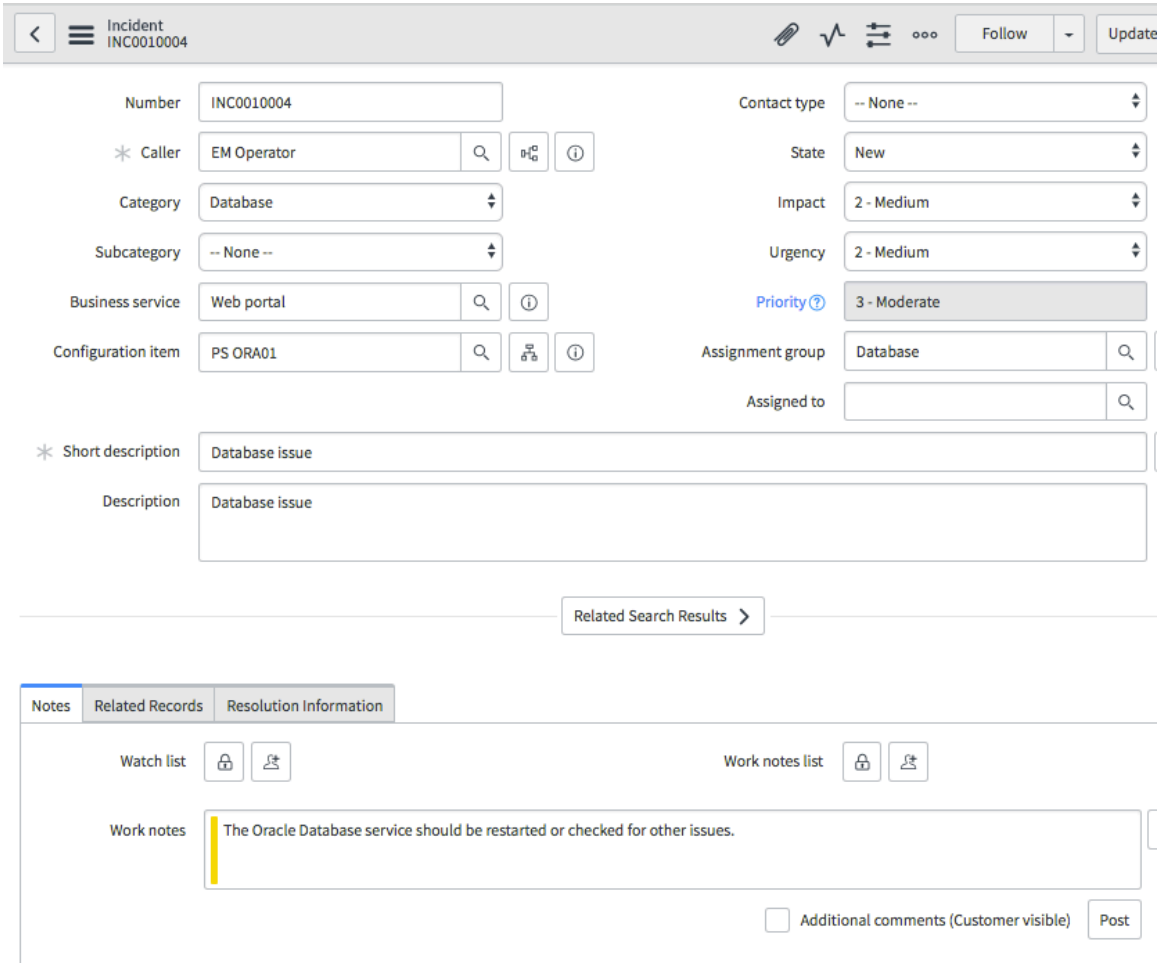
   Die Seite **Ausführungsdetails** wird geöffnet.



5. Klicken Sie auf **Kontextdatensatz öffnen** und füllen Sie das Incident-Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



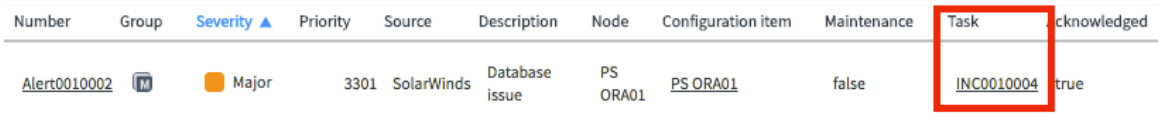
Feld	Beschreibung
Anrufer	Klicken Sie auf das Suchsymbol ( ), und wählen Sie Ihren Namen aus. Der Anrufer ist die Person, die das Problem hinter dem Incident entdeckt hat.
Kategorie und Unterkategorie	Wählen Sie eine Kategorie aus, die diese Warnung am besten beschreibt. In diesem Beispiel ist **Datenbank** die beste Wahl.
Anwendungsservice	Wählen Sie das Anwendungsservice aus, zu dem das CI gehört. In diesem Beispiel ist Anwendungsservice ein **Webportal**.
Konfigurationselement	Wenn es noch nicht ausgefüllt ist, wählen Sie das CI aus. In diesem Beispiel wird die Oracle-Datenbank (**PS ORA01**) automatisch in das Feld eingetragen.
Auswirkung und Dringlichkeit	Wählen Sie die Auswirkungs- und Dringlichkeitsstufen aus, die Sie für angemessen halten.
Zuweisungsgruppe Zugewiesen an	Klicken Sie auf die Suchsymbole ( ) für eines oder beide dieser Felder. Wählen Sie anschließend die Gruppe oder Person aus, die sich dem Problem annehmen soll.

6. Klicken Sie auf **Absenden**, um den Incident zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die von Ihnen bearbeitete Warnung wird erneut angezeigt. Im Warnungsformular wird der Incident im Feld **Aufgabe** ausgefüllt. Die Incident-Nummer wird auch in der Spalte „Aufgabe“ im Dashboard „Service Operations Workspace“ angezeigt.



Number	Group	Severity ▲	Priority	Source	Description	Node	Configuration item	Maintenance	Task	cknowledged
Alert0010002		Major	3301	SolarWinds	Database issue	PS ORA01	PS ORA01	false	INC0010004	true

Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.
- Warnungen in den Status „Wartung“ versetzen Um sie vorübergehend in auszublenden Dashboard „Service Operations Workspace“Wenn die Warnung derzeit keine Aktion erfordert.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Fehlerkorrektur-Workflows für eine Warnung ausführen

Als Ereignismanagement Operator können Sie auch einen Workflow auf Ihrer ServiceNow Instanz ausführen, der Sie bei der Korrektur der Warnung unterstützt. Beispielsweise können Sie einen Workflow ausführen, um automatisch einen Server in Ihrem Netzwerk neu zu starten. Möglicherweise lässt sich so eine Warnung zur CPU-Auslastung lösen.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

Hinweis: Sie können einen Fehlerkorrektur-Workflow ausführen, sofern Ihr Administrator bereits Workflows für Sie eingerichtet hat. Sicherlich sind Sie mit den Richtlinien Ihrer Organisation zur Selektierung von Warnungen vertraut.

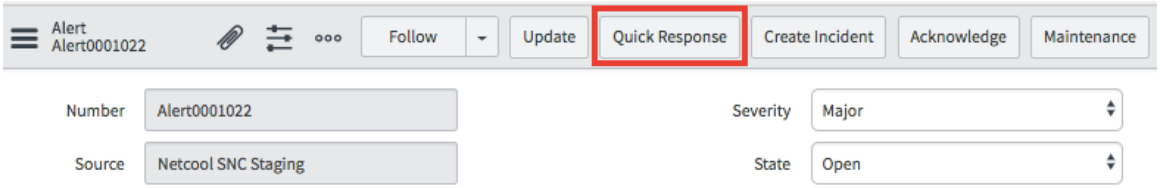
Erforderliche Rolle: evt_mgmt_operator

Automatische Übersetzung

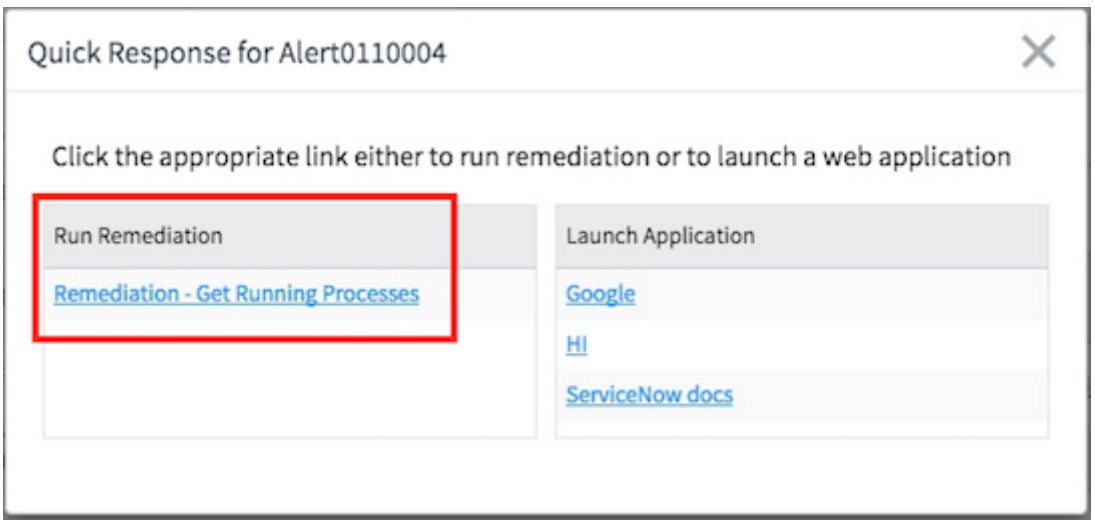
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Von Dashboard „Service Operations Workspace“, Öffnen Sie die Warnung, die Sie in Phase 1 bestätigt haben: Warnung analysieren und bestätigen.
2. Klicken Sie im Warnungsformular auf **Schnelle Antwort**.



3. Klicken Sie im Fenster „Schnelle Antwort“ unter **Fehlerkorrektur ausführen** auf den Namen der Fehlerkorrektur.



Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Warnungen in den Status „Wartung“ versetzen Um sie vorübergehend in auszublenden Dashboard „Service Operations Workspace“Wenn die Warnung derzeit keine Aktion erfordert.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Webanwendungen aus einer Warnung starten

Als Ereignismanagement Operator können Sie auch Webanwendungen aus einer Warnung starten. Die Webanwendung kann eine Konsole für das von Ihrer Organisation verwendete Tool für die Event-Überwachung oder eine externe Website sein, die zusätzliche Informationen zur Warnung bereitstellt.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

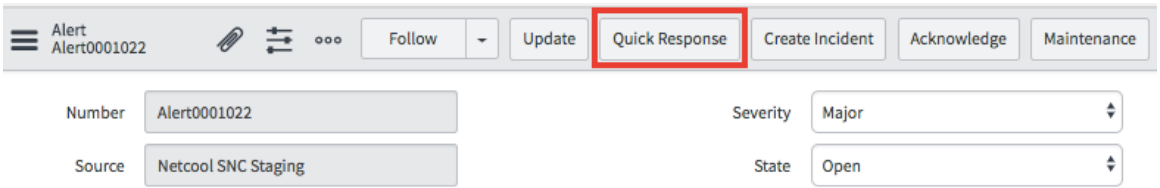
Erforderliche Rolle: evt_mgmt_operator

Sie können eine Webanwendung starten, wenn Ihr Administrator einen Link zur Anwendung eingerichtet hat. Sicherlich sind Sie mit den Richtlinien Ihrer Organisation zur Selektierung von Warnungen vertraut.

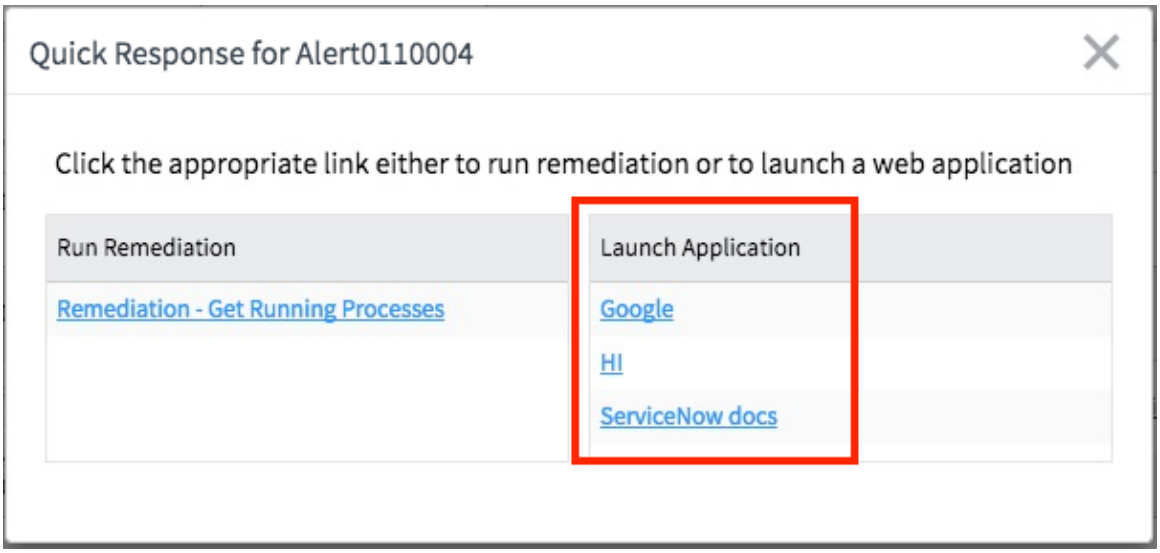
Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Von Dashboard „Service Operations Workspace“, Öffnen Sie die Warnung, die Sie in Phase 1 bestätigt haben: Warnung analysieren und bestätigen.
2. Klicken Sie im Warnungsformular auf **Schnelle Antwort**.



3. Klicken Sie im Fenster „Schnelle Antwort“ unter **Anwendung starten** auf den Namen der Anwendung. Ihr Administrator hat festgelegt, welche Anwendungen in der Liste angezeigt werden sollen.



Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Warnungen in den Status „Wartung“ versetzen Um sie vorübergehend in auszublenden Dashboard „Service Operations Workspace“Wenn die Warnung derzeit keine Aktion erfordert.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Artikel in der Knowledge Base einer Warnung zuordnen

Als Ereignismanagement Operator können Sie der Warnung einen Artikel aus der Knowledge Base (KB) zuordnen, um zusätzliche Informationen zur Warnung zu erfassen. Dazu können Verfahren gehören, die jemand befolgen muss, um das zugrunde liegende Problem in Ihrem Netzwerk zu beheben, oder Best Practices, um ein erneutes Auftreten des Problems zu verhindern.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

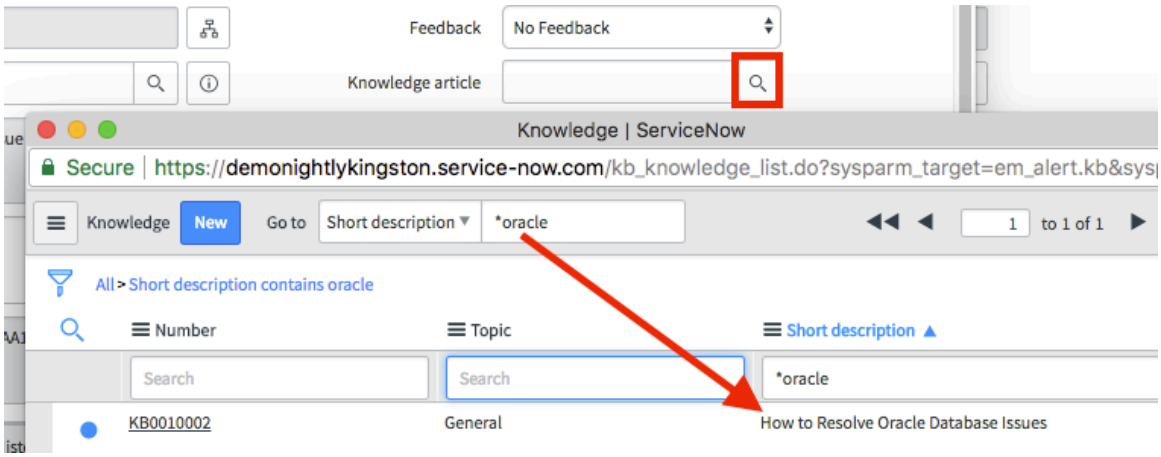
Diese Aufgabe setzt voraus, dass Ihr Unternehmen die Knowledge Base-Anwendung in Ihrer ServiceNow Instanz verwendet.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

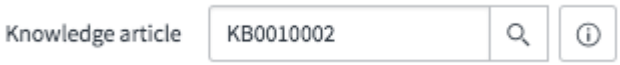
1. Von Dashboard „Service Operations Workspace“, Öffnen Sie die Warnung, die Sie in Phase 1 bestätigt haben: Warnung analysieren und bestätigen.
2. Klicken Sie im Warnungsformular auf das Suchsymbol (🔍) neben dem Feld **Wissensartikel**.
3. Filtern Sie die Liste der vorhandenen KB-Artikel, indem Sie zuerst ein Feld auswählen (z. B. **Kurzbeschreibung**) und dann zugehörigen Text in das Suchtextfeld eingeben.
   Mit dem Operator enthält (*) können Sie nach Artikeln suchen, die Stichwörter enthalten. Nehmen wir z. B. an, dass Sie `*oracle` in die Kurzbeschreibung eingegeben haben. Dann werden die KB-Artikel gefiltert, die das Wort `oracle` in der Kurzbeschreibung enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn Sie keine zugehörigen KB-Artikel finden, können Sie auf **Neu** klicken, einen neuen Artikel erstellen und dann auf **Senden** klicken.

   Die KB-Artikelnummer wird im Feld **Wissensartikel** im Warnungsformular angezeigt.

5. Klicken Sie im Warnungsformular auf **Aktualisieren**, um die Informationen zu speichern.

Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Warnungen in den Status „Wartung“ versetzen Um sie vorübergehend in auszublenden Dashboard „Service Operations Workspace“Wenn die Warnung derzeit keine Aktion erfordert.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Warnungen in den Status „Wartung“ versetzen

Als Ereignismanagement Operator können Sie eine Warnung in den Status „Wartung“ versetzen, wenn keine weiteren Aktionen für die Warnung erforderlich sind, Sie diese jedoch weiterhin aktiviert halten möchten. Wenn Sie die Warnung in die Wartung setzen, wird sie aus dem ausgeblendet Dashboard „Service Operations Workspace“ Damit andere Operatoren nicht darauf zugreifen müssen, die Warnung jedoch nicht geschlossen wird.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Von Dashboard „Service Operations Workspace“, Öffnen Sie die Warnung, die Sie in Phase 1 bestätigt haben: Warnung analysieren und bestätigen.
2. Wählen Sie das Kontrollkästchen **Wartung** aus und klicken Sie auf **Aktualisieren**, oder klicken Sie oben in der Liste auf die Schaltfläche **Wartung**.
3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Ereignismanagement** > **Arbeitsbereich Des Operators**an.

   Beachten Sie, dass Warnungen im Status „Wartung“ standardmäßig nicht in der Liste angezeigt werden. Der Filter schließt Warnungen aus, bei denen `Wartung | = | true`.

Nächste Maßnahme

Wenn das Problem, das zur Warnung geführt hat, später noch weitere Maßnahmen erfordert, navigieren Sie zu **Ereignismanagement** > **Alle Warnungen**, Öffnen Sie die Warnung, und löschen Sie dann **Wartung** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Aktualisieren** . Von dort aus können Sie weitere Selektierungsaktionen ausführen.

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Operator-Phase 3: Warnungen schließen

Nachdem Sie eine Aktion für eine Warnung ergriffen haben, können Sie mehrere Elemente in der Warnung überprüfen und diese dann schließen.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	✓	Warnungen selektieren
Phase 3	○	**Warnungen schließen**

Erforderliche Rolle: evt_mgmt_operator

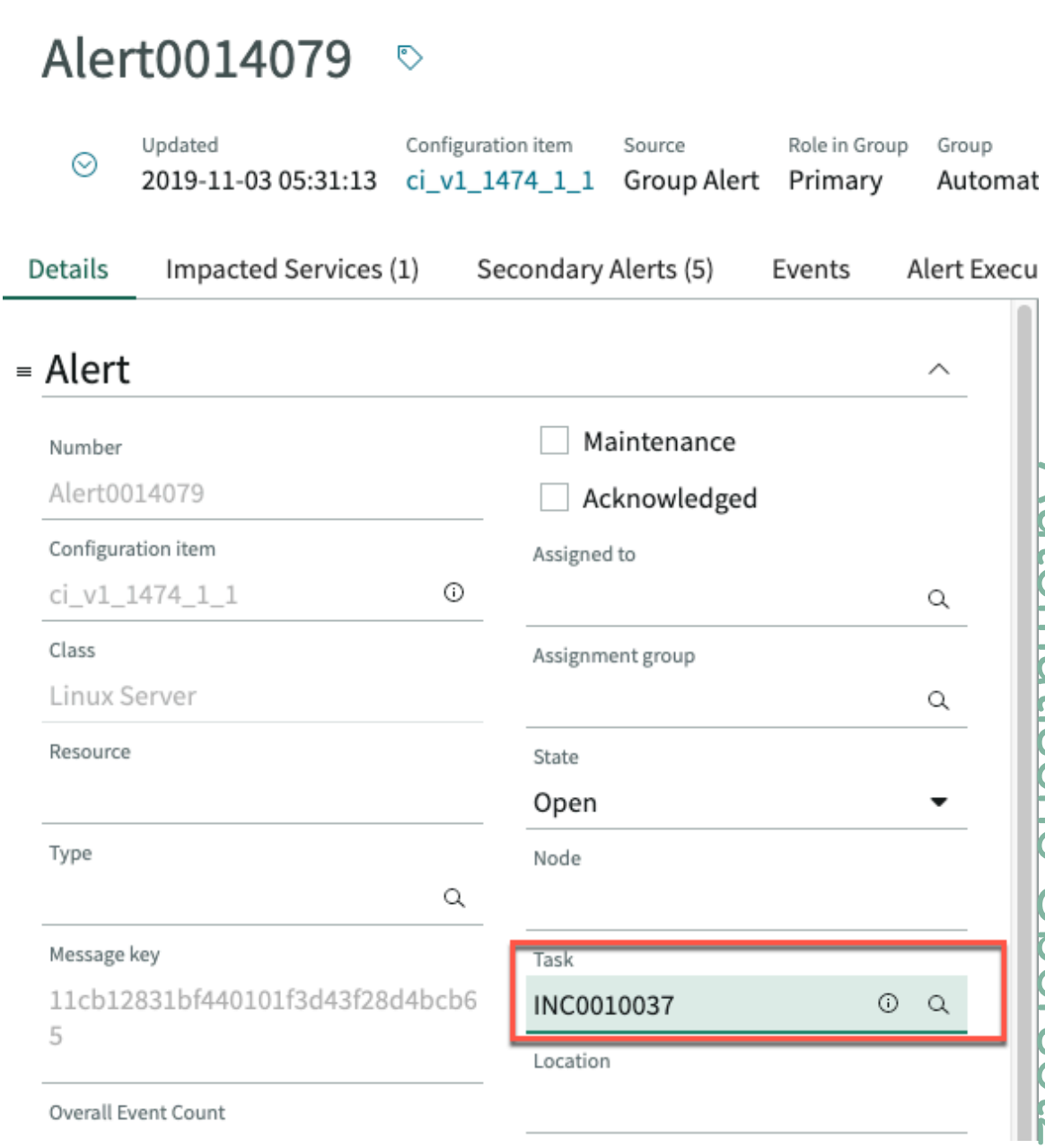
Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Suchen Sie die Warnung, die Sie schließen möchten.
   Wird die Warnung nicht in der Liste angezeigt, z. B. weil sie sich im Status „Wartung“ befindet, ändern Sie nach Bedarf die Filteroptionen.
3. Klicken Sie auf die Warnungsnummer, um die Registerkarte „Warnungsdetails“ zu öffnen und wichtige Informationen zur Warnung zu überprüfen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

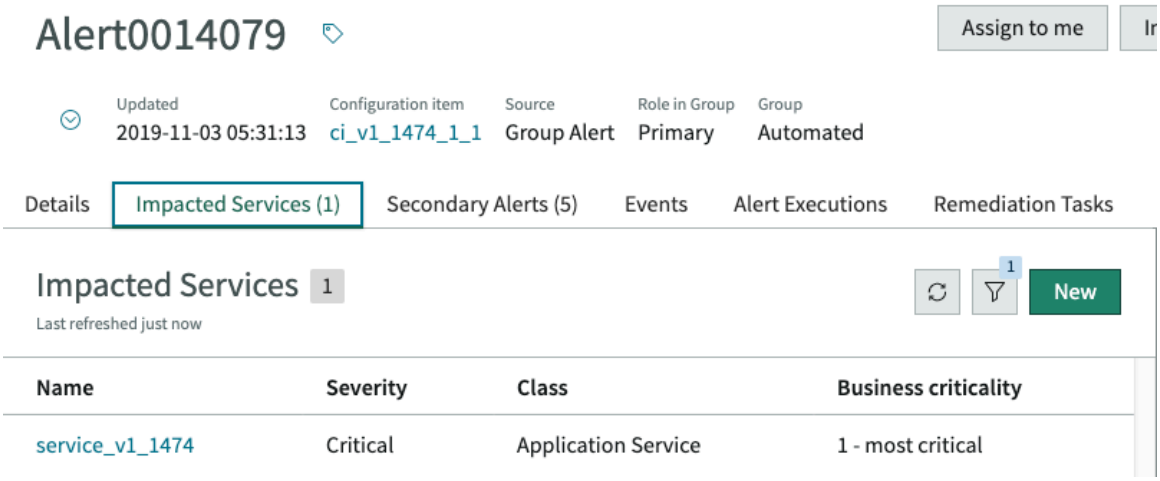


Automatische Übersetzung

4. Überprüfen Sie Informationen zu Anwendungsservices im **Betroffene Services** Registerkarte.

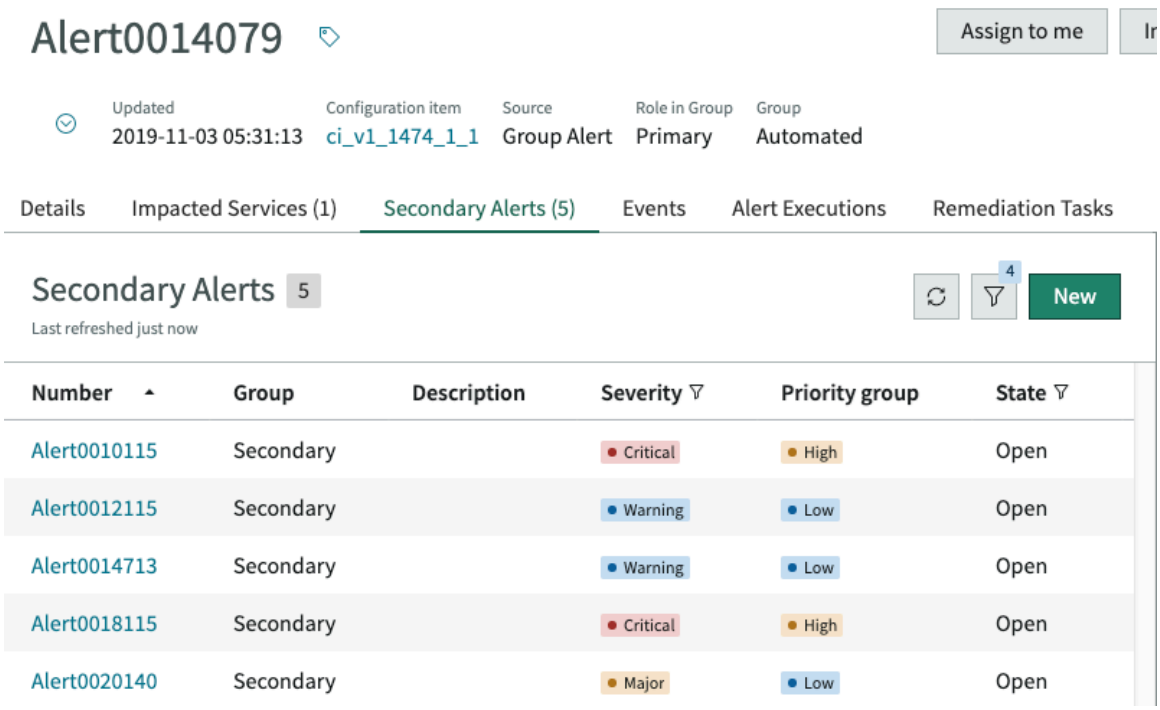
In diesem Beispiel wird service_1474 Anwendungsservice in der Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie weitere Informationen zu einem Anwendungsservice benötigen und die Servicezuordnung anzeigen möchten, klicken Sie auf den Servicenamen und dann auf **Servicezuordnung**.

5. Sehen Sie sich die zugehörigen Warnungen zu diesem Anwendungsservice an, und ändern Sie bei Bedarf die Korrelation.
   Der Prozess für eine primäre Warnung unterscheidet sich vom Prozess für eine sekundäre Warnung.
   - Bei einer primären Warnung werden alle sekundären Warnungen, die mit der primären Warnung korreliert sind, auf der Registerkarte **Sekundäre Warnungen** angezeigt.



Normalerweise müssen Sie nichts mit den sekundären Warnungen tun, es sei denn, Sie möchten weitere sekundäre Warnungen hinzufügen oder die Korrelation vollständig entfernen.

Hinweis: Wenn Sie eine primäre Warnung schließen, werden die sekundären Warnungen standardmäßig ebenfalls geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei sekundären Warnungen:

  Die Warnungsnummer der primären Warnung wird im Feld **Übergeordnet** angezeigt. Sie müssen nichts mit der übergeordneten Warnung tun, es sei denn, Sie möchten die sekundäre Warnung mit einer anderen primären Warnung neu korrelieren. Sie können auch die Korrelation vollständig entfernen, indem Sie das Feld löschen.

Hinweis: Wenn Sie eine sekundäre Warnung schließen, wird die primäre Warnung standardmäßig nicht geschlossen. Sie müssen daher die primäre Warnung separat schließen.

6. Wenn Sie sicher sind, dass das dem Event zugrunde liegende Problem und die entsprechende Warnung behoben wurden, klicken Sie auf **Schließen**.
   Wenn die Warnung Ihrer Meinung nach weitere Aufmerksamkeit erfordert, schließen Sie sie nicht. Versetzen Sie die Warnung stattdessen in den Status „Wartung“, indem Sie das Kontrollkästchen **Wartung** aktivieren.

Nächste Maßnahme

Sie haben das Ereignismanagement Operator-Tutorial abgeschlossen und dabei einen grundlegenden Workflow zum Analysieren, Selektieren und Schließen von Warnungen kennengelernt.

Nachdem Sie eine Warnung geschlossen haben, sind möglicherweise Aktionen für die folgenden Elemente erforderlich:

Warnungen erneut öffnen

Wenn eine Warnung Ihrer Meinung nach weitere Aktionen erfordert, können Sie ihren Status manuell in **Erneut öffnen** ändern. Wenn eine Warnung erneut geöffnet wird, werden zugeordnete Incidents gemäß ihrem Status und den vom Administrator festgelegten Regeln ggf. ebenfalls aktualisiert oder erneut geöffnet.

Hinweis: Jedes Mal, wenn Sie eine Warnung erneut öffnen, müssen Sie die Phasen „Selektierung“ und „Schließen“ erneut durchlaufen.

Warnungen im Status „Fluktuierend“ bearbeiten

In einigen Fällen kann dasselbe Event, das zur soeben geschlossenen Warnung geführt hat, in kurzer Zeit erneut ausgelöst werden, vielleicht sogar mehrmals. In diesem Fall wird der **Status** der soeben geschlossenen Warnung zunächst in **Erneut öffnen** und schließlich je nach vom Administrator konfigurierter Einstellung in **Flatternd** geändert.

Weitere Informationen dazu, wonach Sie suchen müssen, finden Sie unter Warnungen im Status „Fluktuierend“ bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Zusammenfassung anderer Aufgaben, die Sie vielleicht bei Gelegenheit ausführen müssen, finden Sie unter Erweiterte Aufgaben für Ereignismanagement Operatoren.

Erweiterte Aufgaben für Ereignismanagement Operatoren

Als Ereignismanagement Operator müssen Sie möglicherweise zusätzliche Aufgaben ausführen, die außerhalb Ihres typischen Workflows liegen. Manche Aufgaben müssen Sie ggf. auch nur einmal ausführen.

Erweiterte Aufgabe	Beschreibung
Warnungslistenansichten anpassen	Greifen Sie so schnell wie möglich auf die zu analysierenden Warnungen zu.
Mit fluktuierenden Warnungen arbeiten	Wenn sich eine Warnung im Status „Fluktuierend“ befindet, tritt das zugrunde liegende Problem weiterhin auf. Sie müssen die Warnung erneut selektieren und nach einer anderen Lösung suchen.
Warnungen bearbeiten, während sich CIs im Zustand „Wartung“ befinden	Lernen Sie, Warnungen für ein CI zu behandeln, das sich im Status „Wartung“ befindet, also gerade geändert wird.
Warnungsauswirkungen bei der Selektierung von Warnungen anpassen	Indem Sie die Auswirkungsregeln ändern, können Sie die Berechnung der Warnungsauswirkung und den Schweregrad der Warnung festlegen.

Warnungslistenansichten anpassen

Sie können eine oder mehrere benutzerdefinierte Warnungslistenansichten erstellen, um nur für Sie relevante Informationen anzuzeigen. Beispielsweise möchten Sie sich nur auf die Warnungen für Anwendungsservices an einem bestimmten Standort oder nur auf die Warnungen für Anwendungsservices mit hoher Relevanz konzentrieren.

Vorbereitungen

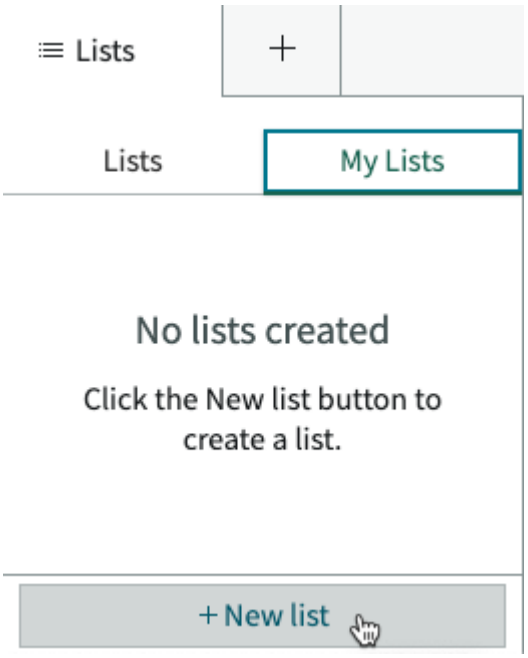
Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

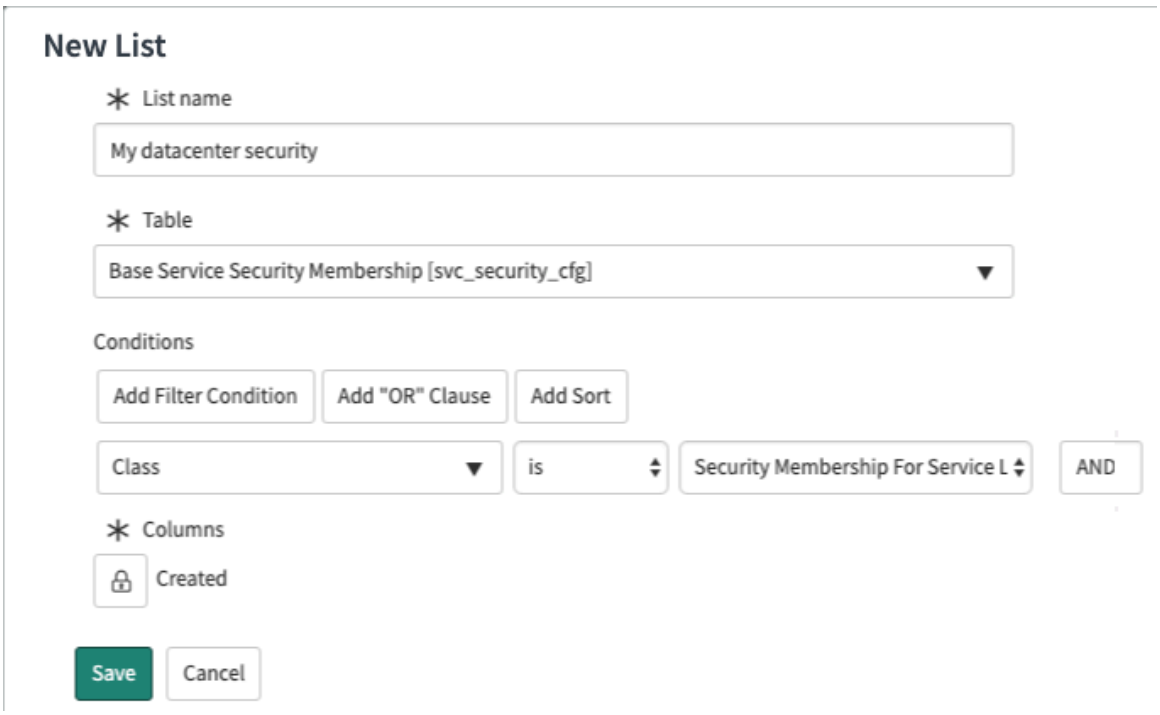
Prozedur

1. Navigieren zu **Ereignismanagement** > **Arbeitsbereich Des Operators**an.
2. Klicken Sie auf der Registerkarte **Listen** auf **Meine Listen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **+ Neue Liste**, füllen Sie das Formular mit Namen und Filterbedingungen aus und klicken Sie dann auf **Speichern**.



Die Liste wird auf der Registerkarte **Meine Listen** angezeigt.

Hinweis: Die Liste gilt nur für Anwendungsservices und nicht für AnwendungsserviceGruppen. Die Gruppen werden angezeigt, unabhängig davon, ob sie selbst oder dort enthaltene Services dem Filter entsprechen.

Mit fluktuierenden Warnungen arbeiten

Wenn sich eine Warnung im Status „Fluktuierend“ befindet, müssen Sie die Warnung möglicherweise erneut selektieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Event wiederholt in kurzer Zeit dieselbe Warnung auslöst, wird die Warnung in den Status „Fluktuierend“ versetzt, auch wenn sie zuvor von einem Operator geschlossen wurde. Das Event kann auch zwischen Schweregraden schwanken, z. B. „Info“ und „Kritisch“. Sie müssen die Warnung nun erneut selektieren und Aktionen ergreifen, um ein erneutes Auftreten des Events zu verhindern.

Hinweis: Ihr Ereignismanagement Administrator kann mit verschiedenen Einstellungen festlegen, wann eine Warnung als „Fluktuierend“ markiert wird und welche Aktionen Sie ergreifen können. In diesem Thema behandeln wir ein generisches Beispiel.

Prozedur

1. Warnungen im Status „Fluktuierend“ suchen:
   a. Navigieren zu **Ereignismanagement** > **Arbeitsbereich Des Operators**an.
   b. Ändern Sie die Liste der Warnungen, indem Sie auf das Filtersymbol ( ) klicken und Kriterien angeben, um fluktuierende Warnungen zu finden.
   Klicken Sie auf **Erweiterte Ansicht**, um die Filtereinstellungen zu ändern. Beispielsweise können Sie Folgendes angeben:

   `Status | ist | Flatternd.`

2. Klicken Sie auf die Warnungsnummer, um die Warnung zu öffnen.
3. Klicken Sie in der Warnung auf die Registerkarte **Flatternd**, und überprüfen Sie diese Informationen:

Feld	Beschreibung
Anzahl der Fluktuationen	Die Häufigkeit, mit der die Warnung seit dem Zeitpunkt im Feld **Startfenster der Fluktuation** zu fluktuieren begonnen hat.
Flattern – Startfenster	Die Zeit, zu der die Fluktuation begann.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Instanz, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.

4. Entscheiden Sie basierend auf der Fluktuationshäufigkeit, welche Aktion ausgeführt werden soll.
   Sie haben die folgenden Möglichkeiten, je nach den Standard Operating Procedures Ihrer Organisation und den Einstellungen des Ereignismanagement Administrators:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie einen Fehlerkorrektur-Workflow aus, um z. B. einen Server neu zu starten oder einen Router zurückzusetzen.
- Greifen Sie auf eine Webanwendung zu, z. B. auf die Anwendung für die Event-Überwachungssoftware in Ihrem Netzwerk.
- Ändern Sie einen zugehörigen Incident oder einen KB-Artikel, um zusätzliche Informationen oder Schritte hinzuzufügen.

5. Nachdem Sie das zugrunde liegende Problem sicher behoben haben, schließen Sie die Warnung.

Warnungen bearbeiten, während sich CIs im Zustand „Wartung“ befinden

Wenn eine Warnung für ein CI auftritt, das sich im Wartungsstatus befindet, wird der Warnstatus ebenfalls in „In Wartung“ geändert. Sie sollten den Status dieser Warnungen herausfinden und überwachen. Wenn die Änderungen am CI später abgeschlossen sind, beenden Sie die Selektierung der Warnung und schließen Sie diese.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Bevor Sie diese Aufgabe abschließen, machen Sie sich mit der grundlegenden Formularkonfiguration einer Instanz vertraut. Möglicherweise müssen Sie Felder und zugehörige Listen zu Formularen hinzufügen.

Im Beispiel in diesem Thema wird davon ausgegangen, dass ein Netzwerkadministrator eine Change-Anforderung geöffnet hat, um einen problematischen Webserver neu zu konfigurieren.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Warnungen im Status „Wartung“ suchen:
   a. Navigieren zu **Ereignismanagement** > **Arbeitsbereich Des Operators**an.
   b. Klicken Sie auf das Filtersymbol ( ), klicken Sie im Feld „Filter“ auf **Erweiterte Ansicht**, und geben Sie Folgendes an:

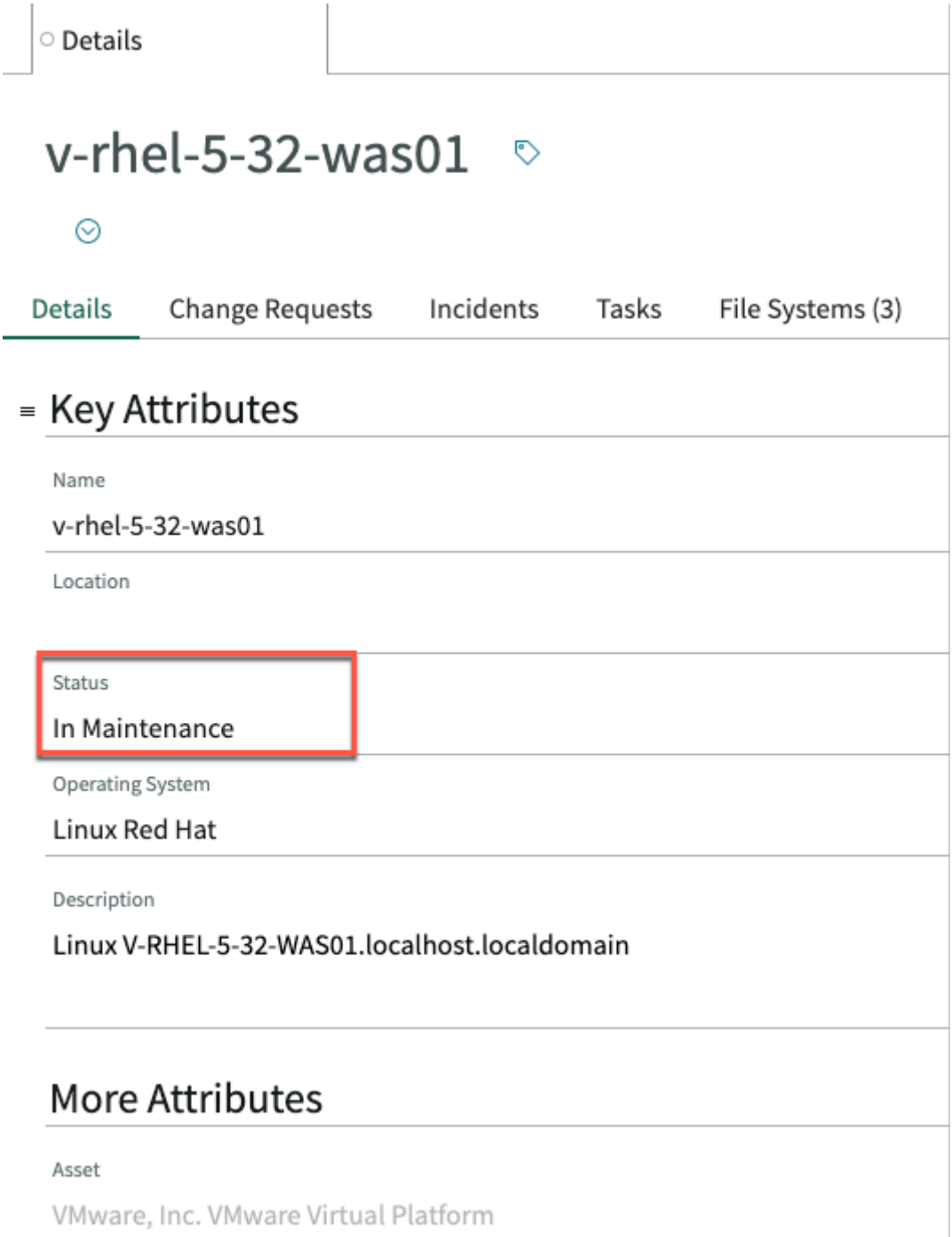
      `Status | ist | Wartung.`

2. Suchen Sie eine Warnung in der Liste, die über einen Wert in der Spalte **Konfigurationselement** verfügt. Dies ist das CI, in dem die Warnung aufgetreten ist.
3. Klicken Sie auf den CI-Namen, um das Formular mit Informationen zum CI zu öffnen.

   In diesem Beispiel ist der Status des Webservers **In Wartung** und eine Change-Anforderung wurde geplant, sodass jemand den Server neu konfigurieren kann.
4. Klicken Sie auf den CI-Namen, um das Formular mit Informationen zum CI zu öffnen.

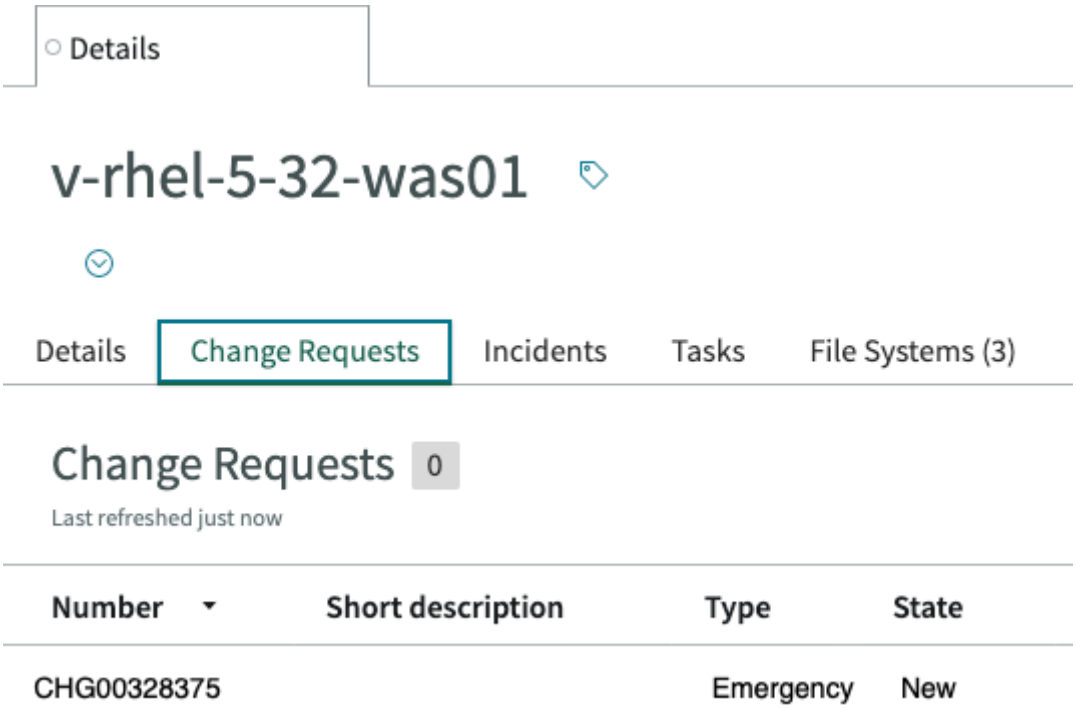
   In diesem Beispiel hat der Server (auf der Registerkarte **Details**) den Status **In Wartung**. Sie können die geplante Change-Anforderung auf der Registerkarte **Change-Anforderungen** anzeigen (jemand konfiguriert das CI neu).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Zu diesem Zeitpunkt sollten Sie die diesem CI zugeordnete Warnung nicht ändern.
   Sie können die Change-Anforderung öffnen, um angehängte Zeitpläne anzuzeigen, oder Sie stimmen sich mit Ihrem Team ab, um herauszufinden, wann das CI nicht mehr „In Wartung“ ist.
6. Verifizieren Sie zunächst, dass das Feld **Status** im CI nicht den Wert **In Wartung** hat. Öffnen Sie dann die Warnung erneut, und deaktivieren Sie das Kontrollkästchen **Wartung**.
7. Fahren Sie mit der Selektierung der Warnung fort.

Warnungsauswirkungen bei der Selektierung von Warnungen anpassen

Als Ereignismanagement Operator müssen Sie möglicherweise die Auswirkungen einer Warnung auf einen Anwendungsservice und auf die CIs in einem Service ändern. Tun Sie dies, wenn Sie der Meinung sind, dass die Auswirkung nicht genau mit Ihrer Netzwerkumgebung übereinstimmt. So können andere Operatoren und Administratoren die richtigen Auswirkungsinformationen sehen.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Änderungen an Auswirkungsberechnungen vornehmen, stellen Sie sicher, dass Sie verstehen, wie die Anwendungsservices und die CIs tatsächlich funktionieren. Möglicherweise müssen Sie dazu die Netzwerkinfrastruktur testen, oder sich an jemanden wenden, der dies für Sie tun kann.

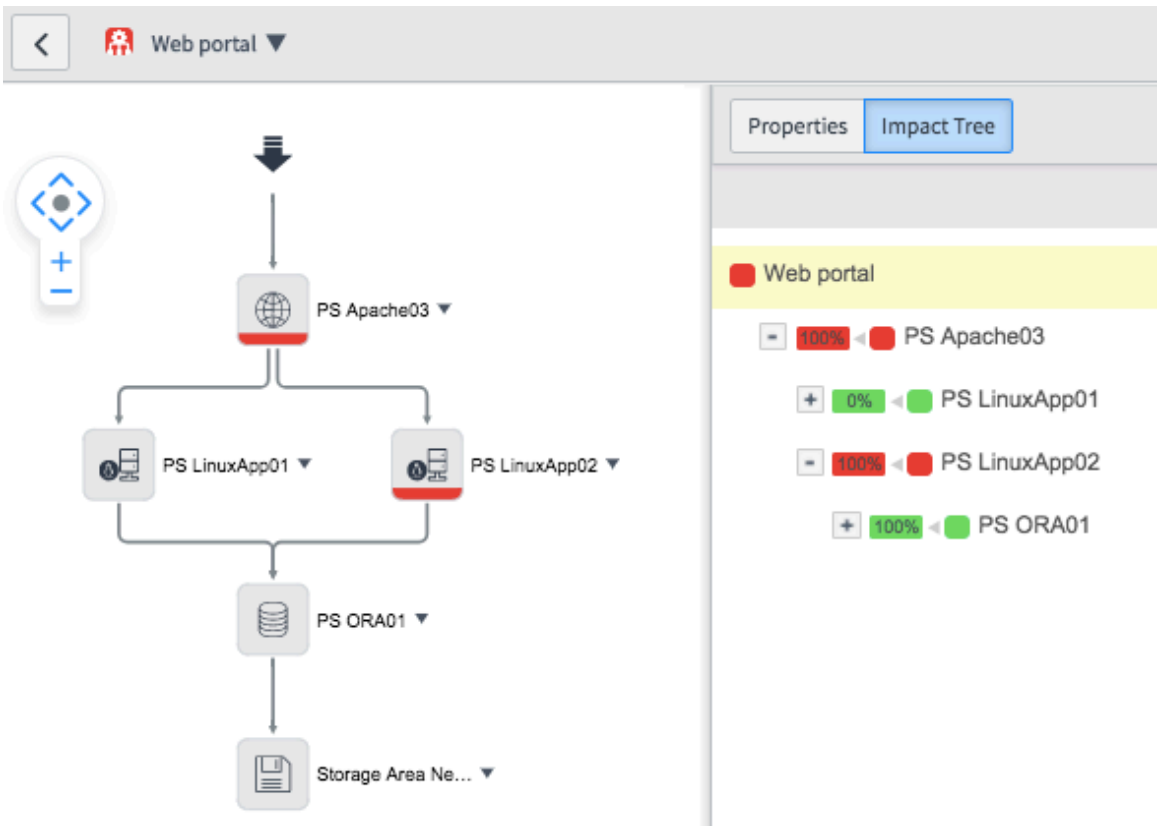
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Arbeitsbereich Des Operators**an.
2. Doppelklicken Sie auf den Namen des AnwendungsserviceMit den Warnungen, die Sie ändern möchten.
3. Klicken Sie auf der Registerkarte Details auf **Servicezuordnung** .
4. Auf der **Servicezuordnung** Klicken Sie auf die Registerkarte **Vollständige Zuordnung** Struktur.
5. Klicken Sie in der Zuordnung auf **Auswirkungsstruktur**.
6. Analysieren Sie den Anwendungsservice, und ermitteln Sie basierend auf Ihren Informationen über die beteiligten CIs, ob die Auswirkungsstruktur die Auswirkung der Warnungen genau widerspiegelt.

   In diesem Beispiel deutet eine kritische Warnung auf ein schwerwiegendes Problem mit einem Linux-Server hin, der Teil von einem Webportal Anwendungsservice ist.



   Beachten Sie, dass die Auswirkung auf das Webportal selbst in roter Farbe dargestellt ist, da es sich um eine kritische Auswirkung handelt – obwohl nur einer der Linux-Server, auf die sich das Portal verlässt, tatsächlich eine kritische Warnung hat. Der andere Linux-Server ist von der Warnung nicht betroffen. Nehmen Sie für dieses Beispiel an, dass die Linux-Server unterschiedliche Rollen für den Webservice ausführen, und dass **PS LinuxApp02** zwar eine kritische Warnung hat, der Server **PS LinuxApp01** Server jedoch alle erforderlichen Services bereitstellen kann, um den Anwendungsservice betriebsbereit zu halten.

7. Klicken Sie auf das CI **PS Apache03**, und klicken Sie dann auf **Auswirkung**, um die Auswirkungsregeln für das CI anzuzeigen.
   Standardmäßig wird die CI-Auswirkungsregel mit folgenden Informationen angezeigt:

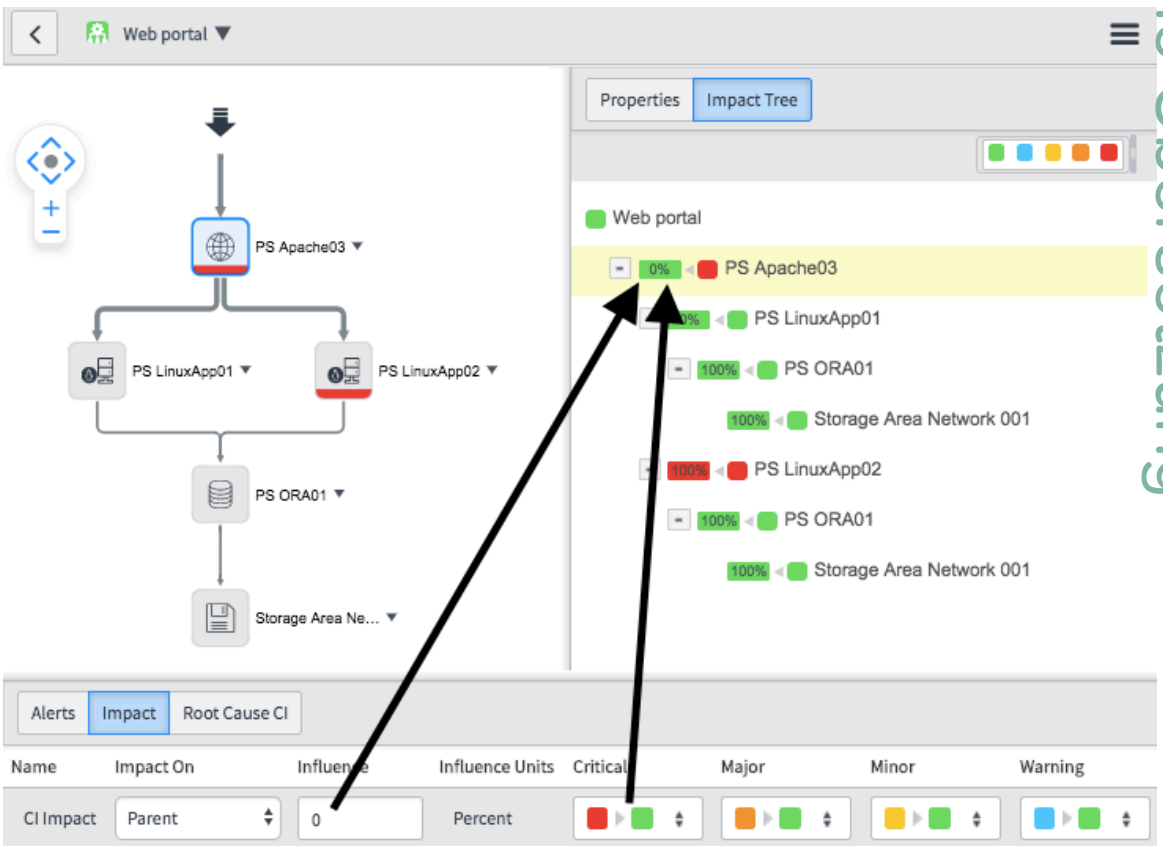
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Spalten **Auswirkung auf** und **Einfluss** zeigen an, dass das CI (**PS Apache03**) 100 % der Auswirkung aller untergeordneten CI-Auswirkungen erbt, was in diesem Fall die kritischen Auswirkungen auf den Server **PS LinuxApp02** umfasst. Diese Einstellung ist der Grund, warum der Webserver **PS Apache03** und der Anwendungsservice als Ganzes die Auswirkung zu 100 % erben.
- Die Spalte **Kritisch** zeigt an, dass eine kritische Warnung (rot) als kritische Warnung (rot) geerbt wird.

8. Ändern Sie den Wert **Einfluss** auf 0, da der Webserver noch betriebsbereit ist. Ändern Sie dann die Spalte **Kritisch**, um anzugeben, dass ein kritischer Auswirkungsstatus (rot) als „Nicht-Auswirkung“ (grün) geerbt werden soll.
9. Warten Sie, bis das Dashboard automatisch aktualisiert wird, oder klicken Sie auf **Ereignismanagement** > **Service Operations-Arbeitsbereich** Und doppelklicken Sie darauf AnwendungsserviceUm eine Aktualisierung zu erhalten AnwendungsserviceZuordnung.

   Beachten Sie, dass der Einfluss auf den Apache-Webserver 0 % beträgt und der Auswirkungsstatus grün ist. Beachten Sie auch, dass der kritische Warnungsstatus (rot) unverändert bleibt, obwohl die Auswirkung zu grün geändert wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Navigieren Sie zurück zum Dashboard „Service Operations Workspace“.
    Beachten Sie, dass Anwendungsservice jetzt grün ist, was darauf hinweist, dass der gesamte Anwendungsservice betriebsbereit ist. Die kritische Warnung wird weiterhin unten in der Warnungsliste angezeigt und gibt an, dass noch ein Problem besteht, das Sie oder andere Operatoren beheben können.

Nächste Maßnahme

Unter Umständen konfiguriert Ihr Administrator zusätzliche Auswirkungsregeln, die angezeigt werden, wenn Sie in der Anwendungsservice-Zuordnung auf ein CI klicken. Sie können Anpassungen an den **Einflussfeldern** jeder Auswirkungsregel vornehmen, um die genaueste Auswirkungsstruktur zu erhalten.

Ereignismanagement-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Ereignismanagement-Listen und -Formularen.

Mit Ereignismanagement installierte Komponenten

Durch die Aktivierung des Plugins Ereignismanagement (com.glideapp.itom.snac) werden mehrere Rollen, Scheduled Jobs und Tabellen hinzugefügt.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Mit Ereignismanagement installierte Rollen

Von der Anwendung Ereignismanagement verwendete Rollen.

Ereignismanagement fügt diese Rollen hinzu.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Ereignismanagement Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.	• evt_mgmt_user • template_editor_global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Seien Sie mit der Rolle „evt_mgmt_admin“ vorsichtig, da sie auf die Administratorrolle hochgestuft werden kann. Ein Anwender mit der Rolle „evt_mgmt_admin“ kann Skripts hinzufügen und ändern, die in einem globalen Bereich ausgeführt werden. Stellen Sie eine ordnungsgemäße Zugriffssteuerung sicher. Mit dieser Rolle kann der Anwender die folgenden Skripts erstellen und/oder aktualisieren: • Regeln zur Warnungskorrelation • Warnungsverwaltungsregeln • Wartungsregeln • Erweiterte Skripts • Ereignisfeldzuordnung • Skripts vor und nach der Bindung	
Ereignismanagement Operator [evt_mgmt_operator]	Neben den evt_mgmt_user-Berechtigungen können auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktiviert werden.	evt_mgmt_user
Ereignismanagement Benutzer [evt_mgmt_user]	Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat die Rolle, um Vorfälle verwalten zu können, die aus Alerts erstellt werden.	itil
Ereignismanagement-Integrator [evt_mgmt_integration]	Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie mit externen Ereignisquellen zu integrieren.	

Mit Ereignismanagement installierte geplante Aufgaben

Liste der Scheduled Jobs, die mit Ereignismanagement bereitgestellt werden.

Um die Liste der geplanten Aufgaben zu überprüfen, navigieren Sie zu **Systemzeitplaner** > **Geplante Aufgaben**. Ereignismanagement Fügt die folgenden geplanten Aufgaben hinzu.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Connector-Ausführungsjob	Vergleicht die aktuelle Zeit mit der Zeit der letzten Ausführung von aktiven Connector-Instanzen und legt relevante Connectors zur Ausführung fest. Wird alle 10 Sekunden ausgeführt.
Ereignismanagement – Auswirkungen von abgebrochenen Services behandeln	Löst abgebrochene Services und markiert sie in der Tabelle „Auswirkungsänderungen“ als neu zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
	erstellende Services, um die Auswirkungsstruktur neu zu erstellen. Wird alle 2 Minuten und 31 Sekunden ausgeführt.
Ereignismanagement – Auswirkungsrechner auslösen	Löst die Auswirkungsberechnung aus. Das Dashboard Ereignismanagement und die Auswirkungsstruktur werden anhand der berechneten Zahlen aktualisiert. Wird alle 6 Sekunden ausgeführt.
Ereignismanagement – Auswirkungstopologie-Verbraucher	Verbraucht Topologieänderungen und markiert die zugehörigen Services in der Tabelle „Auswirkungsänderungen“ als „Neuerstellung erforderlich“, um ihre Auswirkungsstruktur neu zu erstellen. Wird alle 19 Sekunden ausgeführt.
Ereignismanagement – Connectors für abgebrochene Updates	Löst Connector-Instanzen, die abgebrochen werden. Wird alle 2 Minuten ausgeführt.
Ereignismanagement – Warteschlange für Warnungspriorität	Berechnet die Warnungspriorität. Zwei Jobs für Warteschlange für Warnungspriorität sind aktiv und verfügbar und können mit Multi-Thread ausgeführt werden. Wird jede Minute ausgeführt.
Ereignismanagement – Warnungen für automatisches Schließen	Warnungen, die länger als 7 Tage inaktiv sind (Standardzeitraum), werden geschlossen. Ändern Sie den Standardwert mit der Eigenschaft `evt_mgmt.alert_auto_close_interval`. Wird alle 10 Minuten ausgeführt.
Ereignismanagement – Warnungsprioritätsgruppen berechnen	Führt die Prioritätsgruppen aus und berechnet sie: dringend, hoch, mittel und niedrig für die Warnungen gemäß der höchsten und niedrigsten Priorität im System. Wird alle 30 Minuten ausgeführt.
Ereignismanagement – Fluktuierende Warnungen schließen	Schließt fluktuierende Warnungen. Wird alle 5 Minuten ausgeführt.
Ereignismanagement – Schwellenwertwarnung schließen	Schließt Schwellenwertwarnungen. Wird alle 2 Minuten ausgeführt.
Ereignismanagement – Bereichsbezogene Warnungsregelverwaltung0 Auswerten	Führt Warnungsverwaltungsregeln aus. Zwei separate Aufträge werden ausgeführt, um das System zu entlasten.
Ereignismanagement – Bereichsbezogene Warnungsregelverwaltung1 Auswerten	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
	Wird alle 11 Sekunden ausgeführt.
Ereignismanagement – Services nach Impact filtern – Warteschlangen-Handler	Verarbeiten Sie Änderungen aus em_Impact_Inclusion_class und em_Impact_Filter_Service. Wird jede Minute ausgeführt.
Ereignismanagement – Auswirkungsstrukturgenerator	Verarbeitet alle Services mit Änderungen aus der Tabelle „em_impact_changes“ und erstellt ihre Auswirkungsstruktur neu. Wird alle 11 Sekunden ausgeführt.
Ereignismanagement – Systemüberwachung einfügen	Auftrag zum Erstellen von **ServiceNow-Ereignismanagement** Anwendungsservices. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – Wartungsrechner	Berechnet die Wartung für CIs. Wird jede Minute ausgeführt.
Ereignismanagement – Knotenanzahl	Berechnet die Lizenznutzung. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – Tabelle „Betroffene Services“ Ausfüllen	Scannen Sie cmdb_ci_Service_Auto, und kopieren Sie alle Services zusammen mit allen zugehörigen Klassen in „em_Impact_Inclusion_class“. Wird einmal nach dem Upgrade ausgeführt.
Ereignismanagement – Events verarbeiten	Job, der jedes Bereit-Event ausführt und verarbeitet (Event-Regel anwenden, Zuordnungsregel anwenden und Warnung erstellen oder aktualisieren) Wird alle 5 Sekunden ausgeführt.
Ereignismanagement – Metrikbindung verarbeiten	Verarbeitet Metrikbindungen. Wird alle 5 Sekunden ausgeführt.
Ereignismanagement — Prozessdatensätze in em_extra_data_json	Erstellt Events für Protokollanalyseanomalien. Wird alle 13 Sekunden ausgeführt.
Ereignismanagement – Connector-Prozessor der Warteschlange	Bidirektionale Funktionalität. Verarbeitet alle ausstehenden Warnungen in der Update-Warteschlange und sendet sie an den MID-Server. Standardmäßig wird dieser Prozess aus der Warteschlange in Batches von 1.000 Warnungen ausgeführt. Wird alle 30 Sekunden ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Auswirkung für Gruppen neu berechnen	Dieser Job ist standardmäßig nicht aktiv. Kann bei Bedarf ausgeführt werden, um die Auswirkungen auf Servicegruppen zu korrigieren. Wird bei Bedarf ausgeführt.
Ereignismanagement – Abgebrochene Events wiederherstellen	Verarbeitet alle Events, die sich in der Warteschlange befinden, und stellt sie zurück auf den Status „Bereit“, um Events vom Anfang an zu verarbeiten. Wird beim Systemstart ausgeführt.
Ereignismanagement – Systemüberwachung aktualisieren	Aktualisieren Sie **ServiceNow-Ereignismanagement** Anwendungsservices. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – SLA-Konfigurationsergebnis aktualisieren	Synchronisiert die CIs, die dem SLA-Konfigurationsfilter entsprechen, mit der Tabelle Ereignismanagement-SLA [em_ci_severity_task]. Wird alle 10 Minuten ausgeführt.
Ereignismanagement – SLA-Schweregrad aktualisieren	Aktualisiert die Tabelle Ereignismanagement-SLA [em_ci_severity_task] mit dem neuen Schweregrad. Wird einmal pro Minute ausgeführt.
Ereignismanagement – IT-Service konvertieren	Führen Sie diese Eigenschaft bei Bedarf aus, um manuelle Services in Anwendungsservices zu konvertieren. Wird alle 30 Minuten ausgeführt.
Ereignismanagement – xmlstats erfassen	Erfasst Event-Verarbeitungsstatistiken. Wird einmal pro Minute ausgeführt.
Ereignismanagement – Auswirkungsrechner für Warnungsgruppen und SLA	Berechnet die Auswirkung von Warnungen auf Warnungsgruppen-Services.
Ereignismanagement – Manueller Auswirkungsrechner-Auslöser	Manueller Auslöser der Auswirkungsberechnung für alle operativen Services.
4x Ereignismanagement– Auswirkungsrechner für BS_0	Berechnet die Auswirkung von Warnungen auf Anwendungsservices und erstellt die Auswirkungsstruktur im Dashboard Ereignismanagement. Vier separate Jobs werden ausgeführt, um das System zu entlasten.
4x Ereignismanagement– Auswirkungsrechner für BS_1	
4x Ereignismanagement– Auswirkungsrechner für BS_2	
4x Ereignismanagement– Auswirkungsrechner für BS_3	
Ereignismanagement – Tabelle mit Auffüllungswarnungen	Sucht redundante Datensätze in der Tabelle „em_Alert_history“ und bricht sie ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Auswirkungsstatustabelle für Auffüllung	Sucht redundante Datensätze in der Tabelle „em_Impact_Status“ und bricht sie ab.
Ereignismanagement – Auswirkung für Gruppen	Berechnet die Auswirkung von Warnungen auf Servicegruppen.
Ereignismanagement – Tabelle mit Warnungsverlauf bereinigen	Bereinigt die Tabelle mit dem Warnungsverlauf (em_alert_history), indem Datensätze entfernt werden, die älter als 90 Tage sind. Sie können die Zeitspanne anpassen, nach der Warnungen entfernt werden, indem Sie *evt_mgmt.impact_calculation.cleanup_age_seconds.e* in der Tabelle sys_properties.list konfigurieren.
Ereignismanagement – Tabelle mit Auswirkungsstatus bereinigen	Bereinigt die Tabelle mit dem Auswirkungsstatus (em_impact_status), indem Datensätze entfernt werden, die älter als 90 Tage sind. Sie können die Zeitspanne anpassen, nach der Warnungen entfernt werden, indem Sie *evt_mgmt.impact_calculation.cleanup_age_seconds.e* in der Tabelle sys_properties.list konfigurieren.

Ereignismanagement fügt die folgenden Scheduled Jobs hinzu, um die Warnungszusammenfassung und RCA zu unterstützen.

Name	Beschreibung
Serviceanalytik löscht alte Beobachtungsdaten – Täglich	Bereinigt die bereitgestellten Daten.
Service Analytics – RCA-Lernereingabedaten vorbereiten – täglich	Bereitet RCA-Eingabedaten vor. Speichert und prüft MID-Server, um statistische Informationen zu Warnungen zu erfassen
Serviceanalytik-Gruppenwarnungen mithilfe von RCA/ Warnungszusammenfassung	Wendet RCA und Warnungszusammenfassung auf offene Warnungen an und bereitet automatisierte Warnungsgruppen vor.
Serviceanalytik Warnungszusammenfassungs-Learner – Täglich	Lernt Informationen zu vorhandenen Warnungen kennen und gruppiert neue offene Warnungen.
Serviceanalytik-RCA-Konfiguration	Konfiguriert die Ursachenanalyse.
Service Analytics – Dateisystemspeicherplatz in Analytics MID überprüfen – täglich	Überprüft die Datenträgernutzung auf dem dedizierten MID-Server, Und generiert ein Ereignis, wenn der in festgelegte Schwellenwert überschritten wird *sa_analytics.rca.mid_max_allowed_space*Eigenschaft.
Serviceanalytik sammelt Berichtsdaten – Täglich	Sammelt Daten für den Wertbericht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Serviceanalytik – Virtuelle Warnungen für Zusammenfassungsgruppen aktualisieren	Aktualisiert die virtuellen Warnungen, die erstellt wurden, um Warnungszusammenfassungsgruppen darzustellen, mit allen Änderungen an Warnungen, die zu dieser Gruppe gehören. Wird jede Minute ausgeführt.
Serviceanalytik Attributausfüllung für historische Warnungen	Füllt Attribute aus, die im Feature-Bezeichner für historische Warnungsdaten mittels Event-Regeln verwendet werden. Wird bei Bedarf ausgeführt.
Ereignismanagement – Analytics-Warnungssynchronisierung	Sammelt Warnungsdaten, die vom Gruppierungsauftrag verwendet werden.

Eigenschaften zum Personalisieren der Domänentrennung für Ereignismanagement Connectors

Eigenschaften stellen die Metadaten zur Identifizierung der Domäne bereit.

Sie können die Werte ändern, wenn Sie andere Tabellen oder Felder für die Domänenidentifizierung verwenden möchten, stellen Sie jedoch sicher, dass die Tabelle domänengetrennt ist.

Hinweis: Beim Personalisieren der Domänentrennung für Ereignismanagement-Connectors können alle Eigenschaften auch auf Connector-Ebene überschrieben werden.

Für die Personalisierung der Domänentrennung werden drei Caches verwaltet (Main, user_Access, missing_Domain). Sie können einige Systemeigenschaften erstellen, um sie zu steuern.

Standardsystemeigenschaften

Eigenschaft	Beschreibung
evt_mgmt. Connector_Domain_info_table_Name	Die Tabelle, in der Sie Domäneninformationen zum Personalisieren der Domänentrennung speichern. • **Typ**: Zeichenfolge • **Standardwert** : Core_Company
evt_mgmt. Connector_Domain_info_column_Name	Der Feldname in der Tabelle zur Identifizierung der angegebenen Domäne für die Personalisierung der Domänentrennung. • **Typ**: Zeichenfolge • **Standardwert** : Name
evt_mgmt. Connector_Domain_ID_column_Name	Das Feld, aus dem die Domänen-ID zum Personalisieren der Domänentrennung abgerufen werden soll. • **Typ**: Zeichenfolge • **Standardwert** : Sys_Domain

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardsystemeigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
evt_mgmt. Connector_Domain_path_column_Name	Das Feld, aus dem der Domänenpfad zum Personalisieren der Domänentrennung abgerufen werden soll. • **Typ**: Zeichenfolge • **Standardwert** : Sys_Domain_path

Eigenschaft	Beschreibung
evt_mgmt.Connector_custom_Domain_sep_Cache_expire_in_seconds	Zum Personalisieren der Domänentrennung, wenn Ihr Haupt-Cache nicht jede Woche abläuft.
evt_mgmt.Connector_custom_Domain_sep_user_Access_on_Domain_Cache_size	Zum Personalisieren der Domänentrennung, wenn Sie die Größe des Anwenderzugriffs-Caches erhöhen möchten.
evt_mgmt.Connector_custom_Domain_sep_missing_Domain_Cache_expire_in_seconds	Zum Personalisieren der Domänentrennung, wenn Sie die Ablaufzeit für die Cache-Speicherung von Informationen zur fehlenden Domäne erhöhen möchten.
evt_mgmt.Connector_custom_Domain_sep_Cache_size	Zum Personalisieren der Domänentrennung, wenn Sie eine größere Haupt-Cache-Größe zum Speichern von Domäneninformationen benötigen.

Automatische Übersetzung

Mit Ereignismanagement installierte Tabellen

Tabellen, die bereitgestellt werden, wenn Ereignismanagement aktiviert ist.

Ereignismanagement fügt diese Tabellen hinzu.

Tabelle	Beschreibung
Warnung [em_alert]	Warnungen, die Ereignismanagement verwaltet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Warnungskorrelationsregel [em_alert_correlation_rule]	Regeln, die primäre und sekundäre korrelierte Warnungen angeben.
Gruppenwarnungen für Warnungszusammenfassung [em_agg_group_alert]	Speichert Warnungen, die zusammengefassten Warnungsgruppen zugeordnet sind.
Gruppe für Warnungszusammenfassung [em_agg_group]	Beziehungen zwischen zusammengefassten Gruppen und primären Warnungen.
Warnungsverlauf [em_alert_history]	Verlauf von Warnungen. Wird für Auswirkungsberechnungen verwendet.
Warnungsregel [em_alert_rule]	Zuordnungen von Warnungsfeldern zur Incident-Tabelle [Incident].
Warnvorlage [em_alert_template]	Warnungsvorlagen. Diese Tabelle erweitert die Vorlagentabelle [sys_template].
Ereignismanagement SLA [em_ci_severity_task]	Ereignismanagement-SLA-Aufgaben für CIs und Services.
Connector-Definition [em_connector_definition]	Einstellungen zum Erheben von Events aus externen Event-Quellen.
Anschlussinstanz [em_connector_instance]	Connector-Details für externe Event-Quellen.
MID-Server zu Connector-Instanz [em_connector_instance_to_mid]	Zuordnungen von MID Servers zu Connector-Instanzen
Ereignismanagement-Lizenznutzung [em_unique_nodes]	Wenn Ereignisse von ITOM-Integrität empfangen werden, wird ein Eintrag in dieser Tabelle basierend auf dem in der empfangenen Nachricht angegebenen überwachten Ziel hinzugefügt oder aktualisiert. Der Eintrag ist mit dem entsprechenden CI in der CMDB verknüpft. Wenn kein CI gefunden wird, wird dem Eintrag das Attribut *Type = Unknown* zugewiesen.
Event [em_event]	Events, die von Ereignismanagement empfangen wurden.
Event-Filter [em_event_filter]	Speicher für definierte Event-Filter.
Event-Abgleichregel	Aktualisierte Events für die Warnungsverarbeitung. Wird von Event-Regeln verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[em_match_rule]	
Feld zur Ereignisabstimmung [em_match_field]	Zuordnungen von Event-Feldern zu Warnungsfeldern. Einfache Zuordnung. Wird von Event-Regeln verwendet.
Feld zur Ereigniserstellung [em_compose_field]	Zuordnungen von Event-Feldern zu Warnungsfeldern. Zusammengesetzte Zuordnung. Wird von Event-Regeln verwendet.
Event-Zuordnungsregeln [em_mapping_rule]	Aktualisierte Event-Felder für die Warnungsverarbeitung.
Ereignisverarbeitungsstatistiken [em_event_stats]	Statistiken zur Leistung von Ereignismanagement.
Ereignistyp [em_event_type]	Event-Typen.
Aufgabenvorlage [em_incident_template]	Vorlagen, die definieren, wie neue Aufgaben ausgefüllt werden. Beispielsweise müssen Felder eines Incidents, der aus einer Warnung erstellt wird, ausgefüllt werden. Diese Tabelle erweitert die Vorlagentabelle [sys_template].
Registrierte Knoten [em_registered_nodes]	Registriert Knotendaten.
Schwellenwertregel [em_threshold_rule]	Warnung für Schwellenwertregeln.
Gerätezuordnung verbinden [Em_binding_device_map]	Event-Bindung an Netzwerk- und Speicherpfade.
Prozess für CI-Typ-Zuordnungen [Em_binding_process_map]	Event-Bindung an bestimmte Prozesse.
CI-Fehlerkorrektur [em_ci_remediation]	Regeldefinitionen für Fehlerkorrektur.
Auswirkungsgrafik [em_impact_graph]	Auswirkungsstruktur von CIs, die eine CI-Hierarchie und Auswirkungsregeln für die Auswirkungsberechnung enthalten.
Auswirkungsgrafik-Verläufe [em_impact_graph_history]	Verlauf der Änderungen in der Auswirkungsstruktur.
Auswirkungsregeldefinitionen	Definition der Regeln für die Auswirkungsberechnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[em_impact_rule_definition]	
Auswirkungsregelinstanz [em_impact_rule]	Regeln basierend auf Auswirkungsregeldefinitionen.
Impact-Inklusionsklassen [Em_Impact_Inclusion_class]	Gibt die Klassen an, die für die Auswirkungsberechnung verwendet werden sollen.
Impact-Filterservices [Em_Impact_Filter_Service]	Gibt Services an, die von der Auswirkungsberechnung eingeschlossen oder ausgeschlossen werden sollen.
Infrastrukturbeziehungen [em_impact_infra_rel_def]	Unter-/übergeordnete Paare oder CI-Typen. CIs, die diesen Definitionen entsprechen, werden den Auswirkungsstrukturen hinzugefügt.
Auswirkungswartungs-CIs [em_impact_maint_ci]	CIs, die sich in der Wartung befinden und daher von der Auswirkungsberechnung ausgeschlossen sind.
Auswirkungsstatus [em_impact_status]	Berechneter Status von CIs und Services, die im Dashboard und in Service Mapping für dynamische CI-Gruppen angezeigt werden sollen.
SLA-Konfiguration [em_sla_configuration]	SLA-Konfigurationsdatensätze, die die CIs identifizieren, auf denen SLAs ausgeführt werden können.
Serviceanalytik Metriktypregistrierung [sa_metric_registration]	Quellregistrierungsdetails für die Verarbeitung von Rohdaten.
Systemüberwachungsskripts [em_monitor_scripts]	Diese Skripts bestimmen, wie beispielsweise bei Verwendung des Connectors-Überwachungsskripts Überwachungen oder Überprüfungen durchgeführt werden. Sie können ein benutzerdefiniertes Skript zur Überwachung eines Geräts oder einer Entität erstellen. Die mit der Basisinstanz bereitgestellten Skripts sind: • Verzögerung bei der Event-Verarbeitung überprüfen • Connector-Überwachung • Status der Event-Verarbeitung abrufen • MID-Server-Schwellenwertwarnungen
Überwachungskonfiguration [em_monitor_conf]	Verwenden Sie diese Tabelle, um zu konfigurieren, was entsprechend den aufgeführten Skripts überwacht werden soll. Konfigurieren Sie, wie oft jedes Skript ausgeführt werden soll. Wenn ein Skript über einen Schwellenwert verfügt, wird bestimmt, welcher Warnungsschweregrad angezeigt werden soll. Schwellenwerte werden in Minuteneinheiten angegeben und geben die Verzögerungszeit an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration** Um die Liste der Überwachungskonfigurationen anzuzeigen oder eine neue zu erstellen. Verwenden Sie dieses Skript, um die Überwachung des Rechenzentrums zu testen. Die mit der Basisinstanz bereitgestellten Skripts sind: • Überwachung Connectors im Ruhezustand – Überwachung, um zu überprüfen, ob sich einer der Connectors im Ruhezustand befand und den konfigurierten Schwellenwert [in Minuten] überschritten hat. • Connector-Status – Überwachung zur Nachverfolgung des aktiven Status der Connectors. • Verzögerung bei der Event-Verarbeitung – Überwachung der Dauer [in Minuten] von Events, die im Status „Bereit“ blieben und nicht verarbeitet wurden. • Event-Verarbeitungsjob – Überwachung des Status der Event-Verarbeitungsaufgaben. • MID-Server-Schwellenwertwarnung – Überwacht der Integrität des MID-Server
Event Management-Aufgaben überwachen [em_monitor_jobs_state]	Überwachen Sie Ereignismanagement-Aufgaben, indem Sie dieser Tabelle die entsprechenden Aufgaben hinzufügen. **Hinweis:** Die folgenden Aufgaben werden von dieser Tabelle nicht überwacht: • Ereignismanagement – Events verarbeiten • Ereignismanagement – Auswirkungsstrukturgenerator • Ereignismanagement – Abgebrochene Events wiederherstellen • Event-Verarbeitung
Überwachungsstatus [em_monitor_state]	Verwenden Sie diese Tabelle, um den Schwellenwert für jeden Connector festzulegen. Wenn ein Wert über einem Schwellenwert liegt, wird eine Warnung generiert.
EM-XMLStats-Daten [em_xmlstats_data]	Selbstintegritätsstatistiken und Diagnosedetails für Metrikdaten und Ereignismanagement, die zur Erstellung der XMLStats-Seite verwendet werden.

Ereignismanagement fügt die folgenden Tabellen hinzu, um die Warnungszusammenfassung und RCA zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
SA-RCA-Status [sa_rca_status]	Informationen (z. B. IDs) für die neuesten Nachrichten, die während der RCA für einen Service an die ECC-Warteschlange gesendet wurden.
SA-RCA-Ausgabe [sa_rca_output]	Ausgabedaten RCA-Learner.
SA-RCA-Gruppe [sa_rca_group]	Automatisierte Warnungsgruppen für die RCA-Abfrage.
Staging des SA-Analysealarms [sa_analytics_alert]	Bereitstellungstabelle für Warnungen, die für Analysen verwendet werden.
SA-RCA-Eingabe [sa_rca_input]	Eingabe von Daten für den RCA-Learner.
SA-Analysestatus [sa_analytics_status]	Informationen der letzten Ausführung, die für die Warnungszusammenfassung und RCA verwendet werden sollen.
SA-RCA-Gruppenwarnung [sa_rca_group_alert]	Warnungen, die automatisierten Warnungsgruppen zugeordnet sind.
Verknüpfung des SA-RCA-Service-Configuration Items [sa_rca_svc_ci_assoc]	Zuordnungen zwischen CIs und Services.
SA-Warnungszusammenfassung – Erlerntes Muster [sa_agg_pattern]	Erlerntes Muster der Warnungszusammenfassung.
SA-Alarmzusammenfassung – erlernte Musterelemente [sa_agg_pattern_element]	CI-/Metriknamenpaare, die erlernten Mustern zugeordnet sind.
Abfragegruppen-Muster für SA-Warnungszusammenfassung [sa_agg_group_pattern]	Beziehungen zwischen Gruppen, die in Abfragen zur Warnungszusammenfassung erkannt wurden, und Mustern, die im Lernen gefunden wurden.
Abfrage für SA-Warnungszusammenfassung -- bereitgestellte (letzte) Warnungen [sa_agg_group_alert_staging]	Eine Bereitstellungstabelle für Warnungen, die noch keiner zusammengefassten Warnungsgruppe zugeordnet wurden.
SA-Zusammenfassung – Musterattribut [sa_agg_pattern_attribute table]	CI/Warnungsattribute, die zum Auffinden von Mustern für die Warnungszusammenfassung verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
SA-Warnungsattribut-Populator-Status [sa_alert_attribute_populator_status table]	Status und Statistiken für das Ausfüllen des Attributjobs.
SA-Warnungszusammenfassung Erlerntes Musterelement Paarweise Gegenseitige Informationen und Gemeinsame Wahrscheinlichkeit [sa_agg_pattern_element_pair]	Paarweise Wahrscheinlichkeiten für Musterelemente.
EM-Agg.-Gruppenvorhersage [em_agg_group_prediction]	Warnungsvorhersagen für Warnungsgruppen.

Event Management Lösungen für Performance Analytics and Reporting

Lösungen für Performance Analytics and Reporting enthalten vorkonfigurierte Dashboards. Diese Dashboards enthalten Visualisierungen handlungsrelevanter Daten, mit denen Sie Ihre Geschäftsprozesse und -praktiken optimieren können.

Lösungen für Performance Analytics and Reporting

Platform Analytics Datenvisualisierungen verwenden Performance Analytics *Indikator*Daten, die Ihnen Daten im Zeitverlauf anzeigen, damit Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Lösungen für Performance Analytics and Reporting können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Um die Lösung für zu aktivieren Event Management, Kann ein Administrator zu navigieren **Performance Analytics** > **Geführtes Setup**an. Klicken Sie auf **Erste Schritte**, und scrollen Sie dann zum Abschnitt für Event Management. Das geführte Setup führt Sie durch den gesamten Einrichtungs- und Konfigurationsprozess.

Datenvisualisierung in ITOM Enthält jetzt eine Trichterkomponente, mit der Sie den Metrikfortschritt phasenübergreifend nachverfolgen können, wodurch es einfacher ist, Abgaben oder Engpässe in Prozessen zu identifizieren. Weitere Informationen finden Sie unter Datenvisualisierung in ITOM.

Zugehörige Informationen

Performance Analytics-Abonnement aktivieren

Performance Analytics-Widgets anpassen

Passen Sie die Darstellung von Widgets beim Anzeigen an Performance Analytics Visualisierungen.

Vorbereitungen

Erforderliche Rolle: Benutzer

Prozedur

1. Navigieren zu **Alle** > **Performance Analytics** > **Dashboards**an.
2. Wählen Sie auf der Seite **Dashboards** ein Dashboard aus, das angezeigt werden soll.
3. Wählen Sie oben rechts auf der Seite das Freigabesymbol ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wechseln Sie zum oberen Abschnitt des entsprechenden Widgets, und wählen Sie das Symbol Widget bearbeiten ( ).
5. Konfigurieren Sie im Dialogfeld „Widget bearbeiten“ die entsprechenden Optionen.
   Details finden Sie unter Performance Analytics – Dialogfeld „Widget bearbeiten“.
6. Wählen Sie im Dialogfeld „Widget bearbeiten“ die Option **Fertig** aus.

Nächste Maßnahme

Benutzer mit der Administratorrolle können Farben und Schriftarten anpassen.

- Weitere Informationen zum Anpassen von Farben finden Sie unter Performance Analytics-Widgets .
- Navigieren Sie zum Anpassen von Schriftarten zu **sys_ux_Theme_property.list** Und bearbeiten Sie die entsprechenden Schriftarten.

Lösungen für maschinelles Lernen für Event Management

Erstellen Sie Lösungen für Event Management mit Predictive Intelligence.

Lösungsdefinition

Lösungsdefinition für Event Management

Lösungsdefinition	Beschreibung
Ähnlichkeit mit geschlossener Warnung	Die Ähnlichkeit geschlossener Warnungen ist eine Ähnlichkeitslösungsdefinition, die verwendet wird, um ähnliche Warnungsdatensätze basierend auf diesen Feldern zu empfehlen: Beschreibung, Knoten, Ressource, CI-Typ, Quelle und Metrikname aus der Warnungstabelle [em_Alert]. Die Ergebnisse sind für Benutzer im Formular „Warnung“ und auf der Registerkarte „Ähnliche Warnungen“ in Workspace einsehbar.
EM-Warnungs-Clustering-Lösung	DIE EM-Warnungs-Clustering-Lösung ist eine Clustering-Lösungsdefinition, die im Ereignismanagement verwendet wird. Ermöglicht das Erstellen von Clustering-Modellen, die die Identifizierung gängiger Textmuster in Warnungen ermöglichen, um Warnungsgruppen zu erstellen. Textcluster basieren auf diesen Feldern: Beschreibung, Metrikname, Konfigurationselementklasse aus der Tabelle „Warnung“ [em_Alert].

Performance Analytics – Dialogfeld „Widget bearbeiten“

Felder im Dialogfeld zum Bearbeiten eines Widgets im Performance Analytics-Dashboard.

Abschnitt	Beschreibung
Echtzeit-Updates anzeigen	Durch die Auswahl werden Aktualisierungen in Echtzeit im Widget angezeigt.
Anzeigen	Aktivieren oder deaktivieren Sie die Kontrollkästchen, um Folgendes im Widget anzuzeigen oder auszublenden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Beschreibung
	• Rahmen • Kopfzeile • Titel
Titelausrichtung	Wählen Sie die Ausrichtung des Widget-Titels aus: • Left (Links) • Mitte • Mitte
Titelfarbe	Durch die Auswahl wird die Farbe des Widget-Titels konfiguriert.
Farbe der Kopfzeile	Durch die Auswahl wird die Farbe des Widget Headers konfiguriert.
Interaktivität	Wählen Sie aus den angezeigten Optionen aus. • Interaktivem Filter folgen • Anzeigen, wenn Filter gefolgt wird

Formular „Ereignismanagement MID-Webserver erweiterung“

Felder im Formular zum Erstellen oder Ändern einer MID-Webserver erweiterung.

Formular „MID-Webserver-Kontext“

Feld	Beschreibung
Name	Eindeutiger Name für die Erweiterung zur einfachen Identifizierung
Kurzbeschreibung	Kurze, aussagekräftige Beschreibung der Erweiterung
Status	Dieses Feld wird automatisch mit dem Status der Erweiterung ausgefüllt. Das Feld ist leer, bis die Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die Erweiterung wird einer der folgenden Werte angezeigt: • Gestartet: Die Erweiterung wird ausgeführt. • Angehalten: Die Erweiterung wird nicht ausgeführt. • Offline: Der MID-Server ist nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
	• Fehler: Die Erweiterung ist mit einem Fehler fehlgeschlagen. Die Fehlermeldung wird im Feld **Fehlermeldung** angezeigt. • Warnung: Eine Laufzeitausnahme ist aufgetreten. Die Erweiterung funktioniert weiterhin.
HTTP/HTTPS-Port	Portnummer, die die Erweiterung auf eingehende Anforderungen abhört
Authentifizierungstyp	Die verfügbaren Authentifizierungstypen sind: • **API-Schlüssel** (Standard): Von jedem Client, von dem eine Verbindung mit der Erweiterung hergestellt wird, muss ein API-Schlüssel in den Autorisierungsheader der Anforderung eingegeben werden. Weitere Informationen zum Anzeigen vorhandener API-Schlüssel finden Sie unter API-Schlüsselauthentifizierung für MID-Webserver konfigurieren. • **Schlüsselbasiert** (veraltet und nur aus Gründen der Kompatibilität mit Releases vor Zurich beibehalten): Der Wert im Feld **Geheimer Key** wird dazu verwendet, ein Authentifizierungstoken zu generieren, das im **Autorisierungsheader** eingehender Client-Anforderungen gesendet wird. Details finden Sie unter Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren. • **Standard** : Definieren Sie einen Anwendernamen und ein Passwort in **Anwender Für Standardauthentifizierung** Und **Anwenderpasswort Für Standardauthentifizierung** Felder, die bei Auswahl dieser Option angezeigt werden. • **mTLS**: Eine zertifikatbasierte Authentifizierung, bei der das TLS-Protokoll verwendet wird Details finden Sie unter MID-Webserver Und Agent-mTLS-Authentifizierung.
Geheimer Schlüssel	Der Wert, der generiert wird, wenn die schlüsselbasierte Authentifizierung für den Wert im Authentifizierungstyp ausgewählt ist Feld.
Standardauthentifizierungsbenutzer	Benutzername, der bei der Auswahl der Standardauthentifizierung verwendet werden soll

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
Benutzerkennwort für Standardauthentifizierung	Passwort, das bei der Auswahl der Standardauthentifizierung verwendet werden soll
Sichere Verbindung	Option zur Angabe, dass von der Erweiterung das TLS-Protokoll zum Verschlüsseln eingehender Verbindungen verwendet werden soll. Für die Erweiterung muss auch eine Kombination aus Zertifikat und privatem Schlüssel angegeben werden. Wenn Sie diese Option auswählen, wird das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden** angezeigt.
Einheitlichen MID-Schlüsselspeicher verwenden	Option zur Verwendung der Option des einheitlichen MID Server-Schlüsselspeichers für eine sichere Verbindung. Deaktivieren Sie diese Option, um den **Webserver-Schlüsselspeicher** zu verwenden. Details finden Sie unter Sichere MID-Webserver erweiterung konfigurieren.
Schlüsselspeicher-Zertifikatalias	Der Aliasname des Schlüsselpaars im ausgewählten Schlüsselspeicher, der von der Erweiterung zum Herstellen einer sicheren Verbindung verwendet wird. Lassen Sie dieses Feld leer, um den Standardalias zu verwenden, wenn Sie den einheitlichen MID-Schlüsselspeicher oder den Webserver-Schlüsselspeicher mit einem einzelnen Alias verwenden.
Schlüsselspeicher-Passwort	Das Passwort für den Webserver-Schlüsselspeicher, wenn dieser zum Herstellen einer sicheren Verbindung verwendet wird
Schlüsselpasswort des Schlüsselspeichers	Das Passwort des privaten Schlüsseleintrags, der dem angegebenen Alias des Webserver-Schlüsselspeichers zugeordnet ist. Dieses Feld kann leer gelassen werden, wenn das Passwort mit dem Eintrag im Feld „Schlüsselspeicher-Passwort“ übereinstimmt.
Truststore-Passwort	Das Passwort für den Truststore, der die Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) enthält, die zum Validieren der Signaturen der Client-Zertifikate verwendet werden. Wird angezeigt, wenn **mTLS** als Authentifizierungstyp ausgewählt ist. Lassen Sie dieses Feld leer, wenn die Erweiterung für die Verwendung des cacerts-Truststore der JRE konfiguriert ist, in der der MID-Server ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
Fehlermeldung	Nachricht, die Fehler beschreibt, die dazu führen, dass Befehle wie „Starten“ oder „Stoppen“ fehlschlagen. Dieses Feld wird nur angezeigt, wenn der Wert im Feld Status auf Fehler festgelegt ist.
Ausführen auf	Ausführungsort dieser Erweiterung. Die verfügbaren Optionen sind **Spezieller MID Server** oder **Spezieller MID Server-Cluster**.
MID Server	Je nachdem, was Sie im Feld **Ausführen auf** ausgewählt haben, ist dies der Name des festgelegten MID-Server s oder MID-Server-Clusters. • Wenn Sie **Spezifischer MID Server** ausgewählt haben: Name des festgelegten MID-Server • Wenn Sie **Spezifisches MID Server-Cluster** ausgewählt haben: Name des festgelegten MID-Server-Clusters
Ausführung auf	Zeigt den Namen des MID-Server s an, auf dem die Erweiterung ausgeführt wird, auch wenn der MID-Server nicht verfügbar ist. Wenn der Benutzer die Erweiterung stoppt, ist dieses Feld leer.

Ereignismanagement-Formular „Tag-basiertes Warnungs-Clustering-Tag“

Im Formular zum Erstellen oder Ändern eines Tag-basierten Warnungs-Clustering-Tags werden detaillierte Informationen zum Tag angezeigt.

Formular „Tag-basiertes Warnungs-Clustering-Tag“

Feld	Beschreibung
Name	Name des Clustering-Tags. Standardmäßig ist dies eine Beschreibung des konfigurierten Tags (z. B. **Exakte Übereinstimmung mit dem Warnungsfeld „ Metrikname“**). Der Standardname ist erst nach dem Speichern des Tags sichtbar. Tag-Namen müssen eindeutig sein.
Benutzerdefinierter Name	Aktivieren Sie das Kontrollkästchen, um den Wert im Feld **Name** anzupassen.
Domäne	Die Domäne, in der der aktuelle Datensatz erstellt wurde. Schreibgeschützt.
Beschreibung	Geben Sie eine optionale Beschreibung des Tags ein.
Quelle	Wählen Sie die Quelle aus, aus der das abzugleichende Feld ausgewählt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basiertes Warnungs-Clustering-Tag“ (Fortsetzung)

Feld	Beschreibung
	• **Warnungsfeld** • **Zusätzliche Warnungsinformationen** • **Warnungs-CI** • **Warnungs-CI-Schlüssel** • **Warnungstags** Wenn Sie auswählen **Zusätzliche Warnungsinformationen** , Wählen Sie eine aus **Schlüssel Für Zusätzliche Informationen** Anstelle eines Felds. **Zusätzliche Warnungsinformationen** Ist ein Feld in der Warnung, das das Schlüssel-Wert-Paar im Jason-Format enthält, und wir können einen bestimmten Schlüssel verwenden. **Warnungs-CI-Schlüssel** : Erstellen Sie CMDB-Schlüsselwerte, um Warnungen basierend auf der Tabelle „cmdb-Schlüsselwerte“ [cmdb_key_value] zu Clustern. Schlüsselwerte bieten eine zusätzliche Methode zum Bestimmen von Gemeinsamkeiten zwischen Warnungs-CIs.
Ausgewähltes Feld	Geben Sie das Feld an, das zwischen Warnungen übereinstimmen muss, damit die Warnungen in eine Gruppe aufgenommen werden. Wird angezeigt, wenn Sie **Alert Field** (Warnungsfeld) oder **Alert CI** (Warnungs-CI) im Feld **Source** (Quelle) auswählen. Wenn Sie auswählen **Warnungs-CI** In **Quelle** Feld müssen Sie einen CMDB-Schlüssel auswählen. Dem CI der Warnung wird ein CMDB-Schlüssel zugewiesen.
Schlüssel	Geben Sie den Schlüssel an, der zwischen Warnungen übereinstimmen muss, damit die Warnungen in eine Gruppe aufgenommen werden sollen. Wird angezeigt, wenn Sie auswählen **Zusätzliche Warnungsinformationen** In **Quelle** Feld, oder wird angezeigt, wenn Sie auswählen **Warnungs-Tags** In **Quelle** Feld. Wenn **Zusätzliche Warnungsinformationen** Ist ausgewählt, geben Sie den Namen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basiertes Warnungs-Clustering-Tag“ (Fortsetzung)

Feld	Beschreibung
	eines der Felder in das Feld zusätzliche Informationen ein. Wenn **Warnungs-Tags** Ist ausgewählt, geben Sie den Namen des relevanten Warnungs-Tags ein.
CMDB-Schlüssel	Geben Sie den CMDB-Schlüssel an, der bei Warnungen übereinstimmen muss, die in eine Gruppe aufgenommen werden sollen. Das Feld wird angezeigt, wenn Sie **Alert CI Key** (Warnungs-CI-Schlüssel) im Feld **Quelle** auswählen.
Übereinstimmungsmethode	Wählen Sie die Art der Übereinstimmung aus, die erforderlich ist, damit die Warnungen in eine Gruppe aufgenommen werden. • **Exact** (Genau): Gibt an, dass der Feldwert genau übereinstimmen muss, damit die Warnung in eine Gruppe aufgenommen wird. Sie können beispielsweise ein Alarm-Clustering-Tag konfigurieren, das angibt, dass das Feld **Metrikname** der Warnung genau übereinstimmen muss, um eine Gruppe zu bilden. Wenn man dieses Tag aufruft, sind alle Warnungen mit identischen Werten in dem Feld **Metrikname** in der gleichen Gruppe enthalten. • **Fuzzy** (Ungefähr): Gibt an, dass der Feldwert eine ungefähre Übereinstimmung sein muss (abhängig vom im Feld **Similarity** (Ähnlichkeit) konfigurierten Wert), damit die Warnung in eine Gruppe aufgenommen werden kann. • **Muster**: Gibt an, dass der Feldwert dem Muster im Feld **Muster** folgen muss. Informationen zur richtigen Syntax und Verwendung finden Sie unter Musterübereinstimmung .
Ähnlichkeit	Geben Sie den Ähnlichkeitsprozentsatz an, den die Warnungen erfüllen müssen, um in eine Gruppe aufgenommen zu werden. Wenn Sie beispielsweise 50 eingeben, müssen mindestens 50 Prozent des angegebenen Werts in der Warnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basiertes Warnungs-Clustering-Tag“ (Fortsetzung)

Feld	Beschreibung
	angezeigt werden, damit die Warnung in die Gruppe aufgenommen wird. Erscheint nur, wenn **Fuzzy** (Ungefähr) als Wert für **Match Method** (Übereinstimmungsmethode) ausgewählt wurde. Standardwert = 90

Liste der vordefinierten Warnungsgruppierungs-Tags

Eine Liste der vordefinierten Warnungs-Clustering-Tags, die mit der#Anwendung Tag-basierte Warnungs-Clustering-Engine bereitgestellt werden.

Vordefinierte Warnungs-Clustering-Tags

Name	Quelle	Übereinstimmungsmethode
CI	EM_Alert.cmdb_ci	Genaue Übereinstimmung
Beschreibung	em_alert.description	Genaue Übereinstimmung
Metrikname	EM_Alert.metric_Name	Genaue Übereinstimmung
Knoten	em_alert.node	Genaue Übereinstimmung
Ressource	EM_Alert.resource	Genaue Übereinstimmung
Quelle	EM_Alert.Source	Genaue Übereinstimmung
Quellinstanz	EM_Alert.event_class	Genaue Übereinstimmung
Typ	EM_Alert.type	Genaue Übereinstimmung
Zuweisungsgruppe	EM_Alert.assignment_Group	Genaue Übereinstimmung
CI-Klasse	cmdb_ci.sys_class_Name	Genaue Übereinstimmung
DNS-Domäne	cmdb_ci.dns_Domain	Genaue Übereinstimmung
ip-Adresse	cmdb_ci.ip_address	Genaue Übereinstimmung
Standort	cmdb_ci.location	Genaue Übereinstimmung
Umgebung	cmdb_ci.Environment	Genaue Übereinstimmung
CI-Name	cmdb_ci.name	Genaue Übereinstimmung
Namespace	cmdb_ci.namespace	Genaue Übereinstimmung

Vordefinierte Tags, die aus der Connector-Nutzlast extrahiert wurden

Name	Beschreibung	Standardzuordnung aus CMDB
t_ip_address	IP-Adresse	cmdb_ci.ip_address
t_Application	Anwendung	-
t_Region	Region	-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vordefinierte Tags, die aus der Connector-Nutzlast extrahiert wurden (Fortsetzung)

Name	Beschreibung	Standardzuordnung aus CMDB
t_location	Standort	cmdb_ci.location
t_Environment	Umgebung	cmdb_ci.Environment
t_Namespace	Namespace	cmdb_ci.namespace

Ereignismanagement Formular zur Definition der Tag-basierten Warnungsgruppierung

Im Formular zum Erstellen oder Ändern einer Tag-basierten Warnungs-Clustering-Definition werden detaillierte Informationen zur Definition angezeigt.

Formular „Tag-basierte Warnungs-Clustering-Definition“

Feld	Beschreibung
Name	Name der Alarm-Clustering-Definition. Definitionsnamen müssen eindeutig sein.
Aktiv	Wählen Sie die Option, um die Definition zu aktivieren. Diese Option ist standardmäßig ausgewählt.
Reihenfolge	Die Reihenfolge, in der Definitionen für eingehende Warnungen getestet werden. Solche mit niedrigeren Ordnungswerten werden zuerst getestet. Wenn eine Warnung mit einem der Filter der Definitionen übereinstimmt, wird die Suche nach weiteren Definitionen fortgesetzt. Standardwert = 1.000
Domäne	Die Domäne, in der der aktuelle Datensatz erstellt wurde. Schreibgeschützt.
Zuweisungsgruppe	Zuweisungsgruppe, die an der Warnung arbeitet. Wenn in der Warnungsregel keine Zuweisungsgruppe definiert ist, wird diese Warnungsregel als globale Regel betrachtet. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln und dann die Regeln ausgeführt, die zur Zuweisungsgruppe der Warnung gehören.
Beschreibung	Geben Sie eine optionale Beschreibung der Alarm-Clustering-Definition ein.
Filter	Legen Sie Bedingungen fest, die eingehende Warnungen erfüllen müssen, um von den Tags der Alarm-Clustering-Definition gemessen zu werden. Wenn die Tags Warnungen entsprechen, die im System vorhanden sind und sich innerhalb des Werts **Clustering timeframe (minutes)**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basierte Warnungs-Clustering-Definition“ (Fortsetzung)

Feld	Beschreibung
	(Clustering-Zeitrahmen (Minuten)) befinden, werden die eingehenden Warnungen mit den vorhandenen Warnungen verbunden, um eine Warnungsgruppe zu bilden. Nachdem Sie den Filter konfiguriert haben, können Sie auf die Schaltfläche **Vorschau** klicken, um anzuzeigen, wie viele vorhandene Warnungen der Bedingung des Filters entsprechen. **Hinweis:** • Übereinstimmende Warnungen werden nicht automatisch zusammen in eine Warnungsgruppe aufgenommen. Warnungen werden nur gruppiert, wenn sie über entsprechende Alarm-Clustering-Tags verfügen. • Bei Filterparametern wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. Um die Unterscheidung zwischen Groß- und Kleinschreibung zu deaktivieren, setzen Sie den *sa_analytics.correlation_case_sensitive*-Parameter auf **false**. • Sie können Warnungsfelder auch so konfigurieren, dass sie von der Suche ausgeschlossen werden, indem Sie die Eigenschaft *sn_em_tbac.tag_excluded_alert_fields* verwenden. Standardmäßig werden mit dieser Eigenschaft folgende Elemente ausgeschlossen: ○ Typ ○ event_class
Gruppenbeschreibung überschreiben	Standardgruppenbeschreibungen beginnen mit dem Präfix „Gruppe von Warnungen“, gefolgt von der Beschreibung der primären Warnung in der Gruppe. Sie können diese Gruppenbeschreibung überschreiben, indem Sie auswählen **Gruppenbeschreibung überschreiben** Kontrollkästchen. Dann in **Anwenderdefinierte Beschreibung** Feld eine Beschreibung eingeben. Diese Beschreibung wird als Beschreibung der Gruppen verwendet, die von dieser Warnungs-Clustering-Definition erstellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basierte Warnungs-Clustering-Definition“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Sie können das Formular nicht speichern, wenn Sie das Feld „Anwenderdefinierte Beschreibung“ leer gelassen haben oder den Standardtext „Gruppe von Warnungen“ enthalten.
Clustering-Zeitrahmen	Die maximale Zeit in Minuten, die zwischen der ersten Warnung und nachfolgenden Warnungen zulässig ist, damit sie gruppiert werden können. Beispielsweise gibt der Wert 60 an, dass alle Warnungen, die innerhalb von 60 Minuten nach der ersten Warnung in der Gruppe (der ältesten Warnung) generiert wurden, in die Warnungsgruppe aufgenommen werden. Alle Warnungen, die nach diesem 60-Minuten-Fenster aus der ersten Warnung generiert wurden, sind nicht in der Gruppe enthalten. Erlaubte Werte = 0-1440
M2M-Zuweisung von Definitionen und Tags für tag-basiertes Warnungs-Clustering	Wählen Sie die Alarm-Clustering-Tags aus, die der Alarm-Clustering-Definition zugewiesen werden sollen. Warnungen, die die in den ausgewählten Tags angegebenen Kriterien erfüllen, werden in die Warnungsgruppe aufgenommen. Die verfügbaren Optionen sind die Tags, die auf der Seite **Tag Based Alert Clustering Tags** (Tag-basiertes Alarm-Clustering) erstellt wurden.

Liste der vordefinierten Tag-basierten Warnungsgruppierungsdefinitionen

Eine Liste der vordefinierten Warnungs-Clustering-Definitionen, die mit der#Anwendung Tag-basierte Warnungs-Clustering-Engine bereitgestellt werden.

Vordefinierte Warnungs-Clustering-Definitionen

Name	Beschreibung	Reihenfolge
Gruppieren Sie Warnungen aus derselben Anwendung	Gruppieren Sie alle Warnungen aus derselben Anwendung, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9010
Gruppieren Sie alle Warnungen von derselben IP-Adresse	Gruppieren Sie alle Warnungen aus derselben IP-Adresse, die in den letzten 10 Minuten erstellt wurde.	9020
Gruppieren Sie alle Warnungen aus demselben Namespace	Gruppieren Sie alle Warnungen aus demselben Namespace, der in den letzten 10 Minuten erstellt wurde. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9030

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vordefinierte Warnungs-Clustering-Definitionen (Fortsetzung)

Name	Beschreibung	Reihenfolge
Gruppieren Sie alle Warnungen aus demselben Subnetz	Gruppieren Sie alle Warnungen aus demselben Subnetz, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9040
Gruppieren Sie Warnungen von derselben CI-Klasse und demselben Standort	Gruppieren Sie alle Warnungen aus derselben CI-Klasse und demselben CI-Standort, die in den letzten 10 Minuten erstellt wurden.	9050
Gruppieren Sie Warnungen aus derselben Anwendung und Umgebung	Gruppieren Sie alle Warnungen aus derselben Anwendung und Umgebung, die in den letzten 10 Minuten erstellt wurden.	9060
Gruppieren Sie alle Warnungen von einem ähnlichen Knoten	Gruppieren Sie alle Warnungen von einem ähnlichen Knotennamen, der in den letzten 10 Minuten erstellt wurde.	9070
Gruppieren Sie Warnungen aus demselben Standort und derselben Zuweisungsgruppe	Gruppieren Sie alle Warnungen vom selben Standort und derselben Zuweisungsgruppe, die in den letzten 10 Minuten erstellt wurden.	9080
Gruppieren Sie Warnungen aus derselben Region und Metrik	Gruppieren Sie alle Warnungen aus derselben Region und Metrik, die in den letzten 10 Minuten erstellt wurden.	9090
Gruppieren Sie Warnungen aus derselben CI-Klasse und -Metrik	Gruppieren Sie alle Warnungen aus derselben CI-Klasse und -Metrik, die in den letzten 10 Minuten erstellt wurden.	9100
Gruppieren Sie Warnungen aus demselben Knoten und derselben Metrik	Gruppieren Sie alle Warnungen aus demselben Knoten und derselben Metrik, die in den letzten 10 Minuten erstellt wurden.	9110
Gruppieren Sie Warnungen aus derselben Zuweisungsgruppe und -Klasse	Gruppieren Sie alle Warnungen aus derselben Zuweisungsgruppe und -Klasse, die in den letzten 10 Minuten erstellt wurden.	9120
Gruppieren Sie Warnungen vom selben Typ, derselben Metrik und derselben Quelle	Gruppieren Sie alle Warnungen aus demselben Typ, derselben Metrik und derselben Quellinstanz, die in den letzten 10 Minuten erstellt wurden.	9130
Gruppieren Sie Warnungen vom selben CI	Gruppieren Sie alle Warnungen aus demselben CI, die in den letzten 10 Minuten erstellt wurden. **Wichtig:** Wenn diese Regel aktiv ist, CMDB Gruppierung muss deaktiviert sein.	9140
Gruppieren Sie Warnungen vom selben Knoten	Gruppieren Sie alle Warnungen aus demselben Knoten, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Regel standardmäßig aktiviert.	9150

Mit installierte Domäneneigenschaften Ereignismanagement

Verwenden Sie die mit installierten Domäneneigenschaften Ereignismanagement Um die Metadaten bereitzustellen, die auf die entsprechende Tabelle verweisen, um die Domäne zu identifizieren, damit Sie wissen, in welcher Domäne das Ereignis erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardeigenschaften der Domänenmetadaten

Eigenschaft
evt_mgmt. Connector_Domain_info_table_Name
evt_mgmt. Connector_Domain_info_column_Name
evt_mgmt. Connector_Domain_ID_column_Name
evt_mgmt. Connector_Domain_path_column_Name

Metadaten der Connector-Domäne

Überschreiben Sie die mit installierten Standarddomänen-Metadatenwerte des Push-Connectors Ereignismanagement Mit den Werten in der HTTP-Anforderung des Ereignisses, einschließlich URL, Header, Anforderungstext (Nutzlast) und Connector-Parameter. Überschreiben Sie die Metadatenwerte der Pull-Connector-Domäne nur mit Connector-Parametern.

Domänenmetadatenparameter

Name	Beschreibung	Überschreibt Die Systemeigenschaft
`connectorDomainInfoTableName`	Name der Tabelle, die die Datensätze mit den Domäneninformationen enthält.	evt_mgmt.Connector_Domain_info_table_Name • **Typ**: Zeichenfolge • **Standardwert** : Core_Company
`connectorDomainInfoColumnName`	Name der Spalte, die einen Wert hat, der mit dem Domänenbezeichner abgeglichen werden soll. Sie können beispielsweise einen Datensatz in der Tabelle „Domäneninformationen“ identifizieren, der einen	evt_mgmt.Connector_Domain_info_column_Name • **Typ**: Zeichenfolge • **Standardwert** : Name

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Überschreibt Die Systemeigenschaft
	übereinstimmenden Wert in aufweist **Company_Name** Feld.	
`connectorDomainIdColumnName`	Name der Tabellenspalte, in der die Domänen-ID gespeichert ist.	evt_mgmt.Connector_Domain_ID_column_Name • **Typ**: Zeichenfolge • **Standardwert** : Sys_Domain
`connectorDomainPathColumnName`	Name der Tabellenspalte, die den Domänenpfad speichert.	evt_mgmt.Connector_Domain_path_column_Name • **Typ**: Zeichenfolge • **Standardwert** : Sys_Domain_path

Reihenfolge der Einstellungen für den Zugriff auf Domänenmetadaten

Sie müssen Domänenmetadaten angeben, um personalisierte Push-Connector-Domänen zu konfigurieren. Die Metadaten in der bevorzugten Zugriffreihenfolge sind:

1. Push-Connector-Parameter
2. URL-Abfrageparameter
3. HTTP-Header
4. Anforderungstext (Nutzlast)
5. Standardsystemeigenschaften

URL-Abfrageparameter

Push-Connectors haben die folgende URL-Syntax:

- Instanztyp: `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=<connector-source>`
- MID-Server Typ: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/Mid/em/inbound_event?Transform=<connector-transform-script-name>`

Sie können Domänenmetadaten als zusätzliche Abfrageparameter in einschließen ServiceNow Webhook-URL des Push-Connectors. Wenn die Domäneninformationsquelle beispielsweise die Tabelle sys_user ist, könnte die URL lauten `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=<connector-source>&connectorDomainInfoTableName=sys_user`

Anforderungskopfzeilen.

Jede der Domänenmetadateneigenschaften kann als Teil von HTTP-Anforderungsheadern übergeben werden. Informationen dazu, wie Anforderungsheader festgelegt sind, finden Sie in der Dokumentation Ihres Überwachungstool von Drittparteien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungstext (Nutzlast)

Sie können Domänenmetadaten aus dem Anforderungstext (JSON-Nutzlast) referenzieren, indem Sie die Metadatenparameter als Schlüssel auf Stammebene in der Nutzlast festlegen. Das folgende Beispiel zeigt, wie der `connectorDomainInfoTableName`Und `connectorDomainInfoColumnName`Parameter können als Teil des Anforderungstexts übergeben werden:

```
{
    „Quelle“: „Azure Monitor“,
    „Host“: „127.0,0.1“,
    „Unternehmen“: „ServiceNow“,
    „ConnectorDomainInfoTableName“: „Sys_user“,
    „ConnectorDomainInfoColumnName“: „First_Name“
    }
```

Hinweis: Informationen zu Connector-Parametern finden Sie unter Personalisieren Sie Domänen für Push-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen.

Dynatrace Formular „Connector-Instanz“

Die Dynatrace Das Connector-Instanzformular zeigt die Felder an, die Sie beim Erstellen von ausfüllen müssen Dynatrace Connector-Instanz.

Connector-Instanzseite

Feld	Beschreibung
Name	Eindeutiger Name für Dynatrace Metrik-Connector-Instanz.
Beschreibung	Beschreibung für die Verwendung der Connector-Instanz.
Connector-Definition	Die vom Connector zu verwendende Connector-Definition. Wählen Sie Aus **Dynatrace-Metriken** .
Host-IP	Hostname/IP-Adresse des Dynatrace Server.
Anmeldeinformation	Wählen Sie das Suchsymbol aus, und wählen Sie die vorhandenen API-Schlüssel-Anmeldeinformationen aus. Wenn diese Anmeldeinformationen nicht vorhanden sind, erstellen Sie wie folgt neue Anmeldeinformationen: **1.** Stellen Sie sicher, dass Sie über ein Zugriffstoken mit Berechtigungen „Metrik lesen“ (metrics.read) verfügen, das auf erstellt wurde Dynatrace UI. **2.** Wählen Sie Aus **Neu** Nachdem Sie das Suchsymbol ausgewählt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	3. Wählen Sie Aus **API-Schlüssel-Anmeldeinformationen** . 4. In **API-Schlüssel** Geben Sie das Zugriffstoken aus dem ein Dynatrace UI. 5. In **Name** Geben Sie einen beschreibenden Namen ein, um die Anmeldeinformationen eindeutig zu identifizieren. 6. Füllen Sie alle anderen relevanten Felder aus, und wählen Sie aus **Übermitteln** .
Metriksammlung	Standardmäßig ausgewählt. Schreibgeschützt.
Metriksammlungszeitplan (Sekunden)	Zeitintervall (in Sekunden), in dem der Metrik-Connector Metriken aus dem abruft Dynatrace Server. Standard: 60.
Aktiv	Wählen Sie diese Option aus, um die Connector-Instanz zu aktivieren.

Dynatrace Parameter des Connector-Instanzwerts

In der folgenden Tabelle wird angezeigt Dynatrace Parameter des Connector-Instanzwerts, die Sie bei Bedarf beim Erstellen von eingeben können Dynatrace Connector-Instanz.

Parameter des Connector-Instanzwerts

Parameter	Beschreibung
BaseApiPath	Anwenderdefinierter Basispfad für Dynatrace-API-Aufrufe. Wenn Ihre Dynatrace-Instanz einen anderen Pfad als den Standard verwendet `/api/v2/metrics` Geben Sie den anwenderdefinierten Pfad ein, um eine erfolgreiche Erfassung von Metriken sicherzustellen.
debuggen	Auf festlegen **Wahr** Zum Aktivieren von Debug-Protokollen. Standardwert: false
InitialSyncInMins	Anzahl der Minuten vor dem aktuellen Zeitpunkt, zu dem die anfängliche Metriksammlung ausgeführt wird. Wenn der Wert beispielsweise 15 ist, ruft der Connector Metriken aus den letzten 15 Minuten ab. Standard: 15
LogPayload	Bestimmt, ob die Rohprotokollnutzlast gedruckt werden soll. Auf festlegen **Wahr** Nur zu Debugging-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter des Connector-Instanzwerts (Fortsetzung)

Parameter	Beschreibung
	Zwecken, da durch das Drucken der Rohnutzlast schnell gefüllt wird MID-Server Protokolle. Standardwert: false
MaxMetricsPerQuery	Maximale Anzahl von Metrik-IDs, die pro API-Aufruf abgefragt werden sollen Dynatrace. Der Wert darf 32 nicht überschreiten, den zulässigen Höchstwert von Dynatrace. Standard: 32
pageSize	Maximale Anzahl von Datensätzen, die in einer API-Antwort zurückgegeben werden sollen Dynatrace. Standard: 500
port	Portnummer für Dynatrace Server, mit dem eine Verbindung hergestellt werden soll. Leer
protocol	Protokoll, das beim Herstellen einer Verbindung mit verwendet werden soll Dynatrace Server. Standardwert: https.
DrosselenApiCalls	Bestimmt, ob Drosselung aktiviert ist. Wenn aktiviert (**Wahr**) Wird ein Grenzwert für die Anzahl der API-Aufrufe auf festgelegt Dynatrace Pro Minute. Standardwert: false
AnforderungPerMinute	Der Grenzwert für die Anzahl der API-Aufrufe an Dynatrace Pro Minute. Nur relevant, wenn *`throttleApiCalls`*= **Wahr** . Standardwert: 1000

Push-Connector-Instanzformular

Das Formular „Push-Connector-Instanz“ zeigt die Felder an, die Sie ausfüllen müssen, wenn Sie einen Connector erstellen oder ändern.

Feld	Beschreibung
Name	Ein eindeutiger Name für den Connector-Instanzdatensatz, z. B. der Name eines Ereignisquellhosts.
Beschreibung	Alle optionalen Informationen, die der Administrator zur Identifizierung dieses Datensatzes verwenden möchte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Push-Connector-Definition	Wählen Sie Aus Die Definition für das externe System, von dem Sie Ereignisse empfangen möchten. Sie können eine beliebige vorhandene Definition auswählen, z. B.: • Thousandeyes • Dynatrace • Catchpoints Eine Liste der im Basissystem verfügbaren Connector-Definitionen finden Sie unter Konfigurieren Ereignismanagement Connectors. **Hinweis:** Wenn für den von Ihnen ausgewählten Push-Connector-Typ Konfigurationsparameter verfügbar sind, werden sie unter Push-Connector-Instanzkonfigurationsparameter angezeigt.
MID-Server	Zeigt die Liste von an MID Servers Das mindestens einen hat MID-Server Ereignis-Listener-Kontext wird ausgeführt. Die MID-Server Abschnitt wird nur angezeigt, wenn der MID-Definitionstyp ausgewählt ist.
URL	Dieses Feld wird erst nach dem Speichern der Details der Connector-Instanz automatisch ausgefüllt. Instanz: Die URL muss in einem externen System mit konfiguriert werden ServiceNow Anmeldeinformationen mit der Rolle „evt_mgmt_Integration“ zum Empfangen der Ereignisse. MID-Push-Connector-Instanz: Die URL muss von einem externen System mit konfiguriert werden MID-Webserver erweiterung konfigurieren Anmeldeinformationen zum Empfangen der Ereignisse. Dieses Feld wird erst angezeigt, nachdem das Formular gespeichert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Empfang der Ereignisse von dieser externen Ereignisquelle zu aktivieren. Dieses Feld wird erst angezeigt, nachdem das Formular gespeichert wurde.

Nagios-Connector-Instanzwertparameter

In der folgenden Tabelle werden die Wertparameter der Nagios-Connector-Instanz angezeigt, die Sie bei Bedarf beim Erstellen einer Nagios-Connector-Instanz eingeben können.

Parameter des Connector-Instanzwerts

Parameter	Beschreibung
debuggen	Auf festlegen **Wahr** Zum Aktivieren von Debug-Protokollen. Standardwert: false
max_fetch_interval_min	Begrenzt den Abruf des Metrikverlaufs, um eine Systemüberlastung zu verhindern. Standard: 180 Minuten
offset_min	Fügt einen kleinen Zeitpuffer hinzu, um sicherzustellen, dass keine Metriken verpasst werden. Standard: 5 Minuten

Formular „Nagios-Connector-Instanz“

Das Formular „Nagios-Connector-Instanz“ zeigt die Felder an, die Sie beim Erstellen einer Nagios-Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Eindeutiger Name für die Connector-Instanz der Nagios-Metrik.
Beschreibung	Kurze Erklärung des Zwecks oder der Verwendung der Connector-Instanz.
Connector-Definition	Connector-Definition, die vom Connector verwendet werden soll. Wählen Sie Aus **Nagios-Metriken** .
Metrikendatenbank-Host	Host-IP-Adresse des Hosts, auf dem der Nagios-Server Metriken erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
Metrikendatenbank-Anmeldeinformationen	Anmeldeinformationen, die für den Zugriff auf die Nagios-Datenbank erforderlich sind.
Metriksammlung	Option ist vorausgewählt und schreibgeschützt.
Metriksammlungszeitplan (Sekunden)	Zeitintervall (in Sekunden), in dem der Connector Metriken vom Nagios-Server abruft. Standard: 60 Sekunden.
Aktiv	Option zum Aktivieren der Connector-Instanz.

Zabbix Formular „Connector-Instanz“

Das Formular „Zabbix-Connector-Instanz“ zeigt die Felder an, die Sie beim Erstellen einer Zabbix-Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Eindeutiger Name für die Connector-Instanz der Zabbix-Metrik.
Beschreibung	Kurze Erklärung des Zwecks oder der Verwendung der Connector-Instanz.
Connector-Definition	Connector-Definition, die vom Connector verwendet werden soll. Wählen Sie Aus **Zabbix-Metriken** .
Host-IP	Host-IP-Adresse des Hosts, auf dem der Zabbix-Server Metriken erfasst.
Anmeldeinformation	Anmeldeinformationen, die für den Zugriff auf die Zabbix-Datenbank erforderlich sind. Wählen Sie das Suchsymbol, und wählen Sie die Anmeldeinformationen für Standardauthentifizierung aus. • Name: Geben Sie den eindeutigen Namen für die Zabbix-Anmeldeinformation an. • Anwendername: Geben Sie den Anwendernamen des Zabbix-Servers an • Passwort: Geben Sie das Passwort des Zabbix-Servers an • Wählen Sie **Absenden**.
Metriksammlung	Option ist vorausgewählt und schreibgeschützt.
Metriksammlungszeitplan (Sekunden)	Zeitintervall (in Sekunden), in dem der Connector Metriken vom Zabbix-Server abruft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	Standard: 60 Sekunden.
Aktiv	Option zum Aktivieren der Connector-Instanz.

Parameter des Zabbix-Connector-Instanzwerts

Die folgende Tabelle zeigt die Wertparameter der Zabbix-Connector-Instanz an, die Sie bei Bedarf beim Erstellen einer Zabbix-Connector-Instanz eingeben können.

Parameter des Connector-Instanzwerts

Parameter	Beschreibung
api_Endpoint_Suffix	Legen Sie diesen Wert basierend auf der Installation der Webschnittstelle des Zabbix-Servers fest: https://www.zabbix.com/documentation/current/en/manual/installation/frontend#welcome-screen Standardwert: /zabbix/api_jsonrpc.php [für Apache-Server]
debuggen	Auf festlegen **Wahr** Zum Aktivieren von Debug-Protokollen. Standardwert: falsch
Enable_Batch_processing	Wenn die Batch-Verarbeitung aktiviert ist, werden Metrikdetails im Batch mit Hosts von 1000 (kann geändert werden, indem der entsprechende Wert auf den Parameter „max_Hosts_per_Batch“ festgelegt wird) pro Batch abgerufen. Standardwert: falsch
groupids	Geben Sie die Hostgruppen-IDs an. Diese IDs werden verwendet, um Metriken von den Hosts abzurufen, die an die angegebenen Gruppen angehängt sind. Dies gilt nur, wenn Enable_Batch_processing Ist auf „wahr“ festgelegt.
logPayloadForDebug	Bestimmt, ob die Rohprotokollnutzlast gedruckt werden soll. Auf festlegen **Wahr** Nur zu Debugging-Zwecken, da das Drucken der Rohnutzlast die MID-Serverprotokolle schnell ausfüllt. Standardwert: falsch
max_fetch_interval_min	Konfiguriert über den Parameter „max_fetch_interval_min“: Wenn die Zeit „max_fetch_interval_min“ überschreitet, wird der Abruf von „max_fetch_interval_min“ vor dem aktuellen Zeitpunkt gestartet. Bei einer ERSTEN Ausführung ohne „lastMetricSignature“ wird die Zeit auf „max_fetch_interval_min“ vor dem aktuellen Zeitpunkt festgelegt. Standardwert: 180 Minuten
max_Hosts_per_Batch	Wenn die Batch-Verarbeitung aktiviert ist, werden Metrikdetails im Batch mit Hosts von 1000 (kann geändert werden, indem der entsprechende Wert auf den Parameter „max_Hosts_per_Batch“ festgelegt wird) pro Batch abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter des Connector-Instanzwerts (Fortsetzung)

Parameter	Beschreibung
	Standardwert: 1000
offset_min	Gibt den Zeitversatz in Minuten an, um die Abrufstartzeit relativ zur aktuellen Zeit anzupassen. Standard: 5 Minuten
port	Portnummer für den Zabbix-Server, mit dem eine Verbindung hergestellt werden soll. Standardwert: leer
protocol	Protokoll, das beim Herstellen einer Verbindung mit dem Zabbix-Server verwendet werden soll. Standardwert: http
with_triggers	Dadurch werden die Auslöserinformationen abgerufen. Standardwert: falsch

Hinweis: Bei der Überwachung einer großen Anzahl von Hosts in Zabbix kann sich das Abrufen massiver Metrikdaten auf die Leistung auswirken und API-Zeitüberschreitungen verursachen. Durch Aktivieren der Batch-Verarbeitung (enable_Batch_processing = wahr) wird dies gemindert, indem Metriken in Batches abgerufen werden (Standard: 1000 Hosts, konfigurierbar über `max_hosts_per_batch`), obwohl es Netzwerkanrufe erhöht und bei der Überwachung von mehr als 000 Hosts oder bei Leistungsproblemen verwendet werden muss.

Formular „SCOM-Connector-Instanz“

Das Formular „SCOM-Connector-Instanz“ zeigt die Felder an, die Sie beim Erstellen einer SCOM-Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Einzigartiger Name für die SCOM-Connector-Instanz.
Beschreibung	Beschreibung für die Verwendung der Instanz der SCOM-Ereignissammlung.
Aktiv	Wählen Sie diese Option aus, um die Connector-Instanz zu aktivieren. Wird nur angezeigt, wenn eine Connector-Instanz ausgewählt wird, die bereits erstellt wurde.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Ereignissen aus der externen Quelle verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	Wählen Sie für einen regulären SCOM-Connector aus **SCOM** . Wählen Sie für eine Connector-Instanz, die Sie Metriken überwachen möchten, aus **SCOM-Metriken** . Wenn Sie diese Option auswählen, werden die Felder im angezeigt **Connector-Instanz: Metrikfelder** Tabelle wird angezeigt.
Zuweisungsgruppe	Wählen Sie die Gruppe aus, der die Connector-Instanz zugewiesen ist. Dies kann beispielsweise eine Gruppe von Administratoren oder eine Supportgruppe sein.
Host-IP	Geben Sie die SCOM-IP-Adresse an. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Anmeldeinformation	Wählen Sie die Windows-Anmeldeinformationen aus. **Hinweis:** Vergewissern Sie sich beim Konfigurieren von Windows-Anmeldeinformationen, wenn diese für bestimmte MID Server gelten, dass die von Ihnen im Anmeldeinformationsdatensatz angegebenen MID Server mit den im Abschnitt **MID Server für Anschlüsse** auf dem Formular „Anschlussinstanz“ angegebenen MID Servern übereinstimmen. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Zeit der letzten Ausführung der Eventsammlung	Die letzte Ausführungszeitwert der Ereignissammlung wird automatisch aktualisiert. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Status der letzter Eventsammlung	Die letzte Ausführungszeitstatus der Ereignissammlung wird automatisch aktualisiert. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
Zeitplan für Eventsammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von SCOM sucht. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Bidirektional	Wählen Sie diese Option, um die bidirektionale Option aufzurufen. Diese Option ermöglicht sie den bidirektionalen Austausch von Werten mit der externen Event-Quelle. Für SCOM ist eine Standardimplementierung vorhanden. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt ist. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Letzter bidirektionaler Status	Das Feld wird automatisch mit einem Wert ausgefüllt. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
Letzte Fehlermeldung	Das Feld der letzten Fehlermeldung wird automatisch aktualisiert. Diese Nachricht ist die letzte Fehlermeldung, die vom Connector empfangen wurde. Wenn der Test-Connector fehlschlägt, wird in diesem Feld eine Fehlermeldung angezeigt. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** Ist als Connector-Definition ausgewählt.
MID Server (Abschnitt MID Server für Connectors)	Geben Sie mindestens einen an MID Servers Die aktiv und gültig sind. MID Servers Sortieren Sie gemäß der Reihenfolge, in der die Details in eingegeben wurden MID-Server Für Abschnitt „Connectors“. Die Portanforderung von MID-Server Zum SCOM-Server ist 1433 . Wenn angegeben MID-Server Befindet sich in einem Cluster, es kann nicht ausgewählt werden, und ein anderer ist verfügbar MID-Server Ist an seiner Stelle ausgewählt.Stellen Sie sicher, dass angegeben ist MID Servers Stimmen Sie mit überein MID Servers Wird auf der Seite „Windows-Anmeldeinformationen“ angegeben, da der Connector Windows-Anmeldeinformationen für den Zugriff verwendet MID Servers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

Connector-Instanz – Metrikfelder (angezeigt, wenn Connector-Definition = SCOM-Metriken)

Feld	Beschreibung
Metrikensammlung	Standardmäßig ausgewählt. Schreibgeschützt.
Zeit der letzten Ausführung der Metriksammlung	Die letzte Ausführungszeit der geplanten Aufgabe „Metriksammlung“. Dieses Feld ist schreibgeschützt.
Letzter Metriksammlungsstatus	Status der Aktivität zur Metrikdaten-Erfassung. Das Feld wird automatisch mit einem Wert ausgefüllt. Dieses Feld ist schreibgeschützt.
Zeitplan für Metriksammlung (Sekunden)	Die Zeit in Sekunden zur Wiederholung von Metrikdaten Geplante Aufgabe der Sammlung.
Metrikendatenbank-Host	Die IP-Adresse oder der Hostname des Metrikdatenbank-Hosts.
Verbindung mithilfe einer benannten Instanz	Wenn ausgewählt, wird die Verbindung mit der angegebenen benannten Instanz hergestellt. Andernfalls wird die Verbindung über den angegebenen Port hergestellt.
Metrikendatenbank-Port	Der von der Metrikdatenbank verwendete Port. Die Verbindung wird über JDBC hergestellt. Die Standardportnummer ist 1433. Wenn **Stellen Sie eine Verbindung mit einer benannten Instanz her** Ist ausgewählt, wird diese Option nicht angezeigt.
Metrikendatenbank – benannte Instanz	Der Name der Metrikdatenbank-Instanz.
Datenbank-Login mit Windows-Authentifizierung	Führen Sie die Datenbankanmeldung mit den Anmeldeinformationen des angemeldeten Anwenders durch, der auf definiert ist MID-Server Service.
Metrikendatenbank-Anmeldeinformationen	Anmeldeinformationen für die Metrikdatenbank. Verwenden Sie JDBC-Anmeldeinformationen für den lokalen Datenbankbenutzer. Wenn **Datenbankanmeldung mit Windows-Authentifizierung** Ist ausgewählt, wird diese Option nicht angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „SolarWinds-Connector-Instanz“

Im Formular „SolarWinds-Connector-Instanz“ werden die Felder angezeigt, die Sie beim Erstellen einer SolarWinds-Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Eindeutiger Name für die SolarWinds-Metrik-Connector-Instanz.
Beschreibung	Kurze Erklärung des Zwecks oder der Verwendung der Connector-Instanz.
Connector-Definition	Connector-Definition, die vom Connector verwendet werden soll. Wählen Sie Aus **Solarwinds-Metriken** .
Host-IP	Hostname/IP-Adresse des SolarWinds-Servers.
Anmeldeinformation	Anmeldeinformationen für einen SolarWinds-Anwender mit Standardauthentifizierung und Lesezugriff auf die SWIS-REST-API.
Metriksammlung	Option ist vorausgewählt und schreibgeschützt.
Metriksammlungszeitplan (Sekunden)	Zeitintervall (in Sekunden), in dem der Connector Metriken vom SolarWinds-Server abruft. Standard: 60 Sekunden.
Aktiv	Option zum Aktivieren der Connector-Instanz.

Parameter für SolarWinds-Connector-Instanzwert

In der folgenden Tabelle werden die Wertparameter der SolarWinds-Connector-Instanz angezeigt, die Sie bei Bedarf beim Erstellen einer SolarWinds-Connector-Instanz eingeben können.

Parameter des Connector-Instanzwerts

Parameter	Beschreibung
debuggen	Auf festlegen **Wahr** Zum Aktivieren von Debug-Protokollen. Standardwert: falsch
max_fetch_interval_in_min	Anzahl der Minuten vor dem aktuellen Zeitpunkt, zu dem die anfängliche Metriksammlung ausgeführt wird. Wenn der Wert beispielsweise 180 ist, ruft der Connector Metriken aus den letzten 180 Minuten ab. Standardwert: 180 Minuten
logPayloadForDebug	Bestimmt, ob die Rohprotokollnutzlast gedruckt werden soll. Auf festlegen **Wahr** Nur zu Debugging-Zwecken, da das Drucken der Rohnutzlast die MID-Serverprotokolle schnell ausfüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter des Connector-Instanzwerts (Fortsetzung)

Parameter	Beschreibung
	Standardwert: falsch
Offset	Gibt den Zeitversatz in Minuten an, um die Abrufstartzeit relativ zur aktuellen Zeit anzupassen. Standard: 0 Minuten
Port	Portnummer für den SolarWinds-Server, mit dem eine Verbindung hergestellt werden soll. Standardwert: 17774
protocol	Protokoll, das beim Herstellen einer Verbindung mit dem SolarWinds-Server verwendet werden soll. Standardwert: https

Eigenschaften der Ereignisweiterleitung

Mit mehreren Systemeigenschaften können Sie einen Ereignisweiterleitungsauftrag anpassen.

Hinweis: Um auf die Tabelle „Systemeigenschaften“ [sys_properties] zuzugreifen, geben Sie ein `sys_properties.list` Im Navigationsfilter.

Eigenschaft	Beschreibung
evt_mgmt.Event_Forwarding.sources_to_exclude	Liste der Ereignisquellen, aus denen Ereignisse nicht weitergeleitet werden sollen. Standardmäßig werden alle Ereignisse weitergeleitet. Trennen Sie mehrere Quellen durch Kommas. • **Typ**: Zeichenfolge • **Standardwert** : Leer
evt_mgmt.Event_Forwarding.event_fields_to_include	Liste der Ereignisfelder, die beim Senden von Ereignissen an die Zielinstanz neben den erforderlichen Standardfeldern einbezogen werden sollen: Resolution_State, event_class, additional_info, node, resource, cmdb_ci,Schweregrad, time_of_event, message_key, sys_Domain, metric_Name, ci_type, ci_Identifier, type, Source, description, und sys_Domain_path. Trennen Sie mehrere Felder durch Kommas. • **Typ**: Zeichenfolge • **Standardwert** : Leer
evt_mgmt.Event_Forwarding.event_Batch_size	Maximale Anzahl von Ereignissen, die beim Senden an die Zielinstanz als Batch verwendet werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 500
evt_mgmt.Event_Forwarding.max_Payload_size_in_mb	Maximale Größe der Ereignisnutzlast in MB, die gleichzeitig an die Zielinstanz gesendet wird. • **Typ**: Ganzzahl • **Standardwert**: 5
evt_mgmt.event_Forwarding.max_Events_to_Forward_per_day	Maximale Anzahl von Ereignissen, die pro Tag von der Instanz weitergeleitet werden können, um die Auswirkungen auf die Leistung auf die Quellinstanz zu minimieren. • **Typ**: Ganzzahl • **Standardwert**: 100000
evt_mgmt.Event_Forwarding.log_debug	Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignisweiterleitung. Legen Sie diese Eigenschaft auf „wahr“ fest, um Debugging-Informationen zu protokollieren. • **Typ**: Boolesch • **Standardwert** : Falsch

Teambasierte Integrationseigenschaften

Mit den Systemeigenschaften der teambasierten Integration können Sie die Zuweisungsgruppenfunktionalität für vorhandene und neue Kunden für Ereignisregeln und Ereignisfeldzuordnungen anpassen.

Systemeigenschaften der teambasierten Integration

Eigenschaft	Beschreibung
evt_mgmt.Alert_Auto_assignment_field	Die Eigenschaft bestimmt die automatische Warnungsz geordnete Liste von kommagetrennten Feldern. Der Standardwert dieser Eigenschaft ist cmdl IntegrationGroup. Der Wert der Zuweisungsg übernommen **Supportgruppe** Feld (cmdb_ci.Su CI der Warnung. Wenn dieses Feld leer ist, wi IntegrationGroup-Wert in übernommen **Zuwei** Tabelle „Connector-Instanzen“ [em_Connecto Für aktualisiert Instanzen aus vorherigen Familienveröf leer Um Auswirkungen auf Produktionsinstanzen zu ve • **Typ**: Zeichenfolge • **Standardwert** :

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften der teambasierten Integration (Fortsetzung)

Eigenschaft	Beschreibung
	◦ Leer – für aktualisierte Kunden ◦ cmdb_ci.Support_Group, IntegrationGroup **Hinweis:** Wenn Sie ein Warnungsfeld in diese verwenden Z. B. ein Warnungsfeld in **Zusätzlich** Feld, ein Warnungs-Tag oder ein neues Warnungsf **Zuweisungsgruppe** Feld muss die Gruppen-sys {"Warnungsfeldname":"<sys_ID des gewüns Datensatzes>"} . .
evt_mgmt.enable_Group_level_event_rules	Aktiviert teambasierte Funktionalität zum Aus Ereignisregeln und Ereignisfeldzuordnungsreg haben Vorrang vor bestimmten teambasierten • **Typ**: Boolesch • **Standardwert** : ◦ Falsch: Für aktualisierte Kunden ◦ Wahr: Für neue Kunden

Warnungsabfrageformular

Sie können ähnliche Warnungen kombinieren, die bestimmte Kriterien für einen bestimmten Service erfüllen, indem Sie eine Warnungsabfrage erstellen.

Warnungsabfrageformular

Feld	Beschreibung
Name	Der Name der Warnungsabfrage.
Business-Relevanz	Die Wichtigkeit dieser Warnungsabfrage für das Unternehmen. Dieses Feld kann Notfallwiederherstellungsstrategien für diese Warnungsabfrage bestimmen. • 1: Äußerst kritisch • 2: Etwas kritisch • 3: Weniger kritisch • 4: Nicht kritisch
Verwendet für	Der Zweck der Warnungsabfrage. Wählen Sie aus: • Produktion (Standard) • Staging • QA • Test • Entwicklung • Demonstration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsabfrageformular (Fortsetzung)

Feld	Beschreibung
	• Schulung • Notfallwiederherstellung
Eigentum von	Die Partei, die für die Warnungsabfrage verantwortlich ist.
E-Mail	Der E-Mail-Alias für die Warnungsabfrage.
Telefon (geschäftlich)	Die Telefonnummer für das Unternehmen.
Betriebsstatus	Der Status der Warnungsabfrage. • **Betriebsbereit** : Die Warnungsabfrage wird ausgeführt. Die Auswirkungsberechnung wird nur für Warnungsabfragen im Status „Betrieb“ ausgeführt. Wählen Sie diese Option aus, um diesen Service zu verwenden. Wenn Sie vorkonfigurierte Optionen für diese Kategorie angepasst haben, wählen Sie die Option aus, deren Wert auf 1 festgelegt ist. Ereignismanagement berechnet die Auswirkung nur auf die verwendeten Services. Wenn Sie diesen Service jetzt nicht verwenden möchten, wählen Sie eine der folgenden Optionen: • **Nicht Funktionsfähig** : Die Warnungsabfrage ist nicht verfügbar, deaktiviert oder ausgefallen. • **Reparatur wird ausgeführt** : Die Warnungsabfrage wird gewartet. • **DR-Standby** : Die Warnungsabfrage ist als Notfallwiederherstellungs-Standby (DR) verfügbar. • **Bereit** : Die Warnungsabfrage ist für die Verwendung vorbereitet. • **Stillgelegt** : Die Warnungsabfrage wird aus der aktiven Verwendung zurückgezogen.
Kommentare	Zusätzliche Hinweise und Informationen.
Servicegruppenmitglieder	Die Servicegruppe, die diesen Service enthält.
Filter	Die Bedingungen für das Senden einer Benachrichtigung an die Warnungsabfrage. Die Bedingungen müssen die Warnungswerte erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsabfrageformular (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Wenn Sie einen Warnungsabfragefilter definieren, beziehen Sie nur Felder ein, die in der Tabelle „Warnungsverläufe“ [em_Alert_history] angezeigt werden. Die Auswirkungsberechnung basiert auf Warnungsverlaufsdaten und Feldern wie Gesamtereignisanzahl, Priorität und Prioritätsgruppe werden nicht in die Tabelle „Warnungsverläufe“ [em_Alert_history] kopiert. • Geben Sie keine dynamische Zeitbedingung an. Geben Sie beispielsweise im Filter nicht an Erstellt Bedingung von Letzte 45 MinutenDa die Auswirkungsberechnung durch eine Änderung der Warnung oder Warnungsabfrage ausgelöst wird. Für die dynamische Zeitbedingung hat sich jedoch keine dieser Bedingungen geändert. • Einige Filter können die Auswirkungsberechnung verlangsamen. Um dieses Problem zu lösen, passen Sie Ihre Warnungsabfrage an, indem Sie einen entsprechenden Index hinzufügen, wie in beschrieben Indizieren Sie Vorschläge für langsame Abfragen .

Formular für Warnungskorrelationsregel

Verwalten Sie die Felder, die definieren, wie Warnungen korreliert und gruppiert werden.

Formular für Warnungskorrelationsregel

Feld	Beschreibung
Name	Name der Korrelationsregel.
Reihenfolge	Die Auswertungspriorität für die Regel. Regeln mit niedrigeren numerischen Werten erhalten eine höhere Priorität. Eine Warnung wird für jede Warnungsaktionsregel ausgewertet, bis eine Übereinstimmung gefunden wird. Wenn Sie beispielsweise zwei Warnungskorrelationsregeln mit den Prioritäten 10 und 20 haben, wird die Regel mit Priorität 10 zuerst ausgewertet. Wenn eine Warnung den Kriterien der Regel mit Priorität 10 entspricht, werden keine weiteren Regeln überprüft. Wenn sie nicht übereinstimmt, wird die Warnung anhand der Regel mit Priorität 20 ausgewertet.
Aktiv	Option zum Aktivieren oder Deaktivieren der Regel.
Erweitert	Option zum Wechseln in den erweiterten Modus, mit dem Sie anwenderdefinierte Skripts verwenden können, um Ihre eigene Logik zu definieren. Die Beispielkorrelationsregel **BEISPIEL FÜR Warnungskorrelationsregel**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung
	, Wird sofort als Referenz bereitgestellt. Sie können das verfügbare Skript als Leitfaden verwenden. **Hinweis:** Die **Filter** Bedingung gibt an, für welche Warnungen die Regel gilt. Stellen Sie sicher, dass im erweiterten Skript dieselbe Bedingung verwendet wird, um Warnungen zu identifizieren, die in die Gruppe aufgenommen werden sollen.
Beschreibung	Eine Beschreibung der Regel.
Primäre Warnung	Die Filterbedingung, welche die primäre (bzw. wichtigste) Warnung in einem Satz zugehöriger Warnungen identifiziert. Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.
Sekundäre Warnung	Die Filterbedingung, welche die zur primären Warnung zugehörige Warnung von geringerer Bedeutung identifiziert. Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.
Filter	Die Filterbedingung, welche die Warnung identifiziert, für die das Skript ausgeführt wird. **Filter** ist nur verfügbar, wenn **Erweitert** ausgewählt ist. Bei Filterparametern wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. Um die Unterscheidung zwischen Groß- und Kleinschreibung zu deaktivieren, setzen Sie den *sa_analytics.correlation_case_sensitive*-Parameter auf **false**.
Beziehungstyp	Geben Sie den Beziehungstyp zwischen der primären und sekundären Warnung an: • **Keine Beziehung**: Die Beziehung wird ignoriert, wenn Sie nach einer Übereinstimmung suchen. • **Gleiches CI oder gleicher Knoten**: Beziehen Sie beide Warnungen auf dasselbe CI. Wenn das CI-Feld leer ist, müssen die Warnungen denselben Knotenwert haben. • **Primär ist übergeordnet** : Verknüpfen Sie die Warnungen, bei denen die primäre Warnung das übergeordnete Element in einer über-/untergeordneten Beziehung ist, wie in der Tabelle „CI-Beziehungstypen“ [cmdb_rel_ci] beschrieben. • **Primär ist untergeordnet** : Verknüpfen Sie die Warnungen, bei denen die primäre Warnung das untergeordnete Element in einer untergeordneten Beziehung ist, wie in der Tabelle „CI-Beziehungen“ [cmdb_rel_ci] beschrieben. Dieses Feld wird nicht angezeigt, wenn **Erweitert** Das Kontrollkästchen ist aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung
Zeitunterschied in Minuten	Die Zeitspanne in Minuten, in denen das primäre und das sekundäre Event eintreten müssen, damit diese Regel erfüllt wird. Der Standardwert beträgt 60 Minuten. **Hinweis:** Der Wert für diesen Eintrag kann nicht größer sein als 1440 Minuten (ein Tag). Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.

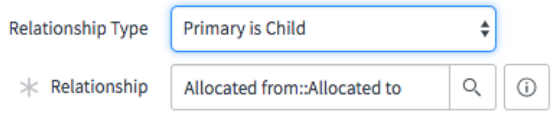
Skript	Ein benutzerdefiniertes Skript, durch dessen Bearbeitung Sie eine JSON-Zeichenfolge zurückgeben können, welche die primären und sekundären Warnungen angibt.
	
	Wählen Sie **Erweitert** aus, um das Skript-Feld anzuzeigen.
	
	`(/* The function needs to return a JSON-{correlationType:[correlatedAlerts]}`
	`for example: if your filter matches the alert, set the alert as the primary alert and set alerts 1, 2 and 3 each as secondary alerts.`
	
	`You can use both multiple primary alerts and multiple secondary alerts.`
	`The correlationType can be PRIMARY or SECONDARY, and the alerts ID must be in an array.`
	`CurrentAlert is the GlideRecord of the currentAlert on which that rule runs.`
	`The system supports only one primary per alert, so:`
	`Do not correlate more than one alert under the PRIMARY array.`
	`Do not correlate alerts that already have a primary under the SECONDARY array.`
	`The system supports open alerts only, so do not correlate alerts that have been closed under either one of the arrays.`
	`*/`
	
	`(function findCorrelatedAlerts(currentAlert){`
	
	`var result = {}; //Insert your code here`
	`result = {'SECONDARY':['alertID1','alertID2','alertID3']};`
	`return JSON.stringify(result);`
	
	`})(currentAlert);`

Beziehung	Beschreibung der CI-Beziehung zwischen den primären und sekundären Elementen, z. B. *`Zugeordnet von::Zugeordnet an`* oder *`Zugeordnet an::Zugeordnet von`*. Dieses Feld wird nur angezeigt, wenn entweder **Primäres Element ist übergeordnet** oder **Primäres Element ist untergeordnet** als **Beziehungstyp** ausgewählt ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung
	 Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.

Health Log Analytics

Mithilfe der Anwendung ServiceNow® Health Log Analytics können Sie IT-Probleme vermeiden, bevor Benutzer durch sie beeinträchtigt werden. Sie hilft Ihnen, die Ursache eines Problems zu identifizieren, indem Sie zugehörige Protokolle selektieren und die Rohdaten analysieren.

Health Log Analytics sammelt Streaming-Rohdaten in Ihrer Instanz und strukturiert Textdaten in Schlüssel-Wert-Paaren. In den Daten werden aussagekräftige Muster erkannt, und wenn eine Anomalie entdeckt wird, wird ein Event an die Anwendung Ereignismanagement gesendet.

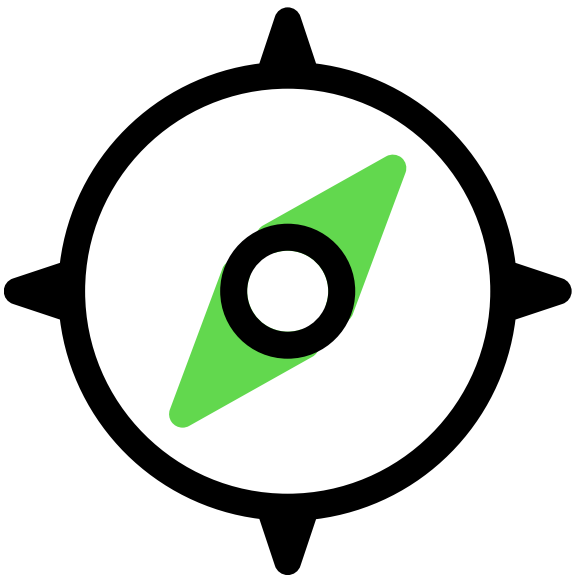
Health Log Analytics Ist in verfügbar ServiceNow Store an.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

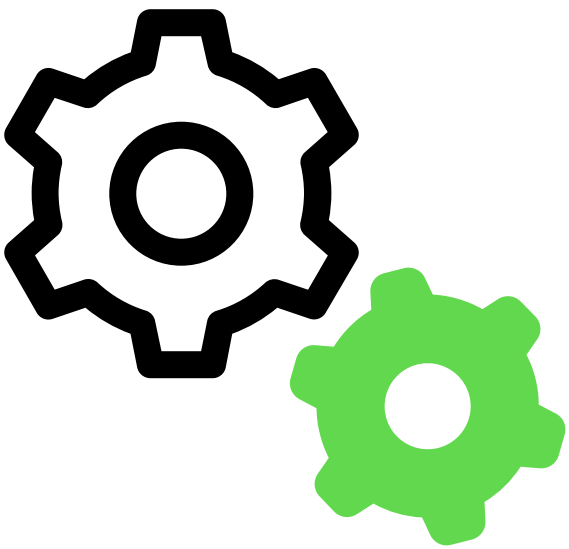
Erste Schritte

Untersuchen



Erkunden Health Log Analytics Workflow, Architektur und allgemeine Aufgaben.

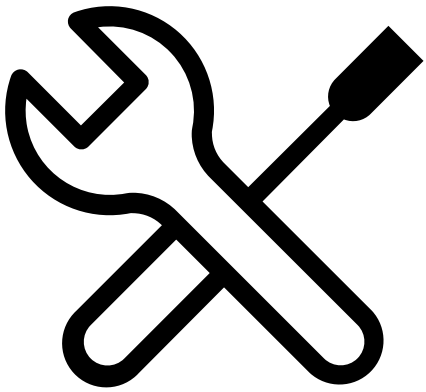
Konfigurieren



Konfigurieren Health Log Analytics Setup- und Konfigurationsaufgaben.

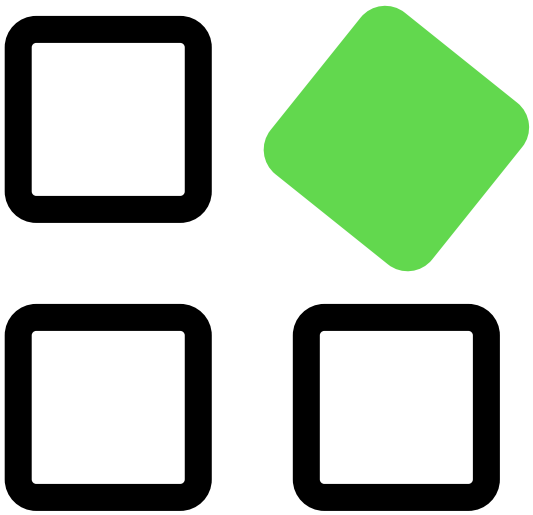
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beheben



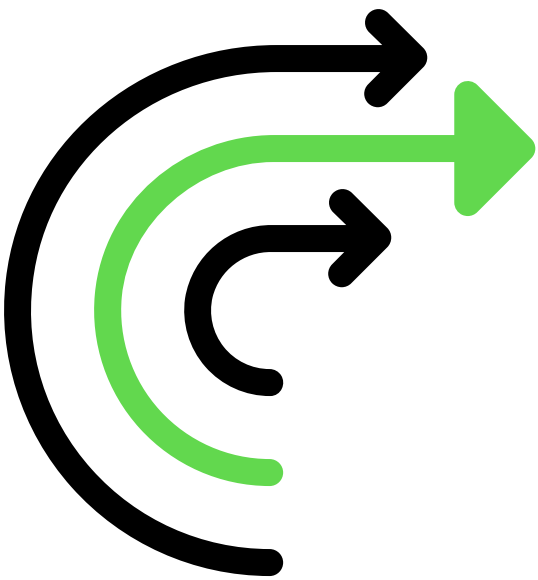
Untersuchen Sie Protokolldaten, und ergreifen Sie Maßnahmen, um das zugrunde liegende Problem zu beheben.

Kontrolle



Beeinflussen Sie, wie HLA Warnungen generiert und priorisiert und Anomalien erkennt.

Systemfunktionen und Integritätswarnungen



Zeigen Sie Systemfunktionen und Kernkomponenten mit zugehörigen Systemintegritätswarnungen an.

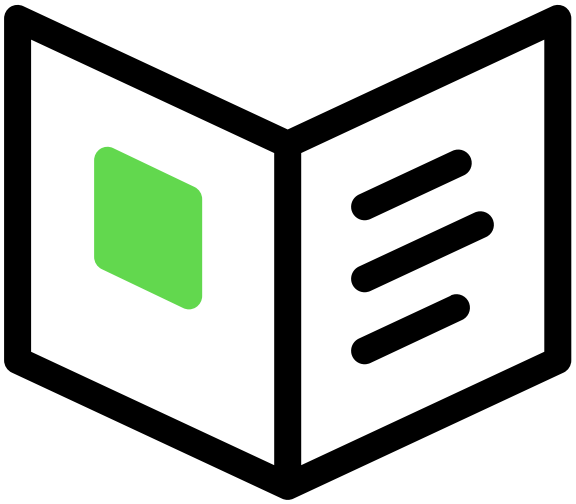
Analytics und Berichterstellung

Erhalten Sie Einblicke in die Anzahl der Probleme, die vorhergesagt wurden, bevor Anwender betroffen waren, und das Geld, das gespart wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Suchen Sie Referenzinformationen zu Health Log Analytics.

Automatische Übersetzung

Health Log Analytics Lizenzierung

Bei der für ServiceNow AI Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von Health Log Analytics, Die als separate Lizenz von verfügbar ist ITOM-Integrität. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung Und -Abonnements.

Abhängigkeiten

Für eine Liste von Health Log Analytics Plugin-Abhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für In ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Health Log Analytics erkunden

ServiceNow Health Log Analytics Prognostiziert IT-Probleme, bevor sie sich auf Ihre Anwender auswirken, indem maschinell generierte Protokolldaten in Echtzeit erfasst, analysiert und korreliert werden. Es erkennt Anomalien und warnt Sie vor potenziellen Problemen.

Health Log Analytics – Übersicht

Health Log Analytics Empfängt und verarbeitet normalerweise Protokolldaten und sendet Ereignisse an ServiceNow Ereignismanagement. Die Anwendung erkennt Anomalien, sobald

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sie auftreten, und hilft Ihnen, die Ursache eines Problems zu identifizieren, indem Sie zugehörige Protokolle selektieren und die Rohdaten analysieren können.

Health Log Analytics kann jede Art von maschinell generierten Textprotokolldaten verarbeiten, einschließlich Anwendungs-, Infrastruktur- und Netzwerkprotokolle sowie andere Arten von Textprotokolldaten. Configuration Management Database (CMDB) kann zwar nützlich sein, um hochwertige Events und Warnungen zu generieren, dies ist aber nicht erforderlich.

Hinweis:

- Health Log Analytics Unterstützt nur UTF-8-Protokolle. Binäre Protokolle werden nicht unterstützt.
- Wenn Sie Protokolle in einer anderen Sprache als Englisch senden, ist möglicherweise eine zusätzliche Konfiguration erforderlich.

Health Log Analytics Anwender

Health Log Analytics-Anwender

Anwender	Beschreibung	Rolle
Administrator	Konfiguriert die Health Log Analytics-Anwendung so, dass sie von Operatoren verwendet werden kann. Führt Verwaltungsaufgaben aus, um den effizienten Betrieb des Systems zu gewährleisten.	evt_mgmt_admin, admin
Operator	Analysiert Log Analytics-Warnungen und ergreift Maßnahmen, um das zugrunde liegende Problem zu lösen.	evt_mgmt_operator

Health Log Analytics – Workflow

Health Log Analytics sammelt und verarbeitet automatisch Protokolldaten. Die Daten werden für die Analyse durch die Betreiber strukturiert, und es werden aussagekräftige Warnungen und Vorschläge generiert, die in Ereignismanagement angezeigt werden.

Das Diagramm zeigt den Health Log Analytics-Workflow vom Sammeln der Daten bis zum Senden eines Events oder einer Warnung an Ereignismanagement.

Health Log Analytics-Workflow

Erfassung

Diese Ebene verbindet Ihre Umgebung mit Health Log Analytics. Sie können Ihre Protokolle direkt von Servern und Endpunkten oder aus Protokoll-Repositorys streamen. Das optionale Guided Setup unterstützt Sie beim Erstellen von Dateneingabe-Connectors für die folgenden häufigen Datenquellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rsyslog
- Beats
- Splunk
- Elasticsearch
- MID-Server
- TCP

Strukturierung

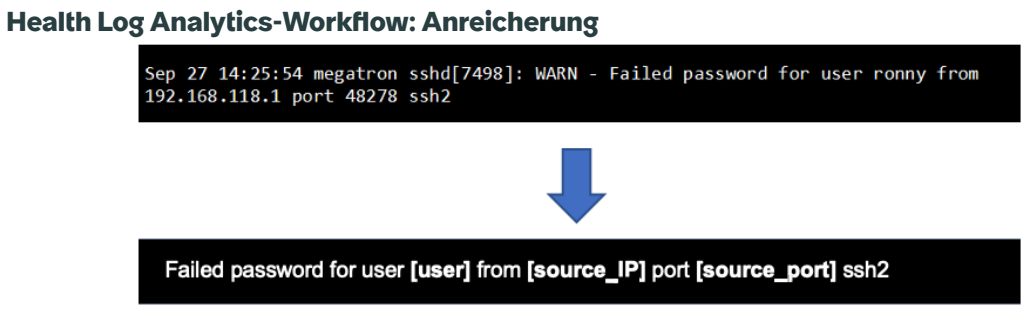
Diese Ebene befasst sich mit der Strukturierung von Protokolldaten und ihrer automatischen Zuordnung zu logischen Silos, die als Komponenten bezeichnet werden. Die Datenstrukturierung kann automatisch oder manuell erfolgen.

Das System strukturiert Protokolldaten automatisch, indem es aus eingehenden Protokollnachrichten die folgenden Eigenschaften extrahiert: Nachricht, Zeitstempel, Host, Schweregrad und externe IDs. Es extrahiert explizite Werte wie „property-name“ und „value is IP“ sowie semantische Werte wie Länge, Anzahl englischer Wörter und Varianz.

Bei der automatischen Zuordnung werden Protokollbeispiele und Metadaten automatisch den entsprechenden Tags zugewiesen. Das System versucht, Protokollzeilen zuzuordnen, indem es die Quelle analysiert, von der die Daten gestreamt werden. Die Zuordnung basiert auf Agent-Hinweisen und allgemeinen Transport-Header-Feldern.

Anreicherung

Auf dieser Ebene geht es um die Identifizierung der variablen Teile einer Protokollnachricht.



Zudem werden Stichwörter und kontextbezogene Eigenschaften identifiziert. Im Bild sind „WARN“ und „Failed“ die zu verfolgenden Stichwörter. „User“, „source IP“ und „port“ sind die kontextbezogenen Eigenschaften.

Analyse

Auf dieser Ebene wird jede Protokollzeile indiziert. Health Log Analytics extrahiert Eigenschaften aus der inneren Protokollnachricht. Diese tragen zu Modellen von dem Verhalten bei, vom dem das System lernt, es zu erwarten. Anomales Verhalten ist Verhalten, das von diesem erwarteten Verhalten abweicht. Sie können nach einem Event und seinen wichtigsten Eigenschaften für die manuelle Fehlerbehebung suchen.

Maschinelles Lernen (ML) und künstliche Intelligenz (KI)

Health Log Analytics nutzt erweiterte, unüberwachte ML-Algorithmen, um Muster in Protokollen zu erkennen und ihr eindeutiges Datenverhalten zu erlernen. Anschließend werden in Echtzeit dynamische Schwellenwerte basierend auf der Datensignatur festgelegt, um Probleme zu erkennen, wenn sie zum ersten Mal auftreten. Wenn das System eine Abweichung vom typischen Muster erkennt, sendet es ein Event an Ereignismanagement.

Warnung in Ereignismanagement

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics sendet Events an Ereignismanagement. In Ereignismanagement werden Health Log Analytics-Warnungen in der Liste **All alerts** (Alle Warnungen) angezeigt. Diese Liste ermöglicht es Betreibern, Warnungen des Events und den Health Log Analytics-Warntyp an einem einzigen Ort anzuzeigen.

Health Log Analytics – Vorteile

Vorteile von Health Log Analytics

Leistung	Funktion	Anwender
Vereinfachen Sie das Setup der Dateneingabe mit dem geführten Setup.	Guided Setup	Administrator
Richten Sie Protokolldaten-Connector-Integrationen schnell und bequem über die ein Integrations Launchpad.	Protokolldaten-Connector-Integrationen	Administrator
Verkürzen Sie die Onboarding-Zeit, indem Sie Inhaltspakete installieren.	Inhaltspakete	Administrator
Sparen Sie Zeit, und reduzieren Sie Fehler, indem Sie Dateneingabekonfigurationen zwischen Instanzen migrieren.	Dateneingabemigrierung	Administrator
Identifizieren Sie die Ursache einer Warnung, indem Sie die Protokolle analysieren, die die Anomalie umgeben.	Surrounding logs (Umgebende Protokolle)	Operator
Visualisieren Sie anomale Protokolldaten im Protokoll-Viewer.	Protokoll-Viewer	Operator
Erkennen Sie Beziehungen in Protokolldaten.	Protokollkorrelatoren	Operator
Weisen Sie Warnungen eine höhere oder niedrigere Bedeutung zu.	Warnungsmetriken stummschalten	Operator
Reduzieren Sie das Rauschen, indem Sie Protokollfilter erstellen.	Warnungsfilter protokollieren	Operator
Beeinflussen Sie wie Health Log Analytics Sucht nach Anomalien, indem Stichwörter verwaltet werden, nach denen in den Protokolldaten gesucht wird.	Lexikalische Stichwörter	Operator
Erstellen Sie Warnungen für angegebene Metriken, indem Sie Regeln hinzufügen, ändern oder löschen.	Benutzerdefinierte Warnungsregeln	Operator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfehlungen für weitere Themen

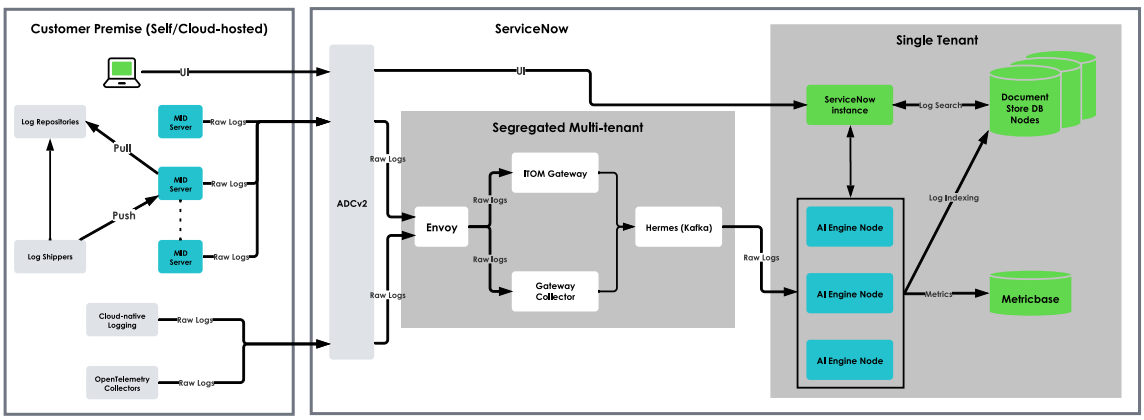
- Health Log Analytics-Architektur
- Wie Health Log Analytics Warnungen generiert

Health Log Analytics-Architektur

Health Log Analytics sammelt Protokolle, die von Endpunkten oder Data Lakes wie Splunk und Elasticsearch in Ihre ServiceNow-Instanz gestreamt werden.

Die ServiceNow Die Instanz empfängt die Protokolle entweder über einen MID-Server Connector-Instanz oder über Aufnahme ohne MID, die die Integration mit Services wie unterstützt AWS Firehose. Health Log Analytics Identifiziert und selektiert Anomalien in Ihren Protokolldaten mithilfe von ML-Modellen (nicht überwachtes maschinelles Lernen). Anschließend werden die Anomalien gruppiert und weitere Algorithmen angewendet, um die Ursache des Problems zu identifizieren.

Health Log Analytics Skalierte Architektur



Wie Health Log Analytics Warnungen generiert

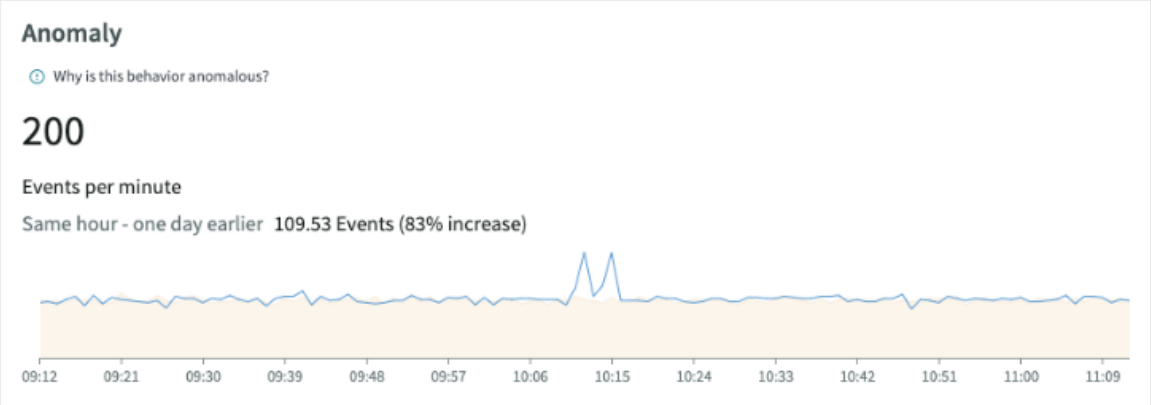
Health Log Analytics Identifiziert Muster in Ihren Protokolldaten und lernt das Musterverhalten. Wenn HLA Die KI-Engine von erkennt anomales Verhalten und sendet ein Ereignis an den ServiceNow Ereignismanagement Anwendung. Als Operator können Sie diese prädiktiven Warnungen verwenden, um neu auftretende IT-Probleme zu behandeln, bevor sie sich auf Anwender auswirken.

Erkennung von Protokollanomalien

Es gibt viele Arten von anomalem (anomalem oder unerwartetem) Verhalten. In diesem Beispiel verfolgt das System die Baselinerate bestimmter Nachrichten (durchschnittliche Anzahl der Events pro Minute). Im Diagramm sind die Werte für den Vortag als hell pfirsichfarben-schattierter Bereich und die Werte für heute als blaue Linie dargestellt. Das Diagramm zeigt eine drastische Abweichung von den erwarteten Baselinewerten ungefähr um 10:10 Uhr. Dieses anomale Verhalten generiert eine Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anomales Verhalten



Health Log Analytics Verwendet verschiedene Methoden, um Anomalien zu erkennen und Warnungen zu generieren.

Warnungsmetriken

Health Log Analytics überwacht mehrere Metriken im Protokollstream, um anomales Verhalten zu erkennen. Jede Metrik ist einer eindeutigen Quelle zugeordnet: Der Kombination aus Serviceinstanz und Komponente. Wenn das System ein anomales Muster für eine Metrik identifiziert, generiert es eine Warnung.

Als Operator können Sie Feedback zu den generierten Warnungen geben. Ihr Feedback „lehrt“ Health Log Analytics Dass eine bestimmte Warnung für Sie bedeutend oder irrelevant ist. Die Anwendung erhöht dann entweder die Priorität der Warnungsmetrik oder schaltet sie stumm, um Rauschen zu reduzieren.

- Eine signifikante Warnung wird wahrscheinlicher in eine Log Analytics-Gruppe aufgenommen, wenn sich die zugehörige Metrik anomal verhält. Weitere Informationen finden Sie unter Markieren Sie eine Warnung in als signifikant Health Log Analytics
- Schalten Sie eine Warnung für eine angegebene Quelle stumm, um störende neue Warnungen für unwichtige Probleme zu vermeiden. Wenn eine Metrik stummgeschaltet wird, entfernt Health Log Analytics die aktuelle Warnung und alle anderen Warnungen basierend auf dieser Metrik aus dem Feed. Außerdem werden keine neuen Warnungen aus dieser Metrik mehr generiert. Weitere Informationen finden Sie unter Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics.
- Wenn sich die Situation ändert, können Sie eine signifikante Metrik auf ihre Standardbedeutung zurücksetzen. Sie können auch eine stummgeschaltete Metrik reaktivieren, damit das System erneut Warnungen generiert. Weitere Informationen finden Sie unter Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics.

Lexikalische Stichwörter

Health Log Analytics durchsucht Ihre Protokolle nach Wörtern, die auf wichtige Probleme hinweisen können. Lexikalische Stichwörter wie „Crash“ oder „Failed“ weisen auf eine Bedingung hin, die der Aufmerksamkeit bedarf.

Das System legt für jedes lexikalische Stichwort einen Schwellenwert fest, der auf den Werten basiert, die es als normales Vorkommensmuster und normale Häufigkeit dieses Stichworts in Ihren Protokollen betrachtet. Beim Scannen Ihrer Protokolle werden alle Vorkommen des Stichworts gefunden. Wenn die Anzahl den Schwellenwert überschreitet,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird eine Warnung generiert. Weitere Informationen finden Sie unter Zeigen Sie die lexikalischen Stichwörter an, die Warnungen in generieren Health Log Analytics.

Weitere Informationen über die Verwaltung globaler Stichwörter finden Sie unter Fügen Sie lexikalische Stichwörter in hinzu, bearbeiten oder löschen Sie sie Health Log Analytics. Informationen zum Erstellen oder Löschen von Stichwörtern für einen bestimmten Quelltyp finden Sie unter Konfigurieren Sie Quelltypfähigkeiten in Health Log Analytics.

Korrelationen

Protokollkorrelatoren sind Schlüssel oder Werte in Protokolldaten, die Korrelationen zwischen Warnungen erkennen. Beispielsweise könnte ein Protokollkorrelator erkennen, wenn die ID eines bestimmten Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Serviceinstanzen auftritt. Weitere Informationen finden Sie unter Identifizierung zugehöriger Warnungen in Protokolldaten mithilfe von Protokollkorrelatoren.

Erweiterte Warnungsfilterung

Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren. Weitere Informationen finden Sie unter Erweiterte Protokollwarnungsfilter erstellen.

Benutzerdefinierte Warnungsregeln

Definieren Sie eine Log Analytics-Warnungsregel, wenn Protokolldaten angezeigt werden, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für eine angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest. Weitere Informationen finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

Typen von Health Log Analytics Warnungen

Health Log Analytics Generiert mehrere Arten von Warnungen.

In einer Liste von Warnungen weisen alle von Health Log Analytics generierten Warnungen in der Spalte **Source** (Quelle) den Wert **Log Analytics** (Protokollanalytik) auf. Der Wert in der Spalte **Group** (Gruppe) identifiziert wie folgt die Art der Warnung:

Komponentenbasierte Warnung

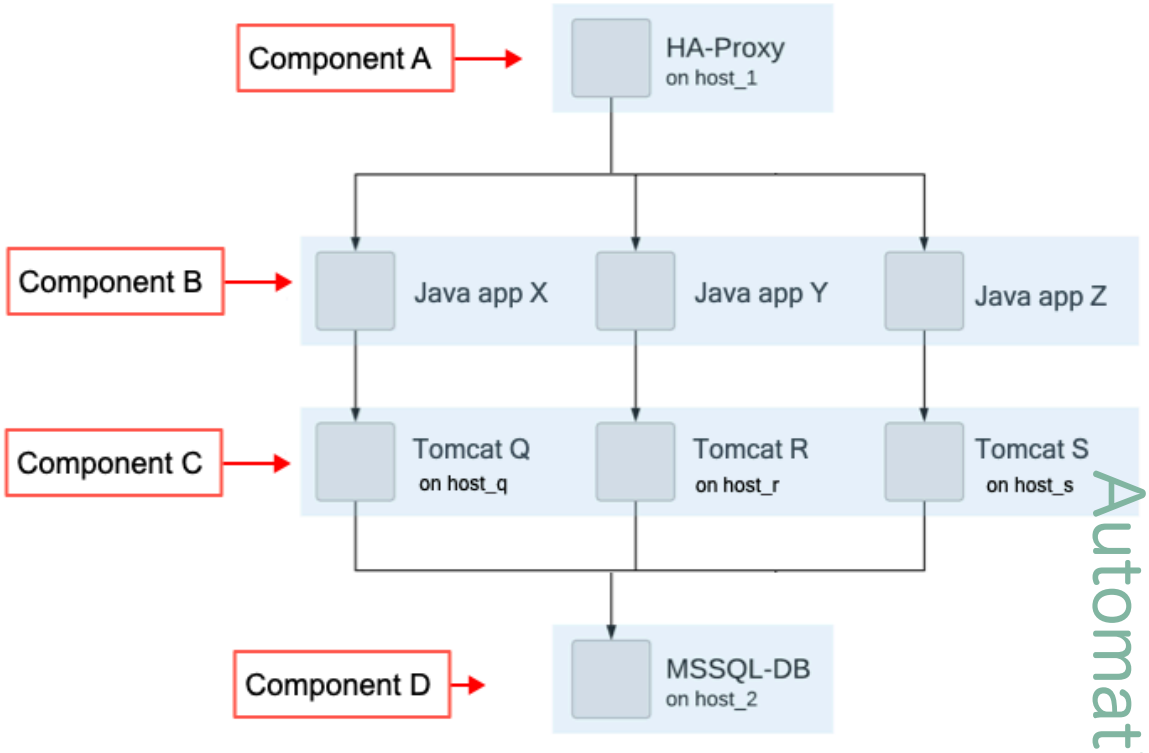
Komponentenbasierte Warnungen betreffen mehr als ein Configuration Item (CI). A *Komponente* Ist eine logische Komponente einer Serviceinstanz, die die Warnung verursacht hat. Eine Komponente kann mehrere CIs umfassen, die dieselbe Funktion ausführen, z. B. mehrere redundante Hosts.

> **Wichtig:** Jede Komponentenbasierte Warnung ist das übergeordnete Element einer Reihe von schreibgeschützten Warnungen. Sie arbeiten nicht direkt mit schreibgeschützten Warnungen. Sie arbeiten nur an der übergeordneten Komponentenbasierte Warnung.

In dieser Beispielserviceinstanz bilden die identischen Java-Apps X, Y und Z eine einzelne Komponente: Komponente B. Tomcat-Server Q, R und S und ihre Hosts bilden eine andere einzelne Komponente: Komponente C.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Serviceinstanz



Log Analytics-Warnung

Eine Log Analytics-Warnung identifiziert eine Anomalie, die ein einzelnes CI betrifft. Eine Log Analytics-Warnung weist in der Spalte **Group** (Gruppe) den Wert **None** (Keine) auf. Die Anomalie, die zur Warnung führt, kann eine unerwartete Anzahl von Protokolleinträgen oder ein unerwarteter Wert einer Metrik sein.

Log Analytics-Gruppe

Wenn das System mehrere Log Analytics-Warnungen identifiziert, die auf wichtige Weise miteinander verknüpft sind, werden sie in einem gruppiert Log Analytics-Gruppe. Eine Log Analytics-Gruppe kann bis zu vier Warnungen gruppieren. Das System generiert eine Log Analytics-Gruppe, wenn die Log Analytics-Warnungen eine oder mehrere der folgenden Beziehungen gemeinsam haben:

- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Hinweis: Sie können eine Warnung als signifikant markieren. Eine signifikante Warnung ist wahrscheinlicher in enthalten Log Analytics-GruppeWenn sich die zugeordnete Metrik anomal verhält. Weitere Informationen finden Sie unter Markieren Sie eine Warnung in als signifikant Health Log Analytics.

Typen von anomalem Verhalten in Health Log Analytics

Anomales Verhalten in einem CI oder einem Service kann auf ein wichtiges Problem hinweisen. Zum Beispiel kann eine Spitze in der Häufigkeit oder Anzahl von Nachrichten eines bestimmten Typs auf ein Problem hinweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anomalien interpretieren

So erstellen Sie Modelle des erwarteten Verhaltens: Health Log AnalyticsÜberwacht den Protokollstream, um Baselines für Muster, Metriken und Anzeigen über verschiedene Zeiträume zu lernen. Zeiträume können stündlich, täglich, wöchentlich oder unbegrenzt sein. Verhalten, das von den erlernten Modellen abweicht, wird als anomales Verhalten betrachtet.

Typen der Protokolleigenschaft

Muster

Ein Muster ist ein Wert oder eine Rate, die sich wiederholt # in Text, Zeit oder Beziehungen.

Zähler

Eine Zählereigenschaft ist ein numerischer Wert oder Textwert. Beispiele: Statuscode, Antwortcode, Aktion oder Muster.

Anzeige

Eine Anzeigeneigenschaft besitzt einen numerischen Wert, der kontinuierlich gemeldet wird. Anzeigeneigenschaften stellen Vorgänge dar, die Ressourcen verbrauchen. Beispiele: CPU-Auslastung, Speicherauslastung oder Antwortzeit

Wie Anomalien in angezeigt werden Health Log Analytics

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

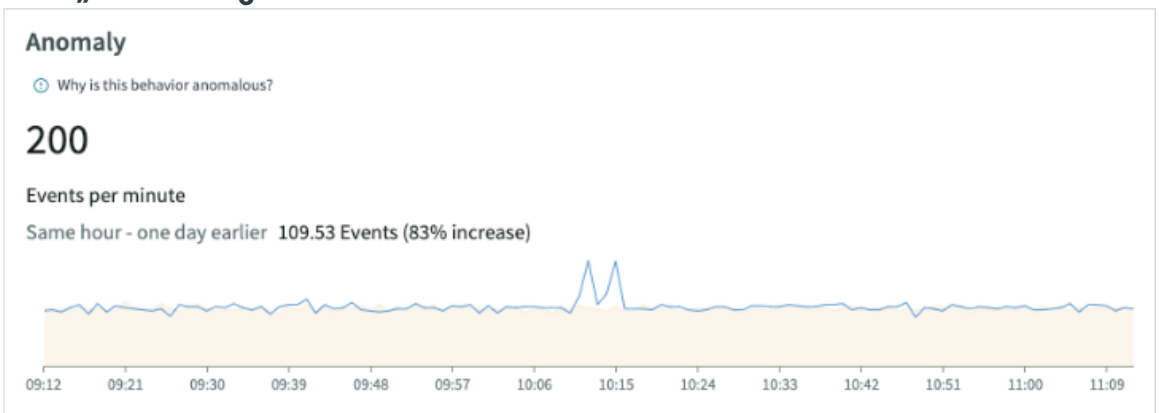
- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Anomalien

Einige der Anomaliearten

Verhalten	Beschreibung
Neues Verhalten	Bisher unbekanntes Muster. Für den Warnungstyp „Neues Verhalten“ wird kein Diagramm angezeigt.
Signal inaktiv/Wird nicht mehr angezeigt	Alle Muster- oder Protokolldaten aus einer Quelle wurden angehalten. Kein Signal für mindestens fünf Minuten.
Signal aktiv/Wird wieder angezeigt	Muster- oder Protokolldaten aus einer „toten“ Quelle werden erneut angezeigt. Bei einer Baseline von einer Stunde ist ein Muster „inaktiv“, wenn es weniger als einmal pro Minute erscheint.
Anomalie über oder unter Durchschnitt	Aktivität, die vom erwarteten Baselineverhalten für Muster-, Zähler- oder Messmetriken abweicht (z. B. Stichwort- oder Schweregradmetriken).
Anstieg oder Sinken einer Baselinereferenz	Eine Erhöhung/Verringerung des Werts oder der Quantität einer Protokolleigenschaft im Vergleich zur Baseline von einer Stunde oder einer Woche.
Korrelation von Schweregrad- und Stichwortwarnungen	Quantitaver Anstieg eines Schweregrads oder Stichworts

Health Log Analytics konfigurieren

Richten Sie als Administrator ein, und konfigurieren Sie Health Log Analytics Damit Operatoren verwenden und Administrationsaufgaben ausführen können, um sicherzustellen, dass das System effizient läuft.

Konfiguration – Übersicht

Führen Sie die folgenden Aufgaben aus, um ein erfolgreiches Setup und eine erfolgreiche Konfiguration von durchzuführen Health Log Analytics.

Wichtig: Unabhängig davon, wie Sie implementieren Health Log Analytics, Für die Protokolldatenerfassung über ein MID-Server Sie müssen zuerst konfigurieren Systemanforderungen des MID-Servers Und stellen Sie sicher, dass die MID-Server Protokollerfassungsfunktion ist aktiviert.

Für MID-Server Proxy-Anforderungen, siehe MID-Server Proxy-Voraussetzungen für das Streaming von Protokollen an Health Log Analytics.

1. Installieren Health Log Analytics(HLA).

   Installieren Sie die Anwendung Health Log Analytics.

2. Richten Sie Protokolldateneingaben für das Streaming von Rohprotokollnachrichten an ein ServiceNow Instanz.

   Verwenden Sie eine der folgenden Methoden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Richten Sie Integrationen für ein Health Log Analytics Von Integrations Launchpad.

  Es wird empfohlen, Dateneingabeintegrationen über einzurichten Integrations Launchpad, Die eine einheitliche Schnittstelle für eine bequeme Integration bietet.

- Richten Sie Dateneingaben in ein Health Log Analytics Mit geführtem Setup.
- Richten Sie Dateneingaben in ein Health Log Analytics Manuell.

3. Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.

   Identifizieren und beheben Sie Protokoll-Streaming-Probleme, um sicherzustellen, dass die von Ihnen konfigurierten Dateneingaben Daten ordnungsgemäß an Ihre Instanz streamen.

4. Bearbeiten Sie Rohprotokolldaten vor der Verarbeitung in Health Log Analytics.

   Ändern Sie Rohprotokollnachrichten, bevor sie in verarbeitet werden MID-Server, Und daher vor Health Log Analytics Ordnet sie zu und strukturiert sie.

5. Ordnen Sie Rohprotokolldaten in zu Health Log Analytics.

   Ordnen Sie Rohprotokolldaten zu, die in Ihre Instanz gestreamt werden, um zu bestimmen, wie die Daten behandelt werden.

   Health Log Analytics Versucht es automatische Zuordnung Jede eingehende Protokollzeile an das richtige Tag. Wenn Eigenschaften nicht automatisch erkannt werden, können Sie die Dateneingabequellen manuell zuordnen.

6. Verfeinern Sie die Quelltypstruktur in Health Log Analytics.

   Feintunen Sie, wie Health Log Analytics Ihre inneren Protokollnachrichten liest und Anomalien erkennt, indem Sie die extrahierten Eigenschaften in der Quelltypstruktur anpassen.

   Mit Health Log Analytics können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern. Diese Anpassungen helfen dem maschinellen Lernen des Systems, Ihre Prioritäten besser zu verstehen.

7. Führen Sie zusätzliche Setup-Aufgaben für die Dateneingabe aus .

   Nachdem Sie das Setup und die Konfiguration der obligatorischen Dateneingabe durchgeführt haben, können Sie mit optionalen Setup-Aufgaben fortfahren.

8. Führen Sie Konfigurationsaufgaben für erweiterte Dateneingaben aus .

Installieren Health Log Analytics(HLA)

Installieren Health Log Analytics Durch Anforderung ServiceNow HLA-Installation von ServiceNow Kundensupport.

Vorbereitungen

Die minimale Version der ServiceNow AI Platform, die zur Installation von Health Log Analytics benötigt wird, ist Zurich.

Wichtig: Health Log Analytics Verwendet den Standardanwender sn_occ_occultus für die interne Kommunikation. Stellen Sie sicher, dass dieser Anwender aktiv ist, und deaktivieren Sie ihn nicht.

Erforderliche Rolle: Administrator

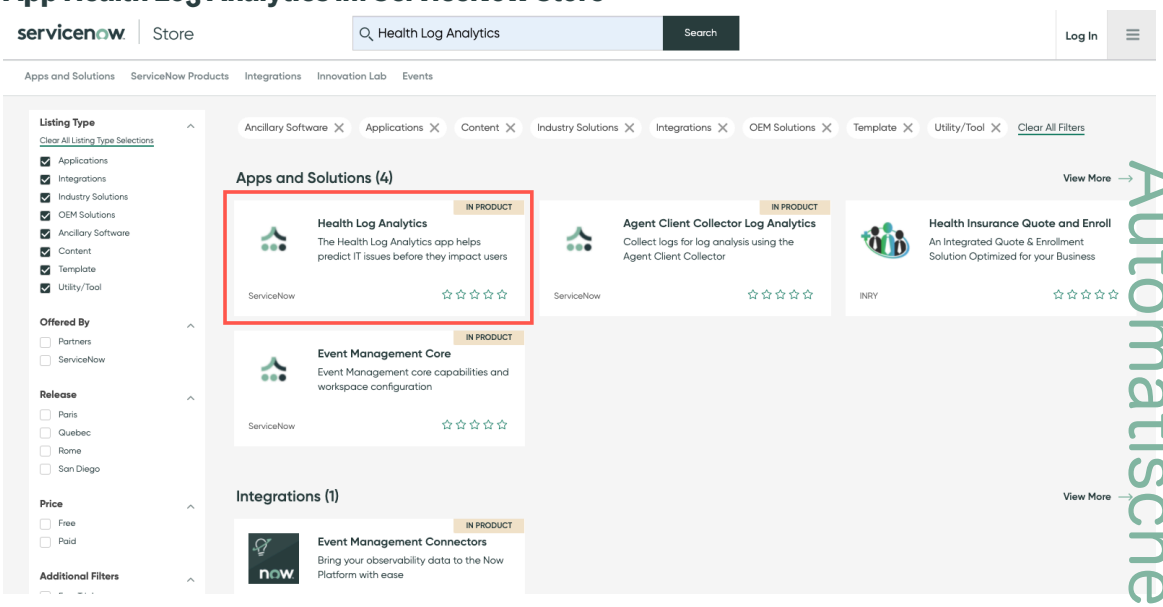
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Vergewissern Sie sich, dass die Anwendung Health Log Analytics und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen.
   Um Berechtigungen zu erhalten, wenden Sie sich an Ihren ServiceNow-Lösungsberater.
2. Melden Sie sich für das Produkt ITOM-Integrität an.

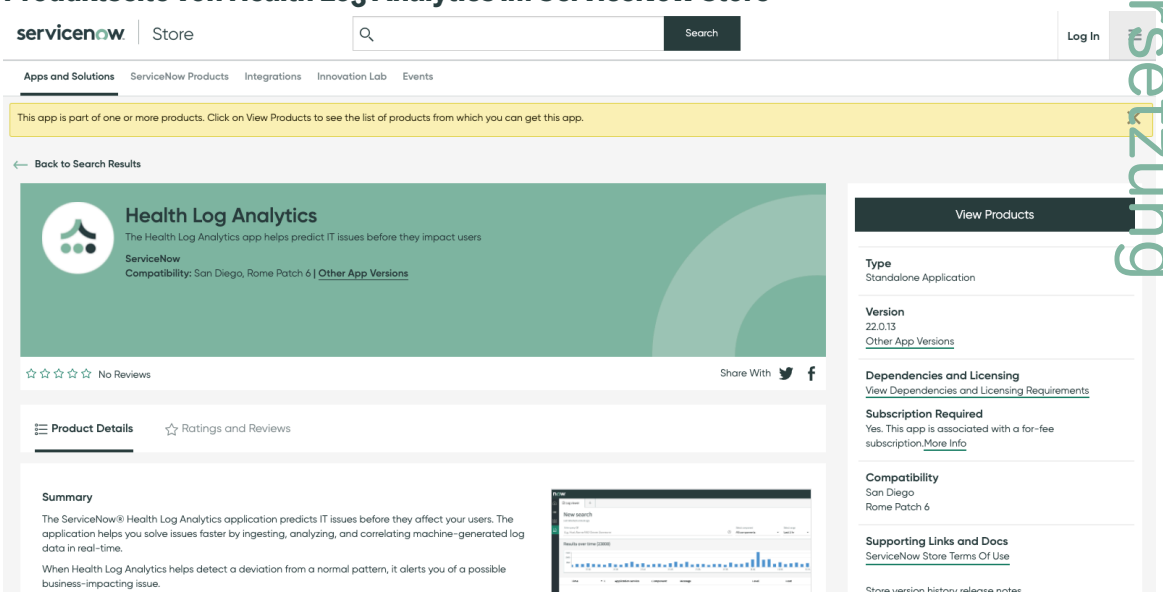
   a. Wechseln Sie zu ServiceNow Store Website und suchen Sie nach Health Log Analytics App.

App Health Log Analytics im ServiceNow Store



   b. Wählen Sie Health Log Analytics aus.
   Die Produktseite von Health Log Analytics wird angezeigt.

Produktseite von Health Log Analytics im ServiceNow Store



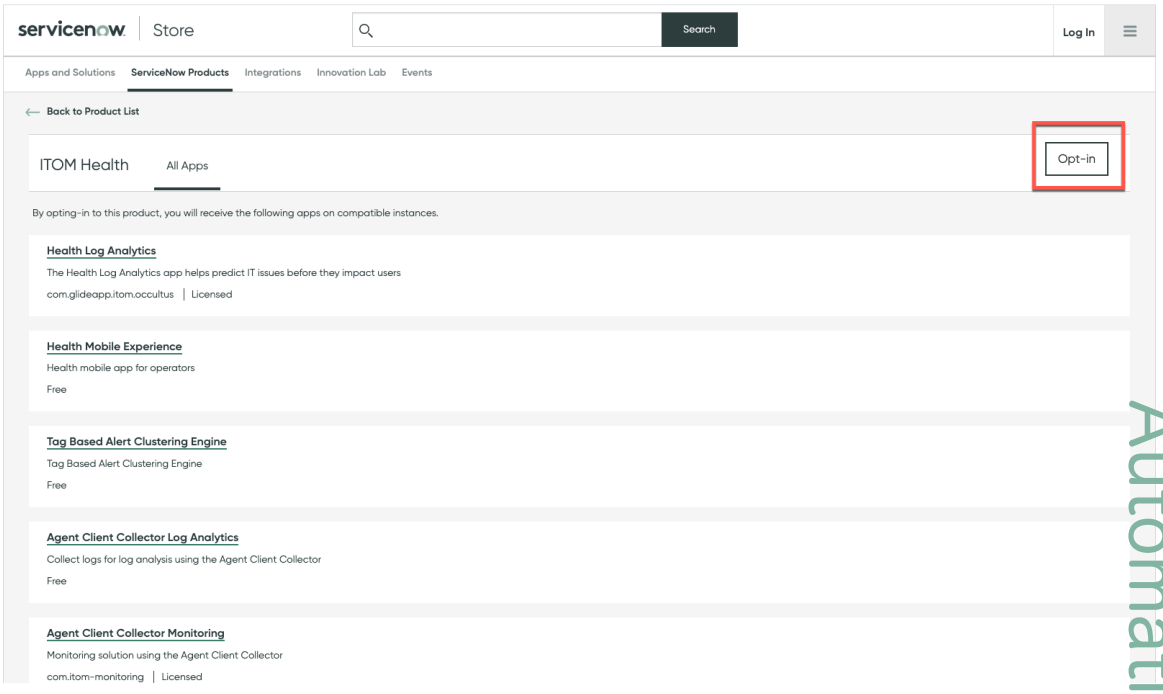
   c. Wählen Sie **Produkte anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Aktivieren**.

Produkt ITOM Health



3. Installieren Sie die Anwendung Health Log Analytics in Ihrer Instanz.

a. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.

b. Suchen Sie die Anwendung Health Log Analytics über die Suchleiste.

c. Wählen Sie auf der Kachel Health Log Analytics die Option **Installieren**.
Wenn die Anwendung erfolgreich in der Instanz installiert wurde, wird eine automatische Change-Anforderung (CHG) ausgelöst, um die Bereitstellung für die erforderlichen Endpunkte anzufordern. Der Instanzadministrator erhält die Anforderung und alle relevanten Benachrichtigungen.

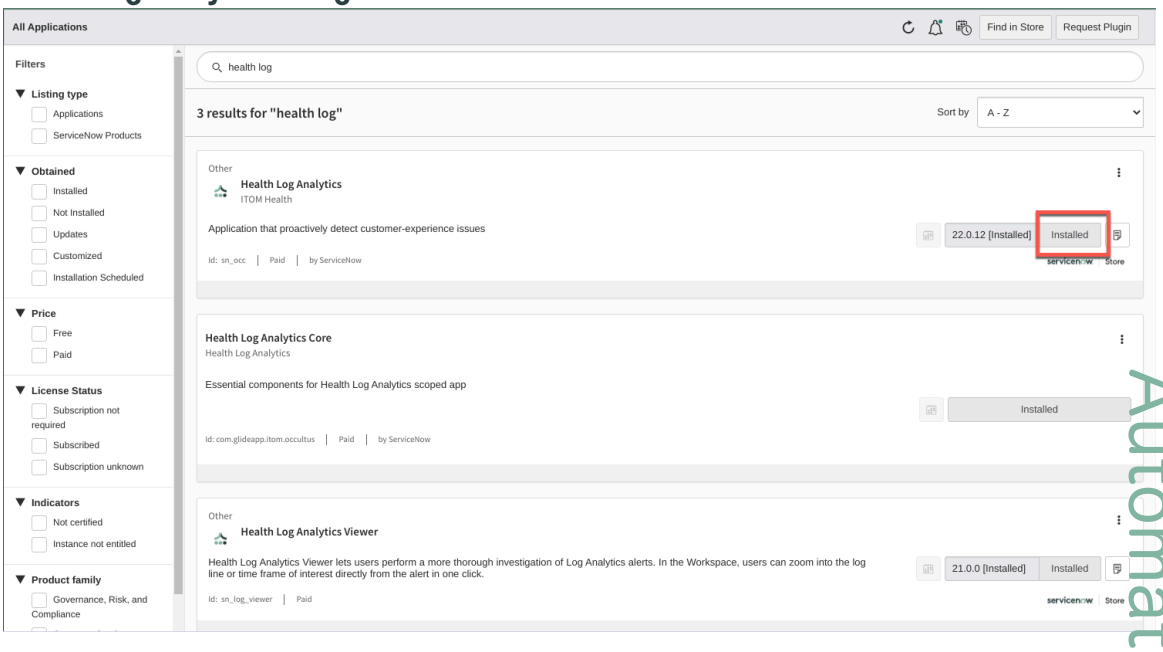
Hinweis: Selbst wenn die Anwendung Health Log Analytics erfolgreich installiert wurde, funktioniert sie erst, nachdem die Endpunkte bereitgestellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Stellen Sie sicher, dass die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden (siehe Abbildung).

Health Log Analytics erfolgreich in der Instanz installiert



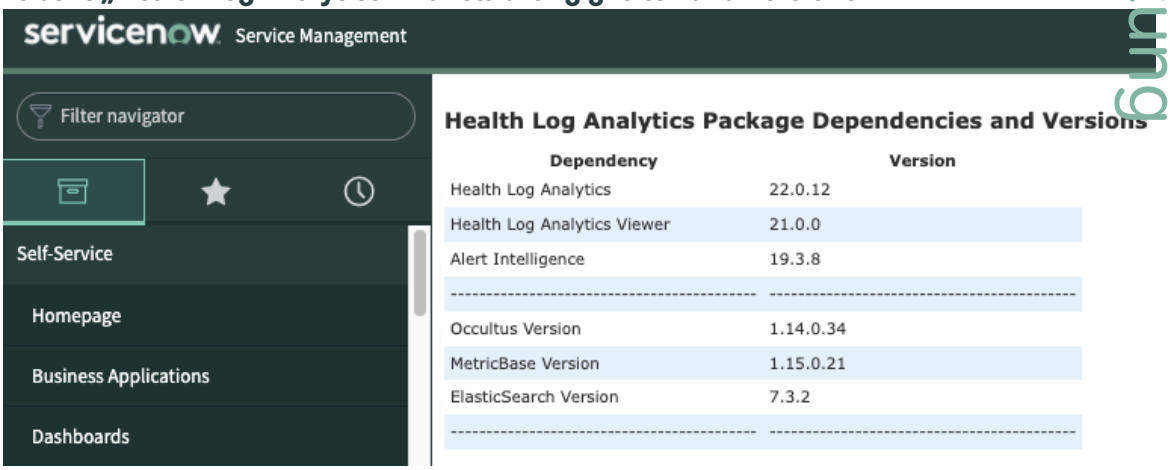
4. Wahlweise: Beobachten Sie den Status des Bereitstellungsprozesses, indem Sie die CHG überprüfen.

Hinweis: Einige Schritte im Bereitstellungsprozess erfordern möglicherweise Ihre explizite Genehmigung. In solchen Fällen wird sich der ServiceNow-Kundensupport mit Ihnen in Verbindung setzen.

5. Stellen Sie nach Abschluss der Bereitstellung sicher, dass die Anwendung Health Log Analytics ausgeführt wird.

a. Geben Sie im Filternavigator `sn_occ_stats.do` ein.
Die Tabelle „Health Log Analytics # Paketabhängigkeiten und Versionen“ wird angezeigt.

Tabelle „Health Log Analytics – Paketabhängigkeiten und Versionen“



Die bereitgestellten Endpunkte werden zusammen mit ihrer Versionsnummer aufgelistet:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Occultus
- MetricBase
- ElasticSearch

Ergebnis
Die Anwendung Health Log Analytics wird in Ihrer Instanz installiert und bereitgestellt.

Nächste Maßnahme

- Richten Sie den Dateneingabeprozess für Health Log Analytics ein.
- (Optional) Installieren Sie das Plugin „ServiceNow® Agent Client Collector Log Analytics“ (ACC-L).

  Agent Client Collector Log Analytics ermöglicht es Ihnen, Protokolldaten von Linux- und Windows-Hosts mit Agent Client Collector an eine ServiceNow-Instanz zu streamen. Weitere Informationen finden Sie in der Dokumentation zu Agent Client Collector Log Analytics.

Einrichten Health Log Analytics Auf Ihrem ServiceNow Instanz

Implementieren Health Log Analytics Auf Ihrem ServiceNow Instanz.

Wichtig:

- Installieren Health Log Analytics In Ihrer Instanz vor der Implementierung. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Unabhängig davon, wie Sie implementieren Health Log Analytics, Müssen Sie konfigurieren Systemanforderungen des MID-Servers Und stellen Sie sicher, dass die MID-Server Protokollerfassungsfunktion ist aktiviert.

  Für MID-Server Proxy-Anforderungen, siehe MID-Server Proxy-Voraussetzungen für das Streaming von Protokollen an Health Log Analytics.

Dateneingaben werden eingerichtet

Es wird empfohlen, Dateneingaben mit zu integrieren Health Log Analytics Von Integrations Launchpad. Dieses Tool bietet eine einheitliche Schnittstelle für die bequeme Integration mit Connectors, die Rohprotokollnachrichten aus externen Quellen zur Verarbeitung und Analyse in Ihre Instanz einspeisen. Weitere Informationen finden Sie unter Richten Sie Integrationen für ein Health Log Analytics Von Integrations Launchpad.

Alternativ können Sie Dateneingaben auf eine der folgenden Arten einrichten:

- Mit geführtem Setup. Das geführte Setup bietet eine Reihe von Aufgaben, mit denen Sie Dateneingaben für konfigurieren können ServiceNow Instanz. Durch die Verwendung des Guided Setups wird sichergestellt, dass Sie über das erforderliche Mindestsetup für den Dateneingabeprozess verfügen. Weitere Informationen finden Sie unter Richten Sie Dateneingaben in ein Health Log Analytics Mit geführtem Setup.
- Manuell. Weitere Informationen finden Sie unter Richten Sie Dateneingaben in ein Health Log Analytics Manuell.

Unterstützte Dateneingaben finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Integrationen für ein Health Log Analytics Von Integrations Launchpad

Richten Sie Integrationen über ein Ereignismanagement Integrations Launchpad In Service Operations-Arbeitsbereich Für ITOM.

Integrations-Launchpad

Die Integrations Launchpad Das Tool bietet eine einheitliche Schnittstelle für die bequeme Integration mit Connectors, die Rohprotokollnachrichten aus externen Quellen in Ihren einspeisen ServiceNow Instanz für Verarbeitung und Analyse. Weitere Informationen finden Sie unter Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM.

Integrationen für Health Log Analytics

Die Integrations Launchpad Aktiviert die folgenden Integrationen für Health Log Analytics:

Integrationen abrufen

Diese Integrationen rufen Protokolldaten aus externen Datenquellen ab und streamen die Daten über eine an Ihre Instanz MID-Server. Wählen Sie eine Integration in der Tabelle aus, um eine Seite mit dem Setup-Verfahren zu öffnen.

Integrationen abrufen

Integration	Beschreibung
Apache Kafka	Streamt Protokolldaten von Apache Kafka An Ihre Instanz.
Elasticsearch	Streamt Protokolldaten von Elasticsearch Indizes für Ihre Instanz.
Microsoft Azure Event Hubs	Streamt Ereignisse von Microsoft Azure Event Hubs An Ihre Instanz.
Microsoft Azure-Ereignis-Hubs (ohne MID)	Streamt Ereignisse von Microsoft Azure Event Hubs An Ihren ServiceNow Instanz ohne MID-Server.
Microsoft Azure Log Analytics	Streamt Protokolldaten von Microsoft Azure Log Analytics An Ihre Instanz. Der -Connector verweist auf Health Log Analytics KI-Engine zu einer Datenquelle in Ihrem Microsoft Azure Log Analytics Account.
ServiceNow-Systemprotokollabruf	Sendet Protokolldaten von ServiceNow Systemprotokolltabelle für Health Log Analytics KI-Engine. **Hinweis:** Nur eine einzelne ServiceNow Die Dateneingabe „Systemprotokolle abrufen“ kann im System vorhanden sein, und nur Anwender mit der Administratorrolle können sie erstellen und konfigurieren. Diese Dateneingabe wird nicht für ausgeführt MID-Server.
Splunk-Poller	Ruft Protokolldaten von ab Splunk An Ihren ServiceNow Instanz regelmäßig durch Abfrage.

Push-Integrationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Integrationen stellen eine Verbindung zu externen Datenquellen her, die Protokolldaten über eine an Ihre Instanz übertragen MID-Server. Wählen Sie eine Integration in der Tabelle aus, um eine Seite mit dem Setup-Verfahren zu öffnen.

Push-Integrationen

Integration	Beschreibung
Amazon Data Firehose	Streamt Protokollnachrichten von AWS Firehose Direkt zum Sammlerservice in ITOM Gateway, für das es sich in der Warteschlange befindet Health Log Analytics Wird verarbeitet.
Cribl	Aktiviert Health Log Analytics Zum Verarbeiten von Cribl-Protokollnachrichten, die in gestreamt werden ServiceNow Instanz.
MID Server	Sammelt Protokollnachrichten von MID-Server Und streamt sie an Ihre Instanz.
REST-API	Streamt Protokolldaten im JSON-Format an Ihre Instanz.
Splunk-TCP	Streamt Protokollnachrichten an ServiceNow Instanz über das TCP-Transportprotokoll mit Splunk Schwerer Forwarder.
Splunk-UDP	Streamt Protokollnachrichten an ServiceNow Instanz über das UDP-Transportprotokoll mit Splunk Schwerer Forwarder.
TCP	Sendet Rohprotokollnachrichten direkt über einen TCP/SSL-Socket an Ihre Instanz.
UDP	Sendet Rohprotokollnachrichten direkt über einen UDP-Socket an Ihre Instanz.

Richten Sie ein Apache Kafka Integration für Health Log Analytics

Richten Sie eine Integration für das Streaming von Protokolldaten aus ein Apache Kafka An Ihren ServiceNow Instanz zur Verarbeitung von Health Log Analytics.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

> **Wichtig:** Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Überlegen Sie, ob die Protokolldaten zu einem einzelnen abgerufen werden sollen MID-Server Oder zu MID-Server Cluster.

  In MID-Server Cluster, mehrere MID Servers Sind für den Failover-Schutz gruppiert. Die aktive Integration wird für eine einzelne ausgeführt MID-Server Im Cluster. Wenn ja MID-Server Schlägt fehl, verschiebt das System seine Aufgaben zur nächsten verfügbaren MID-Server Im Cluster in einer konfigurierten Reihenfolge.

  Wenn Sie sich für die Verwendung eines entscheiden MID-Server Cluster, überprüfen Sie Folgendes:

  - Die MID-Server Cluster enthält nur MID Servers Die die Standardauthentifizierung unterstützen.

    Hinweis: MTLs werden für die Protokollerfassung nicht unterstützt.

  - Die Protokollerfassung ist für jeden aktiviert MID-Server Im Cluster.

    Hinweis: Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.

  - Nicht mehr als das Standardmaximum von 10 Integrationen ruft Protokolle zu einer einzelnen ab MID-Server.

    Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Integrationen, auch wenn dies der Fall ist MID-Server Ist ausgefallen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte, suchen Sie nach `Kafka` .
4. Wählen Sie die Kachel „Kafka-Integration“ aus.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Apache Kafka Integrationskonfigurationsfelder.
6. Wählen Sie **Weiter**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Auf der **Legen Sie die Datenabrufmethode fest** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Legen Sie die Datenabrufmethode fest** Tabelle in Apache Kafka Integrationskonfigurationsfelder.
8. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Apache Kafka Integrationskonfigurationsfelder.
9. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Wählen Sie im Popup-Bildschirm aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

     Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Wählen Sie Aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

   Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Richten Sie ein ein AWS Firehose(Ohne MID) Integration für Health Log Analytics

Richten Sie eine Integration ein, aus der Protokolldaten gestreamt werden sollen AWS Firehose Direkt zu ServiceNow Rechenzentrum, für das es in der Warteschlange steht Health Log Analytics Wird verarbeitet. AWS-Schlüssel müssen nicht auf Ihrem gespeichert werden ServiceNow Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Integration wird nicht für ausgeführt MID-Server.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Feuerwehrschlauch` Im Suchfeld.
4. Wählen Sie aus AWS Firehose Integrationskachel (ohne MID).

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Feldbeschreibungen finden Sie unter AWS Firehose Integrationskonfigurationsfelder.
6. Wählen Sie **Weiter**.
7. Befolgen Sie eines der auf der angegebenen Verfahren **Setup-Anweisung** Bildschirm zum Installieren der Integration in AWS.
   Sie können das Installationsverfahren mit entweder ausführen AWS CloudFormation Oder die AWS-Verwaltungskonsole. Beide Methoden erfordern dieselbe Eingabe. Die entsprechende Auswahl hängt von Ihren Anforderungen und der Größe Ihrer Bereitstellung ab:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AWS CloudFormation Eignet sich am besten für die Bereitstellung standardisierter Konfigurationen in mehreren Umgebungen. Verwenden Sie es, wenn Sie Vorteile von Automatisierung, Wiederholbarkeit und Infrastruktur-as-Code benötigen. AWS CloudFormation Fordert automatisch zur Eingabe auf.
- Die AWS-Verwaltungskonsole eignet sich am besten für manuelle Setups und Schnellkonfigurationen, bei denen Sie keine Automatisierung benötigen.

Bevor Sie eines dieser Verfahren ausführen, kopieren Sie das Zugriffstoken, den ServiceNow Endpunkt-URL und die Integrations-ID für die Zwischenablage. Sie benötigen diese Werte während des Installationsprozesses.

8. Wählen Sie Aus **Entwurf speichern** .
9. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.
   Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt.

Ergebnis

Protokolldaten beginnen mit dem Streaming von AWS Firehose Zu ServiceNow Rechenzentrum. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

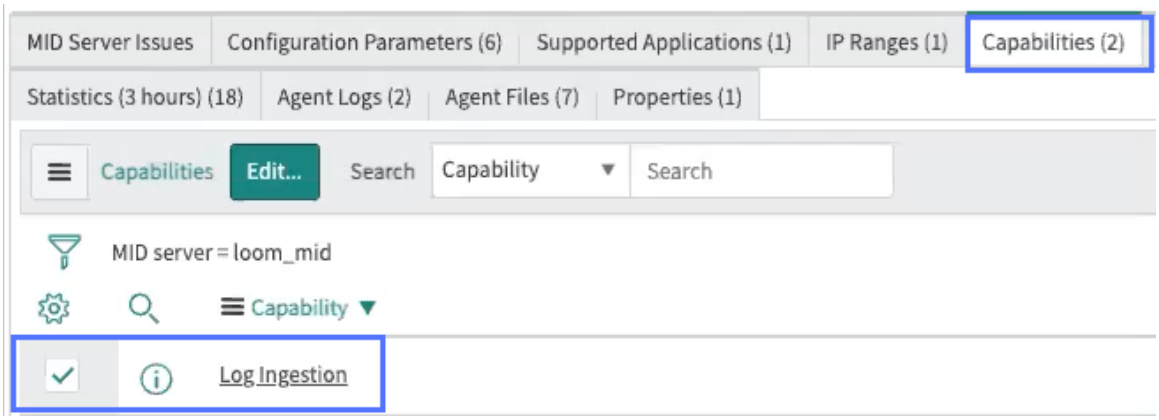
Richten Sie eine Cribl-Integration für ein Health Log Analytics

Richten Sie eine Integration ein, um zu aktivieren Health Log Analytics Zum Verarbeiten von Cribl-Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Cribl zum Filtern und Weiterleiten großer Mengen von Protokolldaten aus verschiedenen Quellen verwendet, das von empfangene Protokollformat Health Log Analytics Unterscheidet sich von anderen Typen. Die Cribl-Integration ermöglicht HLA Um Transport-Header von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen, wird nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weitergeleitet.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben Kribl Im Suchfeld.
4. Wählen Sie die Kachel „Cribl-Integration“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder der Cribl-Integration.
6. Wählen Sie **Weiter**.
7. Auf der **Richten Sie die Verbindung ein** Füllen Sie die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder der Cribl-Integration.
8. Wählen Sie Aus **Entwurf speichern** .
9. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Protokolldaten werden von Cribl in Ihr gestreamt ServiceNow Instanz. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Richten Sie Anmeldeinformationen für die Authentifizierung für die Cribl-Integration in ein Health Log Analytics

Konfigurieren Sie Anmeldeinformationen für die Authentifizierungsmethode, die von der Cribl-Integration verwendet wird.

Vorbereitungen

Entscheiden Sie sich für die entsprechende Authentifizierungsmethode für Ihre Instanz:

- Die Standardauthentifizierung wird für selbst gehostete (lokale) Cribl-Instanzen bevorzugt.
- Für Cribl Cloud-Instanzen ist eine Token-basierte Authentifizierung erforderlich.

Hinweis: Tokenbasierte Authentifizierung wird auch für selbst gehostete (lokale) Cribl-Instanzen unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie für die tokenbasierte Authentifizierung eine Client-ID und ein geheimes Clientgeheimnis in Ihrer Cribl-Instanz, und verwenden Sie sie, um ein Token zu generieren. Zum Beispiel:

- Client-ID: 1234567890abcdef
- Geheimer Clientschlüssel: Abcdef1234567890

Detaillierte Informationen zur Cribl-API finden Sie unter Cribl-API Dokumentation.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Wählen Sie den standardmäßigen Cribl-Anmeldeinformationsalias aus: Cribl_Credential_Alias.
3. Wählen Sie Aus **Neu** Dient zum Erstellen eines Anmeldeinformationsdatensatzes.
4. Wählen Sie den entsprechenden Anmeldeinformationstyp für Ihre Cribl-Instanz aus:
   - Wählen Sie für die Standardauthentifizierung aus **Anmeldeinformationen Für Standardauthentifizierung** .
   - Wählen Sie für die tokenbasierte Authentifizierung aus **Anwenderdefinierte Header-API-Schlüsselanmeldeinformationen** .
5. Füllen Sie die Felder im angezeigten Formular aus.
   - Für Standardauthentifizierung:

Anmeldeinformationsfelder für Standardauthentifizierung

Feld	Beschreibung
Name	Ein Name, der die Anmeldeinformationen beschreibt.
Anwendername	Ihr Cribl-Server-Anwendername. Beispiel: administrator.
Passwort	Ihr Cribl-Server-Passwort. Beispiel: Admin123.

   - Für tokenbasierte Authentifizierung:

Anwenderdefinierte Header-API-Schlüssel-Anmeldeinformationsfelder

Name	Ein Name, der die Anmeldeinformationen beschreibt.
API-Schlüssel	Das Authentifizierungstoken, das Sie in der Cribl-Instanz generiert haben.

6. Wählen Sie Aus **Speichern** Zum Speichern der Konfiguration der Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Überprüfen Sie, ob die angegebenen Anmeldeinformationen über die entsprechenden Berechtigungen für den Zugriff auf Ihre Cribl-Instanz verfügen.
- Stellen Sie sicher, dass unter dem Anmeldeinformationsalias nur ein aktiver Anmeldeinformationsdatensatz jedes Anmeldeinformationstyps vorhanden ist.

Richten Sie ein ein Elasticsearch Integration für Health Log Analytics

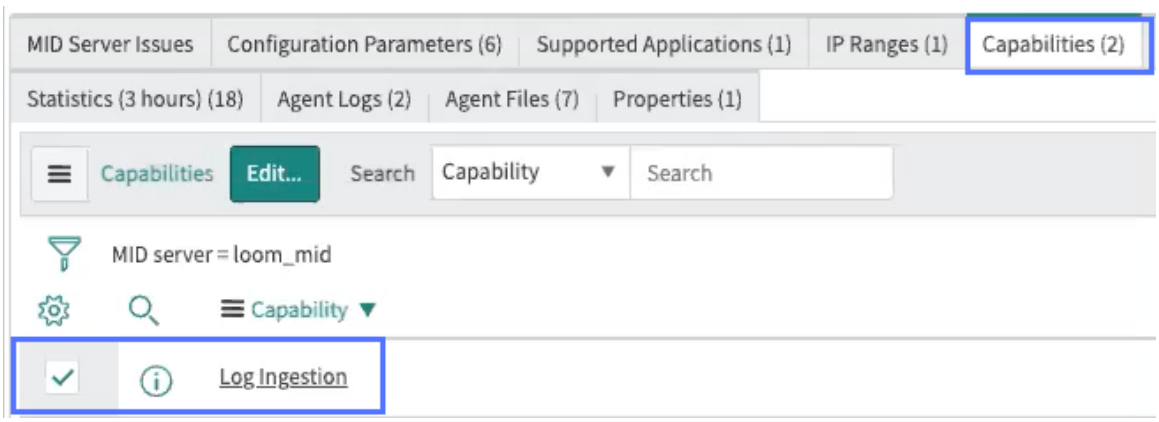
Richten Sie eine Integration für nahtloses Protokolldaten-Streaming von ein Elasticsearch Indizes für Ihre Instanz zur Verarbeitung durch Health Log Analytics.

Vorbereitungen

Hinweis: Health Log Analytics Unterstützt Elasticsearch Versionen über 7.10.2 und unter 8.18.2. Für erweiterte Informationen zum Streaming von Protokolldaten von Elasticsearch Indizes für Ihre Instanz finden Sie unter Protokolle mithilfe der Elasticsearch-Dateneingabe streamen – Erweiterter Leitfaden [KB1080162] artikel in Now Support Knowledge Base.

- Überprüfen Sie, ob Health Log Analytics Die Anwendung wird in Ihrer Instanz installiert und bereitgestellt. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Überprüfen Sie, ob eine Serviceinstanz verfügbar ist.
- Überprüfen Sie, ob Health Log Analytics KI-Engine ist aktiv und wird ausgeführt.

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Elasticsearch`Im Suchfeld.
4. Wählen Sie aus Elasticsearch Integrationskachel.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Elasticsearch Integrationskonfigurationsfelder.
6. Wählen Sie **Weiter**.
7. Auf der **Legen Sie die Datenabrufmethode fest** Füllen Sie die Felder aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Integrationskonfigurationsfelder.
8. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Zum Festlegen von Feldern für erweiterte Konfiguration.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Elasticsearch Integrationskonfigurationsfelder.
9. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Wählen Sie im Popup-Bildschirm aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

     Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Wählen Sie Aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

   Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Richten Sie ein Microsoft Azure Event Hubs Integration für Health Log Analytics

Richten Sie eine Integration für das Streaming von Ereignissen aus ein Microsoft Azure Event Hubs An Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Ereignis-Hubs` Im Suchfeld.
4. Wählen Sie die entsprechende Integrationskachel für Azure Event Hubs aus.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus, und wählen Sie dann aus **Als Nächstes** .
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Microsoft Azure Event Hubs Integrationskonfigurationsfelder.
6. Auf der **Legen Sie den Datenabruf fest** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Legen Sie den Datenabruf fest** Tabelle in Microsoft Azure Event Hubs Integrationskonfigurationsfelder.
7. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Microsoft Azure Event Hubs Integrationskonfigurationsfelder.
8. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Wählen Sie im Popup-Bildschirm aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

     Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Wählen Sie Aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

   Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Richten Sie ein Microsoft Azure Event Hubs(Ohne MID) Integration für Health Log Analytics

Richten Sie eine Integration für das Streaming von Ereignissen aus ein Microsoft Azure Event Hubs An Ihren ServiceNow Instanz ohne MID-Server.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Dies Microsoft Azure Event Hubs Durch die Integration ist kein erforderlich MID-Server, Wodurch das Setup vereinfacht und die Erfassung von Protokolldaten in Ihrer Instanz effizienter wird. Durch Entfernen von MID-Server Anforderung, Protokolldatenerfassung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und -Verarbeitung werden optimiert, um eine schnellere Analyse und Identifizierung der Ursachen zu ermöglichen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Azure-Ereignis-Hubs (ohne MID)` Im Suchfeld.
4. Wählen Sie die Integrationskachel Azure Event Hubs (ohne MID) aus.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus, und wählen Sie dann aus **Als Nächstes** .

   Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine Ereignis-Hubs ohne MID-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Übertragung	Protokoll zum Streamen der Protokolldaten. Dieses Feld ist schreibgeschützt. Diese Integration verwendet Microsoft Azure Event Hubs Dient zum Streamen von Protokolldaten an Ihre Instanz.

6. Auf der **Setup-Anweisung** Führen Sie das entsprechende Verfahren aus, um die Integration in Ihrer Drittanbieterkonsole zu installieren.
   - Installieren Sie die Integration mit Bicep, einer domänenspezifischen Sprache (DSL), die die deklarative Syntax zur Bereitstellung von Azure-Ressourcen verwendet.

     Die Verwendung von Bicep ermöglicht Automatisierung und Konsistenz in Umgebungen über Infrastructure as Code (IAC), sodass Sie Ihre Azure-Umgebung effizienter verwalten können. Außerdem werden Versionssteuerung und Integration mit CI/CD-Pipelines unterstützt.

   - Installieren Sie die Integration im Azure-Portal.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Installation im Azure-Portal ist eine gute Wahl, wenn Sie ein einmaliges Setup durchführen oder eine grafische Oberfläche bevorzugen. Sie bietet eine bequeme Möglichkeit, Ressourcen zu konfigurieren, sodass sie für einfache Bereitstellungen geeignet sind.

Der Bildschirm enthält einen Link zu detaillierten Konfigurationsanweisungen für jede dieser beiden Installationsoptionen.

7. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Auf der **Richten Sie die Verbindung ein** Wählen Sie die Registerkarte aus **Aktivieren** .

   Wenn der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie ein Microsoft Azure Log Analytics Integration für Health Log Analytics

Richten Sie eine Integration für das Streaming von Protokolldaten aus ein Microsoft Azure Log Analytics An Ihren ServiceNow Instanz. Die -Integration verweist auf Health Log Analytics KI-Engine zu einer Datenquelle in Ihrem Microsoft Azure Log Analytics Account.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *`mid.public_ip`* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Azure-Protokoll` Im Suchfeld.
4. Wählen Sie Azure aus Log Analytics Integrationskachel.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus, und wählen Sie dann aus **Als Nächstes** .
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Microsoft Azure Log Analytics Integrationskonfigurationsfelder.
6. Auf der **Legen Sie die Datenabrufmethode fest** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Legen Sie die Datenabrufmethode fest** Tabelle in Microsoft Azure Log Analytics Integrationskonfigurationsfelder.
7. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Microsoft Azure Log Analytics Integrationskonfigurationsfelder.

8. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Wählen Sie im Popup-Bildschirm aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

     Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Wählen Sie Aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

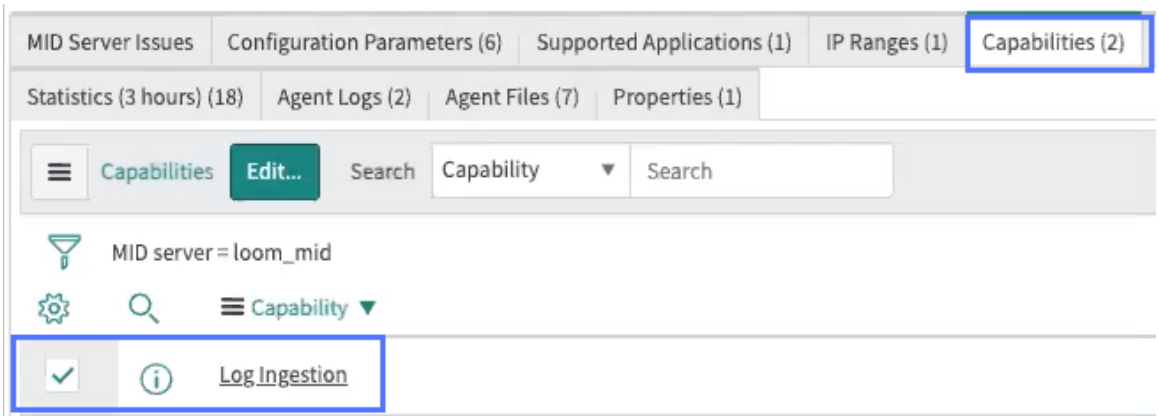
Richten Sie ein MID-Server Integration für Health Log Analytics

Richten Sie eine Integration für das Sammeln und Streamen ein MID-Server Protokollieren Sie Nachrichten für ServiceNow Instanz zur Verarbeitung von Health Log Analytics.

Vorbereitungen

Wichtig: Sie können nur einen erstellen MID-Server Integration pro MID-Server.

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben Mid Im Suchfeld.
4. Wählen Sie aus MID-Server Integrationskachel.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in MID-Server Integrationskonfigurationsfelder.
6. Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in MID-Server Integrationskonfigurationsfelder.
7. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.
   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

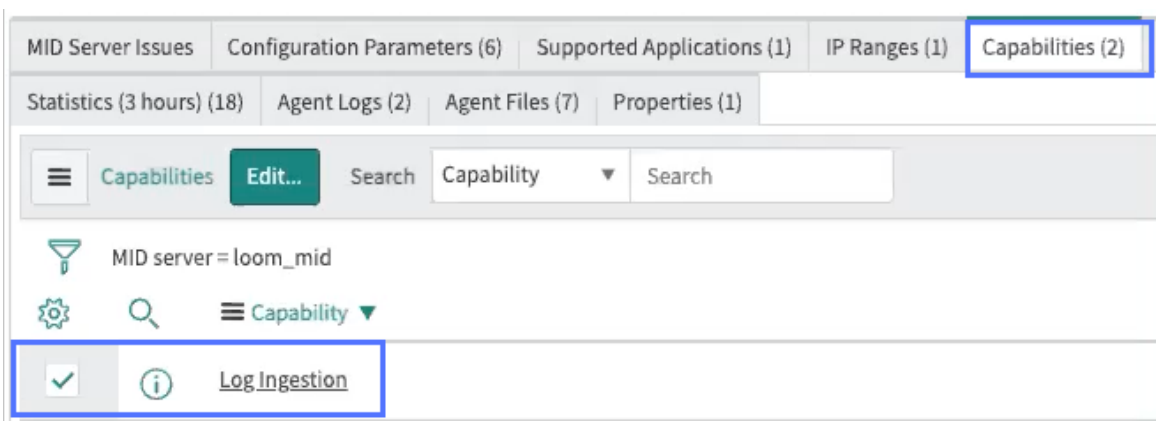
   Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Richten Sie eine REST-API-Integration für ein Health Log Analytics

Richten Sie eine Integration für das Streaming von Protokolldaten an Ihren ein ServiceNow Instanz zur Verarbeitung von Health Log Analytics.

Vorbereitungen

- Überprüfen Sie, ob Health Log Analytics Die Anwendung wird in Ihrer Instanz installiert und bereitgestellt. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Überprüfen Sie, ob eine Serviceinstanz verfügbar ist.
- Überprüfen Sie, ob Health Log Analytics KI-Engine ist aktiv und wird ausgeführt.
- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Wählen Sie im Formular „MID-Webserver-Kontext“ im Feld **Ausführen für** die Option *Spezifischer MID Server* und nicht die Clusteroption aus. In **MID-Server** Wählen Sie das spezifische aus MID-Server Zu dem die Protokolldaten abgerufen werden.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Hinweis: REST API-Integrationen unterstützen nur die UTF-8-Codierung für eingehende Daten.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben REST Im Suchfeld.
4. Wählen Sie die REST API-Integrationskachel aus.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder der REST-API-Integration.
6. Wählen Sie **Weiter**.
7. In **Setup-Anweisung** Kopieren Sie die angegebene URL in die Zwischenablage.

   Das Format der URL ist: `http://(MID_SERVER_IP):(MID_WEB_SERVER_PORT)/ap1/mid/hla/raw` , Wo `/aps/MID/hla/RAW` Ist der Endpunkt. HLA Wurde ersetzt (MID_SERVER_IP) Und (MID_WEB_SERVER_PORT) Mit den Werten, die Sie in konfiguriert haben **Geben Sie Details an** Formular.

8. Wählen Sie Aus **Entwurf speichern** .
9. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können eine konfigurierte Integration nur aktivieren, wenn Sie alle Integrationsvoraussetzungen erfüllt haben.

10. **Wahlweise:** Wenn Sie die Integration im Entwurfsmodus installiert haben, aktivieren Sie sie später, indem Sie die folgenden Schritte ausführen:
    a. Schließen Sie die Integrationsvoraussetzungen ab.
    b. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integration aus.
    c. In **Setup-Anweisung** Bildschirm auswählen **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Die Integration ist aktiviert und die **Übersicht** Bildschirm wird angezeigt. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Weisen Sie Ihren API-Client an, Protokollnachrichten an zu senden MID-Server.

1. Konfigurieren Sie im API-Client eine Anforderung mit den folgenden Parametern:
   - HTTP-Methode: POST.
   - URL: Die URL, die Sie in kopiert haben **Setup-Anweisung** Bildschirm.
   - Authentifizierung: Die erforderlichen Anmeldeinformationen für die Authentifizierung. Beispiel: Standardauthentifizierung (Anwendername und Passwort).

     Hinweis: Die Authentifizierungsmethode muss mit der auf dem MID-Webserver konfigurierten Methode identisch sein.

   - Header: Legen Sie fest `Inhaltstyp` Header, der Ihrem Nutzlastformat entspricht.
     - Für JSON: `Anwendung/JSON` .
     - Für Rohtext: `Text/nur` .
   - Textkörper: Die Protokollnutzlast in JSON oder Rohtext.
2. Senden Sie die Anforderung.

   Eine erfolgreiche Antwort gibt an, dass MID-Server Hat die Nutzlast erhalten. Wenn MID-Server Hat die Protokollnachrichten verarbeitet, die Dateneingabe streamt sie an Ihren ServiceNow Instanz, die das REST-Protokoll verwendet.

Richten Sie ein ServiceNow Systemprotokollabruf-Integration für Health Log Analytics

Richten Sie eine Integration für das Streaming von Protokolldaten von Ihrem ein ServiceNow Systemprotokolltabelle der Plattform an die HLA Engine.

Vorbereitungen

Hinweis: Diese Integration wird nicht für ausgeführt MID-Server. Nur eine einzelne ServiceNow Systemprotokollabrufintegration oder Dateneingabe kann im System vorhanden sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie, ob Health Log Analytics Die Anwendung wird in Ihrer Instanz installiert und bereitgestellt. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Überprüfen Sie, ob eine Serviceinstanz verfügbar ist.
- Überprüfen Sie, ob HLA Engine ist aktiv und wird ausgeführt.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben Systemprotokolle Im Suchfeld.
4. Wählen Sie aus ServiceNow Kachel „Systemprotokolle“.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Die **Geben Sie Details an** Formular wird angezeigt.
   Diese Felder werden automatisch ausgefüllt, da nur eines vorhanden ist ServiceNow Systemprotokollabrufintegration oder Dateneingabe kann im System vorhanden sein. Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in ServiceNow Konfigurationsfelder der Systemprotokolle-Abruf-Integration.
6. Wählen Sie **Weiter**.
7. **Wahlweise:** Auf der **Legen Sie die Datenabrufmethode fest** Seite, Build-Bedingungen zum Filtern von Protokolldaten aus der Tabelle „Systemprotokoll“, bevor sie an gestreamt werden HLA Engine.

   (Optional) Auf dieser Seite können Sie sich auf die spezifischen Protokolle konzentrieren, die Sie überwachen möchten. Beispielsweise möchten Sie sich Discovery-Protokolle ansehen oder E-Mail-Protokolle ausschließen. Standardmäßig sind alle Protokolle enthalten.

8. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

     Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

   - Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

     Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Protokolldaten beginnen mit dem Streaming von ServiceNow Systemprotokolltabelle für Health Log Analytics KI-Engine, basierend auf den konfigurierten Filtern. Dediziert HLA Die Engine für Ihre Instanz beginnt mit der Analyse Ihrer Systemprotokolle in Echtzeit.

Hinweis: Beginnend mit Health Log Analytics Version 37.0,15. Sie können verwenden ServiceNow Systemprotokolle – Abruf-Integration, um Fehler und Anomalien in Ihrem automatisch zu erkennen ServiceNow Systemprotokoll der Instanz. Durch Kombination HLA Anomalieerkennung von mit Now Assist GenAI-Fähigkeiten von können Sie Plattformprobleme effektiver identifizieren und lösen, um eine bessere Anwender-Experience zu gewährleisten. Weitere Informationen finden Sie unter Anwendungsfall: Proaktive Überwachung von ServiceNow Instanz in Health Log Analytics.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten, indem Sie Ihre Integrationskonfiguration anpassen. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Die MID-Server Streaming-Status und **Protokoll-Streaming-Quellen** Tabelle wird nicht auf angezeigt **Übersicht** Registerkarte für diese Integration, da sie nicht für ausgeführt wird MID-Server. Wenn die Integration zum ersten Mal konfiguriert wird, kann es bis zu 24 Stunden dauern, bis die ersten Warnungen angezeigt werden. Sobald die Daten ausgefüllt sind, können Sie den Bildschirm aktualisieren, um Echtzeitmetriken anzuzeigen.

Tipp: Verwenden Sie das Menü Ansicht, um direkt von zu wechseln **Übersicht** Registerkarte zum **Dateneingabezuordnung** , **Quelltypstrukturen** , Und **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Die Anwendung ist installiert, und das Menü Ansicht bietet auch direkten Zugriff auf **Protokoll-Viewer** , In dem Sie die Rohprotokolle sehen können, die die Integration erfasst.

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

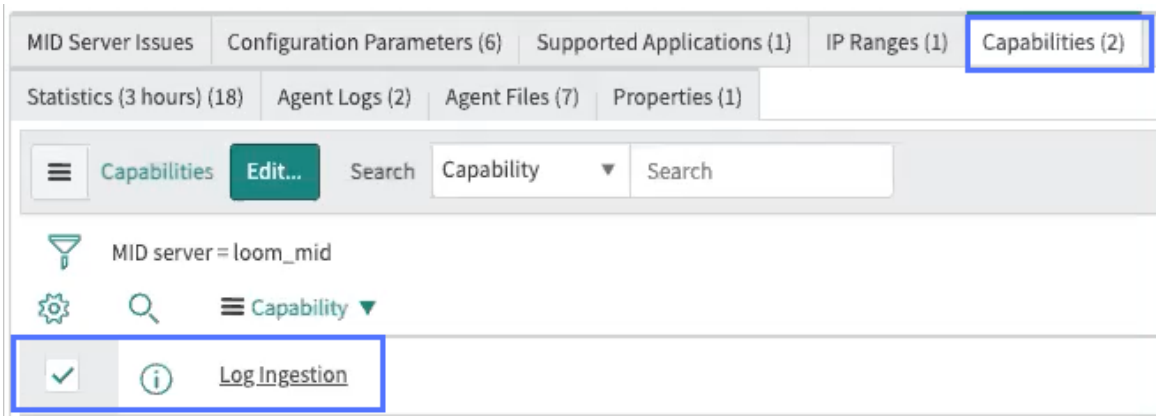
Richten Sie ein Splunk Poller-Integration für Health Log Analytics

Richten Sie eine Integration ein, die regelmäßig Protokolldaten aus abruft Splunk An Ihren ServiceNow Instanz zur Verarbeitung von Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

- Die MID-Server Muss die Standardauthentifizierung unterstützen.

  Hinweis: MTLs werden für die Protokollerfassung nicht unterstützt.

- Nicht mehr als das Standardmaximum von 10 Integrationen streamt Protokolle an eine einzelne MID-Server. Sie können die maximale Anzahl ändern, indem Sie die Eigenschaft hinzufügen sn.occ.log_ingestion.max_datainput_per_MID Zu MID-Server Und dann ändern Sie den Standardwert.

  Um herauszufinden, wie viele Dateneingaben Protokolle an denselben streamen MID-Server, Navigieren Sie zu **Streaming-Quellen** Tabelle und zählen Sie die Dateneingaben, die zu einem bestimmten gestreamt werden MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überlegen Sie, ob die Protokolldaten zu einem einzelnen abgerufen werden sollen MID-Server Oder zu MID-Server Cluster.

  In MID-Server Cluster, mehrere MID Servers Sind für den Failover-Schutz gruppiert. Die aktive Integration wird für eine einzelne ausgeführt MID-Server Im Cluster. Wenn ja MID-Server Schlägt fehl, verschiebt das System seine Aufgaben zur nächsten verfügbaren MID-Server Im Cluster in einer konfigurierten Reihenfolge.

  Wenn Sie einen verwenden möchten MID-Server Cluster, überprüfen Sie Folgendes:

  - Die MID-Server Cluster enthält nur MID Servers Die die Standardauthentifizierung unterstützen.
  - Die Protokollerfassung ist für jeden aktiviert MID-Server Im Cluster.

    Hinweis: Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.

  - Nicht mehr als das Standardmaximum von 10 Integrationen streamt Protokolle an eine einzelne MID-Server.

    Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Integrationen, auch wenn dies der Fall ist MID-Server Ist ausgefallen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben Splunk-Poller Im Suchfeld.
4. Wählen Sie aus Splunk Kachel für Poller-Integration.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Splunk Konfigurationsfelder der Poller-Integration.
6. Wählen Sie **Weiter**.
7. Auf der **Legen Sie die Datenabrufmethode fest** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Legen Sie die Datenabrufmethode fest** Tabelle in Splunk Konfigurationsfelder der Poller-Integration.
8. Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.
   Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder der Poller-Integration.
9. Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie alle Voraussetzungen vor dem Starten der Konfiguration abgeschlossen haben, wählen Sie aus **Aktivieren** .

  Wählen Sie im Popup-Bildschirm aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

  Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Auf der Integrations Launchpad, Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte.

- Wenn Sie nicht alle vorherigen Anforderungen abgeschlossen haben, wählen Sie aus **Entwurf speichern** .

  Das System speichert die Integration als Entwurf in Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** . Sie können die Voraussetzungen abschließen und die Installation später aktivieren. Weitere Informationen finden Sie unter **Was als Nächstes zu tun ist** Abschnitt.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Wenn Sie die Integration als Entwurf gespeichert haben, führen Sie die folgenden Schritte aus, um sie später zu aktivieren:

1. Schließen Sie alle vorherigen Anforderungen ab.
2. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integrationskachel aus.
3. Wählen Sie auf dem Konfigurationsbildschirm aus **Aktivieren** .

   Wählen Sie Aus **Testen und speichern** Um die Integration in der Datenbank zu speichern und die Konnektivität zu testen. Wenn ein Fehler zurückgegeben wird, passen Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration wie in der Fehlermeldung vorgeschlagen an, und versuchen Sie dann erneut, die Integration zu aktivieren.

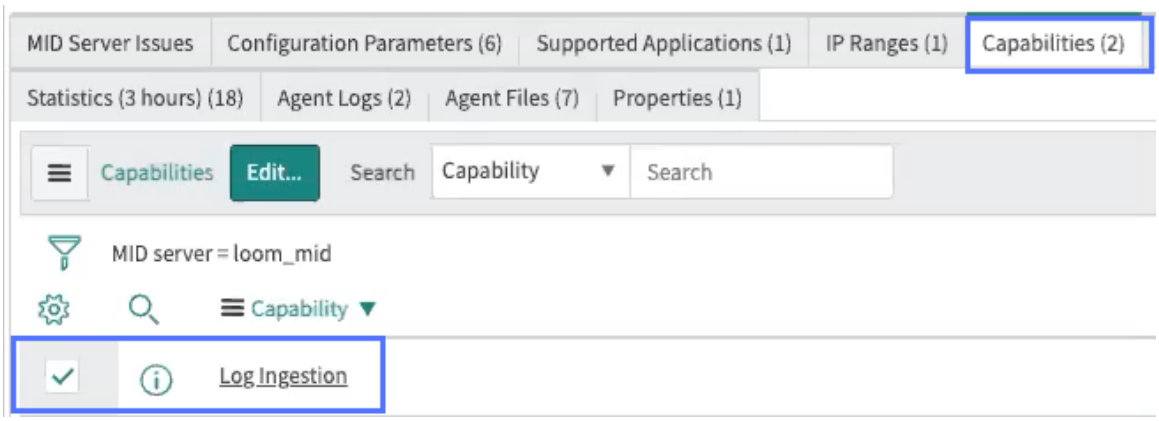
Sobald der Test erfolgreich ist, werden die Integration und die aktiviert **Übersicht** Registerkarte wird angezeigt. Die Integrationskachel ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Richten Sie ein Splunk TCP-Integration für Health Log Analytics

Richten Sie eine Integration ein, um Protokollnachrichten an zu streamen ServiceNow Instanz über das TCP-Transportprotokoll mit Splunk Schwerer Forwarder. Health Log Analytics Verarbeitet die erfassten Protokolldaten.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die MID-Server Muss die Standardauthentifizierung unterstützen.

  Hinweis: MTLs werden für die Protokollerfassung nicht unterstützt.

- Nicht mehr als das Standardmaximum von 10 Integrationen streamt Protokolle an eine einzelne MID-Server. Sie können die maximale Anzahl ändern, indem Sie die Eigenschaft hinzufügen sn.occ.log_ingestion.max_datainput_per_MID Zu MID-Server Und dann ändern Sie den Standardwert.

  Um herauszufinden, wie viele Dateneingaben Protokolle an denselben streamen MID-Server, Navigieren Sie zu **Streaming-Quellen** Tabelle und zählen Sie die Dateneingaben, die zu einem bestimmten gestreamt werden MID-Server.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben Splunk Im Suchfeld.
4. Wählen Sie aus Splunk TCP-Integrationskachel.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Splunk Konfigurationsfelder für TCP-Integration.
6. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Splunk Konfigurationsfelder für TCP-Integration.
7. Wählen Sie **Weiter**.
8. Befolgen Sie das Verfahren auf dem **Setup-Anweisung** Bildschirm zum Installieren der Integration in der Drittanbieterkonsole.

   Hinweis: Das Verfahren hängt von Ihren Konfigurationen ab.

9. Wählen Sie Aus **Speichern Entwurf** .
10. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

    Hinweis: Sie können eine konfigurierte Integration nur aktivieren, wenn Sie alle im Abschnitt vor Beginn aufgeführten Voraussetzungen erfüllt haben.

    Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt.

11. **Wahlweise:** Wenn Sie die Integration im Entwurfsmodus installiert haben, führen Sie die folgenden Schritte aus, um sie zu aktivieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Schließen Sie die Integrationsvoraussetzungen ab.

b. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integration aus.

c. Auf der **Setup-Anweisung** Wählen Sie die Registerkarte aus **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Protokolldaten beginnen mit dem Streamen an Ihren ServiceNow Instanz. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

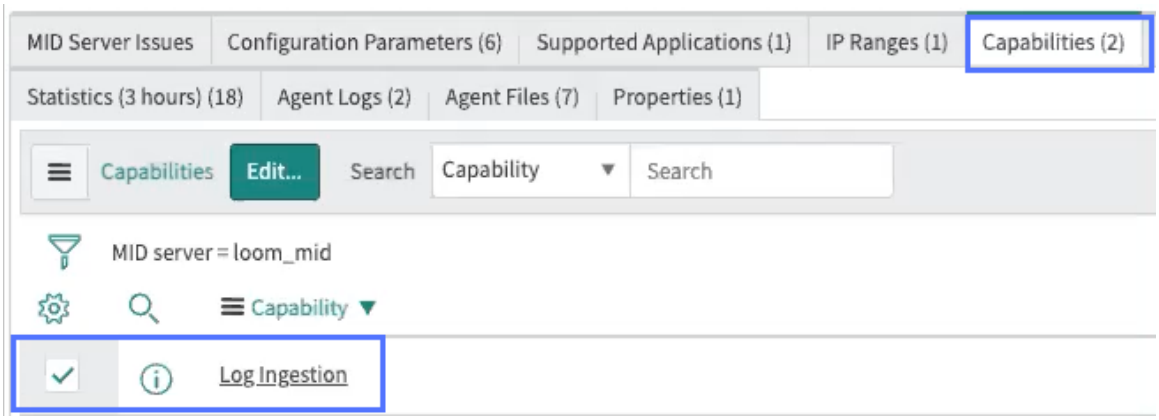
- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Richten Sie ein Splunk UDP-Integration für Health Log Analytics

Richten Sie eine Integration ein, um Protokollnachrichten an zu streamen ServiceNow Instanz über das UDP-Transportprotokoll mit Splunk Schwerer Forwarder. Health Log Analytics Verarbeitet die erfassten Protokolldaten.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben `Splunk` Im Suchfeld.
4. Wählen Sie aus Splunk UDP-Integrationskachel.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Splunk Konfigurationsfelder der UDP-Integration.
6. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Und füllen Sie die Felder für die erweiterte Konfiguration aus.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Splunk Konfigurationsfelder der UDP-Integration.
7. Wählen Sie **Weiter**.
8. Befolgen Sie das Verfahren auf dem **Setup-Anweisung** Bildschirm zum Installieren der Integration in der Drittanbieterkonsole.

   Hinweis: Das Verfahren hängt von Ihren Konfigurationen ab.

9. Wählen Sie Aus **Entwurf speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

    Hinweis: Sie können eine konfigurierte Integration nur aktivieren, wenn Sie alle im Abschnitt vor Beginn aufgeführten Voraussetzungen erfüllt haben.

    Die Integration ist aktiviert. Ist **Übersicht** Registerkarte wird angezeigt.

11. **Wahlweise:** Wenn Sie die Integration im Entwurfsmodus installiert haben, führen Sie die folgenden Schritte aus, um sie zu aktivieren:

    a. Schließen Sie die Integrationsvoraussetzungen ab.

    b. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integration aus.

    c. Auf der **Setup-Anweisung** Wählen Sie die Registerkarte aus **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Protokolldaten beginnen mit dem Streamen an Ihren ServiceNow Instanz. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Richten Sie eine TCP-Integration für ein Health Log Analytics

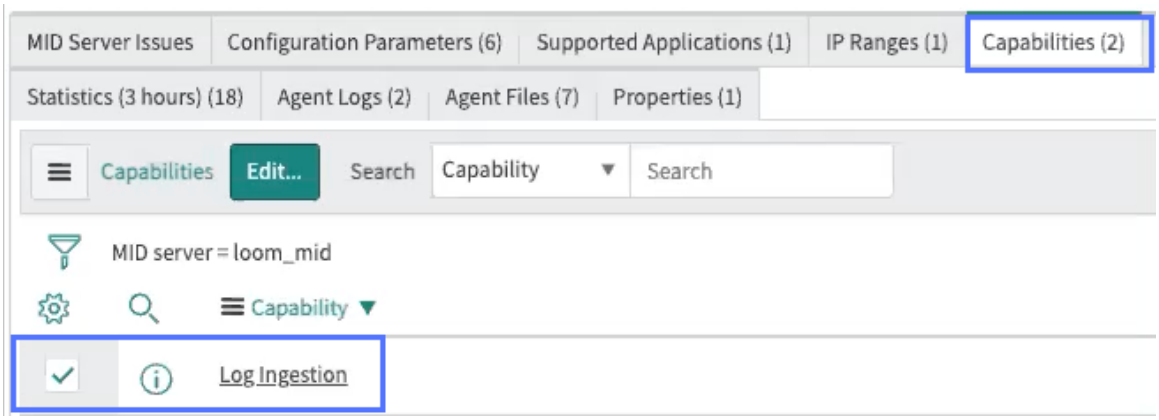
Richten Sie eine Integration für das Senden von Protokolldaten an ein ServiceNow Instanz direkt über einen TCP/SSL-Socket.

Vorbereitungen

- Überprüfen Sie, ob Health Log Analytics Die Anwendung wird in Ihrer Instanz installiert und bereitgestellt. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Überprüfen Sie, ob eine Serviceinstanz verfügbar ist.
- Überprüfen Sie, ob HLA Engine ist aktiv und wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *`mid.public_ip`* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Hinweis: Informationen zum Streamen von Daten aus Logstash an Ihre Instanz finden Sie unter Streaming von Daten aus Logstash an Ihre HLA-Instanz [KB0994735] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen durchsuchen** Registerkarte eingeben TCP Im Suchfeld.
4. Wählen Sie die TCP-Integrationskachel aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Konfigurationsfelder für TCP-Integration.
6. Wählen Sie **Weiter**.
7. In **Setup-Anweisung** Befolgen Sie die Anweisungen auf dem Bildschirm, um die Integration in der Drittanbieterkonsole zu installieren.
8. Wählen Sie Aus **Entwurf speichern** .
9. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

   Hinweis: Sie können eine konfigurierte Integration nur aktivieren, wenn Sie alle im Abschnitt vor Beginn aufgeführten Voraussetzungen erfüllt haben.

   Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt.
10. **Wahlweise:** Wenn Sie die Integration im Entwurfsmodus installiert haben, führen Sie die folgenden Schritte aus, um sie zu aktivieren:
    a. Schließen Sie die Integrationsvoraussetzungen ab.
    b. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integration aus.
    c. Auf der **Setup-Anweisung** Wählen Sie die Registerkarte aus **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Protokolldaten beginnen mit dem Streamen an Ihren ServiceNow Instanz direkt über einen TCP/SSL-Socket. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

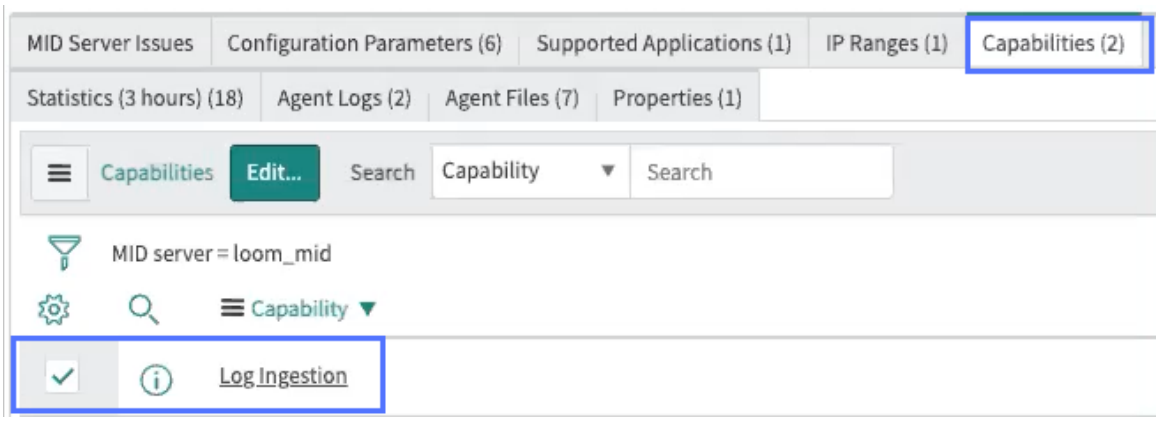
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie eine UDP-Integration für ein Health Log Analytics

Richten Sie eine Integration für das Senden von Protokolldaten an ein ServiceNow Instanz direkt über einen UDP-Socket.

Vorbereitungen

- Überprüfen Sie, ob Health Log Analytics Die Anwendung wird in Ihrer Instanz installiert und bereitgestellt. Weitere Informationen finden Sie unter Installieren Health Log Analytics(HLA).
- Überprüfen Sie, ob eine Serviceinstanz verfügbar ist.
- Überprüfen Sie, ob HLA Engine ist aktiv und wird ausgeführt.
- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. In **Integrationen durchsuchen** Registerkarte eingeben UDP Im Suchfeld.
4. Wählen Sie die Kachel „UDP-Integration“ aus.

   Hinweis: Wenn Sie ein Integrationssetup starten, bevor Sie alle Voraussetzungen erfüllen, wird eine Meldung angezeigt. Sie können entweder das Setup abbrechen und zuerst die vorherigen Anforderungen abschließen oder im Entwurfsmodus fortfahren und sie später abschließen. Beachten Sie, dass Sie die Integration erst aktivieren können, wenn alle Voraussetzungen erfüllt sind.

5. Auf der **Geben Sie Details an** Füllen Sie die Felder aus.
   Eine Beschreibung der Felder finden Sie unter **Geben Sie Details an** Tabelle in Konfigurationsfelder der UDP-Integration.
6. **Wahlweise:** Wählen Sie Aus **Erweiterte Einstellungen** Zum Festlegen von Feldern für erweiterte Konfiguration.
   Eine Beschreibung der Felder finden Sie unter **Erweiterte Einstellungen** Tabelle in Konfigurationsfelder der UDP-Integration.
7. Wählen Sie **Weiter**.
8. In **Setup-Anweisung** Befolgen Sie die Anweisungen auf dem Bildschirm, um die Integration in der Drittanbieterkonsole zu installieren.
9. Wählen Sie Aus **Entwurf speichern** .
10. Wählen Sie Aus **Aktivieren** Zum Aktivieren der Integration.

    Hinweis: Sie können eine konfigurierte Integration nur aktivieren, wenn Sie alle im Abschnitt vor Beginn aufgeführten Voraussetzungen erfüllt haben.

    Die Integration ist aktiviert und die **Übersicht** Registerkarte wird angezeigt.
11. **Wahlweise:** Wenn Sie die Integration im Entwurfsmodus installiert haben, führen Sie die folgenden Schritte aus, um sie zu aktivieren:
    a. Schließen Sie die Integrationsvoraussetzungen ab.
    b. In Integrations Launchpad **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** , Suchen und wählen Sie die Integration aus.
    c. Auf der **Setup-Anweisung** Wählen Sie die Registerkarte aus **Aktivieren** Zum Aktivieren der Integration.

Ergebnis

Protokolldaten beginnen mit dem Streamen an Ihren ServiceNow Instanz direkt über einen UDP-Socket. Die Kachel für die Integration ist in verfügbar **Installierte Integrationen** Registerkarte im Integrations Launchpad.

Nächste Maßnahme

Nutzen Sie die Informationen im **Übersicht** Registerkarte zum Verfeinern der Vorgehensweise HLA Liest die Protokolldaten. Weitere Informationen finden Sie unter Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp: Verwenden Sie das Menü weitere Optionen ( ), um zu öffnen **Dateneingabezuordnung** , **Quelltypstrukturen** , Oder **Protokollquellen** Seiten mit Kontext aus der Integration. Wenn Ihre Protokolldaten nicht ordnungsgemäß zugeordnet, strukturiert oder bezogen sind, kehren Sie zurück, und passen Sie die Konfiguration an. Wenn Service Operations-Arbeitsbereich Log Analytics Anwendung installiert ist, bietet das Menü „weitere Optionen“ auch direkten Zugriff auf **Protokoll-Viewer** , Wo Sie von der Integration erfasste Rohprotokollnachrichten überprüfen können.

Weitere Informationen finden Sie unter:

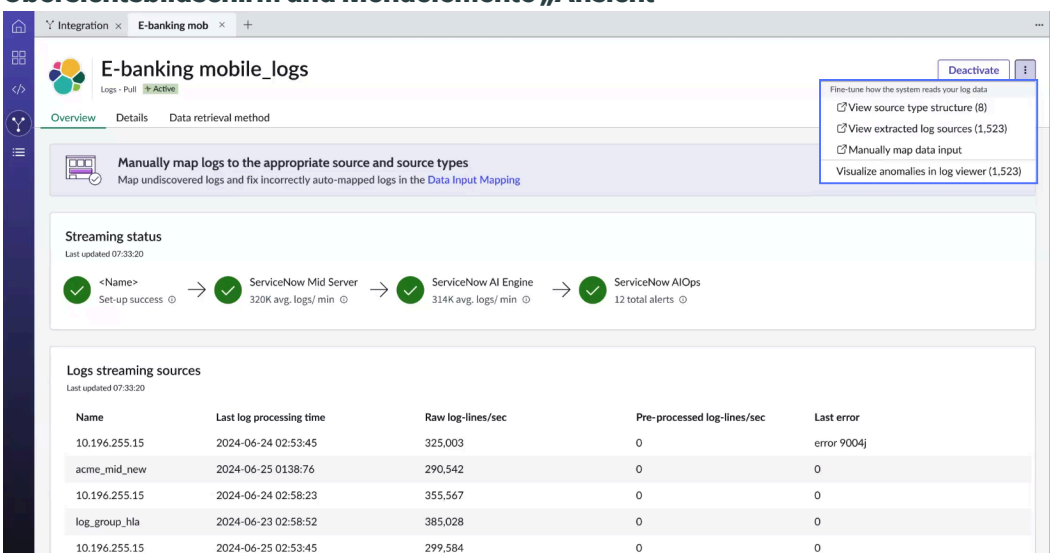
- Automatische Zuordnung und Zuordnung von Protokolldaten
- Quelltypstruktur anpassen
- Überprüfen Sie Protokolle im Protokoll-Viewer

Überwachen des Protokolldaten-Flows und Optimieren der Integrationseinstellungen in Health Log Analytics

Der Übersichtsbildschirm in Health Log Analytics Bietet eine umfassende Ansicht der Komponenten in der Protokollverarbeitungs-Pipeline aktiver Integrationen. Über diesen Bildschirm können Sie Streaming-Probleme beheben und die Einstellungen der Integration bei Bedarf anpassen.

Die **Übersicht** Der Bildschirm zeigt den Status des Protokolldaten-Streamings und die Streaming-Quellen einer aktiven Integration an. Sie bietet direkten Zugriff auf **Dateneingabezuordnung** , **Quelltypstrukturen** , Und **Protokollquellen** -Seiten sowie -Seiten **Protokoll-Viewer** , Alle mit Kontext aus der aktuellen Integration.

Übersichtsbildschirm und Menüelemente „Ansicht“



Streaming-Status

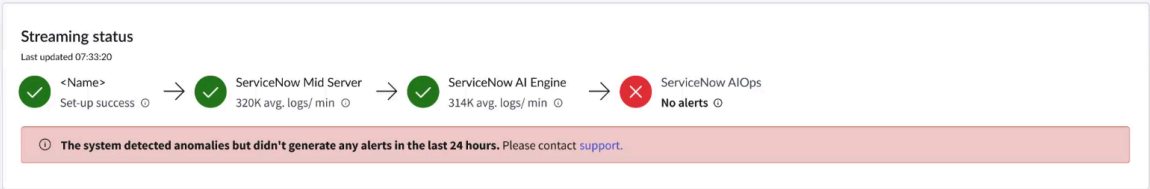
Die **Streaming-Status** Abschnitt auf der **Übersicht** Der Bildschirm zeigt den Status des Daten-Streamings zwischen der Protokollquelle und dem an MID-Server Und zwischen MID-Server Und HLA Engine. Zeigt die Anzahl der Protokolle pro Minute an, die durch den gehen MID-Server Und über HLA Engine.

Hinweis: Für ServiceNow Integration des Abrufs von Systemprotokollen, der **Übersicht** Auf dem Bildschirm wird nicht angezeigt MID-Server Streaming-Status, da diese Integration nicht für ausgeführt wird MID-Server.

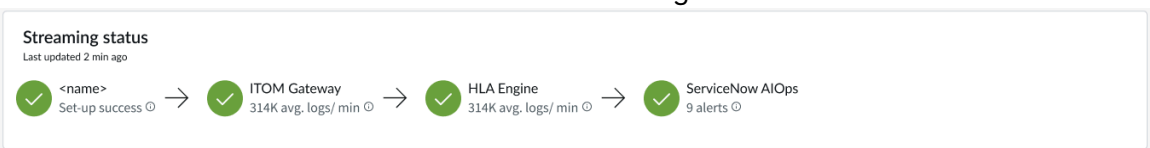
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ServiceNow Die AIOps-Komponente zeigt die Gesamtzahl der Warnungen an, die der hat HLA Engine wurde erstellt. Diese Statistiken werden aktualisiert, wenn **Übersicht** Der Bildschirm wird geladen und jede Minute automatisch aktualisiert, um Live-Daten anzuzeigen. Sie können das standardmäßige Zeitintervall für die automatische Aktualisierung über die Systemeigenschaft ändern *sn_itom_integ_app.overview_page_data_input_stats_auto_refresh_interval_seconds*.

Wenn das Daten-Streaming fehlschlägt, wird die Integration und automatisch deaktiviert **Streaming-Status** Kennzeichnet die Komponente, in der der Fehler aufgetreten ist. Darüber hinaus erklärt ein Banner den Fehler und schlägt entweder Schritte zur Behebung vor, oder verweist auf den ServiceNow-Support.



Für Integrationen ohne MID oder OpenTelemetry Protocol (OTLP), z. B. AWS Firehose, **Übersicht** Der Bildschirm zeigt an ITOM Gateway-Komponente als Schritt in der Protokollverarbeitungs-Pipeline. Die MID-Server Die Komponente wird in der Pipeline nicht angezeigt, da Protokolldaten direkt von der Quelle an gesendet werden ITOM Gateway. Die Protokolle werden dann von verarbeitet HLA Engine zum Suchen von Anomalien.



Für diese Integrationen **Übersicht** Der Bildschirm zeigt die durchschnittliche Rate der Protokolle pro Minute in den letzten 15 Minuten an, die durch das geführt wurden ITOM Gateway und HLA Engine, ähnlich den Metriken, die für die MID-basierte Erfassung angezeigt werden.

Hinweis: Die ITOM Gateway-Komponente wird nur angezeigt, wenn MID-Server Eigenschaft *mid.hla.itom_gateway_streaming.enabled*Ist auf „wahr“ festgelegt. Weitere Informationen finden Sie unter MID Server-Eigenschaften .

Wenn die Integration keine Live-Daten aus der Quelle streamt, wird eine Warnmeldung angezeigt. Es gibt ein 4-Stunden-Intervall zwischen der Zeit der letzten Protokollquelle und der aktuellen Zeit, bevor diese Nachricht generiert wird. Sie können das Standardzeitintervall über die Systemeigenschaft ändern *sn_itom_integ_app.overview_page_log_source_time_threshold_hours*.

Hinweis: Die Nachricht wird nur angezeigt, wenn HLA Engine ist aktiv und wird ausgeführt.

Protokoll-Streamingquellen

Abhängig von Ihrer Integration, die **Protokoll-Streaming-Quellen** Tabelle zeigt die folgenden Informationen zu den Protokoll-Streaming-Quellen der Integration an.

Hinweis: Diese Tabelle ist für nicht verfügbar ServiceNow Integration des Abrufs von Systemprotokollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokoll-Streamingquellen

Spalte	Beschreibung
Name	Der Name der Protokolldatenquelle.
Status	Der Streaming-Status: Aktiv oder nicht aktiv.
Dateneingabe	Die Integration, die die Daten an Ihren streamt ServiceNow Instanz.
MID-Server	Die MID-Server An den die Protokolldaten gestreamt werden.
Zeit des letzten Ereignisses	Der Zeitpunkt, zu dem die Integration das letzte Ereignis empfangen hat.
Zeit der letzten Protokollverarbeitung	Die Zeit, zu der das letzte Protokoll empfangen oder verarbeitet wurde.
Raw log lines/sec (Protokollzeilen im Rohzutand/ Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Protokollzeilen im Rohzutand vor der Vorverarbeitung dar.
Vorverarbeitete Protokollzeilen/Sek	Die durchschnittliche Anzahl der vorbearbeiteten Protokollzeilen, die im letzten Ein-Minuten-Intervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass Protokolle während der Vorverarbeitung gelöscht wurden.

Zugehörige Informationen

Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics

Überprüfen Sie die Protokoll-Streaming-Daten, und passen Sie die Integrationseinstellungen in an Health Log Analytics

Überprüfen Sie den Status des Protokolldaten-Streamings und die Streaming-Quellen einer aktiven Integration für Health Log Analytics Auf dem Übersichtsbildschirm der Integration. Auf dieser Registerkarte können Sie Streaming-Probleme untersuchen und die Integrationseinstellungen verfeinern. Nutzen Sie die angezeigten Daten, um zu verfeinern, wie HLA Liest die Protokolldaten, indem die Konfiguration der Integration angepasst wird.

Vorbereitungen

Bestätigen Sie, dass die Integration auf aktiviert wurde Integrations Launchpad. Weitere Informationen finden Sie unter Richten Sie Integrationen für ein Health Log Analytics Von Integrations Launchpad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie bei Integrationen ohne MID oder OpenTelemetry Protocol (OTLP), ob *mid.hla.itom_gateway_streaming.enabled*Eigenschaft ist in auf „wahr“ festgelegt MID-Server Eigenschaften zum Aktivieren der Anzeige von ITOM Gateway-Komponente auf dem Bildschirm „Übersicht“.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu den auf dem Übersichtsbildschirm angezeigten Daten finden Sie unter Überwachen des Protokolldaten-Flows und Optimieren der Integrationseinstellungen in Health Log Analytics.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. Auf der **Installierte Integrationen** Suchen Sie nach einer aktiven Integration, und öffnen Sie sie.
   Die **Übersicht** Bildschirm wird angezeigt, der den Daten-Streaming-Status der Integration und die Daten der Protokolldatenquellen anzeigt.

   Hinweis: Die ServiceNow Die Integration des Abrufs von Systemprotokollen wird nicht für ausgeführt MID-Server. Daher wird für diese Integration die verwendet **Übersicht** Auf dem Bildschirm wird nicht angezeigt MID-Server Streaming-Status.

4. Analysieren Sie die bereitgestellten Daten, und untersuchen Sie alle Daten-Streaming-Probleme.
5. **Wahlweise:** Passen Sie die Konfiguration der Integration bei Bedarf an.

   Verwenden Sie die Optionen im Menü Ansicht ( ) , Um zur relevanten Tabelle oder zum Protokoll-Viewer zu navigieren.

   Hinweis: Der Inhalt des Menüs „Ansicht“ ändert sich dynamisch, je nachdem, ob die referenzierten Tabellen Daten enthalten.

Menüoptionen anzeigen

Option	Beschreibung
Dateneingabezuordnung	Öffnet **Dateneingabezuordnung** Seite. Auf dieser Seite können Sie Quellen manuell zuordnen, wenn HLA Eigenschaften wurden nicht automatisch erkannt. Weitere Informationen finden Sie unter Ordnen Sie Rohprotokolldaten in zu Health Log Analytics.
Quelltypstruktur	Öffnet **Quelltypstrukturen** Seite. In der Quelltypstruktur werden Protokolldaten basierend auf ihrem Ursprung oder Typ klassifiziert und organisiert. Sie können die Struktur anpassen und überprüfen, ob die HLA KI-Engine extrahiert Eigenschaften ordnungsgemäß und klassifiziert sie korrekt. Weitere Informationen finden Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	unter Anpassung der Quelltypstruktur in Health Log Analytics.
Protokollquellen	Öffnet **Protokollquellen** Tabelle. Mit dieser Tabelle können Sie das überprüfen HLA Hat alle Ihre Protokollquellen erstellt. Wenn eine Protokollquelle fehlt, können Sie sie manuell hinzufügen. Weitere Informationen finden Sie unter Verifizieren Sie Ihre Protokollquellen in Health Log Analytics.
Protokoll-Viewer	Öffnet **Protokoll-Viewer** , Der die Häufigkeit von Anomalien in den Protokolldaten während eines bestimmten Zeitraums anzeigt. Weitere Informationen finden Sie unter Überprüfen der Protokolle, die mit einer Warnung im Protokoll-Viewer in verbunden sind Health Log Analytics. **Hinweis:** Die Option Protokoll-Viewer wird nur angezeigt, wenn Service Operations-Arbeitsbereich Log Analytics Anwendung ist installiert.

6. Wenn Sie Daten-Streaming-Probleme gelöst und die Konfiguration behoben haben, wählen Sie aus **Testen und speichern** .
   Das System speichert die aktualisierte Konfiguration in der Datenbank und testet den konfigurierten Port, wobei entweder Erfolg oder Fehler zurückgegeben werden. Wenn ein Fehler zurückgegeben wird, korrigieren Sie die Konfiguration gemäß den Vorschlägen auf dem Bildschirm, und wählen Sie dann aus **Testen und speichern** Erneut. Sobald der Test erfolgreich ist, fahren Sie mit dem nächsten Schritt fort.
7. Aktivieren Sie die Integration erneut.

Bearbeiten Sie eine installierte Integration in Health Log Analytics

Bearbeiten Sie eine installierte Integration für das Streaming von Protokolldaten nach Health Log Analytics Auf der Integrations Launchpad. Sie können beispielsweise zu einer anderen Serviceinstanz wechseln.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Installierte Integrationen** Suchen Sie nach der Kachel für die Integration, die Sie bearbeiten möchten, und wählen Sie sie aus.
4. Wählen Sie eine Registerkarte aus, die Sie bearbeiten möchten.
5. Wählen Sie Aus **Deaktivieren** Zum Deaktivieren der Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie müssen die Integration deaktivieren, bevor Sie sie bearbeiten können.

6. Wählen Sie **Bearbeiten**.
7. Bearbeiten Sie die Integration entsprechend Ihren Anforderungen.
8. Wählen Sie Aus **Testen und speichern** .
   Health Log Analytics Testet MID-Server Konnektivität, wobei entweder Erfolg oder Fehler zurückgegeben werden. Wenn ein Fehler zurückgegeben wird, nehmen Sie Anpassungen an Ihrer Konfiguration vor, wie auf dem Bildschirm vorgeschlagen, und wählen Sie dann aus **Testen und speichern** Erneut. Wenn der Test erfolgreich ist, können Sie die Integration erneut aktivieren.
9. Wählen Sie **Aktivieren**.

Deaktivieren Sie eine Protokolldatenintegration in Health Log Analytics

Deaktivieren Sie eine Integration für das Streaming von Protokolldaten an Health Log Analytics Auf der Integrations Launchpad. Eine deaktivierte Integration beendet das Streamen von Protokollen an Ihren ServiceNow Instanz, ist aber noch verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Installierte Integrationen** Suchen Sie nach der Integrationskachel für die Integration, die Sie deaktivieren möchten, und wählen Sie sie aus.
4. In **Übersicht** Wählen Sie die Registerkarte aus **Deaktivieren** .

Ergebnis

Die Integration ist deaktiviert und beendet das Streamen von Protokolldaten an die Instanz. Die deaktivierte Integration ist weiterhin auf verfügbar Integrations Launchpad In **Installierte Integrationen** Registerkarte, unter **Warten auf Ihre Aktion** .

Richten Sie Dateneingaben in ein Health Log Analytics Mit geführtem Setup

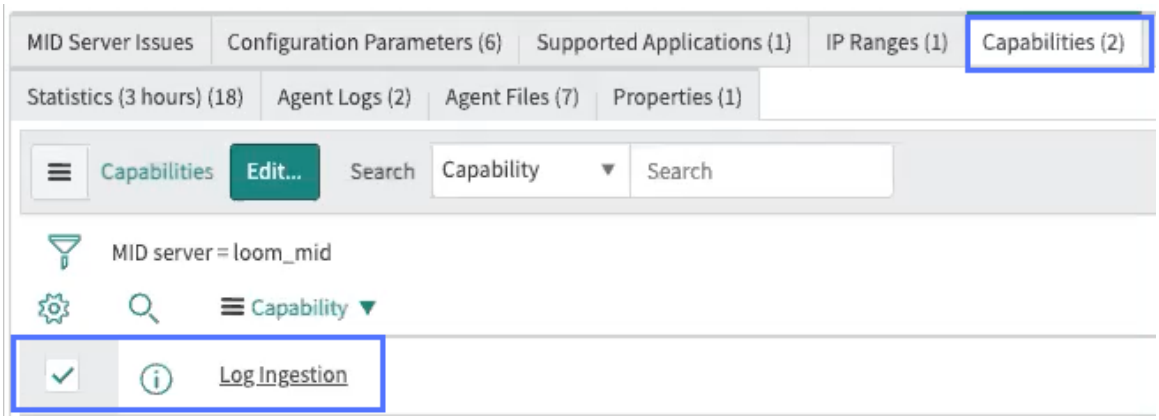
Das Guided Setup von Health Log Analytics bietet eine Reihe von Aufgaben, die Sie beim Erstellen von Dateneingaben für Ihre ServiceNow-Instanz unterstützen. Die Dateneingabekonfiguration ist ein wichtiger Schritt beim Einrichten von Health Log Analytics Anwendung. Durch die Verwendung des Guided Setups wird sichergestellt, dass Sie über das erforderliche Mindestsetup für den Dateneingabeprozess verfügen.

Vorbereitungen

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

- Für MID-Server Proxy-Anforderungen, siehe MID-Server Proxy-Voraussetzungen für das Streaming von Protokollen an Health Log Analytics.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Informationen zur Verwendung der Schnittstelle für das geführte Setup finden Sie unter Mit geführtem Setup .

Prozedur

1. Navigieren zu **Alle** > **Geführtes Setup** > **Geführtes Setup für ITOM** > **Health Log Analytics**an.
2. Befolgen Sie die Anweisungen, um eine Dateneingabe auszuwählen und einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sobald Sie den Dateneingabe-Connector erstellt haben, fahren Sie mit fort Ordnen Sie Ihre Rohprotokolldaten zu .

Zugehörige Informationen

Unterstützte Dateneingaben für Health Log Analytics

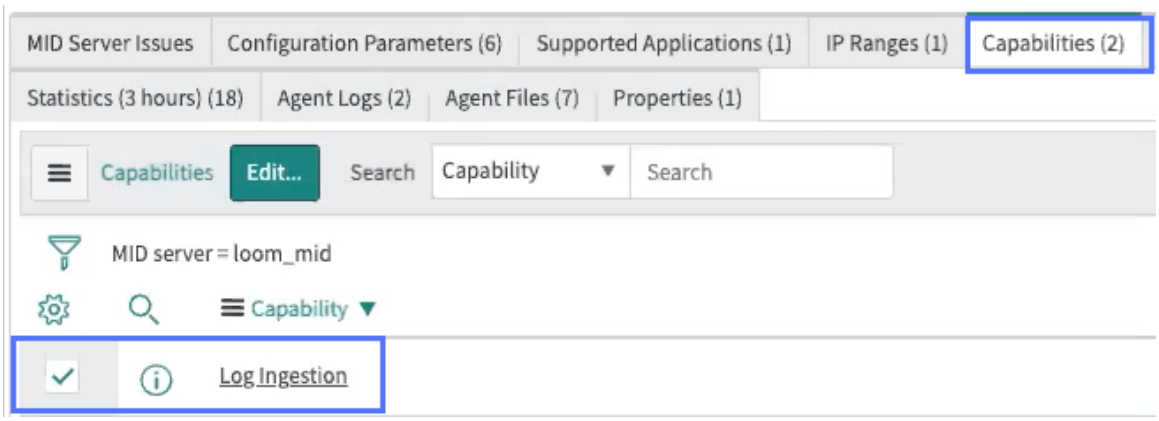
Richten Sie Dateneingaben in ein Health Log Analytics Manuell

Richten Sie Ihr ein Health Log Analytics Dateneingaben für Health Log Analytics Manuell. Die Dateneingabekonfiguration ist ein wichtiger Schritt beim Einrichten von Health Log Analytics Anwendung.

Vorbereitungen

Hinweis: Erwägen Sie die Verwendung von Health Log Analytics Geführtes Setup für die Dateneingabe, das sicherstellt, dass Sie über das erforderliche Minimum für den Dateneingabeprozess verfügen. Weitere Informationen finden Sie unter Richten Sie Dateneingaben in ein Health Log Analytics Mit geführtem Setup.

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

- Für MID-Server Proxy-Anforderungen, siehe MID-Server Proxy-Voraussetzungen für das Streaming von Protokollen an Health Log Analytics.

Erforderliche Rolle: evt_mgmt_admin. Für ServiceNow Dateneingabe für Systemprotokolle: administrator.

Prozedur

1. Richten Sie eine Dateneingabe manuell ein, indem Sie das entsprechende Verfahren ausführen, das in der Produktdokumentation beschrieben wird.

Dateneingaben

Dateneingabe	Beschreibung
Rsyslog oder Beats	Die Dateneingabe streamt Protokolldaten mit Rsyslog oder Beats in Ihre Instanz.
Splunk	Die Dateneingabe streamt Protokolldaten mit Splunk in Ihre Instanz.
Splunk-Abfrage	Die Dateneingabe ruft regelmäßig Protokolldaten aus ab Splunk Mithilfe einer Abfrage.
Elasticsearch	Die Dateneingabe ruft Protokolldaten aus Elasticsearch-Indizes in Ihre Instanz ab.
TCP	Die Dateneingabe sendet Rohprotokollmeldungen direkt über ein TCP/SSL-Socket an Ihre Instanz.
UDP	Die Dateneingabe streamt Rohprotokollnachrichten an Ihren ServiceNow Instanz direkt über einen UDP-Socket.
GCP-PubSub	Die Dateneingabe empfängt Protokollnachrichten, die in einem veröffentlicht werden Google Cloud Pub-/Unterthema und streamt sie an Ihren ServiceNow Instanz.
MID-Server	Die Dateneingabe sammelt MID-Server-Protokolldateien und streamt sie an Ihre Instanz.
Amazon CloudWatch	Die Dateneingabe streamt Protokolldaten aus Amazon CloudWatch an Ihre ServiceNow-Instanz.
Amazon S3 Bucket	Die Dateneingabe streamt Protokolldaten aus dem Amazon S3-Bucket (Simple Storage Service) an Ihre ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateneingabe	Beschreibung
Microsoft Azure Log Analytics	Die Dateneingabe streamt Protokolldaten aus Microsoft Azure Log Analytics an Ihre ServiceNow-Instanz.
Microsoft Azure Event Hubs	Die Dateneingabe streamt Events aus Microsoft Azure Event Hubs an Ihre ServiceNow-Instanz.
Apache Kafka	Die Dateneingabe streamt Protokolldaten aus Apache Kafka an Ihre ServiceNow-Instanz.
REST-API	Die Dateneingabe streamt Protokolldaten im JSON-Format an Ihre ServiceNow-Instanz.
ServiceNow-Systemprotokollabruf	Die Dateneingabe streamt Protokolldaten aus dem ServiceNow Systemprotokolltabelle für Health Log Analytics KI-Engine. **Hinweis:** Nur eine einzelne ServiceNow Die Dateneingabe „Systemprotokolle abrufen“ kann im System vorhanden sein, und nur Anwender mit der Administratorrolle können sie erstellen und konfigurieren. Diese Dateneingabe wird nicht für ausgeführt MID-Server.
Cribl	Die Dateneingabe, die aktiviert werden soll Health Log Analytics Zum Verarbeiten von Cribl-Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz.
Edge Delta	Die Dateneingabe aktiviert Health Log Analytics Dient zur Verarbeitung von Edge-Delta-Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz.
Vector Agent	Die Dateneingabe aktiviert Health Log Analytics Dient zur Verarbeitung von Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz über einen Vector Agent.
Agent Client Collector	Die Dateneingabe streamt Protokollnachrichten mit ServiceNow Agent Client Collector in Ihre ServiceNow-Instanz. Diese Dateneingabe wird für die Verwendung mit der Anwendung Agent Client Collector Log Analytics unterstützt, die im ServiceNow Store verfügbar ist.

Hinweis: Auswählen **Verbindung testen** Stellt am Ende des Verfahrens sicher, dass Ihre Dateneingabe korrekt konfiguriert ist. Sie können eine Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung zwischen besteht MID-Server Und das Daten-Repository wurde eingerichtet.

2. Identifizieren und beheben Sie Streaming-Probleme, um sicherzustellen, dass die Dateneingabe Protokolldaten an den streamt MID-Server Aus allen Quellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.

3. **Wahlweise:** Bearbeiten Sie zuvor Rohprotokolldaten Health Log Analytics Ordnet sie zu und strukturiert sie.
   Weitere Informationen finden Sie unter Bearbeiten Sie Ihre Rohprotokolldaten vor der Verarbeitung .
4. Bestimmen Sie, wie Health Log Analytics Verarbeitet Rohprotokolldaten, die in Ihre Instanz gestreamt werden.
   Standardmäßig wird jede eingehende Protokollzeile automatisch dem richtigen Tag zugeordnet. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren. Weitere Informationen finden Sie unter Ordnen Sie die Rohdaten zu .
5. **Wahlweise:** Optimieren Sie die Quelltypstruktur, um dies sicherzustellen Health Log Analytics Extrahiert und klassifiziert alle Eigenschaften korrekt.
   Weitere Informationen finden Sie unter Verfeinern Sie die Quelltypstruktur in Health Log Analytics.
6. **Wahlweise:** Führen Sie zusätzliche Setup-Aufgaben für die Dateneingabe aus.
   Weitere Informationen finden Sie unter Setup-Aufgaben für zusätzliche Dateneingabe in Health Log Analytics.

Zugehörige Informationen

Unterstützte Dateneingaben für Health Log Analytics

Dateneingaben für werden konfiguriert Health Log Analytics Manuell

Konfigurieren Sie den Dateneingabeprozess manuell in Health Log Analytics. Die Dateneingabekonfiguration ist ein wichtiger Schritt beim Einrichten von Health Log Analytics Anwendung.

Konfigurieren Sie einen Amazon CloudWatch Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus ein Amazon CloudWatch An Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Amazon CloudWatch-Dateneingabe.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Dateneingabekonfigurationsfelder. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Amazon CloudWatch Dateneingaben in Health Log Analytics Manuell.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Dateneingabekonfigurationsfelder.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Dateneingabekonfigurationsfelder. Diese Felder sind obligatorisch.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Amazon CloudWatch An Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Amazon CloudWatch Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie einen Amazon S3 Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus ein Amazon S3(Simple Storage Service) Buckets an Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *`mid.public_ip`* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Amazon S3-Dateneingabe.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Amazon S3 Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbeschreibungen finden Sie unter Amazon S3 Dateneingabekonfigurationsfelder. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Amazon S3 Dateneingaben in Health Log Analytics Manuell.

6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
7. Füllen Sie das Feld auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Amazon S3 Dateneingabekonfigurationsfelder.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Amazon S3 Buckets an Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Amazon S3 Dateneingaben in Health Log Analytics Manuell

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen Apache Kafka Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus ein Apache Kafka An Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Apache Kafka-Dateneingabe.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Apache Kafka Dateneingabekonfigurationsfelder. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Apache Kafka Dateneingaben in Health Log Analytics Manuell.
6. Füllen Sie das Feld auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Dateneingabekonfigurationsfelder.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Dateneingabekonfigurationsfelder.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

- Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

  Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Apache Kafka An Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Apache Kafka Dateneingaben in Health Log Analytics Manuell

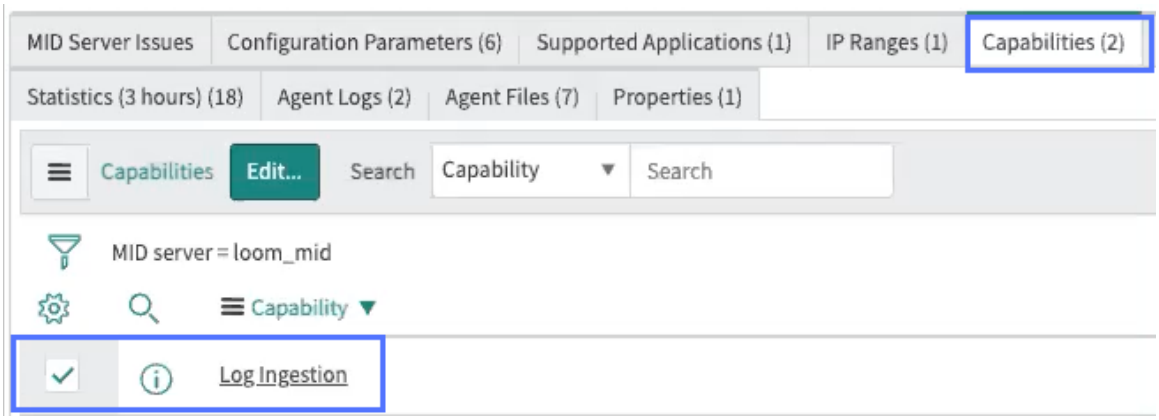
Konfigurieren Sie eine Cribl-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine dedizierte Cribl-Dateneingabe ein, um zu aktivieren Health Log Analytics Zum Verarbeiten von Cribl-Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Cribl zum Filtern und Weiterleiten großer Mengen von Protokolldaten aus verschiedenen Quellen verwendet, das Protokollformat Health Log Analytics„Empfangen“ unterscheidet sich von anderen Typen. Die Cribl-Dateneingabe aktiviert HLA Um Transport-Header von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen, wird nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weitergeleitet.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Cribl-Dateneingabe aus.
4. Auf der **Erste Schritte** Füllen Sie die Formularfelder aus, und wählen Sie dann aus **Als Nächstes** . Feldbeschreibungen finden Sie unter Konfigurationsfelder für Cribl-Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Auf der **Konfiguration** Füllen Sie die Formularfelder aus, und wählen Sie dann aus **Als Nächstes** . Feldbeschreibungen finden Sie unter Konfigurationsfelder für Cribl-Dateneingabe.
6. Auf der **Prozess** Wählen Sie die gewünschte Route aus, und wählen Sie dann aus **Als Nächstes** .

   Weitere Informationen finden Sie unter Konfigurationsfelder für Cribl-Dateneingabe.

   Hinweis: Informationen zur Behebung von Problemen im Zusammenhang mit diesem Schritt finden Sie unter Cribl – Cribl-Dateneingabe einrichten | Fehlerbehebung bei Setup- und Datenerfassungsproblemen [KB0558611] artikel in der Now Support Knowledge Base.

   Die **Beenden** Registerkarte wird geöffnet.
7. Überprüfen Sie in der Cribl-Instanz, ob die Konfiguration der Dateneingabe korrekt ist.
   Sie können die Cribl-Befehle verwenden, die im angezeigt werden **Beenden** Registerkarte nach Bedarf.
8. Wenn die Konfiguration korrekt ist, kehren Sie zur Dateneingabekonfiguration zurück **Beenden** Registerkarte und wählen Sie aus **Veröffentlichen** Zum Veröffentlichen der Dateneingabe.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Die Dateneingabe beginnt mit dem Streamen von Protokolldaten an Ihren ServiceNow Instanz.

Informationen zur Lösung von Problemen im Zusammenhang mit der Erfassung von Protokolldaten aus Cribl finden Sie unter Cribl – Cribl-Dateneingabe einrichten | Fehlerbehebung bei Setup- und Datenerfassungsproblemen [KB0558611] artikel in Now Support Knowledge Base.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

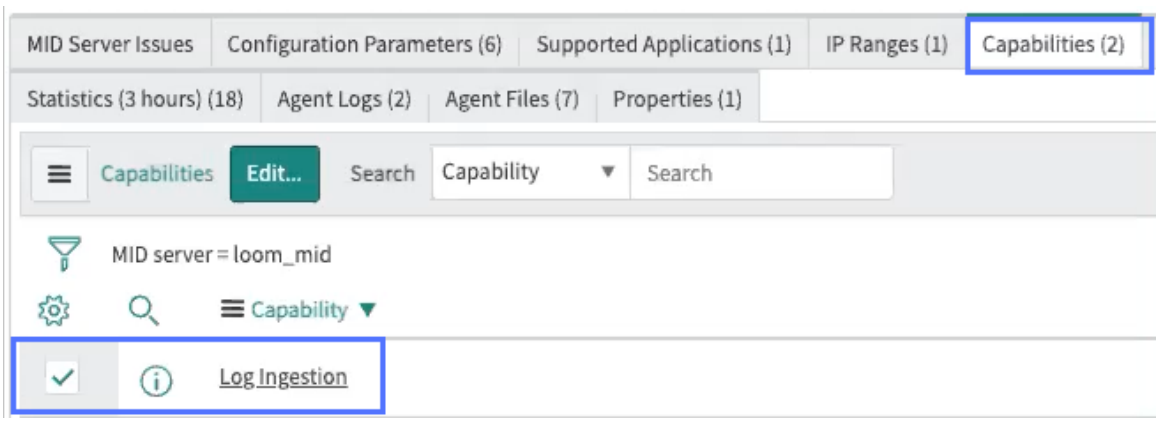
Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie eine Edge-Delta-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Edge Delta-Dateneingabe ein, um zu aktivieren Health Log Analytics Dient zur Verarbeitung von Edge-Delta-Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Edge Delta verwendet, um große Mengen von Protokolldaten aus mehreren Quellen zu verarbeiten, bevor sie an gesendet werden Health Log Analytics, Das Protokollformat HLA„Empfangen“ unterscheidet sich von anderen Typen. Die Edge Delta-Dateneingabe aktiviert HLA Um Transport-Header von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen, wird nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weitergeleitet.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Edge Delta-Dateneingabe aus.
4. Füllen Sie im Formular die Felder aus.
   Eine detaillierte Beschreibung der Felder finden Sie unter Edge Delta-Dateneingabekonfigurationsfelder.
5. Wählen Sie Aus **Speichern** Um Ihre Konfiguration zu speichern.
6. Wählen Sie Aus **Veröffentlichen** Zum Veröffentlichen der Dateneingabe.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle . Die Dateneingabe beginnt mit dem Streamen von Protokolldaten an Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

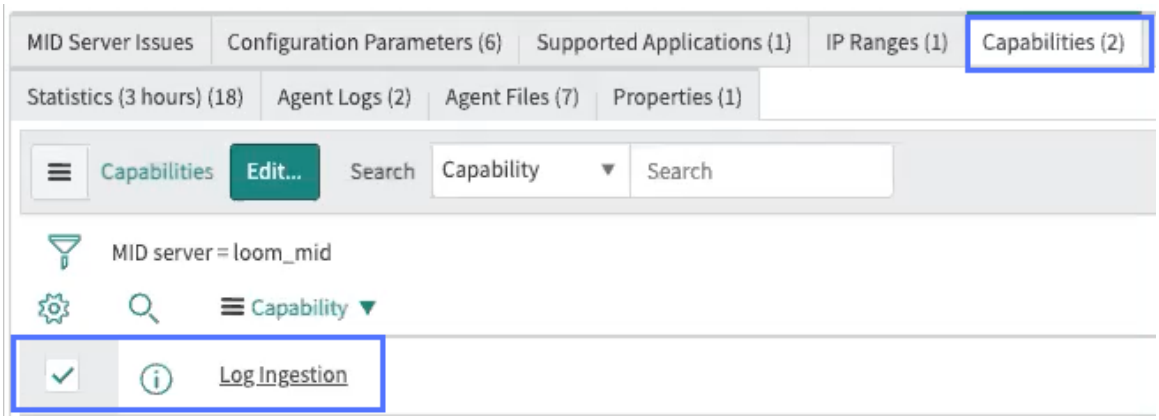
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen Elasticsearch Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus ein Elasticsearch Indizes für Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Health Log Analytics Unterstützt Elasticsearch Versionen über 7.10.2 und unter 8.18.2.

Hinweis: Für erweiterte Informationen zum Streaming von Protokolldaten von Elasticsearch Indizes für Ihre Instanz finden Sie unter Protokolle mithilfe der Elasticsearch-Dateneingabe streamen – Erweiterter Leitfaden [KB1080162] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Elasticsearch-Dateneingabe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie Aus **Erweitert** Zum Festlegen von Feldern für erweiterte Konfiguration.
   Feldbeschreibungen finden Sie unter Elasticsearch Dateneingabekonfigurationsfelder. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Elasticsearch Dateneingaben in Health Log Analytics Manuell.
6. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Dateneingabekonfigurationsfelder.
7. Füllen Sie die Formularfelder auf der Registerkarte **Query Settings** (Abfrageeinstellungen) aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Dateneingabekonfigurationsfelder.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld . Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.
10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Elasticsearch Indizes für Ihren ServiceNow Instanz.

Weitere Informationen zum Streaming von Protokollen mit finden Sie unter Elasticsearch Dateneingabe, siehe Protokolle mithilfe der Elasticsearch-Dateneingabe streamen – Erweiterter Leitfaden [KB1080162] artikel in Now Support Knowledge Base.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

Zugehörige Informationen

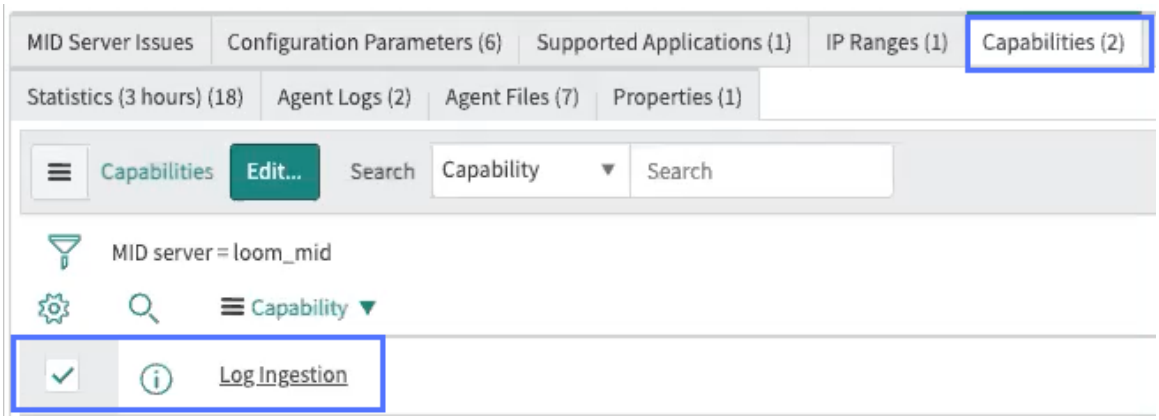
Konfigurieren Sie erweiterte Einstellungen für Elasticsearch Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie eine GCP PubSub-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für den Empfang von Protokollnachrichten ein, die in veröffentlicht wurden Google Cloud Pub-/Unterthema „Platform“ (GCP) und Streaming an Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den GCP PubSub-Dateneingabetyp aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder der GCP-PubSub-Dateneingabe.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder der GCP-PubSub-Dateneingabe.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Empfang von Protokollnachrichten vom Google Cloud Pub-/Unterthema und streamt sie an Ihren ServiceNow Instanz über MID-Server.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Konfigurieren Sie ein Microsoft Azure Event Hubs Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Ereignissen aus ein Microsoft Azure Event Hubs An Ihren ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Microsoft Azure Event Hubs-Dateneingabe.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder.
   Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Event Hubs Dateneingaben in Health Log Analytics Manuell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Microsoft Azure Event Hubs An Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Event Hubs Dateneingaben in Health Log Analytics Manuell

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie ein Microsoft Azure Log Analytics Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus ein Microsoft Azure Log Analytics An Ihren ServiceNow Instanz. Die Dateneingabe verweist die KI-Engine von Health Log Analytics an eine Datenquelle in Ihrem Microsoft Azure Log Analytics-Konto.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *`mid.public_ip`* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Microsoft Azure Log Analytics-Dateneingabe.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder.
   Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Log Analytics Dateneingaben in Health Log Analytics Manuell.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.

   Health Log Analytics Verwendet die in diesen Feldern festgelegten Werte, um die Abfrage für den Empfang von Protokolldaten von zu generieren Microsoft Azure Log Analytics.

   Zum Beispiel:

   ```
   {"query": "ContainerLog | where TimeGenerated > %s | take 500", "project":
    ["TimeGenerated", "LogEntry", "LogEntrySource"]}
   ```

   wobei:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `ContainerProtokoll` : Der Datenquellenname.
- `Zeitgenerierung` : Der Name der Ereigniszeiteigenschaft.
- `500` : Die maximale Anzahl von Zeilen, die in jeder Abfrage abgerufen werden.
- `["TimeGenerated", "LogEntry", "LogEntrySource"]` : Die Ereigniszeit und die kommagetrennte Liste der zurückzugebenden Spaltennamen.

Alternativ können Sie eine anwenderdefinierte Abfrage in konfigurieren **Protokollabfrage** Feld. Der Wert, den Sie in diesem Feld festlegen, überschreibt die Werte in allen anderen Feldern in **Abfrageeinstellungen** Registerkarte mit Ausnahme der **Von** Feld. Wenn **Protokollabfrage** Feld ist leer, Health Log Analytics Generiert die Abfrage anhand der Werte, die in den anderen Feldern auf der Registerkarte festgelegt sind.

Für eine Beschreibung von **Abfrageeinstellungen** Felder, siehe Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder.

7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus Microsoft Azure Log Analytics An Ihren ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

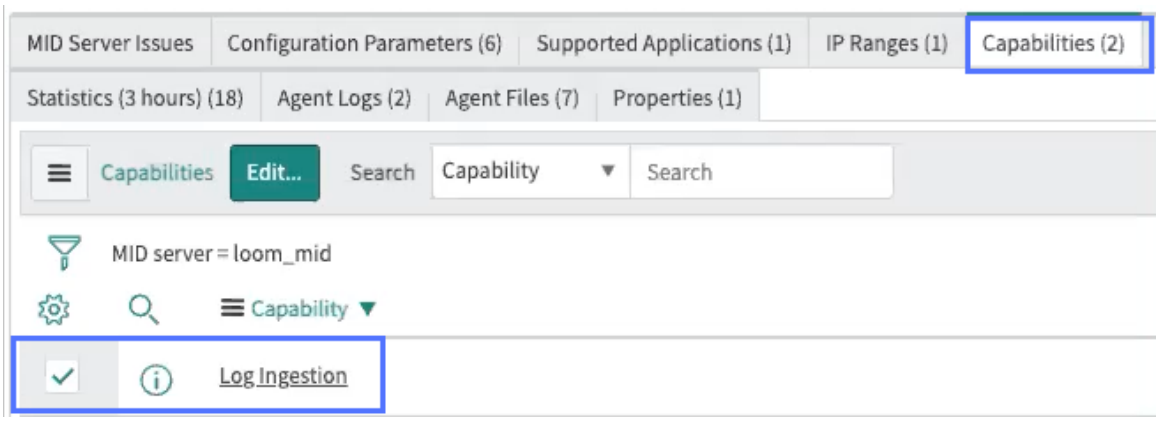
Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Log Analytics Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie ein MID-Server Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Sammeln und Streamen ein MID-Server Protokollieren Sie Nachrichten für ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt, wie Sie eine MID-Server-Dateneingabe auf der Seite „Dateneingaben“ erstellen. Um die MID-Server-Dateneingabe automatisch zu konfigurieren, klicken Sie auf den zugehörigen Link im Formular „MID-Server“.

Wichtig:

- Wenn Sie einen erstellen MID-Server Dateneingabe: Alle Protokolle werden automatisch dem vordefinierten Quelltyp „MID_Server_log“ zugeordnet. Dieser Quelltyp enthält vorkonfigurierte Zuordnungseinstellungen, um den Wert der Überwachung von zu maximieren MID-Server Protokolle. Um das Zuordnungsskript zu überprüfen, navigieren Sie direkt vom Dateneingabekonfigurationsformular zum Zuordnungsformular, indem Sie auswählen **Wechseln Sie zu Zuordnung** Unter zugehörige Links. Überprüfen Sie den Quelltyp, indem Sie zu Quelltypstrukturen navigieren und den Quelltyp MID_Server_log auswählen.
- Um eine optimale Leistung zu erzielen, debuggen MID-Server Protokollnachrichten werden standardmäßig nicht verarbeitet. Wenn Sie Debug-Nachrichten an senden möchten Health Log Analytics Fügen Sie zur Verarbeitung Folgendes zu hinzu MID-Server Eigenschaften: Mid.hla.Mid_Data_input.ignore_debug_level_Logs = falsch.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die MID-Server-Dateneingabe.
4. Geben Sie im Formular eine Beschreibung der Dateneingabe und den Namen des MID-Server an, von dem die Protokolle gestreamt werden.
   Feldbeschreibungen finden Sie unter MID-Server Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen. Füllen Sie im Formular die Felder aus. Feldbeschreibungen finden Sie unter MID-Server Dateneingabekonfigurationsfelder. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für MID-Server Dateneingaben in Health Log Analytics Manuell.
6. Wählen Sie **Absenden**.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit der Erfassung und dem Streaming MID-Server Protokollieren Sie Nachrichten für ServiceNow Instanz.

Eine Beschreibung, wie diese Dateneingabe Ihnen helfen kann, neu auftretende Probleme in Ihrer Organisation zu erkennen und zu lösen ServiceNow Instanz, siehe Anwendungsfall: Proaktive Überwachung von ServiceNow Instanz in Health Log Analytics.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

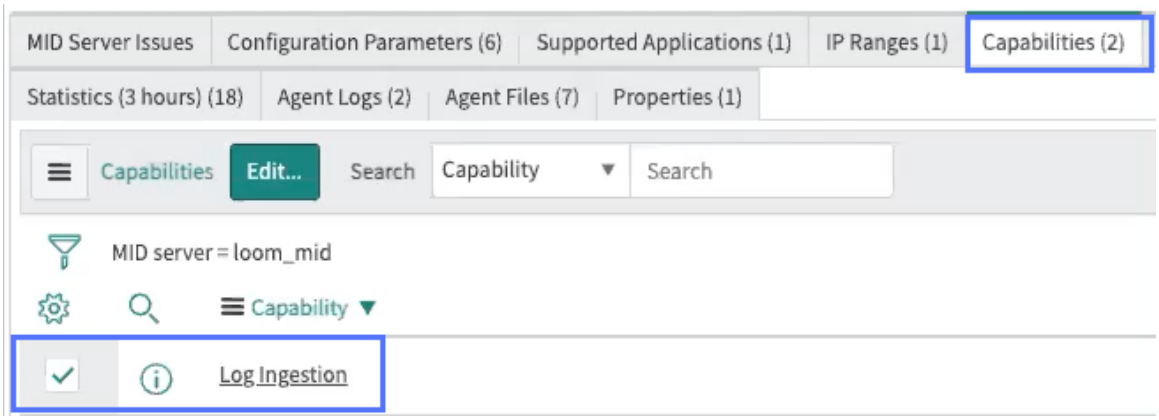
Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie eine REST-API-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine REST-API-Dateneingabe für das Streaming von Protokolldaten an Ihren ein ServiceNow Instanz.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Wählen Sie im Formular „MID-Webserver-Kontext“ im Feld **Ausführen für** die Option *Spezifischer MID Server* und nicht die Clusteroption aus. In **MID-Server** Wählen Sie das spezifische aus MID-Server Zu dem die Protokolldaten abgerufen werden.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die REST API-Dateneingabe aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für REST-API-Dateneingabe.
5. Wählen Sie **Speichern**.
   - Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle.
   - Das System generiert automatisch die REST API-Dateneingabe-URL zum Senden von Protokollen an die MID-Server. Die generierte URL hat dieses Format: `http://(MID_SERVER_IP):(MID_WEB_SERVER_PORT)/ap1/mid/hla/raw` . HLA Ersetzt `(MID_SERVER_IP)` Und `(MID_WEB_SERVER_PORT)` Mit den von Ihnen konfigurierten Werten.
6. Kopieren Sie die generierte URL.
7. Weisen Sie Ihren API-Client an, Protokollnachrichten an zu senden MID-Server.

   a. Konfigurieren Sie im API-Client eine Anforderung mit den folgenden Parametern:
      - HTTP-Methode: POST.
      - URL: Die URL, die Sie im vorherigen Schritt kopiert haben.
      - Authentifizierung: Die erforderlichen Anmeldeinformationen für die Authentifizierung. Beispiel: Standardauthentifizierung (Anwendername und Passwort).

        Hinweis: Die Authentifizierungsmethode muss mit der auf dem MID-Webserver konfigurierten Methode identisch sein.

      - Header: Legen Sie fest `Inhaltstyp` Header, der Ihrem Nutzlastformat entspricht.
        - Für JSON: `Anwendung/JSON` .
        - Für Rohtext: `Text/nur` .
      - Textkörper: Die Protokollnutzlast in JSON oder Rohtext.

   b. Senden Sie die Anforderung.
      Eine erfolgreiche Antwort gibt an, dass MID-Server Hat die Nutzlast erhalten. Wenn MID-Server Hat die Protokollnachrichten verarbeitet, die Dateneingabe streamt sie an Ihren ServiceNow Instanz, die das REST-Protokoll verwendet.

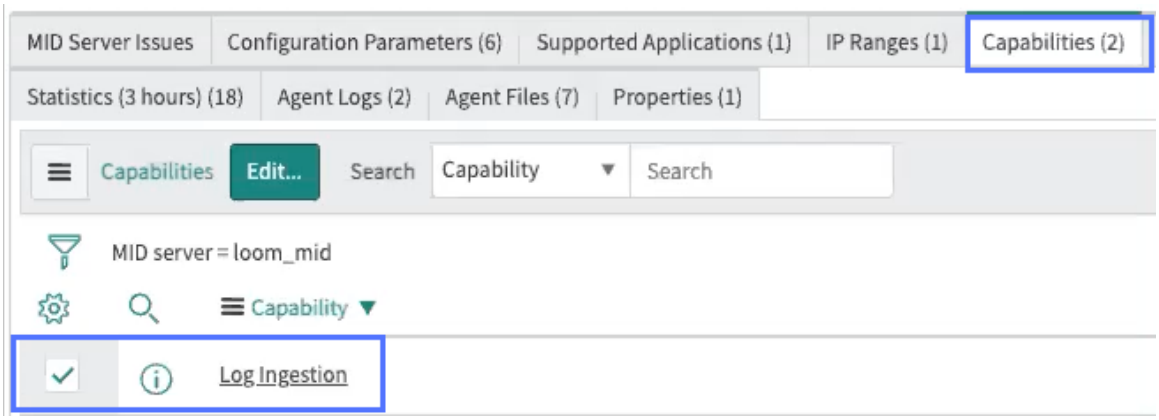
Konfigurieren Sie ein Rsyslog, Filebeat, Oder Winlogbeat Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokollnachrichten an ein ServiceNow Instanz mit Rsyslog, Filebeat, Oder Winlogbeat Service Desk-Mitarbeiter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den zu erstellenden Dateneingabetyp aus den in der Tabelle beschriebenen verfügbaren Dateneingabetypen aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateneingabetypen

Typ	Beschreibung
Rsyslog	Streamt Protokollmeldungen von UNIX-basierten Servern an die KI-Engine von ServiceNow mit dem Rsyslog-Agent
Linux mit Filebeat	Streamt Systemprotokollnachrichten und lokale Dateien aus Linux Server zur -Instanz mit Filebeat Service Desk-Mitarbeiter.
Windows Anwendungsprotokolle mit Filebeat	Streamt lokale Dateien aus Microsoft Windows-Geräte für ServiceNow Instanz, die verwendet Filebeat Service Desk-Mitarbeiter.
Windows Betriebssystem mit Winlogbeat	Streams Windows Ereignisprotokolle für ServiceNow Instanz, die verwendet Winlogbeat Service Desk-Mitarbeiter.

4. Füllen Sie das Formular auf der Registerkarte **Erste Schritte** aus.

   Feldbeschreibungen finden Sie unter Rsyslog Dateneingabekonfigurationsfelder , Filebeat oder Winlogbeat.

   Hinweis: Beim Erstellen einer Dateneingabe für Linux mit Filebeat, Sie können ein Inhaltspaket aus auswählen **Inhaltspaket** Dropdown-Liste. Das Inhaltspaket enthält Standardquelltypen und Zuordnungsskriptvorlagen, die Ihnen die Zeit sparen, die Sie benötigen, um sie von Grund auf neu zu erstellen. Weitere Informationen finden Sie unter Health Log Analytics Inhaltspakete für kürzere Amortisierungszeit.

5. Wenn Rsyslog, Filebeat, Oder Winlogbeat Agent wurde nicht bereits installiert. Laden Sie ihn herunter, und installieren Sie ihn aus dem **Installation** Registerkarte.
   Installationsanweisungen finden Sie in der Produktdokumentation des jeweiligen Service Desk-Mitarbeiters.

   Hinweis: Stellen Sie sicher, dass Sie die neueste Version des Agent ausführen. Frühere Versionen funktionieren, aber mit eingeschränkter Funktionalität.

6. Auf der **Tagging und Bindung** Registerkarte Protokolle einer Serviceinstanz in zuweisen Configuration Management Database (CMDB) Damit der Service die Protokolldaten korrelieren und dem System die Ursachenanalyse ermöglichen kann.

   a. Konfigurieren Sie für jede Quelle den Pfad und die Serviceinstanz für die Protokolle, die gestreamt werden sollen.

      Hinweis: Standardmäßig nur die Pflichtfelder **Pfad** Und **Serviceinstanz** Angezeigt.

      Feldbeschreibungen finden Sie unter Rsyslog Dateneingabekonfigurationsfelder , Filebeat oder Winlogbeat.

   b. Wenn Sie mehrzeilige Protokolle mit versenden möchten Filebeat, Konfigurieren Sie die Eigenschaften, die steuern, wie Filebeat Verarbeitet Nachrichten, die sich über mehrere Textzeilen erstrecken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übereinstimmung	Gibt an, wie Filebeat Kombiniert übereinstimmende Positionen in einem Ereignis.
Negieren	Definiert, ob das in den Protokollzeilen identifizierte Muster negiert wird
Regulärer Ausdruck	Gibt den regulären Ausdruck an

Hinweis: Health Log Analytics unterstützt derzeit keine mehrzeiligen Eigenschaften für Rsyslog.

c. Wahlweise: Definieren Sie zusätzliche Protokollpfade, damit die Dateneingabe Protokolltypen aus mehreren Pfaden streamen kann.
Gehen Sie für jeden zusätzlichen Protokollpfad wie folgt vor:

i. Fügen Sie eine neue Zeile ein.

ii. Konfigurieren Sie den Protokollpfad.

iii. Wählen Sie eine Serviceinstanz aus.

iv. (Optional) Wählen Sie eine Komponente und einen Quelltyp aus.

Hinweis: Diese Option ist bei Verwendung von nicht verfügbar oder erforderlich Winlogbeat, Weil Health Log Analytics Streamt Windows Ereignisprotokolle.

7. Schließen Sie auf der Registerkarte **Fertigstellen** die Konfiguration für Ihren Dateneingabetyp ab.

- Rsyslog:

  a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/rsyslog.d/rsyslog.conf`.

  Hinweis: Wenn Sie Health Log Analytics Anwendung, Version 20.0.11 – Juli 2021, verfügbar über ServiceNow Store verwenden, gehen Sie stattdessen wie folgt vor:

  i. Installieren Sie auf dem Endpunktgerät die Konfigurationsdatei im Verzeichnis `/etc/rsyslog.d/`.

  ii. Erstellen Sie ein Spool-Verzeichnis, indem Sie den Befehl `sudo mkdir -p/var/spool/rsyslog` ausführen.

  b. Validieren Sie die Konfiguration, indem Sie den Befehl `rsyslogd -N1` ausführen und die Ausgabe überprüfen.

  c. Starten Sie Rsyslog neu, indem Sie den Befehl `sudo systemctl restart rsyslog` ausführen.

  d. Überprüfen Sie die Ausgabe. Wenn die Systemprotokolldatei `/var/log/messages` Fehler enthält, prüfen und beheben Sie die Fehlermeldungen.

- Linux Verwenden Filebeat:

  a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/filebeat/`.

  b. Starten Sie den Agent-Service, indem Sie den Befehl `sudo service filebeat start` ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfiguration ändern.

c. Starten Sie den Agent-Service neu, indem Sie den entsprechenden Befehl ausführen.

- Windows Verwenden Beats(Filebeat Oder Winlogbeat):

a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis C:\Programme\.

b. Starten Sie den Agent-Service neu, indem Sie den entsprechenden PowerShell-Befehl ausführen.

- Filebeat: `PS > Start-Service filebeat`
- Winlogbeat: `PS > Start-Service winlogbeat`

Hinweis: Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfiguration ändern.

c. Starten Sie den Agent-Service neu, indem Sie den entsprechenden Befehl ausführen.

8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

10. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streamen von Protokolldaten an Ihren ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Konfigurationsdatei Health Log Analytics Generiert für neu Filebeat Dateneingaben sind kompatibel mit Filebeat Version 7,14 und höher. Das Minimum Filebeat Version, die Elasticsearch Derzeit unterstützt wird 7,17, das sich dem Ende seiner Lebensdauer nähert.

Vorhanden Filebeat Dateneingabekonfigurationsdateien in HLA Sind kompatibel mit Filebeat Versionen bis zu 8.x. Für Filebeat Version 9,0 und höher: Migrieren Sie entweder von der Protokolleingabe zur Dateistromeingabe, oder generieren Sie eine neue Konfigurationsdatei. Weitere Informationen zum Migrationsprozess finden Sie unter Filebeat Dokumentation an.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Beats Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie ein ServiceNow Systemprotokolle – Dateneingabe in abrufen Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokolldaten aus dem ein ServiceNow Systemprotokolltabelle für HLA Engine (auch bekannt als Occultus).

Vorbereitungen

Hinweis: Nur eine einzelne ServiceNow Die Dateneingabe „Systemprotokolle abrufen“ kann im System vorhanden sein. Diese Dateneingabe wird nicht auf einem MID-Server ausgeführt.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie aus ServiceNow Systemprotokolle – Dateneingabe abrufen.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter ServiceNow Systemprotokolle – Dateneingabekonfigurationsfelder abrufen.
5. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an.

Die Dateneingabe beginnt mit dem Streaming ServiceNow Protokollieren Sie Daten aus der Tabelle „Systemprotokoll“ in Health Log Analytics KI-Engine, basierend auf den konfigurierten Filtern. Administratoranwender können Filter festlegen, um die Tabelle „Systemprotokoll“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abzufragen. Operatoren können die Protokolle überwachen und die Warnungen anzeigen, die darauf hinweisen Health Log Analytics Generiert aus ihnen.

Eine Beschreibung, wie diese Dateneingabe Ihnen helfen kann, neu auftretende Probleme in Ihrer Organisation zu erkennen und zu lösen ServiceNow Instanz, siehe Anwendungsfall: Proaktive Überwachung von ServiceNow Instanz in Health Log Analytics.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

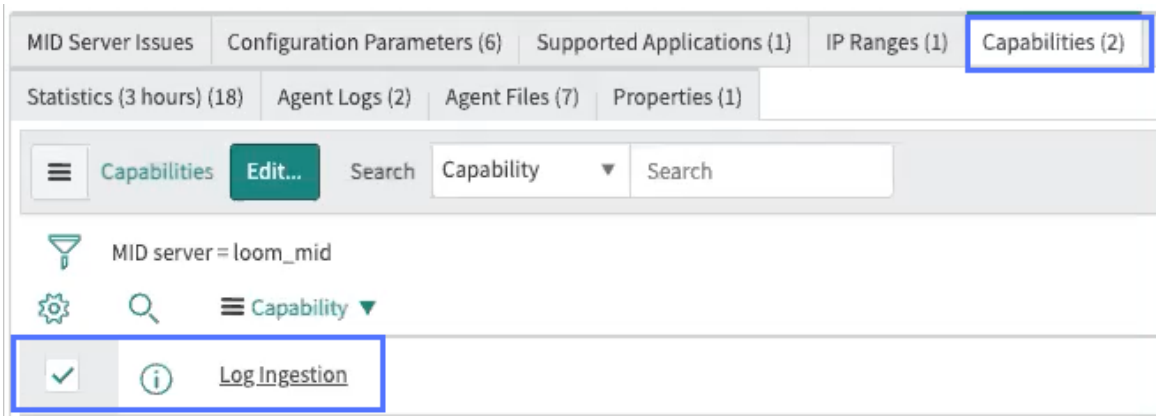
Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie ein Splunk Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Streaming von Protokollnachrichten an ein ServiceNow Instanz mit Splunk Schwerer Forwarder.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

- Konfigurieren Sie Splunk, um Protokolle mit Syslog an Ihre ServiceNow-Instanz weiterzuleiten.
- Die Konfiguration dieser Dateneingabe setzt das Vorhandensein einer Umgebungsvariablen namens $ SPLUNK_HOME voraus. In Unix-ähnlichen Umgebungen verweist diese Variable normalerweise auf /opt/splunk.

Hinweis: Die Windows Die Umgebung verwendet dieselbe Verzeichnisstruktur, jedoch mit umgekehrten Schrägstrichen (\).

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Setupverfahren dient zum Streamen von Protokollen an Ihre Instanz mit einem Splunk Heavy Forwarder. Wenn Sie keinen schweren Forwarder verwenden können, können Sie einen verwenden Splunk Stattdessen Universal Forwarder. Weitere Informationen finden Sie im Artikel Splunk Universal Forwarder as a Shipping method [KB0961378] (Splunk Universal Forwarder als Versandmethode) in der Knowledge Base des Now Support.

Startet in Yokohama Familien-Release, können Sie neu verwenden Splunk Dateneingaben zum Erfassen von Daten im vorverarbeiteten Protokollweiterleitungsformat („gekocht“), das Splunk Verwendet standardmäßig. Im Modus „warm“ Splunk Weiterleitung bettet Konfigurationsdetails wie Host, Quelltyp, Quelle und andere Einstellungen in die Protokolldaten ein. Daten werden in erfasst HLA In diesem Format Verifizieren S, dass jede Protokollzeile alle relevanten kontextbezogenen Informationen enthält. Wenn Sie die Option „gekochte Daten“ in verwenden HLA, Es ist nicht erforderlich, den zu bearbeiten Eigenschaften.Konf. Und Transforms.conf Dateien während Splunk Dateneingabekonfiguration.

Hinweis: Alle Splunk-Konfigurationsdateien befinden sich im Ordner $SPLUNK_HOME/etc/system/local/. Wenn eine Konfigurationsdatei, die Sie ändern müssen, nicht vorhanden ist, erstellen Sie sie und speichern Sie sie in diesem Ordner.

Hinweis: Ein ausgefallener MID-Server kann eine Blockade in Ihrer Splunk-Pipeline verursachen. Eine volle Verarbeitungswarteschlange wirkt sich nicht auf die Pipeline aus.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie aus Splunk Dateneingabe Zum Streamen von Protokollen über einen Splunk Schwerer Forwarder oder Universal-Forwarder .
4. Füllen Sie die Formularfelder auf der Registerkarte **Erste Schritte** aus.
   Feldbeschreibungen finden Sie unter Splunk Dateneingabekonfigurationsfelder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Fügen Sie auf der Registerkarte **Outputs.conf** der Datei outputs.conf die folgenden Absätze hinzu, damit der Versender Protokolldaten über das ausgewählte Transportprotokoll und den ausgewählten Port weiterleitet, und wählen Sie dann **Weiter** aus.

   Hinweis: Wenn Sie bereits Ausgaben konfiguriert haben, führen Sie diese Zeilen mit Ihrer vorhandenen Konfiguration zusammen.

   - Weiterleitung über TCP:

     Hinweis: Verwenden Sie den ersten Absatz nur, wenn Sie noch keinen tcpout-Absatz konfiguriert haben. Der zweite Absatz ist für die Weiterleitung an Health Log Analytics über TCP erforderlich.

     ```
     [tcpout]
     indexAndForward = 1
     defaultGroup = nothing

     [tcpout:health_log_analytics]
     server = ip-172-31-17-121.us-east-2.compute.internal:5000
     sendCookedData = false
     compressed = false
     ```

   - Weiterleitung über UDP:

     Hinweis: Verwenden Sie den ersten Absatz nur, wenn Sie noch keinen syslog-Absatz konfiguriert haben. Der zweite Absatz ist für die Weiterleitung an Health Log Analytics über UDP erforderlich.

     ```
     [syslog]defaultGroup = nothing

     [syslog:health_log_analytics]
     server = ip-172-31-17-121.us-east-2.compute.internal:5000
     ```

6. Bearbeiten Sie auf der Registerkarte **Props.conf** die Datei props.conf und wählen Sie **Weiter** aus.

   Hinweis: Wenn Sie ausgewählt haben **Gearbeitete Daten Verwenden** Option auf **Erste Schritte** Registerkarte, muss nicht bearbeitet werden Eigenschaften.Konf. Datei.

   a. Ändern Sie vorhandene Strophe, oder fügen Sie Strophe hinzu, um Quelltypen, Serviceinstanzen und Hosts für die Weiterleitung an zu markieren Health Log Analytics.

      Hinweis: Um optimale Ergebnisse zu erzielen, markieren Sie nur Quelltypen zur Weiterleitung.

      Verwenden Sie beim Hinzufügen von Absätzen folgende Namenformate:

      - Quelltypen: [<source type>]. Beispiel: [syslog]
      - Quellen (nicht empfohlen): [source::<source>]. Beispiel: [source::myApp]
      - Hosts (nicht empfohlen): [host::<host>]. Beispiel: [host::10.9.8.7]

   b. Fügen Sie am Ende jedes Absatzes, den Sie entweder über TCP oder UDP an Health Log Analytics weiterleiten möchten, die folgende Zeile hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weiterleitung über TCP:

```
TRANSFORMS-cloned_data = clone_for_hla_store_sourcetype, clone_for_hla
```

- Weiterleitung über UDP:

```
TRANSFORMS-cloned_data = clone_for_hla_store_sourcetype, clone_for_hla_udp
```

Diese Zeile wendet die Transformation CLONE_SOURCETYPE auf die Daten an, um zu verhindern, dass die für die Health Log Analytics-Verarbeitung erforderliche Bearbeitung Ihre vorhandene Datenpipeline beeinträchtigt. Um beispielsweise alle Protokolle vom Quelltyp „syslog“ an Health Log Analytics zu senden, gehen Sie wie folgt vor:

```
[syslog]
                        #existing configuration goes here
                        TRANSFORMS-cloned_data = clone_for_hla_store_sourcetype,
clone_for_hla_udp
```

c. Fügen Sie den folgenden Absatz hinzu, um alle relevanten Transformationen anzuwenden, die für die Health Log Analytics-Verarbeitung erforderlich sind:

Hinweis: Mit Splunk können Sie vertrauliche Daten im geklonten Quelltyp für das ausgewählte Protokoll anonymisieren. Weitere Informationen finden Sie im Abschnitt „Anonymize data“ (Daten anonymisieren) in der Splunk-Dokumentation .

- Weiterleitung über TCP:

```
[send_to_hla_tcp]
TRANSFORMS-health_log_analytics = health_log_analytics_add_sourcetype,
 health_log_analytics_add_host, health_log_analytics_add_source,
 health_log_analytics_add_syslog5424, health_log_analytics_add_index,
 health_log_analytics_add_syslogHost, health_log_analytics_add_time
```

- Weiterleitung über UDP:

```
[send_to_hla_udp]
TRANSFORMS-health_log_analytics = health_log_analytics_add_sourcetype,
 health_log_analytics_add_host, health_log_analytics_add_source,
 health_log_analytics_add_syslog5424, health_log_analytics_add_index,
 health_log_analytics_add_syslogHost, health_log_analytics_add_time
```

7. Fügen Sie auf der Registerkarte **Transforms.conf** der Datei transforms.conf die folgenden Absätze hinzu und wählen Sie anschließend **Weiter** aus.

Hinweis: Wenn Sie ausgewählt haben **Gearbeitete Daten Verwenden** Option auf **Erste Schritte** Registerkarte, muss nicht bearbeitet werden Transforms.conf Datei.

Der dritte Absatz klont die Protokolle zur weiteren Bearbeitung, ohne sich auf die vorhandene Indizierung auszuwirken. Die verbleibenden Absätze fügen die Informationen hinzu, die für die korrekte Verarbeitung von Health Log Analytics erforderlich sind.

Hinweis: Sie können sensible Daten verschleiern, indem Sie hier eine Transformation hinzufügen und dann den Absatz des geklonten Quelltyps in der Datei props.conf ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
[accepted_keys]
#Custom field for preserving sourcetype
hla_sourcetype_preservation=_hla_sourcetype

#Store sourcetype in a custom field, since CLONE_SOURCETYPE overwrites it
[clone_for_hla_store_sourcetype]
SOURCE_KEY = MetaData:Sourcetype
REGEX = ^sourcetype::(.+)$
FORMAT = hla_sourcetype::$1
DEST_KEY = _hla_sourcetype

[clone_for_hla]
REGEX=.
DEST_KEY = _TCP_ROUTING
FORMAT = health_log_analytics
CLONE_SOURCETYPE=send_to_hla_tcp

#Only used in case of UDP forwarding
[clone_for_hla_udp]
REGEX=.
DEST_KEY = _SYSLOG_ROUTING
FORMAT = health_log_analytics
CLONE_SOURCETYPE=send_to_hla_udp

#Add metadata to the log message, since metadata is lost when forwarding externally
[health_log_analytics_add_sourcetype]
SOURCE_KEY = _hla_sourcetype
REGEX = ^hla_sourcetype::(.+)$
FORMAT = sourcetype="$1"] $0
DEST_KEY = _raw

[health_log_analytics_add_host]
SOURCE_KEY = MetaData:Host
REGEX = ^host::(.+)$
FORMAT = host="$1" $0
DEST_KEY = _raw

[health_log_analytics_add_source]
SOURCE_KEY = MetaData:Source
REGEX = ^source::(.+)$
FORMAT = source="$1" $0
DEST_KEY = _raw

[health_log_analytics_add_syslog5424]
REGEX=.
FORMAT = - - [sdid@1234 $0
DEST_KEY = _raw

[health_log_analytics_add_index]
SOURCE_KEY = _MetaData:Index
REGEX = ^(.+)$
FORMAT = $1 $0
DEST_KEY = _raw

[health_log_analytics_add_syslogHost]
SOURCE_KEY = MetaData:Host
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
REGEX = ^host::(.+)$
FORMAT = $1 $0
DEST_KEY = _raw

[health_log_analytics_add_time]
SOURCE_KEY = _time
REGEX = ^(.+)$
FORMAT = <182>1 $1 $0
DEST_KEY = _raw
```

8. Starten Sie auf der Registerkarte **Finish.conf** Splunk neu, indem Sie den Befehl `$SPLUNK_HOME/bin/splunk restart splunkd` ausführen.
9. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
10. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

    Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

    - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
    - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

      Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

      Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

    Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

11. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streamen von Protokolldaten an Ihren ServiceNow Instanz mit Splunk Absender.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

Automatische Übersetzung

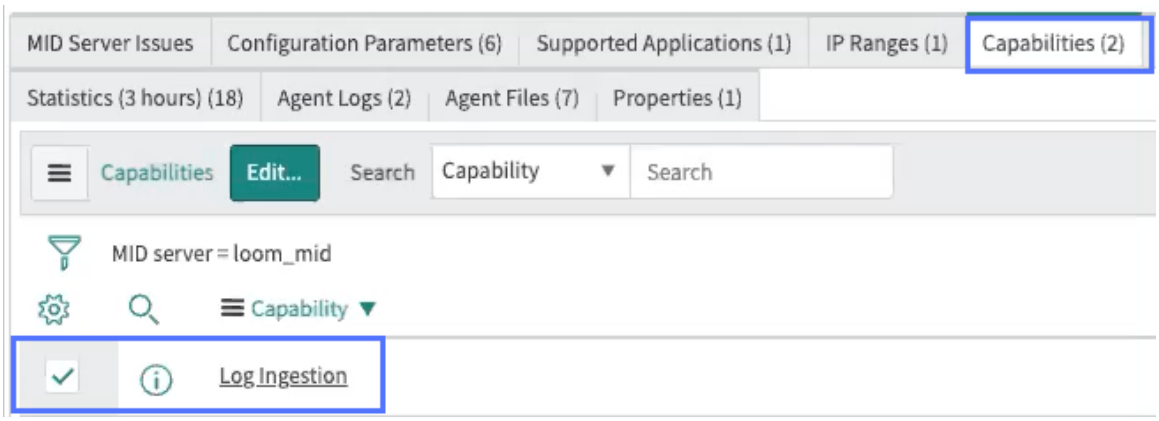
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie ein Splunk Dateneingabe in wird abgefragt Health Log Analytics Manuell

Richten Sie eine Dateneingabe ein, die regelmäßig Protokolldaten aus abruft Splunk Mithilfe einer Abfrage.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie aus Splunk Dateneingabe wird abgefragt.
4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder der Dateneingabe für Abfrage.

5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen. Auf der **Registerkarte „Transport“** Und **Registerkarte „Erweitert“** , Füllen Sie die Felder aus. Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder der Dateneingabe für Abfrage.
6. Wählen Sie **Speichern**. Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** . Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository. Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden.

   Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

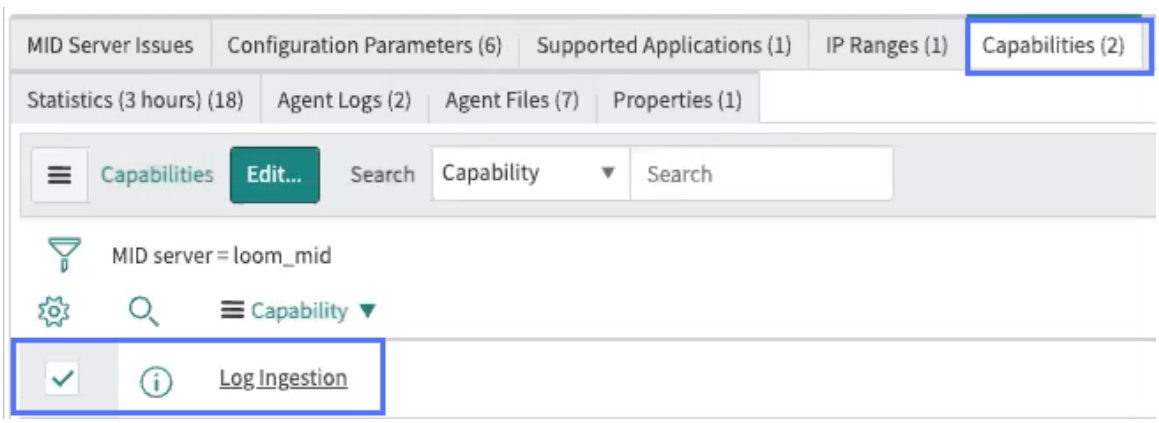
8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Konfigurieren Sie eine TCP-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Senden von Rohprotokollnachrichten an ein ServiceNow Instanz direkt über einen TCP/SSL-Socket.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Hinweis: Informationen zum Streamen von Daten aus Logstash an Ihre Instanz finden Sie unter Streaming von Daten aus Logstash an Ihre HLA-Instanz [KB0994735] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den TCP-Dateneingabetyp.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für TCP-Dateneingabe.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für TCP-Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Senden von Rohprotokollnachrichten an Ihren ServiceNow Instanz direkt über einen TCP/SSL-Socket.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

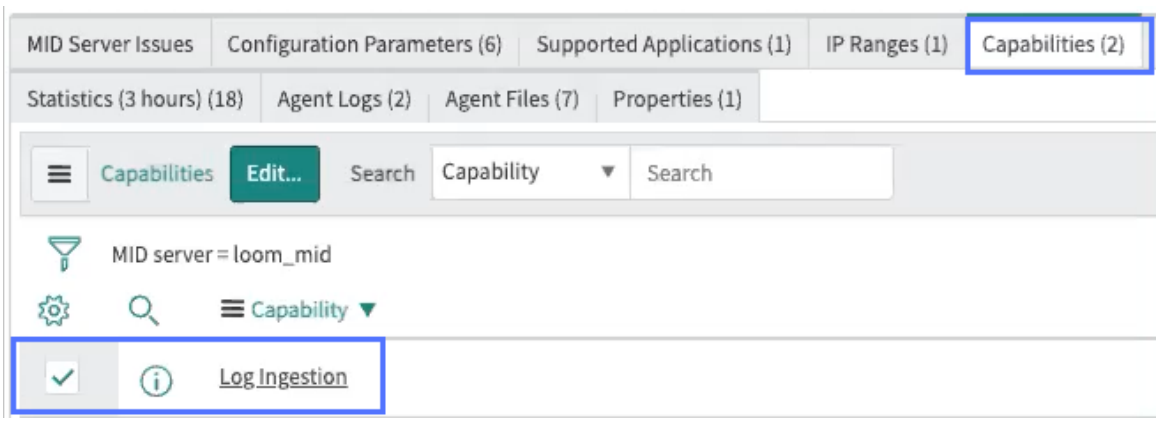
Konfigurieren Sie eine UDP-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Dateneingabe für das Senden von Rohprotokollnachrichten an ein ServiceNow Instanz direkt über einen UDP-Socket.

Vorbereitungen

Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 25.0.17 – November 2022 und höher, verfügbar über ServiceNow Store .

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Informationen zum Versand Ihrer mit SSL TLS verschlüsselten Protokolle finden Sie unter Streaming von Daten mit rsyslog und Filebeat unter Verwendung von SSL [KB0866319] artikel in Now Support Knowledge Base.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den UDP-Dateneingabetyp aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für UDP-Dateneingabe.
5. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für UDP-Dateneingabe.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Überprüfen Sie, ob die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Senden von Rohprotokollnachrichten an Ihren ServiceNow Instanz direkt über einen UDP-Socket.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

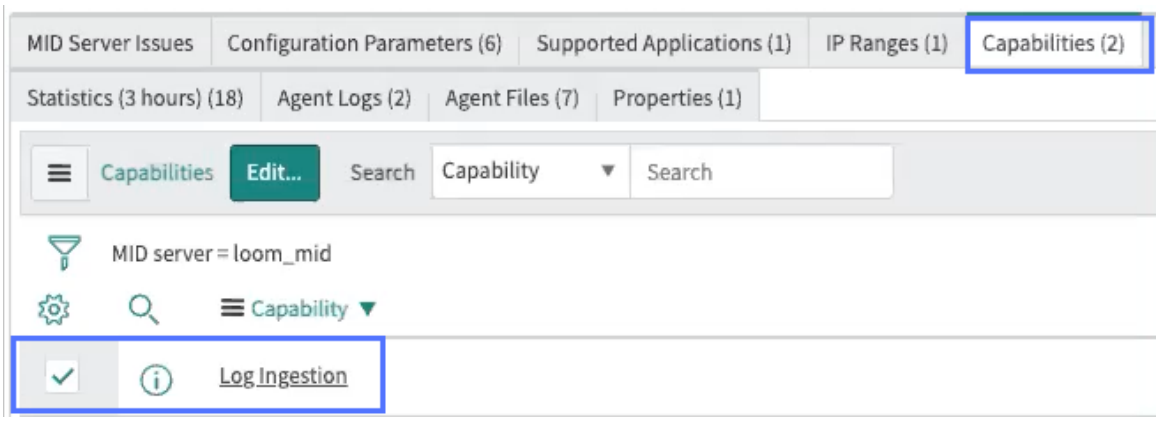
Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie eine Vector Agent-Dateneingabe in Health Log Analytics Manuell

Richten Sie eine Vector Agent-Dateneingabe ein, um zu aktivieren Health Log Analytics Dient zur Verarbeitung von Protokollnachrichten, die in Ihren gestreamt werden ServiceNow Instanz über einen Vector Agent.

Vorbereitungen

- Überprüfen Sie, ob ein MID-Server Wird mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn MID-Server Die IP-Adresse wird durch Netzwerkadressübersetzung (Network Address Translation, NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät bereitgestellt MID-Server Muss eine öffentliche IP-Adresse haben, um von externen Clients erreichbar zu sein, z. B. Filebeat Service Desk-Mitarbeiter, die sich außerhalb des Netzwerks befinden. Private IP-Adressen können nicht über das Internet weitergeleitet werden. Ohne eine öffentliche IP können diese externen Clients keine Verbindung mit herstellen MID-Server Auch wenn sie mit der Adresse konfiguriert sind. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

  Hinweis: Wenn MID-Server Und externe Clients befinden sich im selben Netzwerk, eine öffentliche IP ist nicht erforderlich, und Verbindungen können über die private IP-Adresse hergestellt werden.

- Überprüfen Sie, ob Sie über einen verfügen Vector.yaml Datei auf Ihrem System oder erstellen Sie eine.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Vector by verwendet Datadog Dient zur Verarbeitung von Protokolldaten aus mehreren Quellen, bevor sie an gesendet werden Health Log Analytics, Das Protokollformat HLA„Empfangen“ unterscheidet sich von anderen Typen. Die Dateneingabe Vector Agent aktiviert HLA Um Transport-Header von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen, wird nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weitergeleitet.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie Aus **Vektor: Stream von Protokollen von Vector Agent** .
4. Auf der **Erste Schritte** Füllen Sie das Formular aus, und wählen Sie dann aus **Als Nächstes** .
   Eine detaillierte Beschreibung der Felder finden Sie unter Vector Agent-Dateneingabekonfigurationsfelder.
5. Auf der **Vector.yaml** Registerkarte den Code nach Bedarf mit den relevanten Werten aktualisieren.
   Sie können beispielsweise die Quellen oder Quelldatei angeben, aus der die Protokolle gestreamt werden.

   Hinweis: Dem Code, den Sie nicht ändern sollten, ist eine kommentierte Notiz vorangestellt.

   Weitere Informationen finden Sie unter Die Vektordokumentation .
6. Kopieren Sie den aktualisierten Code, und fügen Sie ihn in ein Vector.yaml Datei auf Ihrem System.
7. Wählen Sie **Weiter**.
   Die **Beenden** Auf der Registerkarte wird eine Nachricht angezeigt, die bestätigt, dass der Dateneingabekonfigurationsprozess abgeschlossen ist.
8. Starten Sie das Streaming von Protokolldaten, indem Sie Vector mit der Konfigurationsdatei ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie den folgenden Befehl aus: `Vektor --config /path/to/your/vector.yaml` , Wo `/Path/to/your/` Ist der tatsächliche Pfad zu Ihrer YAML-Datei.

9. **Wahlweise:** Verwenden Sie die anderen Befehle, die im angezeigt werden **Beenden** Registerkarte nach Bedarf.
10. Wählen Sie Aus **Speichern** Zum Speichern der Dateneingabe.

Ergebnis

Health Log Analytics Fügt den Dateneingabedatensatz zu hinzu **Dateneingaben** Tabelle. Die Dateneingabe beginnt mit dem Streamen von Protokolldaten an Ihren ServiceNow Instanz.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics

Suchen und beheben Sie Protokoll-Streaming-Probleme, um sicherzustellen, dass Ihre Dateneingaben Protokolldaten ordnungsgemäß an Ihre Instanz streamen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Streamingquellen**an.
   Auf der Seite „Streaming-Quellen“ werden alle Dateneingaben und angezeigt MID Servers Die Protokolle von ihnen erhalten.

   Hinweis:

   - Wenn in der Konfiguration der erweiterten Dateneingabe die Option **Look up hostnames** (Nach Hostnamen suchen) ausgewählt ist, wird auf der Seite „Streaming Sources“ (Streaming-Quellen) der Hostname von Geräten angezeigt, die einen Rsyslog- oder Filebeat-Absender verwenden. Für Elasticsearch -Indizes wird der Indexname angezeigt.
   - „Streaming Sources“ (Streaming-Quellen) ist auch als zugehörige Liste im Dateneingabeformular verfügbar. In der zugehörigen Liste werden nur die Endpunktgeräte angezeigt, die für diese Dateneingabe relevant sind.
   - Wenn HLA Engine ist ausgefallen, und das Streaming der Daten wurde beendet. Oben auf der Seite „Streaming-Quellen“ wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

2. Wählen Sie einen Dateneingabedatensatz aus, um die Streaming-Daten seiner Quellen anzuzeigen und Streaming-Probleme und ihre mögliche Ursache zu identifizieren.
   Wenn beispielsweise die letzte aufgezeichnete Event-Zeit für den Endpunktserver einer Dateneingabe gestern war, ist dieser Server möglicherweise ausgefallen oder falsch konfiguriert. Ein Streaming-Problem kann auch dadurch verursacht werden, dass die Dateneingabe-Konfigurationsdatei nicht auf dem Endpunkt installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter	Beschreibung
Status	Status der Quelle. Ein rotes Aufzählungszeichen zeigt an, dass diese Quelle in der letzten Stunde keine Daten gestreamt hat.
Last event time (Zeit des letzten Events)	Die letzte aufgezeichnete Zeit, zu der auf dem MID-Server ein Event im letzten Ein-Minuten-Intervall eingetroffen ist. Health Log Analytics aktualisiert kontinuierlich die Zeit des letzten Events. Wenn die Zeit des letzten Events nicht aktuell ist, werden keine Daten gestreamt.
Raw log lines/sec (Protokollzeilen im Rohzutand/Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Protokollzeilen im Rohzutand vor der Vorverarbeitung dar.
Preprocessed log lines/sec (Vorverarbeitete Protokollzeilen/Sek.)	Die durchschnittliche Anzahl der vorbearbeiteten Protokollzeilen, die im letzten Ein-Minuten-Intervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass Protokolle während der Vorverarbeitung gelöscht wurden.

3. Untersuchen und lösen Sie alle Probleme beim Datenstreaming.

Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

Nächste Maßnahme

Wenn die Protokolle ordnungsgemäß gestreamt werden, fahren Sie mit der Zuordnung Ihrer Protokolldaten im Rohzustand fort.

Hinweis: Sie können eingehende Protokolldaten im Rohzustand bearbeiten, bevor Health Log Analytics sie verarbeitet. Mit der Vorverarbeitung können Sie beispielsweise Protokollteile verwerfen oder vertrauliche Daten aus Ihren Protokollen entfernen. Diese Aufgabe ist optional.

Setup-Aufgaben für zusätzliche Dateneingabe in Health Log Analytics

Nachdem das Setup und die Konfiguration der ersten Dateneingabe in durchgeführt wurden Health Log Analytics, Fahren Sie mit den verbleibenden Setup-Aufgaben für die Dateneingabe fort.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie in ein Zeitstempelformat hinzu Health Log Analytics

Definieren Sie ein Zeitstempelformat, das nicht in der Liste der definierten Formate angezeigt wird. Health Log Analytics muss Zeitstempel jedes Formats lesen können, das in Ihren Protokolldateien enthalten ist.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Zeitstempelformate**an.
2. Um zu bestimmen, ob Ihr Zeitstempelformat mit einem vordefinierten Format im System übereinstimmt, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Find format** (Format suchen).
   b. Geben Sie ein Beispiel für Ihren Zeitstempel ein.
   c. Klicken Sie auf **Find format** (Format suchen).
   Wenn das Beispiel einem vorhandenen Format entspricht, gibt das System seine ID an.
3. Wenn das Zeitstempelbeispiel nicht mit einem vorhandenen Format übereinstimmt, definieren Sie Ihr benutzerdefiniertes Format manuell, und fügen Sie es den verfügbaren Zeitstempelformaten hinzu.
   a. Wählen Sie auf der Seite „Timestamp Formats“ (Zeitstempelformate) die Option **New** (Neu) aus.
   b. Füllen Sie die Felder des Formulars aus.

Formular „Zeitstempelformat“

Feld	Beschreibung
ID	ID des Zeitstempelformats. Dieser Wert ist automatisch ausgewählt.
Format	Gültiges Zeitstempelformat. Beispiel: tt-MMM-jjjj, HH:mm. **Hinweis:** Für die Zeitstempelsyntax verwendet Health Log Analytics die Java 8-API .
Beispiel	Beispiel für das Zeitstempelformat. Beispiel: 03. Mai 2018, 10:20
Beschreibung	Beschreibung des Zeitstempelformats.

4. Wählen Sie **Absenden** aus.

Ergebnis

Das System validiert das Zeitstempelformat und fügt es der Liste der verfügbaren Zeitstempel hinzu.

Fügen Sie einen Quelltyp manuell in hinzu Health Log Analytics

Erstellen Sie einen Quelltyp manuell, bevor Sie eine Dateneingabe konfigurieren, wenn Sie Protokolldaten nicht an den Quelltyp streamen möchten, der während des Zuordnungsprozesses von Health Log Analytics automatisch extrahiert wird, sondern an einen bestimmten Quelltyp.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Quelltypen**an.
2. Wählen Sie auf der Registerkarte „Quelltypen“ **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Quelltyp“

Feld	Beschreibung
Name	Name des Quelltyps. Der Name muss zwischen 3 und 50 Zeichen lang sein. Zulässige Zeichen sind Buchstaben, numerische Werte, Bindestriche und Unterstriche.
Beispiele	Mindestens ein Beispiel für Roheingaben für diesen Quelltyp. Geben Sie jedes Beispiel in eine neue Zeile ein. **Hinweis:** Dieses Feld muss Daten enthalten.

Die Felder in der folgenden Tabelle sind schreibgeschützt.

Feld	Beschreibung
Manuell erstellt	Option zum Angeben, dass dieser Quelltyp manuell erstellt wurde. Standardwert: true
Auto-extraction enabled (Automatische Extraktion aktiviert)	Standardmäßig ist die automatische Extraktion für diesen Quelltyp deaktiviert.
Lernmodus	Option zur Angabe, dass der Lernmodus für den Quelltyp ausgeführt wird. Die KI-Engine muss das Format der Protokollnachrichten in jedem neuen Protokollstream erlernen. Im Lernmodus erlernt sie das Format von Nachrichten für diesen Quelltyp und extrahiert Eigenschaften basierend auf diesen Informationen.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie **Load examples** (Beispiele laden), um die Roheingabebeispiele für diesen Quelltyp zu laden, die Sie im Feld **Beispiele** angegeben haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Laden der Protokollbeispiele erfolgreich abgeschlossen wurde, werden das Feld **Beispiele** und die Schaltflächen **Load examples** (Beispiele laden) nicht mehr im Formular angezeigt.

6. **Wahlweise:** Überprüfen Sie, wie die KI-Engine die Roheingabebeispiele analysiert hat, indem Sie auf den zugehörigen Link **Go to Source Type Structure** (Gehe zu Quelltypstruktur) klicken, und ändern Sie die extrahierten Eigenschaften gegebenenfalls.
7. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Konfigurieren Sie eine Dateneingabe, und ordnen Sie sie dann dem neuen Quelltyp zu. Weitere Informationen finden Sie unter Richten Sie Dateneingaben in ein Health Log Analytics Manuell und Ordnen Sie Rohprotokolldaten in zu Health Log Analytics.

Zugehörige Informationen

Verfeinern Sie die Quelltypstruktur in Health Log Analytics

Konfigurieren Sie Quelltypfähigkeiten in Health Log Analytics

Health Log Analytics extrahiert Quelltypen im Zuordnungsprozess automatisch. Sie können Zeitstempelformate hinzufügen und Stichwörter für einzelne Quelltypen angeben, löschen oder ausschließen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Quelltypen**an.
   Die Tabelle „Quelltypen“ enthält alle Quelltypen, die während der Zuordnung von Rohdaten automatisch extrahiert wurden.

Quelltypen

Feld	Beschreibung
Automatische Extraktion aktiviert	Die automatische Extraktion für diesen Quelltyp ist entweder aktiviert oder deaktiviert. Dieser Wert wird im Formular „Source Type Structure“ (Quelltypstruktur) festgelegt. Standardwert: true
Lernmodus	Der Lernmodus für den Quelltyp ist entweder fortlaufend oder abgeschlossen. Die KI-Engine muss das Format der Protokollnachrichten in jedem neuen Protokollstream erlernen. Im Lernmodus erlernt sie das Format von Nachrichten für diesen Quelltyp und extrahiert Eigenschaften basierend auf diesen Informationen.
Stack trace detection enabled (Stack Trace-Erkennung aktiviert)	Die Erkennung der aktiven Stack Frames für diesen Quelltyp ist entweder aktiviert oder deaktiviert. Normalerweise ermöglicht ein Stack Trace die Nachverfolgung eines Fehlers in dem Protokoll, aus dem er stammt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Öffnen Sie einen Datensatz.
3. **Wahlweise:** Fügen Sie ein Zeitstempelformat für diesen Quelltyp hinzu.
   a. Wählen Sie auf der Registerkarte **Source Type Timestamps** (Quelltyp-Zeitstempel) die Option **New** (Neu) aus.
   b. Wählen Sie im Feld **Timestamp format** (Zeitstempelformat) ein Format aus der Liste der verfügbaren Zeitstempelformate aus.
   c. Wählen Sie **Absenden** aus.
4. **Wahlweise:** Geben Sie ein Stichwort für diesen Quelltyp an.
   a. Wählen Sie auf der Registerkarte **Lexical Keywords** (Lexikalische Stichwörter) **New** (Neu) aus.

      Hinweis: Die Registerkarte **Lexical Keywords** (Lexikalische Stichwörter) enthält sowohl globale als auch angegebene Stichwörter. Durch die Auswahl von **New** (Neu) wird ein angegebenes Stichwort für diesen Quelltyp erstellt.

   b. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für das Stichwort
Regulärer Ausdruck	Der reguläre Ausdruck („Regex“), mit dem Übereinstimmungen definiert werden
Exact match (Genaue Übereinstimmung)	Boolescher Wert. Wenn er auf True gesetzt ist, erwartet Health Log Analytics eine exakte Übereinstimmumg mit dem regulären Ausdruck. Beispiel: „NullPointerException“ würde in einer Nachricht nicht mit dem regulären Ausdruck „exception“ übereinstimmen. Standardwert: True
Groß-/Kleinschreibung beachten	Boolescher Wert. Wenn diese Option ausgewählt ist, sucht Health Log Analytics nach einer Übereinstimmung des regulären Ausdrucks, bei der die Groß-/Kleinschreibung übereinstimmt. Standardwert: False

   c. Wählen Sie **Absenden** aus.
5. **Wahlweise:** Löschen Sie ein Stichwort, das für diesen Quelltyp festgelegt ist.
   a. Markieren Sie die Zeile des angegebenen Stichworts, das Sie löschen möchten.
   b. Wählen Sie in der Liste **Actions on selected rows** (Aktionen für ausgewählte Zeilen) unten auf der Seite die Option **Exclude keyword** (Stichwort ausschließen) aus.
   c. Klicken Sie auf **Continue** (Fortsetzen), um das Stichwort zu löschen.
6. **Wahlweise:** Schließen Sie ein globales Stichwort für diesen Quelltyp aus.
   Wenn Sie ein Stichwort ausschließen, sucht Health Log Analytics in den Protokolldaten dieses Quelltyps nicht mehr danach.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Markieren Sie die Zeile des globalen Stichworts, das Sie ausschließen möchten.

b. Wählen Sie in der Liste **Actions on selected rows** (Aktionen für ausgewählte Zeilen) unten auf der Seite die Option **Exclude keyword** (Stichwort ausschließen) aus.

Hinweis: Sie können globale Stichwörter auf der Seite Lexical Keywords (Lexikalische Stichwörter) löschen.

7. Wählen Sie **Aktualisieren**.

Verifizieren Sie Ihre Protokollquellen in Health Log Analytics

Überprüfen Sie, ob alle Ihre Protokollquellen vorhanden und aktiv sind nach Health Log Analytics Das Tagging hat einer Serviceinstanz und Komponenten ein Protokoll zugewiesen und das Protokoll automatisch einer Quelle zugeordnet.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**an.
Die Tabelle „Log Sources“ (Protokollquellen) enthält Informationen zu den Quellen, die beim Zuordnen der Streaming-Daten erstellt wurden. In der Tabelle werden diese Quellen nach Serviceinstanz aufgelistet.

Spalte	Beschreibung
Serviceinstanz	Die Serviceinstanz. Serviceinstanzen stellen große oder vollständige Geschäftsprozesse dar. Eine einzelne Serviceinstanz kann aus mehreren Komponenten bestehen, während verschiedene Serviceinstanzen dieselben Komponenten enthalten können.
Komponente	Die Komponenten, aus denen die Serviceinstanz besteht. Komponenten stellen kleine technische Teile oder Geschäftsprozesse dar. In der Regel stellen sie Konfigurationselemente (CIs) dar. Mehrere Komponenten werden häufig in einer einzigen Serviceinstanz gruppiert.
Status	Status der Protokollquelle: „Active“ oder „Inactive“ (Aktiv oder Inaktiv). Der Status „Active“ gibt an, dass während der letzten Stunde Protokolle aus dieser Quelle in das System gestreamt wurden.
Erstellt	Datum und Uhrzeit der Erstellung dieser Protokollquelle
Last event time (Zeit des letzten Events)	Zeitpunkt, an dem zum letzten Mal Protokolle aus dieser Quelle in das System gestreamt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Stellen Sie sicher, dass im System alle Ihre Protokollquellen erstellt wurden.
3. Überprüfen Sie Erstellung, Status und Protokollbeispiele einer bestimmten Quelle im Quelldatensatz.

   Hinweis: Da bei der automatischen Zuordnung Protokolldaten mehreren Quellen zugeordnet werden können, müssen Sie diese Informationen für jede einzelne Quelle überprüfen.

4. Wenn eine Protokollquelle fehlt, fügen Sie sie hinzu.

   a. Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Dateneingabezuordnung**an.

   b. Verwenden Sie die JavaScript-Funktion, um ein Protokollbeispiel manuell der richtigen Serviceinstanz, Komponente und Quelltyp zuzuordnen.
   Weitere Informationen finden Sie unter Ordnen Sie Rohprotokolldaten in zu Health Log Analytics.

   c. Navigieren Sie zurück zur Seite „Log Sources“ (Protokollquellen), und stellen Sie sicher, dass der Status der neuen Protokollquelle „Active“ lautet.

   Das System erstellt eine Protokollquelle.

5. Stellen Sie sicher, dass der Status aller Protokollquellen „Active“ ist.
   Wenn der Status einer Quelle „Inactive“ ist, doppelklicken Sie darauf, und ändern Sie sie manuell in „Active“.
6. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Löscht eine Protokollquelle in Health Log Analytics

Extraktion nicht benötigter Protokolldaten in stoppen Health Log Analytics

Extrahieren Sie bestimmte Protokolldaten in Health Log Analytics

Löscht eine Protokollquelle in Health Log Analytics

Löscht eine Protokollquelle mit oder ohne die zugehörigen Protokolldaten in Health Log Analytics.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Protokollquelle löschen, Health Log Analytics Löscht automatisch die zugehörigen Protokolldaten. Sie können auch eine Quelle löschen, während Sie die Protokolldaten beibehalten. Die zugehörigen Daten werden dann gemäß der Protokollaufbewahrungsrichtlinie gelöscht. Weitere Informationen finden Sie unter Speicherplatz für die Protokollaufbewahrung in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Protokollquellen**an.
2. Öffnen Sie einen Quelldatensatz.
3. Löschen Sie die Protokollquelle auf eine der folgenden Arten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Löschen Sie die Quelle und die zugehörigen Daten, indem Sie auswählen **Löschen** .
- Löschen Sie die Quelle ohne die zugehörigen Daten, indem Sie auswählen **Ohne Protokolle löschen** Zugehöriger Link.

Überprüfen Sie Eigenschaften, die aus einem Quelltyp in extrahiert wurden Health Log Analytics

Überprüfen Sie die Eigenschaften, die aus allen Quelltypen in einer Quelltypstruktur extrahiert wurden, in einer einzigen Tabelle, um Setup-Probleme zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

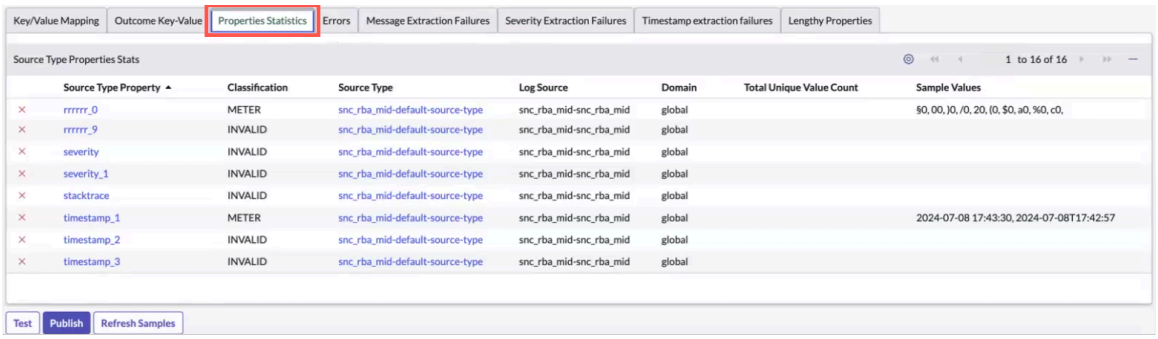
Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „Statistiken zu Quelltypeigenschaften“ bietet einen umfassenden Überblick über die Eigenschaften, die aus den Quelltypen extrahiert wurden. Indem Sie die statistische Verteilung ihrer Werte überprüfen, können Sie die Klassifizierung dieser Eigenschaften bewerten und bei Bedarf Ihre Einstellungen anpassen.

Das Verfahren in diesem Abschnitt erklärt, wie Sie über die Quelltypstruktur auf die Tabelle „Quelltypeigenschaften“ zugreifen. In einem Quelltyp-Datensatz können Sie zur Quelltypstruktur navigieren, indem Sie auswählen **Wechseln Sie zu Quelltypstruktur** Zugehöriger Link.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Quelltypstrukturen**an.
2. Öffnen Sie einen Quelltypstrukturdatensatz.
3. Öffnen Sie **Eigenschaftsstatistiken** Registerkarte „zugehörige Links“.



Die **Statistiken Zu Quelltypeigenschaften** Die Tabelle zeigt die Eigenschaften aller Quelltypen, die Teil dieser Quelltypstruktur sind.

Statistiken zu Quelltypeigenschaften

Spalte	Beschreibung
Quelltypeigenschaft	Die aus dem Quelltyp extrahierte Eigenschaft.
Klassifizierung	Die Klassifizierung der Eigenschaft. Die verfügbaren Typen sind: METER, ANZEIGE, ARC und UNGÜLTIG.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Hinweis: Eine Eigenschaft, die als UNGÜLTIG klassifiziert ist (Standardklassifizierung), wird nicht für die Anomalieerkennung nachverfolgt oder in der Analyse aussagekräftiger Eigenschaften angezeigt.
Quelltyp	Der Quelltyp, aus dem die Eigenschaft extrahiert wurde.
Protokollquelle	Die Liste der Protokollquellen, in denen diese Eigenschaft angezeigt wurde.
Domäne	Die Domäne, zu der die Protokollquelle gehört.
Gesamtanzahl eindeutiger Werte	Nur für Eigenschaften, die als „ZÄHLER“ klassifiziert sind: Die Gesamtzahl der darin enthaltenen eindeutigen Werte. Dieses Feld ist inaktiv, wenn die Eigenschaft als ARC oder ANZEIGE klassifiziert ist. **Hinweis:** Die Gesamtanzahl eindeutiger Werte wird einmal täglich aktualisiert. Datensätze, die älter als 24 Stunden sind, werden automatisch gelöscht.
Beispielwerte	Nur für Eigenschaften, die als ZÄHLER klassifiziert sind: Beispiel für eindeutige Werte, die vom System nachverfolgt werden. Der Standardwert ist 30 Beispiele. Dieses Feld ist inaktiv, wenn die Eigenschaft als ARC oder ANZEIGE klassifiziert ist.

4. Überprüfen Sie die Eigenschaften, und identifizieren Sie mögliche Klassifizierungsprobleme.
5. **Wahlweise:** Zeigen Sie Statistiken für einzelne Quelltypeigenschaften an, die als ARC_ONLY oder GAUGE klassifiziert sind.
   a. Öffnen Sie eine Quelltypeigenschaft, die als ARC_ONLY oder GAUGE klassifiziert ist, aus dem **Eigenschaftsstatistiken** Registerkarte „zugehörige Links“.
   b. Auf der **Quelltypeigenschaft** Formular auswählen **Statistiken Zu Quelltypeigenschaften** .
   Die folgenden Informationen werden in einem Popup-Fenster angezeigt:
   - Für eine ARC-Eigenschaft: Die prozentuale Verteilung von Begriffen basierend auf den verarbeiteten Protokollen. Beispiel: Der Prozentsatz der ungültigen Anforderung vs. Erfolg.
   - Für eine ANZEIGEEIGENSCHAFT: Die durchschnittliche, minimale und Standardabweichung vom erwarteten numerischen Wert.
6. **Wahlweise:** Ändern Sie die Klassifizierungseinstellungen in **Schlüssel-/Wert-Zuordnung** Registerkarte.
   Weitere Informationen finden Sie unter Verfeinern Sie die Quelltypstruktur in Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie Muster, die aus einem Quelltyp in extrahiert wurden Health Log Analytics

Überprüfen Sie alle erlernten Muster, die aus einem Quelltyp in einer Quelltypstruktur extrahiert wurden, zusammen mit den Protokollquellen, in denen diese Muster aufgetreten sind. Die Überprüfung dieser Muster kann wertvolle Einblicke in die Protokollnachrichtenmuster bieten, die Health Log Analytics Verfolgt für jeden Quelltyp und jede Protokollquelle nach.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Quelltypstrukturen**an.
2. Wählen Sie im einen Quelltyp aus **Quelltypname** Spalte.
3. Wählen Sie im Formular Quelltyp die aus **Zusammengefasste Protokollmuster** Zugehörige Liste. Auf der Registerkarte werden die folgenden Daten für jedes Muster angezeigt, das aus diesem Quelltyp extrahiert wurde. Die angezeigten Daten werden stündlich aktualisiert.

Zusammengefasste Protokollmuster

Spalte	Beschreibung
Mustertext	Der Inhalt des aggregierten Musters.
Quellen	Die Quellen, in denen das Muster aufgetreten ist.
Domäne	Die Domäne, zu der das Muster gehört.

Ändern Sie eine Dateneingabekonfiguration in Health Log Analytics

Ändern Sie die Konfiguration einer Dateneingabe für Health Log Analytics Durch Hinzufügen eines neuen Pfads zu einer vorhandenen Dateneingabekonfiguration oder Ändern der Dateneingaben MID-Server Ziel und Port.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie einen Datensatz aus der Tabelle der Dateneingaben.
3. Bearbeiten Sie die Konfiguration der Dateneingabe.

Spalte	Beschreibung
Name	Name der Dateneingabe
Beschreibung	Beschreibung der Dateneingabe
Port	Port auf dem MID-Server. **Hinweis:** Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
MID	Der MID-Server, an den die Protokolle gestreamt werden **Hinweis:** ○ Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. ○ Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.

Einstellungen

Spalte	Beschreibung
Pfad	Der vollständige Pfad, aus dem Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. **Hinweis:** Diese Spalte ist in Windows-Systemen, in denen Winlogbeat verwendet wird, nicht verfügbar.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.
Komponente	Gerätetyp oder Stapelebene als Kontext für die Protokolle, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat. Komponenten stellen normalerweise CIs in der CMDB dar. Mehrere Komponenten werden häufig in einer einzigen Serviceinstanz gruppiert.
Quelltyp	Quelltyp, der definiert, wie Health Log Analytics eine bestimmte Anwendung behandelt und die Protokolldaten analysiert. Beispiel: Tomcat Catalina. Jede Dateneingabe kann je nach Vielfalt ihrer Protokollformate mehrere Quelltypen haben. Serviceinstanzen und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	-Komponenten können eine beliebige Anzahl von Quelltypen haben.
Nur zur Verarbeitung mehrzeiliger Nachrichten in Linux-/Windows-Systemen mit Filebeat:	
Match (Übereinstimmung)	Gibt an, wie Filebeat übereinstimmende Zeilen zu einem Event kombiniert, entweder **nach** oder **vor**.
Negieren	Boolescher Wert, der definiert, ob das in den Protokollzeilen identifizierte Muster negiert wird. Der Standardwert ist **false**.
Regulärer Ausdruck	Der entsprechende reguläre Ausdruck

Hinweis: Sie können die Rsyslog-Konfigurationsdatei ändern, damit der Agent zusätzlich zu den Anwendungsprotokollen Systemprotokolle versendet. Weitere Informationen finden Sie im Artikel Shipping system logs using Rsyslog (Übermittlung von Systemprotokollen mit Rsyslog) [KB0954507] in der Knowledge Base des Now Support.

4. Wählen Sie **Aktualisieren**.
5. Erstellen Sie für Dateneingaben, die nur Rsyslog- oder Beats-Agents verwenden, die serverseitige Konfigurationsdatei neu, und installieren Sie sie auf dem Endpunktgerät.
   a. Wählen Sie **Rebuild configuration file** (Konfigurationsdatei neu erstellen) aus.

      Health Log Analytics erstellt die Datei neu und speichert sie im Abschnitt „Manage Attachments“ (Anhänge verwalten). Abhängig vom verwendeten Agent wird die neu erstellte Datei als rsyslog.yml, filebeat.yml oder winlogbeat.yml gespeichert.

      Das System benennt die vorherige Konfigurationsdatei automatisch um, indem ein Suffix mit Datum und Uhrzeit an den Dateinamen angehängt wird. Damit wird angegeben, wann die Datei neu erstellt wurde.

   b. Installieren Sie die neu erstellte Konfigurationsdatei auf dem Endpunkt entsprechend Ihrem Dateneingabetyp.

Dateneingabetyp	Aktion
Rsyslog	i. Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis /etc/rsyslog.d/rsyslog.conf. ii. Validieren Sie die Konfiguration, indem Sie den Befehl `rsyslogd -N1` ausführen. iii. Überprüfen Sie die Ausgabe. Wenn die Systemprotokolldatei /var/log/messages Fehler enthält, prüfen und beheben Sie die Fehlermeldungen. iv. Starten Sie Rsyslog neu, indem Sie den Befehl `sudo systemctl restart rsyslog` ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateneingabetyp	Aktion
Linux	i. Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis /etc/filebeat/. ii. Starten Sie den Agent-Service neu, indem Sie den Befehl sudo service filebeat restart ausführen. **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfigurationsdatei ändern.
Windows mit Beats (Filebeat oder Winlogbeat):	i. Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis C:\Programme\. ii. Starten Sie den Agent-Service neu, indem Sie den entsprechenden PowerShell-Befehl ausführen: ▪ Filebeat: PS > Restart-Service filebeat ▪ Winlogbeat: PS > Restart-Service winlogbeat **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfigurationsdatei ändern.

Zugehörige Informationen

Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Beats Dateneingaben in Health Log Analytics Manuell

Erweiterte Dateneingabekonfiguration in Health Log Analytics

Wenn Sie eine Dateneingabe erfolgreich konfiguriert haben, fügt Health Log Analytics der entsprechenden Tabelle einen Datensatz hinzu und hängt die Konfigurationsdatei an. Für Ihre Dateneingabe können Sie erweiterte Einstellungen konfigurieren. Die Konfiguration von erweiterten Einstellungen ist optional.

Konfigurieren Sie erweiterte Einstellungen für Rsyslog, Splunk, Oder TCP-Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die Rsyslog-, Splunk- oder TCP-Agents verwenden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zum Ändern der Einstellungen, die beim Erstellen der Dateneingabe konfiguriert wurden, wie das Hinzufügen eines neuen Pfads oder das Ändern des MID-Server-Ziels oder Ports der Dateneingabe, finden Sie unter Ändern Sie eine Dateneingabekonfiguration in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie einen Rsyslog-, Splunk- oder TCP-Dateneingabe-Datensatz aus der Dateneingabentabelle.

   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Rsyslog Dateneingabekonfigurationsfelder , Filebeat oder Winlogbeat.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Konfigurieren Sie erweiterte Einstellungen für Beats Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die Beats-Agents verwenden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die beim MID-Server eintreffenden Protokolldaten ausführt. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zum Ändern der Einstellungen, die beim Erstellen der Dateneingabe konfiguriert wurden, wie das Hinzufügen eines neuen Pfads oder das Ändern des MID-Server-Ziels oder Ports der Dateneingabe, finden Sie unter Ändern Sie eine Dateneingabekonfiguration in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Beats-Dateneingabe aus der Dateneingabentabelle.
   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Rsyslog Dateneingabekonfigurationsfelder , Filebeat oder Winlogbeat.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen**.

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.
8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie ein Rsyslog, Filebeat, Oder Winlogbeat Dateneingabe in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Elasticsearch Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten von Elasticsearch-Indizes an Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zu Streaming-Protokollen mit der Elasticsearch-Dateneingabe finden Sie im Artikel Stream logs using Elasticsearch data input – Advanced Guide [KB1080162] (Protokolle mit Elasticsearch-Dateneingabe streamen - Erweiterte Anleitung) in der Now Support-Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Elasticsearch-Dateneingabe aus der Dateneingabentabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Dateneingabe-Konfiguration wird angezeigt.

Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.

   Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie einen Elasticsearch Dateneingabe in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für MID-Server Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die zum Sammeln und Streamen von MID-Server-Protokollnachrichten verwendet werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer MID-Server-Dateneingabe aus der Dateneingabentabelle.
   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter MID-Server Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Aktualisieren**.

Ergebnis

Health Log Analytics aktualisiert die Systemparameter.

Zugehörige Informationen

Konfigurieren Sie ein MID-Server Dateneingabe in Health Log Analytics Manuell

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie erweiterte Einstellungen für Amazon CloudWatch Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Amazon CloudWatch an Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Amazon CloudWatch-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Dateneingabekonfigurationsfelder.

   Das Feld **Zeichencodierung** ist schreibgeschützt. Standardmäßig lautet die für diese Dateneingabe verwendete Zeichenkodierung UTF-8.

5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie einen Amazon CloudWatch Dateneingabe in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Amazon S3 Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten von Amazon S3-Buckets an Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Amazon S3-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Amazon S3 Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

- Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie einen Amazon S3 Dateneingabe in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Log Analytics Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Microsoft Azure Log Analytics an Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Microsoft Azure Log Analytics-Dateneingabe aus der Dateneingabentabelle.

Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie ein Microsoft Azure Log Analytics Dateneingabe in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Microsoft Azure Event Hubs Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Microsoft Azure Event Hubs an Ihre Instanz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Microsoft Azure Event Hubs-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie ein Microsoft Azure Event Hubs Dateneingabe in Health Log Analytics Manuell

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie erweiterte Einstellungen für Apache Kafka Dateneingaben in Health Log Analytics Manuell

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Apache Kafka an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Apache Kafka-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Konfigurationsseite der Dateneingabe wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie im Formular die Felder aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Dateneingabekonfigurationsfelder.
5. **Wahlweise:** Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

   Wenn die Dateneingabe so konfiguriert ist, dass sie auf einem ausgeführt wird MID-Server Cluster, versucht das System, alle zu verbinden MID Servers Enthalten im Cluster für das Repository. Der Cluster besteht den Test, wenn mindestens einer davon besteht MID Servers Wird verbunden. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

   - Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

8. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Zugehörige Informationen

Konfigurieren Sie einen Apache Kafka Dateneingabe in Health Log Analytics Manuell

Beenden Sie eine Dateneingabe in oder starten Sie sie neu Health Log Analytics

Sie können die Verwendung einer Dateneingabe zum Streamen von Protokollnachrichten an Ihren beenden ServiceNow Instanz. Starten Sie die Dateneingabe neu, wenn das Streamen von Daten fortgesetzt werden soll.

Vorbereitungen

Diese Funktionalität ist nur verfügbar, wenn die Dateneingabekonfiguration veröffentlicht wurde.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Protokollieren Sie Dateneingaben**an.
2. Öffnen Sie den Datensatz einer Dateneingabe aus der Dateneingabentabelle.
3. Klicken Sie auf **Stop Data Input** (Dateneingabe anhalten).
   Der Name der Schaltfläche ändert sich in **Start Data Input** (Dateneingabe starten).
4. Um die Dateneingabe erneut zu verwenden, klicken Sie auf **Start Data Input** (Dateneingabe starten).

Bearbeiten Sie Rohprotokolldaten vor der Verarbeitung in Health Log Analytics

Sie können Rohprotokolldaten ändern und Protokollnachrichten verwerfen oder aufteilen, bevor sie in behandelt werden MID-Server, Und daher vor Health Log Analytics Ordnet sie zu und strukturiert sie. Sie können beispielsweise verhindern, dass vertrauliche Daten erreichen Health Log Analytics Durch Ersetzen von Anwendernamen und Passwörtern durch ein Sternchen (*).

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingabe-Präprozessor**an.
2. Öffnen Sie einen Datensatz.

Hinweis: Wenn das Vorverarbeitungsformular zum ersten Mal angezeigt wird, ruft Health Log Analytics automatisch Protokollbeispiele ab. Rufen Sie in nachfolgenden Sitzungen neue Beispiele manuell ab, indem Sie auswählen **Aktualisieren Sie Beispiele** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Verhindern Sie, dass Protokollbeispiele angezeigt werden, die aus den Protokolldaten im Rohzustand Ihrer Organisation stammen, indem Sie **Disable raw log samples** (Rohprotokollbeispiele deaktivieren) auswählen.
   Wählen Sie diese Option aus, wenn Sie Ihre Protokolle nicht für Health Log Analytics verfügbar machen möchten.
4. **Wahlweise:** Schauen Sie sich an, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
5. Wählen Sie im Feld **Unformatierte Eingabebeispiele** ein Protokollbeispiel aus, das die Auswirkungen Ihrer neuen JavaScript-Funktion auf Protokollzeilen veranschaulicht, wenn Sie sie testen.
6. Definieren Sie eine JavaScript-Funktion, die Ihre Protokolldaten im Rohzustand ändert, bevor Health Log Analytics sie zuordnet und strukturiert.

   Hinweis:

   (Nur ACC-Dateneingaben) wenn Agent Client Collector Wechselt zu einem anderen MID-Server Um Failover-Schutz bereitzustellen, muss er zu einer anderen ACC-Dateneingabe wechseln. Daher müssen alle ACC-Dateneingaben dieselbe JavaScript-Funktion aufweisen. Von Health Log Analytics wird die neueste veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt. Das vorherige Skript wird dabei ersetzt. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Informationen zum Failover-Schutz in Agent Client Collector Log Analytics (ACC-L) finden Sie unter Agent Client Collector Log Analytics.

   a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

      Hinweis: Zusätzlich zur JavaScript-Standardfunktion für die Datenvorverarbeitung bietet Health Log Analytics eine JavaScript-Funktionsvorlage mit dem Namen `Scrubbing`. Diese JavaScript-Funktion entfernt personenbezogene Daten wie E-Mail-Adressen, Sozialversicherungsnummern und Passwörter aus den Rohprotokolldaten. Die Vorlage kann als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

      Hinweis: (Nur ACC-Dateneingaben) Stellen Sie sicher, dass Ihre JavaScript-Funktion zur Verarbeitung von Daten verwendet werden kann, die von allen ACC-Dateneingaben gestreamt werden.

      Die JavaScript-Funktionen zur Vorverarbeitung von Rohprotokolldaten verwenden die folgenden Objekte:

      - Signatur: Funktionsprozess (Beispiel, Metadaten)

Objekt	Beschreibung
Beispiel	Das aktuelle Protokollbeispiel
Metadaten	Objekt, das den Event-Stream enthält. Um auf den Event-Stream zuzugreifen, rufen Sie die Funktion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekt	Beschreibung
	`metadata.eventStream` auf. Da der Event-Stream ein Objekt ist, können Sie auf jede seiner Eigenschaften zugreifen, indem Sie die Funktionen `metadata.eventStream.origin` oder `metadata.eventStream.LocalPort` aufrufen. Die Liste der verfügbaren Event-Stream-Eigenschaften ist auf der Registerkarte **Event Stream: access via metadata** (Event-Stream: Zugriff über Metadaten) verfügbar.

- Typ und Struktur der Rückgabe

  Hinweis: Die JavaScript-Funktion gibt eine Zuordnung mit zwei Einträgen zurück. Ändern Sie diese Rückgabestruktur nicht.

Objekt	Beschreibung
modifiedInput	Die aktuelle Protokollnachricht, nachdem die JavaScript-Funktion die ursprüngliche Nachricht geändert hat. Falls dies Null ist, wird die ursprüngliche Protokollnachricht verwendet.
splitEvents	Array der Protokollnachrichten, nachdem die JavaScript-Funktion die ursprüngliche Nachricht aufgebrochen hat.

- Um eine Protokollnachricht zu verwerfen, rufen Sie `return drop ()` auf.

b. Testen Sie die JavaScript-Funktion, indem Sie **Test** wählen und das Ergebnis in Ihrem Protokollbeispiel in zugehörigen Listen anzeigen.

Registerkarte	Beschreibung
Ergebnis	Ergebnis der Ausführung der JavaScript-Funktion für Ihr Protokollbeispiel
Event-Stream: Zugriff über Metadaten	Schlüssel-Wert-Paare, die die Event Stream-Metadaten darstellen
Failures (Fehler)	Protokollbeispiele, in denen die JavaScript-Funktion nicht erfolgreich ausgeführt werden konnte

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

c. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Save template** (Vorlage speichern), um die JavaScript-Funktion zu speichern. Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.
   - Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
   - Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.
8. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnis

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie, um Ihre Protokolldaten im Rohzustand vorzuverarbeiten, bevor sie zugeordnet und strukturiert werden.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

(Nur ACC-Dateneingaben) Health Log Analytics bietet die veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben. Die neue JavaScript-Funktion ersetzt das vorherige Skript.

Nächste Maßnahme

Fahren Sie mit der Seite **Data Input Mapping** (Dateneingabezuordnung) fort, indem Sie auf den zugehörigen Link **Go to Mapping** (Zu Zuordnung wechseln) klicken. Ordnen Sie Rohdaten zu, die in Ihre Instanz gestreamt werden, um festzustellen, wie sie durch Health Log Analytics verarbeitet werden.

Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics

Standardmäßig ist HLA Die Engine versucht, jede eingehende Protokollzeile automatisch den richtigen Tags zuzuordnen. Sie können die Ergebnisse der automatischen Zuordnung manuell ändern, indem Sie eine JavaScript-Funktion definieren.

Automatische Zuordnung eingehender Protokollzeilen

Health Log Analytics Bei der automatischen Zuordnung werden Protokollbeispiele und Metadaten drei Tags zugewiesen: Serviceinstanz, Komponente und Quelltyp. Die Zuweisung der Serviceinstanz basiert auf der Serviceinstanz, die im Setup der Dateneingabe angegeben ist. Die verbleibenden Tags werden automatisch zugewiesen.

In der folgenden Beispielprotokollzeile verwendet Health Log Analytics beispielsweise das Feld „source“, um die Komponente und den Quelltyp zu finden.


```
{"beat":{"version":"6.8","name":"abc3.prd.acme.com","hostname":"abc3.prd.acme.com"},"@time
stamp":"2020-08-27T10:12:24.792Z","prospector":{"type":"log"},"message":"**** User null
 is requesting the following page http://www.acme.com PROPS:{"subcategory1":"home
 pages","httpStatus":"200","loginLevel":"Anonymous","userAgent":"Mozilla5.0",
 ("pageUrl":\"http://www.acme.com","host":"abc3.prd.acme.com","@version":"1","source":"/o
pt/oracle/weblogic/abc/online_store3/logs/online_store3.out","offset":3951550786}
```


Im Beispiel extrahiert Health Log Analytics die Zeichenfolge „online_store“. Es analysiert die folgenden Felder, wenn sie in der Protokollzeile vorhanden sind: source, path, channel, namespace_name, name, pod_name, source_name und aws_lambda_name. Wenn Daten über Syslog gesendet werden, wird auch das syslog-Tag analysiert.

Extraktion nicht benötigter Daten stoppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine extrahierte Zeichenfolge nicht aussagekräftig genug ist oder redundanten Text oder Informationen enthält, können Sie die Extraktion von verzichtbaren Daten dieser Art stoppen. Weitere Informationen finden Sie unter Extraktion nicht benötigter Protokolldaten in stoppen Health Log Analytics.

Extraktion bestimmter Daten sicherstellen

Sie können sicherstellen, dass Health Log Analytics bestimmte gewünschte Begriffe extrahiert. Weitere Informationen finden Sie unter Extrahieren Sie bestimmte Protokolldaten in Health Log Analytics.

Dateneingabequellen zuordnen

Sie können die Ergebnisse der automatischen Zuordnung manuell ändern, indem Sie eine JavaScript-Funktion definieren. Dateneingabezuordnung Ermöglicht Ihnen, Ihre Protokolldaten nach Serviceinstanz und Verfügbarkeitszone zu organisieren. Eine einzelne Serviceinstanz kann mehrere Komponenten enthalten, und eine Komponente kann Protokolle aus vielen verschiedenen Quelltypen empfangen. Ein Serviceinstanz-Komponentenpaar ist jedoch eindeutig. Quelltypen basieren auf einer bestimmten Protokollstruktur und einem bestimmten Format. Serviceinstanzen und -Komponenten sind breiter definiert und werden daher hauptsächlich für logische Zuordnungen verwendet.

Wird Aktiviert **Testmodus** Vermeidet Explosion Elasticsearch Speicher mit Beispieldaten, der nur zur Optimierung der Protokolldatenzuordnung verwendet wird. Wenn sich die Dateneingabe im Testmodus befindet, Health Log Analytics Erstellt keine Quelltypen, Quellen oder anderen Objekte, die im Standard-Flow erstellt werden. Die gestreamten Daten werden in dedizierten temporären Dateien gespeichert Elasticsearch Indizes, die im Protokoll-Viewer als Komponenten angezeigt werden. Wenn Sie das Skript veröffentlichen und den Testmodus beenden, werden diese temporären Indizes gelöscht, um den Speicherplatzverbrauch zu minimieren.

Wenn Sie eine JavaScript-Funktion definieren, wählen Sie aus **Testen** Zum Anzeigen des Ergebnisses des Skripts, wie es derzeit angegeben ist. Mit dieser Funktionalität können Sie eine Vorschau der erstellten Quelltypen und Quellen anzeigen. Sie können das Skript dann verfeinern, bis es das gewünschte Ergebnis erreicht. Beispielsweise kann es nützlich sein, das Testergebnis mehrerer Versionen der JavaScript-Funktion zu vergleichen.

Hinweis: Standardmäßig verarbeitet der Test 100 Protokolldatenbeispiele. Sie können diese Zahl in den Systemeigenschaften anpassen. Weitere Informationen finden Sie unter Globale Health Log Analytics-Systemeigenschaften konfigurieren.

Während des Setups der Dateneingabe erstellt das System unter Umständen eine zu hohe Gesamtzahl von Dateneingabequellen. Dies kann beispielsweise auf ein fehlerhaftes Zuordnungsskript zurückzuführen sein. In den Systemeigenschaften können Sie Grenzwerte für die Anzahl der pro Dateneingabe erstellten Quellen konfigurieren:

Systemeigenschaft	Beschreibung	Standard
log_source.sources_warning_limit	Warngrenze für die Anzahl der pro Dateneingabe erstellten Quellen.	500
log_source.sources_critical_limit	Kritische Grenze für die Anzahl der pro Dateneingabe erstellten Quellen.	600

Die Anzahl der Protokollquellen, die eine bestimmte Dateneingabe erstellt hat, wird in angezeigt **Anzahl der Quellen** Feld für diese Dateneingabe. Wenn die Gesamtanzahl der während der Dateneingabekonfiguration erstellten Quellen die Warngrenze erreicht, sendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das System eine Warnbenachrichtigung per E-Mail. Außerdem wird eine Nachricht auf den Seiten **Dateneingabezuordnung**, **Protokollquellen** und **Dateneingabe** angezeigt. Die Benachrichtigung und die Nachricht enthalten die Gesamtzahl der bisher erstellten Quellen und die drei Dateneingaben, die die meisten Quellen zu dieser Gesamtzahl beigetragen haben. Wenn keine Aktion ausgeführt wird, erstellt das System weiterhin Quellen, bis die Gesamtzahl die kritische Grenze erreicht. In diesem Fall werden das Setup der Dateneingabe und das Streaming aus allen Dateneingaben automatisch beendet. Sie können Dateneingaben nicht manuell erneut starten, bis das Problem gelöst wurde. Um diesen Status zu beheben, folgen Sie den Anweisungen im Artikel How to handle too many sources in data inputs [KB0963067] (Umgang mit zu vielen Quellen in Dateneingaben) in der Knowledge Base des Now Support.

Protokolldaten binden

Durch das Binden von Protokolldaten an Konfigurationselemente (CIs) in Configuration Management Database (CMDB) können Sie die CMDB nach Endpunkten durchsuchen, die einem Protokoll entsprechen. Wenn Sie eine Dateneingabe konfigurieren, binden Sie Protokolleinträge an eine Serviceinstanz, die an ein CI in der CMDB gebunden ist. Durch die Bindung von Protokolleinträgen, Serviceinstanzen und CIs wird aktiviert HLA Engine zum Korrelieren der Elemente zur Verwendung in der Ursachenanalyse (Ursachenanalyse, RCA). Weitere Informationen finden Sie unter Konfigurieren Sie ein Rsyslog, Filebeat, Oder Winlogbeat Dateneingabe in Health Log Analytics Manuell oder Konfigurieren Sie einen Elasticsearch Dateneingabe in Health Log Analytics Manuell.

Ordnen Sie Rohprotokolldaten in zu Health Log Analytics

Die Zuordnung von Protokolldaten im Rohzustand, die in Ihre Instanz gestreamt werden, bestimmt, wie die Daten behandelt werden. Health Log Analytics strukturiert Protokolle automatisch, erstellt Metriken zur Erkennung von Anomalien und zeigt Warnungen abhängig vom Tagging Ihrer Daten an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig versucht Health Log Analytics, jede eingehende Protokollzeile automatisch den richtigen Tags zuzuordnen. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren.

In der JavaScript-Funktion müssen Sie nur die Serviceinstanz zuordnen (hier als Anwendungsservice bezeichnet). Die Zuordnung der Komponente und des Quelltyps ist optional: Health Log Analytics versucht, ihre Werte automatisch aus den Protokolldaten zu extrahieren. Wenn der Versuch fehlschlägt, werden die Standardwerte zugewiesen. Wenn Sie die Komponente zuordnen, aber nicht den Quelltyp oder umgekehrt, versucht das System, den fehlenden Wert aus den Protokolldaten zu extrahieren. Wenn dies fehlschlägt, wird der Komponentenwert dem Quelltyp zugewiesen (oder umgekehrt, je nachdem, welchen Sie zugeordnet haben). Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

(Nur ACC-Dateneingaben) wenn Agent Client Collector Wechselt zu einem anderen MID-Server Um Failover-Schutz bereitzustellen, muss er zu einer anderen ACC-Dateneingabe wechseln. Daher müssen alle ACC-Dateneingaben dieselbe JavaScript-Funktion aufweisen. Von Health Log Analytics wird die neueste veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt. Das vorherige Skript wird dabei ersetzt. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Informationen zum Failover-Schutz in Agent Client Collector Log Analytics (ACC-L) finden Sie unter Agent Client Collector Log Analytics.

Hinweis: Sie können Protokolldaten im Rohzustand ändern, bevor Health Log Analytics sie zuordnet und strukturiert. Weitere Informationen finden Sie unter Protokolldaten im Rohzustand vor der Verarbeitung bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Dateneingabezuordnung**an.
2. Öffnen Sie einen Datensatz.

   Hinweis: Wenn das Formular „Dateneingabezuordnung“ angezeigt wird, ruft Health Log Analytics automatisch Protokollbeispiele ab. Rufen Sie in nachfolgenden Sitzungen neue Beispiele ab, indem Sie **Refresh Samples** (Beispiele aktualisieren) auswählen.

   Hinweis: Wenn HLA Engine ist ausgefallen, und das Streamen von Daten wurde beendet. Oben auf der Seite „Dateneingabezuordnung“ wird eine Benachrichtigung angezeigt. Wenn dies geschieht, wenden Sie sich an ServiceNow Support.

3. **Wahlweise:** Um die vollständige Protokollnachricht im Rohzustand weiterzuleiten, deaktivieren Sie die automatische Erkennung der Headereigenschaften für diese Dateneingabe, indem Sie **Disable header detection** (Headererkennung deaktivieren) auswählen.
   Weitere Informationen finden Sie unter Erkennung von Headereigenschaften in Health Log Analytics.
4. **Wahlweise:** Aktivieren Sie den Testmodus, indem Sie festlegen **Testmodus** Wert auf EIN.
   Im Testmodus Health Log Analytics Erstellt nicht die Quelltypen, Quellen oder andere Objekte, die im Standard-Flow erstellt werden, um zu vermeiden, dass sie explodieren Elasticsearch Speicher mit Beispieldaten. Weitere Informationen finden Sie unter Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics.
5. **Wahlweise:** Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
6. Wählen Sie im Feld **Unformatierte Eingabebeispiel** ein Protokollbeispiel aus, das die Auswirkungen Ihrer neuen JavaScript-Funktion auf Protokollzeilen veranschaulicht, wenn Sie sie testen.
7. Definieren Sie eine JavaScript-Funktion, die Ihre Dateneingabequellen der richtigen Serviceinstanz (hier als Anwendungsservice bezeichnet), Komponente und Quelltyp zuordnet.

   Hinweis: (Nur ACC-Dateneingaben) Stellen Sie sicher, dass Ihre JavaScript-Funktion zur Verarbeitung von Daten verwendet werden kann, die von allen ACC-Dateneingaben gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

> **Hinweis:** Neben der JavaScript-Standardfunktion bietet Health Log Analytics JS-Funktionsvorlagen für die Datenzuordnung für Linux-Betriebssystem-Protokolle, die mit syslog gestreamt werden, und Windows-Event-Protokolle, die mit Filebeat gestreamt werden, oder Winlogbeat-Event-Protokolle, die mit Winlogbeat gestreamt werden. Die Vorlagen können als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

JavaScript-Funktionsvorlagen

Vorlage	Beschreibung
Mit Syslog gestreamte Linux-Betriebssystemprotokolle	Skript für die Zuordnung von Linux-Protokollen. Ordnet Protokolle der verschiedenen Daemons den richtigen Quelltypen, Komponenten und Serviceinstanzen zu (hier als Anwendungsservices bezeichnet). **Hinweis:** Damit diese JavaScript-Funktion ordnungsgemäß funktioniert, müssen Protokolle über einen Syslog-Wrapper verfügen.
Mit Filebeat gestreamtes Windows-Event-Protokoll	Skript für die Zuordnung von Windows-Event-Protokollen, die mit Filebeat gestreamt werden. Ordnet die verschiedenen zu und gruppiert sie Windows Services für Quelltypen, Komponenten und Serviceinstanzen (hier als Anwendungsservices bezeichnet).
Windows # Mit Winlogbeat gestreamte Winlogbeat-Protokolle	Skript für die Zuordnung von Windows-Event-Protokollen, die mit Winlogbeat gestreamt werden. Ordnet die verschiedenen zu Windows Services für die richtigen Quelltypen, Komponenten und Serviceinstanzen (hier als Anwendungsservices bezeichnet).

Die JavaScript-Funktion zur Vorverarbeitung von Rohprotokolldaten verwendet die folgenden Objekte:

- Signatur: Funktionszuordnung (Beispiel, Metadaten)

Objekt	Beschreibung
Beispiel	Das aktuelle Protokollbeispiel nach der Vorverarbeitung
Metadaten	Objekt, das Folgendes enthält: ▪ Event-Stream: Zugriff über: <Metadatenwert>. Beispiel: `metadata.eventStream.origin` ▪ Transform-Header 1: Zugriff über: <Metadatenwert>. Beispiel: `metadata.headers.i1.type`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekt	Beschreibung
	▪ Transform-Header 2: Zugriff über: <Metadatenwert>. Beispiel: metadata.headers.i2.type ▪ type-Transform-Header 3: Zugriff über: <Metadatenwert>. Beispiel: `metadata.headers.i3.type` ▪ Fallback-Zuweisung: Zugriff über: <Metadatenwert>. Beispiel: `metadata.fallBacks.host`

Hinweis: Sie können mehrere Services pro Quelltyp erstellen und zuordnen.

- Typ und Struktur der Rückgabe

Hinweis: Die JavaScript-Funktion gibt eine Zuordnung mit zwei Einträgen zurück. Ändern Sie diese Rückgabestruktur nicht.

Objekt	Beschreibung
applicationService	Der vorhandene Anwendungsservice (d. h. die Serviceinstanz), dem dieses Beispiel zugewiesen wird. **Hinweis:** Die Serviceinstanz muss an Anomaliewarnungen im Zusammenhang mit dem Protokoll gebunden werden.
Komponente	Komponente, der dieses Beispiel zugewiesen wird
sourceType	Quelltyp, dem dieses Beispiel zugewiesen wird

- Um eine Protokollnachricht zu verwerfen, rufen Sie `return drop ()` auf.

b. Testen Sie die JavaScript-Funktion, indem Sie auf **Test** klicken.

Durch das Testen der JavaScript-Funktion können Sie das Ergebnis des Skripts im Protokollbeispiel anzeigen. Eine Beschreibung der angezeigten Felder finden Sie unter Ergebnisfelder des JavaScript-Funktionstests.

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

c. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

d. Wahlweise: Vergleichen Sie das Ergebnis mehrerer Tests.
Durch den Vergleich der Testergebnisse mehrerer Versionen der JavaScript-Funktion können Sie das Skript verfeinern, bis das gewünschte Ergebnis erreicht wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wenn Sie die JavaScript-Funktion abgeschlossen haben, wählen Sie aus **Speichern Sie die Vorlage** Um es zu speichern.
   Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.
   - Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
   - Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.
9. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnis

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie zum Zuordnen von Dateneingabequellen.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

(Nur ACC-Dateneingaben) Health Log Analytics bietet die veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben. Die neue JavaScript-Funktion ersetzt das vorherige Skript.

Nächste Maßnahme

- (Optional) Ändern Sie Rohprotokolldaten, bevor Health Log Analytics sie zuordnet und strukturiert. Wenn Sie diese Aufgabe sofort ausführen möchten, klicken Sie auf den zugehörigen Link **Go to Preprocessor** (Zu Präprozessor wechseln), um zur Seite **Data Input Preprocessor** (Dateneingabe-Präprozessor) zu wechseln.
- (Optional) Feintunen Sie, wie das System Ihre Protokolldaten liest, indem Sie die Quelltypstruktur verfeinern. Mit diesem Schritt können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern.

Zugehörige Informationen

Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics

Zeigen Sie die Beziehungen zwischen Quelltypen und Protokollquellen in an Health Log Analytics

Erkennung von Headereigenschaften in Health Log Analytics

Extraktion nicht benötigter Protokolldaten in stoppen Health Log Analytics

Extrahieren Sie bestimmte Protokolldaten in Health Log Analytics

Zeigen Sie die Beziehungen zwischen Quelltypen und Protokollquellen in an Health Log Analytics

Erkunden Sie die viele-zu-viele-Beziehungen zwischen Quelltypen und Protokollquellen, um Ihre Dateneingabezuordnung zu optimieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Health Log Analytics Verwendet Quelltypen zum Analysieren von Protokollen und verwendet Protokollquellen als Framework für die Erkennung von Anomalien. Jeder Quelltyp stellt Protokolle bereit, die von mehreren Protokollquellen analysiert werden, und jede Protokollquelle empfängt Protokolle, die von mehreren Quelltypen analysiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die Überprüfung der Zuordnungen zwischen Quelltypen und Protokollquellen können Sie Ihre Dateneingabezuordnung verbessern, um die Leistung und die Ergebnisse zu verbessern.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Dateneingabezuordnung**an.
2. Stellen Sie sicher, dass Protokolldaten in Ihre Instanz gestreamt werden, und öffnen Sie dann einen Dateneingabezuordnungsdatensatz.
3. Zeigen Sie die Zuordnungen zwischen den Protokollquellen und den Quelltypen an.
   - Zeigen Sie die Protokollquellen an, die einem Quelltyp zugeordnet sind:
     a. Öffnen Sie **Quelltypen** Registerkarte zum Anzeigen der generierten Quelltypstrukturen.
     b. Öffnen Sie einen Quelltypstrukturdatensatz.
     c. Wählen Sie einen Quelltyp aus.
     d. Unter **Quellen** , Zeigen Sie alle Protokollquellen an, die Daten von diesem Quelltyp empfangen.
   - Zeigen Sie die Quelltypen an, die einer Protokollquelle zugeordnet sind:
     a. Öffnen Sie **Quellen** Registerkarte zum Anzeigen der generierten Protokollquellen.
     b. Wählen Sie einen Protokollquelldatensatz aus.
     c. Auf der **Quelltypen** Registerkarte alle Quelltypen anzeigen, die Daten in diese Protokollquelle einspeisen.

Hinweis: Die angezeigten Ergebnisse werden einmal täglich aktualisiert. Ergebnisse, die älter als 24 Stunden sind, werden automatisch gelöscht.

Erkennung von Headereigenschaften in Health Log Analytics

In Health Log Analytics, Die automatische Erkennung von Headereigenschaften trennt den Transport-Header von der inneren Protokollnachricht und leitet nur die innere Protokollnachricht an die Quelltypstruktur weiter. Die innere Nachricht enthält die tatsächlichen Protokolldaten ohne Informationen zur Übermittlung.

Die Health Log Analytics Die Anwendung unterstützt die Erkennung von Headereigenschaften für Fluentd, Beats und Syslog (RFC 3164, RFC 5424).

Ab Version 33.0.27 – August 2024 unterstützt das System auch die Erkennung von Headereigenschaften für Protokolle, die dem Datenmodell und semantischen Konventionen für OpenTelemetry-Protokolle entsprechen. Weitere Informationen finden Sie unter OpenTelemetry-Protokolle – Datenmodell-Dokumentation .

Erkennung von Headereigenschaften wird deaktiviert

Wenn Sie die Erkennung von Headereigenschaften für eine Dateneingabe deaktivieren, stoppt die KI-Engine von Health Log Analytics das Extrahieren von Eigenschaften aus dem Header. Das Weiterleiten der vollständigen Rohnachricht kann in den folgenden Situationen nützlich sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die innere Protokollnachricht enthält keine Informationen zum Analysieren, z. B. Zeitstempel und Schweregrad.
- Die Dateneingabe enthält Informationen, die zur Strukturierung verwendet werden können.
- Die Dateneingabe leitet die vollständig analysierten Protokolle weiter.

Informationen zum Deaktivieren der Erkennung von Headereigenschaften finden Sie unter Ordnen Sie Rohprotokolldaten in zu Health Log Analytics.

Extrahieren Sie bestimmte Protokolldaten in Health Log Analytics

Festlegen Health Log Analytics Um angegebene Begriffe aus Protokollen zu extrahieren und bestimmten Komponenten zuzuordnen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Extrahierte Werte**an.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Value to extract** (Zu extrahierender Wert) den Begriff ein, den Health Log Analytics aus den Protokollen extrahieren soll.
4. Geben Sie im Feld **Map to component** (Zu Komponente zuordnen) die Komponente ein, der der Wert zugeordnet werden soll.
5. Wählen Sie im Feld **Property** (Eigenschaft) eine Eigenschaft aus der Liste aus.
6. **Wahlweise:** Verfeinern Sie die Festlegung der Werte, die extrahiert werden sollen, indem Sie zusätzliche Optionen auswählen:
   - Exact match (Genaue Übereinstimmung)
   - Case sensitive (Groß-/Kleinschreibung beachten)
7. **Wahlweise:** Fügen Sie im Feld **Beschreibung** eine Beschreibung des Werts hinzu.
8. Wählen Sie **Absenden** aus.

Extraktion nicht benötigter Protokolldaten in stoppen Health Log Analytics

Wenn eine extrahierte Datenzeichenfolge nicht aussagekräftig genug ist oder redundanten Text oder Informationen enthält, können Sie Health Log Analytics so konfigurieren, dass die Extraktion solcher Daten aus den Protokollen gestoppt wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Ausgeschlossene Werte**an.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Value to exclude** (Auszuschließender Wert) die Zeichenfolge ein, die Health Log Analytics nicht mehr extrahieren soll.
4. **Wahlweise:** Verfeinern Sie die Festlegung der Werte, die nicht mehr extrahiert werden sollen, indem Sie zusätzliche Optionen auswählen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Starts with (Beginnt mit)
- Ends with (Endet mit)
- Enthält
- Case sensitive (Groß-/Kleinschreibung beachten)

5. **Wahlweise:** Fügen Sie im Feld **Beschreibung** eine Beschreibung des Werts hinzu.
6. Wählen Sie **Absenden** aus.

Anpassung der Quelltypstruktur in Health Log Analytics

Mit Health Log Analytics können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern. Durch diese Anpassungen können die ML-Funktionen (maschinelles Lernen) Health Log Analytics Ihre Prioritäten besser verstehen.

Health Log Analytics trennt den Transport-Header automatisch von der inneren Protokollnachricht und sendet die innere Protokollnachricht an die Quelltypstruktur. Eigenschaften werden aus eingehenden Protokollnachrichten extrahiert, und Quelltypfeldern werden automatischBeschriftungen zugeordnet.

Das Ändern der Quelltypstruktur und -Klassifizierung ist Ihre Chance, sicherzustellen, dass der HLADie Engine extrahiert alle Eigenschaften ordnungsgemäß und klassifiziert sie entsprechend.

Hinweis: Da eine einzelne Dateneingabe mehr als einen Quelltyp enthalten kann, strukturiert das System Protokolldaten nach Quelltyp und nicht nach Dateneingabe.

Betrachten Sie beispielsweise das folgende Protokoll:

```
{
 "TenantId": "abc-01-02-03-04-05050708091011121314",
 "@timestamp": "2020-08-28T08:29:23.967Z",
 "Computer": "john Doe_computer",
 "EventType_s": "LogMessage",
 "Job_s": "johnDoe_cell",
 "IP_s": "1.00.00.00",
 "message": "This is the extracted message. This part of the message includes superfluous
content and values",
 "MessageType_s": "OUT",
 "Timestamp_d": 1598603359017850000,
 "Type": "my_LogMessage_is",
 "_ResourceId": ""
}
```

Der Beispielcode enthält „Schlüssel“:„Wert“-Paare. Der Schlüssel ist der Eigenschaftsname, und der Wert ist der Eigenschaftswert.

Der Schlüssel „message“ hat den folgenden Wert: „This is the extracted message. This part of the message includes superfluous content and values“. Wenn Sie möchten, dass Ihre Protokolle nur den aussagekräftigen Teil dieser Nachricht enthalten, fügen Sie JavaScript-Code hinzu, der das System anweist, nur diesen Teil zu extrahieren.

```
//Added JavaScript to extract only the first sentence in the message! if (output['message'] !=
null){ output['message'] = output['message'].slice(0, output['message'].indexOf("\.")); }
(edited)
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieselbe Logik können Sie verwenden, um einen Wert neu zu klassifizieren. Wenn beispielsweise der Schlüssel „Computer“ unbedeutend ist, können Sie seinen Wert auf „ungültig“ festlegen.

Weitere Informationen zur Quelltypstruktur finden Sie im Artikel Source Type Structure – Labels & Classifications (Quelltypstruktur – Bezeichnungen und Klassifizierungen) [KB0863562] in der Now Support-Knowledge Base.

Hinweis: Sie können den Lernmodus für eine Quelltypstruktur erneut aktivieren, wenn Sie die Lernfunktion der KI-Engine erneut verwenden möchten, nachdem der anfängliche Lernzeitraum veraltet ist. Auf der **Quelltypstruktur** Formular auswählen **Erlernen Sie Erneut** Um Analyse, Extraktion, Klassifizierung und Kennzeichnung für die Quelltypstruktur zurückzusetzen und den Lernprozess erneut zu starten.

Zugehörige Informationen

Verfeinern Sie die Quelltypstruktur in Health Log Analytics

Verfeinern Sie die Quelltypstruktur in Health Log Analytics

Feintunen Sie, wie Health Log Analytics Ihre inneren Protokollnachrichten liest und Anomalien erkennt, indem Sie die extrahierten Eigenschaften in der Quelltypstruktur anpassen.

Vorbereitungen

Um die Gründe für die Anpassung von automatisch klassifizierten Eigenschaften und automatisch zugeordneten Bezeichnungen in der Quelltypstruktur besser zu verstehen, finden Sie unter Anpassung der Quelltypstruktur in Health Log Analytics.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingaben** > **Quelltypstruktur**an.
2. Öffnen Sie einen Datensatz.

   Hinweis:

   - Standardmäßig ist **Auto extraction** (Automatische Extraktion) ausgewählt, damit Health Log Analytics den Transport-Header automatisch von der inneren Protokollnachricht trennt.
   - Wenn das Formular „Source Type Structure“ (Quelltypstruktur) zum ersten Mal angezeigt wird, ruft Health Log Analytics Protokollbeispiele automatisch ab. Rufen Sie in nachfolgenden Sitzungen die neuesten Beispiele ab, indem Sie **Refresh Samples** (Beispiele aktualisieren) auswählen.

3. **Wahlweise:** Schauen Sie sich an, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie auf der Registerkarte **Key/Value Mapping** (Schlüssel-Wert-Zuordnung), wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
4. Wählen Sie im Feld **Raw input sample** (Roheingabebeispiel) eine Protokollnachricht aus.

   Health Log Analytics verwendet diese Beispielnachricht, um den kombinierten Effekt der automatischen Extraktion und der JavaScript-Funktion in den Protokollzeilen zu veranschaulichen, wenn Sie Ihre JavaScript-Funktion testen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Felder sind schreibgeschützt:

Feld	Beschreibung
Duration (ms) (Dauer (ms))	Verarbeitungszeit aller Beispiele in Millisekunden
Dropped (Verworfen)	Gesamtzahl der in allen Beispielen verworfenen Protokolle
Fehler	Gesamtzahl der in allen Beispielen aufgetretenen Fehler
Zeitstempel-Extraktionsfehler	Anzahl der Zeitstempel-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Severity extraction failures (Schweregrad-Extraktionsfehler)	Gesamtzahl der Schweregrad-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Message extraction failures (Nachrichten-Extraktionsfehler)	Gesamtzahl der Nachrichten-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Lengthy properties (Lange Eigenschaften)	Gesamtzahl der längeren Eigenschaften in allen Beispielen. Lange Eigenschaften sind Eigenschaften mit mehr als 256 Zeichen. **Hinweis:** Da Health Log Analytics solche Eigenschaften nicht extrahiert, werden sie in Elasticsearch nicht als Stichwörter indiziert.

5. Definieren Sie eine JavaScript-Funktion, die automatisch extrahierte Eigenschaften anpasst oder der Quelltypstruktur Eigenschaften hinzufügt.

   a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

   Hinweis: Zusätzlich zur JavaScript-Standardfunktion bietet Health Log Analytics mehrere JS-Funktionsvorlagen zum Verfeinern der Quelltypstruktur. Die Vorlagen können als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

JS-Funktionsvorlagen	Beschreibung
Key_Values mit regulärem Ausdruck extrahieren	Skript, das zum Analysieren von Protokollen in einer Reihe von Schlüssel-Wert-Paaren verwendet wird, indem reguläre Ausdrücke verwendet werden, um bestimmte Muster von regulären Ausdrücken zu identifizieren. Abhängig von den Protokolldaten, die an den Quelltyp gesendet werden, analysiert es entweder die innere Nachricht oder die vollständige Protokollzeile. Sie können sich anschauen, wie die Daten in den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JS-Funktionsvorlagen	Beschreibung
	Beispielen angezeigt werden, die in die Quelltypstruktur geladen werden. Dieser Prozess ist iterativ. Er wird wiederholt, bis alle Schlüssel-Wert-Paare gefunden wurden.
Key_Values mit split-regex extrahieren	Skript, das zum Analysieren von Protokollen in einer Reihe von Schlüssel-Wert-Paaren verwendet wird, indem reguläre Ausdrücke verwendet werden, um bestimmte Muster von regulären Ausdrücken zu identifizieren. Dieser Prozess erfasst zuerst die Werte in einem LIST-Formular und verwendet dann die Java-Split-Funktion, um Schlüssel-Wert-Paare zu erstellen. Je nachdem, wie die Daten in der Roheingabe angezeigt werden, ist diese Funktion möglicherweise effizienter als das Extrahieren von Key_Values mit regulärem Ausdruck. Die Roheingabe ist entweder die innere Nachricht, die die Headererkennung weiterleitet, oder das vollständige Rohprotokoll, wenn die Headererkennung deaktiviert ist oder für dieses bestimmte Protokoll nicht funktioniert.
JSON-Analyse - reduzieren	Skript, das zum Extrahieren von JSON-Informationen verwendet wird, die Teil einer anderen Textzeichenfolge aus der Roheingabe sind. Beispielsweise könnten die Informationen eine JSON-Anforderung sein, die als Teil einer längeren inneren Nachricht geschrieben wurde. Innere JSON-Abschnitte sind schwer aufzuteilen. In solchen Fällen kann dieses Skript verwendet werden, um die Schlüssel-Wert-Paare zu „reduzieren“ oder zu analysieren.
Neues Feld aus Roheingabe extrahieren	Skript, das zum Extrahieren eines neuen Felds aus der Roheingabe verwendet wird, indem ein regulärer Ausdruck mit Erfassungsgruppen verwendet wird, um das Muster des neuen Felds zu identifizieren.
XML-Format analysieren	Skript, das zum Extrahieren von Schlüssel-Wert-Paaren aus dem XML verwendet wird, indem das XML-Format mithilfe eines regulären Ausdrucks identifiziert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JS-Funktionsvorlagen	Beschreibung
	Dieser Prozess ist iterativ. Er wird wiederholt, bis alle Schlüssel-Wert-Paare gefunden wurden.
Numerischen Schweregrad als Textwerte festlegen	Skript, das zum Konvertieren von numerischen Schweregradwerten in entsprechende Textschweregradwerte verwendet wird. **Hinweis:** Damit das System den Schweregrad eines Protokolls richtig identifizieren kann, muss der Schweregrad im Textformat angegeben werden. Es dürfen keine numerischen Schweregradwerte übrig bleiben.
Trim-Funktion	Skript, das zum Entfernen der doppelten Anführungszeichen verwendet wird, die die Zeichenfolge von VALUE umgeben. Sie können diese Funktion anpassen, um alle anderen Zeichen zu entfernen, die den Ausgabewert eines Schlüssel-Wert-Paares umgeben.

Die JavaScript-Funktion zum Verfeinern der Quelltypstruktur verwendet die folgenden Objekte:

Signatur: Funktionskonstrukt (Beispiel, Ausgabe)

Objekt	Beschreibung
Beispiel	Aus der Beispielnachricht extrahierte innere Nachricht
Ausgabe	Objekt, das die Schlüssel-Wert-Paarzuordnung enthält

b. Testen Sie die JavaScript-Funktion, indem Sie auf **Test** klicken.

c. Zeigen Sie das Ergebnis der JavaScript-Funktion in den zugehörigen Listen an, und nehmen Sie bei Bedarf Änderungen vor.

- Die Registerkarte **Schlüssel/Wert-Zuordnungen** zeigt die Auswirkungen Ihrer JavaScript-Funktion in Kombination mit der automatischen Extraktion des Systems für Ihr Roheingabebeispiel.

  Gegebenenfalls können Sie Schlüssel ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit dem Feld **Classification** (Klassifizierung) können Sie die Klassifizierung einer Eigenschaft zurücksetzen. Die verfügbaren Typen lauten:

Typ	Beschreibung	Beispiel
Zähler	Eine Eigenschaft bei dieser Klassifizierung erkennt Anomalien anhand der Häufigkeit, in der die Eigenschaft in jeder Protokollnachricht erscheint. Sie stellt Änderungen in der Menge dieses Werts als Teil der automatischen Ursachenanalyse dar. **Hinweis:** Als Zähler klassifizierte Eigenschaften verbrauchen Ressourcen.	Statuscodes, Antwortcodes, Aktionen oder Muster
Anzeige	Eine Eigenschaft mit dieser Klassifizierung erkennt Anomalien in einem numerischen Wert, der kontinuierlich gemeldet wird. **Hinweis:** Als Anzeige klassifizierte Eigenschaften verbrauchen Ressourcen.	CPU, Arbeitsspeicher oder Antwortzeit
Anzeige ohne Zeit	Eine Eigenschaft mit dieser Klassifizierung erkennt Anomalien in einem numerischen Wert, der nicht kontinuierlich gemeldet wird. Das System meldet eine Anomalie in diesem Wert, egal wann die Anomalie aufgetreten ist. **Hinweis:** Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .	
Automatische Ursachenanalyse (nur ARC)	Eine Eigenschaft mit dieser Klassifizierung meldet die Eigenschaft nicht als eigenständige Anomalie, sondern als Teil der	Benutzername, IP-Adressen, Anwendungskomponenten oder Rechenzentrum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung	Beispiel
	automatischen Ursachenanalyse einer anderen Anomalie.	
Ungültig	Eine Eigenschaft mit dieser Klassifizierung wird in der automatischen Ursachenanalyse nicht berechnet oder angezeigt. **Hinweis:** Als ungültig klassifizierte Eigenschaften sparen Ressourcen.	

- Über das Feld **Bezeichnungen, die zugewiesen werden sollen** können Sie eine Eigenschaft für eine Bezeichnung festlegen.

Bezeichnung	Beschreibung
Zeitstempel	Eigenschaft, die den Zeitstempel des Events enthält **Hinweis:** Wenn die automatische Erkennung von Headereigenschaften aktiviert ist und der Quelltyp keinen Zeitstempel hat, extrahiert das System den Zeitstempel aus dem Übertragungsheader. Wenn die Headererkennung deaktiviert ist oder für die relevanten Protokollzeilen in der Dateneingabe nicht funktioniert, müssen alle Protokollzeilen über die richtigen Zeitstempel verfügen.
Schweregrad	Eigenschaft, die den Schweregrad des Protokolls darstellt
Nachricht	Protokollnachricht Das System verwendet diese Eigenschaft, um Textmuster in den Daten zu identifizieren.
Host	Eigenschaft, die den Host darstellt, von dem das Event gesendet wurde **Hinweis:** Wenn die automatische Erkennung von Headereigenschaften aktiviert ist und der Quelltyp keinen Host hat, extrahiert das System den Host aus dem Übertragungsheader. Wenn die Headererkennung deaktiviert ist oder für die relevanten Protokollzeilen in der Dateneingabe nicht funktioniert, müssen alle Protokollzeilen über die einen Host verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Beschreibung
Externe ID	Eigenschaft, die als eindeutiger Bezeichner für diesen Event-Typ dient. Beispiel: Event-ID im Windows-Event-Protokoll

- Im Feld **Rename key** (Schlüssel umbenennen) können Sie den Schlüssel umbenennen.

- Die Registerkarte **Outcome Key-Value** (Ergebnis-Schlüssel-Wert) zeigt, wie Ihre JavaScript-Funktion die Daten verarbeitet hat.
- Die **Dateneingabezuordnungen** Auf der Registerkarte werden die Dateneingabezuordnungen für den aktuellen Quelltyp angezeigt.

  Die **Zeit des letzten Ereignisses** Die Spalte auf dieser Registerkarte zeigt das letzte Datum und die letzte Uhrzeit an, zu der die KI-Engine ein Protokoll für die Dateneingabezuordnung verarbeitet hat. Das System aktualisiert diese Informationen alle 5 Minuten. Wenn Sie wissen, wann das letzte Protokoll für diese Dateneingabezuordnung verarbeitet wurde, können Sie leichter überprüfen, ob Protokolldaten gestreamt werden.

- Die übrigen Registerkarten zeigen Fehler, Nachrichten-Extraktionsfehler, Schweregrad-Extraktionsfehler, Zeitstempel-Extraktionsfehler und lange Eigenschaften an.

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

d. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

6. Klicken Sie auf **Save template** (Vorlage speichern), um die JavaScript-Funktion zu speichern. Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.
   - Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
   - Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.
7. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnis

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie, um zu optimieren, wie sie Ihre inneren Protokollnachrichten liest und Anomalien erkennt.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Nächste Maßnahme

Fahren Sie mit den verbleibenden Setup-Aufgaben für Dateneingaben fort: Stellen Sie sicher, dass alle Protokollquellen vorhanden und aktiv sind, und fügen Sie gegebenenfalls Zeitstempelformate hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics Inhaltspakete für kürzere Amortisierungszeit

Verkürzen Sie die Onboarding-Zeit für Health Log Analytics Anwendung durch Installation von Inhaltspaketen. Die Pakete enthalten Standardquelltypen und Zuordnungsskriptvorlagen, die Ihnen die Zeit sparen, die Sie benötigen, um sie von Grund auf neu zu erstellen.

Nach der Installation eines Inhaltspakets Health Log Analytics Beginnt sofort mit dem Streamen und Analysieren Ihrer Protokolldaten. Die Anwendung erkennt und analysiert die Daten, generiert relevantere Warnungen und reduziert Rauschen ab dem Zeitpunkt der Integration. Sie können die Zuordnungskonfiguration auch später bei Bedarf anpassen.

Sie können Inhaltspakete auf zwei verschiedene Arten integrieren:

- Wählen Sie ein Inhaltspaket aus, wenn Sie eine Dateneingabe konfigurieren. Health Log Analytics Aktiviert das ausgewählte Paket automatisch und verwendet sein Zuordnungsskript für die Zuordnung der Dateneingabequellen.
- Aktivieren Sie ein Inhaltspaket, bevor Sie eine Dateneingabe konfigurieren . Wenn Sie die Dateneingabe konfiguriert haben und die Rohprotokolldaten zuordnen, wählen Sie das Zuordnungsskript des Inhaltspakets aus **Dateneingabezuordnung** Formular.

Derzeit ist ein Inhaltspaket für das Streaming von Protokollen aus verfügbar Linux Verwenden Filebeat.

Hinweis: Alle Konfigurationen in Inhaltspaketen sind in der globalen Domäne vorhanden. Wenn Sie Domänentrennung verwenden, ist der Inhaltspaketinhalt nur für Protokolle in der globalen Domäne verfügbar.

Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 25.0.17 – November 2022 und höher, verfügbar über ServiceNow Store .

Aktivieren Sie ein Inhaltspaket in Health Log Analytics

Sie können ein Inhaltspaket aktivieren, bevor Sie eine Dateneingabe konfigurieren.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics Inhaltspakete für kürzere Amortisierungszeit.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

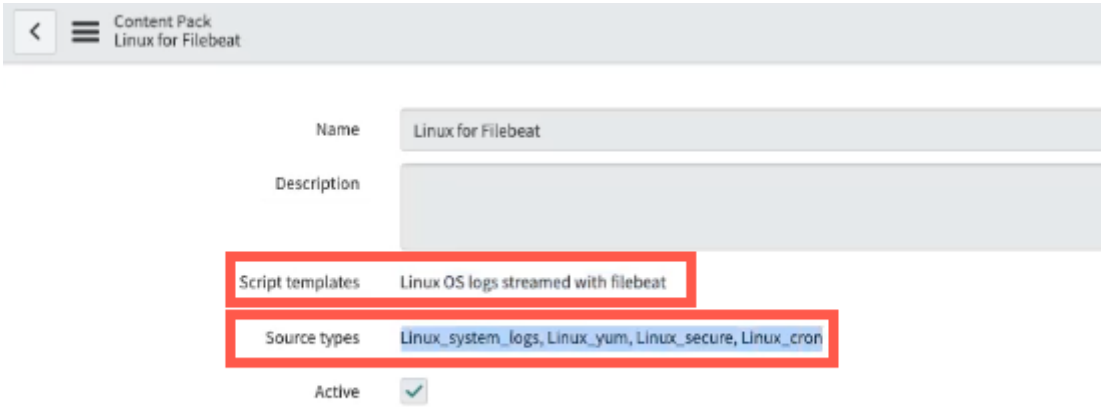
1. Navigieren zu **Alle** > **Health Log Analytics** > **Inhaltspakete**an.
2. Öffnen Sie das entsprechende Inhaltspaket für Ihre Dateneingabe.

   Hinweis: Derzeit ist ein Inhaltspaket für das Streaming von Protokollen aus verfügbar Linux Verwenden Filebeat.

3. Auf der **Inhaltspaket** Formular auswählen **Aktivieren** .
   Die **Aktiv** Das Kontrollkästchen wird ausgewählt angezeigt. Das aktivierte Inhaltspaket zeigt die Skriptvorlagen und Quelltypen an, die ihm zugeordnet sind.

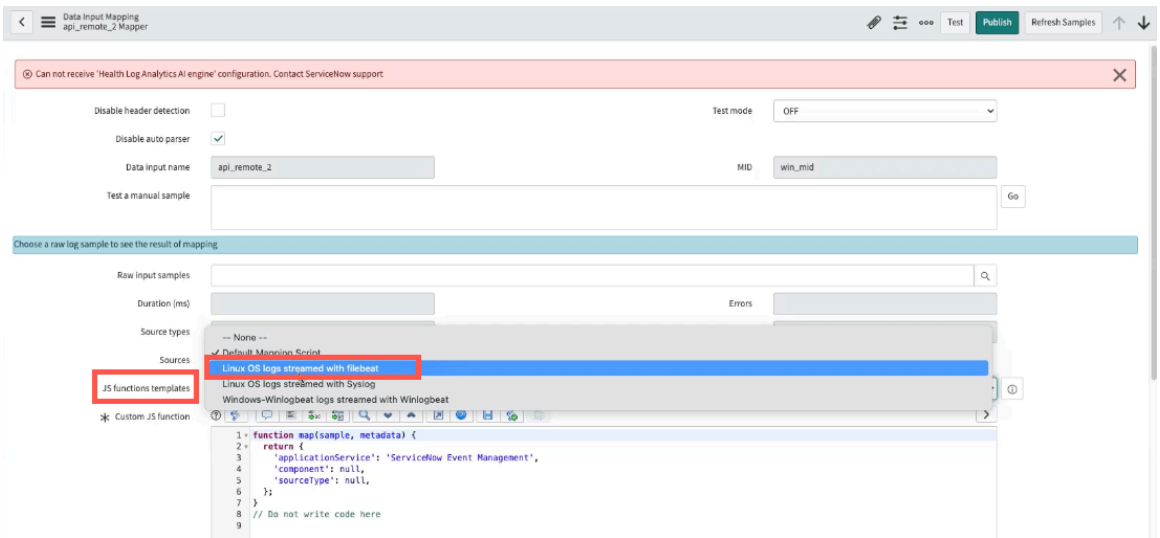
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Die im Inhaltspaket enthaltenen Quelltypen sind möglicherweise bereits auf Ihrem vorhanden ServiceNow Instanz. In diesem Fall Health Log Analytics Benennt die Inhaltspaketquelltypen automatisch um, indem dem Namen ein Inhaltspaketsuffix hinzugefügt wird. Wenn Sie die Inhaltspaketquelltypen und ihre Zuordnung verwenden möchten, löschen oder benennen Sie die ursprünglichen Quelltypen um, und entfernen Sie dann das Suffix aus den Inhaltspaketquelltypen. Andernfalls Health Log Analytics Verwendet die ursprünglichen Quelltypen.

Auf der **Dateneingabezuordnung** Formular, wird das Zuordnungsskript als Vorlagenoption für JavaScript-Funktionen aufgeführt.



Nächste Maßnahme

Wenn Sie die Dateneingabe konfiguriert haben und Ihre Rohprotokolldaten zuordnen, können Sie das Zuordnungsskript des Inhaltspakets aus auswählen **JS-Funktionsvorlagen** Dropdown-Liste.

Migrieren von Health Log Analytics Dateneingabekonfiguration zwischen Instanzen

Exportieren Sie ein Health Log Analytics Konfiguration der Dateneingabe- und Quelltypen als Update-Satz, und importieren Sie sie in ein anderes ServiceNow Instanz. In der Zielumgebung können Sie die migrierte Dateneingabe zum Streamen und Verarbeiten von Protokolldaten verwenden. Diese Funktionalität spart Zeit und reduziert mögliche Fehler, indem vermieden wird, dass die Einstellungen in der Zielinstanz erneut konfiguriert werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die migrierte Konfiguration umfasst die Zuordnung und alle anderen relevanten Einstellungen, mit Ausnahme der Anmeldeinformationen. Abhängig von der Dateneingabe, die Sie exportieren, müssen Sie möglicherweise Anmeldeinformationen in der Zielumgebung konfigurieren. Wenn Sie beispielsweise Amazon CloudWatch- oder Amazon S3-Dateneingaben exportieren, müssen Sie Anmeldeinformationen für Amazon Web Services (AWS) konfigurieren.

Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 25.0.17 – November 2022 und höher, verfügbar über ServiceNow Store .

Für allgemeine Informationen zu Update-Sätzen in ServiceNow AI Platform, Siehe System-Update-Sätze .

Exportieren Sie ein Health Log Analytics Dateneingabekonfiguration

Exportieren Sie die Konfiguration von Health Log Analytics Dateneingabe mit oder ohne die zugehörigen Quelltypen für einen Update-Satz. Sie können dann den Update-Satz in die Zielumgebung importieren.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Migrieren von Health Log Analytics Dateneingabekonfiguration zwischen Instanzen.

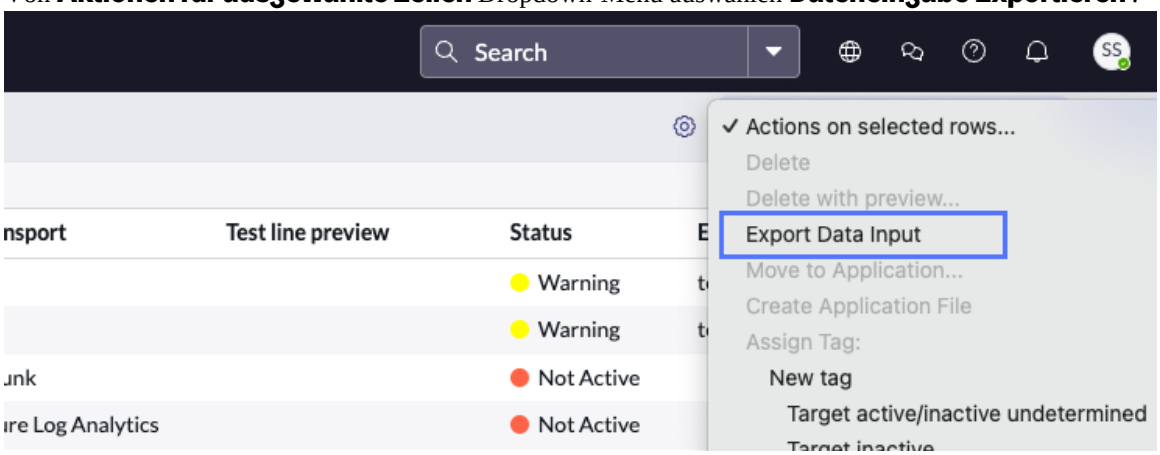
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**an.
2. Wählen Sie in der Liste Dateneingaben die Dateneingabe aus, die Sie exportieren möchten.
3. Exportieren Sie die Dateneingabe in einen Update-Satz.

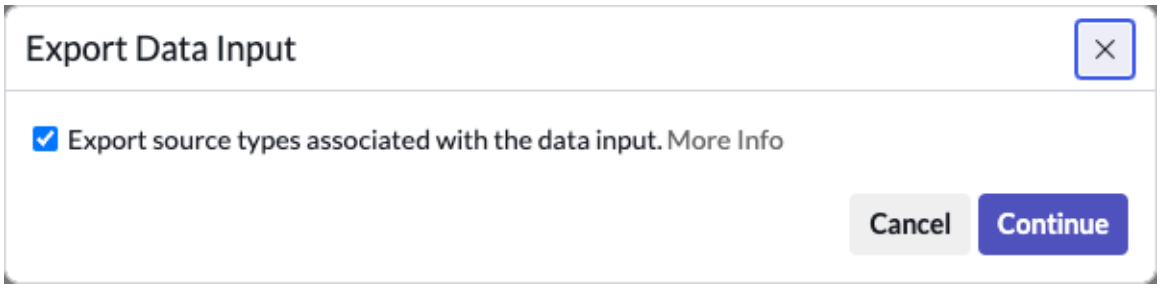
> **Hinweis:** Die exportierte Konfiguration enthält nicht die für die Dateneingabe konfigurierte Serviceinstanz.

   a. Von **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Dateneingabe Exportieren** .



   b. In **Dateneingabe Exportieren** Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Lassen Sie das Kontrollkästchen aktiviert, um die Quelltypen einzubeziehen, die der Dateneingabe in den Update-Satz zugeordnet sind.

  Wenn das Kontrollkästchen aktiviert ist, enthält der Update-Satz die folgenden Quelltypbezogenen Tabellen:

  - sn_occ_Source_type
  - sn_occ_Source_type_Structure
  - sn_occ_Sources
  - sn_occ_timestamp_Formats
  - sn_occ_lexical_keywords
  - sn_occ_log_Correlator
  - sn_occ_log_Source_Retention
  - sn_occ_Quick_Replacements
  - sn_occ_rekonstruktors
  - sn_occ_Replacements
- Deaktivieren Sie das Feld, um die Dateneingabe ohne die zugehörigen Quelltypen zu exportieren. Wenn Sie beispielsweise die Dateneingabekonfiguration wiederverwenden möchten, aber die Quelltypen von Grund auf neu konfigurieren möchten.

  Wenn das Feld leer ist, enthält der Update-Satz keine Quelltypbezogenen Tabellen.

  Hinweis: Sie können Quelltypen separat exportieren. Weitere Informationen finden Sie unter Exportieren Sie Quelltypen in einen Update-Satz in Health Log Analytics.

c. Wählen Sie **Fortsetzen**.

Die Dateneingabe mit oder ohne Quelltypen wird in einen Update-Satz exportiert.

Hinweis: Ein Update-Satz kann als übergeordnetes Element für mehrere untergeordnete Update-Sätze fungieren.

4. Wählen Sie Aus **Update-Satz herunterladen** Zum Herunterladen des Update-Satzes in die Instanz. Der Update-Satz wird als XML-Datei heruntergeladen.

Nächste Maßnahme

Importieren Sie den Update-Satz in den erforderlichen ServiceNow Instanz. Weitere Informationen finden Sie unter Importieren Sie ein Health Log Analytics Dateneingabe für eine Zielinstanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie ein Health Log Analytics Dateneingabe für eine Zielinstanz

Importieren Sie eine Dateneingabekonfiguration, die Sie aus einer anderen Instanz als Update-Satz exportiert haben.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Migrieren von Health Log Analytics Dateneingabekonfiguration zwischen Instanzen.

Bevor Sie dieses Verfahren ausführen, exportieren Sie die Dateneingabe in einen Update-Satz. Weitere Informationen finden Sie unter Exportieren Sie ein Health Log Analytics Dateneingabekonfiguration.

Erforderliche Rolle: Administrator

Prozedur

1. Importieren Sie in der Zielinstanz den Update-Satz, der die Dateneingabekonfiguration enthält.
   a. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
   b. Wählen Sie unter zugehörige Links die Option aus **Update-Satz aus XML importieren** .
   c. Wählen Sie Aus **Wählen Sie die Datei aus** Und öffnen Sie die XML-Datei des Update-Satzes im Ordner Downloads.
   d. Wählen Sie **Hochladen** aus.
   Der Update-Satz wird in die Instanz hochgeladen und in angezeigt **Update-Sätze Abgerufen** Liste im Status „geladen“.
2. Identifizieren und beheben Sie Fehler im Update-Satz.
   a. In **Update-Sätze Abgerufen** Liste, öffnen Sie den Update-Satz-Datensatz.
   b. Wählen Sie Aus **Vorschau Des Update-Satz-Batches Anzeigen** Um Fehler zu erkennen.
   Die **Vorschau Des Batch-Update-Satzes** Dialogfeld zeigt den Fehler an, was das erwartete Verhalten ist.
   c. Schließen Sie das Dialogfeld, und beheben Sie die Fehler in **Update-Satz-Vorschauprobleme** Zugehörige Liste.

   Weitere Informationen finden Sie unter Vorschau eines Remote-Update-Satzes anzeigen .

   Sie können Fehler ignorieren, die mit „Datensatz in [Tabelle] nicht gefunden“ für die folgenden Tabellen beginnen:
   - aws_credentials
   - azure_sas_credentials
   - azure_Service_Principal
   - Basic_auth_credentials
   - cmdb_ci_Service_Auto: Serviceinstanz
   - ecc_Agent: MID

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ecc_Agent_Cluster: MID-Server-Cluster
- kafka_ssl_credentials
- sn_occ_Data_input_preprocess_example
- sn_occ_Data_input_preprocess_example_row
- sn_occ_gcp_credentials
- sn_occ_mapper_example
- sn_occ_Source_type_Examples
- sn_occ_Source_type_Structure_Data

d. Wählen Sie die Fehler aus, die Sie ignoriert haben, und wählen Sie dann aus **Wählen Sie Alle Aus** Kontrollkästchen.

e. Von **Aktionen für ausgewählte Zeilen...** Dropdown-Menü auswählen **Akzeptieren Sie das Remote-Update** .

f. In **Vorschau der Probleme für Batch anzeigen** Wählen Sie in der zugehörigen Liste alle verbleibenden Fehler aus, und akzeptieren Sie das Remote-Update, wie in den vorherigen Schritten erläutert.

3. Wenn alle Fehler im Update-Satz behoben wurden, wählen Sie aus **Update-Satz-Batch Bestätigen** . Die importierte Dateneingabe wird in der Liste Dateneingaben angezeigt. Der Import enthält Zuordnungseinstellungen und alle anderen relevanten Konfigurationen.
4. Konfigurieren Sie in der importierten Dateneingabe Folgendes.
   - Der MID-Server, an den die Protokolle gestreamt werden
   - Anmeldeinformationen.

     Hinweis: Ob Sie Anmeldeinformationen konfigurieren müssen, hängt von der Dateneingabe ab, die Sie importiert haben. Sie müssen beispielsweise Anmeldeinformationen für Amazon Web Services (AWS) konfigurieren Amazon CloudWatch Und Amazon S3 Dateneingaben.

   - (Optional) die Serviceinstanz, an die die Protokolldaten gebunden werden sollen.

   Weitere Informationen finden Sie in der Konfigurationsdokumentation für die relevante Dateneingabe: Richten Sie Dateneingaben in ein Health Log Analytics Manuell.

Ergebnis
Sie können die Dateneingabe zum Streamen und Verarbeiten von Protokolldaten verwenden.

Exportieren Sie Quelltypen in einen Update-Satz in Health Log Analytics

Exportieren Sie Quelltypen in einen Update-Satz, der getrennt von ist Health Log Analytics Dateneingabekonfiguration. Sie können dann den Update-Satz in die Zielumgebung importieren.

Vorbereitungen
Eine Übersicht über diese Funktion finden Sie unter Migrieren von Health Log Analytics Dateneingabekonfiguration zwischen Instanzen.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Quelltypen**an.
2. Wählen Sie in der Liste Quelltypen einen oder mehrere Quelltypen aus, die Sie exportieren möchten.
3. Von **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Quelltypen Exportieren** .
   Die Quelltypen werden in einen Update-Satz exportiert.

   Hinweis: Ein Update-Satz kann als übergeordnetes Element für mehrere untergeordnete Update-Sätze fungieren.

4. Wählen Sie Aus **Update-Satz herunterladen** Zum Herunterladen des Update-Satzes in die Instanz.
   Der Update-Satz wird als XML-Datei heruntergeladen.

Nächste Maßnahme

Importieren Sie den Update-Satz in den erforderlichen ServiceNow Instanz. Weitere Informationen finden Sie unter Importieren Health Log Analytics Quelltypen für eine Zielinstanz.

Importieren Health Log Analytics Quelltypen für eine Zielinstanz

Importieren Sie Quelltypen, die Sie getrennt von exportiert haben Health Log Analytics Dateneingabekonfiguration.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Migrieren von Health Log Analytics Dateneingabekonfiguration zwischen Instanzen.

Bevor Sie dieses Verfahren ausführen, exportieren Sie die Quelltypen in einen Update-Satz. Weitere Informationen finden Sie unter Exportieren Sie Quelltypen in einen Update-Satz in Health Log Analytics.

Erforderliche Rolle: Administrator

Prozedur

1. Importieren Sie in der Zielinstanz den Update-Satz, der die Quelltypen enthält.

   a. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.

   b. Wählen Sie unter zugehörige Links die Option aus **Update-Satz aus XML importieren** .

   c. Wählen Sie Aus **Wählen Sie die Datei aus** Und öffnen Sie die XML-Datei des Update-Satzes im Ordner Downloads.

   d. Wählen Sie **Hochladen** aus.
   Der Update-Satz wird in die Instanz hochgeladen und in angezeigt **Update-Sätze Abgerufen** Liste im Status „geladen“.

2. Identifizieren und beheben Sie alle Fehler im Update-Satz.

   a. In **Update-Sätze Abgerufen** Liste, öffnen Sie den Update-Satz-Datensatz.

   b. Wählen Sie Aus **Vorschau Des Update-Satz-Batches Anzeigen** Um Fehler im Update-Satz zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Vorschau Des Batch-Update-Satzes** Dialogfeld zeigt den Fehler an, was das erwartete Verhalten ist.

c. Schließen Sie das Dialogfeld, und beheben Sie die Fehler in **Update-Satz-Vorschauprobleme** Zugehörige Liste.
Sie können Fehler ignorieren, die mit „Datensatz in [Tabelle] nicht gefunden“ für die folgenden Tabellen beginnen:

d. Wählen Sie die Fehler aus, die Sie ignoriert haben, und wählen Sie dann aus **Wählen Sie Alle Aus** Kontrollkästchen.

e. Von **Aktionen für ausgewählte Zeilen...** Dropdown-Menü auswählen **Akzeptieren Sie das Remote-Update** .

f. In **Vorschau der Probleme für Batch anzeigen** Wählen Sie in der zugehörigen Liste alle verbleibenden Fehler aus, und akzeptieren Sie das Remote-Update, wie in den vorherigen Schritten erläutert.

3. Wenn alle Fehler im Update-Satz behoben wurden, wählen Sie aus **Update-Satz-Batch Bestätigen** .

Ergebnis
Die importierten Quelltypen werden in der Liste Quelltypen angezeigt.

Überprüfen Sie die gRPC- und Netzwerkkonnektivität für Health Log Analytics Auf der MID-Server

Verifizieren Sie das Health Log Analytics Kann ordnungsgemäß funktionieren, indem Diagnosetests auf durchgeführt werden MID-Server Dient zum Überprüfen der gRPC- und Netzwerkkonnektivität.

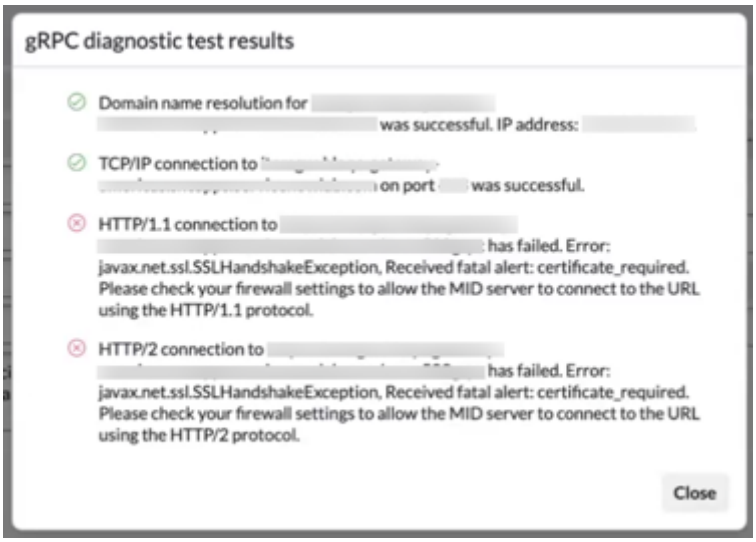
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Netzwerk- und Sicherheitskonfiguration Ihrer Organisation wird möglicherweise beibehalten Health Log Analytics Von funktioniert ordnungsgemäß. Beispielsweise können komplexe Konfigurationen mit Proxy- und Firewall-Einstellungen ausgehende Verbindungen blockieren. Um Betriebsprobleme zu vermeiden, können Sie gRPC und Netzwerkkonnektivität auf dem testen MID-Server.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**an.
2. Öffnen Sie das entsprechende MID-Server Datensatz.
3. Wählen Sie unter zugehörige Links die Option aus **Testen Sie die gRPC-Verbindung** .
   Das System führt gRPC-Konnektivitätstests durch, z. B. Domänennamensauflösung, TCP/IP und HTTP-Verbindung. Wenn der Test abgeschlossen ist, werden die Testergebnisse angezeigt. Erfolgreiche Tests werden durch ein grünes Häkchen vorangestellt, während fehlgeschlagene Tests durch ein rotes x-Zeichen gekennzeichnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Beheben Sie die Probleme, die zum Fehlschlagen von Tests geführt haben, indem Sie die Anweisungen auf befolgen **Ergebnisse des gRPC-Diagnosetests** Bildschirm.
5. Wählen Sie Aus **Testen Sie die gRPC-Verbindung** Erneut und bestätigen Sie, dass alle Tests erfolgreich abgeschlossen wurden.

Health Log Analytics verwalten

In diesem Abschnitt werden Aufgaben behandelt, die an beteiligt sind Health Log Analytics Verwaltung. Sie enthält Informationen, die Sie aufbewahren müssen Health Log Analytics Wird effizient ausgeführt.

Health Log Analytics-Systemeigenschaften für eine einzelne Protokollquelle konfigurieren

Konfigurieren Sie Systemeigenschaften für eine bestimmte Protokollquelle, wenn Sie die Standardwerte ändern müssen. Normalerweise sollte das nicht erforderlich sein.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Ändern der Health Log Analytics-Systemeigenschaften wirkt sich auf Back-end-Prozesse aus und kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Eigenschaften ändern müssen, sollten Sie daher Ihre Anpassungen dokumentieren. Notieren Sie sich beispielsweise den Wert vor und nach einer Änderung und den Zeitpunkt der Änderung.

Hinweis: Dient zum Ändern von Health Log Analytics Systemeigenschaft, deren **Neustart erforderlich** Wert ist **Wahr** , Kontakt ServiceNow Unterstützung, um sie für Sie zu ändern.

Für eine vollständige Beschreibung aller Health Log Analytics Systemeigenschaften, siehe HLA-Systemeigenschaften [KB0869842] artikel in Now Support Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**an.
2. Klicken Sie auf der Registerkarte **Source properties** (Quelleigenschaften) mit der rechten Maustaste auf eine Eigenschaft.
3. Wählen Sie im Popup-Menü **Override property value** (Eigenschaftswert überschreiben) aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie im Feld **Value** (Wert) den entsprechenden Wert ein.
5. Wählen Sie **Absenden** aus.

Ergebnis
Die vorherige Einstellung für die ausgewählte Protokollquelle wird mit dem neuen Wert überschrieben.

Zugehörige Informationen

Globale Health Log Analytics-Systemeigenschaften konfigurieren

Globale Health Log Analytics-Systemeigenschaften konfigurieren

Konfigurieren Sie global Health Log Analytics Systemeigenschaften, wenn Sie die Standardwerte ändern müssen, was normalerweise nicht erforderlich sein sollte.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Das Ändern der Health Log Analytics-Systemeigenschaften wirkt sich auf Back-end-Prozesse aus und kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Eigenschaften ändern müssen, sollten Sie daher Ihre Anpassungen dokumentieren. Notieren Sie sich beispielsweise den Wert vor und nach einer Änderung und den Zeitpunkt der Änderung.

Hinweis: Dient zum Ändern von Health Log Analytics Systemeigenschaft, deren **Neustart erforderlich** Wert ist **Wahr** , Kontakt ServiceNow Unterstützung, um sie für Sie zu ändern.

Für eine vollständige Beschreibung aller Health Log Analytics Systemeigenschaften, siehe HLA-Systemeigenschaften [KB0869842] artikel in Now Support Knowledge Base.

Prozedur
1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Systemeigenschaften**an.
2. Wählen Sie eine Eigenschaft mit dem Bereich „Source“ (Quelle) aus.
3. Geben Sie im Feld **Value** (Wert) den entsprechenden Wert ein.
4. Wählen Sie **Aktualisieren**.
   Die Einstellung gilt für Protokollquellen, die ab diesem Zeitpunkt erstellt werden.
5. Bestimmen Sie den Anwendungsbereich der neuen Einstellung.
   - Um die Einstellung nur auf Protokollquellen anzuwenden, die ab diesem Zeitpunkt erstellt werden, wählen Sie **Update** (Aktualisieren).
   - Um Werte für diese Eigenschaft in allen vorhandenen Protokollquellen zu überschreiben und die geänderte Einstellung auf alle neuen Protokollquellen anzuwenden, wählen Sie **Override source property** (Quelleigenschaft überschreiben).

Zugehörige Informationen

Health Log Analytics-Systemeigenschaften für eine einzelne Protokollquelle konfigurieren

Health Log Analytics-Systemfunktionen aktivieren oder deaktivieren

Passen Sie die Basiskonfiguration von Health Log Analytics an, indem Sie Systemfunktionen aktivieren oder deaktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Features**an. Standardmäßig zeigt die Tabelle die Systemfunktionen, die Administratoren am häufigsten ändern. Um die vollständige Liste der Funktionen anzuzeigen, verwenden Sie die Filteroptionen.
2. Wählen Sie in der Tabelle einen Funktionsdatensatz aus.
   Der Datensatz enthält die folgenden Informationen:
   - Name der Funktion
   - Beschreibung des Zwecks der Funktion
   - Standardstatus der Funktion
   - Aktueller Status der Funktion
3. Legen Sie den Status einer Systemfunktion auf EIN fest, um die Funktion zu aktivieren, bzw. auf AUS, um sie zu deaktivieren.
4. Wählen Sie **Aktualisieren**.

Health Log Analytics Warnungsbenachrichtigung in Slack Oder Microsoft Teams Kanäle

Von Health Log Analytics werden Benachrichtigungen für neue Anomaliewarnungen in Echtzeit an Slack- oder Microsoft Teams-Kanäle gesendet. Diese integrierte Funktionalität befreit Sie von der kontinuierlichen Überwachung von Protokollen, um Incidents zu vermeiden.

Die Benachrichtigungen enthalten die Nummer der Warnung, die Beschreibung, den Schweregrad, das zugehörige Konfigurationselement, den Status und die Prioritätsgruppe. Sie können die Warnungen filtern, für die Benachrichtigungen an Ihren Kanal gesendet werden. Beispielsweise kann es empfehlenswert sein, nur Warnungen mit dem Schweregrad „Schwerwiegend“ oder der Prioritätsgruppe „Hoch“ zu erhalten. Standardmäßig werden bei sekundären Warnungen keine Benachrichtigungen gesendet.

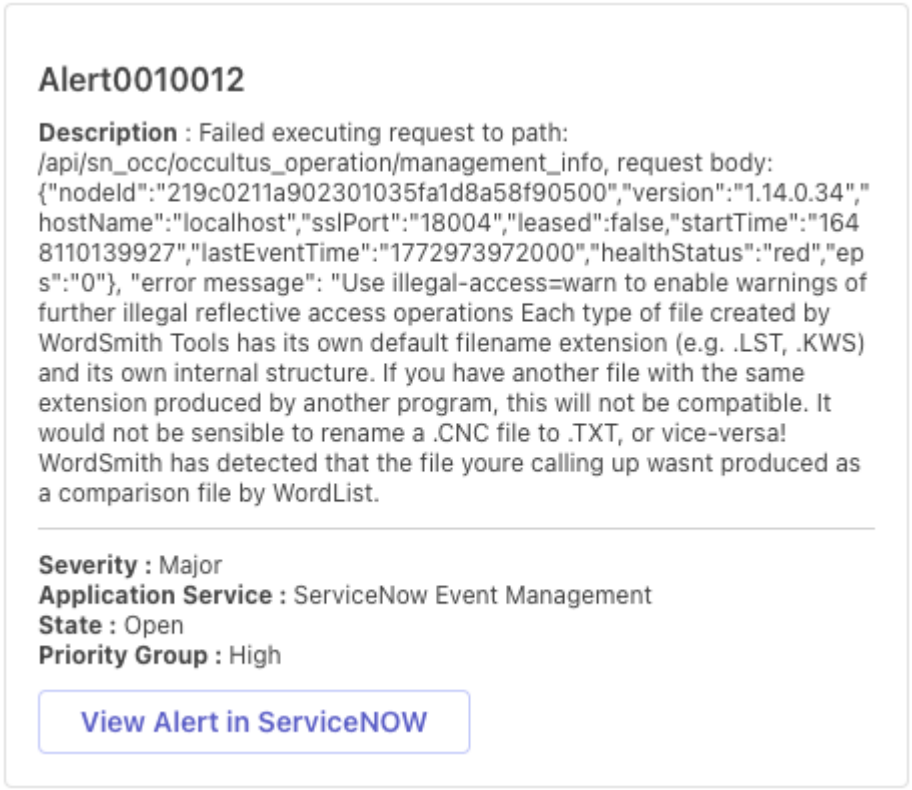
Um die Kanalbenachrichtigung zu unterstützen, muss der Kanal für den Empfang von Health Log Analytics-Benachrichtigungen konfiguriert sein.

Ab Version 33.0.27 – August 2024, Health Log Analytics Verwendet Microsoft Teams Graph-Spoke-Anwendung zum Senden von Benachrichtigungen zu neuen Anomaliewarnungen. Die Anwendung ersetzt Microsoft Teams Spoke-Plugin, das veraltet ist. Wenn Sie eine HLA-Version vor 33.0,27 verwenden, befolgen Sie das Setup-Verfahren in Einrichten Health Log Analytics Warnungsbenachrichtigungen in Kanälen. Andernfalls finden Sie unter Einrichten Health Log Analytics Warnungsbenachrichtigungen in einem Microsoft Teams Kanal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HLA-Warnungsbenachrichtigungen in Microsoft Teams – Beispiel



Einrichten Health Log Analytics Warnungsbenachrichtigungen in Kanälen

Richten Sie Benachrichtigungen für neu ein Health Log Analytics Anomaliewarnungen in entweder einem Slack Oder Microsoft Teams Kanal.

Vorbereitungen

Ab Version 33.0.27 – August 2024, Health Log Analytics Verwendet Microsoft Teams Graph-Spoke-Anwendung zum Senden von Benachrichtigungen für neue Anomaliewarnungen. Die neue Anwendung ersetzt Microsoft Teams Spoke-Plugin, das veraltet ist. Wenn Sie eine HLA-Version vor 33.0,27 verwenden, befolgen Sie das folgende Setup-Verfahren. Andernfalls siehe Einrichten Health Log Analytics Warnungsbenachrichtigungen in einem Microsoft Teams Kanal.

Hinweis: Wenn Sie ein Upgrade von einer früheren Version auf Version 33.0.27 – August 2024 oder höher durchführen, wiederholen Sie das Setup mit dem in beschriebenen Verfahren Einrichten Health Log Analytics Warnungsbenachrichtigungen in einem Microsoft Teams Kanal.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Erstellen Sie eine Webhook-URL für einen Kanal in Slack oder Microsoft Teams.

   Von Health Log Analytics wird der Webhook dazu verwendet, im Kanal über die Warnungen zu informieren.

   Führen Sie das entsprechende Verfahren aus:

   - Erstellen Sie eine Webhook-URL für einen Kanal in Slack
   - Webhook-URL für einen Kanal in Microsoft Teams erstellen

2. Ordnen Sie die Webhook-URL für den Kanal der Serviceinstanz zu, die der Warnung zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Health Log Analytics-Verwaltung** > **Webhook-Benachrichtigung**an.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Webhook für Warnungsbenachrichtigungen – Formular

Feld	Beschreibung
Webhook	Webhook-URL, die Sie für den Kanal erstellt haben.
Aktiv	Wählen Sie diese Option aus, um den Webhook zu aktivieren.
Konfigurationselement	Die Serviceinstanz, die der Warnung zugeordnet ist. Wenn dieses Feld leer ist, verwendet das System die Standardeigenschaft für den Kanal: Default.Slack.webhook.url für Slack Oder default.Teams.Webhook.url für Microsoft Teams.

d. Wählen Sie **Absenden**.

3. Aktivieren Sie die Health Log Analytics-Warnungsverwaltungsregel, um Warnungen an den entsprechenden Kanal zu übermitteln.

a. Navigieren zu **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln**an.

b. Suchen Sie nach der entsprechenden Regel:

- Für Slack: HLA-Warnungen an Slack übermitteln.
- Für Microsoft Teams: HLA-Warnungen an Microsoft Teams übermitteln.

c. Legen Sie den Wert in der Spalte **Aktiv** für die Regel auf `true` fest.

4. **Wahlweise:** Filtern Sie die Warnungen, für die Benachrichtigungen an den Kanal gesendet werden.

a. Wählen Sie in der Tabelle „Warnungsverwaltungsregeln“ die Regel für Ihren Kanal aus.

b. Wählen Sie **Warnungsfilter** aus.

c. Legen Sie im Formular die Bedingungen fest, die erfüllt sein müssen, damit eine Benachrichtigung über die Warnung an den Kanal gesendet wird.

d. Wählen Sie **Aktualisieren**.

Einrichten Health Log Analytics Warnungsbenachrichtigungen in einem Microsoft Teams Kanal

Richten Sie Benachrichtigungen für neu ein Health Log Analytics Anomaliewarnungen in einem Microsoft Teams Kanal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Ab Version 33.0.27 – August 2024, Health Log Analytics Verwendet Microsoft Teams Graph-Spoke-Anwendung zum Senden von Benachrichtigungen zu neuen Anomaliewarnungen. Weitere Informationen finden Sie unter . Wenn Sie eine HLA-Version vor 33.0,27 verwenden, lesen Sie das Setup-Verfahren in Einrichten Health Log Analytics Warnungsbenachrichtigungen in Kanälen.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Installieren Sie die neueste Version von Microsoft Teams Graph-Spoke von ServiceNow Store an.
2. Richten Sie ein Microsoft Teams Graph-Spoke.
   Anweisungen finden Sie unter: .
3. Aktivieren Sie Health Log Analytics Warnungsverwaltungsregel zum Senden von Warnungen an Microsoft Teams Kanal.
   a. Navigieren zu **Ereignismanagement** > **Bedingungen** > **Warnungsverwaltungsregeln**an.
   b. Suchen Sie die entsprechende Regel: HLA-Warnungen an Teams senden.
   c. Legen Sie den Wert in der Spalte **Aktiv** für die Regel auf `true` fest.
4. Ordnen Sie die Serviceinstanz zu Microsoft Teams Kanal.
   a. In **Alle** Navigationsmenü, Typ `sn_occ_Teams_Alert_Notification_config` Und drücken Sie dann die Eingabetaste.
   b. Wählen Sie **Neu**.
   c. Füllen Sie im Formular die Felder aus.

      Hinweis:

      - Sie können die Teams-ID und die Kanal-ID aus dem abrufen Microsoft Teams Kanal.
      - Die **Konfigurationselement** Feld muss der Serviceinstanz entsprechen. Wenn kein CI erforderlich ist, lassen Sie dieses Feld leer. In diesem Fall wird der Datensatz für Warnungen verwendet, wenn kein Datensatz vorhanden ist, der dem CI entspricht.

   d. Wählen Sie **Absenden**.
   e. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4, um zusätzliche Konfigurationen hinzuzufügen.

Speicherplatz für die Protokollaufbewahrung in Health Log Analytics

Das Health Log Analytics-Basissystem bietet normalerweise 1.000 GB Speicherplatz für die Aufbewahrung der Protokollquelle, obwohl die Speicherkapazität je nach Lizenz variieren kann. Die Standardaufbewahrungszeit für Protokolle beträgt drei Tage. Sie können diesen Zeitraum jedoch ändern.

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Wenden Sie sich an Ihren ServiceNow Account Manager oder den ServiceNow Support, um sie zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der von allen Protokollquellen verwendete Speicherplatz 80 Prozent der Gesamtmenge überschreitet, erhalten Sie eine E-Mail-Benachrichtigung. Sie können den Prozentsatz des Standardschwellenwerts ändern, indem Sie ändern `sn_occ.elastic_storage.utilization_limit.percent`Systemeigenschaft in der Tabelle „Systemeigenschaften“.

Automatische Reduzierung der Protokollaufbewahrungstage

Standardmäßig werden Protokolle drei Tage lang gespeichert. Sie können diesen Zeitraum auf 3, 7, 14 oder 30 Tage anpassen. Weitere Informationen finden Sie unter Ändern Sie den Aufbewahrungszeitraum der Protokollquelle in Health Log Analytics.

Wenn der von allen Protokollquellen verwendete Speicherplatz 100 Prozent erreicht, wird die Anzahl der pro Quelle zugewiesenen Aufbewahrungstage automatisch um eine Ebene verringert und Sie erhalten eine E-Mail-Benachrichtigung mit den Details. Der automatische Reduzierungsprozess beginnt mit den Quellen, denen die höchste Anzahl von Aufbewahrungstagen zugewiesen wurde. Beispiel: Für eine Quelle mit 30 Aufbewahrungstagen wird die Anzahl auf 14 reduziert. Wenn die Quelle 14 Aufbewahrungstage hat, wird die Anzahl auf 7 reduziert usw.

Sie können den Schwellenwert für die automatische Reduzierung der Protokollaufbewahrungstage ändern, indem Sie ändern `sn_occ.log_retention.automatic_reduction_utilization_percent`Systemeigenschaft in der Tabelle „Systemeigenschaften“.

Zugehörige Informationen

Ändern Sie den Aufbewahrungszeitraum der Protokollquelle in Health Log Analytics

Ändern Sie den Aufbewahrungszeitraum der Protokollquelle in Health Log Analytics

Ändern Sie den Zeitraum, über den Health Log Analytics Protokolle aus einer bestimmten Quelle aufbewahrt. Sie können die Auswirkungen Ihrer beabsichtigten Änderung auf den Speicher berechnen, um eine fundierte Entscheidung zu treffen.

Vorbereitungen

Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store . Wenden Sie sich an Ihren ServiceNow Account Manager oder den ServiceNow Support, um sie zu aktivieren.

Zum Anzeigen **Aufbewahrung der Protokollquelle** Im Filternavigator:

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Geben Sie den Eigenschaftsnamen ein `sn_occ.activate_log_source_retention`Im Suchfeld.
3. Stellen Sie sicher, dass der Eigenschaftswert auf festgelegt ist **Wahr** .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ist die Aufbewahrungsdauer für Protokolle pro Quelle auf drei Tage festgelegt. Sie können diese Zahl auf 7, 14 oder 30 Tage ändern. Weitere Informationen finden Sie unter Speicherplatz für die Protokollaufbewahrung in Health Log Analytics. Beachten Sie, dass eine längere Protokollaufbewahrung zu einer höheren Speichernutzung führt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Aufbewahrung der Protokollquelle**an.
2. **Wahlweise:** Berechnen Sie, wie sich das Ändern des Aufbewahrungszeitraums für Protokolle aus einer bestimmten Quelle auf den Speicher auswirkt.
   a. Öffnen Sie einen Protokollquelldatensatz.
   b. Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Calculate how retention impacts storage** (Auswirkung der Aufbewahrung auf den Speicher berechnen) aus.
   c. Wählen Sie in der Liste „New retention“ (Neue Aufbewahrung) die vorgeschlagene Anzahl von Aufbewahrungstagen für Protokolle aus dieser Quelle aus.
   d. Wählen Sie **Berechnen** aus.
   Im Feld **Projected storage usage (GB)** (Prognostizierte Speichernutzung (GB)) wird die Speichermenge in GB angezeigt, die die Quelle bei Implementierung der neuen Richtlinie verwenden würde.

   Hinweis: Health Log Analytics basiert die Berechnung der prognostizierten Speichernutzung auf dem Umfang der Protokolldaten, die in der Vergangenheit gestreamt wurden. Die Schätzung kann sich ändern, wenn das Volumen der gestreamten Protokolldaten variiert.

   e. Vergleichen Sie die prognostizierte Nutzung mit der Speichermenge, die für die aktuelle Richtlinie erforderlich ist, die im Feld **Current storage usage (GB)** (Aktuelle Speichernutzung (GB)) angezeigt wird.
   f. Wählen Sie **Abbrechen** aus, um das Dialogfeld zu schließen.
3. Aktualisieren Sie die Protokollaufbewahrungsrichtlinie pro Quelle oder für mehrere Quellen auf einmal.
   - So aktualisieren Sie die Protokollaufbewahrung für eine einzelne Quelle:
     a. Öffnen Sie einen Protokollquelldatensatz.
     b. Wählen Sie aus der Liste „Retention days“ (Aufbewahrungstage) die erforderliche Anzahl von Aufbewahrungstagen für Protokolle aus dieser Quelle aus.
     c. Wählen Sie **Aktualisieren**.
   - So aktualisieren Sie die Protokollaufbewahrung für mehrere Quellen:
     a. Wählen Sie mehrere Protokollquelldatensätze aus.
     b. Wählen Sie in der Auswahlliste „Aktionen für ausgewählte Zeilen“ die Option **Update multiple source retentions** (Mehrere Quellenaufbewahrungen aktualisieren) aus.
     c. Wählen Sie aus der Liste „New retention policy“ (Neue Aufbewahrungsrichtlinie) die erforderliche Anzahl von Aufbewahrungstagen für Protokolle aus den ausgewählten Quellen aus.
     d. Wählen Sie **Aktualisieren**.

   Die aktualisierte Richtlinie wird in bis zu 15 Minuten wirksam.
4. **Wahlweise:** Stellen Sie die standardmäßige Protokollaufbewahrungsrichtlinie pro Quelle oder für alle Protokollquellen wieder her.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- So stellen Sie die Standardrichtlinie für eine einzelne Quelle wieder her:
  a. Öffnen Sie einen Protokollquelldatensatz aus der Tabelle.
  b. Wählen Sie im Abschnitt „Zugehörige Links“ des Datensatzes die Option **Standardwerte wiederherstellen** aus.

  Die Protokollaufbewahrungsrichtlinie für diese Protokollquelle wird auf den Standardwert von drei Tagen zurückgesetzt.
- So stellen Sie die Standardrichtlinie für alle Quellen wieder her:
  a. Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Standardwerte wiederherstellen** aus.
  b. Wählen Sie im Bestätigungsdialogfeld **Fortsetzen** aus.

  Die Protokollaufbewahrungsrichtlinie für alle Protokollquellen wird auf den Standardwert von drei Tagen zurückgesetzt.

Skalierung Health Log Analytics Dient zum Streamen von Protokollen mit einer höheren Rate

Protokolldaten streamen nach Health Log Analytics Skalierbar, stabiler mit Advanced ServiceNow Infrastruktur.

Das neue ServiceNow Architektur nutzt Warteschlangentechnologie in IT Operations Management Cloud-Services für Authentifizierung und Protokollierung. Die Health Log Analytics Die KI-Engine wurde erweitert, um als Reaktion auf eine erhöhte Protokollierung durch Ihre Organisation dynamisch zu skalieren. Health Log Analytics Kann so skaliert werden, dass mehr als 50.000 Ereignisse pro Sekunde (EPS) oder mehr als 10.000 Ereignisse pro Sekunde unterstützt werden Abonnementeinheiten (SUS) .

Sie können zum erweiterten wechseln ServiceNow Infrastruktur durch Senden einer Skalierungsanforderung über die Now Support Katalog. Weitere Informationen finden Sie unter Übermitteln Sie einen Health Log Analytics Anforderung über skalieren Now Support Katalog. Sie können sich auch an wenden ServiceNow Account-Manager zum anfordern der Skalierung. Wenn Ihre Skalierungsanforderung genehmigt wird, ServiceNow Stellt die Anzahl von bereit Elasticsearch Und HLA KI-Engine-Knoten, die zur Unterstützung Ihrer Abonnementeinheiten erforderlich sind.

Übermitteln Sie einen Health Log Analytics Anforderung über skalieren Now Support Katalog

Anforderung Health Log Analytics Skalierung zur Unterstützung von Streaming-Protokollen mit einer höheren Rate.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
In diesem Verfahren wird erläutert, wie Sie eine Skalierungsanforderung über übermitteln Now Support Katalog. Sie können sich auch an wenden ServiceNow Anzufordernder Account-Manager Health Log Analytics Skalierung.

Prozedur

1. An Now Support , Navigieren Sie zu **Alle** > **Servicekatalog**an.
2. Wählen Sie im Dialogfeld „Skalierung anfordern“ die entsprechende Option aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Installieren Sie Health Log Analytics Prime-App aus dem ServiceNow Speichern.

  Wenn die App installiert ist, können die zusätzlichen Services zur Unterstützung Ihrer Anforderung gemeinsam genutzte Ressourcen in anderen Rechenzentren außer denen verwenden, in denen Ihr gehostet wird ServiceNow Instanz. Diese Fähigkeit ermöglicht eine bessere Ressourcenzuteilung zur Unterstützung Ihrer aktuellen und zukünftigen Anforderungen.

  Hinweis: Um zu installieren Health Log Analytics Prime-App, Sie müssen die Nutzungsbedingungen akzeptieren.

- Fordern Sie eine Skala an, ohne zu installieren Health Log Analytics Prime-App.

  Wenn Sie diese Option auswählen, befinden sich die zusätzlichen Ressourcen zur Unterstützung Ihrer Anforderung im selben Rechenzentrum wie Ihre Instanz. Möglicherweise sind bei der Kapazität einige Einschränkungen aufgetreten.

3. Füllen Sie die Felder aus.

Skalierungsfelder anfordern

Feld	Beschreibung
Wählen Sie Instanz aus	Der Name von ServiceNow Instanz.
Anzahl der Abonnementeinheiten	Die Anzahl der Abonnementeinheiten Health Log Analytics Muss unterstützen.

4. Wählen Sie **Absenden**.
   Ihre Skalierungsanforderung wird übermittelt. Wenn es genehmigt wird, ServiceNow Benachrichtigt Sie per E-Mail.

Verbesserung der CMDB mit Hostdaten Health Log Analytics In Protokollen gefunden

Wenn Health Log Analytics Protokolle streamt, werden Hostdaten aus den Protokollereignissen extrahiert. Wenn Hostdaten erkannt werden, die nicht mit den Informationen in übereinstimmen Configuration Management Database (CMDB), Erstellt das System einen Konfigurationselement-Kandidaten (Configuration Item, CI), den Sie basierend auf den Daten in den Protokollen überprüfen können.

Nachdem Sie einen CI-Kandidaten überprüft haben, können Sie ihn entweder der CMDB hinzufügen oder als irrelevant ablehnen. Die Tabelle **Log-Based CI Candidates** (Protokollbasierte CI-Kandidaten) listet alle von Health Log Analytics erstellten CI-Kandidaten sortiert nach Systemaktualisierungszeit auf. In der Spalte **Vorgang** wird die vorgeschlagene Aktion für jeden CI-Kandidaten angezeigt. Sie werden automatisch benachrichtigt, wenn neue CI-Kandidaten für Ihre Berücksichtigung in Frage kommen. Weitere Informationen finden Sie unter Fügen Sie der CMDB in protokollbasierte CIs hinzu Health Log Analytics.

Eine Beschreibung aller zugehörigen Systemeigenschaften finden Sie im Abschnitt „logsourceinfo (CMDB)“ im Artikel HLA System Properties [KB0869842] (HLA-Systemeigenschaften) in der Now Support-Knowledge Base.

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Sie können sie auf der ServiceNow AI Platform mit dem Release Rome Patch 6 (geplant für den 27. Januar 2022) oder höher verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie der CMDB in protokollbasierte CIs hinzu Health Log Analytics

Behalten Sie die bei Configuration Management Database (CMDB) Mit Hostdaten aktualisiert Health Log Analytics In Ihren Protokollen erkannt, indem der Datenbank protokollbasierte Konfigurationselemente (CIs) hinzugefügt werden.

Vorbereitungen

Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store . Sie können es auf verwenden ServiceNow AI Platform Mit Rome Patch 6-Release (Veröffentlichung geplant am 27. Januar 2022) oder höher.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Protokollbasierte CI-Kandidaten**an.
2. Behandeln Sie einen einzelnen CI-Kandidaten oder mehrere CI-Kandidaten auf einmal.

Option	Prozedur
Maßnahmen für einen einzelnen CI-Kandidaten ergreifen	**a.** Wählen Sie einen CI-Kandidatendaten–satz aus und überprüfen Sie die Informa–tionen im Formular. Feldbeschreibungen finden Sie unter Pro-tokollbasierte CI-Kandidatenfelder in Health Log Analytics. **b.** Fügen Sie der CMDB den CI-Kandidaten hinzu oder löschen Sie ihn. ▪ Wenn der CI-Kandidat geeignet ist, fü–gen Sie ihn entweder unverändert der CMDB hinzu oder fügen Sie weitere In–formationen hinzu, bevor Sie ihn der CMDB hinzufügen. ▪ Um den CI-Kandidaten unverändert der CMDB hinzuzufügen, wählen Sie **Add to CMDB** (Zu CMDB hinzufügen) und dann **Fortsetzen** aus. ▪ Um weitere Informationen hinzuzu–fügen, wählen Sie **Edit additional CI fields** (Zusätzliche CI-Felder bear–beiten) aus. Geben Sie Daten ein, die nicht aus den Protokollen extrahiert wurden, z. B. den Namen des Unter–nehmens, das dem CI zugeordnet ist, und wählen Sie dann **Absenden** aus. Das CI wird der CMDB hinzugefügt. In der CMDB-Tabelle für den entspre–chenden Klassentyp ist die Erken–

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Prozedur
	nungsquelle für das neue CI Health Log Analytics. Der CI-Kandidatendatensatz wird automatisch aus der Tabelle mit den protokollbasierten CI-Kandidaten gelöscht. ▪ Wenn der CI-Kandidat irrelevant ist, löschen Sie ihn, indem Sie **Löschen** auswählen.
Maßnahmen für mehrere CI-Kandidaten gleichzeitig ergreifen	**Hinweis:** Mit dieser Option können Sie den ausgewählten CIs keine zusätzlichen Informationen hinzufügen. ○ Fügen Sie der CMDB mehrere CIs hinzu. **a.** Wählen Sie in der Tabelle der protokollbasierten CI-Kandidaten die CI-Kandidaten aus, die Sie der CMDB hinzufügen möchten. **b.** Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen“ unten auf der Seite **Add to CMDB** (Zu CMDB hinzufügen) aus. Die ausgewählten CIs werden der CMDB hinzugefügt. Die CI-Kandidatendatensätze werden automatisch aus der Tabelle mit den protokollbasierten CI-Kandidaten gelöscht. ○ Löschen Sie mehrere CI-Kandidaten. **a.** Wählen Sie in der Tabelle der protokollbasierten CI-Kandidaten die CI-Kandidaten aus, die Sie löschen möchten. **b.** Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen“ unten auf der Seite **Löschen**.

Wird analysiert und aufgelöst Log Analytics Warnungen

Analysieren und lösen Log Analytics Warnt, indem Protokolldaten untersucht und Maßnahmen ergriffen werden, um das zugrunde liegende Problem zu beheben.

Übersicht über Analysieren und Lösen von Log Analytics Warnung

Als Operator sind Sie für die Analyse und Lösung der Warnungen verantwortlich, die auftreten Health Log Analytics Generiert. Wenn HLA Erstellt eine Warnung, überprüfen Sie den Schweregrad der Warnung, das betroffene Konfigurationselement (CI), die Protokolldaten, die der Anomalie zugeordnet sind, und die betroffenen Services. Sie versuchen, die Ursache zu identifizieren, indem Sie die Protokolle untersuchen, die die Anomalie umgeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Express-Liste, Überprüfen Sie die Warnungsdetails, und verwenden Sie Now Assist Um eine eingehende Analyse der Warnungen und potenziellen Lösungen in einer übersichtlichen, visuell lesbaren Sprache zu erhalten. Durch Drilldown in die Warnung können Sie das Problem schnell identifizieren und mit der Lösung fortfahren, bevor es sich auf Ihre Anwender auswirkt.

Mit dem Protokoll-Viewer können Sie die Warnungsprotokolle nach Zeitstempel oder Bereich für weitere Untersuchungen durchsuchen. Sie können die Häufigkeit anomaler Protokolllinien in einem Diagramm visualisieren.

- Starten Sie die Korrektur von Log Analytics Warnung auf der Registerkarte Übersicht

  Beginnen Sie den Korrekturprozess von Log Analytics Warnung aus der Warnung **Übersicht** Registerkarte. Diese Registerkarte enthält Informationen zur Warnung, Protokolldaten, die dem anomalen Verhalten zugeordnet sind, CIs, die der Warnung zugeordnet sind, und Services, die davon betroffen sind.

- Analysieren Sie die Protokolle, die die Anomalie umgeben

  Überprüfen Sie die Protokollzeilen, die die Anomalie umgeben, auf Hinweise zum Status fehlerhafter Systeme. Diese Informationen können Ihnen helfen, die Ursache der Warnung einzugrenzen.

- Verwenden Sie Protokollkorrelatoren, um Beziehungen in Protokolldaten zu identifizieren

  Identifizieren Sie Beziehungen zwischen Warnungen, damit Sie feststellen können, ob eine Warnung Teil eines größeren Problems ist.

- Navigieren Sie zu Express-Liste Und wählen Sie eine Warnung aus der Liste Warnungen aus.

  Verwenden Now Assist Um eine eingehende Analyse der Warnung und potenziellen Lösungen zu erhalten. Durch Drilldown in die Warnung können Sie das Problem schnell identifizieren und mit der Lösung fortfahren.

- Überprüfen Sie die Protokolle auf eine Warnung im Protokoll-Viewer

  Für weitere Untersuchungen können Sie zu navigieren **Protokoll-Viewer** Um die Warnungsprotokolle nach Zeitstempel oder Zeitbereich zu durchsuchen und die Anomaliehäufigkeit innerhalb eines Zeitraums zu visualisieren, um eine umfassende Ansicht der Protokolldaten über einen bestimmten Zeitraum zu erhalten.

- KB-Artikel einer Log Analytics-Warnung hinzufügen

  Wenn Sie eine Warnung gelöst haben Health Log Analytics Generiert, können Sie ihm einen Knowledge Base-artikel (KB) hinzufügen. Geben Sie beispielsweise Informationen an, die anderen helfen könnten, ähnliche Probleme zu lösen.

Anwendungsfälle

Anwendungsfall: Proaktive Überwachung von ServiceNow Instanz in Health Log Analytics– Verwenden Health Log Analytics Zum Erkennen und Lösen neu auftretender Probleme in Ihrer Organisation ServiceNow Instanz, bevor sie sich auf Plattformanwender auswirken.

Starten Sie die Korrektur von Log Analytics Warnung auf der Registerkarte Übersicht

Beginnen Sie den Korrekturprozess von Log Analytics Warnung aus der Warnung **Übersicht** Registerkarte. Diese Registerkarte enthält Informationen zur Warnung, zu den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolldaten, die dem anomalen Verhalten zugeordnet sind, zu CIs, die der Warnung zugeordnet sind, und zu den von ihr betroffenen Services.

Vorbereitungen

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.
3. Wählen Sie die entsprechende Liste in der Unterliste Warnungen aus, und navigieren Sie zur relevanten Warnung oder Gruppe.

   Alle Health Log Analytics-Warnungen weisen in der Spalte **Quelle** den Wert **Log Analytics** auf. Durch den Wert in der Spalte **Gruppe** wird die Art der Log Analytics-Warnung identifiziert. Unter Typen von Health Log Analytics Warnungen finden Sie eine detailliertere Beschreibung der einzelnen Arten von Warnungen oder Gruppen.

   Tipp: Um die Vorschau einer Warnung in der Liste anzuzeigen, klicken Sie auf das zugehörige Info-Symbol ( ).

4. Wählen Sie die Warnungsnummer aus.

   Die Registerkarte **Übersicht** wird angezeigt.

5. Zeigen Sie den Abschnitt der Registerkarte **Übersicht** an, der die Informationen enthält, die Sie benötigen.

   Eine Beschreibung der Abschnitte und Karten finden Sie unter Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics.

   Hinweis: Da in einigen Abschnitten der Registerkarte **Übersicht** nur ein Teil der Informationen zu sehen ist, enthalten viele Abschnitte einen Link, über den Sie andere oder vollständigere Informationen aufrufen können.

6. **Wahlweise:** Führen Sie vordefinierte Korrekturaufgaben aus, um Warnungsprobleme zu lösen.
   a. Wählen Sie Aus **Starten Sie das Playbook** .
   b. Wählen Sie die Registerkarte **Playbook** aus.

      Die **Führen Sie die Korrektur aus** Die Karte zeigt die verfügbaren Korrekturaktionen an.

   c. Wählen Sie die Kachel aus, die der Aktion entspricht, die Sie ausführen möchten.
   Wenn die Aktion abgeschlossen ist, wird sie in angezeigt **Abgeschlossen** Karte.

Analyse der Protokolle um eine Anomalie, um die Ursache der Warnung zu finden

Wenn Health Log Analytics eine Anomalie identifiziert, gibt die Anzeige der die Anomalie umgebenden Protokolle Hinweise auf den Status fehlerhafter Systeme. Diese Informationen können Ihnen helfen, die Ursache einer Warnung einzugrenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beim Anzeigen von Log Analytics Warnung, die **Umgebende Protokolle** Auf der Registerkarte werden die Protokollzeilen aufgelistet, die eine Minute vor und eine Sekunde nach dem Auftreten der Anomalie generiert wurden. Die Protokollzeilen beziehen sich auf die Metrik oder das Muster, die die Warnung ausgelöst hat. Die Liste wird nach der entsprechenden Komponente gefiltert.

Protokolle, die unmittelbar vor der Anomalie generiert wurden, können auf Warnzeichen oder Bedingungen verweisen, die zu dem Problem geführt haben. Durch die Überprüfung dieser Protokolle können Sie die Sequenz der Ereignisse nachverfolgen, die zur Anomalie geführt haben, um zu verstehen, was schief gelaufen ist. Protokolle, die direkt nach der Anomalie erstellt wurden, können Ihnen helfen, die Auswirkungen des Ereignisses zu bewerten, indem analysiert wird, wie das System reagiert hat und ob andere Komponenten betroffen waren. Die Zeitleiste der Protokolle um die Anomalie kann helfen, zu klären, was das Problem verursacht haben könnte, z. B. eine Konfigurationsänderung oder ein Software-Update.

Sie können den Zeitbereich der angezeigten Protokollzeilen ändern, z. B. um Protokolle von mehr als einer Minute vor der Anomalie oder mehr als einer Sekunde danach zu untersuchen.

Hinweis: Protokolle, die die Anomalie umgeben, werden aufbewahrt und sind nach Erstellung der Warnung 30 Tage lang verfügbar. Diese Protokolle werden vom System nicht gelöscht, wenn der globale Aufbewahrungszeitraum der Protokolle abgelaufen ist. Wenn der Aufbewahrungszeitraum abgelaufen ist, sind die umgebenden Protokolle nur auf der Registerkarte **Umgebende Protokolle** und nicht im Protokoll-Viewer verfügbar.

Health Log Analytics Ermöglicht Ihnen das grafische Anzeigen der anomalen Protokolldaten im Protokoll-Viewer, auf den über zugegriffen wird Service Operations-Arbeitsbereich. Der Protokoll-Viewer zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und einer Minute nach an Log Analytics Warnung und listet die zugehörigen Protokollzeilen auf. Er zeigt automatisch die Abfrage im Zusammenhang mit der Anomalie, der ausgewählten Komponente und dem entsprechenden Zeitfilter an. Weitere Informationen finden Sie unter Überprüfen der Protokolle, die mit einer Warnung im Protokoll-Viewer in verbunden sind Health Log Analytics.

Zugehörige Informationen

Analysieren Sie Protokollzeilen, die eine Anomalie in umgeben Health Log Analytics

Analysieren Sie Protokollzeilen um die Anomalie, um die Ursache zu finden

Zeigen Sie die Protokollzeilen um eine Anomalie an, um die Ursache einer Log Analytics-Warnung zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Analysieren Sie Protokollzeilen, die eine Anomalie in umgeben Health Log Analytics.

Identifizierung zugehöriger Warnungen in Protokolldaten mithilfe von Protokollkorrelatoren

Protokollkorrelatoren sind Schlüssel oder Werte in Protokolldaten, die Korrelationen zwischen Warnungen erkennen, um festzustellen, ob eine Warnung Teil eines größeren Problems ist. Beispielsweise könnte ein Protokollkorrelator erkennen, wenn die Schnittstellen-ID eines bestimmten Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Serviceinstanzen auftritt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können zugehörige Warnungen in Ihren Protokolldaten mithilfe von Protokollkorrelatoren identifizieren. Das Basissystem enthält mehrere Protokollkorrelatoren, und Sie können anwenderdefinierte Korrelatoren für eine bestimmte Protokollquelle, alle Protokollquellen oder nur Protokollquellen definieren, die nach der Aktivierung des Korrelators erstellt wurden.

Die meisten Protokollzeilen enthalten einen Metadatenabschnitt plus einen Nachrichtenteil. Einige Protokollzeilen enthalten jedoch nur Nachrichtentext mit Metadaten im Text. Mit den beiden Arten von Protokollkorrelatoren, Freitextkorrelatoren und Protokolleigenschaftskorrelatoren, werden die verschiedenen Teile jedes Protokolls analysiert, damit Beziehungen zwischen Protokolldaten aus mehreren Protokollquellen identifiziert werden können.

Freitextkorrelatoren

Freitextkorrelatoren analysieren den Text im Protokollnachrichtsteil von Protokollzeilen, die einer Anomalie zugeordnet sind. Das System verwendet Freitextkorrelatoren, um Korrelationen zwischen Warnungen zu identifizieren. Sie verwenden Freitextkorrelatoren, um einen Begriff hinzuzufügen, der voraussichtlich in Protokollnachrichten angezeigt wird. Eine gute Wahl ist ein Begriff, der nicht strukturiert ist und andernfalls nicht als Protokolleigenschaft extrahiert würde. Beispiel: „Richtlinien-ID“ oder „Thread-ID“.

Normalerweise fügen Sie auch Freitextkorrelatoren für die Namen von Systemen, Anwendungen und Services hinzu, die für Ihre Umgebung eindeutig sind. Da auf einen solchen Wert von mehreren Quellen, Ebenen, Middleware oder Datenbanken verwiesen werden kann, kann der Freitextkorrelator eine effektive Erkennung korrelierter Warnungen sein. Wenn der Service Ihrer Organisation beispielsweise teatime heißt, können Sie „teatime“ als Freitextkorrelator hinzufügen. Der Korrelator identifiziert Warnungen, die im Zusammenhang miteinander stehen, da sie für Ressourcen generiert wurden, die den Service „TeaTime“ unterstützen, z. B. eine Datenbanksperre oder ein Verbindungsfehler zwischen Komponenten von „TeaTime“.

Protokolleigenschaftskorrelatoren

Protokolleigenschaftskorrelatoren analysieren den Metadatenanteil von Protokollzeilen. Der Korrelator kann beispielsweise den Namen einer Serviceinstanz, die Schnittstellen-ID eines Netzwerkgeräts oder die Anforderungs-ID einer webbasierten Komponente analysieren. Ein Protokolleigenschaftskorrelator kann eine Korrelation markieren, wenn die Schnittstellen-ID eines Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Protokollquellen auftritt. Protokolleigenschaftskorrelatoren sind spezifisch für den Geschäftskontext Ihrer Umgebung.

Sie können den Satz von Protokollquellen angeben, deren Protokolldaten von einem Protokollkorrelator analysiert werden. Die Auswahlmöglichkeiten lauten wie folgt:

- **Nur neue Quellen** : Das System wendet den Protokollkorrelator nur auf Protokollzeilen aus Protokollquellen an, die erstellt wurden, nachdem dieser Protokollkorrelator aktiviert wurde.
- **Alle Quellen** : Das System wendet den Protokollkorrelator auf Protokollzeilen aus allen Protokollquellen an.
- **Angegebene Quelle** : Für einen Protokollkorrelator analysiert das System nur Protokollzeilen aus der von Ihnen angegebenen Protokollquelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einen Protokollkorrelator hinzu, um Beziehungen zwischen Warnungen in Protokolldaten zu identifizieren

Erkennen Sie zugehörige Warnungen in Protokolldaten, indem Sie Protokollkorrelatoren hinzufügen. Das Basissystem enthält mehrere Protokollkorrelatoren, und Sie können anwenderdefinierte Protokollkorrelatoren definieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Informationen zu den Typen und Funktionen von Protokollkorrelatoren finden Sie unter Identifizierung zugehöriger Warnungen in Protokolldaten mithilfe von Protokollkorrelatoren.

Prozedur

1. Verwenden Sie eine der folgenden Methoden, um einen Protokollkorrelator hinzuzufügen.

Option	Prozedur
Fügen Sie einen Protokollkorrelator für eine bestimmte Protokollquelle hinzu	**a.** Navigieren zu **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Protokollkorrelatoren**an. Die Liste der vorhandenen Protokollkorrelatoren wird geöffnet. **b.** Klicken Sie auf den Namen eines Protokollkorrelators. Die Namen werden in der Spalte **Korrelationsindikator** angezeigt. **c.** Klicken Sie auf **Neu**.
Fügen Sie einen Protokollkorrelator hinzu, der entweder für alle Protokollquellen oder nur für die Protokollquellen gilt, die aktiv werden, nachdem Sie diesen Protokollkorrelator definiert haben	**a.** Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**an. **b.** Klicken Sie auf den Namen der Protokollquelle. Die zugehörige Liste Protokollkorrelatoren zeigt die Liste der vorhandenen Protokollkorrelatoren an, die Protokolldaten aus der ausgewählten Protokollquelle analysieren. **c.** Klicken Sie auf der Registerkarte **Log correlators** (Protokollkorrelatoren) auf **Neu**.

2. Füllen Sie das Formular Protokollkorrelator aus.
   Feldbeschreibungen finden Sie unter Formularfelder für Protokollkorrelatoren.
3. Aktivieren Sie **Aktiv**, und klicken Sie dann auf **Absenden**.

Quellen aus einem Protokollkorrelator ausschließen

Verhindern Sie, dass das System Protokollzeilen aus einer bestimmten Quelle analysiert, indem Sie diese Quelle aus dem Protokollkorrelator ausschließen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**an.
2. Öffnen Sie die entsprechende Quelle im Formular „Protokollquellen“.
3. Wählen Sie auf der Registerkarte **Protokollkorrelatoren** die Option für den Protokollkorrelator.
4. Wählen Sie in der Liste „Actions on selected items“ (Aktionen für ausgewählte Elemente) die Option **Exclude from this source** (Aus dieser Quelle ausschließen) aus.

Überprüfen der Protokolle, die mit einer Warnung im Protokoll-Viewer in verbunden sind Health Log Analytics

Die **Protokoll-Viewer** Auf der Registerkarte können Sie die Protokolle für eine Warnung nach Zeitstempel oder Zeitbereich durchsuchen und die Anomaliehäufigkeit innerhalb eines bestimmten Zeitraums visualisieren. Durch das Anpassen der angezeigten Daten und das Anpassen der Zeitfilter können Sie das Framework, in dem die Anomalie aufgetreten ist, besser verstehen und so die Ursache schneller finden.

Der Protokoll-Viewer zeigt alle Daten an, die mit verbunden sind Log Analytics Warnung. Zeigt die Abfrage, die sich auf die Anomalie, die ausgewählte Komponente und den entsprechenden Zeitfilter bezieht. Sie können die angezeigten Daten personalisieren und den Zeitbereich manuell anpassen, ohne die anderen Einstellungen zu beeinträchtigen. Die angewendeten Filter werden in angezeigt **Filter** Bereich. Sie können Filter nach Bedarf hinzufügen oder entfernen, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Die **Protokoll-Viewer** Zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und einer Minute nach an Log Analytics Warnung und listet die zugehörigen Protokolldaten auf. Diese Informationen helfen Ihnen, Trends zu identifizieren, die vor und nach dem Ereignis führen, und bieten Kontext für die Ursachenanalyse.

Während Sie die Protokolle für eine Warnung im analysieren **Protokoll-Viewer** , Sie können die Abfrage ändern, um die Suche zu optimieren, nützliche Suchen zu speichern und für andere freizugeben. Für eine Beschreibung der Informationen, die in angezeigt werden **Protokoll-Viewer** Tabelle, siehe Protokollbetrachter-Tabellenfelder.

Sie können die folgenden Aufgaben auf ausführen **Protokoll-Viewer** :

- Zeigen Sie Protokolldaten für eine Warnung in an Health Log Analytics

  Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

- Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics

  Optimieren Sie die Suchabfrage, um die Ursachen des Problems zu bestimmen, und speichern und nützliche Suchen freigeben zu können.

- Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics

  Verwenden Sie eine gespeicherte Suche. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

- Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics

  Wenden Sie Filter an, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics

  Fügen Sie Spalten in der Tabelle hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Wenn Sie eine wichtige Metrik in den Protokolldaten erkennen, können Sie sie verwenden, um eine neue zu definieren Log Analytics Warnungsregel. Weitere Informationen finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

Zugehörige Informationen

Analyse der Protokolle um eine Anomalie, um die Ursache der Warnung zu finden

Zeigen Sie Protokolldaten für eine Warnung in an Health Log Analytics

Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokolllinien und der zugehörigen Protokolldaten im Protokoll-Viewer an.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Zeigen Sie Protokolldaten für eine Warnung in an Health Log Analytics.

Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics

Definieren, speichern und teilen Sie Suchen nach Protokolldaten, um die Ursachen von Log Analytics-Warnungen zu ermitteln.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics.

Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics

Verwenden Sie eine gespeicherte Suche nach Protokolldaten, um die Ursachen einer Warnung besser zu verstehen. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wenn Sie nicht der Besitzer der gespeicherten Suche sind, speichern Sie die Suche unter einem anderen Namen. Anschließend können Sie Suchwerte aktualisieren, Ihre Änderungen speichern und die Suche für andere freigeben.

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics.

Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics

Wenden Sie Filter auf an **Protokoll-Viewer** Um nur die gewünschten Daten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

> **Wichtig:** Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics.

Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics

Fügen Sie Spalten in hinzu, oder entfernen Sie sie **Protokoll-Viewer** Tabelle, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

> **Wichtig:** Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics.

KB-Artikel einer Log Analytics-Warnung hinzufügen

Fügen Sie Ihren eigenen KB-Artikel (Knowledge Base) einer Warnung hinzu, die von Health Log Analytics generiert wurde. Sie können beispielsweise zusätzliche Informationen angeben, die zur Lösung des zugrunde liegenden Problems beitragen können. Health Log Analytics verwendet Ihr Wissen auch, um ähnliche Warnungen zu verbessern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

> **Wichtig:** Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: KB-Artikel einer Log Analytics-Warnung hinzufügen.

Anwendungsfall: Proaktive Überwachung von ServiceNow Instanz in Health Log Analytics

Verwenden Health Log Analytics Zum Erkennen und Lösen neu auftretender Probleme in Ihrer Organisation ServiceNow Instanz, bevor sie sich negativ auf Anwender auswirken.

Verwenden der ServiceNow-Systemprotokollabrufintegration, um Plattformprobleme automatisch zu erkennen

Ab Version 35.0.26 von Health Log Analytics, Können Sie verwenden ServiceNow-Systemprotokollabrufintegration Um Fehler und Anomalien in Ihrem automatisch zu erkennen ServiceNow Systemprotokolle der Instanz. Als Operator können Sie die generierten Warnungen in anzeigen, verwalten und darauf reagieren Express-Liste . Filtern Sie die Liste, um nur Warnungen für den betroffenen Service anzuzeigen. Verwenden Sie dann Now Assist Um eine eingehende Analyse der Warnungen und potenziellen Lösungen in einer übersichtlichen, visuell lesbaren Sprache zu erhalten. Dieses KI-gesteuerte Tool demonstriert ein tiefes Verständnis des Glide-Systems und bietet umsetzbare Einblicke.

Wird Kombiniert HLA Anomalieerkennung von mit Now Assist GenAI-Fähigkeiten von bieten ein umfassendes Toolkit für die effektivere Identifizierung und Lösung von Plattformsystemproblemen. Diese Zusammenarbeit ermöglicht Health Log Analytics Um zu verhindern, dass Systemprobleme Ihre Plattformanwender beeinträchtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit MID-Server Und Systemprotokolle rufen Dateneingaben zusammen ab, um Ihre Instanz zu überwachen

Sie können auch Unterbrechungen Ihres voraus bleiben ServiceNow-Umgebung mithilfe von MID-Server-Dateneingabe Und ServiceNow-Systemprotokolle – Dateneingabe abrufen Zusammen.

Als Administrator wählen Sie einen aus MID-Server Von MID Servers Liste. Wählen Sie unter zugehörige Links die Option aus **Erstellen Sie die MID-Server-Dateneingabe mit HLA** Dient zum Erstellen einer Dateneingabe, die für die ausgewählte spezifisch ist MID-Server. Aktivieren Sie dann die Dateneingabe „Systemprotokolle abrufen“, und konfigurieren Sie sie für die Erfassung von ServiceNow Systemprotokolle der Instanz.

Als Operator navigieren Sie zu Express-Liste Und wählen Sie eine Warnung aus der Liste Warnungen aus. Überprüfen Sie die Warnungsdetails, einschließlich Dauer und betroffene Services, und analysieren Sie die Protokolle, die die Anomalie umgeben. Verwenden Now Assist Um eine eingehende Analyse der Warnungen und potenziellen Lösungen in einer übersichtlichen, visuell lesbaren Sprache zu erhalten. Bei Bedarf können Sie für weitere Untersuchungen zu navigieren Protokoll-Viewer Für eine visuelle Präsentation der Systemprotokolle. Wählen Sie in der Dropdown-Liste „Komponenten“ die Option Systemprotokollabruf aus, um alle Fehler anzuzeigen, die in aufgetreten sind ServiceNow Instanz. Sie können die Visualisierung mithilfe von Filtern anpassen.

Durch Drilldown in die Warnung und MID-Server Protokolle können Sie das Problem schnell identifizieren und beheben, bevor es Ihre Plattformanwender betrifft.

Steuerung Health Log Analytics Warnungserstellung, Priorisierung und Anomalieerkennung

Beeinflussen Sie wie Health Log Analytics Generiert und priorisiert Warnungen und identifiziert Anomalien. Verwenden Sie Warnungsfilter, um Rauschen durch unwichtige Probleme zu reduzieren.

Übersicht über Wirkt sich auf die Generierung, Priorisierung und Anomalieerkennung von Warnungen aus

Erkunden Sie, wie Sie die Warnungserstellung und die Anomalieerkennung in beeinflussen können Health Log Analytics. Sie können Regeln erstellen und ändern, um Warnungen für bestimmte Metriken zu generieren, um sicherzustellen, dass Sie über wichtige Probleme informiert sind. Sie können Warnungen auch verschiedene Bedeutungsebenen zuweisen, was hilft Health Log Analytics Priorisieren Sie sie basierend auf ihrer Relevanz. Darüber hinaus können Sie die Anomalieerkennung beeinflussen, indem Sie die Stichwörter verwalten, die Health Log Analytics Sucht in Ihren Protokolldaten nach und verwenden Sie erweiterte Protokollwarnungsfilter, um Rauschen zu reduzieren.

- Verwenden Sie Warnungsregeln, um zu steuern, wann Health Log Analytics Generiert Warnungen

  Verwalten Sie zu generierende Warnungsregeln Log Analytics Warnungen für angegebene Metriken.

- Weisen Sie einer Warnung in eine höhere oder niedrigere Bedeutung zu Health Log Analytics

  Weisen Sie einer Warnung eine höhere oder niedrigere Bedeutung zu, um die Warnungen zu priorisieren, die diese haben Health Log Analytics Generiert.

- Beeinflussen Sie die Anomalieerkennung in Health Log Analytics Mit lexikalischen Stichwörtern

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beeinflussen Sie wie Health Log Analytics Sucht nach Anomalien, indem Stichwörter verwaltet werden, nach denen in Ihren Protokolldaten gesucht wird.

- Reduzierung von Rauschen durch Hinzufügen erweiterter Protokollwarnungsfilter in Health Log Analytics

  Verwenden Sie erweiterte Protokollwarnungsfilter, um Rauschen durch zu reduzieren Health Log Analytics Verwerfen Sie Warnungen, die nicht auf ein schwerwiegendes Problem hinweisen.

Verwenden Sie Warnungsregeln, um zu steuern, wann Health Log Analytics Generiert Warnungen

Mit Warnungsregeln können Sie Schwellenwerte und Bedingungen festlegen, die bestimmen, wann Health Log Analytics Löst eine Warnung aus. Wenn die Bedingungen einer Warnungsregel erfüllt sind, generiert das System einen Log Analytics Warnung. Sie können Warnungsregeln hinzufügen, ändern oder löschen, um sie zu erstellen Log Analytics Warnungen für eine angegebene Metrik.

In Health Log Analytics Mit Warnungsregeln können Sie angeben, wann Warnungen ausgelöst werden. Mit diesen Regeln stellen Sie sicher, dass eine Warnung generiert wird, wenn bestimmte Bedingungen erfüllt sind, wodurch eine proaktive Überwachung und Behebung neu auftretender Probleme ermöglicht wird. Sie können Warnungsregeln erstellen, wenn Protokolldaten angezeigt werden, die eine Warnung auslösen sollen, und von Ihnen definierte Warnungsregeln ändern oder löschen.

Sie können die folgenden Aufgaben im Zusammenhang mit Warnungsregeln ausführen:

- Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics

  Fügen Sie ein hinzu Log Analytics Warnungsregel, wenn Protokolldaten gefunden werden, die eine Warnung generieren sollen.

- Ändern Sie A Log Analytics Warnungsregel in Health Log Analytics

  Bearbeiten Sie ein Log Analytics Warnungsregel, die Sie definiert haben.

- Löschen Sie einen Log Analytics Warnungsregel in Health Log Analytics

  Löschen Sie einen Log Analytics Warnungsregel, die Sie definiert haben, wenn sie nicht mehr benötigt wird.

Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics

Definieren Sie eine Log Analytics-Warnungsregel, wenn Protokolldaten angezeigt werden, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für eine angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

Ändern Sie A Log Analytics Warnungsregel in Health Log Analytics

Sie können ändern Log Analytics Warnungsregel, die Sie definiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Ändern Sie A Log Analytics Warnungsregel in Health Log Analytics.

Löschen Sie einen Log Analytics Warnungsregel in Health Log Analytics

Löschen Sie eine definierte Log Analytics-Warnungsregel, wenn sie nicht mehr erforderlich ist.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Löschen Sie einen Log Analytics Warnungsregel in Health Log Analytics.

Weisen Sie einer Warnung in eine höhere oder niedrigere Bedeutung zu Health Log Analytics

Bezeichnen Sie eine Warnung in Health Log Analytics Als aussagekräftig oder unbedeutend, oder stellen Sie die normale Wichtigkeit der Metrik wieder her, die an der Generierung beteiligt ist.

Wenn Sie einer Warnung eine höhere oder niedrigere Bedeutung zuweisen, können Sie die Warnungen priorisieren Health Log Analytics Generiert. Hier sind einige häufige Anwendungsfälle zum Anpassen der Wichtigkeit einer Warnung:

- Kennzeichnung von Warnungen als aussagekräftig: Sie können eine signifikante Warnung wahrscheinlicher machen, dass sie in einen eingeschlossen wird Log Analytics Gruppieren Sie, wenn sich die zugehörige Metrik anomal verhält. Dadurch wird sichergestellt, dass wichtige Warnungen angemessene Aufmerksamkeit erhalten.
- Störende Warnungen stummschalten: Sie können Warnungen für unbedeutende Probleme stummschalten, um Rauschen zu reduzieren und zu vermeiden, dass sie von Warnungen bei geringfügigen Problemen überfordert werden. Dadurch können Sie sich auf kritischere Warnungen konzentrieren. Sie können eine Liste der stummgeschalteten Metriken anzeigen, um sicherzustellen, dass Sie Metriken kennen, die keine Warnungen mehr generieren.
- Empfindlichkeit für bestimmte Anomalien reduzieren: Sie können die Empfindlichkeit der Anomalieerkennung auf eine bestimmte Anomalie reduzieren. Dies kann Ihnen helfen, sich auf wichtigere Anomalien zu konzentrieren.
- Normale Bedeutung wiederherstellen: Wenn Sie eine Warnung zuvor als signifikant markiert, stummgeschaltet oder die Empfindlichkeit für bestimmte Anomalien verringert haben, können Sie die zugehörige Metrik auf ihre normale Bedeutung zurücksetzen. Dies ist nützlich, wenn Sie die Warnung nicht mehr speziell behandeln möchten.

Sie können die Wichtigkeit einer Warnung anpassen oder die Empfindlichkeit auf bestimmte Anomalien reduzieren:

- Markieren Sie eine Warnung in als signifikant Health Log Analytics

  Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

- Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten. Zeigen Sie die Liste der Metriken an, die stummgeschaltet wurden Und generieren keine Warnungen mehr.

- Verringern Sie die Empfindlichkeit gegenüber ähnlichen Anomalien in Health Log Analytics

  Verringern Sie bei der Health Log Analytics-Anomalie-Erkennung die Sensitivität gegenüber Anomalien wie denjenigen, durch die die aktuelle Log Analytics-Warnung ausgelöst wurde.

- Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics

  Stellen Sie die normale Signifikanz der Metrik wieder her, die an der Generierung einer Log Analytics-Warnung beteiligt ist.

Detaillierte Informationen zu Warnungsmetriken finden Sie unter Wie Health Log Analytics Warnungen generiert.

Markieren Sie eine Warnung in als signifikant Health Log Analytics

Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Markieren Sie eine Warnung in als signifikant Health Log Analytics.

Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics

Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics.

Zeigen Sie die Liste der stummgeschalteten Metriken in an Health Log Analytics

Zeigen Sie die Liste der Metriken an, die stummgeschaltet wurden, damit sie keine Warnungen mehr generieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Stummgeschaltete Metriken**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stummgeschaltete Metriken

Feld	Beschreibung
Serviceinstanz	Serviceinstanz, in der die stummgeschaltete Warnung angezeigt wird, der die Metrik zugeordnet ist.
Komponente	Logische Komponente von Service Instanz , die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Mustertext	Text für die Metrik, die der stummgeschalteten Warnung zugeordnet ist.
Metrik	Protokolltext oder -schlüssel, der einen Zähler- oder Anzeigewert in den Daten darstellt. Zum Beispiel Muster, Rohmetriken, Stichwort, Schweregrad, alle Event-Metriken
Erstellt	Datum und Uhrzeit, zu der die Metrik der Liste hinzugefügt wurde.

Zugehörige Informationen

Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics

Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics

Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics

Wenn eine stummgeschaltete oder als signifikant markierte Warnung nicht mehr besonders behandelt werden soll, können Sie die normale Relevanz der Metrik wiederherstellen, die an der Generierung der Warnung beteiligt ist.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release wird die **Operator-Arbeitsbereich** Ist veraltet und durch ersetzt Service Operations-Arbeitsbereich. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in Service Operations-Arbeitsbereich Für ITOM-Dokumentation: Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics.

Beeinflussen Sie die Anomalieerkennung in Health Log Analytics Mit lexikalischen Stichwörtern

Beeinflussen Sie wie Health Log Analytics Sucht nach Anomalien, indem Stichwörter verwaltet werden, nach denen in Ihren Protokolldaten gesucht wird. Wenn Text in Protokolldaten für eine Quelle mit einem lexikalischen Stichwort übereinstimmt, das einen angegebenen Schwellenwert überschreitet, identifiziert das System eine Anomalie und generiert eine Warnung.

Health Log Analytics durchsucht Ihre Protokolle nach Wörtern, die auf wichtige Probleme hinweisen können. Lexikalische Stichwörter wie Signalbedingungen „abgestürzt“ oder „fehlgeschlagen“, die möglicherweise Aufmerksamkeit erfordern. Die Anwendung legt einen Schwellenwert für jedes lexikalische Stichwort basierend auf dem Muster und der Häufigkeit des normalen Vorkommens in Ihren Protokollen fest.

Wenn Health Log Analytics Scannt Ihre Protokolle und identifiziert alle Vorkommen des Stichworts. Wenn die Häufigkeit eines lexikalischen Stichworts in den Protokolldaten für eine Quelle den angegebenen Schwellenwert überschreitet, identifiziert das System eine Anomalie und generiert eine Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics Enthält viele standardmäßige globale Stichwörter. Sie können diese globalen Stichwörter oder Ausdrücke hinzufügen, bearbeiten und löschen, die für alle Quelltypen gelten.

Hinweis: Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Konfigurieren Sie Quelltypfähigkeiten in Health Log Analytics.

Sie können lexikalische Stichwörter wie folgt verwalten:

- Fügen Sie lexikalische Stichwörter in hinzu, bearbeiten oder löschen Sie sie Health Log Analytics

  Fügen Sie globale Stichwörter oder Ausdrücke hinzu, bearbeiten und löschen Sie sie.

- Zeigen Sie die lexikalischen Stichwörter an, die Warnungen in generieren Health Log Analytics

  Zeigen Sie die Liste der lexikalischen Stichwörter an, die auf wichtige Probleme in Protokolleinträgen hinweisen können. Standardmäßig werden in der Tabelle nur globale Stichwörter aufgelistet.

Fügen Sie lexikalische Stichwörter in hinzu, bearbeiten oder löschen Sie sie Health Log Analytics

Verwalten Sie die Stichwörter, nach denen Health Log Analytics in Ihren Protokolldaten sucht.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
In den Protokolldaten werden Begriffe wie „Crash“ oder „Failed“ als *lexikalische Stichwörter* bezeichnet, da sie auf Probleme hinweisen, die der Aufmerksamkeit bedürfen. Wenn Text in Protokolldaten für eine Quelle mit einem lexikalischen Stichwort übereinstimmt, das einen angegebenen Schwellenwert überschreitet, identifiziert das System eine Anomalie und generiert eine Warnung.

Wichtig: Ein lexikalisches Stichwort unterscheidet sich von einem *Schlüssel* in einem Schlüssel:Wert-Paar in einer Protokollzeile. Zum Beispiel ist `Hostname` ein Schlüssel, der einen Wert annimmt: den Namen oder die IP-Adresse des Hosts. Im Gegensatz dazu ist ein Stichwort wie `Failed` selbst wichtig und nimmt keinen Wert an.

Die Anwendung enthält viele standardmäßige globale Stichwörter. Sie können globale Stichwörter oder Ausdrücke hinzufügen, bearbeiten und löschen. Diese Stichwörter gelten für alle Quelltypen.

Hinweis: Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Konfigurieren Sie Quelltypfähigkeiten in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Lexikalische Stichwörter**an.
   Standardmäßig werden in der Tabelle „Lexikalische Stichwörter“ nur globale Stichwörter aufgelistet.
2. **Wahlweise:** Fügen Sie ein globales Stichwort hinzu.
   a. Wählen Sie **Neu**.
   b. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Lexikalische Stichwörter“

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für das Stichwort
Regulärer Ausdruck	Regulärer Ausdruck („Regex“), mit dem Übereinstimmungen definiert werden.
Exact match (Genaue Übereinstimmung)	Option, damit Health Log Analytics dem genauen regulären Ausdruck entspricht. Beispiel: „NullPointerException“ würde in einer Nachricht nicht mit dem regulären Ausdruck „exception“ übereinstimmen. Dieses Feld wird automatisch auf **True** gesetzt.
Groß-/Kleinschreibung beachten	Option, damit Health Log Analytics nach einer Übereinstimmung des regulären Ausdrucks sucht, bei der die Groß-/Kleinschreibung übereinstimmt. Dieses Feld wird automatisch auf **False** gesetzt.
Analyseumfang	Bereich von Quelltypen, in denen Health Log Analytics nach dem Stichwort in den Protokolldaten sucht: Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Alle Quelltypen** ▪ **Angegebener Quelltyp**
Excluded source types (Ausgeschlossene Quelltypen)	Quelltypen, denen das Stichwort nicht zugeordnet ist. Health Log Analytics sucht in den Protokolldaten dieser Quelltypen nicht nach dem Stichwort.

c. Wählen Sie **Absenden** aus.

3. **Wahlweise:** Bearbeiten Sie ein globales Stichwort.
   a. Klicken Sie in der Liste auf das Stichwort, das Sie bearbeiten möchten.
   b. Bearbeiten Sie im Formular die relevanten Felder.
   c. Wählen Sie **Aktualisieren**.
4. **Wahlweise:** Löschen Sie eines oder mehrere globale Stichwörter.
   a. Markieren Sie die Zeile des angegebenen Stichworts, das Sie löschen möchten.
   b. Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen“ unten auf der Seite **Löschen**.
   c. Wählen Sie **OK** aus.

Zugehörige Informationen

Zeigen Sie die lexikalischen Stichwörter an, die Warnungen in generieren Health Log Analytics

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die lexikalischen Stichwörter an, die Warnungen in generieren Health Log Analytics

Zeigen Sie die Liste der lexikalischen Stichwörter an, die auf wichtige Probleme in Protokolleinträgen hinweisen können.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Lexikalische Stichwörter**an.
Die Tabelle „Lexikalische Stichwörter“ wird angezeigt. Standardmäßig werden in der Tabelle nur globale Stichwörter aufgelistet.

Weitere Informationen über das Hinzufügen, Bearbeiten oder Löschen globaler Stichwörter finden Sie unter Fügen Sie lexikalische Stichwörter in hinzu, bearbeiten oder löschen Sie sie Health Log Analytics.

Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Konfigurieren Sie Quelltypfähigkeiten in Health Log Analytics.

Reduzierung von Rauschen durch Hinzufügen erweiterter Protokollwarnungsfilter in Health Log Analytics

Verwenden Sie erweiterte Protokollwarnungsfilter, um zu bestimmen, ob eine Warnung zugelassen oder verworfen werden soll. Diese Filter reduzieren das Rauschen, indem Warnungen abgelegt werden, die nicht auf ein signifikantes Problem hinweisen.

Sie können erweiterte Protokollwarnungsfilter hinzufügen, um Warnungen für Ihre definierten Bedingungen zu scannen. Sie können beispielsweise einen Filter definieren, der Warnungen aus bestimmten Protokollquellen oder Warnungen für Anomalien abgibt, die den angegebenen Schwellenwert nicht überschreiten.

Einige Beispiele für Aktionen, die mit erweiterten Filtern möglich sind:

- Warnung nur bei Anomalien, die auf mehreren Hosts auftreten.
- Keine Warnung bei Anomalien, die außerhalb der Arbeitszeit auftreten.
- Warnen Sie nicht, wenn die Anomalie den angegebenen Schwellenwert nicht überschreitet.
- Warnung nur bei Anomalien, die Teil einer Korrelation sind.

Sie können erweiterte Protokollwarnungsfilter wie folgt verwalten:

- Erweiterte Protokollwarnungsfilter erstellen

  Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren.

- Setzen Sie das Ändern des Filters fort, indem Sie den Filterdatensatz aus dem erneut öffnen Filterliste . Sie können den Filter dann bearbeiten, testen, veröffentlichen und aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere technische Informationen zu Protokollwarnungsfiltern finden Sie unter Erweiterte Protokollwarnungsfilterung [KB0863538] artikel in Now Support Knowledge Base.

Erweiterte Protokollwarnungsfilter erstellen

Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren.

Vorbereitungen

Die Funktionen „Disable Alert Rule Engine“ (Warnungsregel-Engine deaktivieren) und „Disable Detection Rule Engine“ (Erkennungsregel-Engine deaktivieren) müssen sich im Status AUS befinden. Sie legen die Werte fest, indem Sie zu navigieren **Health Log Analytics** > **Verwaltung von Integritätsvorhersagen für KI-Vorgänge** > **Features**an.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

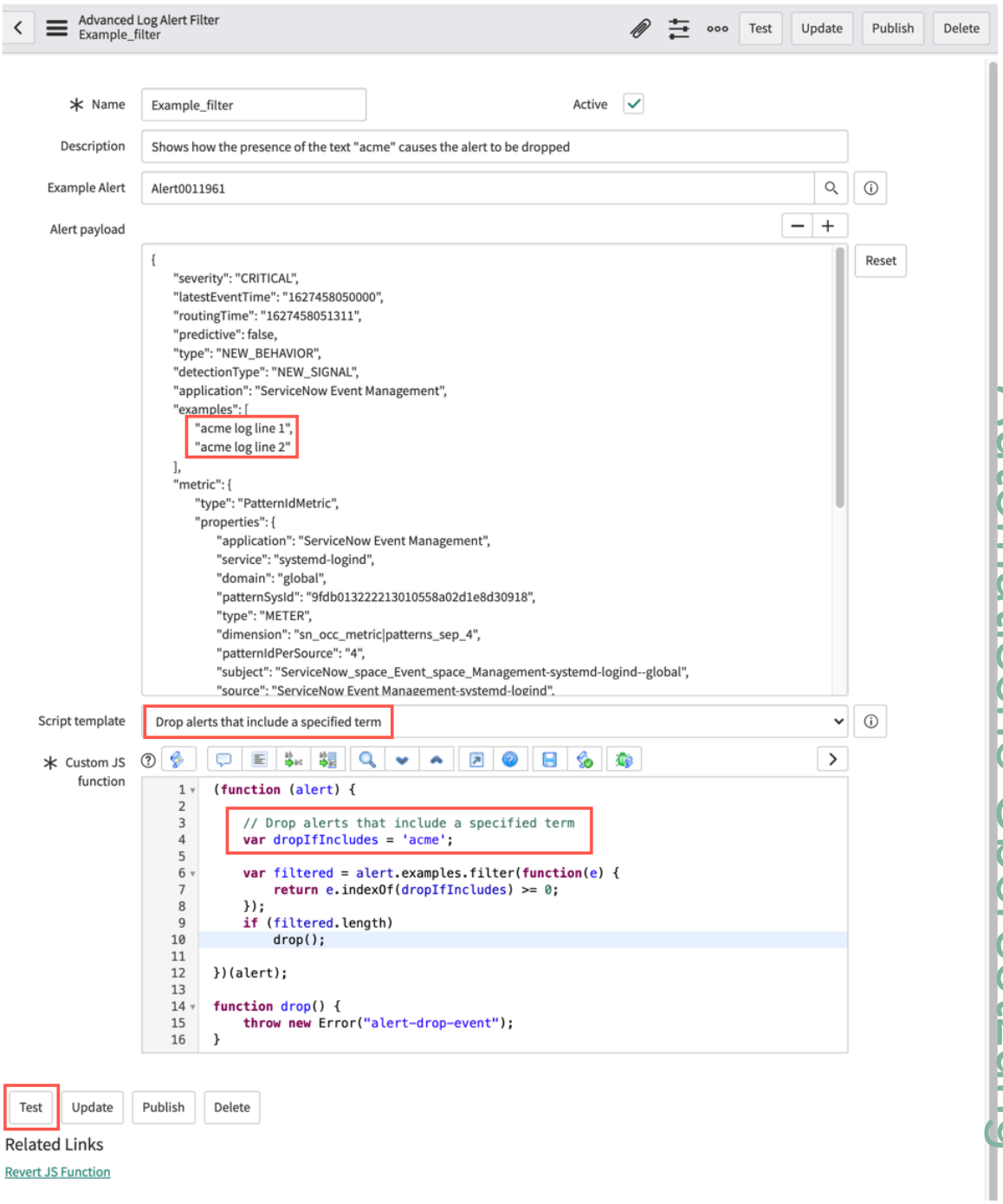
1. Navigieren zu **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Erweiterter Protokollwarnungsfilter**an.
2. Wählen Sie **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden Namen für den Filter an.
4. **Wahlweise:** Geben Sie eine Beschreibung für den Betrieb des Filters ein.
5. Wählen Sie im Feld **Skriptvorlage** das Skript aus, das Ihrer beabsichtigten Logik am ehesten entspricht. Die Vorlage kann als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen.
   Nachdem Sie eine Vorlage ausgewählt haben, wird das Textfeld Benutzerdefinierte JS-Funktionen mit der entsprechenden JavaScript-Funktion ausgefüllt. Die JavaScript-Funktion wendet den Filter auf die Nutzlastdaten der Warnung an und lässt die Warnung entweder zu oder fallen. Die Warnungsnutzlast besteht aus dem Text und den Metadaten für die Art der Warnung, die der Filter analysiert.
6. Speichern Sie den Datensatz, indem Sie **Absenden** auswählen.
   Um weiterhin die Filter ändern zu können, müssen Sie den Datensatz aus der Filterliste wieder öffnen. Sie können den Filter dann bearbeiten, testen, veröffentlichen und aktivieren.
7. Bearbeiten Sie den Standardtext der **Warnungsnutzlast**, um die beabsichtigte Logik zu testen.

   Um Ihre Änderungen zu entfernen und das Textfeld „Warnungsnutzlast“ wiederherzustellen, klicken Sie auf **Zurücksetzen**.

   Um es Ihnen leichter zu machen, bietet Health Log Analytics Beispielwarnungen mit vorkonfigurierten Nutzlasten. Wählen Sie eine Beispielwarnung im Feld **Beispielwarnung** aus, um die Nutzlast im Textfeld „Warnungsnutzlast“ anzuzeigen.
8. **Wahlweise:** Speichern Sie die aktuellen Werte des Filters ohne Tests, indem Sie **Aktualisieren** auswählen.
9. Wenn Ihr Inhalt für die Warnungsnutzlast und Ihre JavaScript-Funktion abgeschlossen sind, wählen Sie **Test**.
   Um den Warnungsvorgang zu simulieren, speichert das System die Filterwerte, wendet den Filter auf den Text der **Warnungsnutzlast** an und zeigt dann eines der folgenden Ergebnisse an:
   - Warnung wird verworfen.
   - Warnung ist zulässig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript testen, um festzustellen, ob die Warnung zugelassen oder verworfen wird



Automatische Übersetzung

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

10. Wiederholen Sie den Vorgang zum Aktualisieren der Warnungsnutzlast und zum Testen der JavaScript-Funktion so oft wie erforderlich.
11. Wenn Sie mit dem Filter zufrieden sind, speichern Sie seine Werte, und bestimmen Sie, ob er auf den Protokollstream angewendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Werte zu speichern und den Filter auf den Protokollstream anzuwenden, stellen Sie sicher, dass das Kontrollkästchen **Aktiv** aktiviert ist, und wählen Sie **Veröffentlichen**.
- Um den Filter zu speichern, ohne ihn auf den Protokollstream anzuwenden, deaktivieren Sie das Kontrollkästchen **Aktiv** und wählen **Veröffentlichen**.

Hinweis: Wenn Sie einen veröffentlichten Filter bearbeiten, müssen Sie den geänderten Filter veröffentlichen, um ihn auf den Protokollstream anzuwenden.

Ergebnis

Die Werte des aktiven Filters werden gespeichert. Wenn Sie die Option „Aktiv“ wählen, wird der Filter auf den Protokollstream angewendet.

Analytics und Reporting in Health Log Analytics

Erhalten Sie wertvolle Einblicke in die Anzahl der IT-Probleme, die vorhergesagt wurden, bevor Ihre Anwender betroffen waren, und die Einsparungen für Ihr Unternehmen durch Analytics und Reporting in Health Log Analytics.

Lösungen für Performance Analytics and Reporting für Health Log Analytics

Platform Analytics-Lösungen enthalten vorpaketierte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen ServiceNow AI Platform-Produkten. Dies Lösung für Performance Analytics and Reporting Bietet wertvolle Einblicke in die Anzahl der IT-Probleme Health Log Analytics Vorhergesagt, bevor Ihre Anwender betroffen waren, und das Geld, das Ihr Unternehmen durch die Verhinderung kritischer Ausfälle gespart hat.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform-Administrator (admin): Installiert und aktiviert diese Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Aktivieren Sie Lösung für Performance Analytics and Reporting Für Health Log Analytics

Aktivieren Sie das Inhaltspaket ServiceNow Store Anwendung für Lösung für Performance Analytics and Reporting.

Vorbereitungen

Aktivieren Sie die vollständige Abonnementversion von Performance Analytics auf der Instanz, auf der Sie diese Lösung für Performance Analytics and Reporting aktivieren. Sie können Performance Analytics in einer Instanz außerhalb der Produktion aktivieren, ohne ein Abonnement zu erwerben. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**an.
2. Suchen Sie nach Health Log Analytics Und überprüfen Sie, ob Sie über die erforderlichen gültigen Berechtigungen verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie benötigen ein HI-Konto und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen. HI-Konto und Instanz müssen zum selben Unternehmen gehören. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.

3. Suchen Sie nach Health Log Analytics (sn.occ).
4. Installieren Sie die Anwendung.

   Wenn Sie diese Anwendung installieren, aktivieren Sie auch das Plugin „Performance Analytics - Premium“ (com.snc.pa.premium).

   Hinweis: Für dieses Plugin wird eine zusätzliche Gebühr fällig.

Konfigurieren Sie Lösung für Performance Analytics and Reporting Für Health Log Analytics

Führen Sie Diagnosen aus, überprüfen Sie Komponenten, passen Sie sie an, und beginnen Sie mit der Datenerfassung.

Vorbereitungen

Ein ServiceNow AI Platform-Administrator muss die Plugins für Inhaltspakete oder die ServiceNow Store-Anwendung für diese Lösung für Performance Analytics and Reporting installiert haben.

Erforderliche Rolle: pa_admin

Prozedur

1. Führen Sie Diagnosen für alle Datensätze aus.

   Diese Diagnosen können viele Diskrepanzen zwischen der Konfiguration Ihrer Platform Analytics-Lösungen und Ihren Tabellen erkennen.

2. Navigieren zu **Alle** > **Performance Analytics** > **Administrationskonsole**an.
3. Überprüfen Sie den Namen des Dashboards, das mit installiert wurde Lösung für Performance Analytics and Reporting:
   Health Log AnalyticsÜbersicht Dashboard.
4. Öffnen Sie die Registerkarte **Indikatorquellen**.
5. Für jedes Dashboard, das in dieser Platform Analytics-Lösung enthalten ist:

   a. Filtern Sie die Indikatorquellen nach dem Dashboardnamen.

   b. Überprüfen Sie die Faktentabelle, die Bedingungen und die Häufigkeit der Indikatorquellen im Vergleich zur Datenstruktur auf Ihrer eigenen Instanz.

   Wichtig: Achten Sie besonders auf Zeitstempelfelder wie „Gelöst“ oder „Erstellt“, auf die im Feld **Bedingungen** verwiesen wird. Möglicherweise müssen Sie andere Zeitstempelfelder verwenden.

   c. Öffnen Sie bei Bedarf eine Indikatorquelle, und nehmen Sie Korrekturen vor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wenn Sie einen Indikatorquelldatensatz bearbeiten, wechseln Sie zur zugehörigen Liste „Indikatoren“, und überprüfen Sie das Feld Bedingungen für jeden Indikator.
Das Ändern der Indikatorquelle kann sich auch auf die zusätzlichen Bedingungen für die einzelnen Indikatoren auswirken.

6. Wenn Sie die Zeitfeldstempel in einer Indikatorquelle geändert haben, ändern Sie alle zugehörigen Performance Analytics-Skripts.
7. Öffnen Sie **Aufgliederungsquellen** Registerkarte.
8. Für jedes Dashboard, das in dieser Platform Analytics-Lösung enthalten ist:
   a. Filtern Sie die Aufgliederungsquellen nach dem Dashboardnamen.
   b. Überprüfen Sie die unter Aufgliederungsquellen überprüfen beschriebenen Bedingungen der Aufgliederungsquelle.
9. Navigieren zu **Alle** > **Performance Analytics** > **Aufträge**an.
10. Richten Sie den Verlaufsauftrag dafür ein, und führen Sie ihn aus Lösung für Performance Analytics and Reporting, *[PA HLA] Historic Data Collection*.
11. Bearbeiten und aktivieren Sie die geplante Datensammlungsaufgabe dafür Lösung für Performance Analytics and Reporting, *[PA HLA] Historic Data Collection*.

Dashboard „Health Log Analytics Overview“ (Health Log Analytics - Übersicht)

Im Dashboard „Health Log Analytics Overview“ (Health Log Analytics - Übersicht) wird Performance Analytics verwendet, um einen Trend aus Verlaufsdaten sowie regelmäßige Berichte bereitzustellen.

Ab dem Xanadu-Release wird die Health Log AnalyticsÜbersicht Dashboard wurde veraltet und durch das Dashboard „HLA-Betrieb“ ersetzt. Das Dashboard „HLA-Betrieb“ verwendet Performance Analytics, mit dem Sie Protokolldaten, Warnungen und Fehlerquoteninformationen in überwachen können Service Operations-Arbeitsbereich Und behandeln Probleme, wenn sie im System auftreten. Weitere Informationen finden Sie unter Dashboard „HLA-Betrieb“.

Health Log Analytics-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Health Log Analytics.

Mit Health Log Analytics installierte Komponenten

Durch Aktivieren der Plugins „Health Log Analytics, „Health Log Analytics Viewer“ und „Health Log Analytics Core“ werden mehrere Komponenten hinzugefügt.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Plugins

Plugin	Beschreibung
Health Log Analytics	Health Log Analytics ist eine KI-gestützte Protokollanalyselösung, die IT-Incidents verhindern kann, bevor Benutzer betroffen sind. Sie identifiziert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin	Beschreibung
	automatisch Ihre Umgebung, protokolliert und prognostiziert IT-Incidents, generiert Warnungen und bietet Expertenvorschläge zur Behebung von Problemen. Health Log Analytics ist eine App aus dem ServiceNow Store. Nach der Installation ist das Modul verfügbar, Sie können sich jedoch dafür entscheiden, es nicht zu nutzen. Abhängigkeit: • Health Log Analytics Zentral • Die ServiceNow® Ereignismanagement Anwendung
Health Log Analytics-Betrachter	Ereignismanagement-Betreiber verwenden das Plugin „Health Log Analytics Viewer“, um Protokolle nach Zeitstempel oder Zeitbereich zu durchsuchen. Mit dem Health Log Analytics Viewer können Ereignismanagement-Betreiber nach einem bestimmten Protokolltext suchen und die Häufigkeit der Treffer in einem bestimmten Zeitraum anzeigen. Abhängigkeit: Die ServiceNow® Ereignismanagement Anwendung.
Health Log Analytics Zentral	Dieses Plugin enthält wichtige Komponenten für Health Log Analytics, z. B. die KI-Engine und Elasticsearch. Health Log Analytics Core ist eine App aus dem ServiceNow Store. Nach der Installation ist das Modul verfügbar, Sie können sich jedoch dafür entscheiden, es nicht zu nutzen. Abhängigkeit: Die ServiceNow® Ereignismanagement Anwendung.

Rollen

Health Log Analytics verwendet die folgenden Rollen.

Rollentitel [Name]	Beschreibung
Ereignismanagement-Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Health Log Analytics.
Ereignismanagement-Betreiber [evt_mgmt_operator]	Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat Schreibzugriff auf Warnungen, um den Lebenszyklus der Warnungenen zu verwalten. Verfügt über die itil-Rolle, um Incidents verwalten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
	zu können, die aus Warnungen erstellt wurden. Kann auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktivieren

Listen

Mit Health Log Analytics werden die folgenden Listen hinzugefügt.

Tabelle [name]	Beschreibung
Erweiterte Protokollwarnungsfilterung [sn_occ_advanced_alert_filtering]	Steuert die Verarbeitung von Warnungsmetriken mit Feedbackoptionen. Ermöglicht die Bereitstellung komplexeren Feedbacks für die KI-Engine Ab Version 20.0.11 - Juli 2021 von Anwendung Health Log Analytics, verfügbar im ServiceNow Store , wird diese Erklärung nicht mehr angezeigt.
Erweiterte Protokollwarnungsfilterung [sn_occ_advanced_alert_filter]	Steuert die Verarbeitung von Warnungsmetriken mit Feedbackoptionen. Ermöglicht die Bereitstellung komplexeren Feedbacks für die KI-Engine **Hinweis:** Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .
Dateneingaben [sn_occ_base_data_input_config]	Ermöglicht das Einrichten von Dateneingabe-Connectors zum Streamen von Protokolldaten in die Instanz
Dateneingabezuordnung [sn_occ_event_mapper]	Ermöglicht die Zuordnung von unbearbeiteten Protokolldaten, die in Ihre Instanz gestreamt werden, um zu bestimmen, wie Health Log Analytics sie verarbeitet
Dateneingabe-Präprozessor [sn_occ_data_input_preprocess_screen]	Ermöglicht das Bearbeiten von unbearbeiteten Protokolldaten, bevor das System sie zuordnet und strukturiert
Warnung definieren [sn_occ_custom_alert]	Ermöglicht das Erstellen benutzerdefinierter Warnungen basierend auf einem vordefinierten Regelsatz
Ausgeschlossene Werte [sn_occ_auto_service_normalizer]	Ermöglicht die Konfiguration von Health Log Analytics, um das Extrahieren bestimmter Protokolldaten zu stoppen, die nicht aussagekräftig genug sind oder redundanten Text oder Informationen enthalten
Extrahierte Werte [sn_occ_auto_service_mapper]	Ermöglicht die Konfiguration von Health Log Analytics, um einen bestimmten Begriff aus einem Feld zu extrahieren und einer angegebenen Komponente zuzuordnen
Funktionen [sn_occ_features]	Listet alle Health Log Analytics-Funktionen auf. Die Funktionen können aktiviert und deaktiviert werden.
Lexikalische Stichwörter [sn_occ_lexical_keywords]	Zeigt alle standardmäßigen lexikalischen Stichwörter an, nach denen Health Log Analytics in Protokolldaten sucht
Protokollkorrelator [sn_occ_log_correlator]	Zeigt alle Korrelatoren an, die bestimmen, ob unterschiedliche Warnungen mit derselben Gruppe korreliert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle [name]	Beschreibung
	werden sollen. Ermöglicht das Hinzufügen von Korrelatoren zu Health Log Analytics
Protokollquellen [sn_occ_sources]	Bietet eine Ansicht aller Dateneingabequellen, wenn die Protokolldaten zugeordnet wurden. Ermöglicht die Steuerung von Eigenschaften und Korrelatoren für diese Quellen
Stummgeschaltete Metriken [sn_occ_metric_state]	Zeigt alle stummgeschalteten Warnungsmetriken zusammen mit den stummgeschalteten Komponenten an. Ermöglicht die Reaktivierung der stummgeschalteten Warnungsmetriken
Quelltyp [sn_occ_source_type]	Enthält die Quelltypen, die im Zuordnungsprozess extrahiert wurden
Quelltypstruktur [sn_occ_source_type_structure]	Ermöglicht die Feinabstimmung der Quelltypstruktur. Bietet eine Ansicht aller Quelltypen, wenn die Protokolldaten zugeordnet wurden. Mit Quelltypen wird definiert, wie Health Log Analytics bestimmte Quellen behandelt und wie die Protokolle analysiert werden.
Streaming-Quellen [sn_occ_log_streaming_source_stats]	Ermöglicht die Überwachung aller Entitäten, die Protokolldaten an die Instanz streamen
Systemintegrität # Benachrichtigungen [sn_occ_health_check]	Zeigt alle Systemintegritätsbenachrichtigungen zusammen an und ermöglicht die Aktualisierung ihres Status
Systemeigenschaften [sn_occ_system_settings]	Zeigt Systemeigenschaften an und ermöglicht die Anpassung ihrer Werte
Zeitstempelformate [sn_occ_timestamp_formats]	Zeigt vordefinierte Zeitstempelformate an. Ermöglicht das Definieren und Hinzufügen von Zeitstempelformaten
Zeitzonen [sn_occ_time_zones]	Aktiviert das Löschen von Datensätzen in sn_occ_time_zones für Benutzer mit der Rolle evt_mgmt_admin

Forms

Mit Health Log Analytics werden die folgenden Formulare hinzugefügt.

Tabelle [name]	Beschreibung
Beats-Dateneingabe [sn_occ_data_input_config_filebeat]	Ermöglicht die Konfiguration erweiterter Einstellungen für Beats-Dateneingabe-Connector
Beats Linux (Filebeat) [sn_occ_data_input_connector_filebeat]	Ermöglicht die Konfiguration von Filebeat-Dateneingabe-Connectors
Elasticsearch-Dateneingabe [sn_occ_data_input_config_filebeat]	Ermöglicht die Konfiguration einer Elasticsearch-Dateneingabe
MID-Server-Dateneingabe [sn_occ_data_input_config_midserver]	Ermöglicht die Konfiguration einer MID-Server-Dateneingabe
Rsyslog [sn_occ_data_input_connector_rsyslog]	Ermöglicht die Konfiguration von Rsyslog-Dateneingabe-Connectors
Rsyslog-Dateneingabe [sn_occ_data_input_config_rsyslog]	Ermöglicht die Konfiguration erweiterter Einstellungen für Rsyslog-Dateneingabe-Connector
TCP-Dateneingabekonfiguration [sn_occ_data_input_config_tcp]	Ermöglicht die Konfiguration erweiterter Einstellungen für TCP-Dateneingabe-Connectors

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle [name]	Beschreibung
Windows Beats [sn_occ_data_input_connector_winbeat]	Ermöglicht die Konfiguration von Windows Beats-Dateneingabe-Connectors
WinLog Beats [sn_occ_data_input_connector_winlogbeat]	Ermöglicht die Konfiguration von WinLog Beats-Dateneingabe-Connectors

Unterstützte Dateneingaben für Health Log Analytics

Health Log Analytics(HLA) Ermöglicht Ihnen, eine Verbindung mit herzustellen ServiceNow Instanz für mehrere Arten von Dateneingaben.

HLA Unterstützt die folgenden Dateneingabetypen:

- Passive Dateneingaben (Listener), die darauf warten, dass Protokolldaten an sie übertragen werden. Diese Dateneingaben erfordern, dass ein Netzwerkport auf dem geöffnet ist MID-Server:
  - Rsyslog
  - Beats
  - Splunk
  - TCP
  - UDP
  - MID-Server
  - GCP-PubSub
  - REST-API

  Die Agent Client Collector-Dateneingabe wird für die Verwendung mit der Anwendung Agent Client Collector Log Analytics unterstützt, die im ServiceNow Store verfügbar ist.
- Aktive Dateneingaben (Abzieher), die Daten aus Repositorys abrufen:
  - Elasticsearch
  - Splunk-Abfrage
  - Amazon CloudWatch
  - Amazon S3
  - Microsoft Azure Log Analytics
  - Microsoft Azure Event Hubs
  - Apache Kafka

  Für alle aktiven Dateneingaben Health Log Analytics Unterstützt MID-Server Cluster für Failover-Schutz. Die aktive Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster. Wenn ja MID-Server Schlägt fehl, verschiebt das System seine Aufgaben zur nächsten verfügbaren MID-Server Im Cluster in einer konfigurierten Reihenfolge.

  Die Elasticsearch Die Dateneingabe ruft Daten aus einem Daten-Repository oder einer Datenbank mithilfe von Anmeldeinformationen ab. Wenn sich Ihre Daten in Elasticsearch befinden, muss Health Log Analytics über Folgendes verfügen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Berechtigungen zum Abfragen von Elasticsearch

  Eine der folgenden Arten von Anmeldeinformationen:

  - Standardauthentifizierung (Benutzer und Kennwort)
  - AWS, für Elasticsearch unter Amazon AWS Cloud

- Netzwerkverbindung zum relevanten Elasticsearch-Cluster

Hinweis: Health Log Analytics muss auf den richtigen Index verweisen, um mit dem Abrufen der Daten zu beginnen.

Darüber hinaus Health Log Analytics Unterstützt Kribel , Edge-Delta , Und Vektor-Agent Dateneingaben. Diese Dateneingaben aktivieren HLA Dient zur Verarbeitung von Protokollnachrichten, die von diesen Tools in Ihre Instanz gestreamt werden.

Nativ ServiceNow Dateneingaben

Streaming-Protokolle von Cloud Observability Bis Health Log Analytics

Health Log Analytics Kann Protokolldaten verarbeiten, die es aus dem erfasst ServiceNow® Cloud Observability Anwendung, früher#Lightstep. HLA Richtet automatisch die Konfiguration ein, die zum Aktivieren des Protokoll-Streamings von erforderlich ist Cloud Observability Als Teil der nativen Integration.
Die Verbindung wird von eingerichtet Cloud Observability Bis HLA Muss in ausgeführt werden Cloud Observability Anwendung. In HLA, Behandeln Sie Protokolldatensätze von Cloud Observability Wie bei allen anderen Datensätzen für Dateneingabezuordnung und Quelltypstruktur, wie in erläutert Automatische Datenzuordnung und -Zuordnung in protokollieren Health Log Analytics Und Anpassung der Quelltypstruktur in Health Log Analytics. Weitere Informationen zu finden Cloud Observability, Siehe Erkunden Sie die Cloud Observability-Dokumentation .

Zugehörige Informationen

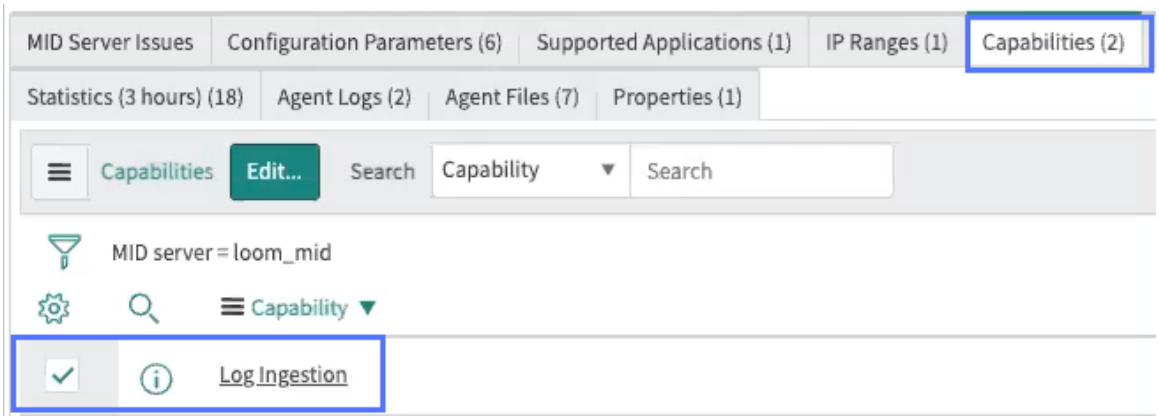
Einrichten Health Log Analytics Auf Ihrem ServiceNow Instanz

MID-Server Proxy-Voraussetzungen für das Streaming von Protokollen an Health Log Analytics

Anforderungen für die Verwendung von MID-Server Proxy, an den Protokolldaten gestreamt werden sollen Health Log Analytics.

- Verwenden Sie eine Squid MID-Server Proxy zum Aktivieren des Streamings von Protokolldaten an Health Log Analytics. Weitere Informationen finden Sie unter Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden.
- Installieren und konfigurieren Sie MID-Server Proxy mit aktivierter Protokollerfassungsfunktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurieren Sie darüber hinaus die folgenden Eigenschaften:

- mid.proxy.use_proxy = wahr
- mid.proxy.host = <proxy_ip>
- mid.proxy.port = <proxy_port>

Health Log Analytics-Konfigurationspräferenzen

Häufig verwendete Einstellungen für Health Log Analytics-Eigenschaften und allgemeine Konfiguration

MID-Server-Einstellungen

- Die MID-Server-Protokollerfassungsfunktion muss aktiviert sein.

  Hinweis: Wird Aktiviert **Alle Fähigkeiten** Auf der MID-Server Umfasst die Aktivierung der Protokollerfassungsfunktion.

- Verwenden Sie nach Möglichkeit dedizierte MID Servers für die Protokollerfassung.
- Damit MID Servers mehrere Produkte ausführen können, muss Health Log Analytics für jede MID-Server-Thread-Konfiguration mindestens die JVM-Speichereinstellung (Java Virtual Machine) für das Standardprodukt aufweisen.

Der bevorzugte MID-Server Einstellungen für Health Log Analytics Sind:

- CPUs: 8
- RAM: 32 GB
- Netzwerkbandbreite: Bis zu 10 Gbit/s
- EBS-Bandbreite: Bis zu 4.750 Mbit/s
- Maximale Java-Heap-Größe für MID-Server: 8.192 MB

Mit den obigen Spezifikationen beträgt der erwartete Protokollerfassungsdurchsatz in einer Washington DC-Instanz wie folgt:

- Für eine Protokollnachricht von 300 Byte: 20.000
- Für eine Protokollnachricht von 1,1 KB: 12.300
- Für eine Protokollnachricht von 2 KB: 7.970

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Mindestanforderungen für das Streaming von Protokollen an Health Log Analytics Sind:

- CPUs: 4
- RAM: 16 GB
- Java-Heap-Größe für MID-Server: 8 GB

Allgemeine Informationen finden Sie unter: Systemanforderungen des MID-Servers .

- Um den Durchsatz der Protokollerfassung zu erhöhen, können Sie entweder die ulimit-Einstellung oder die Netzwerkbandbreite erhöhen oder die Größe der gestreamten Protokolle verringern. Die ulimit-Einstellung kann für einen einzelnen MID-Server konfiguriert werden. Die Korrelation zwischen dem ulimit und dem Durchsatz kann jedoch nicht geändert werden.

  In der folgenden Tabelle sind die ulimit-Einstellungen für offene Dateien im Zusammenhang mit dem Netzwerkdurchsatz auf dem MID-Server aufgeführt . Es zeigt die Größe der Protokolle, die vom MID-Server an den Agent gestreamt werden, und die gRPC-Streaming-Rate, die dem Durchsatz entspricht.

  Ulimit-Einstellungen im Verhältnis zum Durchsatz

Warteschlangentyp	Protokollzeilengröße	GRPC-Rate
In Arbeitsspeicherwarteschlange	300 Byte	18,000
In Arbeitsspeicherwarteschlange	1.1 KB	13,000
In Arbeitsspeicherwarteschlange	2 KB	10.000
Festplattenbasierte Warteschlange	300 Byte	11.000
Festplattenbasierte Warteschlange	1,1 KB	5.000
Festplattenbasierte Warteschlange	2 KB	3,000

  Ab Release August 2024 , Können Sie verbessern MID-Server Kommunikation mit der ServiceNow-Instanz durch Verwendung des Lightning gRPC-Clients, wodurch die Protokoll-Streaming-Geschwindigkeiten auf erhöht werden können Health Log Analytics Bis zu sechsmal. Die Aktivierung des Lightning gRPC-Clients erfordert eine manuelle Konfiguration. Weitere Informationen finden Sie unter Lightning gRPC-Client – Aktivieren der neuen MID-gRPC-Streaming-Architektur [KB1648419] artikel in Now Support Knowledge Base.

- Standardmäßig ist die Anzahl der Dateneingaben pro MID-Server auf 10 beschränkt. Sie können diese Einschränkung für einen einzelnen MID-Server oder für alle MID Servers konfigurieren.
- Sowohl im FIPS- als auch im Nicht-FIPS-Modus müssen MID Servers mit Health Log Analytics-Funktionalität in der Java Runtime Environment (JRE) 11 oder höher ausgeführt werden.

  Hinweis: Zur Unterstützung von BC-FIPS Version 2,0: Health Log Analytics Erfordert ein Upgrade auf Version 34.0,37, Dezember 2024.

Einstellungen für Protokollquellenaufbewahrung

Standardmäßig ist die Protokollaufbewahrung pro Quelle auf drei Tage festgelegt. Diese Einstellung kann nicht geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Verwendung der Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store können Sie die Protokollaufbewahrungsrichtlinie pro Quelle oder für mehrere Quellen auf einmal ändern. Weitere Informationen finden Sie unter Ändern Sie den Aufbewahrungszeitraum der Protokollquelle in Health Log Analytics.

Health Log Analytics-Systemintegritätsbenachrichtigungen

Health Log Analytics Benachrichtigungen zur Systemintegrität helfen, sicherzustellen, dass Sie über potenziell gefährliche Bedingungen informiert sind. Sie können den Status einer Benachrichtigung manuell anpassen, während das Problem behoben wird.

Von Health Log Analytics werden Selbstintegritätsprüfungen dazu verwendet, die Integrität der zugehörigen Komponenten zu überwachen. Wenn ein Systemintegritätsproblem erkannt wird, wird eine Benachrichtigung erstellt und eine E-Mail an alle Abonnenten gesendet. In der (unter „Health Log Analytics-Verwaltung“ verfügbaren) Liste **Systemintegrität – Benachrichtigungen** werden alle Benachrichtigungen zur HLA-Systemintegrität angezeigt, einschließlich der Benachrichtigungen zu internen Fehlern. Bitten Sie Ihren Administrator, die Benachrichtigungen zur Systemintegrität für Sie zu abonnieren.

Health Log Analytics – Systemintegrität – Benachrichtigungen

Feld	Beschreibung
Name	Header der Benachrichtigung.
Beschreibung	Beschreibung der Benachrichtigung.
Erstellt	Datum, an dem die Benachrichtigung erstellt wurde.
Status	Status der Benachrichtigung. • **Neu**: Die Benachrichtigung wurde neu hinzugefügt. • **Bestätigt**: Der Benachrichtigungsdatensatz wurde gelesen. • **In Bearbeitung**: Das in der Benachrichtigung beschriebene Problem wird aktuell behoben. Passen Sie den Wert manuell an. • **Geschlossen**: Das Problem ist nicht mehr aktiv. Passen Sie den Wert manuell an. **Hinweis:** Das Ändern des Status einer Benachrichtigung wirkt sich nicht auf den Status des darin beschriebenen Problems aus. Eine Benachrichtigung im Status „Geschlossen“ wird weiterhin in der Tabelle angezeigt. Die Benachrichtigung wird nur dann automatisch aus der Tabelle herausgefiltert, wenn das Problem als behoben erkannt wird (d. h. wenn der Status „Fehlerfrei“ auf **True** festgelegt ist).
Fehlerfrei	Feld, das den Status des in der Benachrichtigung genannten Problems angibt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics – Systemintegrität – Benachrichtigungen (Fortsetzung)

Feld	Beschreibung
	In der Tabelle werden nur Benachrichtigungen angezeigt, bei denen der Statuswert „Fehlerfrei“ auf **False** festgelegt ist. Wenn das Problem als behoben erkannt wird, wird der Wert automatisch in **True** geändert, und die Benachrichtigung wird aus der Tabelle herausgefiltert.

Health Log Analytics Selbst- Integrität Prüfungen, Benachrichtigungen , Und vorgeschlagene Aktionen

Health Log Analytics bietet Selbstintegritätsprüfungen, Benachrichtigungen und vorgeschlagene Problemlösungsschritte.

Health Log Analytics-Systemintegritätsbenachrichtigungen

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
Maximale Warteschlangengröße der KI-Engine überschritten	The AI engine is running at overcapacity (size=%s, threshold=%s, duration=%s). (Die KI-Engine wird mit Überkapazität ausgeführt.) As a result, the accuracy of anomaly detection might deteriorate. (Dadurch kann sich die Genauigkeit der Anomalie-Erkennung verschlechtern.)	Wenden Sie sich an den Support von ServiceNow.
Hohe Rate nicht klassifizierter Fehler in %s %s	"%s %s has a high rate of unclassified errors and is failing frequently. ("%s %s weist eine hohe Rate nicht klassifizierter Fehler auf und schlägt häufig fehl.)	Wenden Sie sich an den Support von ServiceNow.
Fehler beim Aufrufen der Glide-API	Errors invoking '%s' for %s. (Fehler beim Aufrufen von '%s' für %s.)	Wenden Sie sich an den Support von ServiceNow.
Protokollgrößenbeschränkung wurde überschritten	Log messages from %s: %s are being dropped because the log size limitation was exceeded. (Protokollnachrichten von %s: %s werden verworfen, da die Protokollgrößenbeschränkung überschritten wurde.)	Wenn der Unterschied gering ist, erhöhen Sie die Beschränkung der Protokollgröße, indem Sie die Eigenschaft `mid.data_inputs.max_length_bytes_per_` im Formular „MID-Server-Eigenschaften“ anpassen. Wenn die Protokolle zu lang oder mehrzeilig sind, können Sie auch die Protokollgröße an der Quelle der Protokolle ändern.
Übermäßiges Datenvolumen für Dateneingabe %s.	The data volume for data input %s is too high. (Das Datenvolumen	Wenden Sie sich an den Support von ServiceNow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
	für Dateneingabe %s ist zu hoch.) Log messages are being discarded. (Protokollnachrichten werden verworfen.)	
Protokollnachrichten werden aufgrund einer fehlgeschlagenen automatischen Strukturierung verworfen	Log messages are being dropped because auto-structuring of Source Type %s failed. (Protokollnachrichten werden verworfen, da die automatische Strukturierung von Quelltyp %s fehlgeschlagen ist.)	Finden Sie im Quelltyp heraus, was dazu führen könnte, dass die automatische Strukturierung fehlschlägt. Überprüfen Sie die Fehlerprotokolle, um festzustellen, welche Komponente oder Analyseaktion fehlschlägt.
Übermäßige Anzahl von Skriptfehlern pro Sekunde in %s: %s	The rate of script errors in %s: %s is too high. (Die Rate der Skriptfehler in %s:%s ist zu hoch.)	Überprüfen Sie den JavaScript-Analysefehler in der Quelle, die in der Nachricht angegeben ist: Bildschirm der Dateneingabezuordnung oder Bildschirm der Quelltypstruktur.
Protokollnachrichten, die die zulässige Anzahl von Eigenschaften überschreiten, werden verworfen	The source type %s contains multiple log messages with too many properties. (Der Quelltyp %s enthält mehrere Protokollnachrichten mit zu vielen Eigenschaften.) Such log messages are discarded. (Solche Protokollnachrichten werden verworfen.) Review the Source Type Structure record. (Überprüfen Sie den Datensatz der Quelltypstruktur.)	Überprüfen Sie im entsprechenden Datensatz der Quelltypstruktur die Eigenschaften, die extrahiert werden. Suchen Sie nach Skriptschleifen oder Bedingungen, die dazu führen könnten, dass zu viele Eigenschaften erstellt werden. Vermeiden Sie die Verwendung eines dynamischen Eigenschaftsnamens. Weitere Informationen finden Sie unter Verfeinern Sie die Quelltypstruktur in Health Log Analytics.
Es werden zu viele Cluster generiert. Die Genauigkeit der Anomalie-Erkennung könnte sich verschlechtern.	Too many clusters are being generated for Source Type %s. (Zu viele Cluster werden für Quelltyp %s generiert.) As a result, the accuracy of anomaly detection might deteriorate. (Dadurch kann sich die Genauigkeit der Anomalie-Erkennung verschlechtern.)	Überprüfen Sie die erstellten Muster, und vergewissern Sie sich, dass die Nachrichtenbezeichnung korrekt zugewiesen wird. Überprüfen Sie im Formular der Quelltypstruktur die Nachrichteneigenschaft.
Quellen werden sehr schnell erstellt	Sources are being created at a very high rate. (Quellen werden sehr schnell erstellt.) Data input %s was stopped automatically. (Dateneingabe %s wurde automatisch angehalten.)	Überprüfen Sie im Formular „Dateneingabezuordnung“ das Zuordnungsskript, und beheben Sie alle JavaScript-Fehler, die dazu führen könnten, dass zu viele Quellen erstellt werden.
Quelltypen werden sehr schnell erstellt	Source Types are being created at a very high rate. (Quelltypen werden sehr schnell erstellt.) Data input %s was stopped	Überprüfen Sie im Formular „Dateneingabezuordnung“ das Zuordnungsskript, und beheben Sie alle JavaScript-Fehler, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
	automatically. (Dateneingabe %s wurde automatisch angehalten.)	dazu führen könnten, dass zu viele Quelltypen erstellt werden.
Metriken werden sehr schnell erstellt	Source Type %s is generating too many metrics. (Quelltyp %s generiert zu viele Metriken.) The properties %s were automatically classified as invalid. (Die Eigenschaften %s wurden automatisch als ungültig klassifiziert.)	Beobachten Sie im Formular der Quelltypstruktur die generierten Metriken. Stellen Sie sicher, dass die Metrikbezeichnung nur den erforderlichen Eigenschaften zugewiesen ist. Ein dynamischer Eigenschaftsname oder eine ungenaue JavaScript-Funktion können dazu führen, dass zu viele Eigenschaften generiert werden.
Die Verarbeitungsdauer von REST-Aufrufen in der KI-Engine ist zu lang	Processing of REST calls in the AI Engine is taking too long. (Die Verarbeitung von REST-Aufrufen in der KI-Engine dauert zu lange.)	Wenden Sie sich an den Support von ServiceNow.
Die Anzahl der verworfenen Protokollnachrichten ist zu hoch	Too many log messages are being discarded from source %s. (Zu viele Protokollnachrichten werden von der Quelle %s verworfen.)	Überprüfen Sie die Einstellungen für die Protokollaufbewahrung. Vergewissern Sie sich, dass der Zeitstempel der Protokollzeilen korrekt ist und keine zukünftige oder vergangene Zeit außerhalb des Aufbewahrungszeitraums darstellt.
Durch automatische Strukturierung wird die KI-Engine verlangsamt	Auto-structuring is slowing down the AI engine. (Durch automatische Strukturierung wird die KI-Engine verlangsamt.)	Wenden Sie sich an den Support von ServiceNow.
Protokollnachrichten werden aufgrund eines Fehlers bei der Zeitstempelanalyse verworfen	Log messages from %s %s are being dropped due to a timestamp parsing failure. (Protokollnachrichten von %s %s werden aufgrund eines Fehlers bei der Zeitstempelanalyse verworfen.) Suchen Sie in den Protokollen für die relevante nach „Zeitstempel aus Protokollnachricht fehlgeschlagen“ Service Instanz Und Komponente und beheben Sie das Problem.	Suchen Sie im Formular „Dateneingabezuordnung“ nach dem extrahierten Zeitstempel. Wenn dieser fehlt, navigieren Sie vom Formular zur entsprechenden Quelltypstruktur, und öffnen Sie die Registerkarte „Timestamp Parsing Error“ (Fehler bei Zeitstempelanalyse). Auf der Registerkarte wird das Problem angezeigt, das zum Analysefehler geführt hat. Beheben Sie das Problem.
Kein Rückgang des Arbeitsspeicherverbrauchs	Memory consumption hasn’t dropped in the last few minutes. (Der Arbeitsspeicherverbrauch ist in den letzten Minuten nicht gesunken.)	Wenden Sie sich an den Support von ServiceNow.
Pingt zur Bestimmung der Verbindungsintegrität die Integritätsendpunkte der Elasticsearch-Cluster	Elasticsearch connectivity issues. (Elasticsearch-Verbindungsprobleme.)	Wenden Sie sich an den Support von ServiceNow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
Verwendet die Clientverbindungsprüfung der Metrikbasis zur Bestimmung der Verbindungsintegrität	Metric base connectivity issues. (Verbindungsprobleme bei Metrikbasis.)	Wenden Sie sich an den Support von ServiceNow.
Verwendet die Prüfung der Glide-Clientverbindung zur Bestimmung der Verbindungsintegrität	Glide connectivity problems. (Glide-Konnektivitätsprobleme.)	Wenden Sie sich an den Support von ServiceNow.
Die Dateneingabe weist den Status „Fehlgeschlagen“ auf	The data input %s failed to stream logs. (Das Streamen von Protokollen von Dateneingabe %s ist fehlgeschlagen.)	Überprüfen Sie im Formular „Dateneingabe“ die Verbindung zum MID-Server, und überprüfen Sie die Fehlermeldung.

Health Log Analytics Sprachunterstützung

Health Log Analytics Bietet Unterstützung für internationale Sprachen. Die Standardsprache ist US-Englisch.

Sprachunterstützung-Abdeckung

Die aktuell verfügbaren Sprachen für Health Log Analytics Sind wie folgt: US-Englisch, UK-Englisch, Französisch, Deutsch, Italienisch, Japanisch und Spanisch.

Hinweis: Um Stichwortbasierte Warnungen für andere Sprachen als Englisch zu erhalten, müssen dem System Stichwörter in der entsprechenden Sprache hinzugefügt werden, bevor Sie mit dem Streaming beginnen. Kontakt ServiceNow Unterstützung für Hilfe.

Domain Separation und Health Log Analytics

Domänentrennung wird für Health Log Analytics unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und Health Log Analytics o Anzeigen

Domänentrennung ist in allen Aspekten der Anwendung Health Log Analytics vorhanden. Benutzer, die zu einer bestimmten Domäne gehören, sehen nur die Daten, die in ihrer eigenen Domäne vorhanden sind.

So funktioniert Domain Separation in Health Log Analytics

Wenn Daten mit einem einzelnen Health Log Analytics-Server domänengetrennt sind, kann jeder Managed Service Provider (MSP) die Protokolldaten nur in seiner eigenen Domäne oder den untergeordneten Domänen darunter sehen. Benutzer können Warnungen anzeigen, die Health Log Analytics nur in ihrer eigenen Domäne generiert. Aktionen zum Korrigieren der Warnungen gelten nur für den Bereich dieser Domäne. Standardmäßig werden alle Benutzer und Datensätze auf die übergeordnete Domäne festgelegt, es sei denn, der Administrator weist sie einer bestimmten Domäne zu.

Das Plugin „Health Log Analytics Domain Separation“ muss installiert sein, bevor Sie Ihre Dateneingaben in der Anwendung Health Log Analytics konfigurieren. Es gibt kein Setup-Verfahren für das Plugin. Installieren Sie das Plugin mit der Anwendung Health Log Analytics Version 21.0.1 - September 2021 und aktivieren Sie es dann. Stellen Sie sicher, dass Sie Ihre Daten logischen Silos zuordnen und Regeln und Entitäten konfigurieren.

Sie definieren die domänengetrennte Umgebung, wenn Sie Ihre Dateneingaben konfigurieren. Benutzer können Dateneingaben verwenden, die nur in ihrer eigenen Domäne verfügbar sind. Health Log Analytics erstellt Warnungen nur für Protokolle, die in diesen Dateneingaben ankommen. Alle relevanten Datensätze und die gesamte Datenverarbeitung im Health Log Analytics-Programmablauf befinden sich in derselben Domäne wie die Dateneingabe. Der Domänenname einer Dateneingabe wird in der Spalte **Domäne** angezeigt, die in den Tabellen Ihrer Instanz angezeigt wird.

Die Verwendung der Domänentrennung in Ihrer Instanz ist für Health Log Analytics transparent. Die Anwendung verwaltet alle Aspekte der Daten, z. B. Systemeinstellungen und benutzerdefinierte Vorgänge, separat. Wenn eine Eigenschaft geändert wird, wirkt sich der neue Wert nur auf neue Quellen in der spezifischen Domäne aus. Systemeigenschaften, die den Server betreffen, gelten für alle Domänen, da alle Domänen den Health Log Analytics-Server verwenden.

Hinweis: Health Log Analytics unterstützt bis zu 60 Kilobyte Events pro Sekunde (EPS) über alle Domänen hinweg, ohne die Möglichkeit, eine Servicelevel-Vereinbarung (SLA) für eine bestimmte Domäne bereitzustellen, und ohne Fairness. Wenn eine Domäne eine große Datenmenge streamt, verarbeitet der Health Log Analytics-Server sie. Andere Domänen können daher Latenz, Abbrüche oder andere Probleme erfahren, auch wenn sie eine geringe Anzahl von Protokollen streamen. Auf der MID-Server-Seite werden 10 Kilobyte EPS erwartet.

Anwendungsfälle

- Ein MSP möchte die Anwendung Health Log Analytics mehreren Kunden in einer ähnlichen Umgebung mit einer einzelnen Instanz bereitstellen.
- Eine Organisation mit vielen Mandanten möchte ihre vertraulichen Daten, wie beispielsweise Sicherheitsprotokolle, isolieren.
- Ein Administrator einer Mandantenorganisation möchte eine Dateneingabe nur für seine eigene Domäne definieren.
- Ein Operator in einer Mandantenorganisation möchte Protokolle nur in seiner eigenen Domäne anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Operator in einer Mandantenorganisation möchte Feedback für Warnungen nur in seiner eigenen Domäne bereitstellen.
- Ein MSP-Administrator möchte Protokolldaten aus allen Mandantendomänen seiner Organisation anzeigen.

Zugehörige Informationen

Domänentrennung für Service Provider

Ergebnisfelder des JavaScript-Funktionstests

Beschreibung der Ergebnisfelder des JavaScript-Funktionstests.

Die folgenden Felder sind schreibgeschützt:

Feld	Beschreibung
Duration (ms) (Dauer (ms))	Verarbeitungszeit aller Beispiele in Millisekunden
Quelltypen	Die Anzahl der Quelltypen, die für diese Dateneingabe vorhergesagt oder erstellt wurden.
Quellen	Die Anzahl der für diese Dateneingabe vorhergesagten oder erstellten Quellen.
Fehler	Die Anzahl der JavaScript-Fehler, die in allen Beispielen aufgetreten sind.
Nicht zugeordnet	Anzahl der Protokollzeilen, die nicht zugeordnet werden konnten. Diese Protokollzeilen sind Standard-Tags zugeordnet.
Muster	Die Anzahl der Protokollbeispiele, für die der Test ausgeführt wird. Der Standardwert ist 1.000. **Hinweis:** Sie können die Anzahl der Protokollbeispiele in der Systemeigenschaft Data_input_Mapping.max_Examples auf maximal 5.000 Muster erhöhen. Weitere Informationen finden Sie unter Globale Health Log Analytics-Systemeigenschaften konfigurieren.

Zeigen Sie in den zugehörigen Listen die vorhergesagten oder erstellten Quelltypen und Quellen an.

Liste/Registerkarte	Beschreibung
Zuordnung des Ergebnis-Schlüssel-Werts	Die Ergebnisse der Ausführung der JavaScript-Funktion für die Protokollbeispiele.
Quelltypen (aus Beispielen)	Die vorhergesagten oder erstellten Quelltypen. **Hinweis:** Sie können Quelltypen öffnen, die bereits erstellt wurden, indem Sie den entsprechenden Link auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste/Registerkarte	Beschreibung
Quellen (aus Beispielen)	Die vorhergesagten oder erstellten Quellen. **Hinweis:** Sie können Quellen öffnen, die bereits erstellt wurden, indem Sie den entsprechenden Link auswählen.
Testergebnis	Die Protokollbeispiele zum Testen Ihrer JavaScript-Funktion, sortiert nach Quellen und Quelltypen. Die **Testergebnis** Die Liste zeigt die Anzahl der Protokollbeispiele für jede Quell-Quell-Typ-Kombination an und wird aktualisiert, wenn die Protokollbeispiele aktualisiert werden und Sie mit dem Testen Ihres Skripts beginnen. Die Liste verknüpft mit Beispielen in **Zuordnungsbeispiele** Tabelle, die das Ergebnis der JavaScript-Funktion für jedes Beispiel anzeigt. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .
Quelltypstrukturen	Die Quelltypstrukturen für diese Dateneingabe. Die Überprüfung der Quelltypstrukturen kann Ihnen helfen, den Daten-Flow besser zu verstehen. Die **Zeit des letzten Ereignisses** Die Spalte auf dieser Registerkarte zeigt das letzte Datum und die letzte Uhrzeit an, zu der die KI-Engine ein Protokoll für die Quelltypstruktur verarbeitet hat. Das System aktualisiert diese Informationen alle 5 Minuten. Wenn Sie wissen, wann das letzte Protokoll für diese Quelltypstruktur verarbeitet wurde, können Sie leichter überprüfen, ob Protokolldaten gestreamt werden.

Health Log Analytics Schweregradzuordnung

Health Log Analytics (HLA) verwendet allgemeine Schweregradwerte, um Schweregradbezeichnungen in der Quelltypstruktur zu identifizieren.

Die **Protokollschweregradzuordnung** Tabelle zeigt, wie HLA Wörter mit Schweregrad aus Rohprotokollen identifiziert (in der linken Spalte angezeigt), sie seinen eigenen Schweregradwerten (mittlere Spalte) zugeordnet und dann in angezeigt werden Ereignismanagement Warnungen (rechte Spalte).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollschweregradzuordnung

Schweregrad des Rohprotokolls	Schweregrad des HLA-Protokolls	Ereignismanagement Warnungsschweregrad
TRACE	TRACE	Stichwortbasiert
AUSFÜHRLICH	TRACE	Stichwortbasiert
IN ORDNUNG	TRACE	Stichwortbasiert
FEIN	TRACE	Stichwortbasiert
AM BESTEN	TRACE	Stichwortbasiert
DEBUG	DEBUG	Stichwortbasiert
DBG	DEBUG	Stichwortbasiert
KONFIGURATION	DEBUG	Stichwortbasiert
INFORMATIONAL	INFORMATIONAL	Stichwortbasiert
INFORMATIONEN	INFORMATIONAL	Stichwortbasiert
INF	INFORMATIONAL	Stichwortbasiert
INFO	INFORMATIONAL	Stichwortbasiert
UNBEKANNT	UNBEKANNT	Stichwortbasiert
HINWEIS	HINWEIS	LOW
BENACHRICHTIGUNG	HINWEIS	LOW
WARNUNG	WARNUNG	MEDIUM
WARN	WARNUNG	MEDIUM
ERROR	ERROR	HIGH
FEHLER	ERROR	HIGH
CRITICAL	CRITICAL	CRITICAL
KRIT	CRITICAL	CRITICAL
FAT	CRITICAL	CRITICAL
FATAL	CRITICAL	CRITICAL
SCHWERWIEGEND	CRITICAL	CRITICAL
WARNUNG	WARNUNG	CRITICAL
NOTFALL	NOTFALL	CRITICAL
EMER	NOTFALL	CRITICAL

Hinweis: Wenn Ihr Rohprotokoll numerische Schweregrade oder nicht erkannte Wörter enthält, ordnen Sie diese Werte der Spalte „Schweregrad des HLA-Protokolls“ zu, indem Sie mithilfe der Funktion „JS“ in der Quelltypstruktur eine bedingte Anweisung erstellen. Weitere Informationen finden Sie unter Anpassung der Quelltypstruktur in Health Log Analytics.

Beschreibungen des Dateneingabekonfigurationsfelds

Dieser Abschnitt enthält Beschreibungen der Felder im Health Log Analytics Formulare zur Dateneingabekonfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon CloudWatch Dateneingabekonfigurationsfelder

Beschreibung der Felder in Amazon CloudWatch Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server An, von dem Daten protokolliert werden Amazon CloudWatch Wird abgerufen. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Amazon CloudWatch zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“

Feld	Beschreibung	Beispiel
Von	Datum und Uhrzeit für den Beginn des Lesenvorgangs der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche
Gruppenname(n)	Die zu durchsuchenden Protokollgruppen. Wenn mehrere Protokollgruppen durchsucht werden müssen, geben Sie die Gruppen in einer kommagetrennten Liste an. Um Protokolldaten aus allen Gruppen abzurufen, verwenden Sie ein Sternchen (*) als Platzhalterzeichen. Dies ist ein Pflichtfeld.	hla-cw-loggroup1,hla-cw-loggroup2
Präfix	Namenspräfix für die Amazon CloudWatch-Protokollstreams, aus denen gelesen werden soll.	hla-cw

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“ (Fortsetzung)

Feld	Beschreibung	Beispiel
	Die Dateneingabe wird nur aus Protokollstreams mit diesem Namenspräfix gelesen. **Hinweis:** Pro Datenelement wird nur ein Protokollstream-Präfix unterstützt. Um mehrere Präfixe nutzen zu können, erstellen Sie mehrere Dateneingaben.	
Filtermuster	Muster, nach dem eingehende Events gefiltert werden sollen. Es werden verschiedene Arten von Filtermustern unterstützt. Beispiel: • Ein Muster zum Abrufen von Protokoll-Events, die einen einzelnen Begriff enthalten. • Ein Muster zum Abrufen von Protokoll-Events, die mehrere Begriffe enthalten. • Ein Muster zum Abrufen von Protokoll-Events, die einen Begriff enthalten und einen anderen ausschließen. **Hinweis:** Bei Filtermustern wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html	• Ein Muster zum Abrufen von Protokoll-Events, die den einzelnen Begriff „STATUS_CODE“ enthalten: „STATUS_CODE“ • Ein Muster zum Abrufen von Protokoll-Events, die mehrere Begriffe enthalten, „STATUS_CODE“ und „200“: „STATUS_CODE 200“ • Ein Muster zum Abrufen von Protokoll-Events, die den Begriff „STATUS_CODE“ enthalten und einen anderen Begriff („200“) ausschließen: “STATUS_CODE” – “200”

Registerkarte „Transport“

Feld	Beschreibung
AWS-Anmeldeinformationen	Feld, das auf die Liste „AWS-Anmeldeinformationen“ (aws_credentials.list) verweist. Die Liste enthält den AWS-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
	Zugriffsschlüssel und den geheimen Zugriffsschlüssel.
AWS-Region	Die AWS-Region, in der der Amazon CloudWatch-Cluster ausgeführt wird , z. B. us-west-1. Eine Liste der AWS-Regionen finden Sie unter https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions . Dies ist ein Pflichtfeld.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Verbindungstimeout	Anzahl der Millisekunden, die gewartet werden soll, bevor der AWS-Verbindungsversuch abgebrochen wird.	1.000
Batchgröße	Maximale Anzahl der pro Abfrage abgerufenen Protokolle.	2.500
Socket-Zeitüberschreitung	Anzahl der Millisekunden, die gewartet werden soll, bevor bei einer Datenübertragung über eine hergestellte Verbindung eine Zeitüberschreitung auftritt.	10000
Standardzeitzone	Standardzeitzone, wenn Datum und Uhrzeit des Protokolls keine Zeitzoneninformationen enthalten.	GMT
Anteil der zu verwerfenden Unterstichproben	Anzahl der Protokolle, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Protokolle zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Protokolle, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Protokolle zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Protokolle zurückgegeben hat.	60

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Protokolle abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

Amazon S3 Dateneingabekonfigurationsfelder

Beschreibung der Felder in Amazon S3 Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server An, von dem Daten protokolliert werden Amazon S3 Wird abgerufen. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge. **Hinweis:** • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Amazon S3 zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe gestoppt wurde oder fehlgeschlagen ist.
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in die Dateneingabe gestreamt wurde.
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“

Feld	Beschreibung	Beispiel
Von/Bis	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. • Von: Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt.	Von: Jetzt -1 Woche Bis: 2300-01-01 15:59:59

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“ (Fortsetzung)

Feld	Beschreibung	Beispiel
	• Bis: Daten, die neuer als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. Legen Sie für Live-Daten dieses Datum weit in die Zukunft. Dies ist ein Pflichtfeld.	
Bucket-Name	Das zu streamende Amazon S3-Bucket Dies ist ein Pflichtfeld.	my-s3-bucket
Präfix	Präfix für die abzurufenden Objekte. Die Dateneingabe ruft nur Objekte ab, die mit diesem Präfix beginnen. Dieses Feld wird normalerweise verwendet, um nur bestimmte Ordner in einem Bucket abzurufen.	/nur/dieses/verzeichnis/
Einbeziehen	Datei oder Objekt, die/das einbezogen werden soll, wenn das System einen Musterabgleich durchführt.	.*bezieh-mich-ein.*
Ausschließen	Datei oder Objekt, die/das ausgeschlossen werden soll, wenn das System einen Musterabgleich durchführt.	.*überspring-mich.*

Registerkarte „Transport“

Feld	Beschreibung
AWS-Anmeldeinformationen	Feld, das auf die Liste „AWS-Anmeldeinformationen“ (aws_credentials.list) verweist. Die Liste enthält den AWS-Zugriffsschlüssel und den geheimen Zugriffsschlüssel.
AWS-Region	AWS-Region, in der sich das Amazon S3-Bucket befindet, z. B. us-west-1. Eine Liste der AWS-Regionen finden Sie unter https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions . Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Anonym	Option zum Erzwingen des Zugriffs auf den Amazon S3-Bucket ohne Anmeldeinformationen, wobei Standardanmeldeinformationen, falls vorhanden, ignoriert werden.	Falsch
Durchlaufen	Option für den Zugriff auf jedes Verzeichnis im Bucket.	Falsch
Objekte sortiert nach dem Zeitpunkt der letzten Änderung	Option zum Abrufen von Objekten, wenn die Objekte im Bucket nach Zeit sortiert sind.	Falsch
Verbindungstimeout	Anzahl der Millisekunden, die gewartet werden soll, bevor der AWS-Verbindungsversuch abgebrochen wird.	100
Threadpool-Größe	Anzahl der gleichzeitigen Threads, die Dateien aus dem Bucket herunterladen.	1
Puffergröße	Größe des Download-Puffers in Byte.	100 MB
Socket-Zeitüberschreitung	Anzahl der Millisekunden, die gewartet werden soll, bevor bei einer Datenübertragung über eine hergestellte Verbindung eine Zeitüberschreitung auftritt.	10000
Max retry for file (Max. Wiederholungsversuche für Datei)	Maximale Anzahl der Wiederholungen der Dateiverarbeitung im Fehlerfall.	10
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	UTC
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Quotengrenze	Maximale Anzahl von Events pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

Apache Kafka Dateneingabekonfigurationsfelder

Beschreibung der Felder in Apache Kafka Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server An, von dem Daten protokolliert werden Apache Kafka Wird abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Apache Kafka zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche

Registerkarte „Transport“

Feld	Beschreibung	Beispiel
Kafka-Knotennamen	Kommagetrennte Liste im Format HOST:PORT,HOST:PORT. Die Liste muss nicht alle Server des Apache Kafka-Clusters enthalten.	123.4.5.6:9092,123.3.4.5:9093
Themen	Kommagetrennte Liste von Themen, die die Dateneingabe abonnieren muss. Dies ist ein Pflichtfeld.	ErstesThema,ZweitesThema,DrittesThema

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung	Beispiel
Kafka-Anmeldeinformationen	Verweis auf die Apache Kafka-Anmeldeinformationen. Sie können das Formular „Kafka SSL-Anmeldeinformationen“ anzeigen, indem Sie das Informationssymbol (ⓘ) und dann **Datensatz öffnen** auswählen. Im Formular können Sie das Sicherheitsprotokoll für die Authentifizierung mit Apache Kafka aus den folgenden Optionen auswählen: • **SSL**: SSL-Kanal. • **SASL_SSL**: SASL-authentifizierter SSL-Kanal. • **SASL_PLAINTEXT**: SASL-authentifizierter, nicht verschlüsselter Kanal. Eine Beschreibung der Felder im Formular „Kafka SSL-Anmeldeinformationen“ finden Sie unter Kafka SSL-Anmeldeinformationen – Felder.	Keine
Gruppen-ID	Name der Apache Kafka-Verbrauchergruppe.	Protokolle

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Zeitüberschreitung	Zeit in Millisekunden, die beim Abruf gewartet wird, wenn in den Themen keine Daten verfügbar sind.	500
Zeitüberschreitung bei Knotenerkennung	Zeit in Millisekunden vor dem Ablaufen der Knotenerkennung.	30
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	GMT

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

Kafka SSL-Anmeldeinformationen – Felder

Beschreibung der Felder im Formular „Kafka SSL-Anmeldeinformationen“.

SSL-Sicherheitsprotokoll

Feld	Beschreibung
SSL-Schlüsselspeicher	Der Inhalt einer tatsächlichen Datei server.keystore.jks, codiert als base64-Zeichenfolge.
SSL-Schlüsselspeicher-Typ	Format der SSL-Schlüsselspeicherdatei. Standard: Java KeyStore (JKS).
SSL-Schlüsselspeicher-Passwort	Passwort für den Schlüsselspeicher, identisch mit dem Wert der Eigenschaft ssl.keystore.password in Apache Kafka.
SSL-Schlüsselpasswort	Passwort, identisch mit dem Wert der Eigenschaft ssl.key.password in Apache Kafka.
SSL-Truststore	Inhalt einer tatsächlichen Datei client.truststore.jks, codiert als base64-Zeichenfolge.
SSL-Truststore-Typ	Format der Truststore-Datei. Standard: Java KeyStore (JKS).
SSL-Truststore-Passwort	Passwort für den Truststore, identisch mit dem Wert der Eigenschaft ssl.truststore.password in Apache Kafka.
SSL-Anbieter	Name des für SSL-Verbindungen verwendeten Sicherheitsanbieters.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSL-Sicherheitsprotokoll (Fortsetzung)

Feld	Beschreibung
Verifizierung des Hostnamens deaktivieren	Option zum Deaktivieren der Überprüfung des Hostnamens.
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

SASL_SSL-Sicherheitsprotokoll

Feld	Beschreibung
SSL-Truststore	Inhalt einer tatsächlichen Datei client.truststore.jks, codiert als base64-Zeichenfolge.
SSL-Truststore-Typ	Format der SSL-Truststore-Datei. Standard: Java KeyStore (JKS).
SSL-Truststore-Passwort	Passwort für den Truststore, identisch mit dem Wert der Eigenschaft ssl.truststore.password in Apache Kafka.
SSL-Anbieter	Name des für SSL-Verbindungen verwendeten Sicherheitsanbieters.
Verifizierung des Hostnamens deaktivieren	Option zum Deaktivieren der Überprüfung des Hostnamens.
Benutzername	Der diesen Anmeldeinformationen zugeordnete Benutzername (sofern vorhanden). **Hinweis:** Der angegebene Benutzername wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLoginModule required username=<user_name> password=<password>`.
Passwort	Das mit diesen Anmeldeinformationen verknüpfte Passwort. **Hinweis:** • Das angegebene Passwort wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLoginModul required username=<user_name> password=<password>`. • Das von Ihnen angegebene Passwort ist unsichtbar. Es wird in verschlüsselter Form in der Datenbank gespeichert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SASL_SSL-Sicherheitsprotokoll (Fortsetzung)

Feld	Beschreibung
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

SASL_PLAINTEXT-Sicherheitsprotokoll

Benutzername	Der diesen Anmeldeinformationen zugeordnete Benutzername (sofern vorhanden). **Hinweis:** Der angegebene Benutzername wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLoginModule required username=<user_name> password=<password>`.
Passwort	Das mit diesen Anmeldeinformationen verknüpfte Passwort. **Hinweis:** • Das angegebene Passwort wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLoginModul required username=<user_name> password=<password>`. • Das von Ihnen angegebene Passwort ist unsichtbar. Es wird in verschlüsselter Form in der Datenbank gespeichert.
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

Automatische Übersetzung

Konfigurationsfelder für Cribl-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für Cribl-Dateneingabe.

Erste Schritte

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte (Fortsetzung)

Feld	Beschreibung
MID-Server verwenden	Die MID-Server An den die Cribl-Protokolle gestreamt werden. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.

Konfiguration

Feld	Beschreibung
URL der Cribl-Instanz	Die URL der Cribl-Instanz. HLA Verwendet diese URL, um die Verbindung mit der Cribl-Instanz herzustellen.
Cribl-API-Token	Das Cribl-API-Token HLA Verwendet zur Authentifizierung bei Cribl und zum Durchführen von API-Aufrufen.

Prozess

Feld	Beschreibung
Cribl-Route	Die Cribl-Route, die Protokolldaten an ein bestimmtes Ziel weiterleitet. Dieses Feld wird automatisch mit einer Dropdown-Liste aller verfügbaren Routen ausgefüllt, die jeweils mit einem Standardziel konfiguriert sind. Sie müssen die gewünschte Route aus dieser Liste auswählen. Dies ist ein Pflichtfeld.
Cribl-Ziel	Das erstellte Cribl-Ziel. Das Cribl-Ziel zeigt auf MID-Server In der Dateneingabe konfigurierter Host und Port. Dieses Feld ist schreibgeschützt.

Edge Delta-Dateneingabekonfigurationsfelder

Beschreibung der Felder im Konfigurationsformular „Edge Delta-Dateneingabe“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Delta-Dateneingabekonfigurationsformular

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Übertragung	Das Edge-Delta-Ziel, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz. Die Optionen sind: • TCP: Wird häufig für die Verarbeitung großer Mengen von Protokolldaten verwendet. Wenn Sie TCP auswählen, müssen Sie angeben MID-Server Und Port. Wenn Sie die Option „TCP-Transport“ auswählen, erstellen Sie ein TCP-Ziel in Edge Delta, um Protokolldaten aus einer beliebigen Quelle an die Instanz zu senden MID-Server Host und Port, den Sie für die Edge Delta-Dateneingabe konfiguriert haben. **Hinweis:** Für TCP wird TLS/SSL nicht unterstützt. • HTTP: Wird häufig zum Senden kleinerer Protokolle über RESTful APIs verwendet, HTTP oder HTTPS für sichere Übertragung . **Hinweis:** Für das HTTP-Protokoll wird die Authentifizierung verwendet. Wenn Sie HTTP auswählen, müssen Sie den MID-Webserver angeben, der auf dem ausgeführt wird MID-Server. Das System füllt dann aus MID-Server Und Portfelder automatisch basierend auf dem bereitgestellten MID-Webserver. Abhängig von der MID-Webserverkonfiguration können Sie Protokolle entweder über HTTP oder HTT senden P S. Wenn **Sichere Verbindung** Das Kontrollkästchen im MID-Webserver-Erweiterungsformular ist deaktiviert. Verwenden Sie HTTP. Wenn diese Option ausgewählt ist, verwenden Sie HTTPS. Weitere Informationen finden Sie unter Formular „Ereignismanagement MID-Webserver erweiterung“. Zusätzlich, wenn **Authentifizierungstyp** Geben Sie im Formular „MID-Webserver-Erweiterung“ im Header „Autorisierung“ Details zur Standardauthentifizierung an. Wenn **Authentifizierungstyp** Ist API-Schlüssel, geben Sie den Schlüssel als „ an Schlüssel Api_Key „. Wenn Sie die HTTP-Transportoption auswählen, erstellen Sie ein HTTP-Ziel in Edge Delta, und geben Sie die Endpunkt-URL im folgenden Format ein: http://{MID_SERVER_IP}:{MID_WEB_SERVER_PORT}/api/mid/hla/raw. Erstellen Sie in den erweiterten Einstellungen zwei Header, die an die HTTP-Anforderung angehängt werden sollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Edge Delta-Dateneingabekonfigurationsformular (Fortsetzung)

Feld	Beschreibung
	○ Ein Autorisierungsheader mit dem Schlüsselwert der MID-Webserver-API Oder grundlegende Anmeldeinformationen, wie MID-Webserver konfiguriert . ○ Ein Inhaltstyp-Header mit dem Wert „Application/JSON“.
MID-Webserver	Der MID-Webserver, an den die Protokolldaten gestreamt werden.
MID-Server verwenden	Die MID-Server An den die Edge-Delta-Protokolle gestreamt werden. Dies ist ein Pflichtfeld. Wenn Sie HTTP in ausgewählt haben **Transport** Feld, wird dieses Feld basierend auf dem ausgewählten MID-Webserver automatisch ausgefüllt.
Port	Der Port auf der MID-Server Wird zum Abhören von Protokollen verwendet. Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Im Falle eines TCP-Transports darf der Port nicht von einem anderen Prozess belegt werden. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld. Wenn Sie HTTP in ausgewählt haben **Transport** Feld, wird dieses Feld basierend auf dem ausgewählten MID-Webserver automatisch ausgefüllt.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. Durch Auswahl der Serviceinstanz wird aktiviert HLA Zum Korrelieren von CIs und Serviceinstanzen in der CMDB für die Ursachenanalyse. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.

Elasticsearch Dateneingabekonfigurationsfelder

Beschreibung der Felder in Elasticsearch Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmter MID-Server oder ein MID-Server-Cluster verwendet werden soll. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	2023 und höher, verfügbar über ServiceNow Store .
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server, von dem Protokolldaten aus Elasticsearch-Indizes abgerufen werden **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Feld ist auf spezifisch festgelegt MID-Server Cluster) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben gemäß der konfigurierten Reihenfolge zum nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 26.0.17 – Februar 2023 und höher, verfügbar über ServiceNow Store .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Wenn Elasticsearch Verwendet Client-Zertifikat- oder CA-Zertifikat-Authentifizierung, alle MID Servers Im Cluster muss über die entsprechenden Zertifikate verfügen. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu MID-Server-Clustern finden Sie unter Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Diese Dateneingabe verwendet Elastic, um Protokolldaten an Ihre Instanz zu streamen.
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Registerkarte „Transport“

Feld	Beschreibung
Server-URL	URL für den Zugriff auf das Cluster. Dies ist ein Pflichtfeld.
Max. Anzahl von Verbindungen pro Route	Maximale Anzahl der pro Knoten zu öffnenden Verbindungen. Standardwert: 2
Max. Bildlaufsegmente	Die Anzahl der Shards, die für den relevanten Index in konfiguriert sind Elasticsearch. Diese Zahl gibt Elastic an, wie viele parallele Abfragen in jeder Abfrageanforderung ausgeführt werden sollen.
Proxy-Host	Hostname des HTTP-Proxys, über den Anforderungen gesendet werden.
Proxy-Port	Port des HTTP-Proxy, über den Anforderungen gesendet werden
Authentifizierungsmethode	Die Authentifizierungsmethode, die zum Authentifizieren der Dateneingabe verwendet wird Elasticsearch. Die Optionen sind: Standardauthentifizierung, apiKey oder Client-Zertifikat. **Hinweis:** Wenn Sie die erforderliche Authentifizierungsmethode auswählen, werden die entsprechenden Anmeldeinformationsfelder im Formular angezeigt.
Anmeldeinformationen für Standardauthentifizierung	Anwendername und Passwort, die für die Verbindung mit verwendet werden Elasticsearch Suchmaschine. **Hinweis:** Füllen Sie entweder dieses Feld oder das Feld **AWS-Anmeldeinformationen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
AWS-Anmeldeinformationen	AWS-Anmeldeinformationen für die Verbindung mit der von AWS gehosteten Elasticsearch-Such-Engine **Hinweis:** Füllen Sie entweder dieses Feld oder das Feld **Anmeldeinformationen für Standardauthentifizierung** aus.
AWS-Region	AWS-Region, in der das Elasticsearch-Cluster ausgeführt wird
Anmeldeinformationen für API-Keys	Der API-Schlüssel, der für die Verbindung mit verwendet wird Elasticsearch Suchmaschine.
Client-Zertifikat	Das Clientzertifikat, das für die Verbindung mit verwendet wird Elasticsearch Suchmaschine.
MID-Zertifikatrichtlinienprüfung verwenden	Option zum Aktivieren der Prüfung der MID-Zertifikatsrichtlinie. Wählen Sie diese Option aus, wenn Sie die Protokolle mit SSL/TLS verschlüsselt senden möchten. Navigieren Sie dann zu **Alle** > **MID-Server** > **MID-Sicherheitsrichtlinie** Und fügen Sie der Tabelle die MID-Zertifikatrichtlinienprüfung hinzu. Weitere Informationen finden Sie unter Richtlinien für die Zertifikatprüfung des MID-Servers .

Registerkarte „Abfrageeinstellungen“

Feld	Beschreibung	Beispiel
Von/Bis	Von- und Bis-Datum und Uhrzeit zum Lesen der Daten • Von: Es werden keine Daten gelesen, die älter als dieses Datum sind. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. • Bis: Nach diesem Datum werden keine Daten gelesen. Legen Sie für Live-Daten dieses Datum weit in die Zukunft.	Von: 1970-01-01 15:59:59 Bis: 2300-01-01 15:59:59
Cross-Cluster-Suche verwenden	Option für die Suche nach Daten in Elasticsearch Cluster.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“ (Fortsetzung)

Feld	Beschreibung	Beispiel
	Wenn dieses Kontrollkästchen aktiviert ist, wird **Cluster, die gesucht werden sollen** Feld wird angezeigt. **Hinweis:** Ihre Einstellungen in **Verwenden Sie minimale Berechtigungen** Kontrollkästchen und **Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)** Feld auf der **Erweiterte Konfiguration** Das Formular wirkt sich auf die Erfassung von Daten in mehreren Clustern aus.	
Cluster für Suche	Die Elasticsearch Cluster, die gesucht werden sollen. Dieses Feld wird nur angezeigt, wenn **Verwenden Sie die clusterübergreifende Suche** Das Kontrollkästchen ist aktiviert. Führen Sie einen der folgenden Schritte aus: • Lassen Sie dieses Feld leer, oder geben Sie „*“ ein, um alle in definierten Remote-Cluster zu durchsuchen Elasticsearch. • Geben Sie die Cluster an, die in einer kommagetrennten Liste gesucht werden sollen. **Hinweis:** Um auch den lokalen Cluster zu durchsuchen, fügen Sie ein Komma am Anfang oder Ende hinzu, oder fügen Sie der Liste zwei Kommas hintereinander hinzu. Beispiel: „East,,West“ oder „,East,West“ oder „,*,“	ost, West, Süd
Indexpräfix	Präfix für die Elasticsearch-Indizes, aus denen gelesen werden soll. Die Dateneingabe wird nur aus Indizes mit diesem Präfix gelesen. Dies ist ein Pflichtfeld.	only-read-these-indices-*
Minimale Berechtigungen verwenden	Option zum direkten Lesen von Protokolldaten aus Elasticsearch Indizes mit dem konfigurierten Präfix. • Wenn diese Option ausgewählt ist, liest die Dateneingabe die Protokolldaten direkt aus Elasticsearch Indizes mit dem konfigurierten Präfix.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“ (Fortsetzung)

Feld	Beschreibung	Beispiel
	Zum Ausführen dieser Aufgabe sind nur Leseberechtigungen erforderlich. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist und Sie die clusterübergreifende Suche verwenden, werden Daten aus allen Clustern gleichzeitig erfasst. • Wenn diese Option deaktiviert ist, ruft die Dateneingabe alle Indizes mit dem Präfix ab, filtert sie und liest die Protokolldaten aus den gefilterten Indizes. Die Ausführung dieser Aufgabe erfordert zusätzliche Berechtigungen. **Hinweis:** Wenn Sie dieses Kontrollkästchen deaktivieren, wirkt sich die Verwendung der clusterübergreifenden Suche darauf aus, wie Daten aus den Clustern erfasst werden. Weitere Informationen finden Sie unter Aktivieren und Verwenden der clusterübergreifenden Suche für Elasticsearch-Dateneingaben in Health Log Analytics [KB1556079] artikel in Now Support Knowledge Base. Weitere Informationen zu Streaming-Protokollen mit der Elasticsearch-Dateneingabe finden Sie im Artikel Stream logs using Elasticsearch data input – Advanced Guide [KB1080162] (Protokolle mit Elasticsearch-Dateneingabe streamen - Erweiterte Anleitung) in der Now Support-Knowledge Base.	
Zeitstempelfeld des Dokuments	Zeitstempelfeld in Dokumenten, die in den Leseindizes gespeichert sind. Dies ist ein Pflichtfeld.	
Format des Zeitstempelfelds	Format des Zeitstempelfelds in den Dokumenten. Wenn kein Format angegeben ist, wird das standardmäßige Unix-Epochenzeitformat in Millisekunden verwendet. Zum Beispiel:	jjjj-MM-tt'T'HH:mm:ss.SSSSSSS'Z'

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“ (Fortsetzung)

Feld	Beschreibung	Beispiel
	1684168407 (15. Mai 2023 16:33:27 Uhr)	
Begriffsfilter	JSON-Zuordnung der zu filternden Begriffe **Hinweis:** Vermeiden Sie die Verwendung von Begriffsabfragen für Textfelder. Wenn das Zielfeld sowohl als Text als auch als Stichwort zugeordnet ist, referenzieren Sie das Stichwort mit feldname.stichwort.	{"severity": ["error", "warning"]}
Max. Anzahl von Dokumenten pro Abfrage	Maximale Anzahl von Dokumenten, die in einer einzelnen Abfrage abgerufen werden	
Sliced-Scrolling-Tiebreaker	Wert, der zum Teilen der Daten verwendet wird. Jeder Teil wird parallel gescrollt. Standard: _id	
Search-after-Tiebreaker	Eindeutiger Wert pro Dokument, der beim Sortieren von Protokolleinträgen nach Zeitstempel als Tiebreaker verwendet werden soll.	
Search-after-API verwenden	Option für das Wechseln zwischen Sliced-Scrolling- und Search-after-APIs. **Hinweis:** Sliced-Scrolling-APIs sind beim Lesen historischer Daten vorzuziehen, während Search-after-APIs besser zum Lesen von Echtzeitdaten geeignet sind.	
Zeitsuffixformat für Index	Format des Zeitsuffix bei Verwendung von zeitbasierten Indexnamen, z. B. [logstash-]JJJJ.MM.TT. Wenn Sie Aliasse verwenden, lassen Sie dieses Feld leer.	uuuu.MM.tt

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung
Datenlese-Zeitüberschreitung (Millisekunden)	Dauer in Millisekunden, bevor eine Anforderung an den Elasticsearch-Cluster abläuft
Intervall für Indexerkennung (Sekunden)	Anzahl der Sekunden zwischen intermittierenden MID-Server-Anforderungen an das Elasticsearch-Cluster für neue Indizes, aus denen Daten gelesen werden sollen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung
Scroll-Kontextzeit (Millisekunden)	Lebensdauer des erstellten Scroll, wenn die Scroll-API zum Lesen von Daten aus Elasticsearch verwendet wird. Weitere Informationen finden Sie in der Elasticsearch Dokumentation zur Scroll API .
Event Processor Worker	Maximale Anzahl von CPU-Kernen, die parallel zur Verarbeitung von aus Elasticsearch abgerufenen Events verwendet werden. Eine höhere Einstellung erhöht den Dateneingabedurchsatz auf Kosten einer höheren CPU-Auslastung.
Größe der Worker-Warteschlange	Maximale Anzahl von Stapeln, die zur Verarbeitung in die Warteschlange gestellt werden. Eine höhere Einstellung erhöht den Durchsatz auf Kosten einer höheren RAM-Auslastung.
Standardzeitzone	Standardzeitzone, wenn Datum und Uhrzeit des Events keine Zeitzoneninformationen enthalten.
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Ruheintervall (Sekunden)	Intervall der Wartzeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Daten zurückgegeben hat
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte
Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)	Die Anzahl der Sekunden vor dem aktuellen Zeitpunkt, zu dem verzögerte Daten abgefragt werden sollen. Die konfigurierte Anzahl von Sekunden wird von der aktuellen Zeit für das Lesen des letzten Zeitstempels abgezogen. **Hinweis:** Wenn dieser Wert 0 ist und Daten aus mehreren Clustern gleichzeitig erfasst werden, enthält die Abfrage möglicherweise keine Daten, die mit einer Verzögerung an einem der Cluster gesendet wurden.

Konfigurationsfelder der GCP-PubSub-Dateneingabe

Beschreibung der Felder im Formular „GCP PubSub-Dateneingabekonfiguration“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) Der MID-Server, an den die Protokolle gestreamt werden. **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge. **Hinweis:** • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übertragung	Protokoll, das zum Senden der Protokolldaten verwendet wird: Pubsub.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Registerkarte „Transport“

Feld	Beschreibung
Projekt-ID	Die Projekt-ID des Google Cloud Projekt. Beispiel: My-project-ID
Themenname	Die Google Cloud Pub/Unterthema, das abonniert werden soll Health Log Analytics. Beispiel: My_topic.
Alias für GCP-Anmeldeinformationen	Der zu verwendende Anmeldeinformationsalias. Geben Sie einen GCP-Anmeldeinformationsalias an, indem Sie das Lupensymbol auswählen und dann entweder einen vorhandenen Anmeldeinformationsalias aus auswählen **Aliasse Für Verbindungen Und Anmeldeinformationen** Liste oder Auswahl **Neu** Zum Erstellen eines neuen Datensatzes. Der Standardwert ist sn_occ.HLA_Credential_Alias. Informationen zum Erstellen eines Anmeldeinformationsalias finden Sie unter Anmeldeinformationsaliasse für Discovery .
Aboname	Das Abonnement Health Log Analytics Verwendet, um Protokolldaten zu empfangen, die auf veröffentlicht werden Google Cloud Pub/Unterthema. Wenn Sie dieses Feld leer lassen, Health Log Analytics Verwendet ServiceNow-Abonnement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Registerkarte „Erweitert“

Feld	Beschreibung	Standardwert
Größe des Abonnenten-Thread-Pools	Die Anzahl der gleichzeitigen Threads, die Dateien aus herunterladen Google CloudPub/ Unterthema.	1
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	(Schreibgeschützt) die Zeichencodierung für diese Dateneingabe.	UTF-8
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Quotengrenze	Maximale Anzahl von Events pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	Leeren

Microsoft Azure Event Hubs Dateneingabekonfigurationsfelder

Beschreibung der Felder in Microsoft Azure Event Hubs Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	MID-Server An, von dem Daten protokolliert werden Microsoft Azure Event Hubs Wird abgerufen. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Microsoft Azure Event Hubs zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche
Max. Batchgröße	Maximale Anzahl von Events, die an einen einzelnen Prozessaufruf übergeben werden.	100

Registerkarte „Transport“

Feld	Beschreibung
Event Hubs-Namespace	Bereichscontainer für den/die Event-Hub(s). Dies ist ein Pflichtfeld.
Event Hub-Name	Der Event-Hub, aus dem Protokolldaten abgerufen werden sollen. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
Event Hub credentials (Event-Hub-Anmeldeinformationen)	Freigegebene Zugriffsberechtigungsrichtlinie zur Authentifizierung beim Event-Hub. Dies ist ein Pflichtfeld.
Consumer Group name (Verbrauchergruppenname)	Zu verwendende Verbrauchergruppe. Dies ist ein Pflichtfeld.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Restore point rate (Rate für Wiederherstellungspunkt)	Anzahl der Events, die die Dateneingabe lesen kann, bevor ein Wiederherstellungspunkt gespeichert wird.	100
Processor threads count (Anzahl der Prozessor-Threads)	Gesamtanzahl der Prozessor-Threads.	2
Zeitüberschreitung für Vorgang	Anzahl der Sekunden, die gewartet werden soll, bevor Event-Hub-Vorgänge ablaufen.	120
Leerlauf-Zeitüberschreitung beim Empfang	Anzahl der Sekunden, die gewartet werden soll, bevor Empfangsvorgänge ablaufen.	60
Prefetch count (Anzahl der Vorabrufe)	Anzahl der Events, die vor Event-Hub-Vorgängen vorab empfangen wurden.	500
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	GMT
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

Microsoft Azure Log Analytics Dateneingabekonfigurationsfelder

Beschreibung der Felder in Microsoft Azure Log Analytics Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server, von dem die Protokolldaten aus Microsoft Azure Log Analytics abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Microsoft Azure Log Analytics zum Streamen von Protokolldaten an Ihre Instanz.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“

Health Log Analytics *Verwendet die in diesen Feldern festgelegten Werte, um die Abfrage für den Empfang von Protokolldaten von zu generieren* **Microsoft Azure Log Analytics**. *Die* **Protokollabfrage** *Mit dem Feld können Sie eine anwenderdefinierte Abfrage konfigurieren*

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche
Datenquellenname	Die Name der Tabelle in Microsoft Azure Log Analytics Wo die Dateneingabe die Protokolldaten abruft. Weitere Informationen finden Sie im Abschnitt Tabelleninformationen anzeigen in Microsoft Azure-Dokumentation .	ContainerProtokoll

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“

Health Log Analytics *Verwendet die in diesen Feldern festgelegten Werte, um die Abfrage für den Empfang von Protokolldaten von zu generieren* **Microsoft Azure Log Analytics**. *Die* **Protokollabfrage** *Mit dem Feld können Sie eine anwenderdefinierte Abfrage konfigurieren*

(Fortsetzung)

Feld	Beschreibung	Beispiel
	Dies ist ein Pflichtfeld.	
Name der Eigenschaft für die Ereigniszeit	Das Microsoft Azure Log Analytics-Feld, in dem die Events-Zeit erkannt werden soll. Dies ist ein Pflichtfeld.	TimeGenerated
Max. Anzahl von Dokumenten pro Abfrage	Die höchste Anzahl von Zeilen, die in jeder Abfrage abgerufen werden.	500
Spaltenauswahl	Kommagetrennte Liste der Spaltennamen, die zurückgegeben werden sollen. **Hinweis:** Dieses Feld wird ignoriert, wenn Sie eine benutzerdefinierte Abfrage angeben.	LogEntry,LogEntrySource

Protokollabfrage	Eine anwenderdefinierte Abfrage zum Empfangen von Protokolldaten von Microsoft Azure Log Analytics.
	
	Die Einstellungen in diesem Feld überschreiben die in allen anderen Feldern auf der **Abfrageeinstellungen** Registerkarte mit Ausnahme der **Von** Feld. Wenn **Protokollabfrage** Feld ist leer, Health Log Analytics Generiert die Abfrage anhand der in den anderen Feldern festgelegten Werte.
	
	Verwenden Sie für die anwenderdefinierte Abfrage das folgende JSON-Format:
	
	{"query": „Query | Where timeGenerated > %s | Take 500"}
		<pre>{
		"query":"ContainerLog
		| where
		LogEntry contains
		'cartservice'
		| where
		TimeGenerated > %s
		| take 500",
		"workspaces":
		["defaultworkspace-3ab145
		ff-f9cd-433f-8533-d1b1ee24
		aee6-eus"],
		"project": ["TimeGenerated",
		"LogEntry",
		"LogEntrySource"]
		}</pre>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“

Feld	Beschreibung
Umleitungs-URL	Die Umleitungs-URL der Zugriffsprotokollanwendung. Die URL bezieht sich auf Microsoft Azure Autorisierungseigenschaft „Redirect_URI“. Weitere Informationen finden Sie im Abschnitt Autorisierungscode-URL (GET-Anforderung) im Microsoft Azure-Dokumentation . Dies ist ein Pflichtfeld.
Azure-Service-Prinzipal-Anmeldeinformationen	Die Anmeldeinformationen, die für den Zugriff auf Microsoft Azure-Ressourcen verwendet werden. Wählen Sie aus der Dropdown-Liste **Geheimer Clientschlüssel** aus. **Hinweis:** Sie benötigen keine Anmeldeinformationen für Azure Enterprise Agreement (EA). Dies ist ein Pflichtfeld.
Arbeitsbereich-ID	Kunden-ID, die zum Aufrufen der Microsoft Azure Log Analytics-REST API verwendet wird.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Event Processor Worker	Anzahl der gleichzeitigen Event-Verarbeitungs-Worker, wobei jeder Worker einen Event-Batch verarbeitet.	4
Worker queue size (Größe der Worker-Warteschlange)	Warteschlangengröße der Event-Prozessor-Worker.	5
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

MID-Server Dateneingabekonfigurationsfelder

Beschreibung der Felder in MID-Server Formular für Dateneingabekonfiguration.

Basiskonfiguration

Feld	Beschreibung
Beschreibung	Beschreibung der Dateneingabe
MID	Der Name des MID-Server Von dem die Protokolle gestreamt werden.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Diese Dateneingabe verwendet MID-Server Dient zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn das Protokoll keine Zeitzone angibt.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Verwerfen von Protokollen, wenn der MID-Server ausgelastet ist	

Konfigurationsfelder für REST-API-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für REST-API-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Webserver	MID-Server, an den die Protokolldaten abgerufen werden. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. Wenn Sie den MID-Server auswählen, werden die Felder **MID** und **Port** automatisch gefüllt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID-Server-Eigenschaften ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet REST zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Rsyslog Dateneingabekonfigurationsfelder , Filebeat oder Winlogbeat

Beschreibung der Felder in Rsyslog Dateneingabekonfigurationsformulare , Filebeat und Winlogbeat.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
Inhaltspaket	(Linux nur mit Filebeat) das zu verwendende Inhaltspaket. Inhaltspakete enthalten Standardquelltypen und Zuordnungsskriptvorlagen. Health Log Analytics Aktiviert das ausgewählte Paket automatisch und verwendet sein Zuordnungsskript für die Zuordnung der Dateneingabequellen. Weitere Informationen finden Sie unter Health Log Analytics Inhaltspakete für kürzere Amortisierungszeit.

Registerkarte „Tagging und Bindung“

Feld	Beschreibung
Pfad	Der vollständige Pfad, aus dem Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. Dies ist ein Pflichtfeld.
Service Instanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Tagging und Bindung“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.
Komponente	Gerätetyp oder Stapelebene als Kontext für die Protokolle, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat. Komponenten stellen normalerweise CIs in der CMDB dar. Mehrere Komponenten werden häufig in einer einzigen Serviceinstanz gruppiert.
Quelltyp	Quelltyp, der definiert, wie Health Log Analytics eine bestimmte Anwendung behandelt und die Protokolldaten analysiert. Beispiel: Tomcat Catalina. Jede Dateneingabe kann je nach Vielfalt ihrer Protokollformate mehrere Quelltypen haben. Serviceinstanzen und -Komponenten können eine beliebige Anzahl von Quelltypen haben.

Erweiterte Konfiguration

Für Rsyslog Dateneingaben:

Formular für erweiterte rsyslog-Konfiguration

Feld	Beschreibung	Standardwerte
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.	
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard,	GMT

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für erweiterte rsyslog-Konfiguration (Fortsetzung)

Feld	Beschreibung	Standardwerte
	wenn im Protokoll keine Zeitzone angegeben ist.	
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	

Für Dateneingaben, die verwenden Beats Service Desk-Mitarbeiter:

Formular für erweiterte Beats-Konfiguration

Feld	Beschreibung	Standardwert
Client inactivity timeout (sec) (Zeitüberschreitung bei Client-Inaktivität (Sek.))	Die Zeitüberschreitung in Sekunden, nach der ein inaktiver Kanal geschlossen wird	15
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Default time zone (Standardzeitzone)	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Systemprotokolle – Dateneingabekonfigurationsfelder abrufen

Beschreibung der Felder in ServiceNow Formular für Dateneingabekonfiguration des Abrufs von Systemprotokollen.

ServiceNow Systemprotokolle – Dateneingabeformularfelder abrufen

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Der Standardwert ist ServiceNow Glide SYS-Protokoll. Dies ist ein Pflichtfeld. **Hinweis:** Health Log Analytics Enthält den Quelltyp Glide_sys_log für Protokolldatenverkehr von ServiceNow Glide-SYS-Protokollserviceinstanz.
Von	Von-Datum und -Uhrzeit für das Lesen der Daten. Die Dateneingabe liest keine Daten, die älter als dieses Datum und diese Uhrzeit sind. Dies ist ein Pflichtfeld.
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Syslog-Tabellenfilter	Die Kriterien, die zum Filtern von Protokolldaten aus der Tabelle „Systemprotokoll“ verwendet werden, bevor sie an die KI-Engine gestreamt werden.

Splunk Dateneingabekonfigurationsfelder

Beschreibung der Felder in Splunk Formular für Dateneingabekonfiguration.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port auf dem MID-Server öffnet. Dies ist ein Pflichtfeld.
Transportprotokoll	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird. • TCP: Bei Verwendung des TCP-Protokolls (Transmission Control Protocol) erreichen alle Protokolle die Instanz. Die Splunk-Pipeline kann jedoch blockiert werden, wenn der MID-Server inaktiv ist oder die Verbindung unterbrochen wird. TCP ist das Standardtransportprotokoll. • UDP: Bei Verwendung des UDP-Protokolls (User Datagram Protocol) wird die Splunk-Pipeline niemals blockiert. Einige Protokolle werden jedoch möglicherweise gelöscht, bevor sie die Instanz erreichen. Weitere Informationen zum Streamen von Protokolldaten mit dem TCP- oder UDP-Transportprotokoll finden Sie im Artikel Streaming Splunk data using Heavy Forwarder: Select TCP or UDP [KB0998928] (Splunk mit Heavy Forwarder streamen: TCP oder UDP auswählen in der Now Support-Knowledge Base).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
Vorbereitete Daten verwenden	Option zum Erfassen von Protokolldaten aus Splunk Im vorverarbeiteten Format („gekocht“) das Splunk Verwendet im Forwarder. Daten werden in erfasst HLA In diesem Format stellt sicher, dass jede Protokollzeile die relevanten kontextbezogenen Informationen enthält, die Splunk Bettet sich darin ein. **Hinweis:** Wenn Sie diese Option auswählen, muss nicht bearbeitet werden Eigenschaften.Konf. Und Transforms.conf Dateien während Splunk Dateneingabekonfiguration.
Zeitzone der Weiterleitung verwenden	Option zum Übergeben von Informationen zur Zeitzone, in der sich der Weiterleitung befindet. Die MID-Server Verwendet diese Informationen, um die Zeitzone anzupassen, aus der die Protokolle ankommen. Diese Option ist relevant, wenn verwendet wird Splunk Universelle Weiterleitungen.
Komprimierung aktivieren	Option zum Senden von Protokollen im komprimierten Format. Durch das Senden von Protokollen in einem komprimierten Format wird die Größe der übertragenen Daten minimiert, was bei der Verarbeitung großer Mengen von Protokolldaten wichtig ist. Diese Option ist relevant, wenn verwendet wird Splunk Universelle Weiterleitungen und können nur verwendet werden, wenn SSL/TLS aktiviert ist.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwerte
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll. **Hinweis:** Um Protokolle in einem komprimierten Format zu senden, muss SSL/TLS aktiviert sein.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwerte
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	

Splunk Konfigurationsfelder der Dateneingabe für Abfrage

Beschreibung der Felder in Splunk Formular für Dateneingabekonfiguration für Abfrage.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
MID	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt.) Der MID-Server, an den die Protokolle gestreamt werden. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Erweiterte Konfiguration

Registerkarte „Transport“

Feld	Beschreibung
Server-URL	Die URL, die für den Zugriff auf verwendet wird Splunk REST-API.
Abfrage	Die Abfrage Splunk Verwendet, um Ihre Daten zu durchsuchen.
Authentifizierungstyp	Der Authentifizierungstyp. • Standardauthentifizierung: Sendet bei jeder HTTP-Anforderung einen Anwendernamen und ein Passwort. Die Standardauthentifizierung ist einfacher als die tokenbasierte Authentifizierung, aber weniger sicher. • Tokenauthentifizierung: Der Client ruft ein Token von einem Authentifizierungsserver ab und verwendet dieses Token zur Authentifizierung bei Splunk.
Splunk Anmeldeinformationsalias Abfragen	Der zu verwendende Anmeldeinformationsalias. Geben Sie ein an Splunk Rufen Sie den Anmeldeinformationsalias ab, indem Sie das Lupensymbol auswählen und dann entweder einen vorhandenen Anmeldeinformationsalias aus auswählen **Aliasse Für Verbindungen Und Anmeldeinformationen** Liste oder Auswahl **Neu** Zum Erstellen eines neuen Datensatzes. Der ausgewählte Anmeldeinformationsalias kann eine Anmeldeinformation für die Standardauthentifizierung und eine Anmeldeinformation für die Token-Authentifizierung enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
	Informationen zum Erstellen eines Anmeldeinformationsalias finden Sie unter Anmeldeinformationsaliasse für Discovery .
Von	Datum und Uhrzeit, ab der Splunk Durchsucht die Daten.
An	Datum und Uhrzeit, bis zu der Splunk Durchsucht die Daten.

Registerkarte „Erweitert“

Feld	Beschreibung
Max. Anzahl von Dokumenten pro Abfrage	Die maximale Anzahl von Dokumenten, die jedes Mal abgerufen werden, wenn Protokolldaten aus abgerufen werden Splunk. Standard: 10,000.
Splunk Zeitüberschreitung bei Anforderung (Sekunden)	Die maximale Zeit in Sekunden, die für den Datenabruf zulässig ist, bevor die Anforderung abläuft.

Konfigurationsfelder für TCP-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für TCP-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
MID	Der MID-Server, an den die Protokolle gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Senden der Protokolldaten. Rsyslog und Splunk senden Daten mit dem TCP-Protokoll.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.	
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	
Trennzeichen für Trennlinien	Das Zeilenumbruchzeichen, das die Rohprotokollzeilen trennt. Trennwerte müssen durch ein Komma gefolgt von einem Leerzeichen getrennt werden: „, “. Beispiel: „\r, \n, , splitHere, #“.	

Konfigurationsfelder für UDP-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für UDP-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
MID	Der MID-Server, an den die Protokolle gestreamt werden. **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Senden der Protokolldaten: UDP.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Quotengrenze	Begrenzung der Anzahl der Ereignisse pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	false

Vector Agent-Dateneingabekonfigurationsfelder

Beschreibung der Felder im Eingabekonfigurationsformular für Vector Agent-Daten.

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	Die MID-Server An den die Vector Agent-Protokolle gestreamt werden. Dies ist ein Pflichtfeld. **Hinweis:** Wenn MID-Server Ist ausgefallen oder die Verbindung ist unterbrochen, kann die Vektor-Pipeline blockiert werden.
Port	Der Port auf der MID-Server Wird zum Abhören von Protokollen verwendet. Dies ist ein Pflichtfeld. Wählen Sie einen Port im Bereich von 6000 bis 6200 aus.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Derzeit ist nur TCP verfügbar.
Status	Status der Dateneingabe

Beschreibungen des Integrationskonfigurationsfelds

Dieser Abschnitt enthält Beschreibungen der Felder in den Integrationskonfigurationsformularen für Health Log Analytics.

Apache Kafka Integrationskonfigurationsfelder

Beschreibung der Felder in Apache Kafka Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine Kafka-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID-Server-Name	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server, von dem die Protokolldaten aus Apache Kafka abgerufen werden. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können die maximale Anzahl ändern, indem Sie die Eigenschaft hinzufügen sn.occ.log_ingestion.max_datainput_per_MID Zu MID-Server Und dann ändern Sie den Standardwert. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Datenquelle	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Kafka. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode festlegen

Feld	Beschreibung
Kafka-Knotennamen	Kommagetrennte Liste im Format HOST:PORT,HOST:PORT. Dies ist ein Pflichtfeld. Die Liste muss nicht alle Server des Apache Kafka-Clusters enthalten.
Themen	Kommagetrennte Liste von Themen, die die Dateneingabe abonnieren muss. Dies ist ein Pflichtfeld.
Kafka-Anmeldeinformationen	Die Apache Kafka Anmeldeinformationen. Sie können vorhandene Kafka-SSL-Anmeldeinformationen auswählen oder neue erstellen, indem Sie auswählen **Erstellen Sie Kafka-Anmeldeinformationen** Aus der Dropdown-Liste. Eine Beschreibung der Felder im Formular „Kafka SSL-Anmeldeinformationen“ finden Sie unter Kafka SSL-Anmeldeinformationen – Felder.
Gruppen-ID	Name der Apache Kafka-Verbrauchergruppe.

Erweiterte Einstellungen

Feld	Beschreibung	Standardwert
Zeitüberschreitung	Zeit in Millisekunden, die beim Abruf gewartet wird, wenn in den Themen keine Daten verfügbar sind.	500
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.	GMT
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Zeichencodierung	Zeichencodierung für diese Dateneingabe Dieses Feld ist schreibgeschützt.	UTF-8

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung	Standardwert
Zeitüberschreitung bei Knoten-Discovery	Zeit in Millisekunden vor dem Ablaufen der Knotenerkennung.	30
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	Falsch

AWS Firehose Integrationskonfigurationsfelder

Beschreibung der Felder in AWS Firehose Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine Firehose-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre Instanz verwendet wird: Amazon CloudWatch Protokolle. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Konfigurationsfelder der Cribl-Integration

Beschreibung der Felder in den Konfigurationsformularen der Cribl-Integration für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine Cribl-Integration. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
MID-Server-Name	Die MID-Server An den die Cribl-Protokolle gestreamt werden. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Dies ist ein Pflichtfeld. Wählen Sie einen Port im Bereich 6000-6200 aus dem Array aus. Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port im öffnet MID-Server.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Transport (für Push-Integrationen)	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: TCP. Dieses Feld ist schreibgeschützt.
Quelle (für Abrufintegrationen)	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Cribl. Dieses Feld ist schreibgeschützt.

Verbindung einrichten

Feld	Beschreibung
Cribl-URL	Die URL der Cribl-Instanz. Dies ist ein Pflichtfeld. HLA Verwendet diese URL, um die Verbindung mit der Cribl-Instanz herzustellen und die erforderlichen API-Aufrufe durchzuführen. Zum Beispiel: • Vor Ort: https://my-cribl.company.com:9000 • Cloud: https://myorg-12345abcde.cribl.cloud • Sandbox: https://sandbox-xyz789.sandbox.cribl.io
Authentifizierungsmethode	Die von der Cribl-Integration verwendete Authentifizierungsmethode. Dies ist ein Pflichtfeld. Die Cribl-Integration unterstützt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindung einrichten (Fortsetzung)

Feld	Beschreibung
	• Token-basierte Authentifizierung: Erforderlich für Cribl Cloud und wird auch für selbst gehostete (lokale) Cribl-Instanzen unterstützt. • Standardauthentifizierung: Bevorzugt für selbst gehostete (lokale) Cribl-Instanzen. Beide Authentifizierungsmethoden verwenden den standardmäßigen Anmeldeinformationsalias: Cribl_Credential_Alias. Informationen zum Einrichten von Anmeldeinformationen für die von der Cribl-Integration verwendete Authentifizierungsmethode finden Sie unter Richten Sie Anmeldeinformationen für die Authentifizierung für die Cribl-Integration in ein Health Log Analytics. **Wichtig:** Stellen Sie sicher, dass unter dem Anmeldeinformationsalias nur ein aktiver Anmeldeinformationsdatensatz jedes Anmeldeinformationstyps vorhanden ist.
Worker-Gruppe	Die Cribl-Mitarbeitergruppe, von der Protokolldaten an die Instanz gestreamt werden sollen. Dies ist ein Pflichtfeld. In der Dropdown-Liste werden Mitarbeitergruppen basierend auf der angegebenen Cribl-Cloud-Instanz-URL und Authentifizierungsmethode angezeigt. Zum Beispiel: • Standard • entwicklungs-Worker • prod-Worker • Staging-Worker
Cribl-Route	Die Cribl-Route, die Protokolldaten an ein bestimmtes Ziel weiterleitet. Dieses Feld wird automatisch mit einer Dropdown-Liste aller verfügbaren Routen ausgefüllt, die jeweils mit einem Standardziel konfiguriert sind. Wählen Sie die gewünschte Route aus der Liste aus. Dies ist ein Pflichtfeld. Zum Beispiel: • Standard • Demo-Route
Cribl-Ziel	Das Cribl-Ziel, an das die Protokolldaten weitergeleitet werden. Dieses Feld wird automatisch ausgefüllt und ist schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindung einrichten (Fortsetzung)

Feld	Beschreibung
	Wenn HLA Füllt dieses Feld aus und stellt einen Link zum Ziel auf dem Cribl-Server bereit. Beispiel: sn_hla_cribl_tcp_JSON_abcdef

Elasticsearch Integrationskonfigurationsfelder

Beschreibung der Felder in Elasticsearch Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Mein Elasticsearch Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein Spezifisch MID-Server Cluster.
MID-Server-Name	(Nur wenn **Ausführen am** Ist auf spezifisch festgelegt MID-Server) Die MID-Server An, von dem Daten protokolliert werden Elasticsearch Indizes werden abgerufen. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt Spezifisch MID-Server Cluster) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Dies ist ein Pflichtfeld. Wenn Sie einen Cluster auswählen, wird die MID Servers Im ausgewählten Cluster und deren Status werden angezeigt. Die Integration wird auf einem einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Integrationsaufgaben zu den nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster im Integrationsformular auswählen, wird der verwendet MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Wenn Elasticsearch Verwendet Client-Zertifikat- oder CA-Zertifikat-Authentifizierung, alle MID Servers Im Cluster muss über die entsprechenden Zertifikate verfügen. • Die standardmäßige maximale Anzahl von Integrationen, die Protokolle zu einem einzelnen streamen MID-Server Ist 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Integrationen, auch wenn dies der Fall ist MID-Server Ist ausgefallen.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie einen Serviceinstanz Und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.
Datenquelle	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Elastisch. Dieses Feld ist schreibgeschützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Datenabrufmethode

Feld	Beschreibung
Server-URL	Die URL, die für den Zugriff auf den Cluster verwendet wird. Dies ist ein Pflichtfeld.
Authentifizierungsmethode	Die Authentifizierungsmethode, mit der die Integration authentifiziert wird Elasticsearch. Der Standardwert ist „keine“. Wenn Sie die Authentifizierungsmethode auswählen, werden die entsprechenden Anmeldeinformationsfelder im Formular angezeigt. **Hinweis:** Als Administrator können Sie eine Authentifizierungsmethode erstellen, indem Sie zu navigieren **Alle** > **Health Log Analytics** > **Authentifizierungsmethoden** Und auswählen **Neu** .
Indexpräfix	Präfix, das den Namen von vorangestellt ist Elasticsearch Indizes, aus denen Sie Daten lesen möchten. Die Integration liest nur Daten aus Indizes, die dem konfigurierten Präfix entsprechen. Beispiel: Network-Logs-* entspricht Indizes wie Network-Logs-2024.01.01. Dies ist ein Pflichtfeld. Diese Einstellung stellt das sicher HLA Erfasst nur Daten aus den relevanten Indizes. Beispiel: Only-read-this-indices-*
Zeitstempelfeld des Dokuments	Zeitstempelfeld in Dokumenten, die in den Leseindizes gespeichert sind. Dies ist ein Pflichtfeld.
Format des Zeitstempelfelds	Format des Zeitstempelfelds in den Dokumenten. Wenn kein Format angegeben ist, wird das standardmäßige Unix-Epochenzeitformat in Millisekunden verwendet. Beispiel: 1684168407 (15. Mai 2023 4:33:27 PM)
Begriffsfilter	JSON-Zuordnung der zu filternden Begriffe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode (Fortsetzung)

Feld	Beschreibung
	Hinweis: Vermeiden Sie die Verwendung von Begriffsabfragen für Textfelder. Wenn das Zielfeld sowohl als Text als auch als Stichwort zugeordnet ist, referenzieren Sie das Stichwort mit feldname.stichwort. Beispiel: {"severity": ["error", "warning"]}

Erweiterte Einstellungen

Feld	Beschreibung
Max. Anzahl von Verbindungen pro Route	Die maximale Anzahl von Verbindungen, die pro Knoten geöffnet werden sollen.
Max. Bildlaufsegmente	Die Anzahl der Shards, die für den relevanten Index in konfiguriert sind Elasticsearch. Diese Zahl gibt Elastic an, wie viele parallele Abfragen in jeder Abfrageanforderung ausgeführt werden sollen.
Proxy-Host	Hostname des HTTP-Proxys, über den Anforderungen gesendet werden.
Proxy-Port	Port des HTTP-Proxy, über den Anforderungen gesendet werden
MID-Zertifikatrichtlinienprüfung verwenden	Option zum Aktivieren der Prüfung der MID-Zertifikatsrichtlinie. Wählen Sie diese Option aus, wenn Sie die Protokolle mit SSL/TLS verschlüsselt senden möchten. Navigieren Sie dann zu **Alle** > **MID-Server** > **MID-Sicherheitsrichtlinie** Und fügen Sie der Tabelle die MID-Zertifikatrichtlinienprüfung hinzu. Weitere Informationen finden Sie unter Richtlinien für die Zertifikatprüfung des MID-Servers .
Cross-Cluster-Suche verwenden	Option für die Suche nach Daten in Elasticsearch Cluster. Wenn dieses Kontrollkästchen aktiviert ist, wird **Cluster, die gesucht werden sollen** Feld wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	Hinweis: Ihre Einstellungen in **Verwenden Sie minimale Berechtigungen** Kontrollkästchen und **Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)** Feld auf der **Erweiterte Konfiguration** Das Formular wirkt sich auf die Erfassung von Daten in mehreren Clustern aus.
Cluster für Suche	Die Elasticsearch Cluster, die gesucht werden sollen.dieses Feld wird nur angezeigt, wenn **Verwenden Sie die clusterübergreifende Suche** Das Kontrollkästchen ist aktiviert. Führen Sie einen der folgenden Schritte aus: • Lassen Sie dieses Feld leer, oder geben Sie „*“ ein, um alle in definierten Remote-Cluster zu durchsuchen Elasticsearch. • Geben Sie die Cluster an, die in einer kommagetrennten Liste gesucht werden sollen. **Hinweis:** Um auch den lokalen Cluster zu durchsuchen, fügen Sie ein Komma am Anfang oder Ende hinzu, oder fügen Sie der Liste zwei Kommas hintereinander hinzu. Beispiel: „East,,West“ oder „,East,West“ oder „*,“
Minimale Berechtigungen verwenden	Option zum direkten Lesen von Protokolldaten aus Elasticsearch Indizes mit dem konfigurierten Präfix. • Wenn diese Option ausgewählt ist, liest die Integration die Protokolldaten direkt aus Elasticsearch Indizes mit dem konfigurierten Präfix. Zum Ausführen dieser Aufgabe sind nur Leseberechtigungen erforderlich. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist und Sie die clusterübergreifende Suche verwenden, werden Daten aus allen Clustern gleichzeitig erfasst. • Wenn diese Option deaktiviert ist, ruft die Integration alle Indizes mit dem Präfix ab, filtert sie und liest die Protokolldaten aus den gefilterten Indizes. Die Ausführung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	dieser Aufgabe erfordert zusätzliche Berechtigungen. **Hinweis:** Wenn Sie dieses Kontrollkästchen deaktivieren, wirkt sich die Verwendung der clusterübergreifenden Suche darauf aus, wie Daten aus den Clustern erfasst werden. Weitere Informationen finden Sie unter Aktivieren und Verwenden der clusterübergreifenden Suche für Elasticsearch-Dateneingaben in Health Log Analytics [KB1556079] artikel in Now Support Knowledge Base. Für zusätzliche Informationen zum Streaming von Protokollen mit Elasticsearch Integration, siehe Protokolle mithilfe der Elasticsearch-Dateneingabe streamen – Erweiterter Leitfaden [KB1080162] artikel in Now Support Knowledge Base.
Max. Anzahl von Dokumenten pro Abfrage	Maximale Anzahl von Dokumenten, die in einer einzelnen Abfrage abgerufen werden
Tie-Breaker mit Bildlauf in Scheiben	Wert, der zum Teilen der Daten verwendet wird. Jeder Teil wird parallel gescrollt. Standard: _id
Tiebreaker für nicht zunächst auf Suche beschränkt	Eindeutiger Wert pro Dokument, der beim Sortieren von Protokolleinträgen nach Zeitstempel als Tiebreaker verwendet werden soll.
Search-after-API verwenden	Option für das Wechseln zwischen Sliced-Scrolling- und Search-after-APIs. **Hinweis:** Sliced-Scrolling-APIs sind beim Lesen historischer Daten vorzuziehen, während Search-after-APIs besser zum Lesen von Echtzeitdaten geeignet sind.
Zeitsuffixformat für Index	Format des Zeitsuffix bei Verwendung von zeitbasierten Indexnamen, z. B. [logstash-]JJJJ.MM.TT. Wenn Sie Aliasse verwenden, lassen Sie dieses Feld leer. Beispiel: Uuu.mm.tt
Datenlese-Zeitüberschreitung (Millisekunden)	Dauer in Millisekunden, bevor eine Anforderung an den Elasticsearch-Cluster abläuft
Intervall für Index-Discovery (Sekunden)	Die Anzahl der Sekunden zwischen intermittierenden MID-Server-Anforderungen an den Elasticsearch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	Cluster für neue Indizes, aus denen Daten gelesen werden sollen.
Scroll-Kontextzeit (Millisekunden)	Lebensdauer des erstellten Scroll, wenn die Scroll-API zum Lesen von Daten aus Elasticsearch verwendet wird. Weitere Informationen finden Sie in der Elasticsearch Dokumentation zur Scroll API .
Event Processor Worker	Maximale Anzahl von CPU-Kernen, die parallel zur Verarbeitung von aus Elasticsearch abgerufenen Events verwendet werden. Eine höhere Einstellung erhöht den Dateneingabedurchsatz auf Kosten einer höheren CPU-Auslastung.
Größe der Worker-Warteschlange	Maximale Anzahl von Stapeln, die zur Verarbeitung in die Warteschlange gestellt werden. Eine höhere Einstellung erhöht den Durchsatz auf Kosten einer höheren RAM-Auslastung.
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Ruheintervall (Sekunden)	Intervall der Wartzeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Daten zurückgegeben hat
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte
Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)	Die Anzahl der Sekunden vor der aktuellen Abfragezeit, um verzögerte Daten einzubeziehen.die konfigurierte Anzahl von Sekunden wird vom aktuellen Zeitpunkt für das Lesen des letzten Zeitstempels subtrahiert. **Hinweis:** Wenn dieser Wert 0 ist und Daten aus mehreren Clustern gleichzeitig erfasst werden, enthält die Abfrage möglicherweise keine Daten, die mit einer Verzögerung an einem der Cluster gesendet wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Abfrageintervall	Wie häufig das System nach neuen Protokolldaten abfragt.

Microsoft Azure Event Hubs Integrationskonfigurationsfelder

Beschreibung der Felder in Microsoft Azure Event Hubs Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Integration meiner Ereignis-Hubs. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Quelle	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Pubsub. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID-Server-Name	(Nur wenn **Ausführen am** Ist auf bestimmten MID-Server festgelegt.) Der MID-Server, an den die Protokolle gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur auswählen MID-Server Mit Protokollerfassungsfunktion, die die Standardauthentifizierung unterstützt. MID Servers Diese Support-mTLS sind nicht aufgeführt. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.

Datenabrufmethode festlegen

EreignisHubs-Namespace	Bereichscontainer für den/die Event-Hub(s). Dies ist ein Pflichtfeld.
Event Hub-Name	Der Event-Hub, aus dem Protokolldaten abgerufen werden sollen. Dies ist ein Pflichtfeld.
Consumer Group name (Verbrauchergruppenname)	Zu verwendende Verbrauchergruppe. Dies ist ein Pflichtfeld. Der Standardwert ist $Standard.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode festlegen (Fortsetzung)

Authentifizierungsmethode	Der Anmeldeinformationsalias ServiceNowVerwendet, um auf die Ereignis-Hubs zuzugreifen. Dies ist ein Pflichtfeld. **Hinweis:** Sie können der Liste der verfügbaren Aliasse weitere Anmeldeinformationsaliasse hinzufügen, aus denen Sie auswählen können, indem Sie auswählen **Verwalten Sie Anmeldeinformationsaliasse** Aus der Liste und Hinzufügen eines Anmeldeinformationsalias.

Erweiterte Einstellungen

Feld	Beschreibung
Restore point rate (Rate für Wiederherstellungspunkt)	Die Anzahl der Protokolle, die die Integration lesen kann, bevor ein Wiederherstellungspunkt gespeichert wird.
Processor threads count (Anzahl der Prozessor-Threads)	Gesamtanzahl der Prozessor-Threads.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Protokolle. Diese Einstellung bestimmt die Anzahl der zu gruppierenden Protokolle, von denen eines verworfen wird. Verringert die Anzahl der abgerufenen Protokolle. Der Standardwert ist -1: Es werden keine Protokolle verworfen. Wenn Sie beispielsweise eine Abmeldung von fünf ablegen möchten, ändern Sie den Wert in 5.
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Protokolle. Diese Einstellung bestimmt die Anzahl der Protokolle, die gruppiert werden sollen, von denen eines empfangen wird. Dadurch wird die Anzahl der empfangenen Protokolle reduziert. Der Standardwert ist -1, was bedeutet, dass keine Protokolle empfangen werden. Wenn Sie beispielsweise von fünf abmelden möchten, ändern Sie den Wert in 5.
Zeitüberschreitung bei Vorgang (Sekunden)	Anzahl der Sekunden, die gewartet werden soll, bevor Event-Hub-Vorgänge ablaufen.
Leerlauf-Zeitüberschreitung empfangen (Sekunden)	Anzahl der Sekunden, die gewartet werden soll, bevor Empfangsvorgänge ablaufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32766.
Prefetch count (Anzahl der Vorabrufe)	Die Anzahl der Protokolle, die vor Ereignis-Hubs-Vorgängen empfangen wurden.
Max. Batchgröße	Maximale Anzahl von Events, die an einen einzelnen Prozessaufruf übergeben werden. Der Standardwert ist 100.
Standardzeitzone	Die Standardzeitzone von Protokollen. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist. Der Standardwert ist GMT.
Zeichencodierung	Die Zeichencodierung für diese Integration. Der Standardwert ist UTF-8.
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.

Microsoft Azure Log Analytics Integrationskonfigurationsfelder

Beschreibung der Felder in Microsoft Azure Log Analytics Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine Azure Log Analytics-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID-Server-Name	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server, von dem die Protokolldaten aus Microsoft Azure Log Analytics abgerufen werden. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Integrationen, die Protokolle zu einem einzelnen streamen MID-Server Ist 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.
MID MID-Server Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Datenquelle	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Azure Log Analytics. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode festlegen

Feld	Beschreibung
Umleitungs-URL	Die Weiterleitungs-URL der Zugriffsprotokollanwendung. Dies ist ein Pflichtfeld. Die URL bezieht sich auf Microsoft Azure Autorisierungseigenschaft „Redirect_URI“. Weitere Informationen finden Sie im Abschnitt Autorisierungscode-URL (GET-Anforderung) im Microsoft Azure-Dokumentation .
Authentifizierungsmethode	Die Anmeldeinformationen, die für den Zugriff auf Microsoft Azure-Ressourcen verwendet werden. Dies ist ein Pflichtfeld. Wenn keine Anmeldeinformationen vorhanden sind, wählen Sie aus **Erstellen Sie neue Azure-Serviceprinzipalanmeldeinformationen** . Erstellen Sie Anmeldeinformationen, indem Sie die Felder ausfüllen und dann auswählen **Übermitteln** . Für Informationen zu **Mandanten-ID** , **Client-ID** , Und **Geheimer Schlüssel** Felder finden Sie unter Microsoft Azure-Dokumentation . Wenn Sie Anmeldeinformationen erstellt haben, können Sie sie aus der Dropdown-Liste auswählen.
Arbeitsbereich-ID	Kunden-ID, die zum Aufrufen der Microsoft Azure Log Analytics-REST API verwendet wird. Dies ist ein Pflichtfeld.
Tabellenname	Der Name der Tabelle in Microsoft Azure Log Analytics Wo die Dateneingabe die Protokolldaten abruft. Weitere Informationen finden Sie im Abschnitt Tabelleninformationen anzeigen in Microsoft Azure-Dokumentation . Dies ist ein Pflichtfeld.
Name der Eigenschaft für die Ereigniszeit	Das Microsoft Azure Log Analytics-Feld, in dem die Events-Zeit erkannt werden soll. Dies ist ein Pflichtfeld.

Erweiterte Einstellungen

Feld	Beschreibung
Ereignis-Prozessor-Worker	Anzahl der gleichzeitigen Event-Verarbeitungs-Worker, wobei jeder Worker einen Event-Batch verarbeitet.
Größe der Worker-Warteschlange	Warteschlangengröße der Event-Prozessor-Worker.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.
Max. Anzahl von Dokumenten pro Abfrage	Die höchste Anzahl von Zeilen, die in jeder Abfrage abgerufen werden.
Spaltenauswahl	Kommagetrennte Liste der Spaltennamen, die zurückgegeben werden sollen. **Hinweis:** Dieses Feld wird ignoriert, wenn Sie eine benutzerdefinierte Abfrage angeben.
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Ruheintervall (Sekunden)	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.

Protokollabfrage	Option zum Definieren einer eigenen Log Analytics Abfrage. Dieses Feld überschreibt die Werte, die in den anderen Abfrageeinstellungsfeldern konfiguriert sind.
	Hinweis: Wenn dieses Feld leer ist, Health Log Analytics Generiert die Abfrage anhand der in den anderen Feldern festgelegten Werte.
	Verwenden Sie für Ihre anwenderdefinierte Abfrage das folgende JSON-Format:
	`{"query": „Query | Where timeGenerated > %s | Take 500"}`
	Zum Beispiel:
	`{ "query":"ContainerLog | where LogEntry contains 'cartservice' | where TimeGenerated > %s | take 500",`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	"workspaces": ["defaultworkspace-3ab145ff-f9cd-433f-8533-d1b1ee24aee6-eus"], "project": ["TimeGenerated", "LogEntry", "LogEntrySource"] }

MID-Server Integrationskonfigurationsfelder

Beschreibung der Felder in MID-Server Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
MID-Server-Name	Der Name des MID-Server Von dem die Integration Protokollnachrichten sammelt und an die Instanz streamt. **Hinweis:** Sie können nur eine erstellen MID-Server Integration pro verfügbar MID-Server. Wenn vorhanden MID-Server Integration oder Dateneingabe verwendet dasselbe MID-Server, Sie können keine zusätzliche erstellen MID-Server. Dies ist ein Pflichtfeld.
Integrationsname	Der Name der Integration. Wenn Sie auswählen MID-Server Name, dieses Feld wird automatisch mit dem ausgewählten ausgefüllt MID-Server. Dieses Feld ist schreibgeschützt.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. Standardmäßig ist sie auf festgelegt ServiceNow MID-Server. **Hinweis:** Dieses Feld ist nur für verfügbar MID-Server Integrationen, die in Version 36.0.17 oder höher erstellt wurden.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen

Feld	Beschreibung
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events Der Standardwert ist -1.
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events Der Standardwert ist -1.
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32.766.
Zeichencodierung	Zeichencodierung für diese Dateneingabe Der Standardwert ist UTF-8.
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.

Konfigurationsfelder der REST-API-Integration

Beschreibung der Felder in den Konfigurationsformularen der REST-API-Integration für Health Log Analytics.

Hinweis: REST API-Integrationen unterstützen nur die UTF-8-Codierung für eingehende Daten.

Registerkarte „Details angeben“

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine REST-API-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
MID-Webserver	Der zu verwendende MID-Webserver. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details angeben“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine Serviceinstanz Und fügen Sie CIs (Configuration Items) hinzu. Legen Sie den Status der neuen Serviceinstanz auf betriebsbereit fest.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: REST. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
MID-Server-Name	Die MID-Server An den die Protokolldaten übertragen werden. Dieses Feld wird automatisch ausgefüllt, wenn der MID-Webserver ausgewählt wird. Es ist schreibgeschützt.
Port	Port für den MID-Server. Dieses Feld ist schreibgeschützt. Wird automatisch ausgefüllt, wenn der MID-Webserver ausgewählt wird.

ServiceNow Konfigurationsfelder der Systemprotokolle-Abruf-Integration

Beschreibung der Felder in ServiceNow Konfigurationsformular für Systemprotokolle-Abruf-Integration für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Integration meiner Systemprotokolle. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. Die Standardserviceinstanz für diese Integration ist ServiceNow Systemprotokolle.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk Konfigurationsfelder der Poller-Integration

Beschreibung der Felder in Splunk Konfigurationsformulare für Poller-Integration für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
Ausführen auf	Option zum Auswählen, ob ein bestimmtes verwendet werden soll MID-Server Oder ein MID-Server Cluster.
MID-Server-Name	(Nur wenn **Ausführen am** Feld ist auf bestimmten MID-Server festgelegt) MID-Server, von dem die Protokolldaten aus Splunk abgerufen werden. Dies ist ein Pflichtfeld. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.
MID-Server-Cluster	(Nur wenn **Ausführen am** Ist auf festgelegt MID-Server Cluster.) Die MID-Server Cluster, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen ausgeführt MID-Server Im Cluster bis dahin MID-Server Schlägt fehl. Das System verschiebt dann alle Dateneingabeaufgaben

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	in die nächsten verfügbaren Aufgaben MID-Server Im Cluster gemäß der konfigurierten Reihenfolge. **Hinweis:** • Health Log Analytics Unterstützt nur Failover MID-Server Cluster. In diesen Clustern mehrere MID Servers Sind für den Failover-Schutz gruppiert. Wenn Sie einen Cluster aus dem Dateneingabeformular auswählen, wird der MID-Server Die Clusterliste zeigt nur Failover-Cluster an. • Die MID-Server Cluster darf nur enthalten MID Servers Die die Standardauthentifizierung unterstützen. MTLs werden für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden aktiviert sein MID-Server Im Cluster. Wenn die Protokollerfassung für den aktiven nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn er mindestens einen enthält MID-Server Mit weniger als 10 Dateneingaben, selbst wenn dies der Fall ist MID-Server Ist ausgefallen. Weitere Informationen zu finden MID-Server Cluster, siehe Konfigurieren Sie einen MID-Server-Cluster . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Datenquelle	Die Quelle der Protokolldaten, die die Integration an Ihren abruft ServiceNow Instanz: Splunk. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode festlegen

Feld	Beschreibung
URL des REST API-Servers	Die URL, die für den Zugriff auf verwendet wird Splunk REST-API. Dies ist ein Pflichtfeld. **Hinweis:** • Standardmäßig ist Splunk DER REST-API-Endpunkt ist auf Port 8089 verfügbar. Daher der Standardendpunkt für Splunk REST-API ist: `http://<splunk-server>:8089` . • Der REST-API-Endpunkt unterscheidet sich vom Front-End-Endpunkt.
Authentifizierungsmethode	Der zu verwendende Anmeldeinformationsalias. Dies ist ein Pflichtfeld. Die Splunk Die Integration verwendet Anmeldeinformationsaliasse anstelle direkter Verweise auf Anmeldeinformationen für die Authentifizierung. Die Anmeldeinformationsaliasse werden nach Typ aufgelistet: Aliasse, die Anmeldeinformationen für die Standardauthentifizierung enthalten, und solche, die Anmeldeinformationen für die Token-Authentifizierung enthalten. Wenn ein Alias beide Anmeldeinformationstypen enthält, wird er in beiden Kategorien angezeigt. Sie können auswählen **Verwalten Sie Anmeldeinformationsaliasse** Um Ihre Anmeldeinformationsaliasse zu verwalten und neue in zu erstellen **Aliasse Für Verbindungen Und Anmeldeinformationen** Liste.
Abfrage	Die Abfrage Splunk Verwendet, um Ihre Daten zu durchsuchen. Dies ist ein Pflichtfeld. Zum Beispiel die Abfrage `sourcetype="adc_Access_log"` Weist an Splunk Poller-Integration zum Abrufen aller Protokolle mit dem Quelltyp „adc_Access_log“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen

Feld	Beschreibung
Max. Anzahl von Dokumenten pro Abfrage	Die maximale Anzahl von Dokumenten, die jedes Mal abgerufen werden, wenn Protokolldaten aus abgerufen werden Splunk. Standard: 10,000.
Splunk Zeitüberschreitung bei Anforderung (Sekunden)	Die maximale Zeit in Sekunden, die für den Datenabruf zulässig ist, bevor die Anforderung abläuft.

Splunk Konfigurationsfelder für TCP-Integration

Beschreibung der Felder in Splunk TCP-Integrationskonfigurationsformulare für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Mein Splunk TCP-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
MID-Server-Name	MID-Server, von dem die Protokolldaten aus Splunk abgerufen werden. Dies ist ein Pflichtfeld. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.
Port	Port für den MID-Server. Dies ist ein Pflichtfeld. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port im öffnet MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: TCP. Dieses Feld ist schreibgeschützt.
Vorbereitete Daten verwenden	Option zum Erfassen von Protokolldaten aus Splunk Im vorverarbeiteten Format („gekocht“) das Splunk Verwendet im Forwarder. Daten werden in erfasst HLA In diesem Format stellt sicher, dass jede Protokollzeile die relevanten kontextbezogenen Informationen enthält, die Splunk Bettet sich darin ein.

Erweiterte Einstellungen

Feld	Beschreibung
SSL/TLS verwenden	Option zum Auswählen der Verwendung von SSL/TLS zur Verbesserung der Datensicherheit und des Schutzes. **Hinweis:** SSL/TLS muss aktiviert sein, wenn Sie Protokolle in einem komprimierten Format senden möchten.
Hostnamen suchen	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen. Der Standardwert ist „falsch“
Zeitzone der Weiterleitung verwenden	Option zum Übergeben von Informationen zur Zeitzone, in der sich der Weiterleitung befindet. Die MID-Server Verwendet diese Informationen, um die Zeitzone anzupassen, aus der die Protokolle ankommen. Diese Option wird angezeigt, wenn **Gearbeitete Daten Verwenden** Ist ausgewählt. Dies ist relevant, wenn verwendet wird Splunk Universelle Weiterleitungen.
Komprimierung aktivieren	Option zum Senden von Protokollen im komprimierten Format. Durch das Senden von Protokollen in einem komprimierten Format wird die Größe der übertragenen Daten minimiert, was

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	bei der Verarbeitung großer Mengen von Protokolldaten wichtig ist. Diese Option wird angezeigt, wenn **Gearbeitete Daten Verwenden** Und **Verwenden Sie SSL/TLS** Sind ausgewählt. Dies ist relevant, wenn verwendet wird Splunk Universelle Weiterleitungen.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu löschenden Protokolle. Der Standardwert ist -1: Es werden keine Protokolle verworfen. Beispiel: Wenn eines von fünf Protokollen verworfen werden soll, ändern Sie den Wert in 5.
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Protokolle. Der Standardwert ist -1: Es werden keine Protokolle empfangen. Beispiel: Wenn eines von fünf Protokollen empfangen werden soll, ändern Sie den Wert in 5.
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32766.
Zeichencodierung	Zeichencodierung für diese Dateneingabe Der Standardwert ist UTF-8.
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.

Splunk Konfigurationsfelder der UDP-Integration

Beschreibung der Felder in Splunk UDP-Integrationskonfigurationsformulare für Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Mein Splunk UDP-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
MID-Server-Name	MID-Server, von dem die Protokolldaten aus Splunk abgerufen werden. Dies ist ein Pflichtfeld. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für die ausgewählte nicht aktiviert ist MID-Server, Health Log Analytics Aktiviert es automatisch.
Port	Port für den MID-Server. Dies ist ein Pflichtfeld. **Hinweis:** Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port im öffnet MID-Server.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: UDP. Dieses Feld ist schreibgeschützt.

Erweiterte Einstellungen

Feld	Beschreibung
Hostnamen suchen	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen. Der Standardwert ist „falsch“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Protokolle. Der Standardwert ist -1: Es werden keine Protokolle empfangen. Beispiel: Wenn eines von fünf Protokollen empfangen werden soll, ändern Sie den Wert in 5.
Zeichencodierung	Zeichencodierung für diese Dateneingabe Der Standardwert ist UTF-8. Dieses Feld ist schreibgeschützt.
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu löschenden Protokolle. Der Standardwert ist -1: Es werden keine Protokolle verworfen. Beispiel: Wenn eines von fünf Protokollen verworfen werden soll, ändern Sie den Wert in 5.
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32766.
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.

Konfigurationsfelder für TCP-Integration

Beschreibung der Felder in den Konfigurationsformularen der TCP-Integration für Health Log Analytics.

Registerkarte „Details angeben“

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine TCP-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
MID-Server-Name	Der MID-Server, an den die Protokolle gestreamt werden. Dies ist ein Pflichtfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details angeben“ (Fortsetzung)

Feld	Beschreibung
	• Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.
Port	Port für den MID-Server. Dies ist ein Pflichtfeld. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: TCP. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Erweiterte Einstellungen

Feld	Beschreibung
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.
Hostnamen suchen	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden
Lesezeitüberschreitung in Sekunden	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.
Trennzeichen für Trennlinien	Das Zeilenumbruchzeichen, das die Rohprotokollzeilen trennt. Trennwerte müssen durch ein Komma gefolgt von einem Leerzeichen getrennt werden: „, “. Beispiel: „\r, \n, , splitHere, #“.

Konfigurationsfelder der UDP-Integration

Beschreibung der Felder in den UDP-Integrationskonfigurationsformularen für Health Log Analytics.

Registerkarte „Details angeben“

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Beispiel: Meine UDP-Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den von Ihnen eingegebenen Namen angepasst.
MID-Server-Name	Der MID-Server, an den die Protokolle gestreamt werden. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details angeben“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.
Serviceinstanz	Die Serviceinstanz (früher der Anwendungsservice), an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server. Dies ist ein Pflichtfeld. Der Port muss im Bereich von 6000 bis 6200 liegen. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port im öffnet MID-Server.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an verwendet wird ServiceNow Instanz: UDP. Dieses Feld ist schreibgeschützt.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.

Erweitert

Feld	Beschreibung
Standardzeitzone	Die Zeitzone der Ereignisse, die das System verwendet, wenn in einem Protokoll die Zeitzone nicht angegeben ist. Standardmäßig verwendet das System in solchen Fällen GMT, Sie können jedoch eine andere Zeitzone angeben.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events Der Standardwert ist -1.
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events Der Standardwert ist -1.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweitert (Fortsetzung)

Feld	Beschreibung
Quotengrenze	Begrenzung der Anzahl der Ereignisse pro Sekunde, die diese Dateneingabe verarbeitet. Der Standardwert ist -1.
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32.766.
Zeichencodierung	Zeichencodierung für diese Dateneingabe Der Standardwert ist UTF-8. Dieses Feld ist schreibgeschützt.
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.

Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics

Die **Übersicht** Registerkarte hilft Ihnen, komponentenbasierte Warnungen zu verstehen, Log Analytics Warnungen, und Log Analytics Warnungsgruppen.

Informationen auf der Registerkarte Übersicht für eine komponentenbasierte Warnung

Die Warnung **Übersicht** Registerkarte in Health Log Analytics Hilft Ihnen zu verstehen Komponentenbasierte Warnungen.

Abschnitte auf der Registerkarte Übersicht für eine komponentenbasierte Warnung

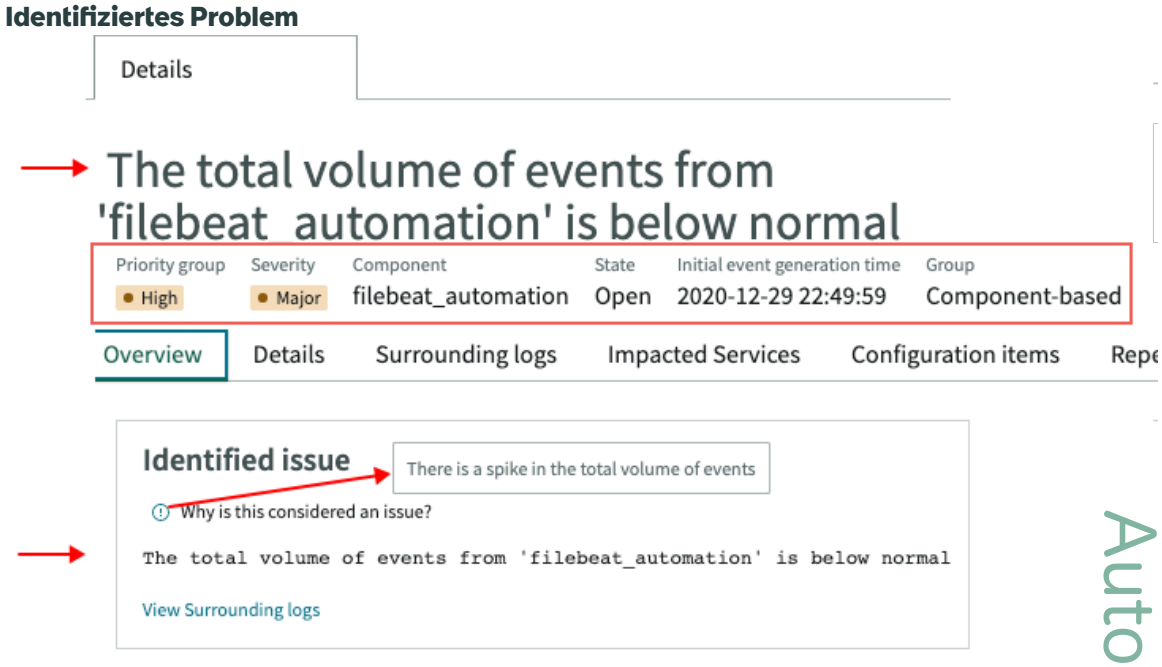
Eine detaillierte Beschreibung von Komponentenbasierte Warnungen finden Sie unter Typen von Health Log Analytics Warnungen.

Identifiziertes Problem

Das „identifizierte Problem“ hat zur Warnung geführt. Das Problem wird im Titel der Warnung und auf einer Karte auf der Registerkarte angezeigt. Informationen zur Warnung werden im Banner angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Klicken Sie auf das Informationssymbol (ⓘ), um zu sehen, wie das Problem identifiziert wurde.
- Klicken Sie auf **Umgebende Protokolle anzeigen**, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Analysieren Sie Protokollzeilen um die Anomalie, um die Ursache zu finden.

Configuration Items

Um Einzelheiten zu den CIs anzuzeigen, die der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Configuration Items** oder auf **View more** (Mehr anzeigen) im Abschnitt „Configuration Items“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Anomaly (Anomalie)

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

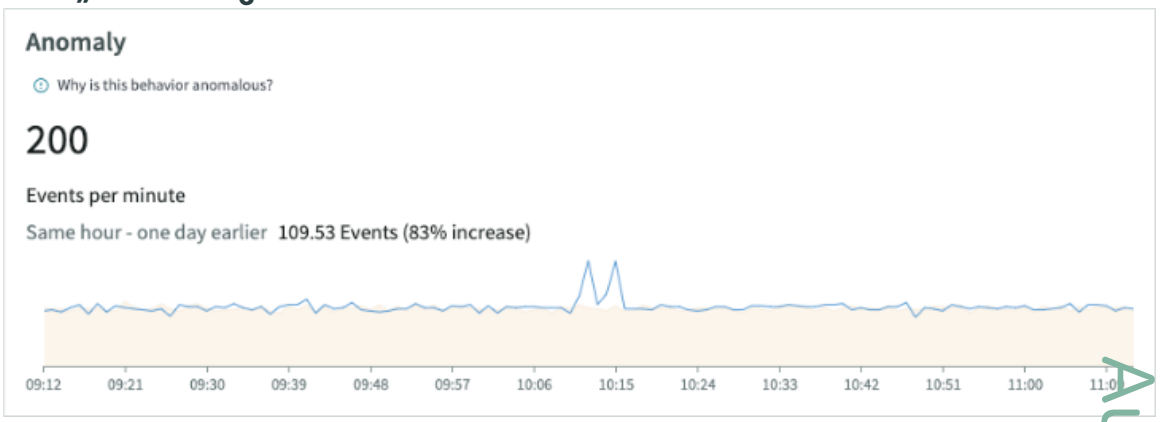
- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

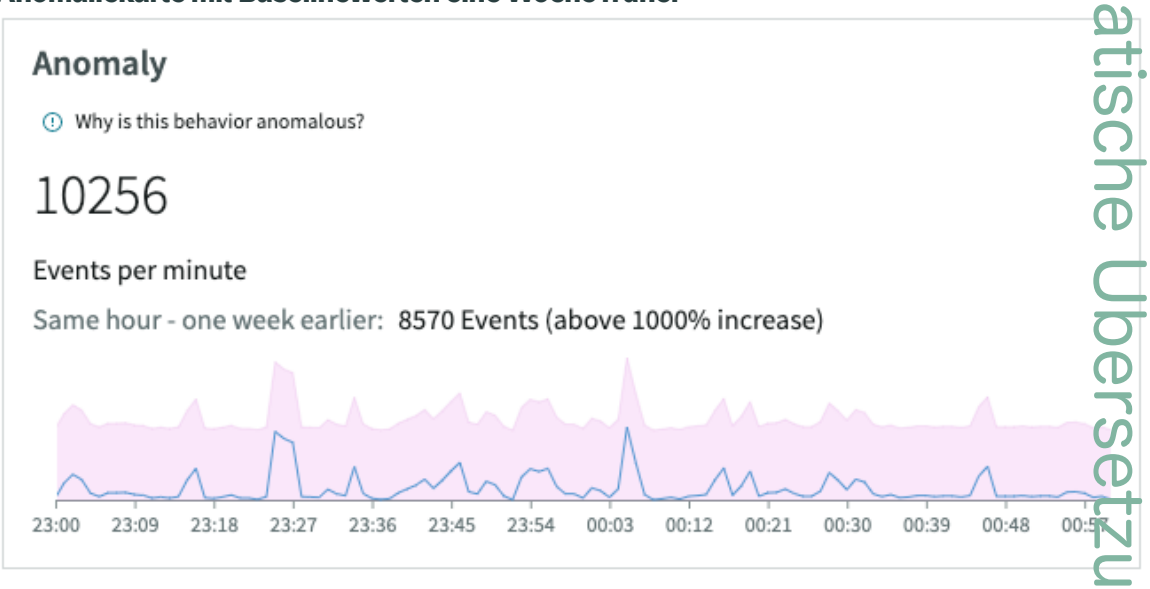
In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Der rosa schattierte Bereich in diesem Beispiel zeigt die Baselinewerte für die gleiche Stunde in der vorherigen Woche an.

Anomaliekarte mit Baselinewerten eine Woche früher



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Typen von anomalem Verhalten in Health Log Analytics.

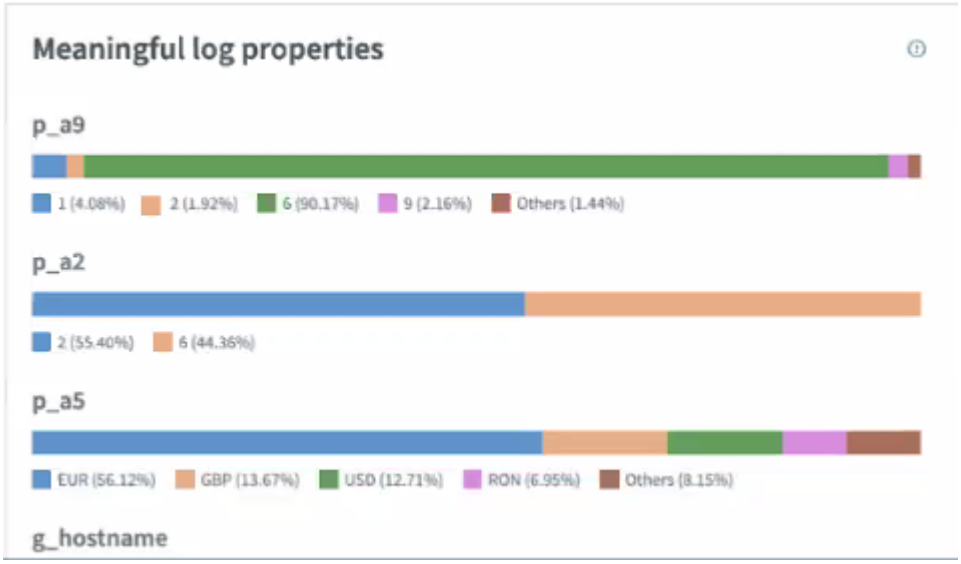
Aussagekräftige Protokolleigenschaften

Auf der Karte Aussagekräftige Protokolleigenschaften zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt. Für die Eigenschaft `p_a5` im Beispiel wurde der Wert *EUR* in 56,12 % der Protokollzeilen gefunden, *GBP* in 13,67 % usw.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

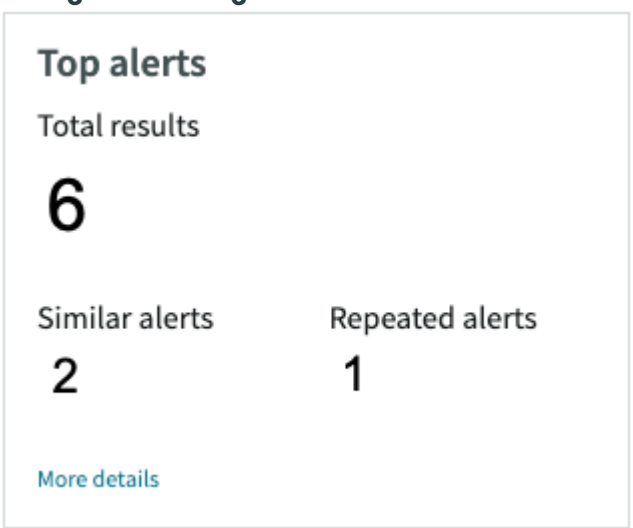
Aussagekräftige Protokolleigenschaften



Häufigste Warnungen

Die Karte „Häufigste Warnungen“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Ähnliche Warnungen** und **Wiederholte Warnungen**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Alert Insight – Ähnliche Warnungen** zu öffnen. Details finden Sie unter Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“.

Häufigste Warnungen



Häufigste Incidents

Die Karte „Häufigste Incidents“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Incidents für CI** und **Incidents bei zugehörigen CIs**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Incidents für CI** zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufigste Incidents

Informationen auf der Registerkarte Übersicht für einen Log Analytics Gruppe

Die Warnung **Übersicht** Registerkarte in Health Log Analytics Hilft Ihnen zu verstehen Log Analytics-Gruppen.

Abschnitte auf der Registerkarte Übersicht für Log Analytics Gruppen

Eine detaillierte Beschreibung von Log Analytics-Gruppen finden Sie unter Typen von Health Log Analytics Warnungen.

Korrelationsbanner

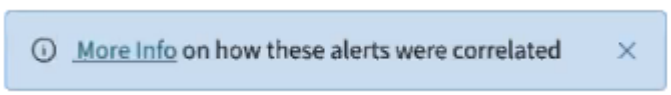
Während der ersten Analyse werden Warnungen bewertet. Jede Korrelation in Protokolldaten einer Warnung mit einer anderen Warnung trägt zur Punktzahl einer Warnung bei. Je höher die Punktzahl, desto wahrscheinlicher ist es, dass die Warnung als Log Analytics-Warnung in eine Log Analytics-Warnung aufgenommen wird.

Die folgenden Arten von Daten werden berücksichtigt, wenn untersucht wird, ob Warnungen miteinander in Beziehung stehen:

- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Klicken Sie auf **Weitere Informationen** Link im Banner „Korrelationen“, um die Liste der Korrelationen anzuzeigen, die sich auf die Log Analytics-Warnungen beziehen.

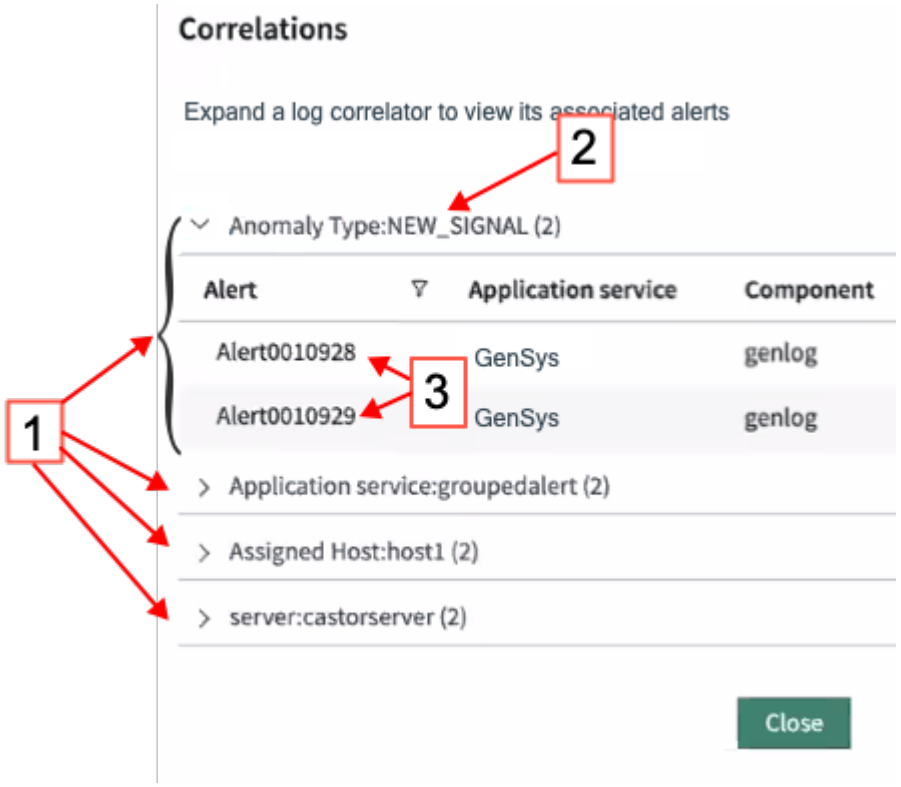
Korrelationsbanner



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationen



1. Liste der Korrelationen: Die erste Korrelation in der Liste wird erweitert, um die einzelnen korrelierten Log Analytics-Warnungen und anzuzeigen ProtokollkorrelatorDie die Warnungen teilen. Die Zahl in Klammern ist die Anzahl der Warnungen in der Korrelation.
2. Ein einzelner Protokollkorrelator: Der Bezeichner für eine Gruppe korrelierter Log Analytics-Warnungen. Die Warnungen werden nach den Protokollzeilendaten oder Metadaten gruppiert, die den Warnungen gemeinsam sind (z. B. IP-Adresse, Hostname oder Anwendername). Die Zahl in Klammern ist die Anzahl der miteinander in Beziehung stehenden Warnungen.
3. Protokollieren Sie Analytics-Warnungen, die korreliert sind.

Warnungen in Gruppe

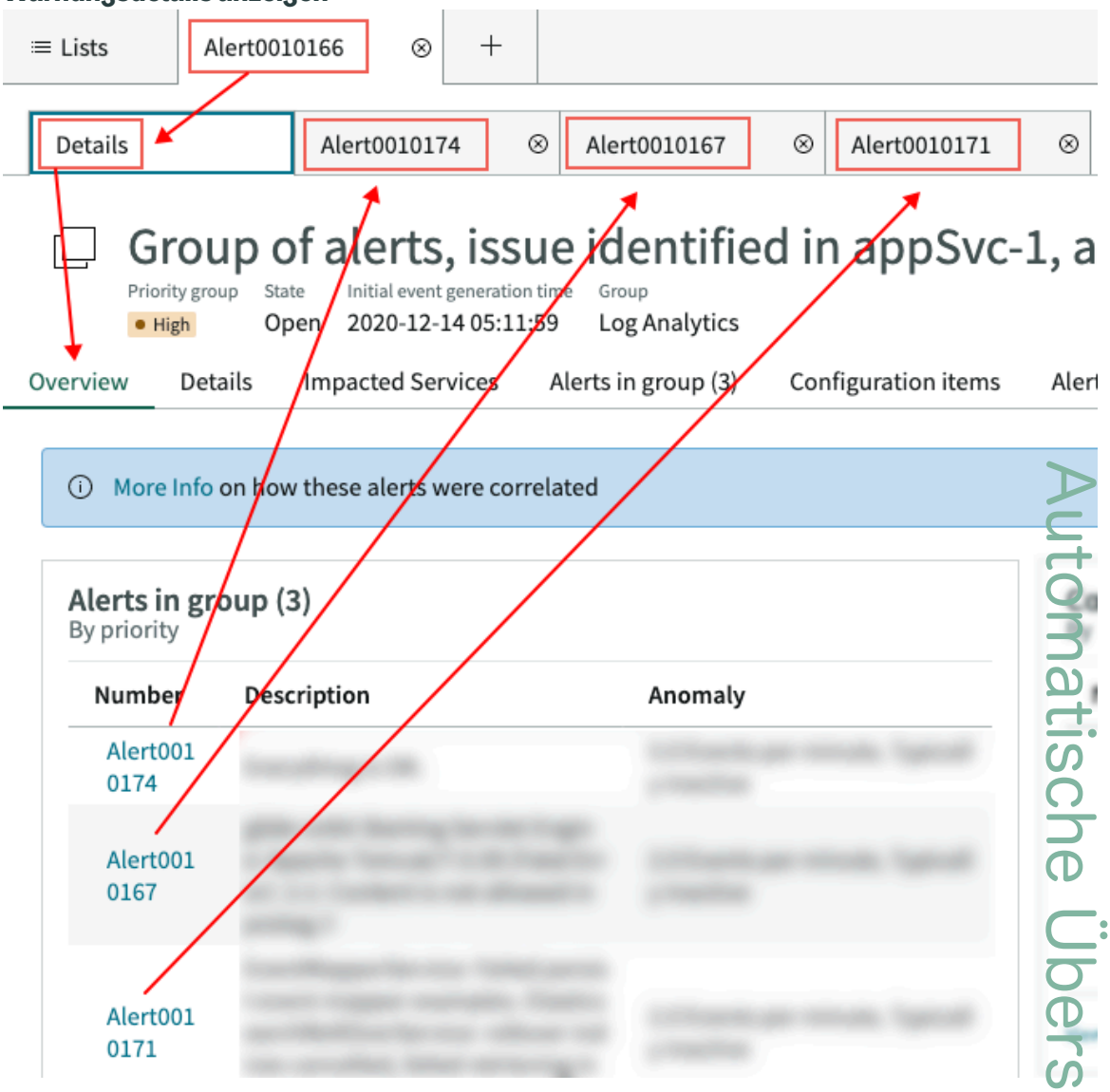
Für eine Log Analytics-Warnung (im Beispiel „Alert0010166“) werden im Abschnitt „Warnungen in Gruppe“ die Log Analytics-Warnungen angezeigt, die unter der Log Analytics-Warnung gruppiert sind.

Klicken Sie auf eine Log Analytics-Warnung, um die zugehörigen Details anzuzeigen. Um die vollständige Liste der Log Analytics-Warnungen anzuzeigen, klicken Sie auf **Weitere anzeigen** Oder klicken Sie auf **Warnungen in Gruppe** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsdetails anzeigen



Automatische Übersetzung

Configuration Items

Um detailliertere Informationen zu den Konfigurationselementen (CIs) anzuzeigen, die der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Konfigurationselemente** oder auf **Mehr anzeigen** im Abschnitt „Konfigurationselemente“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Log Analytics Warnungen auf der Registerkarte Warnungen in Gruppe

In der Tabelle wird beschrieben Log Analytics Warnungen in einem Log Analytics Gruppe in **Warnungen in Gruppe** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Alerts in group“ (Warnungen in Gruppe)

Spalte	Beschreibung
Anzahl	Die Nummer der Warnung, die in der Liste der Warnungen auf angezeigt wird Dashboard des Operator-Arbeitsbereichs. Um detaillierte Informationen für eine Warnung auf der Registerkarte **Details** anzuzeigen, klicken Sie auf die Warnungsnummer. Dieses Feld wird automatisch festgelegt.
Gruppe	Typ der Gruppe, zu der die Warnung gehört: Eine eigenständige Log Analytics-Warnung oder ein Komponentenbasierte Warnung.
Beschreibung	Anomales Muster oder anomale Metrik, die die Generierung der Warnung verursacht haben.
Schweregrad	Schweregradwert für die Warnung. Verfügbare Werte: • **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. • **Schwerwiegend**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert. • **Gering**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor. • **Warnung**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. • **Info**: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. • **Löschen oder Gelöst**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Prioritätsgruppe, die die Reihenfolge angibt, in der Warnungen gelöst werden sollen. Die Auswahlmöglichkeiten lauten wie folgt: • **Dringend** • **Hoch** • **Mittel** • **Niedrig**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Alerts in group“ (Warnungen in Gruppe) (Fortsetzung)

Spalte	Beschreibung
	Der Wert der Prioritätsgruppe ist wichtiger als der Schweregrad allein. Beispielsweise sollte eine Warnung mit hoher Priorität und niedrigem Schweregrad vor einer Warnung mit niedriger Priorität und hohem Schweregrad behandelt werden. Informationen zur Berechnung der Priorität finden Sie unter Warnungspriorität.
Status	Verarbeitungsstatus der Warnung. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status lauten wie folgt: • **Erneut öffnen**: Eine zuvor geschlossene Warnung wurde erneut geöffnet und erfordert Ihre Aufmerksamkeit. • **Flatternd**: Die Warnung erhält identische Events, die mit hoher Häufigkeit aus derselben Quelle eintreffen. Dieser Status kann dazu führen, dass eine Warnung aus dem Status „Geschlossen“ erneut geöffnet wird, was zu einer Anhäufung von Changes mit den Status „Offen“ und „Geschlossen“ führt. • **Geschlossen**: Die Warnung wurde geschlossen und erfordert keine weitere Aktion. Sie schließen eine Warnung, wenn sie behoben wurde.
Konfigurationselement	CI in der CMDB. Das CI wird von der Warnung angewendet.
Knoten	Knotenfeld, das in der Protokollnachricht empfangen wurde. Das in der Protokollnachricht beschriebene Event ist auf diesem Knoten aufgetreten. Oft ist der Knoten der Name des CI, das der Warnung zugeordnet ist. Zum Beispiel ein Computername, eine IP-Adresse, ein FQDN oder eine MAC-Adresse.
Quelle	Alle Log Analytics Warnungen haben den Wert **Log Analytics** In **Quelle** Spalte, um dies anzugeben Health Log Analytics Die Warnung wurde generiert.
Metrikname	Name der Metrik, deren anomales Verhalten zu der Warnung geführt hat. Zum Beispiel die *`I/O request`*Wenn die E/A-Anforderung länger als 15000 ms dauerte.
Aktualisiert	Zeitpunkt der letzten Aktualisierung der Informationen oder des Status der Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen auf der Registerkarte Übersicht für einen Log Analytics Warnung

Die Warnung **Übersicht** Registerkarte in Health Log Analytics Hilft Ihnen zu verstehen Log Analytics-Warnungen.

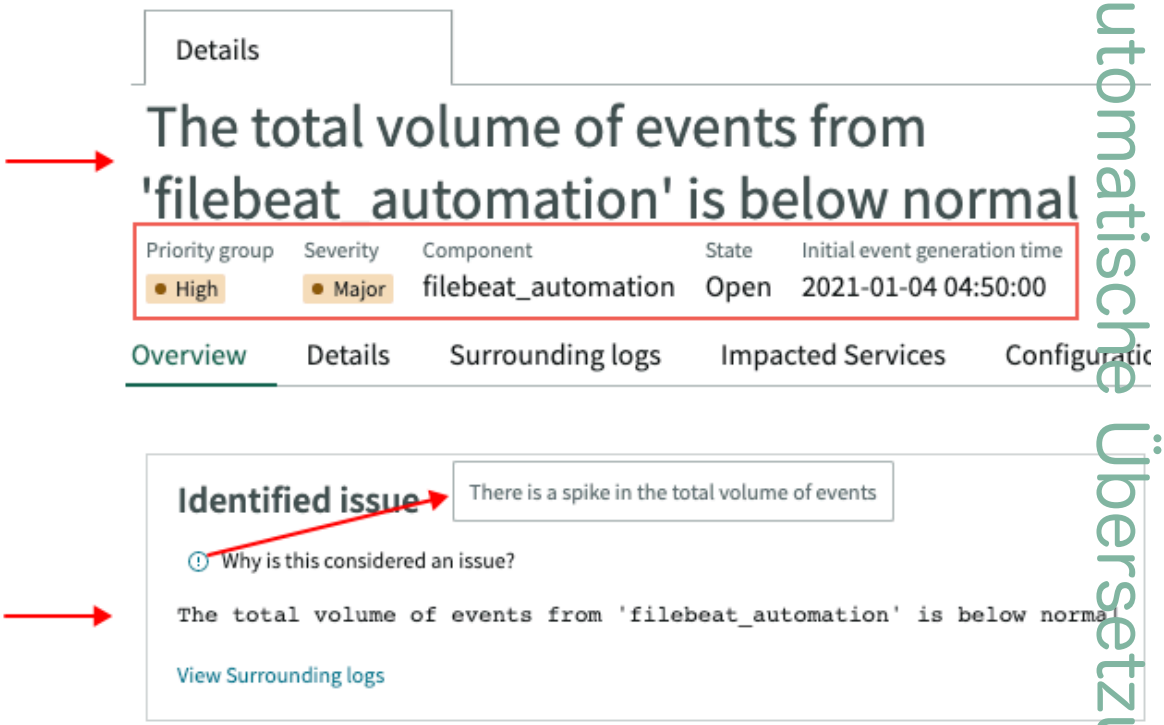
Abschnitte und Karten auf der Registerkarte Übersicht für Log Analytics Warnungen

Für eine detaillierte Beschreibung von Log Analytics-Warnungen, Siehe Typen von Health Log Analytics Warnungen.

Identifiziertes Problem

Das „identifizierte Problem“ hat zur Warnung geführt. Das Problem wird im Titel der Warnung und auf einer Karte auf der Registerkarte angezeigt. Informationen zur Warnung werden im Banner angezeigt.

Identifiziertes Problem



- Klicken Sie auf das Informationssymbol (ⓘ), um zu sehen, wie das Problem identifiziert wurde.
- Klicken Sie auf **Umgebende Protokolle anzeigen**, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Analysieren Sie Protokollzeilen um die Anomalie, um die Ursache zu finden.

Configuration Items

Um Einzelheiten zu dem CI anzuzeigen, das der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Configuration Items** oder auf **View more** (Mehr anzeigen) im Abschnitt „Configuration Items“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Anomaly (Anomalie)

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

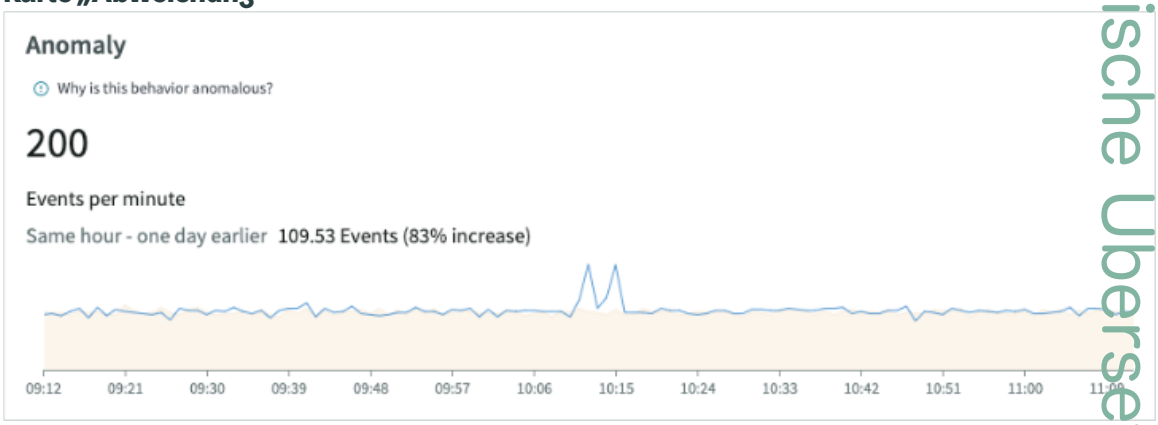
- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“

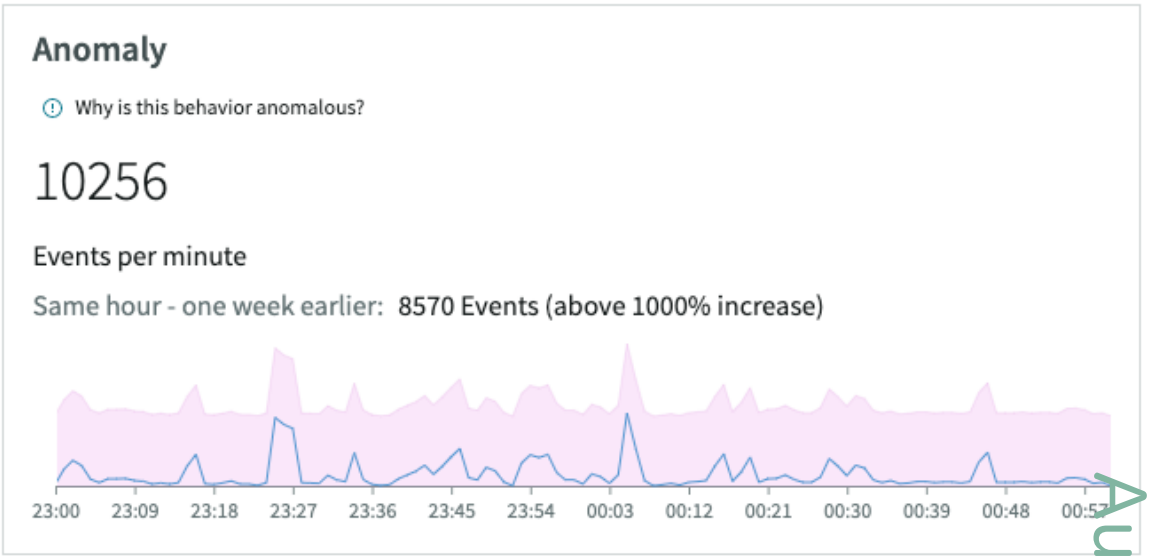


Der rosa schattierte Bereich in diesem Beispiel zeigt die Baselinewerte für die gleiche Stunde in der vorherigen Woche an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anomaliekarte mit Baselinewerten eine Woche früher

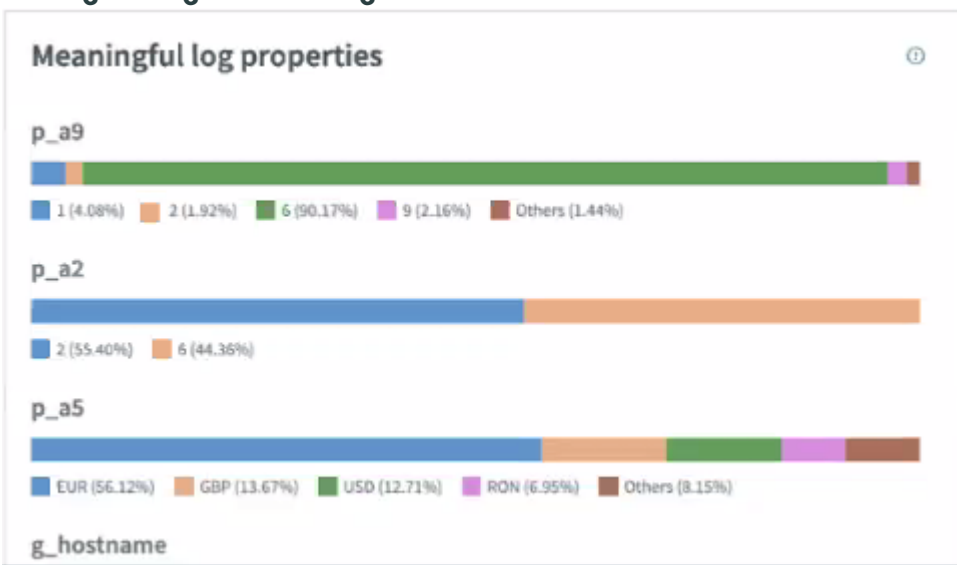


Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Typen von anomalem Verhalten in Health Log Analytics.

Aussagekräftige Protokolleigenschaften

Auf der Karte Aussagekräftige Protokolleigenschaften zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt. Für die Eigenschaft *p_a5* im Beispiel wurde der Wert *EUR* in 56,12 % der Protokollzeilen gefunden, *GBP* in 13,67 % usw.

Aussagekräftige Protokolleigenschaften



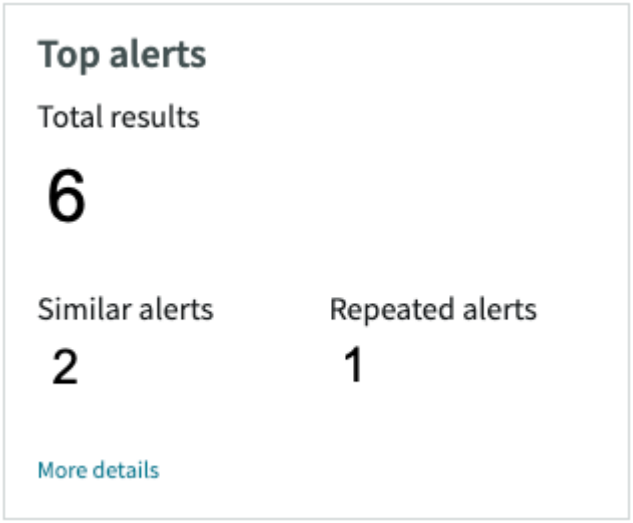
Häufigste Warnungen

Die Karte „Häufigste Warnungen“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Ähnliche Warnungen** und **Wiederholte Warnungen**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Alert Insight – Ähnliche Warnungen** zu öffnen. Details finden Sie unter Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufigste Warnungen



Häufigste Incidents

Die Karte „Häufigste Incidents“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Incidents für CI** und **Incidents bei zugehörigen CIs**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Incidents für CI** zu öffnen.

Häufigste Incidents

Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“

Zeigen Sie die Liste der Warnungen an, die auf der Registerkarte **Alert Insight – Ähnliche Warnungen** von der Alert Insight-Funktion bereitgestellt werden. Die Alert Insight-Funktion generiert die Informationen, die Sie bei der Lösung der Warnung unterstützen.

Registerkarte „Alert Insight – Ähnliche Warnungen“

Die Registerkarte enthält Informationen über andere Warnungen, die in den letzten 30 Tagen generiert wurden und die denselben CI-Typ, dieselbe Quelle, dieselbe Ressource, denselben Metriknamen usw. aufweisen.

Service Operations-Arbeitsbereich Stellt eine kontextbezogene Warnungsselektierung basierend auf Daten von bereit IT Service Management(ITSM), z. B. aus Incidents, Change-Anforderungen und Problemen. Die Funktion Alert Insight hilft Ihnen, die Ursache zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ermitteln, und empfiehlt eine Lösung. Mit dem intelligenten Start im Kontext können Sie eine der folgenden Aktionen ausführen:

- Anwendung starten
- Browser mit einer angegebenen URL öffnen
- Fehlerkorrektur durchführen (basierend auf Orchestrierung)
- Subflow starten (Workflow basierend auf Flow Designer)

Felder der Registerkarte „umgebende Protokolle“

In diesem Abschnitt werden die Informationen beschrieben, die im angezeigt werden **Umgebende Protokolle** Registerkarte.

Registerkarte „Umgebende Protokolle“

Spalte	Beschreibung
Uhrzeit	Zeitstempel der Protokollzeile im Format, das die Quelle verwendet. Wenn kein Wert angezeigt wird, überprüfen Sie die Quelltypstruktur der Rohdaten.
Anwendungsservice	Serviceinstanz, in der die Metrik gefunden wurde.
Komponente	Logische Komponente von Service Instanz , die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Nachricht	Interne Nachricht aus Protokollzeile in Rohform, die den Text der vom System generierten Protokollnachricht über die Art des Vorkommens enthält.
Ebene	Typ des Events. Die verfügbaren Werte sind in der Reihenfolge ihrer Bedeutung: • **Notfall** • **Warnung** • **Kritisch** • **Fehler** • **Warnung** • **Hinweis** • **Informativ** • **Debuggen**
Host	Hostbezeichner aus der Protokollzeile, bestehend aus dem Hostnamen oder der IP-Adresse des Endpunkts.
Protokollnachricht	Die Rohprotokollnachricht ohne Header.

Protokollbetrachter-Tabellenfelder

In diesem Abschnitt werden die Informationen beschrieben, die in angezeigt werden **Protokoll-Viewer** Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollbetrachter-Tabellenfelder

Spalte	Beschreibung
Zeit	Zeitstempel der Protokollzeile im Format, das die Quelle verwendet. Wenn kein Wert angezeigt wird, überprüfen Sie die Quelltypstruktur der Rohdaten.
Serviceinstanz	Serviceinstanz, in der die Metrik gefunden wurde.
Komponente	Logische Komponente von Service Instanz , die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Nachricht	Interne Nachricht aus Protokollzeile in Rohform, die den Text der vom System generierten Protokollnachricht über die Art des Vorkommens enthält.
Ebene	Typ des Events. Die verfügbaren Werte sind in der Reihenfolge ihrer Bedeutung: • **Notfall** • **Warnung** • **Kritisch** • **Fehler** • **Warnung** • **Hinweis** • **Informativ** • **Debuggen**
Host	Hostbezeichner aus der Protokollzeile, bestehend aus dem Hostnamen oder der IP-Adresse des Endpunkts.
Protokollnachricht	Die Rohprotokollnachricht ohne Header.

Hinweis: Die Spalte „Rohnachricht“ wird standardmäßig nicht in der Tabelle „Protokoll-Viewer“ angezeigt. Sie können diese Spalte anzeigen, indem Sie sie aus der auswählen **Filter** Bereich. Weitere Informationen finden Sie unter Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics.

Formularfelder für Protokollkorrelatoren

In diesem Abschnitt werden die Felder im Formular „Korrelatoren protokollieren“ beschrieben.

Formular „Korrelatoren protokollieren“

Feld	Beschreibung
Typ	Typ des Protokollkorrelators. Es gibt folgende Optionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Korrelatoren protokollieren“ (Fortsetzung)

Feld	Beschreibung
	• **Freitextkorrelator** : Der Protokollkorrelator analysiert Text in der Protokollnachricht. • **Protokollschlüssel-Korrelator** : Der Protokollkorrelator analysiert Protokollmetadaten. Zum Beispiel der Name einer Serviceinstanz in Ihrer Infrastruktur. Protokolleigenschaftskorrelatoren sind spezifisch für den Geschäftskontext Ihrer Umgebung. Weitere Informationen finden Sie unter Identifizierung zugehöriger Warnungen in Protokolldaten mithilfe von Protokollkorrelatoren.
Freitextbegriff oder Bezeichner	Text, den der Protokollkorrelator beim Analysieren von Protokollzeilen isoliert. Die Bezeichnung für dieses Feld lautet **Freitextbegriff** Für Freitext-Protokollkorrelatoren und **Bezeichner** Für Protokolleigenschaftskorrelatoren. **Hinweis:** Der Wert dieses Felds kann der Text für jeden Protokollkorrelator-Typ sein. Daher lautet die Bezeichnung für diese Spalte in der resultierenden Liste der Protokollkorrelatoren **Korrelationsindikator** .
Aktiv	Option zum Anwenden des Protokollkorrelators. Wenn Sie dieses Feld auswählen, wendet das System den Protokollkorrelator auf den Protokollstream an.
Analyseumfang	Satz von Quellen, deren Protokolldaten von diesem Protokollkorrelator analysiert werden. Die Auswahlmöglichkeiten lauten wie folgt: • **Alle Quellen** : Der Protokollkorrelator wird auf Protokollzeilen aus allen Quellen im Datenstrom angewendet. • **Nur neue Quellen** : Der Protokollkorrelator wird auf Protokollzeilen aus allen Quellen angewendet, die nach der Aktivierung dieses Protokollkorrelators erstellt wurden. • **Angegebene Quelle** : Der Protokollkorrelator wird nur auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Korrelatoren protokollieren“ (Fortsetzung)

Feld	Beschreibung
	die Protokollzeilen aus der Quelle angewendet, die Sie in diesem Formular angeben.
Ausgeschlossene Quellen	Quellen, die vom Protokollkorrelator ausgeschlossen sind. Das System analysiert keine Protokollzeilen aus Quellen, die in diesem Feld aufgeführt sind. **Hinweis:** Dieses Feld gilt nur, wenn das Feld **Analyseumfang** auf **Alle Quellen** oder **Nur neue Quellen** gesetzt ist. Informationen zum Ausschließen einer Quelle aus einem Protokollkorrelator finden Sie unter Quellen aus einem Protokollkorrelator ausschließen.
Quelle	Quelle des Protokollkorrelators. Der Protokollkorrelator analysiert die Daten dieser Protokollquelle. Dieses Feld wird nur angezeigt, wenn Sie den Protokollkorrelator aus dem Formular „Protokollquellen“ hinzufügen. Das Feld wird automatisch auf die Protokollquelle festgelegt, an der Sie arbeiten.

Protokollbasierte CI-Kandidatenfelder in Health Log Analytics

Feldbeschreibungen für die Tabelle „Log-Based CI Candidates“ (Protokollbasierte CI-Kandidaten), das Formular „Log-Based CI Candidate“ (Protokollbasierter CI-Kandidat) und das Formular „Add CI candidate to CMDB“ (CI-Kandidaten der CMDB hinzufügen).

Tabelle „Log-based CI candidates“ (Protokollbasierte CI-Kandidaten)

Feld	Beschreibung
Host-Name	Der Hostname, den Health Log Analytics in den Protokolldaten erkannt hat.
CI-Klassentyp	Der in den Protokolldaten erkannte CI-Klassentyp. Der CI-Klassentyp wird durch den Dateneingabetyp bestimmt: • Rsyslogs – CI-Klassentyp: Linux-Server • Linux-Filebeat – CI-Klassentyp: Linux-Server • Windows Filebeat – CI-Klassentyp: Windows Server • Winlogbeat – CI-Klassentyp: Windows-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Log-based CI candidates“ (Protokollbasierte CI-Kandidaten) (Fortsetzung)

Feld	Beschreibung
Zeit des letzten Protokolls	(Schreibgeschützt) Das letzte Mal, dass dieser Host in den Protokolldaten gefunden wurde.
Vorgang	(Schreibgeschützt) Vorgeschlagene Aktion: Hinzufügen – Fügt das CI der CMDB hinzu.
Status	(Schreibgeschützt) Der Status des vorgeschlagenen Aktion. • Ausstehend – Es wurde keine Aktion ausgeführt. • Wenn die ausgeführte Aktion fehlgeschlagen ist, enthält dieses Feld eine Fehlermeldung.

Formular „Log-based CI candidate“ (Protokollbasierter CI-Kandidat)

Feld	Beschreibung
CI-Klassentyp	Der in den Protokolldaten erkannte CI-Klassentyp. Der CI-Klassentyp wird durch den Dateneingabetyp bestimmt: • Rsyslogs – CI-Klassentyp: Linux-Server • Linux-Filebeat – CI-Klassentyp: Linux-Server • Windows Filebeat – CI-Klassentyp: Windows Server • Winlogbeat – CI-Klassentyp: Windows-Server
CI-Name	Der Hostname, den Health Log Analytics in den Protokolldaten erkannt hat.
Vorgang	(Schreibgeschützt) Vorgeschlagene Aktion: Hinzufügen – Fügt das CI der CMDB hinzu.
Zeit des letzten Protokolls	(Schreibgeschützt) Das letzte Mal, dass dieser Host in den Protokolldaten gefunden wurde.
Status	(Schreibgeschützt) Der Status der vorgeschlagenen Aktion: • Ausstehend – Es wurde keine Aktion ausgeführt. • Wenn die ausgeführte Aktion fehlgeschlagen ist, enthält dieses Feld eine Fehlermeldung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Add CI candidate to CMDB“ (CI-Kandidaten der CMDB hinzufügen) (Linux-Server)

Feld	Beschreibung
Name	Name des CI
Asset-Tag	Alphanumerische Informationen zum Nachverfolgen des mit dem CI verknüpften Assets.
Hersteller	Hersteller des Geräts
Asset	(Schreibgeschützt) Das dem CI zugeordnete Asset.
Klasse	Die Asset-Gruppe. Zum Beispiel Linux-Server.
Kommentare	Informationen zum Asset.
Unternehmen	Das dem CI zugeordnete Unternehmen. Dies ist ein Pflichtfeld.
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Modell-ID	Modell-ID des Geräts
Zugewiesen an	Person, die dieses Element verwendet oder die Hauptverantwortung dafür trägt.
Host-Name	Der Hostname des CI.
BS-Domäne	Die BS-Domäne des CI.
Betriebssystem	Auf dem CI ausgeführtes Betriebssystem
BS-Version	Version des auf dem CI ausgeführten Betriebssystems
BS-Service Pack	Das auf dem Betriebssystem installierte Service Pack.
DNS-Domäne	Die DNS-Domäne des CI.
IP-Adresse	IP-Adresse für das CI
Festplattenspeicher (GB)	Die Menge des Speicherplatzes in GB.
Beschreibung	Kurze Textbeschreibung des CI.
RAM (MB)	Die Größe des Arbeitsspeichers auf dem Computer in MB.
CPU-Hersteller	Hersteller der CPU
CPU-Typ	CPU-Typ
CPU-Geschwindigkeit (MHz)	Die Geschwindigkeit der CPU in MHz.
CPU-Anzahl	Die Anzahl der Server-CPUs.
Anzahl CPU-Kerne	Die Anzahl der Kerne pro CPU.
IsVirtual	Option zum Angeben, ob das Gerät in einer VM-Instanz ausgeführt wird.

Automatische Übersetzung

Service Reliability Management

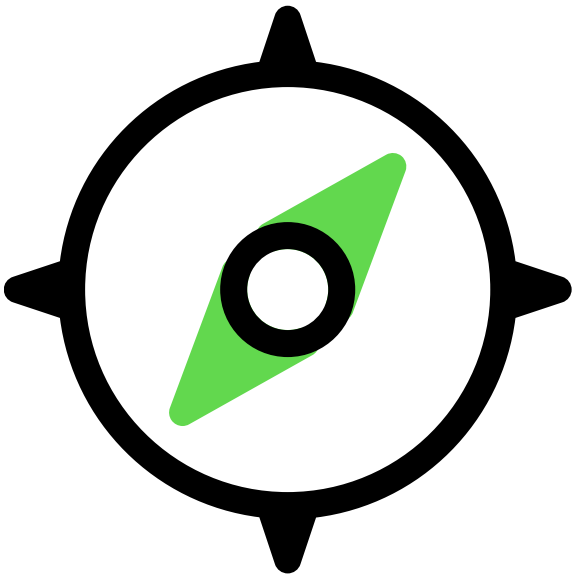
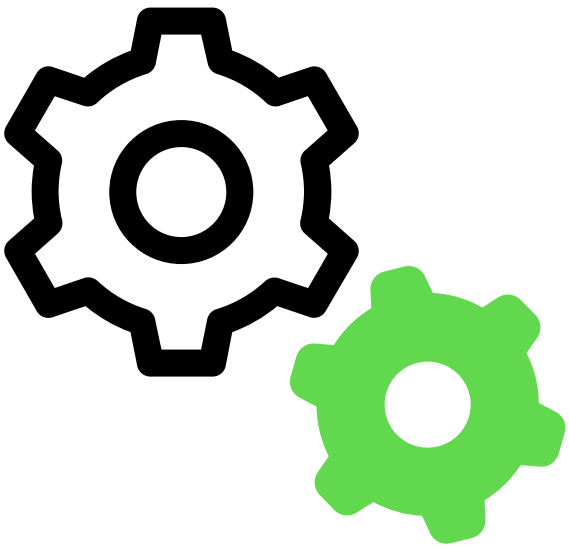
Service Reliability Management(SRM) Hilft Ihrer Organisation, bei der Arbeit an Warnungen und Incidents zu reagieren, zusammenzuarbeiten, nachzuverfolgen und sich selbst zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM Ist verfügbar, wenn Sie sowohl ITSM Standard- als auch ITOM Operator Professional-Abonnements haben.

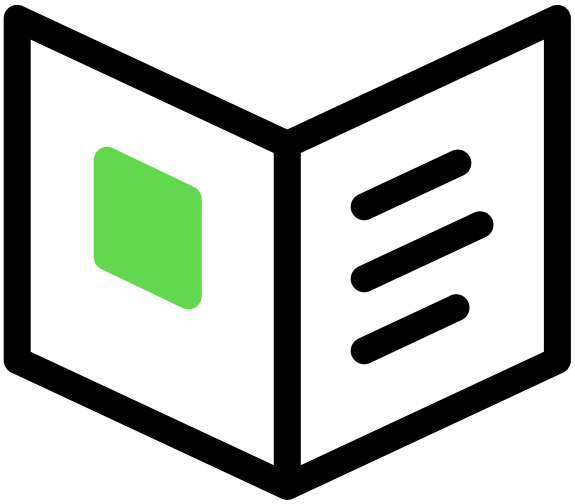
Übersicht über Service Reliability Management

Erste Schritte

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über SRM Konzepte und Funktionen.	Installieren und konfigurieren Sie den SRM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
	
Arbeiten Sie in mit Services, Teams und Zuverlässigkeitsaufgaben SRM.	Rufen Sie Details zu ab SRM Komponenten, z. B. Felder, Tabellen und Eigenschaften.

Installieren Sie aus dem Store

Installieren SRM Von ServiceNow Store. Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Hinweis: Bestätigen Sie bei der Installation aus dem Store zuerst, dass Sie über alle erforderlichen Abhängigkeiten verfügen, indem Sie die Registerkarte Abhängigkeiten auswählen. Weitere Informationen finden Sie unter Installieren Service Reliability ManagementÜber Admin Center oder ServiceNow Store.

Problembehandlung und Hilfe

- Besuchen Sie unsere Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Service Reliability Management erkunden

Service Reliability Management(SRM) Bietet Teams eine geführte Selfservice-Experience zur Verwaltung der Serviceintegrität. Die Experience wird mit der Anwendung Service Operations-Arbeitsbereich erstellt und kombiniert ITOM- und ITSM-Fähigkeiten in einem einzigen Workflow.

SRM – Übersicht

Optimieren Sie die Serviceintegrität mit Praktiken von Site Reliability Engineering (SRE). SRM Ist ein einzelner Betriebsarbeitsbereich, mit dem Teams die Zuverlässigkeit digitaler Services mit SRE verbessern können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwenden Sie Rufbereitschaftseskalationen, um rechtzeitig auf Probleme zu reagieren.
- Reduzieren Sie die Setup-Reibung mit dem geführten Selfservice, um verteilte Teams mit getrennten Daten, erweitertem Zugriff und minimaler Governance von der zentralen IT zu onboarden.

Wenn SRM Ist installiert, werden auch mehrere Plugins und Anwendungen aktiviert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

SRM – Anwender

Anwender

Anwender	Beschreibung	Enthält Rollen
Administrator	Ein ServiceNow-Administrator ist für Verwaltung, Entwicklung, Betrieb, Schulung und Wartung der ServiceNow Platform verantwortlich. Verantwortlich für die Installation und kann die Service Operations-Arbeitsbereich Admin Center-Konfiguration von SRM durchführen.	Alle
Administrator [srm_admin] **Hinweis:** Diese Rolle unterscheidet sich von ServiceNow administratorrolle.	SRM-Administratoren können Accounteinstellungen, Konfigurationen und Benutzer verwalten. Administratoren können folgende Aktionen ausführen: • Alle SRM-Konfigurationen erstellen, bearbeiten oder löschen und darauf zugreifen. • Integrationen hinzufügen oder verwalten. • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring). • Richten Sie Zuverlässigkeitsmetriken ein, und verwalten Sie sie. • Richten Sie Fehlerbudgetrichtlinien ein, und verwalten Sie sie.	• Manager • Beantworter
Manager [srm_Manager]	Manager überwachen ein Team von SREs. Manager weisen dem Rufbereitschaftszeitplan des Teams SREs zu, überwachen ihre Leistung und erstellen Verfahren zur Behandlung von Incidents und zur Entwicklung von	Beantworter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
	Lösungen. Manager fördern Resilienz in allen Systemen und DevOps-Workflows. Manager können im Kontext ihrer Teams folgende Aktionen ausführen: • Definieren und richten Sie Teams, Rufbereitschaftszeitpläne und Services ein. • Fügen Sie Anwender wie Beantworter und Manager für die Teams hinzu, denen sie angehören, und löschen Sie sie. • Integrationen hinzufügen oder verwalten. • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring). • Richten Sie Zuverlässigkeitsmetriken ein, und verwalten Sie sie. • Richten Sie Fehlerbudgetrichtlinien ein, und verwalten Sie sie.	
Beantworter [srm_Responder]	Ein Service Reliability Engineer (SRE), der SRM zur Ausführung alltäglicher Aufgaben verwendet. Beantworter sind die Personen, die Rufbereitschaft haben und Incidents diagnostizieren und beheben. Beantworter können nur auf Konfigurationen zugreifen, denen sie angehören. Sie können nur auf die Warnungen oder Incidents zugreifen, für die sie Berechtigungen haben. SREs können im Kontext ihrer Teams folgende Aktionen ausführen: • Richten Sie Services, Teams und Integrationen ein. • Bestätigen Sie ihre Rufbereitschaftszeitpläne. • Verwalten Sie Incident- und Warnungsdatensätze. • Aktualisieren Sie die von ihnen erstellten Teams.	Erbt 17 Rollen, darunter die folgenden: • cmdb_read • sn_sow.sow_user • sn_sow_srm.srm_responder • workspace_user • slo_Operator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
	• Weitere Beantworter hinzufügen • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring). • Richten Sie Zuverlässigkeitsmetriken ein, und verwalten Sie sie. • Richten Sie Fehlerbudgetaktionen ein, und verwalten Sie sie.	

Weitere Informationen finden Sie unter SRM Rollen und Verantwortlichkeiten.

SRM – Workflow

1. Produktteams in IT oder Geschäftsbereichen stellen kontinuierlich neue technische Services und Anwendungsservices bereit. Beispiel: Neues Kundenabrechnungsportal.
2. Zusammen mit SLO-Management, Teams können Services registrieren und Servicelevel-Ziele (Service Level Objectives, SLOs) definieren, um Geschäftsergebnisse zu erreichen. Beispiel: 95 % monatliche Verfügbarkeit für das Abrechnungsportal.
3. Überwachungsintegrationen werden von den Teams eingerichtet, um die Echtzeitintegrität dieser Services zu erfassen. Beispiel: Cloud Observability.
4. Bei der Überwachung werden Servicelevel-Indikatoren (Service Level Indicators, SLIs) erstellt, die sich auf Warnungen auswirken, wenn Services unterdurchschnittlich sind. Automatisierungsgruppen und Ergänzungen. Beispiel: Die Latenz des Abrechnungsportals überschreitet 7 s.
5. Wenn die Warnungen auf einen Ausfall oder eine Verschlechterung hinweisen, die sich auf den Kunden auswirkt, werden Incidents erstellt, und Rufbereitschaftsbenachrichtigungen benachrichtigen die entsprechenden Teamressourcen. Beispiel: Ein Abrechnungs-SRE-Team wird telefonisch über ein Latenzproblem im Abrechnungsportal benachrichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Nachdem Teams Incidents gemeinsam diagnostiziert und behoben haben, identifizieren sie Aktionselemente zur Verbesserung der Resilienz des Systems. Beispiel: Das Abrechnungsteam entscheidet sich, zusätzliche Webserverkapazität hinzuzufügen.
7. Das Management überprüft kontinuierlich die SLO-Leistung, hilft, Änderungen zu verhindern, wenn das Fehlerbudget erschöpft ist, und priorisiert Verbesserungsinitiativen für unterdurchschnittliche Services.

SRM – Vorteile

Vorteil	Funktion	Anwender
Teambasierte Experience	Mit SRM-Teams arbeiten	SRM-Administratoren, Manager und Beantworter
Serviceregistrierung	Mit SRM-Services arbeiten	SRM-Administratoren, Manager und Beantworter
Vorgefertigte Integrationen	Mit SRM-Integrationen arbeiten	SRM-Administratoren, Manager und Beantworter
Messen Sie die Serviceintegrität	Arbeiten mit Zuverlässigkeitsmetriken	SRM-Administratoren, Manager und Beantworter
Rufbereitschaftsabdeckung	Erstellen Sie einen SRM Rufbereitschaftszeitplan	SRM-Administratoren, Manager und Beantworter
Beheben Sie Warnungen und Incidents mit hohem Schweregrad	Mit SRM-Zuverlässigkeitsaufgaben arbeiten	SRM-Administratoren, Manager und Beantworter

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von SRM finden Sie unter:

- Service Reliability Management konfigurieren
- Service Reliability Management verwenden
- Service Reliability Management – Referenz

Erste Schritte mit Service Reliability Management

Service Reliability Management(SRM) Beschleunigt Ihren Weg zur Anzeige der Serviceintegrität im Kontext von Servicelevel-Zielen und Incident-Lösungen. Die Anwendung unterstützt IT-Betriebs- und DevOps-Teams dabei, ihr Versprechen von Agilität, Leistung und Betriebszeit einzuhalten.

Erste Schritte mit SRM Um die verschiedenen Abschnitte in zu verstehen SRM Schnittstelle.

Weitere Informationen zu Rollen finden Sie unter SRM Rollen und Verantwortlichkeiten.

Grundlegende SRM-Aufgaben

Schritt	Beschreibung	Referenz
Richten Sie Teams und Services ein	Setup-Leitfäden für die Seiten „Startseite“, „Services“ und „Teams“ zeigen, wie Sie ein Team oder einen Service zu SRM hinzufügen.	SRM-Teams hinzufügen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Beschreibung	Referenz
Besuchen Sie, und erfahren Sie mehr über Ihre Homepage	Auf der Homepage finden Sie die für Sie wichtigsten Dinge. Zum Beispiel die Services mit kritischen Warnungen und Incidents und Arbeit, die Ihnen und Ihrem Team zugewiesen sind.	Homepage von SRM
Erfahren Sie, wie Sie navigieren SRM	Machen Sie sich mit den verschiedenen Abschnitten und Elementen von vertraut SRM Schnittstelle. Die Abschnitte und Elemente werden in der gesamten Dokumentation verwendet.	Anwenderoberfläche von SRM

SRM Hilft Ihnen, wenn Sie Teams, Services und Integrationen erstellen und verwalten müssen.

SRM-Aufgaben

Schritt	Beschreibung	Siehe
Anwendungen oder technische Services in SRM verwalten	Definieren Sie die grundlegenden Aufgaben und Parameter, die den Service ausmachen und angeben, wie das Serviceverhalten aussehen soll.	Services zu SRM hinzufügen
SRM-Team einrichten	Richten Sie ein Team ein. Teams sind für die Probleme verantwortlich, die in ihren zugehörigen Services auftreten.	SRM-Teams hinzufügen
Richten Sie Rufbereitschaftszeitpläne und Eskalationsrichtlinien ein	Erstellen Sie einen Rufbereitschaftszeitplan für Ihr Team, um sicherzustellen, dass es zur Lösung von Problemen verfügbar ist. Sie können eine Eskalationsrichtlinie einrichten, um sicherzustellen, dass mindestens ein Teammitglied an der Reaktion auf Incidents beteiligt ist.	Erstellen Sie einen SRM Rufbereitschaftszeitplan
Servicebeziehungen konfigurieren	Verwenden Sie eine Zuordnungs-Canvas, um Services hinzuzufügen, zu konfigurieren und anzuordnen. Sie können untergeordnete Services hinzufügen, die von übergeordneten Services abhängig sind.	Auswirkung des untergeordneten Services auf den übergeordneten Service anzeigen
Services mit Überwachungstools von Drittanbietern integrieren	Richten Sie eine Drittpartei-Integration ein, z. B. Datadog oder ServiceNow Cloud Observability, Mit SRM Damit Warnungen für Ihre Teams in verfügbar sind SRM.	Mit SRM-Integrationen arbeiten
SLOs, SLIs und Fehlerbudgets für Services festlegen	Legen Sie mit Zielen fest, wie gut Ihr Service laufen soll. Geben Sie außerdem die maximale Zeit an, die ein technisches System ohne vertragliche Konsequenzen ausfallen kann.	Servicelevel-Zielmanagement
Warnungsautomatisierungen einrichten	Mit Warnungsautomatisierungen können Sie Warnungsbedingungen definieren. Richten Sie für jedes APM-Tool Warnungsregeln ein, um die Bedingungen zu definieren, unter	Die Anwendung Warnungsautomatisierung ist über verfügbar ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM-Aufgaben (Fortsetzung)

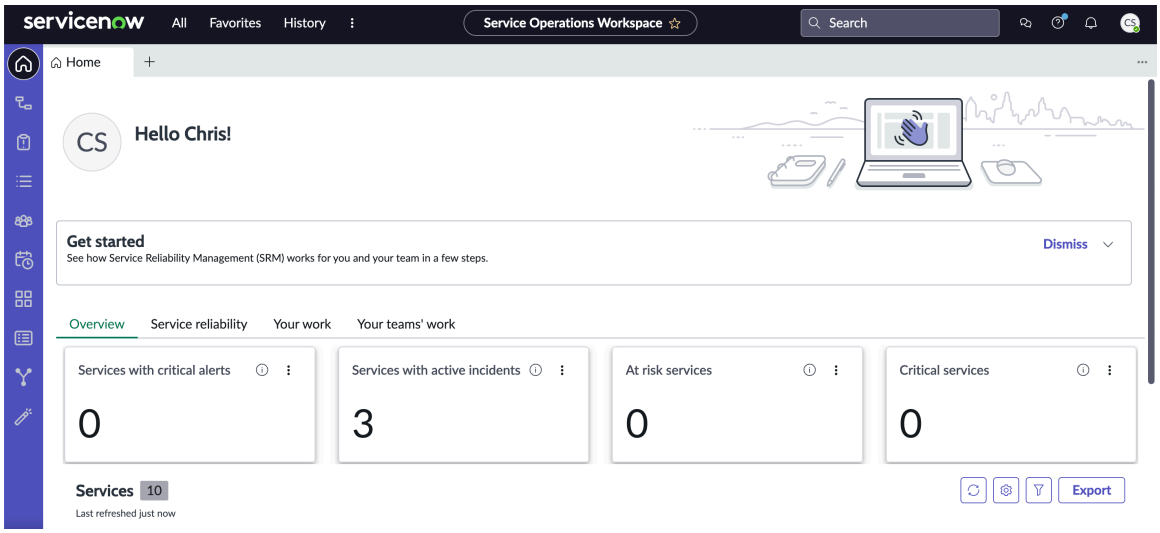
Schritt	Beschreibung	Siehe
Hinweis: Diese Funktionalität ist nur verfügbar, wenn Sie die Anwendung Warnungsautomatisierungen installiert haben.	denen das APM-Tool Benachrichtigungen an SRM senden soll.	

Homepage von SRM

Die Service Reliability Management(SRM) Die Homepage enthält relevante Informationen über Ihre Arbeit, Services, Zeitpläne, Wartungserinnerungen und Teams. Zeigen Sie die Homepage an, indem Sie zu navigieren **Service Reliability Management**an.

Service Reliability Management Startseitenabschnitte

Wählen Sie im Arbeitsbereich aus **Startseite** ( ), um die Homepage anzuzeigen.



Wenn Sie Rufbereitschaft haben, wird Ihr Zeitplan aufgelistet.

Abschnitte der Homepage

Erste Schritte	Enthält Setup-Aufgaben für Teams und Services und deren Fortschritt. Weitere Informationen zum Abschließen des Setups finden Sie unter Services zu SRM hinzufügen Und SRM-Servicedetails bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte der Homepage (Fortsetzung)

	Hinweis: Sie können jeden Abschnitt überspringen und später zurückkehren. Der Fortschritt wird durch die von Ihnen durchgeführten Aktionen in Prozentsätzen markiert. Solange ein Schritt unvollständig bleibt, sind die Kacheln verfügbar. Sie können sie jederzeit minimieren, indem Sie auf das Aufwärts-Symbol klicken . Verwenden Sie **Verwerfen**, um es von Ihrer Seite zu entfernen. Die Prüflistenstatus lauten wie folgt: • **Keine**: Es wurde keine Aktion ausgeführt. • **Fertig**: Alle erforderlichen Felder wurden hinzugefügt. • **Ausstehend** : Einige Felder oder Genehmigungen müssen noch hinzugefügt oder gewährt werden.
Übersicht	Enthält eine Übersicht über alle Servicewarnungen, Incidents sowie gefährdete und kritische Services. **Services mit kritischen Warnungen** ist die Standardlistenansicht. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.
Servicezuverlässigkeit	Zeigt ein Dashboard zur Überwachung und Verwaltung der Serviceleistung an. Das Dashboard bietet mehrere Visualisierungen, mit denen Sie Fehlerbudgets nachverfolgen, Servicelevel-Ziele überwachen und Probleme über Services hinweg identifizieren können.
Ihre Arbeit	Enthält Ihnen zugewiesene Incidents und Warnungen. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.
Die Arbeit Ihres Teams	Enthält Incidents und Warnungen, die Ihrem Team zugewiesen sind. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.

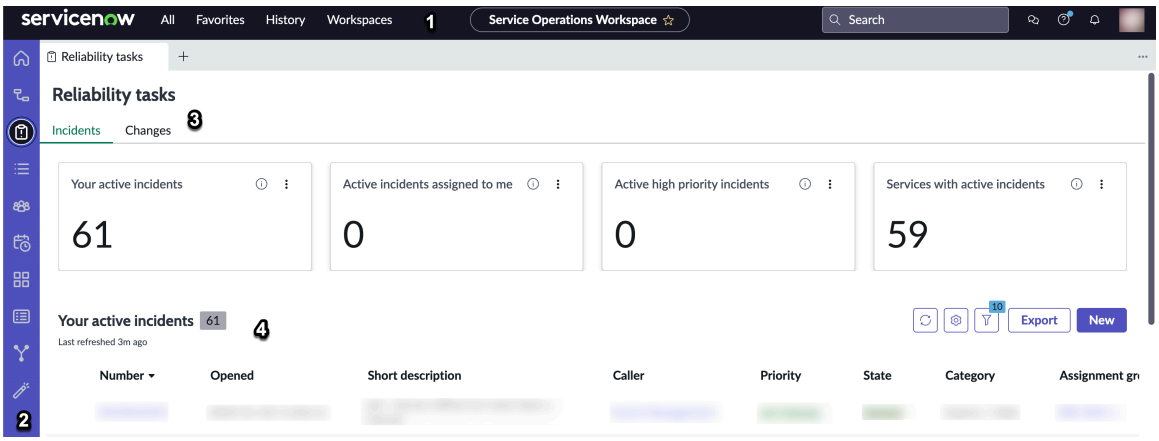
Anwenderoberfläche von SRM

Die verschiedenen Komponenten auf der Service Reliability Management(SRM)-Schnittstelle bietet einfachen Zugriff auf verschiedene Funktionen. Die angezeigten Features und Funktionen hängen von Ihrer Rolle und Ihren Berechtigungen ab.

Die Schnittstelle SRM verfügt über die folgenden verschiedenen Abschnitte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte der Schnittstelle



Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken. Abhängig von Ihrer Rolle werden möglicherweise andere Symbole in der primären Navigation angezeigt.

Wenn die SOW-Homepage angezeigt wird, wählen Sie ein SRM-Symbol aus, um SRM-spezifische Informationen anzuzeigen.

Abschnitte	Beschreibung
1: Header	Eine Startseite für Ihr Organisationslogo und Dienstprogramme auf Systemebene, die überall in der Benutzeroberfläche vorhanden sind. • Alle • Favoriten • Verlauf • Arbeitsbereiche • Aktueller Arbeitsbereich • Suchen • Sidebar-Diskussionen • Hilfe • Benachrichtigungen • Profilsymbol: Stellt Ihr Profil dar
2: Primäre Navigation	Einfacher Zugriff auf bestimmte Seiten in SRM. Die primäre Navigation verwendet Symbole, einschließlich Symbole für Services, Zuverlässigkeitsaufgaben, Teams und Zeitpläne. Verwenden Sie Tooltips, um sie zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte	Beschreibung
	Hinweis: Das Symbol Warnungsautomatisierung Ist nur verfügbar, wenn Sie die Anwendung Warnungsautomatisierung über installiert haben ServiceNow Store.
3: Inhaltsheader	Registerkarten, Karten oder Schaltflächen, mit denen Aufgaben auf Produktebene ausgeführt werden können. Die Elemente im Inhaltsheader unterscheiden sich von Seite zu Seite.
4: Inhaltsbereich	Canvas oder der Hauptbereich, in dem Sie Informationen sammeln, Metriken lesen und Aufgaben ausführen können. **Hinweis:** Wenn Sie den Seitenbereich in Formularen standardmäßig minimieren möchten, navigieren Sie zu **Einstellungen** > **Arbeitsbereich** Und deaktivieren Sie **Sidebar anzeigen** Option. Mit dieser Aktion wird sie im deaktiviert Service Operations-Arbeitsbereich, Nicht nur SRM.

Suche, Filter, Listen, Formulare und Leitfäden

Eine Übersicht über die zusätzlichen Elemente in Service Reliability Management(SRM) Schnittstelle, mit der Sie Elemente finden, verfügbare Formulare und Listen anzeigen und Setup-Prozesse verfolgen können.

Tabellenlistenansicht

Zeigen Sie Services und Incidents als Liste an.

- Suchen Sie mithilfe des Headertextfelds.
- Sortieren Sie Elemente mithilfe der Listenspalten.
- Filtern Sie Listenergebnisse mithilfe der Listenspalten.

Hinweis: Zeigen Sie die aktiven Filter über das Filtersymbol im Header der Listenansicht an.

Jede Ansicht enthält eigene spezifische Elemente. Weitere Informationen finden Sie auf diesen Seiten.

Formularansicht

Wenn Sie einen der Tabellendatensätze aus der Listenansicht öffnen, werden die Details des Datensatzes als Formular angezeigt.

Jede Ansicht enthält eigene spezifische Elemente. Weitere Informationen finden Sie auf diesen Seiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

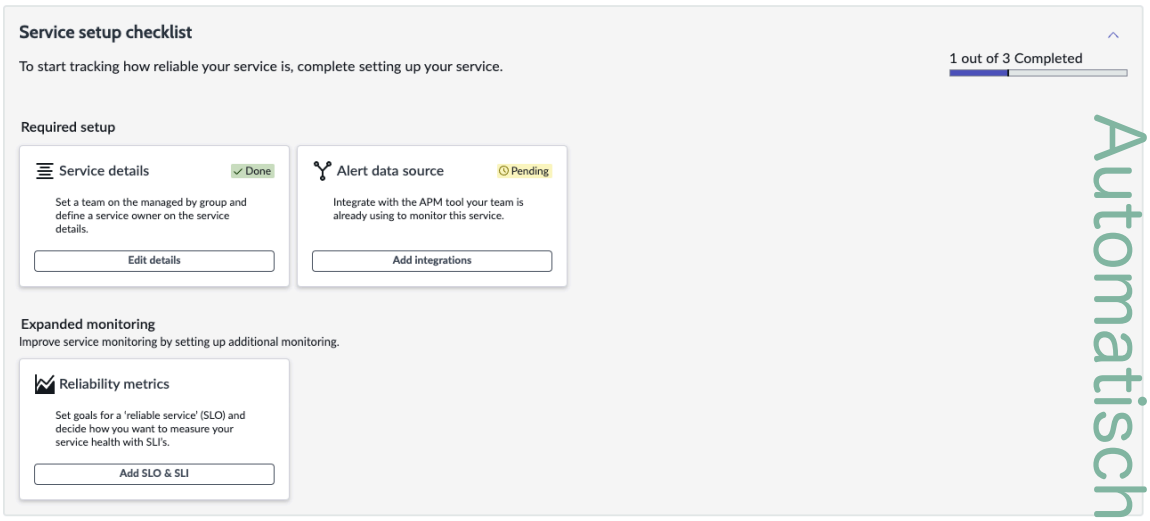
Hinweis: Ausgegraute Felder können nicht geändert werden.

Der Bereich „Anhänge“ ist häufig standardmäßig sichtbar. Um ihn auszublenden, wählen Sie das Symbol „Anhang“ .

Setup-Prüflisten

Verwenden Sie die Setup-Prüflisten, um den Prozess zu visualisieren, den Sie durchlaufen, um Ihre Ziele zu erreichen. Jeder Schritt wird hervorgehoben, wenn Sie ihn abschließen.

Prüflistenbeispiel für Service-Setup



Listeninformationen in eine Datei exportieren

Sie können Live-Informationen in eine Datei exportieren Service Reliability Management(SRM).

Vorbereitungen

Hinweis: Die Massenauswahl wirkt sich nicht auf Exporte aus. Der Export enthält alle Datensätze, die den aktuellen Filterkriterien entsprechen. Die Auswahl, die Sie in der Listenansicht treffen, wird nicht berücksichtigt.

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie die Listenansicht in einem beliebigen Zielseitenabschnitt in SRM über die **Exportieren-Schaltfläche** aus.

3. Legen Sie die zu verwendenden Filter fest, und wählen Sie sie aus dem Menü „Filter“ oder dem Menü „Weitere Aktionen“ in den Listenspalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Die Schaltfläche „Exportieren“ ist nur verfügbar, wenn in der Listenansicht Datensätze vorhanden sind.

Der Export enthält alle Listendaten, die Ihren gefilterten/gruppierten Listen entsprechen.

4. Wählen Sie **Exportieren**.
   Wählen Sie im Popup-Fenster Folgendes aus:
   - Dateityp:
     - Excel
     - CSV
     - JSON
     - PDF
   - Liefertyp:
     - Herunterladen
     - E-Mail: Geben Sie eine E-Mail-Adresse an.

   Für **E-Mail** : Sobald der Export abgeschlossen ist, wird oben im Bildschirm eine Erfolgsmeldung mit Ihrer E-Mail-Adresse angezeigt. Dies ist für größere Dateien nützlich, da der Export je nach Größe der Datei einige Zeit dauern kann. E-Mail wird im Hintergrund ausgeführt, sodass Sie während der Wartezeit etwas anderes tun können.

   Für **Herunterladen** : Das Popup-Fenster beginnt mit dem Export, und die Datei wird in Ihrem Download-Verzeichnis angezeigt. Je nach Größe der Datei kann dies einige Zeit dauern. Sie können sie in jeder Anwendung öffnen, die das Dateiformat unterstützt.

SRM-Tags manuell erstellen

Fügen Sie Tags hinzu, um Daten zu klassifizieren, zu kategorisieren und Kontext hinzuzufügen. Service Reliability Management(SRM) Importiert Tags und hängt sie an Services, Warnungen und Incidents an. Sie können Tags auch manuell erstellen.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, wie Tags in das System gelangen und an eine Warnung oder einen Incident angehängt werden. Die erste ist automatisiert, die andere hingegen manuell.

- Importiert aus einer Drittanbieterintegration wie Datadog.
- Verwenden des Tag-Symbols im Header eines Service, einer Warnung oder eines Incident.
- Hinzugefügt mithilfe der Aktion **Modify field values (Feldwerte ändern)** in einer Automatisierungsregel.

In dieser Aufgabe wird beschrieben, wie Tags zu Services und Incidents in hinzugefügt werden SRM. Informationen zum Verwalten von Warnungen finden Sie unter Warnungen in Service Operations-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Services** Oder **Zuverlässigkeitsaufgaben** .
3. Öffnen Sie einen Service oder Incident.
4. Wählen Sie im Header die Option aus **Tag** Symbol Zum Hinzufügen von Tags.
5. Geben Sie Ihr Tag in das Popup-Fenster ein.
   Ihr Tag wird gespeichert und unter dem Feld Tag hinzufügen neben allen vorhandenen Tags angezeigt.
6. Wählen Sie eine beliebige Stelle im Formular aus, um das Popup-Fenster zu schließen.

Hinweis:

Tags werden auch unter der Beschreibung in der Incident-Listenansicht angezeigt.

SRM Incidents

Verfolgen Sie Incidents auf der Registerkarte „Incidents“ und arbeiten Sie daran zusammen, damit Sie und Ihre Teams Probleme effizient lösen können.

Die Registerkarte Incidents wird in angezeigt Service Reliability Management(SRM) Seite „Zuverlässigkeitsaufgaben“. Der obere Header zeigt Beschreibungsinformationen, Tags, Prioritätsinformationen, Status, Service, und Zuweisungsgruppe.

Hinweis: Tags werden aus Drittanbieterintegrationen importiert und an Warnungen angehängt. Sie können jedoch auch Tags erstellen, um Daten zu kategorisieren und die Systemlogik mithilfe des Tag-Symbols zu steuern . Weitere Informationen zum Erstellen und Anzeigen von Tags finden Sie unter SRM-Tags manuell erstellen.

Wenn Sie einen Incident auswählen, gelangen Sie zu einer Übersicht. Dieser Abschnitt enthält drei Inhaltsbereiche: Zusammenfassung, Aktivität und empfohlene Aktionen.

Hinweis: Wenn ein bearbeitbares Feld aktualisiert wird, werden Benachrichtigungen basierend auf den Benachrichtigungseinstellungen des Anwenders gesendet.

In der Impact-Zusammenfassung finden Sie die folgenden Informationen:

Betroffene CIs

Feld	Beschreibung
Konfigurationselement	Name des Konfigurationselements, das diesem Incident zugeordnet ist, und der zugehörige Link.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betroffene Services

Feld	Beschreibung
Konfigurationselement	Name des Konfigurationselements, das diesem Incident zugeordnet ist, und der zugehörige Link.
Verwaltet von	Für den Incident verantwortliches Team.
Eigentum von	Incident-Besitzer.
Genehmigungsgruppe	Team, das für Genehmigungen verantwortlich ist.
Standort	Geografischer Standort des Incident, falls definiert.
Betriebsstatus	Status des Incident.
Manuell hinzugefügt.	Gibt an, ob dieser Incident manuell hinzugefügt wurde oder das Ergebnis einer Fehlerbudgetrichtlinie ist.

Details

Enthält Incident-Details und zugehörige Warnungen

Feld	Beschreibung
Kurzbeschreibung	Eine kurze Beschreibung des Incident.
Beschreibung	Detaillierte Beschreibung des Incident.
Nummer	Bezeichner des Incident.
Auswirkung	Die Auswirkung ist ein Messwert für den Effekt, den ein Incident auf Geschäftsprozesse hat. Die Auswahlmöglichkeiten lauten wie folgt: • 1 - Hoch • 2 – Mittel • 3 - Niedrig
Zuweisungsgruppe	Team, das dem Incident zugewiesen ist.
Priorität	Die Priorität beruht auf der **Auswirkung** und der **Dringlichkeit**. Sie bestimmt, wie schnell der Incident behandelt werden sollte. Die Auswahlmöglichkeiten lauten wie folgt: • Hohe Auswirkung = Kritische Priorität • Mittlere Auswirkung = Hohe Priorität • Niedrige Auswirkung = Moderat **Hinweis:** Beachten Sie dazu die Regeln für priorisierte Datensuchen unten.
Kategorie	Kategorie des Incident. Die Auswahlmöglichkeiten lauten wie folgt: • Anfrage/Hilfe • Software

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details
Enthält Incident-Details und zugehörige Warnungen

(Fortsetzung)

Feld	Beschreibung
	• Hardware • Netzwerk • Datenbank
Dringlichkeit	Die Dringlichkeit ist ein Messwert dafür, wie lange die Lösung hinausgeschoben werden kann, bis ein Incident maßgebliche Geschäftsauswirkungen hat.
Service	Betroffener Service, der dem Incident zugeordnet ist. Sie können dieses Feld über ein Listenmenü bearbeiten. **Hinweis:** Wenn Sie einen Service festlegen und dieser Service über ein zugewiesenes Team verfügt, wird das diesem Service zugewiesene Team dem Incident automatisch zugewiesen.
Schweregrad	Importierter Schweregrad für den Incident. Werte P1–P5.
Konfigurationselement	Asset, das dem Incident zugeordnet ist.
Zugewiesen an	Einzelperson, die für die Lösung des Incident verantwortlich ist.
Status	Status des Incident. Der Status ändert sich und verfolgt Incidents durch mehrere Lösungsphasen. Die Auswahlmöglichkeiten lauten wie folgt: • Neu • In Bearbeitung • Warten • Gelöst • Abgebrochen
Beobachtungsliste	Einzelpersonen, die an dem Incident interessiert sind. Sie erhalten Benachrichtigungen entsprechend ihren Einstellungen.
Lösungscode	Code, der der Lösung zugeordnet ist. Die Auswahlmöglichkeiten lauten wie folgt: • Keine (Standard) • Duplikat • Known Error • Keine Lösung bereitgestellt • Von Anrufer gelöst • Gelöst durch Change • Gelöst durch Problem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details
Enthält Incident-Details und zugehörige Warnungen

(Fortsetzung)

Feld	Beschreibung
	• Gelöst durch Anforderung • Lösung bereitgestellt
Lösungsnotizen	Detaillierte Informationen zur Lösung. Lösungshinweise werden in der Zeitleiste **Aktivität** veröffentlicht.

Hinweis: Die Priorität wird anhand der folgenden Beispielregeln für die Datensuche berechnet:

Regeln für Datensuche mit Priorität

Auswirkung	Dringlichkeit	Priorität
1 – Hoch	1 – Hoch	1 - Kritisch
1 – Hoch	2 – Mittel	2 – Hoch
1 – Hoch	3 – Niedrig	3 – Mittel
2 – Mittel	1 – Hoch	2 – Hoch
2 – Mittel	2 – Mittel	3 – Mittel
2 – Mittel	3 – Niedrig	4 – Niedrig
3 – Niedrig	1 – Hoch	3 – Mittel
3 – Niedrig	2 – Mittel	4 – Niedrig
3 – Niedrig	3 – Niedrig	5 - In Planung

Wenn ein Service gelöscht wird, werden seine Integrationen, Warnungen, Incidents und Automatisierungen entfernt. Das Löschen eines Service ist keine wiederherstellbare Aktion. Erwägen Sie stattdessen, den Service zu deaktivieren.

Die Registerkarte zugehörige Datensätze enthält alle Warnungen, die diesem Incident zugeordnet sind.

Hinweis: Alle Feldwerte werden aus den zugehörigen Datensätzen importiert und können nicht aus bearbeitet werden SRM.

Untergeordnete Incidents

Feld	Beschreibung
Nummer	Bezeichner des zugehörigen Incidents.
Kurzbeschreibung	Kurze Beschreibung des zugehörigen Incidents.
Priorität	Priorität des zugehörigen Incidents.
Status	Status des zugehörigen Incidents.
Zugewiesen an	Teammitglied, das dem zugehörigen Incident zugewiesen ist.
Zuweisungsgruppe	Team, das dem zugehörigen Incident zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untergeordnete Incidents (Fortsetzung)

Feld	Beschreibung
Service	Service, der dem zugehörigen Incident zugeordnet ist.

Warnungen

Feld	Beschreibung
Nummer	Bezeichner der zugehörigen Warnung.
Schweregrad	Schweregrad der zugehörigen Warnung.
Kurzbeschreibung	Kurze Beschreibung der zugehörigen Warnung.
Bestätigt	Gibt an, ob die zugehörige Warnung bestätigt wurde oder nicht.
Zugewiesen an	Teammitglied, das der zugehörigen Warnung zugewiesen ist.
Konfigurationselement	Asset, das der zugehörigen Warnung zugeordnet ist.
Übergeordnet	Primäre Warnung, die der zugehörigen Warnung zugeordnet ist.

Letzte wirkungsvolle Changes

Feld	Beschreibung
Nummer	Bezeichner für die zugehörigen Changes, die diesem Incident zugeordnet sind.
Kurzbeschreibung	Kurze Beschreibung der zugehörigen Changes, die diesem Incident zugeordnet sind.
Typ	Typ der letzten Changes, die diesem Incident zugeordnet sind.
Status	Status der letzten Changes, die diesem Incident zugeordnet sind.
Geplantes Startdatum	Datum und Uhrzeit, bis zu dem die mit diesem Incident verknüpften Changes gelten.
Geplantes Enddatum	Datum und Uhrzeit, bis zu dem die mit diesem Incident verknüpften Changes gelten.
Zugewiesen an	Teammitglied, das für die Change-Anforderung im Zusammenhang mit diesem Incident verantwortlich ist.

Change-Anforderungen

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung der Change-Anforderung, die diesem Incident zugeordnet ist.
Typ	Typ der Change-Anforderung, die diesem Incident zugeordnet ist.
Status	Status der Change-Anforderung, die diesem Incident zugeordnet ist.
Geplantes Startdatum	Datum und Uhrzeit des Beginns der Arbeiten für die Change-Anforderung, die diesem Incident zugeordnet ist.
Geplantes Enddatum	Datum und Uhrzeit der Beendigung der Arbeiten für diese Change-Anforderung, die diesem Incident zugeordnet ist.
Zugewiesen an	Teammitglied, das für die Change-Anforderung im Zusammenhang mit diesem Incident verantwortlich ist.

Registerkarte „Postmortem“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Über den Postmortem-Besitzer:

- Wenn bereits ein Scribe in der Antwortliste des Zusammenarbeitsbereichs ausgewählt wurde, wird er automatisch zum Besitzer gemacht.
- Wenn mehr als ein Skript vorhanden ist, wird der erste zugewiesene ausgewählt. Andernfalls können Sie einen Besitzer aus dem Listenmenü auswählen.
- Wenn ein neuer Schreiber hinzugefügt oder eine vorhandene Benutzerpersona zum Schreiber gemacht wird, wird dieser Benutzer zum Besitzer.
- Wenn Sie einen Besitzer manuell entfernen, wird nicht automatisch ein neuer Besitzer ausgewählt.

Verwenden Sie die Drag-and-Drop-Funktion, um Postmortem-Abschnitte zu bearbeiten. Sie können Abschnitte aus PDFs ausschließen, Abschnitte löschen oder Abschnitte neu anordnen.

Um neue Abschnitte hinzuzufügen, wählen Sie aus **Hinzufügen** Symbol .
Bereich **Verfassen**

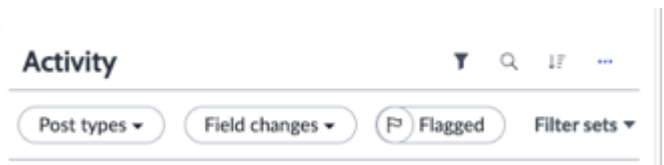
Arbeitsnotizen werden der Aktivitätszeitleiste automatisch hinzugefügt. Sichtbar für Beantworter und höhere Rollen. Fügen Sie Kommentare mithilfe des Textfelds **Verfassen** hinzu.

Kommentare werden der Aktivitätszeitleiste automatisch hinzugefügt. Für alle in SRM sichtbar.

Bereich **Aktivität**

Strom, der alle Systemaktivitäten und Lösungshinweise enthält. Sie können alle Posts mithilfe der Headersymbole filtern, sortieren, erweitern oder reduzieren.

Hinweis: Die Filteroption beinhaltet **Beitragstypen**, **Feldänderungen** und **Filtersätze**. Alle Auswahlmöglichkeiten sind standardmäßig ausgewählt. Es sind entweder alle oder keine Einträge gekennzeichnet.



Bereich **Aktionen**

Hinweis:

Die **Benachrichtigungen** , **Agent Assist** , **Experte in Rufbereitschaft** , Und **E-Mail-Vorlagen** Bereiche werden derzeit in nicht unterstützt SRM.

Abschnitt **Anhänge**

Öffnen Sie **Anhänge** Abschnitt mit dem Symbol „Anhang“ .

Im Bereich **Anhänge** können Sie zunächst Ihre lokale Festplatte nach Dateien **Durchsuchen**.

Sobald Sie Anhänge hinzugefügt haben, haben Sie folgende Möglichkeiten:

- Suchen Sie anhand des Namens oder der Erweiterung nach einem Anhang.

Hinweis: Für eine Suche müssen mindestens zwei Anhänge vorhanden sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Laden Sie einen neuen Anhang mit ( )-Symbol.
- Laden Sie vorhandene Anhänge über das Symbol „weitere Aktionen“ herunter, entfernen Sie sie oder benennen Sie sie um ( ).

Abschnitt **Vorlage**

Öffnen Sie **Vorlage** Bereich mit dem Vorlagensymbol .

Hinweis: Vorhandene Vorlagen werden angezeigt, das Erstellen von Vorlagen ist jedoch in nicht verfügbar SRM.

Bereich **Zusammenarbeit**

Zeigt die verfügbaren Zoom-Meetings, Microsoft Teams oder Slack-Kanäle an, an denen Sie beginnen oder teilnehmen können.

So starten Sie ein Zoom-Meeting oder nehmen daran teil:

Hinweis: Die Zoom-Integration und die erkannten IDs müssen in Ihrer Instanz aktiv sein. Wenn der Startkanal nicht verfügbar ist, wenden Sie sich an Ihren Administrator.

1. Wählen Sie **Start Zoom** (Zoom starten) aus.
   - Ein Besprechungs-Popup wird angezeigt.
   - Fügen Sie Teilnehmer hinzu.
   - Wählen Sie **Besprechung erstellen** aus.
   - Das Meeting wird erstellt, Einladungen werden gesendet und Sie nehmen am Meeting teil.

     Hinweis: Alle beim Starten eines Meetings gefundenen Probleme werden in einer Bannernachricht angezeigt.

2. Wählen Sie **Meeting beitreten** aus.
   - **Melden** Sie sich bei Ihrem Zoom-Konto an.
   - Damit treten Sie dem Zoom-Meeting bei.

1. Wählen Sie **Start Channel** (Kanal starten) aus.
   - Melden Sie sich bei Ihrem Microsoft Teams-Konto an.
   - Wählen Sie **Erstellen** aus. Sie werden zur Microsoft Teams-Anwendung weitergeleitet.
   - Zurück in der Spalte „Zusammenarbeit“ wird die Schaltfläche **Kanal beitreten** aktiviert.

     Hinweis: Alle beim Beitritt zu einem Kanal gefundenen Probleme werden in einer Bannernachricht angezeigt.

2. Wählen Sie im Bereich „Zusammenarbeit“ in SRM die Option **Kanal beitreten** aus.
3. Melden Sie sich bei Ihrem Microsoft Teams-Konto an.

   Sie treten dem Kanal in Microsoft Teams bei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Starten Sie einen Slack-Kanal oder nehmen Sie daran teil:

Hinweis: Die Slack-Integration und die erkannten IDs müssen in Ihrer Instanz aktiv sein. Wenn der Startkanal nicht verfügbar ist, wenden Sie sich an Ihren Administrator.

1. Wählen Sie **Start Slack** (Slack starten) aus.
   - Fügen Sie im Popup-Fenster „Create a Slack channel“ (Slack-Kanal erstellen) Teilnehmer hinzu.
   - Wählen Sie **Erstellen** aus. Sie werden zur Slack-Anwendung weitergeleitet.
   - Zurück in der Spalte „Zusammenarbeit“ wird die Schaltfläche **Join Slack** (Slack beitreten) aktiviert.

     Hinweis: Alle beim Starten eines Kanals gefundenen Probleme werden in einer Bannernachricht angezeigt.
2. Wählen Sie im Slack-Anwendungsfenster **Kanal beitreten** aus.
3. Melden Sie sich bei Ihrem Slack-Konto an.

   Sie treten dem Slack-Kanal bei.

Service Operations-Arbeitsbereich für SRM einrichten

Installieren und konfigurieren Service Reliability Management(SRM) Innerhalb von Service Operations-Arbeitsbereich Admin Center so SRM Administratoren, Manager und Beantworter können Servicezuverlässigkeit effizient bereitstellen.

Sie können Installieren Service Reliability ManagementÜber Admin Center oder ServiceNow Store über das Service Operations-Arbeitsbereich Admin Center.

Hinweis: Die App Datenvisualisierungen v24.1.8 ist ebenfalls erforderlich. Informationen zum Installieren der App finden Sie unter Datenvisualisierungen im ServiceNow Store.

Nach der Installation wird durch die Konfiguration von SRM im Service Operations-Arbeitsbereich Admin Center der SRM-Arbeitsbereich mit Optionen und Aktionen eingerichtet.

Mit den Service Reliability Management-Menüs im Service Operations-Arbeitsbereich Admin Center haben Sie folgende Möglichkeiten:

- Administratoren zu Service Reliability Management zuweisen.
- Aktivieren Sie Teams und Services in SRM
- Passen Sie die Einstellungen für Servicegenehmigungen in an SRM.
- Passen Sie die Einstellungen für Teamgenehmigungen in an SRM
- Greifen Sie auf das Anforderungskatalogelement für Benutzer zu, und veröffentlichen Sie es.
- Konfigurieren Sie Fehlerbudgetaktionen für Verstöße SRM SLOs.

Warnungsautomatisierungen sind Bedingungsauslöser, die auf Basis des Inhalts einer Warnung automatisch Antwortreaktionen ausführen. Diese Funktionalität ist für SRM auf Anforderung in der Anwendung Warnungsautomatisierungen im ServiceNow Store verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Reliability Management konfigurieren

Wird Konfiguriert Service Reliability Management(SRM) Umfasst die Installation von aus ServiceNow Store Oder Service Operations-Arbeitsbereich Admin Center. Sie können auch Administratoren zuweisen und Services und Teams importieren.

Geführtes Setup für verwenden SRM

Das geführte Setup bietet eine Reihe von Aufgaben, die Sie bei der Konfiguration unterstützen SRMIn Ihrer Instanz. Navigieren Sie zum Öffnen des geführten Setups zu **Alle** > *`Service Operations-Arbeitsbereich`* **Admin Center** > **Übersicht**an. Suchen Sie als Nächstes nach Service Reliability Management Kachel und wählen Sie aus **Konfigurieren** .

SRM Konfigurationsdokumentation

Besuchen Sie die folgenden Seiten, um einzurichten und zu konfigurieren SRM. Der Inhalt ist hauptsächlich für srm_admin- oder admin-Anwender bestimmt.

Installieren Service Reliability ManagementÜber Admin Center oder ServiceNow Store

Installieren Sie Service Reliability Management(SRM) Anwendung aus dem Admin Center oder ServiceNow Store.

Vorbereitungen

Erforderliche Abonnements: ITSM Standard- und ITOM Operator Professional-Abonnements.

Hinweis: Die Store-App v24.1.8 für Datenvisualisierungen ist ebenfalls erforderlich. Informationen zum Installieren der App finden Sie unter Datenvisualisierungen im ServiceNow Store.

Um Warnungsautomatisierungen zu erstellen und zu verwalten, installieren Sie die Anwendung „Warnungsautomatisierung“, die auf Anforderung im verfügbar ist ServiceNow Store.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Mit SRM werden Rollen und Demodaten installiert. Die Demodaten enthalten Vorlagen, die die Implementierung und beschleunigen SRM Verwenden.

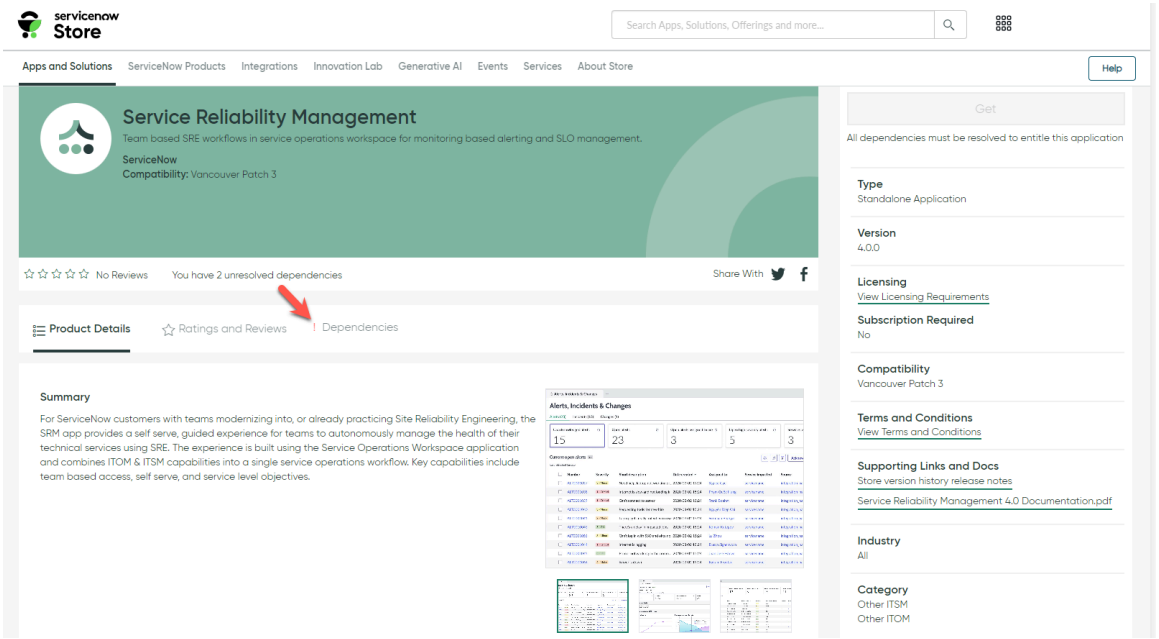
Prozedur

1. Navigieren zu **Alle** > *`Service Operations-Arbeitsbereich`* **Admin Center** > **Übersicht**an.
2. Suchen Sie nach *`Service Reliability Management`*Karte und wählen Sie aus **Installieren** .
3. Wählen Sie im Popup-Fenster **Installation starten**.
   Sie werden zu weitergeleitet ServiceNow Store-Portal.
4. Führen Sie die erforderlichen Schritte aus.

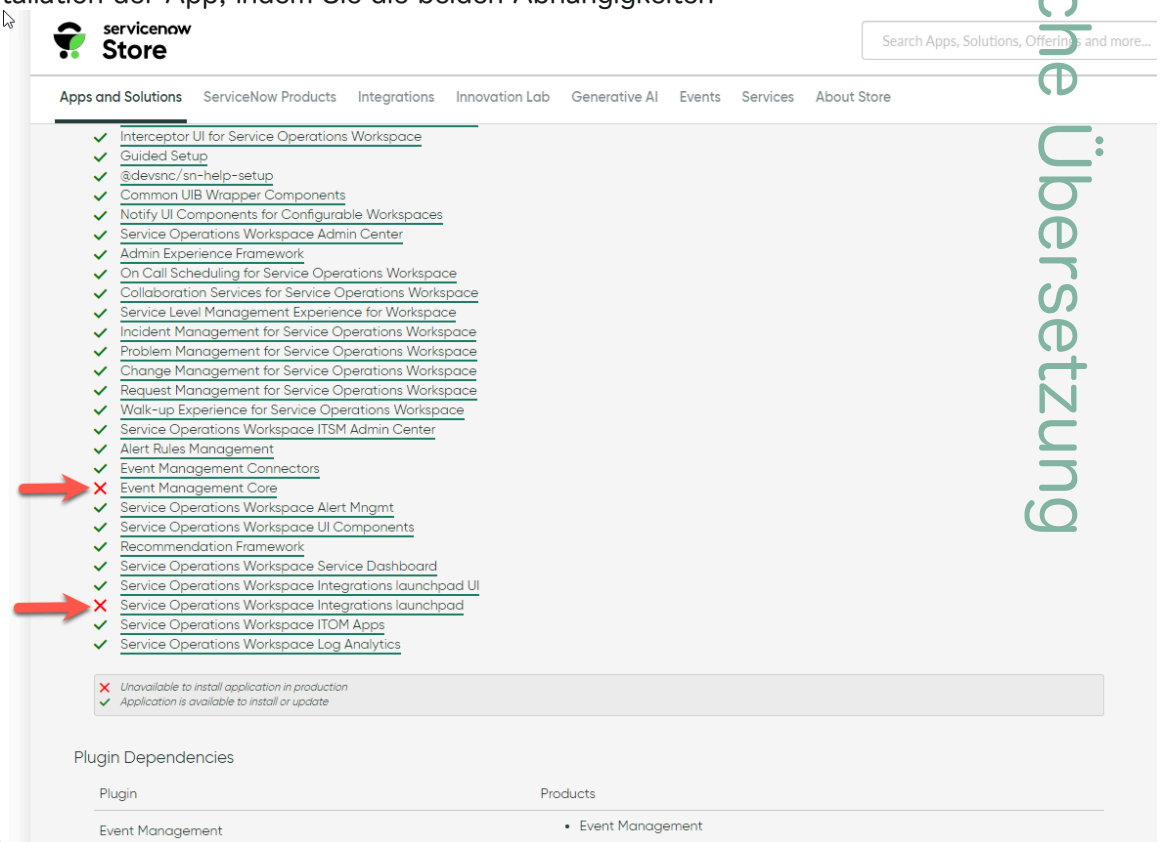
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Abhängigkeiten in der App Store-Liste rot angezeigt werden, wählen Sie die Zeile aus, um die abhängige App zu öffnen und zu installieren. Wenn die abhängige App bereits installiert ist, aber weiterhin rot angezeigt wird, können Sie sie nach Bedarf abrufen oder erneut aktivieren.



Das Beispiel zeigt zwei ungelöste Abhängigkeiten. Lösen Sie die Probleme vor der Installation der App, indem Sie die beiden Abhängigkeiten



auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Demodaten werden geladen, wenn Sie die Anwendung zum ersten Mal in einer Entwicklungs- oder Testinstanz installieren.

Nach der Installation von wird *Service Reliability Management*Die Karte kann zum Konfigurieren verwendet werden SRM.

Administratoren zu Service Reliability Management zuweisen

Fügen Sie Personen aus hinzu ServiceNow Zu verwaltende Instanz Service Reliability Management(SRM) Und Ihren Servicevorgängen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die SRM der administrator kann Teams hinzufügen und erstellen. Sie können auch Daten über verwalten Alle SRM Teams.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Übersicht**an.
2. In *Service Reliability Management* Kachel auswählen **Konfigurieren** .
3. Navigieren zu **Administratoren zuweisen** > **Service-Reliability-Management-Administratoren**an.
4. Geben Sie Anwendernamen in das Feld ein.
5. Wählen Sie **Speichern**.

Aktivieren Sie Teams und Services in SRM

Aktivieren Sie Teams und Services, die in verwaltet werden sollen Service Reliability Management(SRM) Anwendung.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Konfigurationen**an.
2. Auswahlvorgang *Service Reliability Management* > **Aktivieren** > **Teams und Services**an.
3. Wählen Sie Aus **Aktivieren Sie Teams und Services** Um mit dem Importieren oder Hinzufügen von Teams zu beginnen.
4. Verwenden Sie den Bedingungsgenerator, um die Teams zu filtern, die in der Liste „Zuweisungsgruppen“ angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Filter für dieselbe Feldverwendung UND -Logik und Filter für verschiedene Felder verwenden ODER -Logik. Beispiel: Filtern nach mehreren Geschäftsrelevanz Ebenen und Status = Offen , Wird als ausgewertet (Relevanz = 1 ODER 2 ODER 3 ODER 4) UND (Status = Offen) .

Listenansichtsfilter werden automatisch gespeichert und bleiben erhalten, wenn Sie weg und zurück navigieren.

5. Wählen Sie in der Liste Zuweisungsgruppen die Teams aus, die Sie hinzufügen möchten, und wählen Sie dann aus **Aktivieren** .
   Sie erreichen **Aktivieren Sie Services** Option zum Hinzufügen von Services.
6. Von **Wählen Sie eine Serviceklasse aus** Liste einen Service auswählen.
   Die folgenden Servicetypen sind verfügbar:
   - Anwendungsservices
   - Zugeordnete Anwendungsservices
   - Berechnete Anwendungsservices
   - Dynamische CI-Gruppe
   - Technische Services
   - Tag-basierte Services
7. Verwenden Sie den Bedingungsgenerator, um der Listenansicht neue Services hinzuzufügen.
8. Wählen Sie die Services aus, die Sie hinzufügen möchten, und wählen Sie dann aus **Aktivieren** .
   Die **Aktivieren Sie Services** Popup wird geöffnet.
9. Von **Supportgruppe** Wählen Sie in der Dropdown-Liste die entsprechende Supportgruppe aus, und wählen Sie aus **Bestätigen** .

Ergebnis

Auf der **Aktivieren Sie Teams und Services** Seite werden die folgenden Optionen angezeigt:

- Vorhandene Teams
- Vorhandene Services

Sie können die Optionen auswählen, um die Teams oder Services anzuzeigen.

Passen Sie die Einstellungen für Servicegenehmigungen in an SRM

Fügen Sie Ihren Services einen Genehmigungsprozess für Governance hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Genehmigung erforderlich, wenn Service Reliability Management(SRM) Administratoren, Manager oder Beantworter fordern das Erstellen oder Hinzufügen eines Service in an SRM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Konfigurationen**an.
2. Auswahlvorgang *Service Reliability Management* > **Governance und Autonomie** > **Service-Governance**an.
3. Wählen Sie einen oder beide Prozesse aus, indem Sie das entsprechende Kontrollkästchen aktivieren.

   Genehmigungsanforderungstypen:

   - Genehmigung erforderlich, wenn ein neuer Service erstellt wird:

     Erfordert Genehmigung beim Erstellen eines Service in SRM, Und weist sie dem Team zu, das für neue Services verantwortlich ist.

   - Genehmigung erforderlich, wenn ein vorhandener Configuration Management Database (CMDB)-Service zugeordnet wird:

     Erfordert Genehmigung, um einen vorhandenen Service zu hinzuzufügen SRM, Und weist sie dem Team zu, das für vorhandene Services verantwortlich ist.

4. Geben Sie das Team ein, das für Genehmigungen verantwortlich ist, oder wählen Sie es aus.
5. Wählen Sie **Speichern**.
   Diese Aktion initiiert den Genehmigungsprozess und weist die Genehmigung dem Team zu, das für die Genehmigung des neuen Service verantwortlich ist.

   Hinweis: Für Genehmigungen sind zwei Schritte auszuführen. Zuerst wird die Anforderung genehmigt, die in angezeigt wird **Phase** Feld des Anforderungsdatensatzes. Als Nächstes bleibt die Anforderung **Ausstehend** Bis das Anforderungselement in genehmigt wird **Anforderung** Datensatz.

Passen Sie die Einstellungen für Teamgenehmigungen in an SRM

Passen Sie an, wie Teamgenehmigungen funktionieren, wenn nicht-Administratoranwender ein Team in erstellen oder hinzufügen Service Reliability Management(SRM). Diese Funktion, auch als Team-Governance bekannt, hilft Ihnen, den Zugriff zu steuern und an internen Richtlinien auszurichten.

Vorbereitungen

Erforderliche Rolle: srm_admin oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ist Team-Governance in aktiv SRM. Wenn nicht-Administratoranwender ein Team anfordern, SRM Erstellt zwei Datensätze: Eine übergeordnete Anforderung und ein angefordertes Element. Das Genehmigungsteam wird benachrichtigt, und jedes Mitglied kann die Anforderung über meine Genehmigungen genehmigen. Nach der Genehmigung wird das Team erstellt oder hinzugefügt, die übergeordnete Anforderung wird auf festgelegt Genehmigt , Und das angeforderte Element ist auf festgelegt Abgeschlossen .

Sie können die Team-Governance anpassen, indem Sie Genehmigungen deaktivieren oder das Genehmigungsteam ändern.

Hinweis: Nicht-Administratoranwender sind SRM Manager und SRM Beantworter. Wenn Team-Governance aktiv ist, Administratoren und SRM Administratoren können weiterhin Teams ohne Genehmigung erstellen und hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Konfigurationen**an.
2. Unter **Service Reliability Management** , Wählen Sie aus **Governance und Autonomie** Und wählen Sie dann aus **Team-Governance** .
3. Überprüfen oder aktualisieren Sie die Genehmigungsoptionen.

Option	Beschreibung
Genehmigung beim Erstellen eines neuen Teams erforderlich	Deaktivieren Sie diese Option, damit nicht-Administratoranwender Teams in erstellen können SRM Ohne Genehmigung.
Genehmigung beim Zuordnen eines vorhandenen Teams erforderlich	Deaktivieren Sie diese Option, damit nicht-Administratoranwender vorhandene Teams hinzufügen können SRM Ohne Genehmigung.

4. Überprüfen oder aktualisieren Sie das Genehmigungsteam für eine oder beide Optionen. Standardmäßig ist das Genehmigungsteam auf festgelegt SRM-Teamgenehmiger . Sie können seine Mitglieder in anzeigen sys_user_Group.list .

   Hinweis: Jedes Mitglied des Genehmigungsteams kann Anforderungen genehmigen, aber es benötigt den sn_Request_read Rolle zum Anzeigen von Anforderungsdetails. Ohne diese Rolle wird nur die Genehmigungsaufgabe angezeigt.

5. Wählen Sie Aus **Speichern** Um Ihre Team-Governance-Einstellungen zu aktualisieren.

Konfigurieren Sie Fehlerbudgetaktionen für Verstöße SRM SLOs

Konfigurieren Sie die Aktionen, die das Team auswählen kann, wenn das Fehlerbudget eines Servicelevel-Ziels (SLO) verletzt wird.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Konfigurationen**an.
2. Auswahlvorgang *Service Reliability Management* > **Governance und Autonomie** > **Fehlerbudgets**an.
3. Wählen Sie Aus **Konfigurieren Sie Fehlerbudgetaktionen** Dient zum Bearbeiten des Subflows „Schwellenwert für Prozessfehlerbudget-Richtlinie“ in Flow Designer.

   Hinweis: Arbeiten in Flow Designer Erfordert Advanced ServiceNow Fachwissen. Weitere Informationen zum Bearbeiten von Workflows oder zum Erstellen anwenderdefinierter Workflows finden Sie unter Flow Designer .

Genehmigen Sie eine Change-Anforderung für SRM

Genehmigen Sie eine Service-Change-Anforderung in Service Reliability Management(SRM), damit die angeforderte Aktion fortgesetzt werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Nur offene Change-Anforderungen sind im verfügbar **Zuverlässigkeitsaufgaben** Seite.

Erforderliche Rolle: SRM Genehmigungsteam oder -Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Changes**.
4. Wählen Sie eine Change-Anforderung und dann aus **Details** Registerkarte.
5. Auf der **Status** Wählen Sie die Liste aus, und wählen Sie aus **Genehmigt** .
6. Wählen Sie **Speichern**.
   Der Status der Change-Anforderung wird von aktualisiert Bewerten Bis Genehmigt .

   Nach der Genehmigung wird der neue Service erstellt und dem hinzugefügt SRM Team. Der Besitzer ist auf die Person festgelegt, die im Feld Zugewiesen an angezeigt wird. Und die Gruppe verwaltet von ist auf festgelegt SRM Team, das dem Beauftragten zugeordnet ist.

Konfigurieren Twilio Zum Senden von Benachrichtigungen in SRM

Verbinden Sie mit Service Reliability Management(SRM) Instanz und Twilio Account zum Senden von Benachrichtigungen an Teams.

Vorbereitungen

Bevor Sie beginnen, benötigen Sie einen Zeichenfolgenbezeichner (SID) und ein Authentifizierungstoken für einen aktiven Twilio Account.

Hinweis: Das Ausführen dieser Aktion erfordert ServiceNow Fachwissen.

Erforderliche Rolle: Administrator

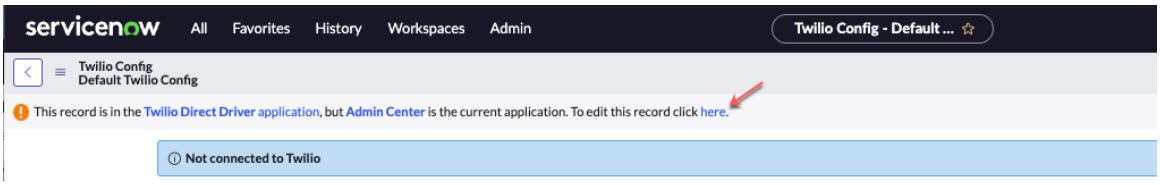
Warum und wann dieser Vorgang ausgeführt wird

Sie können anpassen, was von gesendet wird Twilio Indem Sie den Bereitschafts-Workflow im System bearbeiten.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* **Admin Center** > **Konfigurationen**an.
2. Auswahlvorgang *Service Reliability Management* > **Integrationen** > **Twilio-API-Schlüssel**an.
3. Wählen Sie Aus **Twilio-Konfiguration** .
4. Wählen Sie im neuen Fenster aus **Hier** Dient zum Bearbeiten des Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Geben Sie ein **Account-SID** Wert.
6. **Wahlweise:** Geben Sie ein **Gültigkeitszeitraum** Wert.
7. Wählen Sie Aus **Verbinden** Zum Aktivieren des Schlüssels oder **Speichern** Um Ihre Änderungen ohne Aktivierung zu speichern.

Installieren Sie die Anwendung Warnungsautomatisierung

Installieren Sie **Warnungsautomatisierung** Anwendung und alle unterstützenden Anwendungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliche Abonnements: ITSM Professional- oder ITOM Operator Professional-Abonnements.

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Verwaltungsregeln erstellen, müssen Sie installieren und konfigurieren Service Reliability Management(SRM) Anwendung, verfügbar in ServiceNow Store.

Prozedur

1. Um auf zuzugreifen ServiceNow Store Und laden Sie die Anwendung auf Ihren herunter SRM Instanz wählen Sie den Link in der E-Mail aus, die Sie erhalten haben.
2. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
3. Suchen Sie nach *`Service Operations-Arbeitsbereich`***Warnungsautomatisierung** Anwendung und wählen Sie aus **Installieren** .
   Warnungsautomatisierungsregeln können in verwendet werden SRM.

Service Reliability Management verwenden

Service Reliability Management(SRM) Ermöglicht es Ihnen, Services zu registrieren, die Serviceintegrität zu überwachen, mit Rufbereitschaftsschichten und Eskalationsrichtlinien und -Auslösern auf Serviceveränderungen zu reagieren und verteilte Teams mit minimaler Governance von der zentralen IT aus zu onboarden.

Grundlegende Aufgaben in SRM

Mit SRM-Services arbeiten

Ein Service stellt ein funktionales Ergebnis dar, z. B. Networking, Zahlungen oder HR-Services, für das ein Team verantwortlich ist. Um dieses Ergebnis zu liefern, kann ein Service eine oder mehrere technische Komponenten enthalten, z. B. einen Benutzerauthentifizierungsservice oder eine gemeinsam genutzte Infrastruktur wie eine Datenbank.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Reliability Management(SRM) Arbeitet mit Integrationen zusammen, um Warnungen zu priorisieren und an die relevanten Beantworter weiterzuleiten. Eskalationen werden nachverfolgt, bis die Warnung bestätigt wird und jemand antwortet. Wenn Sie einen Service in erstellen oder hinzufügen SRM, Muss einen Service in widerspiegeln SRM Infrastruktur.

Hinweis: Möglicherweise benötigen Sie mehrere Toolintegrationen, um die einzelnen technischen Services zu überwachen und Events von diesen Tools zu erhalten. Weitere Informationen finden Sie unter Mit SRM-Integrationen arbeiten.

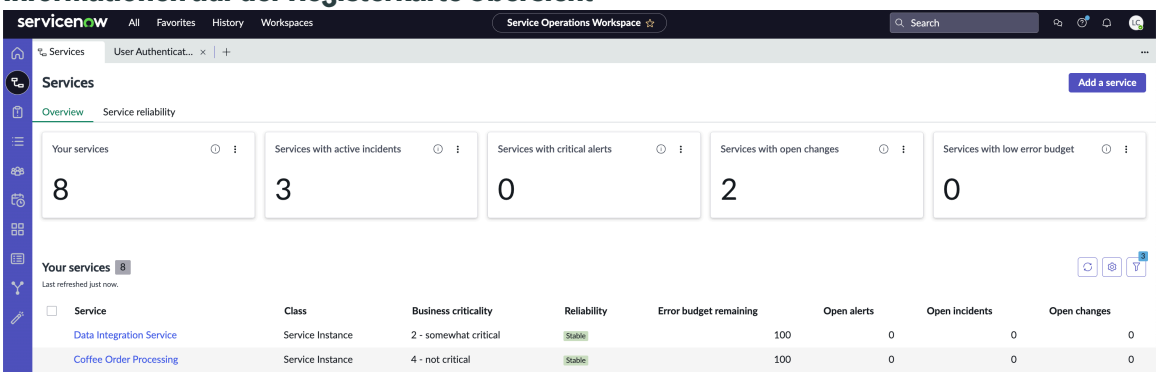
Darüber hinaus können Sie Zuverlässigkeitsmetriken für den Service erstellen. Weitere Informationen finden Sie unter Arbeiten mit Zuverlässigkeitsmetriken.

Die Bindung eines Teams und von Richtlinien an diesen Service erleichtert die Aufteilung von Verantwortlichkeiten und die Nachverfolgung technischer Ergebnisse. Es erleichtert auch die Automatisierung von Antwortroutinen und die Fokussierung darauf, wen Sie wann benachrichtigen.

Der Status eines auslaufenden Service wird geerbt. Der Status eines in erstellten Service SRM Ist **Keine** .

Serviceübersicht

Informationen auf der Registerkarte Übersicht



Die Karten auf der Registerkarte Übersicht zeigen die folgenden Metriken an. Standardmäßig zeigt die Listenansicht Informationen im Zusammenhang mit der Karte „Ihre Services“ an. Wählen Sie eine andere Karte aus, um verschiedene Informationen in der Listenansicht anzuzeigen.

- **Ihre Services** : Anzahl aller Services, die Sie oder Ihr Team auf Zuverlässigkeit verwalten und überwachen.
- **Services mit aktiven Incidents** : Services mit offenen Incidents in folgender Reihenfolge sortiert:
  - Geschäftsrelevanz: Zuerst kritisch.
  - Anzahl der aktiven Incidents – höchste zuerst.
  - Prozentsatz des verbleibenden Fehlerbudgets – niedrigster erster.
- **Services mit kritischen Warnungen** : Services mit offenen Warnungen in folgender Reihenfolge sortiert:
  - Geschäftsrelevanz: Zuerst kritisch.
  - Anzahl der Warnungen: Höchste zuerst.
  - Prozentsatz des verbleibenden Fehlerbudgets – niedrigster erster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Services mit offenen Changes** : Alle Services, die Ihr Team verwaltet und überwacht.
- **Services mit niedrigem Fehlerbudget** : Services mit weniger als 25 % verbleibendem Fehlerbudget.

  Die Fehlerbudgetmetrik wird als Betrag des Servicelevel-Ziels (SLO) dargestellt, das Sie über einen bestimmten Zeitraum ausgeben können. Es kann verwendet werden, um die Release-Geschwindigkeit zu verwalten.

Hinweis: Um die Karten- und Listenwerte zu aktualisieren, wählen Sie Aktualisieren .

Sie können mit der Liste auf folgende Arten interagieren:

- Gruppieren oder filtern Sie Spalten, um die Ansicht anzupassen.
- Bearbeiten, sortieren oder exportieren Sie die Liste nach Bedarf. Weitere Informationen finden Sie unter Listeninformationen in eine Datei exportieren.

Weitere Informationen zu einzelnen Servicedetails finden Sie unter Formular „Servicedetails bearbeiten“.

Definitionen der Servicelistenansicht

Die Spalten enthalten die folgenden Details:

- **Service**: Name des Service.
- **Klasse** : Anwendung oder technischer Service.
- **Geschäftsrelevanz** : Wichtigkeit des Service für das Unternehmen.
- **Offene Warnungen**: Anzahl der offenen Warnungen, die dem Service zugewiesen sind.
- **Offene Incidents**: Anzahl der offenen Incidents, die dem Service zugewiesen sind.
- **Verbleibendes Fehlerbudget**: Prozentsatz des für den Service verbleibenden Fehlerbudgets.

Servicezuverlässigkeit

Die Registerkarte „Service Reliability“ ist ein anpassbares Dashboard, das eine hohe Serviceleistung anzeigt. Weitere Informationen zum Dashboard finden Sie unter Visualisierungen im Dashboard „Service Reliability“.

Services zu SRM hinzufügen

Fügen Sie Services zu hinzu Service Reliability Management(SRM), damit Ihre Teams die Serviceintegrität verwalten können.

Vorbereitungen
Wenn Sie einen technischen Service zu hinzufügen SRM, Stellen Sie sicher, dass keine Supportgruppe vorhanden ist. Sie weisen die Supportgruppe zu zu zu, wenn Sie den Service hinzufügen SRM.

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie einen Service zu hinzu SRM Um es Ihren Teams zuzuweisen und ihnen Zugriff auf ihre Incidents und Warnungen zu ermöglichen. Sie können entweder einen Service erstellen oder einen vorhandenen importieren. SRM Unterstützt sowohl Anwendungsservices als auch technische Services:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwendungsservices: Geschäftsorientierte Services, z. B. ein HR-Portal. Anwendungsservices verfügen häufig über mehrere Infrastrukturkomponenten.
- Technische Services: IT-fokussierte Services, die einen Geschäfts- oder Anwendungsservice unterstützen. Zum Beispiel ein Authentifizierungsservice oder Datenbankservice.

Wenn Sie einen technischen Service zu hinzufügen SRM, Fügen Sie auch seine technischen Serviceangebote (TSOs) hinzu. TSOs sind spezifische Komponenten innerhalb eines übergeordneten technischen Service. Beispielsweise ist die Spam-Filterung ein TSO innerhalb des technischen E-Mail-Service. In SRM, Sie können einen übergeordneten technischen Service und seine TSOs verschiedenen Teams zuweisen.

Hinweis: Wenn Sie einen vorhandenen technischen Service importieren, übernehmen seine TSOs seine Supportgruppe nicht. TSOs behalten entweder ihre vorhandene Supportgruppe bei, oder wenn sie keine haben, müssen Sie sie vor der Einrichtung zuweisen SRM Servicelevel-Ziele (SLOs).

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie das Symbol Services Und wählen Sie dann aus **Fügen Sie einen Service hinzu** .
3. Im Modal „Services für Ihre Teams hinzufügen“ können Sie entweder einen Service erstellen oder vorhandene Services hinzufügen.

Option	Schritte
Erstellen Sie einen neuen Service	**a.** Wählen Sie Aus **Erstellen Sie einen neuen Service** . **b.** Füllen Sie die Felder aus. Feldbeschrei–bungen finden Sie unter Formular „Service hinzufügen“. **c.** Wählen Sie **Weiter**.
Wählen Sie vorhandene Services aus	**a.** Wählen Sie Aus **Wählen Sie vorhandene Services aus** . **b.** Suchen Sie nach Ihrem Service, und wählen Sie ihn aus. Sie können mehrere hinzufügen. **c.** Wählen Sie **Weiter**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
	Tipp: Wählen Sie das Suchfeld aus, um bis zu 25 Services anzuzeigen, die noch nicht in sind SRM, Sortiert nach Erstellungszeit. Nachdem Sie drei Zeichen eingegeben haben, werden bis zu 25 übereinstimmende Ergebnisse angezeigt. Beide Listen können Services mit oder ohne Supportgruppe enthalten. Wenn ein Service einen hat, kann die Supportgruppe ein SRM-Team oder eine Gruppe außerhalb von SRM sein.

4. Weisen Sie im Schritt Team zuweisen Ihren Service einer vorhandenen oder neuen Supportgruppe zu. In SRM, Supportgruppen werden auch als Teams bezeichnet.

Option	Schritte
Wählen Sie ein vorhandenes Team aus	Geben Sie den Namen Ihres Teams in das Suchfeld ein.
Ein Team erstellen	Wählen Sie Aus **Erstellen Sie ein Team** . Weitere Informationen zum Erstellen von Teams finden Sie unter SRM-Teams hinzufügen.

5. Wählen Sie Aus **Service hinzufügen** .
Wenn Genehmigungen nicht aktiviert sind, wird Ihr Service in der Serviceliste angezeigt. Wenn Genehmigungen aktiviert sind, wird Ihre Anforderung zur Genehmigung gesendet. Nach der Genehmigung wird der Service in der Serviceliste angezeigt.

Hinweis: Wenn Sie einen technischen Service hinzugefügt haben, werden seine TSOs auf der Registerkarte „Angebote“ auf der Seite des übergeordneten technischen Service angezeigt. TSOs werden auch in der Serviceliste angezeigt. Um einen TSO ohne zugewiesene Supportgruppe anzuzeigen, entfernen Sie alle Filter aus der Serviceliste.

Nächste Maßnahme

Wenn ein TSO keine Supportgruppe hat, weisen Sie sie einer Supportgruppe zu, bevor Sie SLOs einrichten. Informationen zum Zuweisen von Supportgruppen finden Sie unter SRM-Servicedetails bearbeiten.

Sie können Ihrem Service auch Integrationen hinzufügen, um mit der Überwachung seiner Integrität zu beginnen.

Mit SRM-Integrationen arbeiten

Verbinden Sie Ihre Services mit Überwachungstools mit Die Integrations Launchpad . Integrationen senden Informationen an Service Reliability Management(SRM), mit dem Sie Warnungen nachverfolgen, Incidents verwalten und die Serviceintegrität aufrechterhalten können.

Auf Integrations Launchpad zugreifen

Als SRM administrator, Manager oder Beantworter, Sie können auf zugreifen Integrations Launchpad Gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie in der primären Navigation die aus Integrations Launchpad Symbol ( ).
- Auf der Seite „Services“ ( ), wählen Sie einen Service aus, und wählen Sie aus **Integrationen** Registerkarte und wählen Sie dann aus **Fügen Sie eine Integration hinzu** .
- Auf der Seite „Services“ ( ), wählen Sie einen Service aus, erweitern Sie **Schließen Sie das Setup ab** , Und wählen Sie dann aus **Fügen Sie Integrationen hinzu** .

Integrationsdetails spezifisch für SRM

Beachten Sie bei der Verwendung von Folgendes Integrations Launchpad Für SRM:

Unterstützung des Connector-Typs

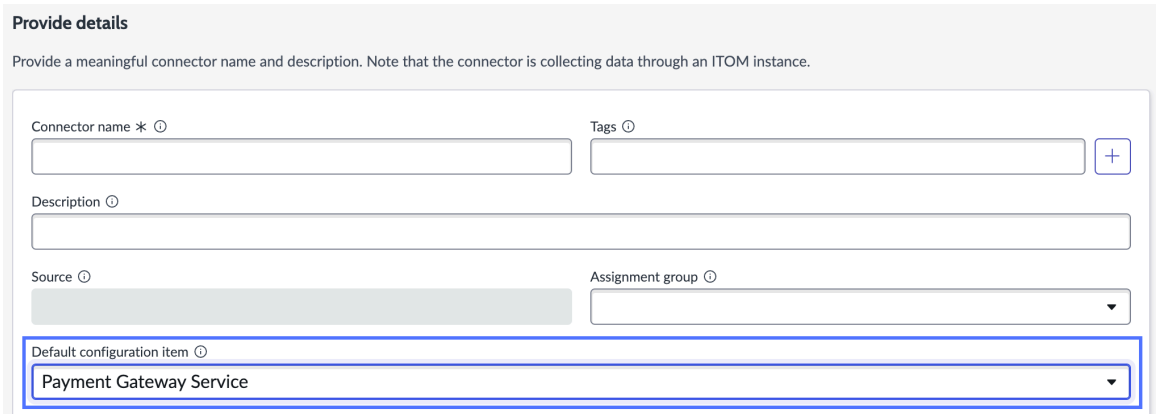
SRM Unterstützt anwenderdefinierte Connectors, Pull- und Push-Connectors. Pull-Connectors rufen Daten aus externen Quellen ab, und Push-Connectors senden Daten aus externen Quellen an Ihre Instanz.

Hinweis: Informationen zum Einrichten von Connectors finden Sie unter Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM.

Feld „Konfigurationselement“

Wenn Sie eine Integration für einrichten SRM, Der Schritt „Details angeben“ hat ein zusätzliches Feld mit der Bezeichnung „Standardkonfigurationselement“.

Legen Sie dieses Feld auf den Service fest, den Ihre Integration überwacht. Wenn eine eingehende Warnung keine Servicedetails enthält, SRM Verwendet dieses Feld, um die Warnung mit dem entsprechenden Service zu verbinden. Dieses Feld hilft sicherzustellen, dass Ihre Teams Warnungen für die von ihnen unterstützten Services erhalten.



Weitere Informationen

Besuchen Sie die folgenden Links, um Integrationen mit einzurichten und zu verwalten Integrations Launchpad. Die Seiten befinden sich in einem anderen Abschnitt, da Integrations Launchpad Ist Teil des breiteren Service Operations-Arbeitsbereich.

- Aktivieren Sie die Integration
- Konfigurieren Sie einen anwenderdefinierten Ereignis-Connector
- Konfigurieren Sie einen Ereignis-Pull-Connector
- Konfigurieren Sie einen Ereignis-Push-Connector

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Deaktivieren Sie die Integration
- Löschen Sie die Integration

SRM-Servicedetails bearbeiten

Bearbeiten Sie einen vorhandenen Service, für den Ihr Team verantwortlich ist. Geben Sie für jeden Service, für den Sie in SRM Support leisten, allgemeine Informationen über den Service und das SRM-Team an, das ihn unterstützt.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

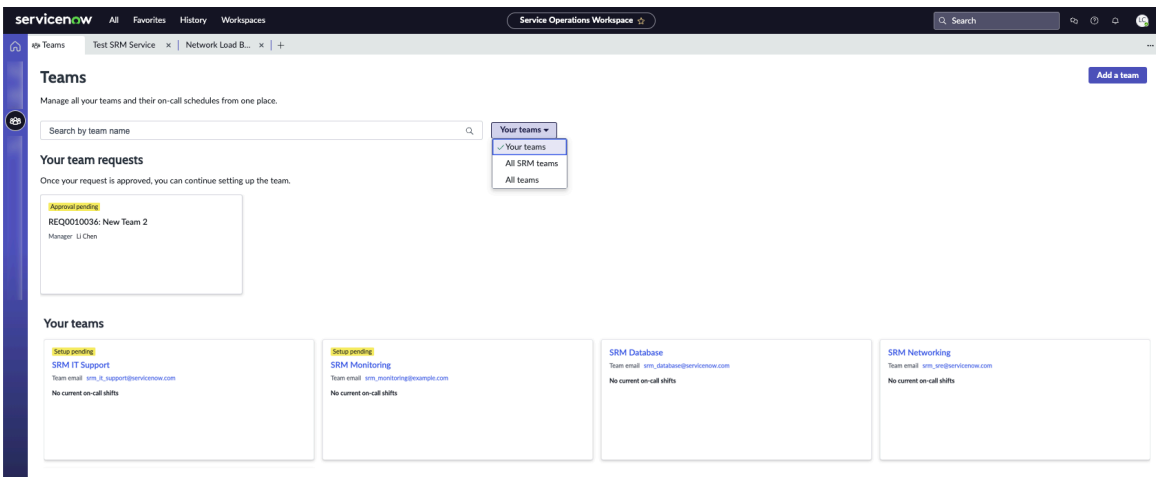
2. Wählen Sie in der primären Navigation die aus **Services** Symbol ( ).
3. Wählen Sie in Ihrer Serviceliste den Service aus, den Sie bearbeiten oder aktualisieren möchten.
   Um ein technisches Serviceangebot (Technical Service Offering, TSO) ohne zugewiesene Supportgruppe anzuzeigen und auszuwählen, entfernen Sie alle Filter aus der Liste „Services“.
4. Wählen Sie auf der Seite Übersicht die aus **Details** Registerkarte.
5. Füllen Sie die Felder aus, oder bearbeiten Sie sie.
   Weitere Informationen zu den Feldbeschreibungen finden Sie unter Formular „Servicedetails bearbeiten“.
6. Um die aktualisierten Servicedetails nach der Bearbeitung zu speichern, wählen Sie aus **Speichern** .

Mit SRM-Teams arbeiten

Verwalten Sie Zeitpläne, und definieren Sie Eskalationsrichtlinien für Ihr Team. Auf diese Weise erkennt Ihr Team, wer Rufbereitschaft hat und verantwortlich ist, und kann sich darauf verlassen, dass kritische Warnungen oder Incidents rechtzeitig bestätigt werden.

Auf der Teams-Zielseite können Sie Ihre Teams und Teamanforderungen anzeigen und verwalten.

Teams-Zielseite



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchen Sie nach Teamnamen unter Teams, denen Sie angehören, alle SRM Teams oder alle Teams in Ihrer Organisation.

Ihre Auswahl bestimmt die Karten, die auf der Teams-Zielseite angezeigt werden.

Die Auswahlmöglichkeiten lauten wie folgt:

- **Ihre Teams** (Standard)
- **Alle SRM-Teams**: Sämtliche Teams in SRM.

  Hinweis: Ihre Fähigkeit, für jedes Team Aktionen auszuführen, hängt von den Berechtigungen für das Team ab.

- **Alle Teams** : Alle Teams, auf die Sie in Ihrer Organisation Zugriff haben.

  Hinweis: Ihre Fähigkeit, für jedes Team Aktionen auszuführen, hängt von den Berechtigungen für das Team ab.

Der Abschnitt Ihr Teamanforderungen enthält Teamkarten für ausstehende Anforderungen, falls vorhanden.

Der Abschnitt „Ihre Teams“ enthält Karten, die Informationen zu einem bestimmten Team enthalten, z. B. Status des Teams, Name des Teams, Manager, Team-E-Mail-Adresse, Name und Dauer der aktuellen Schicht sowie primärer Beantworter. Weitere Informationen finden Sie unter Details Ihres SRM-Teams verwalten.

SRM-Teams hinzufügen

Fordern Sie die Erstellung eines Teams an, um mit der Überwachung Ihrer Services zu beginnen. Teams sind für die Probleme zuständig, die im Zusammenhang mit den zugehörigen Services auftreten.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow-Systemadministrator kann Teams in Ihrem Arbeitsbereich mit einem anderen Prozess einrichten. Weitere Informationen finden Sie unter Aktivieren Sie Teams und Services in SRM.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie Aus **Teams** ( ), wählen Sie aus **Fügen Sie ein Team hinzu** .
3. Erstellen Sie ein neues Team, oder fügen Sie ein vorhandenes hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
Fügen Sie ein neues Team hinzu	**a.** In **Neu oder vorhanden** Feld auswählen **Ich erstelle ein neues Team** . **b.** Füllen Sie im Formular die Felder aus. Weitere Informationen zu den Feldbe–schreibungen finden Sie unter Formular „Team erstellen“. **c.** Wählen Sie **Team hinzufügen**.
Registrieren Sie ein vorhandenes Team	**a.** In **Neu oder vorhanden** Feld auswählen **Ich möchte einer Gruppe Zugriff auf die SRM-App gewähren** . **b.** Wählen Sie ein vorhandenes Team aus der aus **Wählen Sie Team aus** Liste. **c.** Wählen Sie **Team hinzufügen**.

Ergebnis

Wenn die Anforderung genehmigt wird, wird das Team erstellt. Ihr Team wird auf der Teams-Zielseite unter angezeigt **Ihre Teams** .

Nächste Maßnahme

- Details Ihres SRM-Teams verwalten
- Richten Sie Eskalationsrichtlinien für Ihr Team in ein SRM
- Erstellen Sie einen SRM Rufbereitschaftszeitplan
- Teammitglieder zu SRM hinzufügen
- Services verwalten oder Ihrem SRM-Team hinzufügen

Details Ihres SRM-Teams verwalten

Fügen Sie Ihrem Team Mitglieder, Beschreibungen und Kontaktinformationen hinzu, oder bearbeiten Sie diese.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie die Teamkarte aus, deren Details Sie aktualisieren möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Aktualisieren Sie im Formular auf der Registerkarte **Details** die Details nach Bedarf.

Feld	Beschreibung
Name	Eindeutiger Name des Teams
Manager	Person, die das Team verwaltet.
Gruppen-E-Mail	E-Mail-Kontakt, dem alle Teammitglieder zugeordnet sind.
Beschreibung	Beschreibung des Teams, die anderen helfen soll, Verantwortlichkeiten, Zweck oder Standort des Teams zu verstehen.

5. Wählen Sie **Speichern**.

Teammitglieder zu SRM hinzufügen

Fügen Sie Ihrem Team nach Bedarf neue Teammitglieder hinzu, um zu planen, zu verwalten, Probleme zu lösen und die Effizienz des Geschäftsbetriebs zu steigern.

Vorbereitungen

Erforderliche Rolle: Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie die zu öffnende Teamkarte aus.
4. Wählen Sie die Registerkarte **Teammitglieder**.
5. Wählen Sie **Hinzufügen**.
6. Wählen Sie im Popup-Fenster aus dem Listenmenü Mitglieder aus, die hinzugefügt werden sollen.

   Hinweis: Die Mitgliederdetails werden aus Benutzerdatensätzen importiert und können nicht bearbeitet werden.

7. Wählen Sie **Hinzufügen**.

Services verwalten oder Ihrem SRM-Team hinzufügen

Fügen Sie einem Incident einen Service hinzu, um die Datenmenge für den Incident zu erhöhen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie eine Teamkarte aus, um ein Team zu öffnen, dem Sie einen Service anzeigen oder hinzufügen möchten.
4. Wählen Sie auf der Teamseite die Registerkarte **Verwaltete Services**.
   Sie können die Liste der Services exportieren. Weitere Informationen finden Sie unter Listeninformationen in eine Datei exportieren.
5. **Wahlweise:** Fügen Sie Ihrem Team einen Service hinzu, indem Sie auswählen **Hinzufügen** .
6. Fügen Sie einen neuen Service hinzu, oder registrieren Sie einen vorhandenen.

Option	Schritte
Fügen Sie einen neuen Service hinzu	**a.** In **Neu oder vorhanden** Feld auswählen **Er stellen Sie einen neuen Service in Service Reliability Management** . **b.** Füllen Sie im Formular die Felder aus. Weitere Informationen zu den Feldbe–schreibungen finden Sie unter Formular „Service hinzufügen“. **c.** Wählen Sie **Weiter**.
Registrieren Sie einen vorhandenen Service	**a.** In **Neu oder vorhanden** Feld auswählen **Ordnen Sie vorhandene CMDB-Services Service Reliability Management zu** . **b.** Wählen Sie einen oder mehrere Services aus. **c.** Wählen Sie **Weiter**.

7. Füllen Sie im Schritt Team zuweisen die Felder aus.
   - In **Serviceverantwortlicher** Wählen Sie den Anwender aus, der Eigentümer der Services sein soll.
   - In **Supportgruppe** Feld ein Team auswählen, das Services überwacht.

   Der Servicedatensatz wurde hinzugefügt.
8. Schließen Sie die Einrichtung Ihres Service ab, oder tun Sie es später.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
Schließen Sie die Einrichtung Ihres Service ab	**a.** Wählen Sie Aus **Fahren Sie mit dem Setup fort** . **b.** Wählen Sie Aus **Fügen Sie Integrationen hinzu** Und verbinden Sie Ihren Service mit einer Datenquelle, um Ereignisse zu überwachen. **c.** Wählen Sie Aus **Fügen Sie SLO und SLI hinzu** Erstellen Sie ein Servicelevel-Ziel, und messen Sie Ihre Serviceintegrität mit einem Servicelevel-Indikator.
Später erledigen	Wählen Sie Aus **Tun Sie es später** .

Siehe SRM-Servicedetails bearbeiten Und Formular „Servicedetails bearbeiten“ Für Informationen zum Service und zum Abschluss des Setups.

Erstellen Sie einen SRM Rufbereitschaftszeitplan

Richten Sie einen Rufbereitschaftszeitplan ein, um sicherzustellen, dass jemand verfügbar ist, um auf Incidents und kritische Warnungen zu reagieren.

Vorbereitungen

Vor dem Erstellen eines Rufbereitschaftszeitplans muss ein Team in vorhanden sein Service Reliability Management(SRM). Die Warnungstabelle [em_Alert] muss auch der Liste Konfiguration der Auslöserregeltabelle hinzugefügt werden. Siehe SRM-Teams hinzufügen und Fügen Sie eine Warnungstabelle hinzu, um die Bereitschaftsplanung für zu aktivieren Service Operations-Arbeitsbereich Für ITOM, um weitere Informationen zu erhalten.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

Warum und wann dieser Vorgang ausgeführt wird

Mit Schichten können Sie in SRM für Ihr in Schichten arbeitendes Personal variable Zeiträume definieren. Erstellen Sie Schichten für bestimmte Tage und Zeiten, zu denen Sie eine Abdeckung benötigen, und weisen Sie sie den Teammitgliedern zu.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** > **Teams ( )**an.
2. Wählen Sie auf der Seite Teams Ihr Team aus.
3. Wählen Sie aus **Zeitplan** Registerkarte und wählen Sie dann aus **Schicht erstellen** .
4. Wählen Sie im Dialogfeld „Neu erstellen“ eine der beiden Optionen aus **Erstellen Sie neu** Oder **Vorlage verwenden** .
   Ihr Systemadministrator kann vordefinierte Vorlagen erstellen, die Sie zum Erstellen von Schichten verwenden können.
5. Füllen Sie die Felder aus.
   Weitere Informationen zu den Feldbeschreibungen finden Sie unter Erstellen Sie ein Schichtformular in Service Reliability Management.
6. Wählen Sie **Create shift (Schicht erstellen)**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die Einstellungen des Rufbereitschaftsteams in fest SRM

Legen Sie Rufbereitschaftseinstellungen für Teammitglieder fest, um die Effizienz Ihres Geschäftsbetriebs zu steigern.

Vorbereitungen

Erforderliche Rolle: srm_Manager oder srm_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie die zu öffnende Teamkarte aus.
4. Wählen Sie aus **Einstellungen des Rufbereitschaftsteams** Schaltfläche.
5. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Schichtmanager in Rufbereitschaft	Teammanager für die Rufbereitschaftsschicht.
PTO-Anforderungen	Von Teammitgliedern gestellte Anträge auf bezahlte Auszeit. Die Auswahlmöglichkeiten lauten wie folgt: ○ Systemstandard (nicht zulässig) ○ Mit Genehmigung ○ Ohne Genehmigung ○ Nicht zulässig
Erster Wochentag	Erster Tag Ihrer Arbeitswoche. **Hinweis:** Diese Option ist nur für Washington DC und spätere Versionen verfügbar.
Überschneidung von Schichtzeitplänen zulassen	Option, mit der Zeitpläne überlappen können
Eskalationsregel bei Schichtüberschneidung	Die Auswahlmöglichkeiten lauten wie folgt: ○ Systemstandard (an alle Schichten eskalieren) ○ An ausgehende Schicht eskalieren ○ An eingehende Schicht eskalieren ○ An alle Schichten eskalieren

6. Wählen Sie **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Eskalationsrichtlinien für Ihr Team in ein SRM

Richten Sie eine Eskalationsrichtlinie für Ihr Team ein, um sicherzustellen, dass Warnungen oder Incidents vom entsprechenden Teammitglied rechtzeitig gelöst werden.

Vorbereitungen

Bevor Sie eine Eskalationsrichtlinie erstellen, müssen Sie eine Rufbereitschaftsschicht für Ihr Team erstellen.

Hinweis: Nur der Beantworter, der das Team erstellt hat, und der Manager des Teams können Eskalationsrichtlinien für das einrichten.

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Eine Eskalationsrichtlinie ist eine Reihe von Richtlinien, die beschreiben, wie und wann Incidents auf höhere Berechtigungsstufen hochgestuft werden sollen. Sie definiert klare Verfahren und Verantwortlichkeiten für die Eskalation ab, damit Beantworter Probleme schnell beheben können. Definiert die Reihenfolge, in der Benachrichtigungen eskaliert werden sollen, wenn eine Warnung oder ein Incident nicht innerhalb einer definierten Zeit bestätigt oder gelöst wird. Wenn niemand antwortet, basiert die Eskalation auf Ihren definierten Richtlinien, bis jemand antwortet. Nachdem ein Teammitglied geantwortet hat, wird die Eskalationsrichtlinie nicht mehr eskaliert, und es werden keine weiteren Benachrichtigungen gesendet.

Hinweis: Der Eskalations-Workflow wird nur ausgelöst, wenn eine aktive Schicht vorhanden ist.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie die Registerkarte **Eskalationsauslöser und -richtlinien**.
4. Wählen Sie im linken Bereich von **Eskalationsrichtlinien** die Option **Richtlinie erstellen**.
5. Füllen Sie die Felder im Formular „Eskalationsrichtlinie“ aus.
   Weitere Informationen finden Sie unter Formular „Eskalationsrichtlinien einrichten“ in SRM
6. **Wahlweise:** Wählen Sie Aus **Fügen Sie einen Eskalationsschritt hinzu** Zum Definieren der zusätzlichen Schritte für Eskalations- und Eskalationspfad.
   Weitere Informationen zum Formular „Eskalationsschritt hinzufügen“ finden Sie unter Formular „Eskalationsrichtlinien einrichten“ in SRM.
7. Wählen Sie **Änderungen speichern**.
8. **Wahlweise:** Fügen Sie dem Team eine weitere Eskalationsrichtlinie für eine andere Warnungs- oder Incident-Kategorie hinzu, indem Sie auswählen **Fügen Sie eine Richtlinie hinzu** .

Erstellen Sie einen Eskalationsauslöser für ein SRM-Team

Definieren Sie Bedingungen, die die Eskalationsrichtlinie eines Teams in auslösen Service Reliability Management(SRM).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: srm_Manager oder srm_admin

Warum und wann dieser Vorgang ausgeführt wird
Dieses Verfahren zeigt, wie Eskalationsauslöser in erstellt werden SRM. Wenn Ihre Organisation die Bereitschaftsplanung mit verwaltet IT Service Management(ITSM), können Sie auch verwenden ITSM Bereitschaftsplanung Zum Definieren von Eskalationsauslösern. Weitere Informationen finden Sie unter Eskalationsauslöserregeln erstellen . Während dieses Verfahren auflistet ITSM Rollen, SRM Anwender benötigen nur die Rolle srm_Manager oder srm_admin, um die Aufgabe abzuschließen.

Für einen umfassenderen Überblick über Eskalationsprozesse in ITSM, Siehe Eskalationsprozess entwerfen .

Hinweis: Das folgende Verfahren unterstützt Auslöserbedingungen nur basierend auf Änderungen der Zuweisungsgruppe. Für Auslöserbedingungen, die auf anderen Feldern basieren, ist eine Problemumgehung erforderlich. Wenden Sie sich an den ServiceNow-Support, um in der ServiceNow Support Knowledge Base auf KB1702299 zuzugreifen.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Teams** Symbol ( ).
3. Wählen Sie Ihr Team und dann aus **Eskalationsauslöser und -Richtlinien** Registerkarte.
4. Unter **Eskalationsauslöser** Wählen Sie im -Bereich aus **Auslöser erstellen** .
5. Füllen Sie die Felder im Formular „Eskalationsauslöser“ aus.

Formular „Eskalationsauslöser“

Feld	Beschreibung
Name des Eskalationsauslösers	Name des Auslösers.
Reihenfolge	Reihenfolge der Ausführung. Wenn in einem Team mehrere Eskalationsauslöser vorhanden sind, wird zuerst derjenige mit einer kleineren Ordnungsnummer überprüft.
Aktiv	Option zum Aktivieren oder Deaktivieren des Auslösers.
Bedingungen	Bedingungen für den Auslöser. Wählen Sie eine Tabelle und einen Bedingungssatz aus. Wenn die Bedingungen erfüllt sind, werden Eskalationsauslöser für Schichten im SRM-Team ausgelöst.

6. Wählen Sie **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können auch Unterstützung für Eskalationsauslöser hinzufügen, die für Warnungen anstelle von Incidents ausgeführt werden. Sie können bis zu 5000 Ereignisse oder 250 Warnungen pro Sekunde-Stream hinzufügen. Um die Unterstützung für Rufbereitschaft für Warnungen hinzuzufügen, führen Sie entweder die XML-Datei in der Auslösertabelle „Trigger_rule_table_cfg“ aus, oder erstellen Sie den Datensatz manuell auf der Seite „Konfiguration der Auslöserregel-Tabelle“.

Mit SRM-Zuverlässigkeitsaufgaben arbeiten

Warnungen, Incidents und Change-Anforderungen sind Zuverlässigkeitsaufgaben. Von der Erstellung bis zur Lösung, SRM Hilft Ihnen, Ihre Warnungen während des gesamten Antwortlebenszyklus zu verwalten.

Der Bereich „Zuverlässigkeitsaufgaben“ ( ) Hat mehrere Registerkarten:

- **Incidents** Werden manuell oder basierend auf Servicelevel-Zielen (Service Level Objectives, SLOs) und Servicelevel-Indikatoren (Service Level Indicators, SLIs) erstellt. Weitere Informationen zu Incidents finden Sie unter In SRM mit Incidents arbeiten. Weitere Informationen zu SLO-, SLI- und Fehlerbudgetaktionen finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.
- **Changes** Kann in erstellt werden SRM. Weitere Informationen finden Sie unter Change-Aufgabe in SRM manuell erstellen.

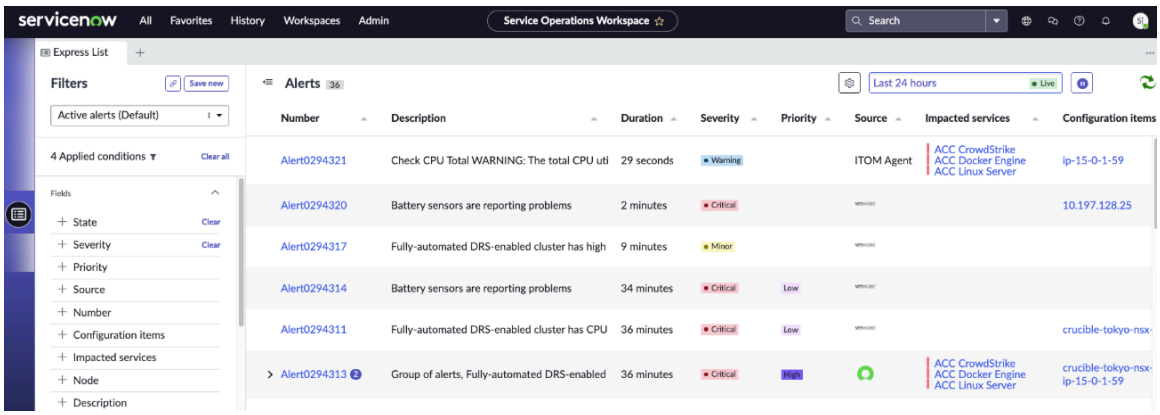
Der Express-Listenbereich ( ) Bietet eine fokussierte Ansicht von Warnungen, damit Sie Integritätsprobleme effizient überwachen, bewerten und lösen können. Sie können Warnungen aus erstellen SRM Serviceseiten oder mithilfe von Integrationen. Weitere Informationen zu Warnungen finden Sie unter Express-Liste In Service Operations-Arbeitsbereich Für ITOM Und SRM-Warnungen manuell erstellen.

Beantworter und höher werden basierend auf ihren Benachrichtigungseinstellungen über Aktualisierungen von Zuverlässigkeitsaufgaben benachrichtigt.

Arbeiten mit Warnungen in SRM

Überwachen, bewerten und lösen Sie Integritätsprobleme in der Express-Liste.

Die Funktion „Ereignismanagement Express-Liste“ bietet eine anpassbare, sortierbare Ansicht für den Zugriff auf und die Verwaltung von Warnungen. Verwenden Sie die Funktion „Express-Liste“, um Warnungen zu priorisieren, ihre Auswirkungen zu verstehen und Probleme schneller zu lösen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Service Reliability Management(SRM) Anwender haben Sie automatisch die Rolle evt_Team_Operator, mit der Sie auf die Express-Listenfunktion zugreifen können ( ). Weitere Informationen zu dieser Rolle finden Sie unter Von verwendete Rollen Express-Liste.

Besuchen Sie Folgendes, um mit Warnungen in der Express-Listenfunktion zu arbeiten:

- Bestätigen Sie die angezeigten Warnungen in Express-Liste
- Weisen Sie Warnungen in zu Express-Liste
- Schließen Sie eine Warnung in Express-Liste
- Erstellen Sie einen Incident aus einer Warnung in Express-Liste
- Eingehende Warnungen überwachen
- Warnungen in den Status „Bestätigt“ versetzen
- Warnungen in den Status „Wartung“ versetzen

In SRM, Integrationen erstellen Warnungen, oder Sie erstellen Warnungen manuell. Unter dem folgenden Link erfahren Sie, wie Sie eine Warnung aus erstellen **Services** Seite:

SRM-Warnungen manuell erstellen

Erstellen Sie eine Warnung zu Testzwecken oder wenn Sie der Meinung sind, dass ein Problem ein Risiko darstellt.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie im Navigationsbereich aus **Services** .
3. Wählen Sie den Service aus, für den Sie eine Warnung auslösen möchten.
4. Wählen Sie aus **Zugehörige Warnungen** Registerkarte.
5. Wählen Sie Aus **Warnung auslösen** Und füllen Sie aus **Lösen Sie eine Warnung aus** Formular.

   Um eine Warnung auszulösen, müssen Sie zuerst ein Ereignis erstellen, um verarbeitet zu werden. Nur **Service** Ist erforderlich.

Eine Warnung auslösen

Feld	Beschreibung
Service	Wählen Sie einen Service für das Ereignis aus.
Quelle	Manuell.
Knoten	Geben Sie den Namen des Knotens (z. B. FQDN, IP-Adresse oder MAC-Adresse) ein, der dem Ereignis zugeordnet ist.
Typ	Geben Sie den Typ des Ereignisses ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ressource	Geben Sie eine Knotenressource (Prozess oder Service) ein, die dem Ereignis zugeordnet ist.
Metrikname	Geben Sie den Namen der Metrik ein, die dem Ereignis zugeordnet ist.
Quellinstanz	Geben Sie eine Datenquelle für das Ereignis ein.
Nachrichtenschlüssel	Geben Sie einen Bezeichner für mehrere Ereignisse ein, die sich auf dasselbe Ereignis beziehen.
Schweregrad	Wählen Sie die erwarteten Auswirkungen dieses Ereignisses aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Kritisch: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ○ Schwerwiegend: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung wurde beeinträchtigt. ○ Geringfügig (Standard): Ein partieller, nicht kritischer Verlust der Funktionalität oder eine Leistungsverschlechterung ist aufgetreten. ○ Warnung: Aufmerksamkeit ist erforderlich, obwohl die Ressource noch funktionsfähig ist. ○ OK: Die Ressource ist weiterhin funktionsfähig.
Zeit des Ereignisses	Wählen Sie das Datum und die Uhrzeit aus, zu der das Ereignis im Quellsystem aufgetreten ist.
Beschreibung	Geben Sie Informationen ein, die das Ereignis beschreiben.
Zusätzliche Informationen	Fügen Sie weitere Informationen hinzu, die für das Ereignis relevant sind.
Verarbeitungsnotizen	Geben Sie relevante Verarbeitungsinformationen ein.

6. Wählen Sie **Auslöser**.
   Service Reliability Management (SRM) erstellt ein Ereignis, um die Warnung zu generieren. Aktualisieren Sie den Bildschirm, um die Ergebnisse der Ereignisverarbeitung anzuzeigen.

   Die Express-Liste zeigt Ihre Warnung automatisch an. Wenn aktiviert, SRM Löst die entsprechenden Automatisierungen und Bereitschaftseskalations-Workflows aus.

Nächste Maßnahme

Erwägen Sie, die folgenden optionalen Anpassungen an Ihrer Warnung zu Testzwecken oder zur Teamzusammenarbeit vorzunehmen:

- Bestätigen Sie die Warnung, oder weisen Sie sie jemandem in Ihrem Team zu.
- Fügen Sie Kommentare oder Arbeitsnotizen in hinzu **Verfassen** Bereich.
- Fügen Sie mithilfe des Anhangssymbols einen Anhang hinzu, der sich auf die Warnung bezieht .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In SRM mit Incidents arbeiten

Planen Sie Serviceunterbrechungen im Voraus, und lassen Sie SRM Benachrichtigungen senden und Status erstellen, wenn Incidents auftreten. Ablenkungen werden minimiert, und der Fokus der Teams liegt stärker auf der Behebung von Problemen.

Sie können Incidents in SRM manuell erstellen oder eine Fehlerbudgetaktion dazu erstellen. Weitere Informationen finden Sie unter SRM-Incidents manuell erstellen und Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

- Manuelle Erstellung aus einer Warnung .
- Manuelle Erstellung in der Incident-Ansicht .
- Automatisch aus Warnungsautomatisierungen, wenn die gleichnamige App installiert ist.

Das Feld **Zugewiesen an** für einen Incident legt fest, wer benachrichtigt werden soll. Wenn ein Team als Beantworter ausgewählt ist, werden Teamautomatisierungen überprüft, um zu bestimmen, welcher Zeitplan für die Benachrichtigungen verwendet werden soll.

Hinweis:

Das Feld **Zugewiesen an** wird gelöscht, wenn das Feld **Assigned-team (Zugewiesenes Team)** oder **Service** eines Incident aktualisiert wird. Eskalationsrichtlinien für neu zugewiesene Teams werden ausgeführt. Das Feld bleibt leer, bis ein Benutzer des neuen Teams eine Eskalationsbenachrichtigung bestätigt.

Wenn der Service geändert wird und dem neuen Service kein Team zugewiesen ist, finden keine Änderungen statt.

Wenn ein Service gelöscht wird, werden seine Integrationen, Warnungen, Incidents und Automatisierungen entfernt. Das Löschen eines Service ist keine wiederherstellbare Aktion. Erwägen Sie stattdessen, den Service zu deaktivieren.

Beantworter und höhere Rollen werden basierend auf ihren Benachrichtigungseinstellungen über Aktualisierungen von Incidents benachrichtigt. Wenn Sie die Aktualisierung vorgenommen haben, werden Sie nicht benachrichtigt.

Sie können Incidents lösen, indem Sie bestimmte Incidents auswählen oder mit einer Mehrfachauswahl arbeiten. Beachten Sie dazu SRM-Incidents lösen, SRM-Incidents schließen oder SRM-Incidents abbrechen.

Hinweis:

Incidents mit dem Status **Gelöst** werden nach 3 Tagen automatisch geschlossen.

Weitere Informationen zu den Bereichen und Feldern, die in einem Incident verfügbar sind, finden Sie unter SRM Incidents.

Listeninformationen in eine Datei exportieren in der Listenansicht.

Reagieren Sie auf einen Incident wie folgt:

- Markieren Sie einen Incident.
- Priorität eines SRM-Incident aktualisieren.
- Legen Sie den Incident-Status fest.
- SRM-Incidents kopieren.
- Services zu einem SRM-Incident hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- SRM Incidents.
- SRM-Incidents lösen.
- SRM-Incidents abbrechen.
- SRM-Incidents schließen.
- SRM-Incidents erneut öffnen.

SRM-Incidents manuell erstellen

Erstellen Sie einen Incident, wenn ein Problem Ihrer Meinung nach ein erhebliches Risiko darstellt und so bald wie möglich behoben werden muss.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte Incidents aus.
4. Wählen Sie **Neu**.
5. Füllen Sie die entsprechenden Felder im Formular „Neuen Incident erstellen“ aus.

   Nur das Feld **Kurzbeschreibung** ist erforderlich.

Incident-Feldzuordnung

Feld	Beschreibung
Kurzbeschreibung	Fügen Sie eine kurze Beschreibung des Incident hinzu.
Beschreibung	Fügen Sie eine detaillierte Beschreibung des Incident hinzu.
Nummer	Bezeichner, der dem Incident zugewiesen ist.
Auswirkung	Die Auswahl ist ein Maß für die Auswirkung des Incident. Die Auswirkung wirkt sich auf die **Priorität** aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 - Hoch ○ 2 – Mittel ○ 3 - Niedrig
Zuweisungsgruppe	Wählen Sie durch Eingabe oder Suche ein Team aus, das an dem Incident arbeiten soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Priorität	Wird automatisch basierend auf **Auswirkung** und **Dringlichkeit** festgelegt. Gibt an, wie schnell der Incident behandelt werden soll. Beachten Sie dazu die Tabelle **Regeln für Datensuche mit Priorität** unten. Werte sind: ○ 3 - Mittel ○ 4 – Niedrig ○ 5 - In Planung
Kategorie	Wählen Sie eine Kategorie für den Incident aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ – Keine Angabe – ○ Anforderung/Hilfe (Standard) ○ Software ○ Hardware ○ Netzwerk ○ Datenbank
Dringlichkeit	Wählen Sie einen Maß dafür, wie lange die Lösung hinausgeschoben werden kann, bis ein Incident erhebliche Geschäftsauswirkungen hat. Die Dringlichkeit wirkt sich auf die **Priorität** aus.
Service	Wählen Sie einen Service aus, der dem Incident zugeordnet ist.
Schweregrad	Wählen Sie durch Eingabe oder Suche einen Schweregrad aus, der dem Incident zugeordnet werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 - Hoch ○ 2 – Mittel ○ 3 - Niedrig
Konfigurationselement	Wählen Sie durch Eingabe oder Suche ein Asset aus, das dem Incident zugeordnet werden soll.
Zugewiesen an	Weisen Sie durch Eingabe oder Suche ein Teammitglied zu, das an dem Incident arbeiten soll.
Status	Wählen Sie einen Status für den Incident aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Neu (Standard) ○ In Bearbeitung ○ Angehalten ○ Gelöst ○ Abgebrochen Weitere Informationen finden Sie unter Status von SRM-Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beobachtungsliste	Wählen Sie durch Eingabe oder Suche Einzelpersonen aus, die an dem Incident arbeiten sollen.
Lösungscode	Wählen Sie (falls vorhanden) einen Lösungscode aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Keine (Standard) ○ Duplikat ○ Known Error ○ Keine Lösung bereitgestellt ○ Von Anrufer gelöst ○ Gelöst durch Change ○ Gelöst durch Problem ○ Gelöst durch Anforderung ○ Lösung bereitgestellt
Lösungsnotizen	Geben Sie alle relevanten Lösungsinformationen ein.

Hinweis: Die Priorität wird anhand der folgenden Beispielregeln für die Datensuche berechnet:

Regeln für Datensuche mit Priorität

Auswirkung	Dringlichkeit	Priorität
1 – Hoch	1 – Hoch	1 - Kritisch
1 – Hoch	2 – Mittel	2 – Hoch
1 – Hoch	3 – Niedrig	3 – Mittel
2 – Mittel	1 – Hoch	2 – Hoch
2 – Mittel	2 – Mittel	3 – Mittel
2 – Mittel	3 – Niedrig	4 – Niedrig
3 – Niedrig	1 – Hoch	3 – Mittel
3 – Niedrig	2 – Mittel	4 – Niedrig
3 – Niedrig	3 – Niedrig	5 - In Planung

6. Wählen Sie **Speichern**.
   Der Incident wird erstellt, und das Formular für einen neuen Incident wird angezeigt.
7. Fügen Sie in einen Anhang hinzu, der sich auf den Incident bezieht **Aktionen** Bereich mit **Anhänge** Symbol .
8. Erstellen Sie eine Incident-Vorlage über das Vorlagensymbol .
9. Starten Sie im Bereich **Zusammenarbeit** ein Zoom-Meeting, Microsoft Teams oder einen Slack-Kanal, oder nehmen Sie daran teil..

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wählen Sie **Speichern**.
    Der Incident wird in Kommentaren, Arbeitsnotizen und Incident-Aktivitäten angezeigt, die im **Aktivitätenstrom** erfasst werden. Weitere Informationen zu Incident-Feldern finden Sie unter SRM Incidents.

SRM-Incidents neu zuweisen

Weisen Sie einen Incident einem Beantworter neu zu, wenn die Incident-Aufgaben von einem bestimmten Teammitglied bearbeitet werden sollen.

Vorbereitungen

Diese Aktion ist verfügbar, wenn das Feld **Zugewiesen an** im Incident ausgefüllt ist.

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Sie haben zwei Möglichkeiten.

Option	Bezeichnung
Option	Beschreibung
In der Incident-Listenansicht	Doppelklicken Sie auf das Feld **Zugewiesen an** für den Incident, und ersetzen Sie das Teammitglied über das Listenmenü.
Auf der Registerkarte Details des Incident-Formulars	Löschen Sie den Namen im Feld **Zugewiesen an**, und weisen Sie ihn neu zu. Wählen Sie **Speichern**.

Der Incident ist jetzt dem neuen Beantworter zugewiesen, dem eine E-Mail-Benachrichtigung zugesendet wird. Der Beauftragte wird in der Listenansicht und im Formular angezeigt.

Priorität eines SRM-Incident aktualisieren

Wenn die Priorität eines Incident geändert werden soll, können Sie sie manuell auf die neue Relevanz aktualisieren.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Wählen Sie in der Ansicht „Incident-Liste“ im Listenmenü einen Wert für **Priorität** aus.
   - 1 – Kritisch
   - 2 – Hoch
   - 3 – Mittel
   - 4 – Niedrig
   - 5 – Planung (Standard)
5. Wählen Sie **OK**.
   Die neue Priorität wird in der Incident-Listenansicht, im Incident-Header und im Formularfeld angezeigt.

Services zu einem SRM-Incident hinzufügen

Fügen Sie einem Incident einen Service hinzu, um die Datenmenge für den Incident zu erhöhen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Sie haben zwei Möglichkeiten.

Option	Beschreibung
In der Incident-Listenansicht	Doppelklicken Sie auf das Feld **Service** für den Incident, und ersetzen Sie das Teammitglied mithilfe der Suche. Wählen Sie **OK**.
Im Incident-Formular	Wählen Sie einen neuen Wert für **Service** aus dem Listenmenü aus. Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Service wird in der Incident-Listenansicht und im Incident-Formular angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM-Incidents Lösungscodes und -hinweise hinzufügen

Fügen Sie einem Incident einen Lösungscode und -hinweise hinzu, wenn Sie den Incident gelöst haben.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident.
4. Wählen Sie im Bereich **Details** des Incident einen **Lösungscode** aus dem Listenmenü aus.
5. Geben Sie Text in das Textfeld **Lösungshinweise** ein.
   Die Lösungshinweise werden im Zeitleistenbereich **Aktivität** angezeigt.
6. Wählen Sie **Speichern**.

SRM-Incidents kopieren

Kopieren Sie einen Incident, wenn Sie ein ähnliches Problem haben.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident, den Sie kopieren möchten.
4. Wählen Sie im Listenmenü unter der Schaltfläche „Weitere Optionen“ die Option **Incident kopieren** aus.
5. Wählen Sie im Listenmenü für das Feld **Anrufer** ein Teammitglied aus.
   Nachdem der Incident kopiert wurde, wird die Zeitleiste **Aktivität** des neuen Incident mit dem ursprünglichen Incident als Arbeitsnotiz aktualisiert.

SRM-Incidents lösen

Lösen Sie einen Incident, wenn dieser überprüft werden muss oder wenn Sie der Meinung sind, dass er bereits bearbeitet wurde, aber noch nicht so weit ist, dass er geschlossen werden könnte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnis
Gelöste Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident lösen, bleiben die zugehörigen Warnungen geöffnet, bis Sie den Incident schließen.

SRM-Incidents abbrechen

Schließen Sie einen Incident, wenn Sie der Meinung sind, dass es sich nicht um ein Problem handelt oder wenn er bereits behandelt wurde.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*an.
   Sie werden zu weitergeleitet SRM Homepage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident, den Sie abbrechen möchten.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnis

Abgebrochene Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident abbrechen, werden die zugehörigen Warnungen geschlossen.

SRM-Incidents schließen

Schließen Sie einen Incident, wenn Sie der Meinung sind, dass es sich nicht um ein Problem handelt oder wenn er bereits behandelt wurde.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Sie haben zwei Möglichkeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnis
Geschlossene Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident schließen, werden die zugehörigen Warnungen geschlossen.

SRM-Incidents erneut öffnen

Öffnen Sie einen geschlossenen Incident erneut, wenn Sie denken, dass das Problem noch nicht gelöst wurde.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation aus **Zuverlässigkeitsaufgaben** ( ).
3. Suchen und öffnen Sie den Incident, den Sie erneut öffnen möchten.
   Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Change-Aufgabe in SRM manuell erstellen

Erstellen Sie eine Change-Aufgabe, um einen kontrollierten Prozess zum Ändern genehmigter und unterstützter Aktionen für SRM zu implementieren.

Vorbereitungen

Allgemeine Informationen zu Change-Anforderungen finden Sie unter Change-Management verwenden .

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie Aus **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Changes**.
4. Wählen Sie im Header der Liste **Changes** die Option **Neu**.
5. Suchen Sie im Fenster **Einen Change auswählen** nach einem Change-Datensatz, oder wählen Sie eine SOW-Karte zur Change-Erstellung aus, um den Typ der Change-Anforderung auszuwählen.
6. Wählen Sie **Weiter**.
7. Füllen Sie auf der Registerkarte „Formulardetails“ die Felder in aus **Change-Anforderung** , **Auswirkung** , **Zuweisung** , **Planung** , **Zeitplan** , **Notizen** , Und **Abschlussinformationen** Formulare.
   Weitere Informationen finden Sie unter Erstellen Sie Change-Anforderungsformulare.
8. **Wahlweise:** Wählen Sie **Mir zuweisen**.
9. Wählen Sie **Speichern**.

   Die Change-Anforderung wird erstellt, und für die Anforderung wird die Registerkarte **Zugehörige Datensätze** angezeigt.

10. **Wahlweise:** Sie können die folgenden Schritte im **Status**-Workflow ausführen.

    (Optional) Wenn die Change-Anforderung eine Genehmigung erfordert, wird angezeigt **Genehmigung anfordern** Schaltfläche. Wählen Sie **Genehmigung anfordern**. Der **Status** wechselt zu **Bewerten**. Siehe Genehmigen Sie eine Change-Anforderung für SRM Für Anweisungen zum Genehmigen einer Change-Anforderung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Change-Anforderung vorab genehmigt wurde oder keine Genehmigung erfordert, können Sie verschieben **Status** Bis **Geplant** .

Nach der Genehmigung und Planung können Sie **Implementieren** wählen, um die Change-Anforderung in die Tat umzusetzen.

Sobald die Change-Anforderung implementiert wurde, prüfen Sie die Details, und wählen Sie „Überprüfen“. Die Change-Anforderung wechselt in den Status **Überprüfen**.

Hinweis: Alle offenen Change-Aufgaben werden auf **Abgebrochen** gesetzt.

Weitere Informationen zum **Status** von Change-Anforderungen finden Sie unter Status von SRM-Change-Anforderungen.

Service Reliability Management – Referenz

Referenzthemen enthalten zusätzliche Informationen zur Verwendung von Service Reliability Management.

SRM Rollen und Verantwortlichkeiten

Mit Rollen können Sie Benutzern Zugriff auf verschiedene Teile der SRM-Konsole gewähren. Rollen bestimmen die Aktionen, in denen Anwender ausführen können oder nicht Service Reliability Management.

SRM besitzt die folgenden vordefinierten Rollen:

Hinweis: Die SRM-Experience wurde so optimiert, dass nur die SRM-Rollen vorhanden sind. Zusätzliche Rollen könnten die UI verändern und unbeabsichtigte Folgen haben.

Rollenliste

Rolle	Aufgaben
SRM-Administrator [srm_admin]	• Aktualisieren Sie einen Service, der von einem beliebigen SRM-Team verwaltet wird • Weisen Sie neue Incidents zu • Erstellen und bearbeiten Sie Incidents • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Aktualisieren Sie ein beliebiges SRM-Team • Erstellen und bearbeiten Sie Rufbereitschaftsschichten • Rufbereitschaftsschichten löschen • Eskalationsrichtlinien und -Auslöser erstellen und bearbeiten • Eskalationsrichtlinien und -Auslöser löschen • Anforderung der Abdeckung planen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenliste (Fortsetzung)

Rolle	Aufgaben
	• Abwesenheit übermitteln • Ereignis erstellen
SRM-Manager [srm_Manager]	• Aktualisieren Sie einen von Ihrem SRM-Team verwalteten Service • Weisen Sie neue Incidents zu • Erstellen und bearbeiten Sie Incidents • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Aktualisieren Sie die von Ihnen verwalteten SRM-Teams • Erstellen und bearbeiten Sie Rufbereitschaftsschichten • Rufbereitschaftsschichten löschen • Eskalationsrichtlinie und -Auslöser erstellen und bearbeiten • Eskalationsrichtlinien und -Auslöser löschen • Anforderung der Abdeckung planen • Abwesenheit übermitteln • Ereignis erstellen
SRM-Responder [srm_Responder]	• Aktualisieren Sie einen Service, wenn Sie sich in der an den Service gebundenen Supportgruppe befinden • Weisen Sie neue Incidents zu • Erstellen und bearbeiten Sie Incidents • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Rufbereitschaftsschichten anzeigen • Zeigen Sie Eskalationsrichtlinien und -Auslöser an • Kontakteinstellungen bearbeiten • Anforderung der Abdeckung planen • Abwesenheit übermitteln • Ereignis erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenliste (Fortsetzung)

Rolle	Aufgaben
Administrator [admin]	• Aktualisieren Sie einen von Ihrem SRM-Team verwalteten Service • Löschen Sie Services • Weisen Sie neue Incidents zu • Erstellen und bearbeiten Sie Incidents • Erstellen und bearbeiten Sie Changes • Löschen Sie Incidents • Erstellen Sie Teams • Aktualisieren Sie die von Ihnen verwalteten SRM-Teams • Rufbereitschaftsschichten löschen • Kontakteinstellungen überschreiben • Warnung manuell erstellen • Löschen Sie Warnungen • Abwesenheit übermitteln

Formular „Team erstellen“

Fordern Sie die Erstellung eines Teams an, um mit der Überwachung Ihrer Services zu beginnen.

Erstellen Sie ein Teamformular

Weitere Informationen finden Sie unter SRM-Teams hinzufügen.

Feld	Beschreibung
Teamname	Name des Teams.
Teammanager	Manager für das Team.
Team-E-Mail	E-Mail-Kontakt für das Team.
Teammitglieder	Mitglieder für Ihr Team.
Tags	Begriffe, die Ihr Team beschreiben oder sich darauf beziehen.
Kurze Beschreibung der Teamverantwortlichkeiten	Beschreibung Ihres Teams. Beispielsweise die Teamverantwortlichkeiten oder der geografische Standort.

Erstellen Sie ein Schichtformular in Service Reliability Management

Richten Sie für Ihr Team einen Rufbereitschaftszeitplan ein, um sicherzustellen, dass immer die richtige Person verfügbar ist, um schnell auf Incidents und kritische Warnungen zu reagieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Schichtformular

Weitere Informationen finden Sie unter Erstellen Sie einen SRM Rufbereitschaftszeitplan.

Create new shift (Neue Schicht erstellen)

Feld	Beschreibung
Schichtname	Name der Schicht.
All day shift (Ganztägige Schicht)	Wenn diese Option ausgewählt ist, ist die Schicht ganztägig.
Schichtbeginn	Datum und Uhrzeit des Schichtbeginns.
Schichtende	Datum und Uhrzeit des Schichtendes.
Wiederholen	Wiederholung der Schicht. Die Auswahlmöglichkeiten lauten wie folgt: • Nie • Täglich • Wöchentlich
Jede/n/s	Gibt an, wie häufig die Wiederholung erfolgt. Die Anzeige hängt vom ausgewählten Zeitrahmen ab.
Weitere Optionen	Weitere Optionen zum Anpassen Ihres Zeitplans.
Zeitzone	Zeitzone des Anwenders.
Feiertagskalender	Für Feiertage zu verwendender Zeitplan.
Wiederholen bis	Datum und Uhrzeit für das Ende der Wiederholung.

Schicht mit Schichtvorlage erstellen

Feld	Beschreibung
Schichtname	Name der Schicht.
Template/Schedule (Vorlage/Zeitplan)	Vorhandene Vorlagen für Schichten. Die Auswahlmöglichkeiten lauten wie folgt: • 24 x 7 • Außerhalb Bürozeit (Arbeitstag 8:00 bis 17:00) • Außerhalb Bürozeit (Arbeitstag 9:00 bis 17:00) • Arbeitstag 8:00 bis 17:00 • Arbeitstag 9:00 bis 17:00

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Service hinzufügen“

Erstellen Sie einen Service, oder fügen Sie Ihrer Instanz einen Service hinzu, damit Warnungen und Incidents zu diesem Service für Ihre Teams in SRM verfügbar sind.

Fügen Sie ein Serviceformular hinzu

Weitere Informationen finden Sie unter Services zu SRM hinzufügen.

Services für Ihre Teams hinzufügen

Feld	Beschreibung
Servicename	Geben Sie einen Namen für Ihren Service ein. Beispiel: Cloud-Speicherservice. Ihren Teams wird dieser Name in SRM angezeigt.
Serviceklasse	Wählen Sie entweder Anwendungsservice oder technischen Service aus.
Business-Relevanz	Geben Sie an, wie wichtig der Service für das Unternehmen ist: • 1 – sehr kritisch • 2 – kritisch • 3 – weniger kritisch • 4 – Nicht kritisch
Betriebsstatus	Wählen Sie den Status Ihres Service aus: • Funktionsfähig • Nicht funktionsfähig • Reparatur in Bearbeitung • DR-Standby • Bereit • Stillgelegt • Pipeline • Katalog
Kurzbeschreibung	Beschreiben Sie Ihren Service, damit Ihre Teams seinen Zweck und andere relevante Informationen verstehen können.

Formular „Servicedetails bearbeiten“

Bearbeiten Sie einen vorhandenen Service, für den Ihr Team verantwortlich ist.

Formular „Servicedetails“

Weitere Informationen finden Sie unter SRM-Servicedetails bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Service
Support-Gruppe	SRM-Team, das den Service verwaltet.
Business-Relevanz	Gibt an, wie wichtig dieser Service für das Geschäft ist.
Eigentum von	Serviceverantwortlicher. Darf nicht Teil eines SRM-Teams sein.
Betriebsstatus	Status für die Fähigkeit des Service, operative Funktionen auszuführen.
Entscheidungsträger	Produkteigentümer oder Serviceverbraucher, die die Zielverfügbarkeit eines Service bestimmen.
Umgebung	Die Auswahlmöglichkeiten lauten wie folgt: • Keine • Entwicklung • Produktion • Test
Verwaltet von Gruppe	Teammanager, der für den Service verantwortlich ist. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Gruppe ändern	Team, das für Changes verantwortlich ist. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Status	Status des Service.
Lebenszyklusphase	Die Auswahlmöglichkeiten lauten wie folgt: • Bereitstellen • Design • Ende der Lebensdauer • Ideation • Funktionsfähig
Phase	Phase des Service. Die Auswahlmöglichkeiten lauten wie folgt: • Keine • Pipeline • Katalog • Deaktiviert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standort	Adresse, unter der sich der Service befindet. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Verwendet für	Zweck des Service. Die Auswahlmöglichkeiten lauten wie folgt: • Produktion (Standard) • Staging • QA • Test • Entwicklung • Demonstration • Schulung • Notfallwiederherstellung
Kurzbeschreibung	Zusätzliche Informationen zum Service.
Support by (Support durch)	SRM-Team, das den Service verwaltet. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.

Formular „Eskalationsrichtlinien einrichten“ in SRM

Eskalationsrichtlinien legen die Reihenfolge und die Bedingungen fest, unter denen Mitglieder oder Geräte Benachrichtigungen erhalten.

Formular „Eskalationsrichtlinie“

Feld	Beschreibung
Name	Name der Eskalationsrichtlinie.
Aktiv in Schicht	Team, das die Benachrichtigungen zu seiner Schicht erhält. .
Von Grund auf neu erstellen	Option zum Erstellen einer eigenen Richtlinie.
Aus Vorlage erstellen	Option zum Erstellen einer Richtlinie mithilfe einer Vorlage, die von Ihrem Administrator erstellt wurde.
Beschreibung	Text, der die Richtlinie beschreibt.
Aktiv	Option zum Aktivieren oder Deaktivieren der Richtlinie.
Als Standard verwenden	Option zur Verwendung dieses Teams als Standard
Reihenfolge	Reihenfolge der Ausführung. Dies ist die Hierarchie oder Befehlskette. Wenn mehrere Eskalationsrichtlinien mit denselben Bedingungen für ein Team vorhanden sind, wird zuerst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Eskalationsrichtlinie mit der kleineren Reihenfolgenummer ausgeführt.
Bedingungen	Bedingungen für die Richtlinie. Die Tabelle und die Bedingungen, die die Eskalationsrichtlinie definieren. Diese Bedingungen werden überprüft, nachdem die Eskalation von einem Eskalationsauslöser gestartet wurde. Wenn die Bedingungen erfüllt sind, wird die Richtlinie ausgeführt.
Eskalationsschritte	Hinzuzufügende Eskalationsschritte. Weitere Informationen zu den Feldern finden Sie im Formular „Eskalationsschritte“.
Eskalationsbenachrichtigungen	Benachrichtigungsbedingungen für die Richtlinie. **Hinweis:** Wenn die Überschreibung der Anwendereinstellungen aktiviert ist, überschreibt Ihre Eskalationsrichtlinie alle Richtlinien, die die Rufbereitschaftsmitarbeiter für ihre eigenen Benachrichtigungseinstellungen festgelegt haben. Wenn die Überschreibung der Anwendereinstellungen deaktiviert ist, haben die Benachrichtigungseinstellungen der Rufbereitschaftsmitarbeiter Priorität gegenüber dieser Eskalationsrichtlinie.
Benachrichtigungsschritt hinzufügen	Zusätzliche hinzuzufügende Benachrichtigungsschritte. Sie können E-Mail, Anruf oder SMS auswählen. Sie können beliebig viele Versuche hinzufügen.

Formular „Eskalationsschritte“

Eskalationsschritt hinzufügen

Feld	Beschreibung
Name des Eskalationsschritts	Name des Eskalationsschrittes.
Reihenfolge	Reihenfolge der Ausführung. Dies ist die Hierarchie oder Befehlskette.
Beantworter-Ebene	Ebene der Befugnis oder Kompetenz, die erforderlich ist, um auf den Incident zu reagieren.
Unter Mitgliedern abwechseln	Option, alle Mitglieder nacheinander zu benachrichtigen, bis eines von ihnen den Incident bestätigt oder bis alle benachrichtigt wurden.
Zusätzliche Zielgruppe	Bestimmte Anwender, Teams, Gruppen oder Geräte, die Sie benachrichtigen möchten.
Zeit bis zum nächsten Schritt nach der letzten Benachrichtigung	Die maximale Zeit, die vergeht, bevor das Problem zum nächsten Schritt eskaliert wird. Wenn ein Beantworter das Problem beispielsweise nicht innerhalb von 30 Minuten nach der Benachrichtigung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eskalationsschritt hinzufügen (Fortsetzung)

Feld	Beschreibung
	lösen kann, wird das Problem an den Manager eskaliert.

Domänentrennung und SRM

Service Reliability Management (SRM) unterstützt Domain Separation.

Support-Stufe: Basis*

Die Supportstufe ist „Basis“, weist jedoch einige Ausnahmen oder besondere Bedingungen auf.

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers (SP) übertragen werden.
- Die Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen verwenden die Domäne alle zur Produktionslaufzeit.
- Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend funktioniert.

Beispiel-Anwendungsfall: Wenn ein SP den Chat verwendet, um auf die Nachricht eines Mandanten zu antworten, muss der Client die Antwort des SP sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Übersicht Von Domänentrennung

- Domänentrennung ist in allen Metadatentabellen in der Anwendung vorhanden. Auch Tabellen auf der Ebene der Instanz verfügen explizit über Domänentrennung. Andere interne Tabellen, z. B. die interne Teamanforderungstabelle, sind implizit domänengetrennt, da sie auf domänengetrennte Datensätze verweisen.
- Systemeigenschaften sind hingegen nicht domänengetrennt, was Auswirkungen auf die Funktionen des Teammanagements hat. Die Eigenschaften werden von mehreren Domänen gemeinsam verwendet und auf Instanzebene festgelegt. Ein domänenspezifisches Setup für diese Eigenschaften wird nicht unterstützt.
- Wenn eine andere Anwendung genutzt wird (z. B. Ereignismanagement-Connectors), hängt die Fähigkeit zur Domänentrennung von den Domänentrennungsfunktionen dieser Anwendung ab.

So funktioniert die Domänentrennung in der Service Reliability Management Anwendung

Die spezifischen Bedingungen, die oben durch die Support-Stufe Basic* angegeben werden, beziehen sich auf Teammanagement:

- Neue Teams werden über ein Katalogelement erstellt, das von einem IntegrationHub-Flow unterstützt wird, der vom Service Operations-Arbeitsbereich-Administrator eingerichtet wird. Sie können das über das Serviceportal initiieren. Ein SRM-Administrator, -Manager oder -Beantworter kann das über den SRM-Arbeitsbereich tun. Anweisungen finden Sie in der SRM-Dokumentation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Subflows und Aktionen von IntegrationHub steuern die Verwaltung von SRM-Teams.
- Für jede Instanz kann nur ein Katalogelement und ein Flow eingerichtet werden. Der Kunde ist für die Einrichtung von Teameigenschaften zur Unterstützung der Domänentrennung als Anpassung der vorhandenen Flows verantwortlich.
- Die anfordernde Person eines Teamkatalogelements ist der Domäne zugeordnet und als Teil des Anforderungselements verfügbar. Daher kann die anfordernde Person gegebenenfalls das Team in einer bestimmten Domäne oder im Katalogelement erstellen und erweitern, um die Domäne auf andere Weise zu erfassen. In beiden Fällen muss der Service Operations-Arbeitsbereich Änderungen an den Flows und Aktionen von IntegrationHub vornehmen, um dies zu unterstützen.

Weitere Informationen finden Sie unter Domain Separation und Bereitschaftsplanung .

Zugehörige Informationen

Domänentrennung für Service Provider

Erstellen Sie Change-Anforderungsformulare

Füllen Sie die Felder in den Formularen aus, um eine Change-Aufgabe zu erstellen, um einen kontrollierten Prozess zum Ändern genehmigter und unterstützter Aktionen für zu implementieren SRM.

Change-Anforderungs-Formular

Erstellen Sie eine neue Change-Anforderung. Weitere Informationen finden Sie unter Change-Aufgabe in SRM manuell erstellen.

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung der Change-Anforderung.
Beschreibung	Beschreibung basierend auf der Kurzbeschreibung.
Nummer	Bezeichner der Change-Anforderung.
Kategorie	Kategorie der Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Hardware • Software • Service • Systemsoftware • Anwendungssoftware • Netzwerk • Telekommunikation • Dokumentation • Sonstige (Standard)
Modell	Für die Change-Anforderung zu verwendendes Modell. Standard (Standard)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Risiko	Risiko, das das Problem darstellt. Die Auswahlmöglichkeiten lauten wie folgt: • Hoch • Mittel (Standard) • Niedrig
Typ	Typ der Change-Anforderung. Standard (Standard) Schreibgeschützt.
Auswirkung	Auswirkung des Problems. Die Auswahlmöglichkeiten lauten wie folgt: • 1 - Hoch • 2 - Mittel • 3 - Niedrig (Standard)
Status	Status der Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Neu (Standard) • Bewerten Wenn eine Genehmigung erforderlich ist, sind keine weiteren Status verfügbar. • Geplant • Implementieren • Abgebrochen
Arbeitsnotizenliste	Teammitglieder, die Benachrichtigungen erhalten, wenn Arbeitsnotizen hinzugefügt werden. **Hinweis:** Ein Administrator muss bereits eine E-Mail-Benachrichtigung für die Arbeitsnotizenliste erstellt haben.
Arbeitsnotizen	Zusätzliche Informationen im Zusammenhang mit dieser Anforderung.

Auswirkung, Zuweisung, Planung, Zeitplan, Notizen, und Abschlussinformationen

Feld	Beschreibung
Konfigurationselement	Asset, das von dem Problem betroffen ist.
Service	Service, der von dem Problem betroffen ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Serviceangebot	Serviceangebot, das von dem Problem betroffen ist.
Zuweisungsgruppe	Team, das der Change-Anforderung zugewiesen ist.
Zugewiesen an	Benutzer, dem die Change-Anforderung zugewiesen ist.
Begründung	Begründung für die Change-Anforderung.
Implementierungsplan	Importierter Text.
Risiko- und Auswirkungsanalyse	Analyse der Risiken und Auswirkungen des Problems.
Rückfallplan	Importierter Text.
Testplan	Importierter Text.
Geplantes Startdatum	Erwartetes Datum für den Beginn des Change.
Geplantes Enddatum	Erwartetes Datum für den Abschluss des Change.
Tatsächliches Startdatum	Datum, an dem die Implementierung des Change begonnen hat.
Tatsächliches Enddatum	Datum, an dem die Implementierung des Change beendet wurde.
Konfliktstatus	Nicht ausgeführt. Schreibgeschützt.
Letzte Konfliktanalyse	In Abhängigkeit vom Konfliktstatus. Abgebrochen
Beobachtungsliste	Interessierte Benutzer.
Arbeitsnotizenliste	Teammitglieder, die Benachrichtigungen erhalten, wenn Arbeitsnotizen hinzugefügt werden. **Hinweis:** Ein Administrator muss bereits eine E-Mail-Benachrichtigung für die Arbeitsnotizenliste erstellt haben.
Zusätzliche Kommentare	Zusätzliche Hinweise für die Anforderung.
Arbeitsnotizen	Zusätzliche Hinweise zur Arbeit, die für die Anforderung ausgeführt wird.
Abschlusscode	Code für die Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Keine (Standard) • Erfolgreich • Erfolgreich mit Problemen • Nicht erfolgreich
Abschlussnotizen	Hinweise zum Abschluss der Change-Anforderung.

Status von SRM-Incidents

Incidents können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In SRM wird ein Incident erstellt, wenn das Überwachungstool eines Drittanbieters ein Event registriert. Incidents können manuell erstellt oder zugewiesen werden. Bearbeiten Sie Aktionen aus dem Incident-Formular über die Status-Schaltfläche im Formular. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen Änderungen beizubehalten. Änderungen an den Incidents in der Listenansicht werden automatisch gespeichert.

Incident-Status

Status	Beschreibung
Neu	Status oder Incident-Erstellung. Der Incident wurde protokolliert, aber noch nicht bearbeitet.
In Bearbeitung	Der Incident wird zur Bearbeitung zugewiesen.
Angehalten	Die Verantwortung für den Incident wurde vorübergehend zu einer anderen Entität verschoben, um weitere Informationen, Indizien oder eine Lösung bereitzustellen.
Gelöst	Für den Incident wurde eine zufriedenstellende Lösung bereitgestellt, um sicherzustellen, dass er nicht erneut auftritt.
Geschlossen	Der Incident wird geschlossen, wenn bestätigt wird, dass der Incident zufriedenstellend gelöst wurde.
Abgebrochen	Der Incident wurde überprüft, aber es wurde festgestellt, dass es sich um einen doppelten Incident, einen unnötigen Incident oder überhaupt keinen Incident handelt. So öffnen Sie einen Incident erneut. Wählen Sie **Neu**.

Status von SRM-Warnungen

Warnungen können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

In SRM wird eine Warnung erstellt, wenn das Überwachungstool eines Drittanbieters ein Event registriert. Warnungen werden manuell zugewiesen. Eine Warnung kann einen von vier Status aufweisen. Sie können Aktionen entweder in der Warnungsliste oder im Warnungsformular bearbeiten. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen Änderungen beizubehalten. Änderungen an Warnungen in der Listenansicht werden automatisch gespeichert.

Hinweis: Sie können Warnungen in jedem Status bestätigen und zuweisen.

Warnungsaktionen

Status	Beschreibung
Offen	Status bei Erstellung der Warnung. In diesem Status können Sie bestätigen und festlegen auf: **Fluktuieren** Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Siehe Fluktuierende Warnungen konfigurieren Weitere Informationen zum Fluktuieren von Ereignissen. **Geschlossen** Schließt die Warnung.
Erneut öffnen	In diesem Status können Sie bestätigen und festlegen auf:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsaktionen (Fortsetzung)

Status	Beschreibung
	Öffnen Legt die Warnung auf den Status **Offen** fest. **Flatternd** Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. **Geschlossen** Schließt die Warnung.
Flatternd	Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Über diesen Status können Sie Folgendes festlegen: **Offen** Legt die Warnung auf den Status **Offen** fest. **Erneut öffnen** Öffnet die Warnung erneut. **Geschlossen** Schließt die Warnung.
Geschlossen	Über diesen Status können Sie Folgendes festlegen: **Offen** Legt die Warnung auf den Status **Offen** fest. **Erneut öffnen** Öffnet die Warnung erneut. **Flatternd** Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden.

Status von SRM-Change-Anforderungen

Incidents können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

Change-Anforderungen können in SRM manuell erstellt werden. Bearbeiten Sie Aktionen im Formular für Change-Anforderungen über das Statusfeld im Formular oder die Schaltflächen im Datensatz für die Change-Anforderung. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen Änderungen beizubehalten. Änderungen an Change-Anforderungen in der Listenansicht werden automatisch gespeichert.

Change-Anforderung – Status

Status	Beschreibung
Neu	Status bei Erstellung der Change-Anforderung. Die Anforderung wurde protokolliert, aber noch nicht bearbeitet.
Bewerten	Die Genehmigung der Change-Anforderung wird bearbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change-Anforderung – Status (Fortsetzung)

Status	Beschreibung
Geplant	Eine Change-Anforderung zur Bearbeitung geplant.
Implementieren	Die Change-Anforderung wird umgesetzt.
Überprüfen	Die Change-Anforderung wechselt in den Status **Überprüfen**. **Hinweis:** Alle offenen Change-Aufgaben werden auf **Abgebrochen** gesetzt.
Geschlossen	Die Change-Anforderung wird geschlossen.
Abgebrochen	Die Change-Anforderung wurde selektiert, aber es wurde festgestellt, dass es sich um ein Duplikat handelt oder sie unnötig ist. **Hinweis:** Sie können eine abgebrochene Change-Anforderung nicht erneut öffnen.

CMDB-Serviceklassen

Service Reliability Management Unterstützt normalerweise mehrere CMDB-Serviceklassen (Configuration Management Database).

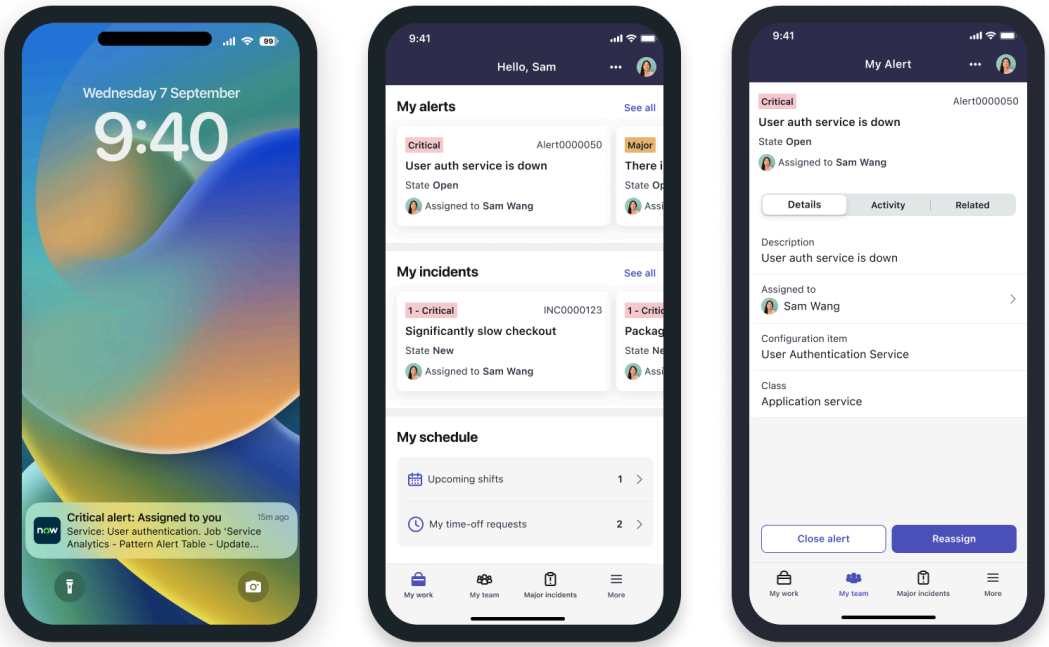
Typen von CMDB-Serviceklassen, die Service Reliability Management Support:

- Serviceinstanzen (cmdb_ci_Service_Auto)
- Technische Services (cmdb_ci_Service_Technical)
- Abfragebasierte Services (cmdb_ci_query_based_Service)
- Zugeordnete Anwendungsservices (cmdb_ci_Service_detected)
- Berechnete Anwendungsservices (cmdb_ci_calculated)
- Tag-basierte Anwendungsservices (cmdb_ci_Service_by_Tags)

ITOM Mobile Agent

Bleiben Sie mit in Verbindung, und sorgen Sie dafür, dass Services zuverlässig sind ITOM Mobile Agent, Mit dem Sie auf zugreifen können Service Reliability Management(SRM) Funktionen in iOS Und Android Geräte. Verwenden Sie es, um Warnungen nachzuverfolgen, Incidents zu verwalten, Change- und Katalogaufgaben zu bearbeiten und Rufbereitschaftsschichten unterwegs zu verwalten.

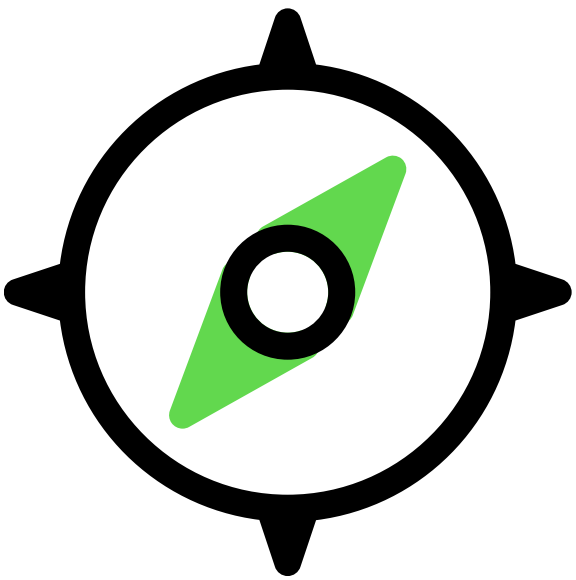
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erste Schritte

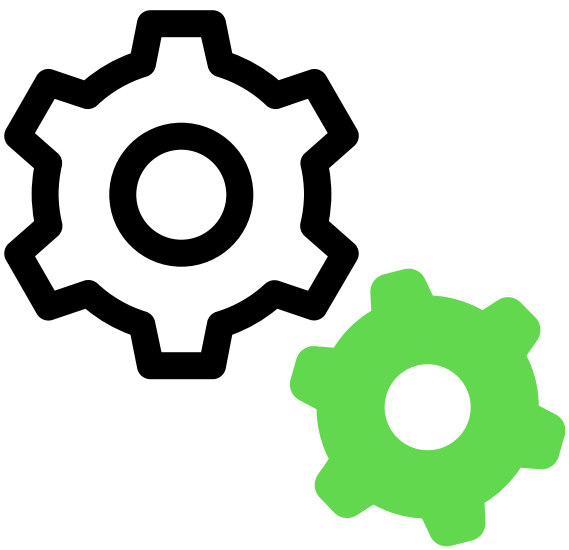
Automatische Übersetzung

Untersuchen



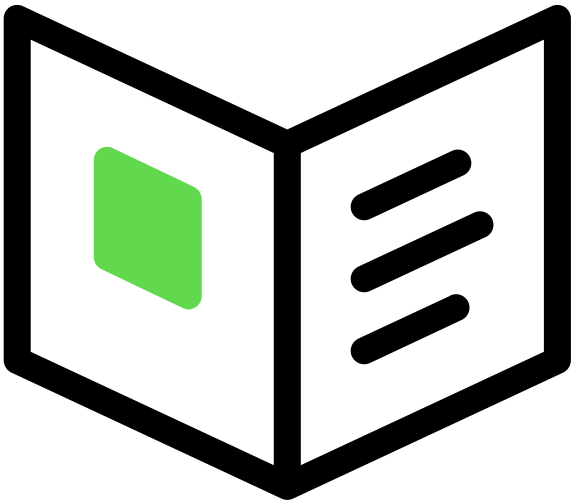
Erfahren Sie mehr über ITOM Mobile Agent, Einschließlich seiner Vorteile und allgemeinen Workflows.

Konfigurieren



Installieren ITOM Mobile Agent Und konfigurieren Sie Benachrichtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
	
Melden Sie sich an, und arbeiten Sie mit Warnungen, Incidents, Aufgaben und Rufbereitschaftszeitplänen.	Rufen Sie Details zu ab ITOM Mobile Agent Einstellungen.

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

ServiceNow Store

ServiceNow Store

Support

- https://support.servicenow.com/now
- Known Error-Portal

ITOM Mobile Agent erkunden

Erfahren Sie, wie Sie verwenden können ITOM Mobile Agent Zur Verwaltung der Servicezuverlässigkeit unterwegs, einschließlich der Fähigkeiten, Vorteile und eines Beispiel-Workflows.

ITOM Mobile Agent – Übersicht

Verwenden ITOM Mobile Agent Um auf zuzugreifen Service Reliability Management(SRM) Funktionen in iOS Und Android Geräte. Mit ITOM Mobile Agent, Sie können Warnungen nachverfolgen, Incidents verwalten und von unterwegs an Change- und Katalogaufgaben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

arbeiten. Sie können Rufbereitschaftszeitpläne auch verwalten, indem Sie Schichten überprüfen, Auszeiten beantragen und Planungslücken schließen.

Damit Sie die Servicezuverlässigkeit an einem Ort verwalten können, ITOM Mobile Agent Wird automatisch in vorhandene integriert ServiceNow Mobile Apps. Wird in ausgeführt ServiceNow Agent App und schließt automatisch ein ITSM Mobile Agent Funktionen. Mit diesem Setup können Sie Warnungen, Incidents, Rufbereitschaftszeitpläne und Aufgaben in einer mobilen App verwalten.

Hinweis: Wenn Sie bereits verwenden ITSM Mobile Agent Installieren Sie für Incidents, Rufbereitschaftszeitpläne und Aufgaben ITOM Mobile Agent Um Ihrer Mobile Experience Warnungen hinzuzufügen. Mit ITOM Mobile Agent, Sie erhalten und konfigurieren Warnungsbenachrichtigungen und zeigen Warnungen auf den Registerkarten „meine Arbeit“, „mein Team“ und „Benachrichtigungen“ an. Siehe ITOM Mobile Agent installieren Für Installationsanweisungen.

ITOM Mobile Agent Anwender

In der folgenden Tabelle werden Anwenderrollen und die Funktionen der einzelnen Anwender in aufgelistet ITOM Mobile Agent:

Anwender	Beschreibung
Administrator	Administratoren installieren ITOM Mobile Agent Damit Teams unterwegs auf Funktionen zur Servicezuverlässigkeit zugreifen können.
SRM-Administrator	SRM Administratoren passen Warnungs- und Incident-Benachrichtigungen für an ITOM Mobile Agent. Sie stellen sicher, dass die relevanten Personen sich kritischer Probleme bewusst sind.
SRM-Manager	SRM Manager verfolgen den Fortschritt des Teams, überwachen nicht zugewiesene Probleme und überprüfen Leistungsmetriken. Sie bearbeiten auch Rufbereitschaftszeitpläne, einschließlich Schichtumplanung, Auszeitanträge und Planungslücken.
SRM Beantworter	SRM Beantworter verwalten Warnungen, Incidents und Aufgaben unterwegs. Sie akzeptieren, weisen Warnungen zu und schließen sie, erstellen Incidents und arbeiten bei ihnen zusammen und verarbeiten kritische Probleme. Sie können auch bevorstehende Schichten anzeigen und Auszeiten beantragen.

ITOM Mobile Agent – Workflow

Dieser Beispiel-Workflow zeigt, wie ITOM Mobile Agent Hilft Ihnen, Services und die ihnen zugewiesenen Teams zu verwalten:

1. Überwachungstools generieren kritische Warnungen, wenn sie Probleme erkennen, und ITOM Mobile Agent Das System sendet mobile Warnungsbenachrichtigungen an Rufbereitschaftsantworter.
2. Als Rufbereitschaft SRM Beantworter: Sie bestätigen die Warnungen, weisen sie neu zu oder schließen sie. Bei Bedarf erstellen Sie Incidents aus den Warnungen und dann aus ITOM Mobile Agent Das System weist sie dem entsprechenden Team zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Sie beheben Incidents und arbeiten an Incidents zusammen, eskalieren sie bei Bedarf zu schwerwiegenden Incidents, lösen und schließen die Incidents dann und geben bei Bedarf relevante Details an.
4. Als SRM manager, passen Sie Schichten an, genehmigen Auszeitanträge und schließen Planungslücken für die Bereitschaftsantworter. Verwenden Sie Dashboards, um Warnungstrends, Zeiten der Incident-Lösung und Teamleistung anzuzeigen.

ITOM Mobile Agent – Vorteile

Arbeiten mit ITOM Mobile Agent Hat die folgenden Vorteile:

Verbessern Sie die Servicezuverlässigkeit

Minimieren Sie Ausfallzeiten, indem Sie Warnungen und Incidents unterwegs verwalten.

Reagieren Sie schneller auf Probleme

Sorgen Sie dafür, dass Bereitschaftstechniker in Verbindung bleiben, damit sie Warnungen von überall annehmen, zuweisen und schließen können.

Benachrichtigen Sie die richtigen Personen

Passen Sie Push-Benachrichtigungen an, um sicherzustellen, dass die relevanten Personen über kritische Probleme informiert sind.

Verbessern Sie die Zusammenarbeit

Helfen Sie Teams, effizient zu arbeiten, indem Sie Rufbereitschaftszeitpläne verwalten und Abdeckungslücken auf Mobilgeräten schließen.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von ITOM Mobile Agent finden Sie unter:

- ITOM Mobile Agent konfigurieren
- ITOM Mobile Agent verwenden
- ITOM Mobile Agent – Referenz

ITOM Mobile Agent konfigurieren

Konfigurieren Sie ITOM Mobile Agent.

Konfiguration – Übersicht

Verwenden Sie die Seiten in diesem Abschnitt zum Einrichten und Konfigurieren ITOM Mobile Agent. Die Informationen umfassen erforderliche und optionale Setup-Schritte, einschließlich der Installation der App, der Verwaltung von Warnungen und der Anpassung von Warnungsempfängern.

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Damit Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Falls relevant, ist dieser Abschnitt mit verknüpft ITSM Mobile Agent Inhalt, der zusätzliche Konfigurationsoptionen für Ihre mobile Experience bereitstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Konfigurationsschritte

Wenn Sie Administrator sind, beginnen Sie mit der Installation ITOM Mobile Agent. Wenn Sie ein sind Service Reliability Management administrator, Manager oder Beantworter können Sie mit dem Herunterladen von beginnen ServiceNow Agent App und dann Anmeldung.

- ITOM Mobile Agent installieren
- Laden Sie herunter ServiceNow Agent App
- Anmeldung bei ITOM Mobile Agent

Optionale Konfigurationsschritte

Nachdem Sie sich bei angemeldet haben ITOM Mobile Agent, Können Sie mit den Kernfunktionen arbeiten. Besuchen Sie die folgenden Links, um zu konfigurieren und anzupassen ITOM Mobile Agent Weitere Informationen zur Erfüllung der Anforderungen Ihres Teams:

- Konfigurieren Sie, wann Warnungsbenachrichtigungen für ITOM Mobile gesendet werden sollen
- Anpassen ITOM Mobile Agent E-Mail-Empfänger
- Anpassen anderer mobiler Einstellungen für ITOM Mobile Agent

ITOM Mobile Agent installieren

Installieren Sie, und gewähren Sie Ihren Teams Zugriff auf ITOM Mobile Agent.

Vorbereitungen

Service Reliability Management(SRM) Services, Serviceintegrationen, Teams und Rufbereitschaftszeitpläne müssen eingerichtet werden. ITOM Mobile Agent Stellt eine Verbindung zu Ihrem vorhandenen her SRM Richten Sie ein, um Ihren Teams bei der Verwaltung von Warnungen, Incidents, Aufgaben und Rufbereitschaftszeitplänen zu helfen.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

ITOM Mobile Agent Wird in ausgeführt ServiceNow Agent App. Wenn Sie installieren ITOM Mobile Agent, Ihre Teams können in darauf zugreifen ServiceNow Agent App auf ihren Geräten.

Dieses Verfahren richtet sich an Administratoren, die den mobilen Zugriff für ihre Teams verwalten. Wenn Sie kein Administrator sind und verwenden möchten ITOM Mobile Agent Auf Ihrem Mobilgerät finden Sie unter Laden Sie herunter ServiceNow Agent App.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen und wählen Sie aus ITOM Mobile Agent.
   Wenn Sie nicht finden können ITOM Mobile Agent, Fordern Sie es über an ServiceNow Store.
3. Überprüfen Sie die aufgeführten Abhängigkeiten, und installieren Sie bei Bedarf die erforderlichen Plugins und Anwendungen.
4. Wählen Sie **Installieren** aus.

   Nach der Installation der Anwendung können Ihre Teams auf zugreifen ITOM Mobile Agent Indem Sie herunterladen ServiceNow Agent App und Anmeldung bei der relevanten Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Um mit zu beginnen ITOM Mobile Agent, Siehe Laden Sie herunter ServiceNow Agent App Und Anmeldung bei ITOM Mobile Agent.

Sie können auch anpassen ITOM Mobile Agent So erfüllen Sie die Anforderungen Ihres Teams:

- Konfigurieren Sie, wann Warnungsbenachrichtigungen für ITOM Mobile gesendet werden sollen
- Anpassen ITOM Mobile Agent E-Mail-Empfänger
- Anpassen anderer mobiler Einstellungen für ITOM Mobile Agent

Laden Sie herunter ServiceNow Agent App

Laden Sie herunter ServiceNow Agent Zu verwendende App ITOM Mobile Agent Auf Ihrem Gerät.

Vorbereitungen

ITOM Mobile Agent muss installiert sein. Weitere Informationen finden Sie unter ITOM Mobile Agent installieren.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

Warum und wann dieser Vorgang ausgeführt wird

Die ITOM Mobile Agent Die Anwendung wird in ausgeführt ServiceNow Agent App. Um auf zuzugreifen ITOM Mobile Agent, Laden Sie herunter ServiceNow Agent App auf Ihrem Gerät.

Prozedur

1. Laden Sie herunter ServiceNow Agent App für Ihr Gerät:
   - Für iOS, Verwenden Sie den App Store.
   - Für Android, Verwenden Sie Google Wiedergabe.
2. Bestätigen Sie, dass sich die App auf Ihrem Gerät befindet.

   Suchen Sie nach ServiceNow Agent App-Symbol ( ). Die App wird auf Ihrem Gerät mit dem Namen Agent angezeigt.

Nächste Maßnahme

Um mit zu beginnen ITOM Mobile Agent, Siehe Anmeldung bei ITOM Mobile Agent. Sie müssen sich anmelden, um Push-Benachrichtigungen zu Warnungen und Incidents zu erhalten.

Anmeldung bei ITOM Mobile Agent

Melden Sie sich bei an ITOM Mobile Agent-Instanz auf der ServiceNow Agent App zum Verwalten von Warnungen, Incidents und Rufbereitschaftszeitplänen unterwegs.

Vorbereitungen

ITOM Mobile Agent Muss installiert sein, und ServiceNow Agent App muss auf Ihr Gerät heruntergeladen werden. Siehe ITOM Mobile Agent installieren und Laden Sie herunter ServiceNow Agent App, um weitere Informationen zu erhalten.

Sie müssen beispielsweise auch Ihre Instanzadresse haben nebula-dev.service-now.com , Oder ein QR-Code für die Instanz. Wenn Sie keinen haben, wenden Sie sich an Ihren Administrator.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Tippen Sie auf ServiceNow Agent Symbol ( ) Auf Ihrem Gerät.
2. Geben Sie die Adresse Ihrer Instanz manuell oder mit einem QR-Code ein.

Option	Bezeichnung
Manuelle Eingabe	Ersetzen example.service-now.com Mit der Adresse Ihrer Instanz. Sie müssen nicht einschließen service-now.com . Geben Sie beispielsweise ein Nebel-dev Für nebula-dev.service-now.com .
QR-Code	Tippen Sie auf das QR-Code-Symbol, und scannen Sie den QR-Code.

3. **Wahlweise:** In **Kurzname** Geben Sie einen alternativen Namen für Ihre Instanz ein.
   Alternative Namen können Ihnen helfen, schnell zwischen verschiedenen Instanzen auf Ihrem Gerät zu navigieren.
4. Tippen Sie Auf **Speichern Sie, und melden Sie sich an** Geben Sie Ihre Anmeldeinformationen ein, und tippen Sie dann auf **Melden Sie sich an** .
   Die App wird angezeigt Als <username> bei <instance-name> angemeldet Und ITOM Mobile Agent **Meine Arbeit** Registerkarte.

   Hinweis: Sie müssen angemeldet sein, um Push-Benachrichtigungen zu Warnungen und Incidents zu erhalten. Wenn nicht, erhalten Sie nur E-Mail-Benachrichtigungen.

Nächste Maßnahme
Besuchen Sie diese Links, um mit zu beginnen ITOM Mobile Agent:

- Arbeiten Sie mit Warnungen in ITOM Mobile
- Verwalten von Incidents und schwerwiegenden Incidents auf Mobilgeräten
- Arbeiten mit Bereitschaftsplanung Auf Mobilgeräten
- Arbeiten mit Aufgaben auf Mobilgeräten

Konfigurieren Sie, wann Warnungsbenachrichtigungen für ITOM Mobile gesendet werden sollen

Halten Sie Ihre Teams auf dem Laufenden, indem Sie konfigurieren, wann ITOM Mobile Agent Sendet eine Benachrichtigung über eine Warnung.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig ITOM Mobile Agent Sendet eine Push-Benachrichtigung und E-Mail, wenn eine Warnung diese Bedingungen erfüllt:

- **„Zugewiesen an“ ist leer** - Die Warnung ist niemandem zugewiesen.
- **Status ist nicht „Geschlossen“** – Der Warnungsstatus ist nicht „Geschlossen“. Es ist entweder leer, fluktuierend, offen oder erneut geöffnet.
- **Schweregrad ist „Kritisch“** – Der Warnungsschweregrad ist „Kritisch“. Es ist nicht klar, leer, OK, schwerwiegend, gering, oder Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Bedingungen nach Bedarf aktualisieren. Zum Beispiel die ITOM Mobile Agent Die App kann Benachrichtigungen für kritische und schwerwiegende Warnungen senden. Wenn Sie jedoch die Bedingungen anpassen, Die Bedingungen erhalten keine zukünftigen Release-Updates. Dieses Verhalten ist beabsichtigt, das Überschreiben Ihrer Arbeit zu vermeiden.

Hinweis: Um Push-Benachrichtigungen zu erhalten, müssen Sie sich bei anmelden ITOM Mobile Agent. Wenn Sie sich abmelden, erhalten Sie nur E-Mail-Benachrichtigungen.

Dieses Verfahren richtet sich an Administratoren, die Push-Benachrichtigungen und E-Mails für Warnungen konfigurieren. Informationen zum Verwalten anderer Benachrichtigungsfunktionen finden Sie unter Anpassen anderer mobiler Einstellungen für ITOM Mobile Agent.

Prozedur

1. Navigieren zu **Alle** > *Mobile App Builder*an.
2. Suchen und wählen Sie aus **ITOM Mobile Agent** .
3. Wählen Sie Aus **Mobile Benachrichtigungen** .
4. In **Zeitpunkt des Sendens** Abschnitt, aktualisieren oder fügen Sie die Bedingungen „Zugewiesen an“, „Status“ und „Schweregrad“ hinzu.
   Beispiel: Fügen Sie die Bedingung hinzu **ODER [Schweregrad][ist][schwerwiegend]** Unter der Bedingung **[Schweregrad][ist][Kritisch]** Sendet eine Push-Benachrichtigung und E-Mail, wenn der **Schweregrad** Das Feld einer Warnung ist kritisch oder schwerwiegend.

5. Implementieren Sie Ihre Änderungen, indem Sie auswählen **Speichern** .
   Die Seite wird angezeigt Ihre Änderungen wurden gespeichert .

Nächste Maßnahme

Informationen zum Anpassen der Empfänger von E-Mails zu Warnungen finden Sie unter Anpassen ITOM Mobile Agent E-Mail-Empfänger. Sie können auch andere Benachrichtigungsfunktionen anpassen, z. B. anwenderdefinierte Benachrichtigungstöne festlegen und die Einstellung nicht stören für kritische Probleme überschreiben. Weitere Informationen finden Sie unter Anpassen anderer mobiler Einstellungen für ITOM Mobile Agent.

Anpassen ITOM Mobile Agent E-Mail-Empfänger

Passen Sie an, wer E-Mails zu Warnungen erhält, um die Überlastung von Benachrichtigungen zu reduzieren und Verantwortlichkeiten effizient zu delegieren.

Vorbereitungen

Erforderliche Rolle: srm_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ITOM Mobile Agent Sendet E-Mails zu Warnungen an alle in der Gruppen-E-Mail eines Teams. Sie können die E-Mail-Empfänger wie folgt anpassen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schließen Sie Manager von Warnungs-E-Mails aus, um die Überlastung von Benachrichtigungen zu reduzieren.
- Beziehen Sie einzelne Teammitglieder in Warnungs-E-Mails ein, um sicherzustellen, dass die richtigen Personen auf dem Laufenden bleiben.

Prozedur

1. Navigieren zu **Alle** > **Service Reliability Management** > **Teams**an.
2. Suchen Sie in der Liste das Team, das Sie anpassen möchten.
3. Wählen Sie eine oder mehrere Optionen aus, um bestimmte Empfänger von E-Mail-Warnungen einzubeziehen oder auszuschließen.

Option	Anweisung
Manager aus Warnungs-E-Mails ausschließen	In **Manager ausschließen** Spalte, festgelegt **Falsch** Bis **Wahr** .
Beziehen Sie einzelne Teammitglieder in Warnungs-E-Mails ein	In **Mitglieder einbeziehen** Spalte, festgelegt **Falsch** Bis **Wahr** .

4. Speichern Sie Ihre Änderungen, indem Sie das Häkchen aktivieren.
   Ihre Updates werden in angezeigt **Teams** Liste, und ITOM Mobile Agent Sendet E-Mails entsprechend.

Anpassen anderer mobiler Einstellungen für ITOM Mobile Agent

Erfahren Sie, wie Sie Ihre mobile Experience weiter anpassen können. Konfigurieren Sie umsetzbare Benachrichtigungen, legen Sie anwenderdefinierte Benachrichtigungstöne fest, und überschreiben Sie die Einstellung nicht stören für kritische Probleme, damit Ihre Teams auf dem Laufenden bleiben.

Erkunden Sie andere Einstellungen

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Mit dem Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Besuchen Sie Folgendes ITSM Mobile Agent Dokumentation, um mehr über die Anpassung mobiler Benachrichtigungen zu erfahren.

- Konfigurierbare umsetzbare Benachrichtigungen für ITSM Mobile Agent
- Push-Benachrichtigungskategorien für ITSM Mobile Agent aktivieren
- ITSM Mobile E-Mail-Benachrichtigungsumleitung über das Web
- Legen Sie anwenderdefinierte Warntöne in fest ITSM Mobile Agent Für andere Incident-Priorität
- Nicht-stören-Modus außer Kraft setzen, um kritische Warnungen zu erhalten

ITOM Mobile Agent verwenden

Arbeiten Sie unterwegs mit Warnungen, Incidents, Rufbereitschaftszeitplänen und Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Mobile Agent-Aufgaben

Arbeiten Sie mit Warnungen in ITOM Mobile

Verwalten Sie Warnungen unterwegs. Erfahren Sie, wie Sie Warnungen in zuweisen, neu zuweisen und schließen ITOM Mobile Agent. Sie können auch Arbeitsnotizen zu Warnungen hinzufügen und Incidents aus Warnungen erstellen.

Fügen Sie einer Warnung Arbeitsnotizen hinzu

Fügen Sie einer Warnung Arbeitsnotizen hinzu, um Ihr Team zu aktualisieren, wichtige Informationen freizugeben und Ihre Aktionen zu dokumentieren.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

1. Tippen Sie auf Ihrem Gerät auf ServiceNow Agent Symbol ( ).
2. Tippen Sie auf **Benachrichtigungen** Registerkarte und wählen Sie die entsprechende Warnung aus.
3. Tippen Sie auf das Symbol „weitere Optionen“ ( ).
4. Wählen Sie Aus **Fügen Sie Arbeitsnotizen hinzu** Und geben Sie Ihre Notizen ein.
5. Speichern Sie, und fügen Sie der Warnung Ihre Notizen hinzu, indem Sie auf tippen **Übermitteln** .

ITOM Mobile Agent Wird angezeigt Erfolg! Kommentare hinzugefügt . Das zugewiesene Teammitglied erhält auch eine Push-Benachrichtigung, dass der Warnung Kommentare hinzugefügt wurden.

Um die Arbeitsnotizen einer Warnung auf Mobilgeräten anzuzeigen, navigieren Sie zur Warnung, und wählen Sie aus **Aktivität** Registerkarte.

Weisen Sie eine Warnung zu

Weisen Sie eine Warnung zu, um sicherzustellen, dass das richtige Teammitglied darauf reagiert. Sie können sich selbst eine Warnung zuweisen.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

1. Tippen Sie auf Ihrem Gerät auf ServiceNow Agent Symbol ( ).
2. Tippen Sie auf **Benachrichtigungen** Registerkarte und wählen Sie die entsprechende Warnung aus.
3. Tippen Sie auf das Symbol „weitere Optionen“ ( ) Und wählen Sie aus **Warnung zuweisen** .
4. Tippen Sie Auf **Zugewiesen an** Und wählen Sie ein Teammitglied aus, dem die Warnung zugewiesen werden soll.
5. Implementieren Sie Ihre Änderungen, indem Sie auf tippen **Übermitteln** .

Das zugewiesene Teammitglied erhält eine Push-Benachrichtigung, dass ihm die Warnung zugewiesen wurde. Die Warnung wird auch in angezeigt **Meine Arbeit** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen schließen

Schließen Sie eine Warnung, um anzuzeigen, dass das Problem gelöst wurde oder dass keine weitere Aktion erforderlich ist.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

1. Tippen Sie auf Ihrem Gerät auf ServiceNow Agent Symbol ( ).
2. Tippen Sie auf **Benachrichtigungen** Registerkarte und wählen Sie die entsprechende Warnung aus.
3. Tippen Sie auf **Weitere Optionen** Symbol ( ) Und wählen Sie aus **Warnung schließen** .

ITOM Mobile Agent Zeigt Warnung erfolgreich geschlossen an. Die Warnung wird nicht mehr in den zugewiesenen Teammitgliedern angezeigt **Meine Arbeit** Registerkarte.

Um geschlossene Warnungen anzuzeigen, die Ihnen zugewiesen wurden, tippen Sie auf **Meine Arbeit** Und tippen Sie dann auf **Alle anzeigen** Im Abschnitt meine Warnungen. Die **Geschlossen** Auf der Registerkarte werden Ihre geschlossenen Warnungen angezeigt.

Erstellen Sie einen Incident aus einer Warnung

Erstellen Sie einen Incident, wenn eine Warnung auf ein kritisches Problem hinweist, das Ihr System stört oder stören könnte.

Wenn Sie einen Incident aus einer Warnung erstellen, ITOM Mobile Agent Weist den Incident demselben Team zu, aber nicht demselben Beantworter. Wenn die Warnung beispielsweise dem Netzwerk-Ops-Team und dem Beantworter Alex zugewiesen ist, wird der Incident dem Netzwerk-Ops-Team zugewiesen.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

1. Tippen Sie auf Ihrem Gerät auf ServiceNow Agent Symbol ( ).
2. Tippen Sie auf **Benachrichtigungen** Registerkarte und wählen Sie die entsprechende Warnung aus.
3. Tippen Sie auf **Weitere Optionen** Symbol ( ) Und wählen Sie aus **Incident erstellen** .

ITOM Mobile Agent Zeigt eine Benachrichtigung ähnlich wie an INC0013579 wurde aus Alert0002468 erstellt . Sie können den Incident in anzeigen **Mein Team** Registerkarte. Weitere Informationen zum Verwalten von Incidents in finden Sie ITOM Mobile Agent, Siehe Verwalten von Incidents und schwerwiegenden Incidents auf Mobilgeräten.

Hinweis: Wenn Sie die Option zum Erstellen eines Incident aus einer Warnung nicht sehen, stellen Sie sicher, dass die Warnung einem Team zugewiesen ist. Informationen zum Zuweisen der Warnung an ein Team finden Sie unter Weisen Sie Warnungen in zu Express-Liste. In Express-Liste, Teams werden auch als Zuweisungsgruppen bezeichnet.

Weisen Sie eine Warnung neu zu

Weisen Sie eine Warnung neu zu, um sicherzustellen, dass das richtige Teammitglied oder ein verfügbares Teammitglied darauf reagiert. Sie können sich selbst eine Warnung neu zuweisen.

Erforderliche Rolle: srm_Manager, srm_Responder oder srm_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

1. Tippen Sie auf Ihrem Gerät auf ServiceNow Agent Symbol ( ).
2. Tippen Sie auf **Benachrichtigungen** Registerkarte und wählen Sie die entsprechende Warnung aus.
3. Tippen Sie auf **Weitere Optionen** Symbol ( ) Und wählen Sie aus **Warnung neu zuweisen** .
4. Tippen Sie Auf **Zugewiesen an** Und wählen Sie ein Teammitglied aus, dem die Warnung neu zugewiesen werden soll.
5. Implementieren Sie Ihre Änderungen, indem Sie auf tippen **Übermitteln** .

ITOM Mobile Agent Zeigt Warnung erfolgreich neu zugewiesen an. Das zugewiesene Teammitglied erhält eine Push-Benachrichtigung, und die Warnung wird in seinem angezeigt **Meine Arbeit** Registerkarte.

Verwalten von Incidents und schwerwiegenden Incidents auf Mobilgeräten

Verwalten und lösen Sie Incidents unterwegs mit ITOM Mobile Agent. Erfahren Sie, wie Sie Incidents auf Ihrem Mobilgerät erstellen, verarbeiten und daran zusammenarbeiten. Sie können auch schwerwiegende Incidents nachverfolgen und bei ihnen zusammenarbeiten.

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Mit dem Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Weitere Informationen finden Sie im Folgenden ITSM Mobile Agent Dokumentation, um mehr über die Verwaltung von Incidents auf Ihrem Mobilgerät zu erfahren.

Verwalten Sie einen Incident

- Zusammenarbeit mit Incidents
- Zusammenarbeit mit Incident-Aufgaben
- Incident über die Zielseite der App erstellen
- Aufgabenzusammenfassung für Incident-Datensätze wird generiert
- Dashboard „Mein Team“
- Leistungsmetriken
- Incidents mit Verstößen verarbeiten
- Gefährdete Incidents bearbeiten
- Nicht zugewiesene Incidents

Schwerwiegende Incidents verwalten

- Aktive schwerwiegende Incidents
- Zusammenarbeit mit schwerwiegenden Incidents
- Dashboard „Schwerwiegender Incident“
- Kandidaten für schwerwiegende Incidents überprüfen und bearbeiten

Arbeiten mit Bereitschaftsplanung Auf Mobilgeräten

Verwalten Sie Rufbereitschaftszeitpläne unterwegs mit ITOM Mobile Agent. Erfahren Sie als Manager, wie Sie Schichten, Urlaubsanträge und Zeitplanlücken verwalten. Erfahren Sie als Beantworter, wie Sie Auszeiten beantragen, anzeigen, wer Rufbereitschaft hat und anstehende Schichten sehen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Mit dem Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Weitere Informationen finden Sie im Folgenden ITSM Mobile Agent Dokumentation, um mehr über die Verwaltung von Rufbereitschaftszeitplänen auf Ihrem Mobilgerät zu erfahren.

Bereitschaftsplanung Für Manager

- Lücken und Konflikte verwalten mit Bereitschaftsplanung
- Urlaubsanträge mit Bereitschaftsplanung verwalten
- Anstehende Schichten mit Bereitschaftsplanung verwalten

Bereitschaftsplanung Für Beantworter

- Urlaub beantragen mit Bereitschaftsplanung
- Mitglieder der Rufbereitschaftsgruppe anzeigen
- Mit Bereitschaftsplanung anstehende Schichten anzeigen

Arbeiten mit Aufgaben auf Mobilgeräten

Verwalten Sie Change- und Katalogaufgaben auf Ihrem Mobilgerät mit ITOM Mobile Agent. Erfahren Sie, wie Sie schnell auf Probleme reagieren können, indem Sie Aufgaben unterwegs Kommentare anzeigen, schließen und hinzufügen.

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Mit dem Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Weitere Informationen finden Sie im Folgenden ITSM Mobile Agent Dokumentation, um mehr über die Verwaltung von Aufgaben auf Ihrem Mobilgerät zu erfahren.

Verwalten Sie Change-Aufgaben

- Change-Aufgaben
- Überfällige Changes

Verwalten Sie Katalogaufgaben

Katalogaufgaben anzeigen

ITOM Mobile Agent – Referenz

Erfahren Sie mehr über ITOM Mobile Agent Einstellungen. Sie können die App-Version anzeigen, Feedback geben und Ihre Einstellungen anpassen.

Erkunden Sie die Referenzdokumentation

ITOM Mobile Agent Wird automatisch in integriert ITSM Mobile Agent, Mit dem Sie Warnungen, Incidents und Rufbereitschaftszeitpläne über dieselbe mobile App verwalten können. Besuchen Sie Folgendes ITSM Mobile Agent Dokumentation, um mehr über die Einstellungen Ihrer mobilen App zu erfahren.

Einstellungen

Servicelevel-Zielmanagement

Servicelevel-Zielmanagement(SLO-Management) Hilft Ihrer Organisation, vereinbarte Servicequalitätsstandards zu definieren, nachzuverfolgen und zu erfüllen. Es arbeitet in Verbindung mit Service Level Agreements (SLAs) zusammen, um sicherzustellen, dass die Servicebereitstellung die Kundenerwartungen erfüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die Vorgehensweise SLO-Management Funktioniert

- SLAs legen die Erwartungen fest

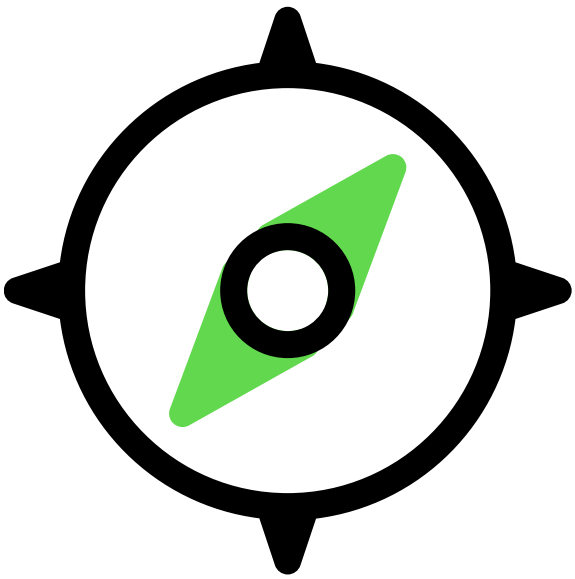
  SLAs sind formelle Vereinbarungen, die das Servicelevel beschreiben, das ein Kunde erwarten kann. Dies kann Dinge wie Antwortzeiten, Lösungszeiten und Betriebszeitziele umfassen.

- SLOs definiert, wie die Erwartungen erfüllt werden können

  SLOs sind spezifische, messbare Ziele, die eine Organisation zum Erreichen der SLAs festlegt. Sie übersetzen die allgemeinen Ziele des SLA in umsetzbare Metriken.

- ServiceNow SLO-Management Hilft bei der Verwaltung von SLOs. Es bietet Funktionen für:
  - Definieren Sie SLOs basierend auf verschiedenen Metriken.
  - Überwachen Sie die SLO-Leistung in Echtzeit.
  - Generieren Sie Warnungen, wenn SLOs gefährdet sind, verletzt zu werden.
  - Verfolgen Sie Verlaufsdaten, um Trends zu identifizieren und Prozesse zu verbessern.

Erste Schritte

Untersuchen	Verwenden
	
Erfahren Sie mehr über Servicelevel-Zielmanagement Konzepte und Funktionen.	Servicelevel-Zielmanagement verwenden

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLO-Management erkunden

Servicelevel-Zielmanagement(SLO-Management) Ist ein entscheidender Aspekt des IT Service Management, der sicherstellt, dass IT-Services die Kundenerwartungen erfüllen.

SLO-Management – Übersicht

SLO-Management Ist ein Framework zum Festlegen klarer Erwartungen und Messen der Leistung von IT-Services. Es hilft Organisationen, eine konsistente Servicebereitstellung sicherzustellen und Bereiche mit Verbesserungspotenzial zu identifizieren. SLOs definieren das Ziel-Servicelevel für einen bestimmten Service, z. B. Incident-Lösung oder Erfüllung von Serviceanfragen. Ein effektives SLO-Management umfasst das Festlegen realistischer Ziele, die Überwachung der Leistung und die kontinuierliche Verbesserung von Services, um die Kundenanforderungen zu erfüllen.

SLO-Management Anwender

Anwender

Anwender	Beschreibung	Enthält Rollen
Administrator	Ein ServiceNow-Administrator ist für Verwaltung, Entwicklung, Betrieb, Schulung und Wartung der ServiceNow Platform verantwortlich. Verantwortlich für die Installation und kann die Service Operations-Arbeitsbereich Admin Center-Konfiguration von SRM durchführen.	Alle
Administrator [srm_admin] **Hinweis:** Nicht die ServiceNow-Rolle `admin`	SRM-Administratoren können Accounteinstellungen, Konfigurationen und Benutzer verwalten. Administratoren können folgende Aktionen ausführen: • Alle SRM-Konfigurationen erstellen, bearbeiten oder löschen und darauf zugreifen. • Integrationen hinzufügen oder verwalten. • Integrationen mit APM-Tools (Application Performance Monitoring) erstellen • Richten Sie Zuverlässigkeitsindikatoren ein, und verwalten Sie sie. • Richten Sie Fehlerbudget-Richtlinien ein, und verwalten Sie sie.	• Manager • Beantworter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
Manager [srm_Manager]	Manager überwachen ein Team von SREs. Manager weisen dem Rufbereitschaftszeitplan des Teams SREs zu, überwachen ihre Leistung, erstellen Verfahren zur Behandlung von Incidents und entwickeln Lösungen. Manager stellen über alle Systeme und DevOps-Workflows hinweg Resilienz sicher. Manager können im Kontext ihrer Teams folgende Aktionen ausführen: • Definieren und richten Sie und Teams, Rufbereitschaftszeitpläne und Services ein. • Benutzer wie Beantworter und Manager für die Teams hinzufügen und löschen, denen sie angehören. • Integrationen hinzufügen oder verwalten. • Integrationen mit APM-Tools (Application Performance Monitoring) erstellen • Richten Sie Zuverlässigkeitsindikatoren ein, und verwalten Sie sie. • Richten Sie Fehlerbudget-Richtlinien ein, und verwalten Sie sie.	Beantworter
Beantworter [srm_Responder]	Ein Service Reliability Engineer (SRE), der SRM zur Ausführung alltäglicher Aufgaben verwendet. Beantworter sind die Personen, die Rufbereitschaft haben und Incidents diagnostizieren und beheben. Beantworter können nur auf Konfigurationen zugreifen, denen sie angehören. Sie können nur auf die Warnungen oder Incidents zugreifen, für die sie Berechtigungen haben. SREs können im Kontext ihrer Teams folgende Aktionen ausführen:	Erbt 17 Rollen, darunter die folgenden: • cmdb_read • sn_sow.sow_user • sn_sow_srm.srm_responder • workspace_user • slo_Operator

Hinweis: Anwender des SLO-Plugins ohne SRM sollten sicherstellen, dass ihren Teammitgliedern der erforderliche Warnungs- und cmdb_ci-Lesezugriff gewährt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLO-Management – Workflow

1. SLOs definieren: Identifizieren Sie kritische Services, und definieren Sie SLOs basierend auf den Kundenerwartungen und Geschäftsanforderungen.
2. SLIs einrichten – entwickeln Sie Servicelevel-Indikatoren (Service Level Indicators, SLIs), um die SLO-Leistung zu messen.
3. Überwachen und analysieren: Verfolgen Sie SLI-Daten, und analysieren Sie die Leistung anhand von SLO-Zielen.
4. Lücken identifizieren und verbessern: Bestimmen Sie Bereiche, in denen SLOs nicht erfüllt werden, und implementieren Sie Changes, um die Serviceleistung zu verbessern.
5. Überprüfen und verfeinern: Überprüfen Sie die SLO-Leistung regelmäßig, und verfeinern Sie SLOs nach Bedarf.

SLO-Management – Vorteile

- Verbesserte Servicequalität – SLOs stellen sicher, dass IT-Services die Kundenerwartungen erfüllen, was zu mehr Zufriedenheit und Loyalität führt.
- Erhöhte Transparenz – klare SLOs bieten ein gemeinsames Verständnis der Serviceerwartungen zwischen IT und Kunden.
- Bessere Ressourcenzuteilung – SLOs helfen, Ressourcen zu priorisieren und sich auf Bereiche zu konzentrieren, die verbessert werden müssen.
- Verbesserte Zusammenarbeit: Das SLO-Management fördert die Zusammenarbeit zwischen IT-Teams und Kunden, um gemeinsame Ziele zu erreichen.
- Datengesteuerte Entscheidungsfindung: SLO-Leistungsdaten sind Grundlage für Entscheidungen und fördern die kontinuierliche Serviceverbesserung.

Arbeiten mit Zuverlässigkeitsmetriken

Erfahren Sie mehr über die Zuverlässigkeitsmetriken und -Funktionen, mit denen Sie die Serviceintegrität nachverfolgen, auf Probleme reagieren und Geschäftsziele unterstützen können.

Servicezuverlässigkeitsdashboard

Das Dashboard „Service Reliability“ zeigt eine anpassbare, allgemeine Ansicht der Serviceleistung an. Sie hilft Ihnen, die Zuverlässigkeit mithilfe von Visualisierungen zu überwachen und zu verwalten, die servicestatus, Fehlerbudgets und Servicelevel-Ziele (Service Level Objectives, SLOs) im Zeitverlauf nachverfolgen.

Das Dashboard zeigt Informationen zu allen Services in an Service Reliability Management(SRM). Sie können in auf das Dashboard zugreifen Service Operations-Arbeitsbereich Gehen Sie wie folgt vor:

- Navigieren zu **Services (** **)** > **Servicezuverlässigkeit**an.
- Navigieren zu **Startseite (** **)** > **Servicezuverlässigkeit**

Weitere Einzelheiten finden Sie unter Visualisierungen im Dashboard „Service Reliability“.

Hinweis: Sie können SLO-Informationen für alle Services auch auf der Registerkarte „Serviceübersicht“ anzeigen. Weitere Informationen finden Sie unter Mit SRM-Services arbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benachrichtigungsziele

Benachrichtigungsziele helfen, Teams über die Zuverlässigkeit der Services auf dem Laufenden zu halten. Hängen Sie sie an Fehlerbudgetrichtlinien an, um Benachrichtigungen zu senden, wenn eine Richtlinie verletzt wird.

Dient zum Anzeigen und Verwalten von Benachrichtigungszielen in Service Operations-Arbeitsbereich, Navigieren Sie zu **Teams** > **[Ihr Team]** > **SLO-Benachrichtigungsziele**an.

Weitere Informationen zum Erstellen und Arbeiten mit Benachrichtigungszielen finden Sie unter den folgenden Links:

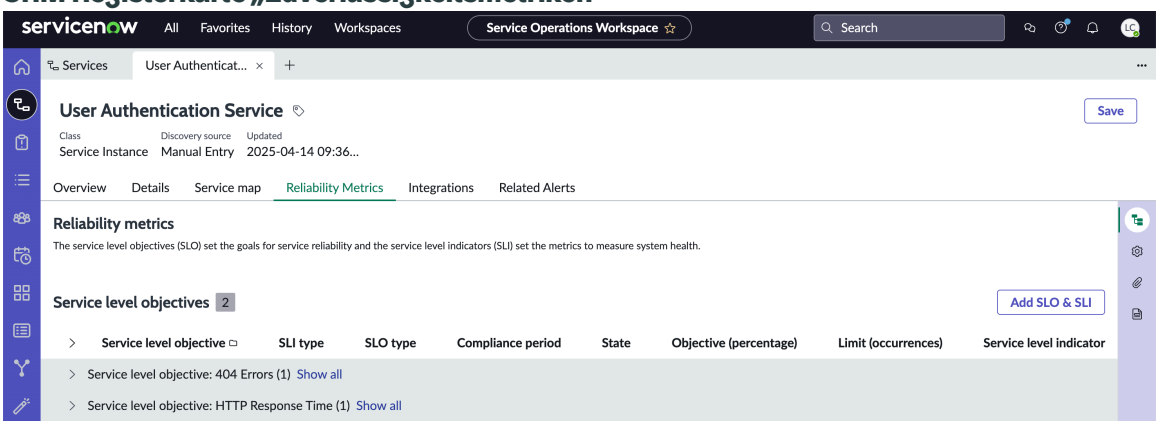
- Erstellen Sie in ein Benachrichtigungsziel SRM
- Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien
- Benachrichtigungen für nicht eingehaltene Fehlerbudgets

Registerkarte „Zuverlässigkeitsmetriken“

Die Registerkarte Zuverlässigkeitsmetriken zeigt, wie gut ein bestimmter Service seine Zuverlässigkeitsziele erfüllt. Verwenden Sie es, um SLOs, Servicelevel-Indikatoren (SLIs) und Fehlerbudgets für einen Service nachzuverfolgen.

Zum Anzeigen der Registerkarte Zuverlässigkeitsmetriken in Service Operations-Arbeitsbereich, Navigieren Sie zu **Services (** **)** > **[Ihr Service]** > **Zuverlässigkeitsmetriken**an.

SRM Registerkarte „Zuverlässigkeitsmetriken“



Unter diesen Links erfahren Sie mehr darüber, was Sie auf der Registerkarte Zuverlässigkeitsmetriken tun können:

- Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien
- Bearbeiten Sie eine Zuverlässigkeitsmetrik
- Anzeigen SRM Zuverlässigkeitsmetriken

Tabelle „Servicelevel-Ziele“

Auf der Registerkarte Zuverlässigkeitsmetriken enthält die Tabelle Servicelevel-Ziele die folgenden Details zum ausgewählten Service:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Servicelevel-Ziel** : Name des SLO. Das SLO ist ein Zielwert oder das Ziel, das Ihr Team erreichen muss, um Ihre Servicelevel-Vereinbarung (SLA) zu erfüllen.
- **SLI-Typ** : Leistungskategorie, die gemessen wird:
  - Verfügbarkeit: Prozentsatz der Zeit, die Ihr Service oder Konfigurationselement verfügbar ist, auch als Betriebszeit bezeichnet.
  - Fehler: Häufigkeit Ihrer Servicefehler.
  - Latenz: Zeit, die für die Bearbeitung einer Anforderung benötigt wird.
  - Sättigung: Vollständigkeit Ihres Systems mit Schwerpunkt auf Ressourcennutzung.
- **Compliance-Zeitraum** : Zeitfenster zur Berechnung der Leistung:
  - Monat: Aktueller Monat. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, ist der Monat der 1. Januar bis 31. Januar.
  - Rollend 7, 30 oder 90 Tage: Anzahl der Tage ab dem aktuellen Datum. Beispiel: Für das Rollieren von 7 Tagen beträgt die Dauer 7 Tage ab dem aktuellen Datum.
- **Status** : Status des SLO, z. B. „Entwurf“, „wird ausgeführt“ oder „stillgelegt“.
- **Ziel (Prozentsatz)** : Zielprozentsatz der SLI-Leistung.
- **Vorkommen begrenzen** : Anzahl der aufgetretenen Grenzwertverletzungen. Wird nur von zählungsbasierten SLOs verwendet.
- **Servicelevel-Indikator** : SLI, das dem SLO zugeordnet ist.
- **Fehlerbudget** : Zulässige Fehlerzeit für den Compliance-Zeitraum, berechnet anhand des Compliance-Zeitraums und des Ziels (Prozentsatz).
- **Verbleibendes Fehlerbudget** : Fehlerbudget noch verfügbar.
- **Verbleibende Verstoßvorkommen** : Anzahl der noch verfügbaren Verstöße, bevor der Grenzwert erreicht ist.

Hinweis: Zu Leistungszwecken werden SLO- und SLI-Datensätze ([sn_SOW_srm_Slo_history] und [sn_SOW_srm_sli_metric]) nach einem Jahr archiviert und fünf Jahre später gelöscht. Archivierte Daten werden in Tabellen und Visualisierungen ausgelassen.

SLO-Management verwenden

Die Verwendung von SLO-Management stellt sicher, dass IT-Services die Kundenerwartungen erfüllen, verbessert die Servicequalität und -Transparenz und ermöglicht datengesteuerte Entscheidungsfindung.

Aktivieren Sie SLO-basierte Change-Genehmigungsentscheidungen

Aktivieren Sie Change-Genehmigungsentscheidungen für Service Level Objective (SLO), um Change-Anforderungen basierend auf der SLO-Leistung zu bewerten.

Vorbereitungen

Überprüfen Sie Richtlinien für Change-Genehmigungen und ihre Terminologie, einschließlich Richtlinieneingaben, Entscheidungen und Genehmigungsdefinitionen. Weitere Informationen finden Sie unter Richtlinien für Change-Genehmigungen .

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie die Entscheidungen der Change-Richtlinie für Servicelevel-Ziele, um die SLO-Leistung in Ihren Change-Management-Prozess einzubeziehen. Die Richtlinie ist standardmäßig aktiv, ihre Entscheidungen sind jedoch inaktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Entscheidungen der Richtlinie aktivieren, wertet die Richtlinie SLOs als Eingaben aus und implementiert Folgendes:

- Gruppenmanager-Genehmigung anfordern, wenn diese Bedingungen wahr sind:
  - Das niedrigste SLO-Fehlerbudget beträgt weniger als 25 %.
  - Die höchste SLO-Durchsatzrate ist größer als 1 %.
- Change-Anforderungen automatisch genehmigen, wenn diese Bedingungen wahr sind:
  - Das niedrigste SLO-Fehlerbudget ist größer als 25 %.
  - Die höchste SLO-Durchsatzrate beträgt weniger als 1 %.

Prozedur

1. Navigieren zu **Alle** > **Change** > **Change-Richtlinie** > **Richtlinien Für Change-Genehmigungen**an.
2. Wählen Sie aus **Change-Richtlinie für Servicelevel-Ziel** .
3. In **Entscheidungen** Registerkarte, festlegen **Aktiv** Auf „wahr“ für diese Entscheidungen:
   - **Budget < 25 % und Durchsatz > 1**
   - **Budget > 25 % und Durchsatz < 1**
4. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
   Die Entscheidungen sind aktiv und Teil Ihres Change-Management-Prozesses.

Nächste Maßnahme

Verwenden Sie eine Test-Change-Anforderung, um sicherzustellen, dass Change-Anforderungen entweder automatisch genehmigt oder wie erwartet an einen Manager weitergeleitet werden.

Sie können auch die Change-Richtlinie für Servicelevel-Ziel nach Bedarf anpassen, einschließlich Name und Bedingungen.

Für erweiterte Setups verwenden Sie Flow Designer, um die SLOs und Services anzupassen, die als Richtlinieneingaben enthalten sind:

Wichtig: Durch das Anpassen des Flows wird verhindert, dass er zukünftige Release-Updates erhält. Dieses Verhalten ist beabsichtigt, um zu vermeiden, dass Ihre Anpassungen überschrieben werden.

1. Navigieren zu **Prozessautomatisierung** > **Flow Designer**an.
2. Wählen Sie in der Liste der Flows die Option aus **Change – SLO – Autorisieren** Und wählen Sie dann aus **SLO: SLOs mit der schlechtesten Leistung abrufen** .
3. Passen Sie an **Aktionseingaben** Abschnitt.
4. Wählen Sie Aus **Fertig** Um Ihre Änderungen zu implementieren.

Erstellen Sie in ein Benachrichtigungsziel SRM

Richten Sie Benachrichtigungsziele ein, um Teams über die Zuverlässigkeit der Services auf dem Laufenden zu halten.

Vorbereitungen

Richten Sie vor dem Erstellen von Benachrichtigungszielen den ein Microsoft Teams Graph Spoke. Beim Registrieren einer Anwendung in Microsoft Azure Portal gewähren Sie Folgendes Microsoft Teams Graph API-Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kanalnachricht.Senden
- Gruppe.Lesen.alle**

Setup-Anweisungen finden Sie unter Richten Sie die Microsoft Teams Graph-Spoke ein .

Erforderliche Rolle: srm_Manager, srm_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie ein Benachrichtigungsziel, um Nachrichten an einen bestimmten zu übermitteln Microsoft Teams Kanal. Nachdem Sie ein Benachrichtigungsziel eingerichtet haben, können Teammitglieder es an Fehlerbudgetrichtlinien anhängen, um Nachrichten über Richtlinienverstöße zu erhalten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
2. Wählen Sie in der primären Navigation aus **Teams** ( ).
3. Wählen Sie auf der Seite Teams das Team aus, das Sie als Benachrichtigungsziel verwenden möchten.
4. Wählen Sie aus **SLO-Benachrichtigungsziele** Wählen Sie die Registerkarte aus **Erstellen Sie ein Ziel** , Und füllen Sie dann das Formular aus.

Feld	Beschreibung
Kanal-URL	Deep-Link zu relevantem Microsoft Teams Kanal. Deep-Links zu Kanälen finden Sie in Microsoft Teams. Sie folgen diesem allgemeinen Format: https://teams.microsoft.com/l/channel/19%abcdef .
Zielname	Anzeigename des Benachrichtigungsziels. Teams sehen diesen Namen, wenn Benachrichtigungsziele zu Fehlerbudgetrichtlinien hinzugefügt werden.

5. **Wahlweise:** Wählen Sie Aus **Testbenachrichtigung senden** Um Ihr Setup zu verifizieren.
   Wenn erfolgreich, wird eine Meldung in der entsprechenden angezeigt Microsoft Teams Kanal. Die Nachricht hat den Titel Testbenachrichtigung Und enthält den folgenden Text:

   ```
   This is a test notification from the Service Reliability Management (SRM) Team '<team-name>'.
   ```

6. Wählen Sie **Speichern**.
   Das Benachrichtigungsziel wird auf der Registerkarte SLO-Benachrichtigungsziele angezeigt. Die Tabelle enthält Details zum Microsoft Teams Kanal und Zeitpunkt der letzten Aktualisierung des Benachrichtigungsziels.

Nächste Maßnahme

Um Benachrichtigungsziele zu verwenden und weitere Informationen zu erhalten, besuchen Sie die folgenden Seiten:

- Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien
- Benachrichtigungen für nicht eingehaltene Fehlerbudgets

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Benachrichtigungsziele auch auf der Registerkarte „SLO-Benachrichtigungsziele“ bearbeiten und löschen. Durch das Löschen eines Benachrichtigungsziels wird es aus allen Fehlerbudget-Richtlinien entfernt, in denen es zuvor verwendet wurde.

Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien

Definieren Sie Servicelevel-Ziele (SLOs), Servicelevel-Indikatoren (SLIs) und Fehlerbudget-Richtlinien, um die Serviceintegrität zu überwachen. Diese Tools helfen Ihnen und Ihren Teams, die Leistung nachzuverfolgen und bei Bedarf Maßnahmen zu ergreifen.

Vorbereitungen

Wenn Sie Teams benachrichtigen möchten, wenn gegen eine Fehlerbudgetrichtlinie verstoßen wird, stellen Sie sicher, dass für Ihr Team ein Benachrichtigungsziel verfügbar ist. Navigieren Sie zum Überprüfen zu **Teams** > **[Ihr Team]** > **SLO-Benachrichtigungsziele** in Service Operations-Arbeitsbereich.

Informationen zum Erstellen eines Benachrichtigungsziels finden Sie unter Erstellen Sie in ein Benachrichtigungsziel SRM.

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien, um die Serviceintegrität zu überwachen und sicherzustellen, dass Ihre Services Geschäftsziele unterstützen.

- SLOs sind spezifische Ziele, die Sie für SLIs festgelegt haben. Sie definieren das erwartete Leistungsniveau.
- SLIs sind Metriken, die die Leistung messen, z. B. Verfügbarkeit oder Latenz.
- Fehlerbudgetrichtlinien definieren die zulässige Fehlerspanne und was geschieht, wenn dieser Schwellenwert überschritten wird.

In Service Reliability Management(SRM), muss ein SLO mindestens einen SLI haben. SLIs können nach einem Service oder Configuration Item (CI) innerhalb der Hierarchie des übergeordneten Service gefiltert werden. Das Filtern eines SLI nach einem CI kann Ihnen helfen, die Serviceintegrität genauer nachzuverfolgen und Ursachen schneller zu identifizieren.

Für weitere allgemeine Informationen zu SLOs, SLIs und Fehlerbudgetrichtlinien in SRM, Siehe Arbeiten mit Zuverlässigkeitsmetriken.

Hinweis: In SRM, Jeder SLI kann nur einem SLO zugeordnet werden. Die Verwendung desselben SLI in mehreren SLOs erstellt mehrere Ziele für dieselbe Metrik, was zu Verwirrung oder in Konflikt stehenden Leistungserwartungen führen kann.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Services** Symbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Auf der **Services** Wählen Sie den Service aus, für den Sie SLOs und SLIs erstellen möchten.
4. Wählen Sie aus **Zuverlässigkeitsmetriken** Registerkarte und wählen Sie dann aus **Fügen Sie SLO und SLI hinzu** .
5. Füllen Sie im Formular „Servicelevel-Ziel (SLO)“ die Felder für Ihr SLO aus.
   Informationen zu den SLO-Feldern finden Sie unter SLO-Formular erstellen.
6. Wählen Sie im Formular Servicelevel-Indikatoren (SLI) die Option aus **Fügen Sie SLI hinzu** , Und füllen Sie die Felder für Ihr SLI aus.
   Weitere Informationen zu den SLI-Feldern finden Sie unter SLI-Formular erstellen.

   Hinweis: Wenn Ihr Service ein oder mehrere CIs in seiner Hierarchie enthält, wird ein Banner unter dem Header „Servicelevel-Indikatoren“ (SLI) angezeigt. Das Banner listet die Anzahl der verfügbaren CIs und Links zur Servicezuordnung auf, sodass Sie ihre Verbindungen visualisieren können. Sie können diese Informationen verwenden, um Ihre SLIs im Formular „SLI hinzufügen“ nach bestimmten CIs zu filtern, was Ihnen ein detaillierteres Maß für die Serviceintegrität bietet.

7. **Wahlweise:** Wählen Sie im Formular „Fehlerbudgetrichtlinien“ die Option aus **Schwellenwert hinzufügen** , Und füllen Sie die Felder für Ihre Fehlerbudget-Richtlinie aus.
   Weitere Informationen finden Sie unter Fügen Sie ein Formular für eine Fehlerbudget-Richtlinie hinzu.

   Hinweis: Wenn Sie keine Fehlerbudget-Richtlinie hinzufügen, ist der Zielprozentsatz des SLO nur informativ. Das Hinzufügen einer Richtlinie hilft Ihnen, Korrekturmaßnahmen basierend auf den Leistungsdaten zu ergreifen. Wenn Sie jetzt noch nicht bereit sind, eine Richtlinie hinzuzufügen, können Sie später eine hinzufügen.

8. Überprüfen Sie Ihre SLO-, SLI- und Fehlerbudgetrichtlinie, und wählen Sie dann aus **Aktivieren** .

   Ihre SLO-, SLI- und, falls hinzugefügt, Fehlerbudget-Richtlinie sind aktiv, sodass Sie die Serviceintegrität überwachen und bei Bedarf Maßnahmen ergreifen können. Informationen zum Anzeigen und Aktualisieren von Zuverlässigkeitsmetriken finden Sie unter Bearbeiten Sie eine Zuverlässigkeitsmetrik.

Bearbeiten Sie eine Zuverlässigkeitsmetrik

Aktualisieren Sie eine Zuverlässigkeitsmetrik, um sie relevant und an den Zielen Ihres Teams ausgerichtet zu halten.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_Manager oder srm_Responder

Das Aktualisieren von Zuverlässigkeitsmetriken, z. B. Servicelevel-Ziele (Service Level Objectives, SLOs) oder Servicelevel-Indikatoren (Service Level Indicators, SLIs), während aktiver Messzeiträume kann zu Inkonsistenzen im Diagramm führen.

Warum und wann dieser Vorgang ausgeführt wird

Damit Sie den Verlauf der Zuverlässigkeitsmetrik verwalten können, Service Reliability Management(SRM) Folgt bestimmten Benennungskonventionen. Wenn Sie eine Zuverlässigkeitsmetrik bearbeiten, SRM Führt Folgendes aus:

- Setzt das vorhandene SLO außer Kraft.
- Erstellt eine Kopie des SLO mit Ihren Bearbeitungen im Entwurfsstatus. Sie können entweder:
  - Speichern Sie die Kopie als Entwurf.
  - Aktivieren Sie die Kopie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Hängt eine Zahl an den Namen der Kopie an, z. B. Betriebszeit (2) oder Betriebszeit (3).
- Zeigt alle SLO-Versionen in an **Zuverlässigkeitsmetriken** Registerkarte.

Hinweis: In **Zuverlässigkeitsmetriken** Registerkarte haben SLO-Header zwei Zahlen, z. B. HTTP-Antwortzeit (2) (3). Die erste Zahl ist ihre Version. Die zweite ist die Anzahl der SLIs, die dem SLO zugeordnet sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Führen Sie die folgenden Schritte aus, um auf zuzugreifen **Zuverlässigkeitsmetriken** Registerkarte:
   a. Wählen Sie aus **Services** Seitensymbol ( ).
   b. Wählen Sie den Service aus, der die Zuverlässigkeitsmetrik verwendet, die Sie bearbeiten möchten.
   c. Wählen Sie die Registerkarte **Zuverlässigkeitsmetriken**.
3. Um eine Zuverlässigkeitsmetrik zu bearbeiten, wählen Sie die relevante Zuverlässigkeitsmetrik aus, und wählen Sie dann aus **Bearbeiten** Und **Fahren Sie mit der Bearbeitung fort** .
4. Wählen Sie aus, um Ihre Änderungen zu speichern und zu implementieren **Aktivieren** .
   Ihre bearbeitete Zuverlässigkeitsmetrik wird in angezeigt **Zuverlässigkeitsmetriken** Registerkarte.
   SRM Legt den Status auf „wird ausgeführt“ fest und enthält eine Versionsnummer in ihrem Namen, z. B. „Betriebszeit“ (3).

Nächste Maßnahme

Die Verwaltung von SLOs erfordert laufende Updates, um sicherzustellen, dass sie Ihre Zuverlässigkeitsziele widerspiegeln. Sie können vorhandene SLOs bearbeiten oder stilllegen und bei Bedarf stillgelegte SLOs erneut aktivieren.

Hinweis: Wenn Sie ein stillgelegtes SLO erneut aktivieren, erstellt und aktiviert SRM eine neue Kopie davon. Beispiel: Wenn es zwei Versionen eines SLO gibt, Betriebszeit (1) und Betriebszeit (2), und Sie die Betriebszeit erneut aktivieren (1), belassen SRM den Status „stillgelegt“ und erstellt eine aktive Version mit der Bezeichnung „Betriebszeit“ (3).

Anzeigen SRM Zuverlässigkeitsmetriken

Zeigen Sie ein Servicelevel-Ziel (Service Level Objective, SLO) und einen Servicelevel-Indikator (Service Level Indicator, SLI) an, die Ihr oder Ihr Team besitzt.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Hinweis: Administratoren können jedes SRM-SLO anzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*an.
   Sie werden zu weitergeleitet SRM Homepage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation die aus **Services** Symbol ( ).
3. Wählen Sie die Registerkarte **Zuverlässigkeitsmetriken**.
4. Öffnen Sie ein **Servicelevel-Ziel**.
5. Zeigen Sie den SLO-Header an.

   Der oberste Header enthält Serviceinformationen für:

   - **SLI-Typ**:

     Typ des SLI, auf dessen Grundlage die Servicelevel-Metriken (SLM) berechnet werden. Die folgenden SLI-Typen sind verfügbar:

     - **Verfügbarkeit**: Prozentsatz der Zeit, während der Ihr Service verfügbar ist. (Standard)
     - **Fehler**: Messung, wie häufig ein Servicefehler auftritt.
     - **Latenz**: Zeit, die für die Bearbeitung einer Anfrage benötigt wird. Die tatsächlich verstrichene Zeit.
     - **Sättigung**: Messung des Systemanteils, wobei die am stärksten eingeschränkten Ressourcen hervorgehoben werden.

     .

   - **SLO-Typ**:

     Typ des SLO basierend auf der von Ihnen ausgewählten Metrik. Die folgenden SLO-Typen sind verfügbar:

     - **Dauer**: Zeit, die der Service ohne Verstoß ausgeführt wird. Dies ist der einzige verfügbare Wert.

       Die Metriken für **Dauer** lauten wie folgt:

       - **Ziel (Prozentsatz)**: Prozentsatz der gewünschten SLI-Leistung.
       - **Fehlerbudget**: Zeigt das verbleibende Fehlerbudget in Tagen und Zeit an.

     - **Anzahl**: Häufigkeit des Auftretens in einem vorgegebenen Konformitätszeitraum.

       Die Metriken für **Anzahl** lauten wie folgt:

       - **Grenze (Vorkommen)**: Anzahl der Vorkommen, nach denen ein Verstoß aufgetreten ist.
       - **Verbleibende aufgetretene Verstöße**: Anzahl der verbleibenden Vorkommen.

   - **Status**:

     Status des SLO. Die Auswahlmöglichkeiten lauten wie folgt:

     - Entwurf: Der SLO wird in Ihrer Instanz noch nicht ausgeführt. Sie können neue SLIs hinzufügen oder vorhandene SLIs aktualisieren, und Sie können den SLO löschen.
     - Wird ausgeführt: Der SLO ist in Ihrer Instanz aktiv. Sie können den SLO bearbeiten, stilllegen oder löschen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen SLO im Ausführungsstatus bearbeiten, wird er deaktiviert und eine neue Kopie wird erstellt.

- Deaktiviert: Der SLO wird in Ihrer Instanz nicht mehr ausgeführt. Sie können ihn reaktivieren.

- **Service**: Service, der dem SLO zugeordnet ist.

- **Zuverlässigkeit**: Gibt an, wie zuverlässig der Service ist.
  - **Stabil**: Für alle SLOs in diesem Service sind noch mehr als 25 % des Fehlerbudgets verfügbar.
  - **Gefährdet**: Alle SLOs in diesem Service verfügen noch über EB, und mindestens ein SLO in diesem Service weist weniger als 25 % des verbleibenden Fehlerbudgets auf.
  - **Kritisch**: Für alle SLOs in diesem Service ist das Fehlerbudget aufgebraucht.

Über den Header können Sie das SLO **löschen**, **stilllegen** oder **bearbeiten**.

Wenn Sie ein SLO löschen, werden auch alle zugehörigen SLIs gelöscht.

Wenn Sie ein SLO stilllegen, ändert sich der Status. Auf der Seite „SLO“ oder später auf der Registerkarte **Zuverlässigkeitsmetriken** können Sie es **erneut aktivieren**.

Hinweis: Wenn Sie ein SLO bearbeiten, ändert es den Status, zieht den SLO-Datensatz zurück und öffnet eine neue Kopie zur Bearbeitung. Weitere Informationen finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien. Sie können das ursprüngliche SLO reaktivieren, indem Sie zur Registerkarte **Zuverlässigkeitsmetriken** zurückkehren.

6. Zeigen Sie an **Übersicht** Registerkarte und wählen Sie im Listenmenü einen Verlaufszeitraum aus.
   Die aufgeführten Zeiträume reichen vom Datum der Erstellung des SLO bis zum aktuellen in den ausgewählten Schritten.
7. Zeigen Sie die **Zusammenfassung**-Metrikkarten für das SLO an.
   Die Metriken zeigen aggregierte oder durchschnittliche Werte an, abhängig vom Typ der ausgewählten SLIs und der ausgewählten Fehlerrichtlinien-Schwellenwerte. Ausführliche Informationen finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.
8. Zeigen Sie den Abschnitt **Servicelevel-Indikatoren** an.

   In diesem Abschnitt werden Ihre Indikatoren nach Namen aufgelistet.
9. Zeigen Sie den Abschnitt **Servicelevel-Ziel (SLO) – Verlauf** an.
   In Abhängigkeit von Ihrem **SLO-Typ** wird in diesem Abschnitt Folgendes in Balkendiagrammberichten angezeigt:

   Für **Dauer**:
   - Genutztes Fehlerbudget
   - Verbleibendes Fehlerbudget
   - Durchsatz

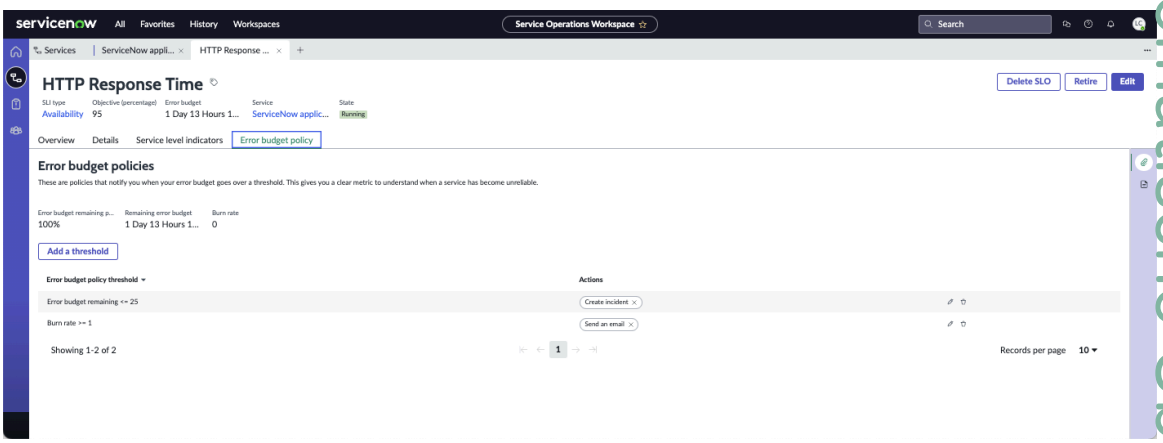
   Für **Anzahl**, **Nach Zeiträumen zählen** oder **Nach Auftreten zählen**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kumulative aufgetretene Verstöße
- Durchsatz
- Warnungen, Incidents und Changes, die sich auf diesen Service auswirken

Wenn Sie in einem der Analytics-Liniendiagrammberichte auswählen, werden die Werte an diesem Tag angezeigt.

10. Rufen Sie die Registerkarte **Details** auf.
    Die Felder auf dieser Registerkarte werden automatisch gefüllt und können nicht bearbeitet werden. Ausführliche Informationen zu den Feldern finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.
11. Zeigen Sie die Registerkarte **Servicelevel-Indikatoren** an.
    Auf dieser Registerkarte werden die SLIs aufgelistet, die diesem SLO zugeordnet sind.
12. Zeigen Sie die Registerkarte **Fehlerbudget-Richtlinie** an.
    Auf dieser Registerkarte können Sie weitere Schwellenwerte hinzufügen und vorhandene bearbeiten oder löschen.



SLO-Management-Referenz

Referenzthemen enthalten zusätzliche Informationen zu Servicelevel-Zielmanagement.

Fügen Sie ein Formular für eine Fehlerbudget-Richtlinie hinzu

Erfahren Sie mehr über die verfügbaren Felder zum Einrichten von Fehlerbudgetrichtlinien.

Felder im Formular Fehlerbudget-Richtlinie hinzufügen

In der folgenden Tabelle werden die verfügbaren Optionen im Formular „Fehlerbudget-Richtlinie hinzufügen“ beschrieben. Eine schrittweise Anleitung finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

Feld	Beschreibung
Richtlinienname	Anzeigename der Fehlerbudget-Richtlinie.
Schwellenwerttyp	Wählen Sie aus, wie Sie Ihr Fehlerbudget nachverfolgen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Durchsatz (Anzahl)** : Verfolgt, wie schnell das Fehlerbudget verbraucht wird. Ein höherer Durchsatz bedeutet schnelleren Verbrauch. • **Verbleibendes Fehlerbudget (%)** : Verfolgt den Prozentsatz des Fehlerbudgets, der während des angegebenen Zeitraums noch verfügbar ist. **Hinweis:** Sie können einer Richtlinie mehrere Schwellenwerte hinzufügen, aber jeder muss eindeutig sein. Wenn Sie versuchen, einen doppelten Schwellenwert hinzuzufügen, wird eine Fehlermeldung angezeigt.
Schwellenwert	Der Punkt, an dem Sie basierend auf dem ausgewählten SLO-Indikator benachrichtigt werden. • Durchsatz: Legen Sie einen Wert fest, der angibt, dass der Durchsatz zu hoch ist. Um beispielsweise benachrichtigt zu werden, wenn Ihr Service oder Konfigurationselement sein Fehlerbudget doppelt so schnell wie erwartet durchbrennt, legen Sie den Schwellenwert auf 2 fest. • Verbleibendes Fehlerbudget: Legen Sie einen Wert fest, der angibt, dass das verbleibende Fehlerbudget zu niedrig ist. Um beispielsweise benachrichtigt zu werden, wenn nur 25 % oder weniger des Fehlerbudgets verbleiben, legen Sie den Schwellenwert auf 25 % fest. **Hinweis:** Die Schwellenwerte unterstützen bis zu 4 Dezimalstellen und runden dann auf.
Richtlinienaktion	[Optional] wenn ein Verstoß auftritt, wählen Sie die Aktion aus, die Sie ausführen möchten: • Incident erstellen. • E-Mail senden • Benachrichtigen Microsoft Teams. Wenn Sie diese Option auswählen, müssen Sie auch ein relevantes Benachrichtigungsziel auswählen. Informationen zum Einrichten eines Benachrichtigungsziels für Ihr Team

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	finden Sie unter Erstellen Sie in ein Benachrichtigungsziel SRM. **Hinweis:** Weitere Informationen zu den Benachrichtigungen, die Teams für verstoßene Fehlerbudgetrichtlinien erhalten, finden Sie unter Benachrichtigungen für nicht eingehaltene Fehlerbudgets.

SLO-Formular erstellen

Erfahren Sie mehr über die verfügbaren Felder zum Hinzufügen eines Servicelevel-Ziels (SLO) zu Service Reliability Management.

Formular „Servicelevel-Ziel“

In der folgenden Tabelle werden die verfügbaren Optionen im Formular „Servicelevel-Ziel“ beschrieben. Eine schrittweise Anleitung finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

Felder im Formular „Servicelevel-Ziel“

Feld	Beschreibung
Name	Name des SLO.
SLI-Typ	Typ des SLI, auf dessen Grundlage die Servicelevel-Metriken (SLM) berechnet werden. Die folgenden SLI-Typen sind verfügbar: • **Verfügbarkeit**: Prozentsatz der Zeit, während der Ihr Service verfügbar ist. (Standard) • **Fehler**: Messung, wie häufig ein Servicefehler auftritt. • **Latenz**: Zeit, die für die Bearbeitung einer Anfrage benötigt wird. Die tatsächlich verstrichene Zeit. • **Sättigung**: Messung des Systemanteils, wobei die am stärksten eingeschränkten Ressourcen hervorgehoben werden.
Wie möchten Sie dieses Ziel messen?	Sie können dieses Ziel wie folgt messen: • **Dauer**: Zeit, die der Service ohne Verstoß ausgeführt wird. Dies ist der einzige verfügbare Wert. • **Anzahl**: Die Anzahl der Zeiträume oder Vorkommen in einem bestimmten Compliance-Zeitraum.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Measuring by Duration (Messung nach Dauer)

Feld	Beschreibung
Ziel (%)	Der Prozentsatz der gewünschten Verfügbarkeit (Betriebszeit) des Service über einen bestimmten Zeitraum. Bei der Messung nach Dauer bedeutet ein Zielprozentsatz von „fünf Neunen“ (die sog. Five-Nines-Verfügbarkeit von 99,999 %), dass der Service 26 Sekunden pro Monat oder etwa 5 Minuten und 35 Sekunden pro Jahr nicht verfügbar war. Dies wird verwendet, um Ihr Fehlerbudget zu berechnen.
Compliance-Zeitraum	Zeitraum, für den die Metriken berechnet werden. Verfügbare Optionen: • **Monat**: Als Dauer wird der aktuelle Monat betrachtet. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer vom 1. Januar bis zum 31. Januar angenommen. • **Rollend, 7 Tage**: Für die Dauer werden 7 Tage ab dem aktuellen Datum angenommen. • **Rollend, 30 Tage**: Für die Dauer werden 30 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Dezember berücksichtigt. • **Rollend, 90 Tage**: Für die Dauer werden 90 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Oktober berücksichtigt.
Fehlerbudget	Automatisch ausgefüllt. Das maximale Fehlerniveau (Ausfallzeit), das über einen bestimmten Zeitraum zulässig ist. Ein Prozentsatz der gesamten Serviceverfügbarkeit. Sobald Sie Ihr Ziel in % festgelegt haben, wird Ihr Fehlerbudget automatisch mit der folgenden Formel berechnet: 1 – (gewünschte) Verfügbarkeit. Das Fehlerbudget eines Service wird in Tagen, Stunden, Minuten und Sekunden für eine gewünschte Verfügbarkeit von 99,99 % (Vier Neunen) des Jahres berechnet durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Measuring by Duration (Messung nach Dauer) (Fortsetzung)

Feld	Beschreibung
	1. Berechnung der Gesamtzeit in Sekunden in einem Jahr: 31536000 Sekunden. 2. Das Fehlerbudget wird als 1 – (gewünschte) Verfügbarkeit bestimmt: 1 – 0,9999 = 0,0001. 3. Konvertieren des Fehlerbudgets in Zeiteinheiten. Wenn das Fehlerbudget beispielsweise 0,0001 beträgt: • Fehlerbudget in Sekunden = 0,0001 * 31.536.000 Sekunden = 3.153,6 Sekunden. • Fehlerbudget in Minuten = 3.153,6 Sekunden / 60 = 52,56 Minuten. • Fehlerbudget in Stunden = 52,56/60 = 0,875 Stunden. • Fehlerbudget in Tagen = 52,56 Minuten / (24 * 60) ≈ 0,0364 Tage. **Hinweis:** Ihr Fehlerbudget wird nur dann in Einheiten von Tagen, Stunden, Minuten und Sekunden angezeigt, wenn Sie Ihr SLO nach Dauer messen.

Messung nach Anzahl

SLO-Typ	„Nach Zeiträumen zählen oder „Nach Auftreten zählen“
Limit occurrences (Limit Vorkommen)	Die Anzahl der Vorkommen, nach denen ein Verstoß auftritt. Grenzwertvorkommen wirken wie ein Fehlerbudget.
Compliance-Zeitraum	Zeitraum, für den die Metriken berechnet werden. Verfügbare Optionen: • **Monat**: Als Dauer wird der aktuelle Monat betrachtet. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer vom 1. Januar bis zum 31. Januar angenommen. • **Rollend, 7 Tage**: Für die Dauer werden 7 Tage ab dem aktuellen Datum angenommen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Messung nach Anzahl (Fortsetzung)

SLO-Typ	„Nach Zeiträumen zählen oder „Nach Auftreten zählen“
	• **Rollend, 30 Tage**: Für die Dauer werden 30 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Dezember berücksichtigt. • **Rollend, 90 Tage**: Für die Dauer werden 90 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Oktober berücksichtigt.

Hinweis: Die **Zuweisungsgruppe** Wird automatisch ausgefüllt.

SLI-Formular erstellen

Erfahren Sie mehr über die verfügbaren Felder zum Hinzufügen eines Servicelevel-Indikators (SLI) zu einem Servicelevel-Ziel (SLO).

Formular „SLI hinzufügen“

In der folgenden Tabelle werden die verfügbaren Optionen im Formular „SLI hinzufügen“ beschrieben. Eine schrittweise Anleitung finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

Felder im Formular „SLI hinzufügen“

Feld	Beschreibung
SLI-Name	Geben Sie einen Namen für Ihr SLI ein. Beispiel: Kritisches Routerproblem.
Datenquelle	Dieses Feld wird automatisch gefüllt. Die Warnungen aus dieser Datenquelle, auch als Integration bezeichnet, werden zur Berechnung des Fehlerbudgets verwendet.
Bedingungen festlegen (optional) Passen Sie Ihr SLI an, indem Sie es nach „spezifisch“ filtern Konfigurationselemente oder Warnungen. Die Felder in diesem Abschnitt sind optional.	
Nach CI filtern	Filtern Sie Ihren SLI nach einem Konfigurationselement (Configuration Item, CI) innerhalb der Hierarchie des übergeordneten Service. Das Filtern eines SLI nach einem CI kann Ihnen helfen, die Serviceintegrität genauer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder im Formular „SLI hinzufügen“ (Fortsetzung)

Feld	Beschreibung
	nachzuverfolgen und Ursachen schneller zu identifizieren.
Fügen Sie einen Bedingungssatz hinzu	Wählen Sie diese Option aus, um die Warnungen anzugeben, die im Fehlerbudget enthalten sind. Beispiel: Wenn Sie die Bedingung auf festlegen **Status ist „Kritisch“** , Werden nur Warnungen mit einem kritischen Status auf das Fehlerbudget angerechnet.

Benachrichtigungen für nicht eingehaltene Fehlerbudgets

Details zu den Benachrichtigungen, die Teams für verstoßene Fehlerbudgetrichtlinien erhalten.

Wenn Benachrichtigungen gesendet werden

Wenn ein Service oder Konfigurationselement gegen seine Fehlerbudget-Richtlinie verstößt und ein Benachrichtigungsziel festgelegt wird, Service Reliability Management(SRM) Sendet eine Benachrichtigung an den konfigurierten Microsoft Teams Kanal.

Benachrichtigungsinhalt

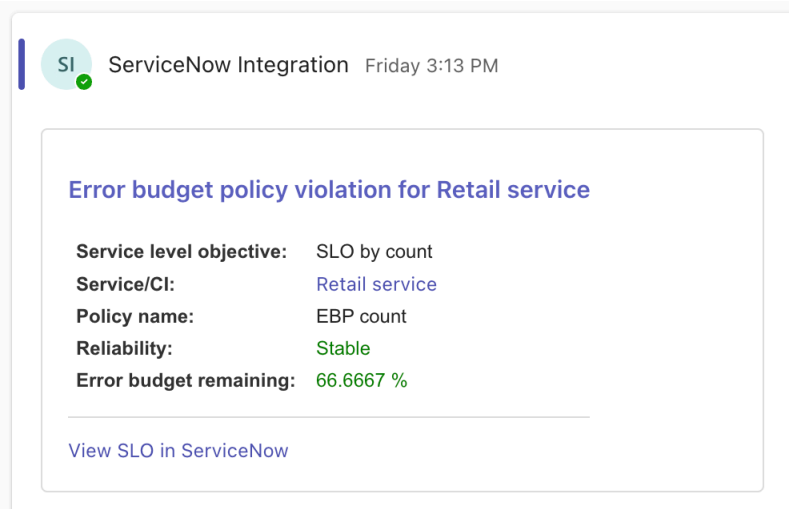
Die Nachricht enthält Details zum Verstoß, damit Teammitglieder mehr über das Problem erfahren und handeln können. In Microsoft Teams, Die Nachricht hat den Titel Verstoß gegen Fehlerbudget-Richtlinie Und listet die folgenden Informationen auf:

- Servicelevel-Ziel: Name des Servicelevel-Ziels (SLO), z. B. Verfügbarkeit des Navigationsservice 99,95 .
- Service/CI: Name des zugeordneten Service oder Konfigurationszeitpunkts. Wählen Sie den Namen aus, in dem der relevante Service geöffnet werden soll SRM.
- Richtlinienname: Name der Fehlerbudget-Richtlinie, die nicht eingehalten wurde.
- Zuverlässigkeit: Der Servicestatus: Kritisch, gefährdet oder stabil.
- Verbleibendes Fehlerbudget: Prozentsatz des verbleibenden Fehlerbudgets zum Zeitpunkt des Verstoßes.
- SLO in ServiceNow anzeigen: Link zum Anzeigen der SLO-Details in SRM.

Beispielbenachrichtigung

Das folgende Bild ist eine Beispielbenachrichtigung in Microsoft Teams. Zeigt einen Verstoß gegen die Fehlerbudget-Richtlinie für den Einzelhandelsservice und Details zum verbleibenden SLO, Servicestatus und Fehlerbudget an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zugehörige Dokumentation

Siehe Erstellen Sie in ein Benachrichtigungsziel SRM und Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

Visualisierungen im Dashboard „Service Reliability“

Liste der Visualisierungen und Optionen im Dashboard „Service Reliability“ in Service Reliability Management(SRM).

Servicestatus-Diagramme

Diagramme der obersten Ebene zeigen die Anzahl der Services in den status „Kritisch“, „gefährdet“ und „stabil“ an. Ihre status basieren auf dem Fehlerbudget, das für ihre Servicelevel-Ziele (Service Level Objectives, SLOs) verbleibt. Sie können die Diagramme auswählen, um Servicenamen anzuzeigen, den Zeitbereich anzupassen und auf zusätzliche Diagrammoptionen zuzugreifen.

Hinweis: Ein Fehlerbudget ist der Betrag des Fehlers, den ein Service erleben kann, bevor er sein SLO verletzt.

Jede Visualisierung enthält auch eine Trendlinie, die Änderungen bei der Anzahl der Services in den letzten 12 Monaten anzeigt. Kleinere Zahlen geben an, wie sich die Anzahl im Vergleich zu vor einer Woche geändert hat, z. B. ↓25 (22 %) seit Juni 11.

Diagramm	Was es ist	Verwendung
Kritisch	Zeigt die Anzahl der Services in einem kritischen Status an. Für kritische Services verbleiben 0 % Fehlerbudget in ihren SLOs.	Zeigen Sie an, wie viele Services ihre Fehlerbudgets verbraucht haben, und identifizieren Sie die Services, die sofortige Aufmerksamkeit erfordern.
Gefährdet	Zeigt die Anzahl der gefährdeten Services an. Gefährdete Services haben <= 25 % Fehlerbudget in ihren SLOs.	Überwachen Sie, wie viele Services sich kritischen Schwellenwerten nähern, und finden Sie Probleme frühzeitig.
Stabil	Zeigt die Anzahl der stabilen Services an. Für stabile Services	Erhalten Sie Einblicke in die allgemeine Serviceintegrität, und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagramm	Was es ist	Verwendung
	verbleiben mehr als 25 % Fehlerbudget in ihren SLOs.	identifizieren Sie, ob Services im Laufe der Zeit zuverlässig bleiben.

Risikotrends im Zeitverlauf

Liniendiagramme verfolgen die Anzahl der SLOs mit hohen Durchsatzraten und geringem Fehlerbudget, das in den letzten 12 Monaten verbleibt. Sie können sie verwenden, um wiederkehrende Muster und potenzielle Zuverlässigkeitsrisiken zu finden.

Diagramm	Was es ist	Verwendung
Hohe Durchsatzrate (>=1)	Zeigt die Anzahl der SLOs mit einer Durchsatzrate >= 1 im Zeitverlauf an. Eine hohe Durchsatzrate weist darauf hin, dass der mit dem SLO verknüpfte Service wahrscheinlich sein Fehlerbudget vor Ende des Compliance-Zeitraums verletzt. Wenn ein Service beispielsweise 30 Tage hat, um sein SLO zu erfüllen, sein Fehlerbudget jedoch innerhalb von 15 Tagen aufgebraucht wird, beträgt die Durchsatzrate 2.	• Erkennen Sie Risiken früh, indem Sie sehen, wann Services zu schnell Fehlerbudgets verbrauchen. • Identifizieren Sie neu auftretende oder wiederkehrende Zuverlässigkeitsprobleme, indem Sie die Durchsatzraten im Laufe der Zeit nachverfolgen. • Zeigen Sie auf das Diagramm, um die Anzahl und den Prozentsatz der SLOs mit einem hohen Durchsatz zu diesem Zeitpunkt anzuzeigen. • Wählen Sie das Diagramm aus, um SLO-Details anzuzeigen, einschließlich gemessener Zuverlässigkeit, Durchsatz und Prozentsatz des verbleibenden Fehlerbudgets.
Geringes verbleibendes Budget (<=25 %)	Zeigt die Anzahl der SLOs an, bei denen im Laufe der Zeit ein niedriges oder kein verbleibendes Fehlerbudget vorhanden ist.	• Überwachen Sie, wie viele Services sich nähern oder ihre SLOs verletzt haben. • Verfolgen Sie steigende Trends, die auf eine abnehmende Zuverlässigkeit oder wiederkehrende Probleme hinweisen können, die untersucht werden müssen. • Zeigen Sie auf das Diagramm, um die Anzahl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagramm	Was es ist	Verwendung
		und den Prozentsatz der SLOs anzuzeigen, deren Fehlerbudget zu diesem Zeitpunkt gering oder gar nicht verbleibt. • Wählen Sie das Diagramm aus, um SLO-Details anzuzeigen, den Zeitbereich anzupassen und auf zusätzliche Diagrammoptionen zuzugreifen.

Tabelle „Servicelevel-Ziele (SLOs)“

Die Tabelle „SLOs“ listet die in Service Reliability Management (SRM) definierten SLOs auf, und sie wird standardmäßig nach SLO-Namen sortiert. Verwenden Sie die Tabelle, um die allgemeine Zuverlässigkeit zu überwachen, gefährdete Services zu identifizieren und die zugewiesenen Teams zu finden.

Die SLO-Tabelle enthält standardmäßig die folgenden Spalten. Um die angezeigten Spalten anzupassen, wählen Sie das Zahnradsymbol aus.

- Name: Name des SLO. Sie können den Pfeil auswählen, um die Tabelle nach SLO-Namen zu sortieren, und den Namen auswählen, um den SLO-Datensatz anzuzeigen.
- Zuverlässigkeit: Aktueller Status des SLO. Zum Beispiel stabil, gefährdet oder kritisch.
- Gemessene Zuverlässigkeit: Prozentsatz, der die tatsächliche Leistung des Service anzeigt. Wenn Ihr SLO beispielsweise 99 % erfolgreich ist und die tatsächliche Leistung für den Monat 99 % beträgt, beträgt die gemessene Zuverlässigkeit 99 %.
- Ziel (Prozentsatz): Ziel-SLO-Wert.
- Durchsatz: Numerischer Wert, der angibt, wie schnell der Service sein Fehlerbudget verbraucht.
- % Verbleibendes Fehlerbudget: Prozentsatz des Fehlerbudgets, das im aktuellen Compliance-Zeitraum noch verfügbar ist.
- Service: Name des Service, der dem SLO zugeordnet ist. Sie können den Servicenamen auswählen, um den Servicedatensatz anzuzeigen.
- Zugewiesen: Team, das für den Service verantwortlich ist.

Dashboard-Filter und -Aktionen

Das Dashboard „Service Reliability“ wurde mit Platform Analytics erstellt und enthält Standard-Dashboard-Funktionen. Details zum Anpassen, Duplizieren oder Freigeben von Dashboards finden Sie unter Dashboards in Platform Analytics Dokumentation.

Hinweis: Änderungen am Dashboard „Service Reliability“ wirken sich auf alle SRM-Anwender in Ihrer Instanz aus. Um eine personalisierte Version zu erstellen, erstellen Sie entweder ein neues Dashboard, oder duplizieren Sie das vorhandene Dashboard, und bearbeiten Sie es. Weitere Informationen finden Sie in Dashboard mit dem Inline-Editor erstellen Und Duplizieren Sie A Platform Analytics Dashboard .

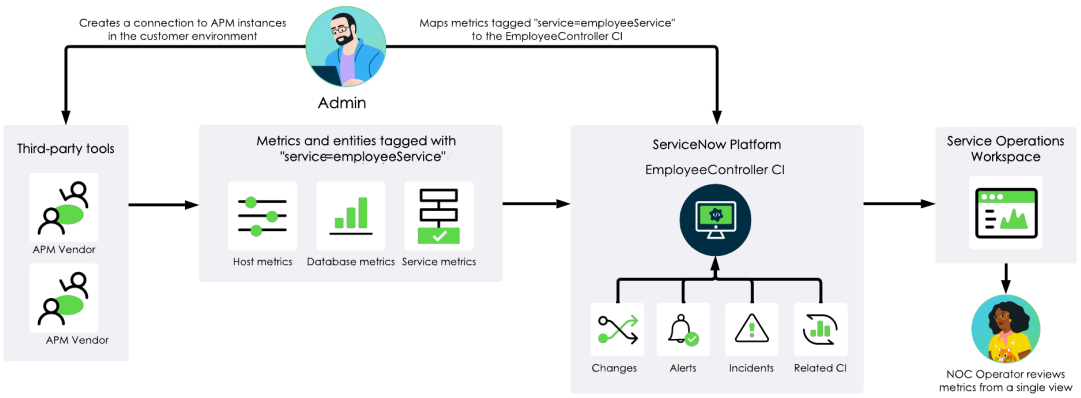
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Observability

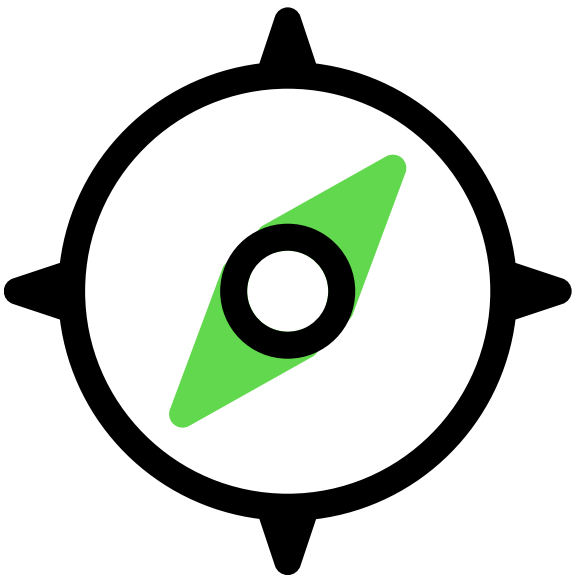
Die ServiceNow® Service-Observability Mit der Anwendung können Operatoren Incidents in einem komplexen und verteilten System selektieren und verwalten. Telemetrieinblicke in Anwendungen und Plattformen aus mehreren Erkennbarkeitstools werden zu einem zentralen Workflow kombiniert.

Übersicht über Service Observability



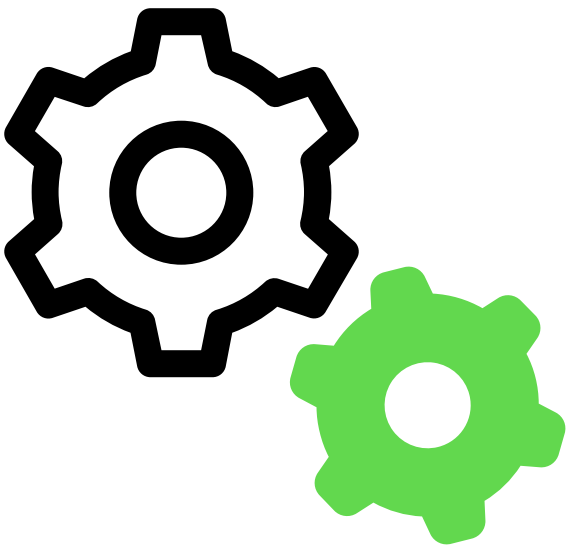
Erste Schritte

Untersuchen



Erfahren Sie, wie Service-Observability Bringt unterschiedliche Daten zusammen, damit Betreiber Probleme in Ihrem System finden können

Konfigurieren



Erfahren Sie, wie Sie installieren und konfigurieren Service-Observability

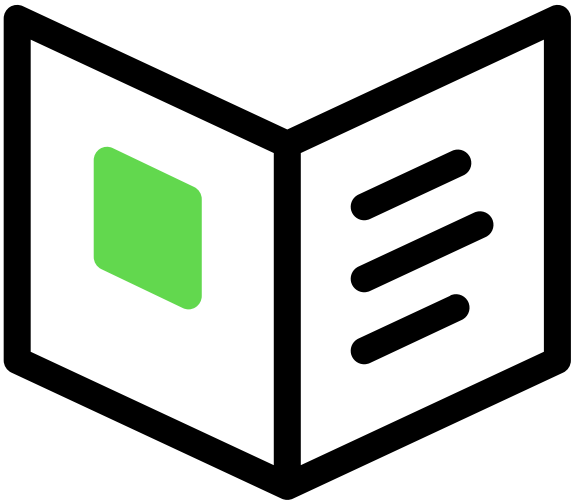
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen und untersuchen

Erfahren Sie, wie Sie die Quelle von Problemen finden und die Integrität von Services und zugehörigen Infrastrukturentitäten anzeigen können

Referenz



Suchen Sie Referenzinformationen zu Service-Observability

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow-Universität

Jetzt erstellen

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://www.servicenow.com

ServiceNow Store

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Store

Support

- https://support.servicenow.com/now
- Known Error-Portal

Service-Observability erkunden

Service-Observability Hilft Betriebsteams bei der Selektierung und Verwaltung von Incidents in einem komplexen und verteilten Produktionssystem. Es kombiniert die Telemetrie externer APM-Systeme (Application Performance Monitoring) mit zugehörigen Daten aus dem Configuration Management Database (CMDB) Und werden in einem einzelnen Workflow in angezeigt Service Operations-Arbeitsbereich(SOW).

Service-Observability – Übersicht

Service-Observability Zeigt Integritätsmetriken in an SOW Bezieht sich auf einen bestimmten Service. Metriken können aus einem externen APM-System erfasst und neben Informationen für zugehörige Konfigurationselemente in angezeigt werden CMDB.

Service-Observability Unterstützt die folgenden APM-Lieferanten:

- Amazon CloudWatch
- Datadog
- Dynatrace
- Microsoft Azure Überwachen
- New Relic
- SolarWinds Lokal
- Splunk Erkennbarkeit

Service-Observability Unterstützt die folgenden Datenbanken:

- MySQL
- PostgreSQL (nicht unterstützt mit Splunk)
- RDS (Relational Database Service) (Amazon CloudWatch)

Nachdem Sie eine APM-Instanz mit verbunden haben Service-Observability, Sie ordnen Services in zu CMDB Zu den APM-Metriken, die vorhandene Tags in den APM-Daten verwenden.

Mit dieser Datenzuordnung Service-Observability Kann Metriken aus APM-Entitäten anzeigen, die Ihrem Service zugeordnet sind, z. B. einem Host oder einer Datenbank, zusammen mit Informationen aus zugehörigen Konfigurationselementen (CIs). Betreiber verwenden die APM-Metriken, zugehörige CI-Informationen und hilfreiche Kontextinformationen, z. B. aktuelle Incidents und Warnungen im Zusammenhang mit dem Service, um die Integrität des Service zu verstehen.

Angenommen, Sie verwenden Dynatrace Zur Überwachung von `Zur Kasse` Service und Metriken aus Ihrer Datenbank und Ihrem Host verwenden das Tag `Checkout-Service` Um Anforderungen zu kennzeichnen, die von diesem Service stammen. Durch Zuordnung von `Zur Kasse` Service-CI für die APM-Daten, die mit gekennzeichnet sind `Checkout-Service`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

, Service-Observability Ruft Metriken für die Datenbanken, Hosts und CIs ab, die sich auf den Service beziehen, und zeigt sie dann zusammen an. Operatoren können Probleme bei Entitäten im Zusammenhang mit dem Service erkennen und den Minderungsprozess eingrenzen, ohne dass sie verlassen müssen SOW.

Service-Observability Anwender

Anwender

Anwender	Beschreibung
Systemadministrator	Nur Version 1,5. Systemadministratoren konfigurieren Anwender und Teams, registrieren zu überwachende Services und stellen eine Verbindung her Service-Observability In APMs und ordnen Sie diese Services dann diesen Daten zu. Sie können die Daten auch in anzeigen SOW
Service-Observability-Administrator	Version 1,6.x und höher. Service-Observability Administratoren können Anwender und Teams konfigurieren und eine Verbindung herstellen Service-Observability In APMs und ordnen Sie dann Services diesen Daten zu. Sie können die Daten auch in anzeigen SOW. Administratoren können auch Dashboard-Vorlagen anpassen, die zum Anzeigen von Metriken und zugehörigen Informationen verwendet werden.
Operator/ Vorgangsmanager **Hinweis:** Diese Anwender müssen zu gehören srm Gruppentyp, um alle Daten anzuzeigen.	Operatoren verwenden Service-Observability Beim Selektieren von Incidents in SOW. Sie können grundlegende Integritätsmetriken für einen Service zusammen mit zugehörigen Incidents, Warnungen und Changes anzeigen. Sie können detailliertere Informationen erhalten, indem Sie zu navigieren **Erkennbarkeit** Registerkarte zum Anzeigen zusätzlicher Servicemetriken zusammen mit Metriken aus zugehörigen Entitäten, z. B. einem Host oder einer Datenbank.

Service-Observability – Workflow

Administratoren konfigurieren Service-Observability Durch Registrierung von Services, Verbindung von APM-Metriken und anschließende Zuordnung der Services zu diesen Daten. Operatoren verwenden Service-Observability Um festzustellen, ob eine andere zugehörige Entität Probleme verursacht, die durch die Leistung des Service auftauchen.

Als Administrator:

1. Bestimmen Sie die Services, die überwacht werden sollen Service-Observability Basierend auf Geschäftsrelevanz.
2. Verbinden Sie vorhandene APM-Instanzen mit Service-Observability.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ordnen Sie Services APM-Metrikdaten basierend auf APM-basierten Tags zu, die für diese Daten verwendet werden.
4. Passen Sie die Vorlagen an, die zum Anzeigen von Metrikdiagrammen verwendet werden.

Als Operator oder Manager gehen Sie wie folgt vor:

1. Erkennen Sie ein Problem mit einem Service, während Sie in arbeiten SOW, Z. B. aus einer Warnung, dem Service-Dashboard oder Express-Liste, Navigieren Sie dann zur Seite „Servicedetails“.
2. Zeigen Sie allgemeine Integritätsmetriken für den Service zusammen mit zugehörigen Incidents, Warnungen und Changes an. Wenn eine der Metriken fehlerhaft erscheint, navigieren Sie zur Registerkarte „Observability“.
3. Zeigen Sie detailliertere Servicemetriken sowie Informationen aus zugehörigen Entitäten an, um die Ursachenuntersuchung zu starten. Wenn Sie feststellen, dass das Problem weiter unten im Stapel des Systems liegt, identifizieren Sie die Verantwortung für diese Entität, um mit der Korrektur zu beginnen.

Service-Observability – Vorteile

Vorteil	Funktion	Anwender
Zentralisieren Sie kritische Signale und überbrücken Sie Workflows, um die Agilität und Zuverlässigkeit zu erhöhen: • Verbinden Sie Daten von externen APMs • Ordnen Sie diese Daten zu CMDB Services • Zeigen Sie kombinierte Daten in an SOW	• Verbinden Sie einen Service-Observability Datenquelle • Erstellen und verwalten Sie Datenzuordnungen an.	Administratoren
Erhöhen Sie die Effizienz, und reduzieren Sie die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR), indem Sie kombinierte Metriken aus Entitäten anzeigen, die einem Service zugeordnet sind. Sie können damit beginnen, den Explosionsradius und den Besitz eines Incident zu bestimmen.	Zeigen Sie Serviceintegritätsmetriken an	Operatoren
Sehen Sie sich zugehörige Änderungen am System und Warnungen an, die einem Service zugeordnet sind, an einem Ort an.	Zeigen Sie die allgemeine Serviceintegrität an.	Operatoren
Passen Sie Dashboard-Vorlagen an.	Passen Sie Dashboard-Vorlagen für Service Observability an	Administratoren

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Service-Observability finden Sie unter:

- Service-Observability konfigurieren
- Zeigen Sie die allgemeine Serviceintegrität an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie Serviceintegritätsmetriken an
- Service-Observability – Referenz

Service-Observability konfigurieren

Nach der Installation Service-Observability, Sie müssen Services registrieren, externe APM-Instanzen (Application Performance Management) verbinden und diese APM-Daten diesen Services zuordnen.

Konfiguration – Übersicht

Service-Observability installieren

Wenn Sie die Systemadministratorrolle innehaben, können Sie installieren Service-Observability Anwendung (`sn_SOW_svcobs`). Die zugehörigen Anwendungsinstallationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfung des folgenden Elements: Service-Observability Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Systemadministrator [admin]

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Service-Observability installiert:

- Plugins
- Store-Anwendungen
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Mit Service-Observability installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Service-Observability Anwendung (`sn_SOW_svcobs`) Mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Teams und Services aktivieren

Führen Sie diesen Schritt nur aus, wenn Sie Version 1.5.0 von verwenden Service-Observability. Weisen Sie vorhandene Teams zu zu Service-Observability Damit sie die von zurückgegebenen Daten anzeigen können Configuration Management Database (CMDB) Auf diesen Seiten. Aktivieren Sie die -Services in CMDB Zur Verwendung in Service-Observability.

Vorbereitungen

- Anwender, die einer Gruppe zugewiesen sind, die die aktivierten Services verwaltet.
- Services, die Sie in überwachen möchten Service-Observability Muss in konfiguriert werden CMDB.

Erforderliche Rolle: Systemadministrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Führen Sie diesen Schritt nur aus, wenn Sie Version 1.5.0 von verwenden Service-Observability.

Teams werden in beiden verwendet Service Reliability Management Und Service-Observability Um vorhandenen Rollen und Gruppen die Möglichkeit zur Anzeige zu geben CMDB Daten in **Übersicht** Und **Erkennbarkeit** Registerkarten.

Die Services, die Sie in überwachen möchten Service-Observability Muss aktiviert sein. Mit der Aktivierung können Sie diesem Service Daten aus einer APM-Instanz (Application Performance Management) zuordnen und dann die zugehörigen Daten dieses Service in anzeigen **Übersicht** Und **Erkennbarkeit** Registerkarten.

Hinweis: Teams und Services für aktiviert Service-Observability Sind auch für aktiviert Service Reliability Management(SRM). Service-Observability Administratoren können einen einzelnen Service erstellen. Weitere Informationen finden Sie unter Services zu SRM hinzufügen. Wenn Service-Observability Administratoren erstellen einen einzelnen Service, für den er automatisch aktiviert wird Service-Observability Und SRM. Weitere Informationen finden Sie unter Service Reliability Management.

Prozedur

1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen** Und wählen Sie aus **Service Operations-Management** Karte.
2. Navigieren zu **Servicebetriebsmanagement** > **Zuweisen und aktivieren** > **Teams und Services aktivieren**an.
3. Wählen Sie Aus **Aktivieren Sie Teams und Services** .
4. Wählen Sie die Zuweisungsgruppen aus, die Sie als Teams in verwenden möchten Service-Observability Und wählen Sie dann aus **Aktivieren** .
   Nur Teams, die noch nicht zugewiesen wurden, werden angezeigt.
5. Wählen Sie im Modal die Option aus **Bestätigen** .
6. Wählen Sie im Dropdown-Menü Serviceklasse eine aus CMDB Servicetyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie in der Liste der Services aus, für welche Services aktiviert werden sollen Service-Observability Und wählen Sie aus **Aktivieren** .
8. Wählen Sie im Modal ein Supportteam für die Services aus, und wählen Sie aus **Bestätigen** .
   Sie haben jetzt Services, die in überwacht werden können Service-Observability

Nächste Maßnahme

1. Verbinden Sie einen Service-Observability Datenquelle
2. Erstellen und verwalten Sie Datenzuordnungen

Verbinden Sie einen Service-Observability Datenquelle

Verbinden Service-Observability An eine externe APM-Instanz (Application Performance Management). Service-Observability Zeigt Metriken in an Service Operations-Arbeitsbereich(SOW) Aus dieser APM-Instanz.

Vorbereitungen

Sie müssen eine Verbindungs-URL und Anmeldeinformationen für Ihren APM-Lieferanten eingeben. Sie können entweder eine vorhandene Verbindung verwenden oder eine erstellen. Beachten Sie Folgendes für bestimmte Lieferanten:

Lieferantenspezifische Verbindungsinformationen

APM-Lieferant	Verbindungsinformation
AWS	Die Verbindungs-URL muss für die zu überwachende Region spezifisch sein, z. B. `https://monitoring.us-east-2.amazonaws.com` .
Azure	Die Verbindungs-URL muss sein `https://management.azure.com` .
Splunk Erkennbarkeit	Die Verbindungs-URL muss die Realm enthalten, z. B. https://stream.[REALM].signalfx.com

Wenn Sie vorhandene Anmeldeinformationen verwenden, benötigen Sie den Anmeldeinformationsnamen. Wenn Sie Anmeldeinformationen erstellen, erfassen Sie die folgenden Informationen.

Lieferantenspezifische Anmeldeinformationsanforderungen

APM-Lieferant	Anmeldeinformationstyp	Informationen erforderlich
Azure	OAuth 2.0	• OAuth-Client-ID • Geheimer OAuth-Client • OAuth-Token-URL • Abonnement-ID
AWS	AWS-Anmeldeinformationen	• Zugriffsschlüssel • Geheimer Schlüssel

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lieferantenspezifische Anmeldeinformationsanforderungen (Fortsetzung)

APM-Lieferant	Anmeldeinformationstyp	Informationen erforderlich
		Wenn der diesem Schlüssel zugeordnete Anwender auf bestimmte Berechtigungen beschränkt ist, muss er Folgendes enthalten, das für alle Ressourcen gilt: • cloudwatch:beschreiben Umfasst alle Ressourcen • cloudwatch:Abrufen Umfasst alle Ressourcen • cloudwatch:Liste Umfasst alle Ressourcen • Cloudtrail: Suchereignisse • Tag: Ressourcen abrufen • Tag: GetTagKeys • Tag: GetTagWerte • Apig:Get
Datadog	API	• API Key • Anwendungsschlüssel Wenn ein Anwendungsschlüssel auf einen bestimmten Umfang beschränkt ist, sind diese Bereiche für die folgenden Endpunkte erforderlich: • https://api.datadoghq.com/api/v2/catalog/entity • https://api.datadoghq.com/api/v1/hosts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lieferantenspezifische Anmeldeinformationsanforderungen (Fortsetzung)

APM-Lieferant	Anmeldeinformationstyp	Informationen erforderlich
		• https://api.datadoghq.com/api/v1/query • https://api.datadoghq.com/api/v2/query/timeseries
Dynatrace	API	API Key Der API-Schlüssel muss haben Entitäten lesen Und Metriken lesen Bereichsberechtigungen.
New Relic	API	• Account-ID • API Key
SolarWinds	Basisauth.	• Anwendername der Anmeldeinformationen für Standardauthentifizierung • Passwort für Anmeldeinformationen für Standardauthentifizierung • Der Name des MID-Servers, auf dem Ihre SolarWinds-Instanz gehostet wird
Splunk Erkennbarkeit	API	Zugriffstoken

Erforderliche Rolle: sn_SOW_svcobs.admin

Warum und wann dieser Vorgang ausgeführt wird

Der erste Schritt zur Erfassung von APM-Daten besteht in der Erstellung einer Verbindung mit der APM-Instanz.

Service-Observability Unterstützt die folgenden APM-Lieferanten:

- Amazon CloudWatch
- Datadog
- Dynatrace
- Microsoft Azure Überwachen
- New Relic
- SolarWinds Lokal
- Splunk Erkennbarkeit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie basierend auf Ihrer Version von Service-Observability.
   - Version 1,5.0: Navigieren Sie zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen**, Navigieren Sie dann zu **Service Observability Management** > **Observability Verwalten** > **Datenquellen**
   - Version 1,6 oder höher: Navigieren Sie zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen**, Navigieren Sie dann zu **Service Observability Datenquellen** .
2. Wählen Sie Ihren APM-Lieferanten aus.
3. Auf der **Verbindung hinzufügen** Füllen Sie die Felder aus.
   Sie können eine vorhandene HTTP- oder HTTPS-Verbindung und vorhandene API-Schlüssel-Anmeldeinformationen verwenden oder erstellen.
4. Wählen Sie **Speichern**.

Ergebnis

Eine neue Verbindung wird in der Liste der Observability-Datenquellen angezeigt. Sie verwenden diese Verbindung, wenn Sie eine Datenzuordnung erstellen.

Nächste Maßnahme

Ordnen Sie Ihre Verbindung den Services zu, die Sie in überwachen möchten Service-Observability. Weitere Informationen finden Sie unter Erstellen und verwalten Sie Datenzuordnungen.

Erstellen und verwalten Sie Datenzuordnungen

Ordnen Sie Ihre Services den Daten einer verbundenen APM-Instanz (APM) zu, und zeigen Sie sie in Diagrammen für den Service und die zugehörigen Entitäten an.

Vorbereitungen

- Wenn Sie Version 1,5 verwenden, aktivieren Sie die Services, die Daten aus einer externen APM-Instanz enthalten. Anweisungen zum Aktivieren der Services finden Sie unter Teams und Services aktivieren. Für spätere Versionen müssen Sie Services nicht aktivieren. Sie können einen der folgenden Servicetypen zuordnen:
  - Anwendung
  - Zugeordnete Anwendung
  - Berechnete Anwendung
  - Dynamische CI-Gruppe
  - Technisch
  - Tag-basiert
  - Serviceangebote
  - Geschäftsservices
- Verbinden Sie einen Service-Observability Datenquelle

Erforderliche Rolle: sn_SOW_svcobs.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein Servicekonfigurationselement (CI) bestimmten Tag-Schlüssel-Wert-Paaren aus den APM-Metrikmetadaten zuordnen, Service-Observability Zeigt alle Metriken mit diesen Tags im Kontext dieses Service an. Diese Metriken sind nach den folgenden Entitätstypen gruppiert:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwendungsmetriken: Metriken, die dem ausgewählten Service zugeordnet sind
- Metriken berechnen: Metriken, die den Hosts zugeordnet sind, auf denen der Service ausgeführt wird
- Datenbanken: Metriken, die den vom Service verwendeten Datenbanken zugeordnet sind

Angenommen, Sie haben Metriken von New Relic Die zur Überwachung von Services, Datenbanken und Hosts verwendet werden. Für diese Metriken haben Sie das Tag verwendet Service_Name . Angenommen, Sie haben auch zugeordnet Zur Kasse Service-CI für das Schlüssel-/Wert-Paar der APM-Metadaten Service_Name = zur Kasse . Service-Observability Zeigt alle mit getaggten Datenbank- und Host-Metriken an Service_Name = zur Kasse Im Kontext von Zur Kasse Service-CI.

Wenn einige Ihrer Metriken für verschiedene Entitäten einen anderen Schlüsselnamen oder einen anderen Schlüsselwert verwenden, können Sie Ausnahmen erstellen. Beispiel: Wenn Ihre Host-Metriken verwenden Service Anstelle von Service_Name , Sie können eine Ausnahme erstellen, um diese Metriken einzubeziehen.

Jeder Entitätstyp hat ein eigenes Dashboard, und jede Metrik und jedes zugehörige CI hat ein eigenes Standarddiagramm. Sie können die für die Dashboards und Diagramme verwendeten Vorlagen anpassen. Weitere Informationen finden Sie unter Passen Sie Dashboard-Vorlagen für Service Observability an.

Hinweis: Um zu verstehen, wie Service-Observability Erstellt diese Zuordnungen, siehe APM-Lieferantenentitätszuordnungen für Service-Observability.

Eine Beschreibung der Feldwerte finden Sie unter Service-Observability Formular „Datenzuordnung“.

Prozedur

1. Navigieren Sie zur Seite „Datenzuordnungen“, und befolgen Sie die Verfahren für Ihre Version von Service-Observability.
   - Version 1,5.0: Navigieren Sie zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen**, Navigieren Sie dann zu **Service Observability Management** > **Observability Verwalten** > **Datenzuordnungen**
   - Version 1,6.x oder höher: Navigieren Sie zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen**, Navigieren Sie dann zu **Service-Observability** > **Datenzuordnungen**an.
2. Wählen Sie Aus **Erstellen Sie Ihre erste Zuordnung** Oder **Erstellen Sie eine Zuordnung** .
3. Geben Sie auf der Seite „Observability-Datenzuordnung“ einen Namen für die Zuordnung ein.
4. Wählen Sie die Services aus, die diese Zuordnung verwenden sollen.
   - Für Version 1,5.0: Geben Sie die Namen der aktivierten Services ein, die Sie zuordnen möchten. Informationen zum Aktivieren von Services finden Sie unter Teams und Services aktivieren
   - Für Version 1,6.x und höher:
     a. Wählen Sie Aus **Wählen Sie Services aus** .
     b. Verwenden Sie die Navigation, um die Liste auf den Typ des Services einzugrenzen, nach dem Sie suchen.
     c. Wählen Sie die Services aus, die der Zuordnung hinzugefügt werden sollen. Sie können Services aus einer beliebigen Kombination von Servicetypen hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie den Filter, um die Serviceliste einzugrenzen.

d. Wählen Sie Aus **Fügen Sie Services hinzu** Um sie der Zuordnung hinzuzufügen.

5. Erstellen Sie eine Regel, um zu bestimmen, wie Service-Observability Sollte den APM-Entitäten Services mithilfe von Tag-Schlüsseln und -Werten zuordnen.

   a. Wählen Sie die Datenquelle für diese Zuordnung aus.

   b. Geben Sie den Tag-Schlüssel ein, den Sie dem aktivierten Service zuordnen möchten.
   Der Schlüssel kann ein beliebiges Tag sein, das Sie beispielsweise für Ihre APM-Metadaten verwenden `Service` .

   Hinweis: Wenn Sie mehr als ein Tag zur Darstellung eines Service verwenden, können Sie eine Ausnahme erstellen. Beispiel: Wenn die meisten Tags verwenden `Service_Name` Mit Ausnahme von Datenbankmetriken, die verwenden `Service` , Sie können eine Ausnahme für die Datenbankmetriken erstellen.

   c. Geben Sie einen Tag-Wert ein.
   Werte können Zeichenfolgen sein, die Felder im CI für den Service darstellen.

   Sie können jetzt Ihre Zuordnung testen oder Ausnahmen hinzufügen.

6. **Wahlweise:** Wenn einige Ihrer Entitäten andere Schlüsselnamen oder -Werte verwenden, erstellen Sie Ausnahmen zur Standardrichtlinie, indem Sie sie auf der Karte „Ausnahmen“ konfigurieren.

7. Wählen Sie Aus **Speichern Sie die Zuordnung** .

Ergebnis

Auf der **Erkennbarkeit** Auf der Registerkarte „Servicedetails“ werden Dashboards und Diagramme für die in der Zuordnung gefundenen Entitäten angezeigt.

Passen Sie Dashboard-Vorlagen für Service Observability an

Sie können die Service Observability-Dashboards sowohl auf den Registerkarten Übersicht als auch Observability der Seite „Servicedetails“ anpassen. Sie können Metriken und zugehörige Daten ändern oder hinzufügen, um sie Ihren Geschäftsanforderungen anzupassen.

Service-Observability Dashboards werden mit Vorlagen erstellt, die für jeden APM-Lieferanten (Application Performance Monitor) und die Entitätsregisterkarte spezifisch sind. Sie werden mit erstellt Platform Analytics, Mit dem Sie Vorlagen an Ihre Geschäftsanforderungen anpassen können. Beispielsweise möchten Sie Metriken Ihres APM-Lieferanten anzeigen, die standardmäßig nicht verfügbar sind.

Die Service-Observability Dashboards verwenden APM-spezifische Vorlagen. Aus dem jeweiligen Referenzthema können Sie sehen, was jede Vorlage standardmäßig anzeigt.

- Amazon CloudWatch Vorlagen für Service-Observability
- Azure Vorlagen für überwachen Service-Observability
- Datadog Vorlagen für Service-Observability
- Dynatrace Vorlagen für Service-Observability
- New Relic Vorlagen für Service-Observability

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- SolarWinds Vorlagen für Service-Observability
- Splunk Vorlagen für Service-Observability

Hinweis: Wenn Sie eine Anpassung vornehmen, ändern Sie die Vorlage und nicht das Dashboard des einzelnen Service. Dies bedeutet, dass Dashboards für alle Services, die auch dieselbe Datenquelle verwenden, ebenfalls geändert werden.

Neben APM-Daten können Sie auch Diagramme für Daten aus hinzufügen ServiceNow Tabellen und auch aus Daten, die in gespeichert sind MetricBase Anwendung.

Wenn Sie eine Vorlage anpassen, wird eine Kopie des Originals gespeichert, damit Sie sie bei Bedarf erneut implementieren können. Standard-Dashboards zeigen an Zertifiziert Tag.

APM-Abfragen für ein Diagramm werden erstellt

Wenn Sie ein Diagramm in einem Dashboard bearbeiten oder hinzufügen, verwenden Sie die Seite „Datenquelle bearbeiten“ von Platform Analytics Dient zum Erstellen einer Abfrage. Sie können den integrierten Abfrageeditor für einfache Metrikabfragen verwenden, oder Sie können den erweiterten Modus verwenden, um eine aus einem Diagramm kopierte Abfrage in Ihre APM-Lieferanteninstanz einzufügen.

Service-Observability Dashboards sind auf den Service ausgerichtet, der derzeit auf der Seite „Servicedetails“ angezeigt wird. Wenn Sie eine einzelne Abfrage für mehrere Services und Entitäten und einen beliebigen Zeitbereich verwenden möchten, können Sie hartcodierte Werte durch ersetzen Service-Observability Vorlagenvariablen .

Hinzufügen ServiceNow Tabellen

Sie können Daten aus einbeziehen ServiceNow Problemdatensätze und Geschäftsanwendungsdatensätze für Dashboards, und die Daten werden für den ausgewählten Service festgelegt.

Hinzufügen MetricBase Datendiagramme

Sie können Diagramme basierend auf Daten hinzufügen, die in gespeichert sind MetricBase Anwendung. Die Daten sind auf den ausgewählten Service beschränkt.

Bearbeiten Sie APM-Datendiagramme in Dashboard-Vorlagen für Service Observability

Bearbeiten Service-Observability Dashboard-Vorlagen, wenn Sie verschiedene Metriken Ihres APM-Lieferanten (Application Performance Monitoring) auf den Registerkarten Übersicht oder Observability in APM-basierten Diagrammen anzeigen möchten.

Warum und wann dieser Vorgang ausgeführt wird
Beim Erstellen eines APM-Diagramms können Sie den Abfragegenerator verwenden, um einfache Abfragen zu erstellen, oder den erweiterten Modus verwenden, um umfangreichere Abfragen zu erstellen.

Mit einfachen Abfragen können Sie im Allgemeinen Metriken abfragen, die den Entitäten zugeordnet sind, für die Metriken angezeigt werden: Services, Hosts und Datenbanken. Die zurückgegebenen Metriken werden über das vom Anwender festgelegte Zeitfenster zusammengefasst.

Mit dem erweiterten Abfragemodus können Sie Abfragen aus vorhandenen APM-Diagrammen ausschneiden und in einfügen Service-Observability. Für die meisten APM-Lieferanten können Sie einfach eine Abfrage aus einem vorhandenen Diagramm in Ihrer APM-Instanz kopieren. Beides jedoch Amazon CloudWatch Und Microsoft Azure Verwendung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bestimmter JSON-Objekte erforderlich. Weitere Informationen finden Sie unter APM-Lieferantenentitätszuordnungen für Service-Observability.

Beide Abfragetypen werden unterstützt Vorlagenvariablen Mit denen Sie dieselbe Abfrage verwenden können, um Metriken für mehrere Entitätsinstanzen zurückzugeben.

Vorbereitungen

Erforderliche Rolle: sn_SOW_svcobs.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
   Sie können auf die Seite „Servicedetails“ von diesen Seiten in zugreifen SOW:
   - **Services** Liste: Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard** : Wählen Sie einen Service im Dashboard aus, und wählen Sie aus **Servicedetails** .
   - **Liste** : Navigieren Sie zu **Anwendungsservices** > **Services** Und wählen Sie einen Service aus.
   - **Express-Liste** Warnung: Wählen Sie einen Service aus **Betroffene Services** Spalte.

   Die Seite „Servicedetails“ wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Informationen zu Fehlermeldungen in Diagrammen finden Sie unter Diagrammfehler status.
2. Öffnen Sie die Vorlage im Bearbeitungsmodus.
   - Wenn Sie eine zertifizierte Vorlage bearbeiten, wählen Sie aus **Duplikat** .
   - Wenn Sie eine anwenderdefinierte Vorlage bearbeiten, wählen Sie aus **Bearbeiten** .

   Hinweis: Durch das Duplizieren einer zertifizierten Vorlage können Sie sie nicht überschreiben, und Sie können sie bei Bedarf auch neu installieren.

   Das neue Dashboard trägt den Namen – Kopieren Angehängt. Verwenden Sie das Bleistiftsymbol, um den Namen des Dashboards zu ändern.
3. Befolgen Sie die Anweisungen für , um grundlegende Bearbeitungen durchzuführen, z. B. das Neuanordnen, Ändern der Größe oder Löschen von Diagrammen Bearbeiten Sie Inline Platform Analytics Dashboard-Elemente .
4. Führen Sie die folgenden Schritte aus, um eine APM-Abfrage für ein neues Diagramm hinzuzufügen:

   a. Wählen Sie im Bearbeitungsmodus aus **Fügen Sie ein neues Element hinzu** Und wählen Sie aus **Datenvisualisierung** .

   b. In **Datenquelle hinzufügen** Seite, navigieren Sie zu **Service Observability** Und wählen Sie Ihren APM-Lieferanten aus.
   Stellen Sie sicher, dass Sie denselben APM-Lieferanten auswählen, der für die Vorlage verwendet wird, die Sie bearbeiten.

   c. Geben Sie eine Abfrage in ein **Metrik** Karte.

   Verwenden Sie den Abfragegenerator, um eine einfache APM-spezifische Abfrage zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine vollständige Abfrage aus Ihrem APM-Lieferantendiagramm zu kopieren, aktivieren Sie **Erweitert** Wechseln und fügen Sie eine Abfrage aus Ihrem APM-Lieferantendiagramm ein.

Für AWS und Azure können Sie ausgewählte Diagramme aus einem vorhandenen Dashboard importieren, anstatt eine Abfrage im erweiterten Modus einzugeben. Wählen Sie Aus **Import aus AWS/Azure-Dashboard** . Wählen Sie einen Datenquellennamen aus, wählen Sie dann ein Dashboard aus, wählen Sie in der Liste der Diagramme das zu importierende Dashboard aus, und wählen Sie dann aus **Importabfrage** . Die Abfrage für das Diagramm wird in das Feld „Abfrage“ eingefügt.

Hinweis: Sie können eine Abfrage auch manuell aus AWS oder Azure kopieren und einfügen, indem Sie die in beschriebenen Verfahren befolgen Erweiterte Abfrageunterstützung für AWS und Azure.

Verwenden Vorlagenvariablen Um hartcodierte Entitäten oder Zeiträume zu ersetzen, damit die Abfrage Ergebnisse zurückgibt, die sowohl dem in der Anwenderoberfläche ausgewählten Service als auch dem Zeitraum entsprechen.

Hinweis: Verwenden Sie **Dokumente** Link, um Hilfe beim Erstellen der Abfrage in der APM-spezifischen Dokumentation zu finden.

d. Um eine Vorschau Ihrer Abfrage anzuzeigen, wählen Sie aus **Ausführen** Und wählen Sie dann einen Service und eine Entität aus.

e. Wenn Sie mit Ihrer Abfrage zufrieden sind, wählen Sie aus **Fügen Sie diese Quelle hinzu** Um das Diagramm der Vorlage hinzuzufügen.

5. Um eine vorhandene Abfrage zu bearbeiten, führen Sie die folgenden Schritte aus.

a. Wählen Sie im Bearbeitungsmodus das zu bearbeitende Diagramm aus.

b. In **Datenquellen** Abschnitt des Konfigurationsbereichs verwenden **Weitere Aktionen** Menü zum Auswählen **Bearbeiten** .

c. In **Bearbeiten Sie die Datenquelle** Seite bearbeiten Sie die Abfrage in **Metrik** Karte.

Verwenden Sie den Abfragegenerator, um eine einfache APM-spezifische Abfrage zu erstellen.

Um eine vollständige Abfrage aus Ihrem APM-Lieferantendiagramm zu kopieren, aktivieren Sie **Erweitert** Wechseln und fügen Sie eine Abfrage aus Ihrem APM-Lieferantendiagramm ein.

Für AWS und Azure können Sie ausgewählte Diagramme aus einem vorhandenen Dashboard importieren, anstatt eine Abfrage im erweiterten Modus einzugeben. Wählen Sie Aus **Import aus AWS/Azure-Dashboard** . Wählen Sie einen Datenquellennamen aus, wählen Sie dann ein Dashboard aus, wählen Sie in der Liste der Diagramme das zu importierende Dashboard aus, und wählen Sie dann aus **Importabfrage** . Die Abfrage für das Diagramm wird in das Feld „Abfrage“ eingefügt.

Hinweis: Sie können eine Abfrage auch manuell aus AWS oder Azure kopieren und einfügen, indem Sie die in beschriebenen Verfahren befolgen Erweiterte Abfrageunterstützung für AWS und Azure.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Vorlagenvariablen Zum Ersetzen hartcodierter Entitäten oder Zeiträume.

Hinweis: Verwenden Sie **Dokumente** Link, um Hilfe beim Erstellen der Abfrage in der APM-spezifischen Dokumentation zu finden.

d. Um eine Vorschau Ihrer Abfrage anzuzeigen, wählen Sie einen Service und eine Entität aus, und wählen Sie aus **Ausführen** .

e. Wenn Sie mit Ihrer Abfrage zufrieden sind, wählen Sie aus **Anwenden** Um das Diagramm der Vorlage hinzuzufügen.

6. Wenn Sie mit der Anpassung fertig sind, wählen Sie aus **Speichern** Und dann **Bearbeitungsmodus beenden.**
7. Um die Vorlage auf die Standardversion (zertifiziert) zurückzusetzen, wählen Sie aus **Bearbeiten** Und verwenden **Weitere Aktionen** Menü zum Auswählen **Zurück zu „zertifiziert“** .

Bearbeiten ServiceNow Daten zu Dashboard-Vorlagen für Service Observability

Bearbeiten Service-Observability Dashboard-Vorlagen, wenn Sie verschiedene Daten aus anzeigen möchten ServiceNow Daten aus Problemdatensätzen und Business-App-Datensätzen zu Dashboards auf den Registerkarten „Übersicht“ oder „Observability“.

Vorbereitungen

Erforderliche Rolle: sn_SOW_svcobs.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
   Sie können auf die Seite „Servicedetails“ von diesen Seiten in zugreifen SOW:
   - **Services** Liste: Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard** : Wählen Sie einen Service im Dashboard aus, und wählen Sie aus **Servicedetails** .
   - **Liste** : Navigieren Sie zu **Anwendungsservices** > **Services** Und wählen Sie einen Service aus.
   - **Express-Liste** Warnung: Wählen Sie einen Service aus **Betroffene Services** Spalte.

   Die Seite „Servicedetails“ wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Informationen zu Fehlermeldungen in Diagrammen finden Sie unter Diagrammfehler status.
2. Öffnen Sie die Vorlage im Bearbeitungsmodus.
   - Wenn Sie eine zertifizierte Vorlage bearbeiten, wählen Sie aus **Duplikat** .
   - Wenn Sie eine anwenderdefinierte Vorlage bearbeiten, wählen Sie aus **Bearbeiten** .

   Hinweis: Durch das Duplizieren einer zertifizierten Vorlage können Sie sie nicht überschreiben, und Sie können sie bei Bedarf auch neu installieren.

   Das neue Dashboard trägt den Namen – Kopieren Angehängt. Verwenden Sie das Bleistiftsymbol, um den Namen des Dashboards zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Befolgen Sie die Anweisungen für , um grundlegende Bearbeitungen durchzuführen, z. B. das Neuanordnen, Ändern der Größe oder Löschen von Diagrammen Bearbeiten Sie Inline Platform Analytics Dashboard-Elemente .
4. Um eine neue hinzuzufügen ServiceNow Führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Bearbeitungsmodus aus **Fügen Sie ein neues Element hinzu** Und wählen Sie aus **Liste: Einfach** .
   b. In **Daten** Abschnitt des Konfigurationsbereichs verwenden **Tabelle** Feld zum Auswählen der Tabelle, deren Daten Sie anzeigen möchten.
   c. In **Standardanzeige** Fügen Sie die anzuzeigenden Spalten hinzu, und ordnen Sie sie an.
5. Um ein vorhandenes Diagramm zu bearbeiten, führen Sie die folgenden Schritte aus.
   a. Wählen Sie im Bearbeitungsmodus das zu bearbeitende Diagramm aus.
   b. In **Daten** Überprüfen Sie im Abschnitt „Konfiguration“, ob die richtige Tabelle in ausgewählt ist **Tabelle** Feld.
   c. In **Standardanzeige** Fügen Sie die anzuzeigenden Spalten hinzu, und ordnen Sie sie an.
6. Wenn Sie mit der Anpassung fertig sind, wählen Sie aus **Speichern** Und dann **Bearbeitungsmodus beenden.**
7. Um die Vorlage auf die Standardversion (zertifiziert) zurückzusetzen, wählen Sie aus **Bearbeiten** Und verwenden **Weitere Aktionen** Menü zum Auswählen **Zurück zu „zertifiziert“** .

Hinzufügen MetricBase Diagramme zu Dashboard-Vorlagen für Service Observability

Hinzufügen MetricBase Daten, für die Diagramme erstellt werden sollen Service-Observability Dashboard-Vorlagen, wenn Sie diese Metriken im Kontext von anzeigen möchten Service-Observability.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Metriken hinzufügen, die in gespeichert sind MetricBase Anwendung An Ihren Service-Observability Dashboards. Diese Diagramme werden mit Daten angezeigt, die auf den ausgewählten Service ausgerichtet sind.

Vorbereitungen

Erforderliche Rolle: sn_SOW_svcobs.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
   Sie können auf die Seite „Servicedetails“ von diesen Seiten in zugreifen SOW:
   - **Services** Liste: Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard** : Wählen Sie einen Service im Dashboard aus, und wählen Sie aus **Servicedetails** .
   - **Liste** : Navigieren Sie zu **Anwendungsservices** > **Services** Und wählen Sie einen Service aus.
   - **Express-Liste** Warnung: Wählen Sie einen Service aus **Betroffene Services** Spalte.

   Die Seite „Servicedetails“ wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Informationen zu Fehlermeldungen in Diagrammen finden Sie unter Diagrammfehler status.
2. Öffnen Sie die Vorlage im Bearbeitungsmodus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine zertifizierte Vorlage bearbeiten, wählen Sie aus **Duplikat** .
- Wenn Sie eine anwenderdefinierte Vorlage bearbeiten, wählen Sie aus **Bearbeiten** .

Hinweis: Durch das Duplizieren einer zertifizierten Vorlage können Sie sie nicht überschreiben, und Sie können sie bei Bedarf auch neu installieren.

Das neue Dashboard trägt den Namen – Kopieren Angehängt. Verwenden Sie das Bleistiftsymbol, um den Namen des Dashboards zu ändern.

3. Befolgen Sie die Anweisungen für , um grundlegende Bearbeitungen durchzuführen, z. B. das Neuanordnen, Ändern der Größe oder Löschen von Diagrammen Bearbeiten Sie Inline Platform Analytics Dashboard-Elemente .
4. Um ein neues Diagramm mit hinzuzufügen MetricBase Führen Sie die folgenden Schritte aus:
   a. Wählen Sie im Bearbeitungsmodus aus **Fügen Sie ein neues Element hinzu** Und wählen Sie aus **Datenvisualisierung** , Wählen Sie aus **Neue Visualisierung** , Und wählen Sie dann aus **Position** .
   b. In **Datenquellen** Wählen Sie im Abschnitt „Konfiguration“ aus **Datenquelle hinzufügen** .
   c. In **Datenquelle hinzufügen** Seite, navigieren Sie zu **MetricBase** , Wählen Sie die anzuzeigenden Daten aus, und wählen Sie dann aus **Fügen Sie diese Quelle hinzu** .
   d. Verwenden Sie die Steuerungen in **Daten** Abschnitt des Konfigurationsbereichs, um die Metrik auszuwählen und die Abfrage zu konfigurieren.
5. Wenn Sie mit der Anpassung fertig sind, wählen Sie aus **Speichern** Und dann **Bearbeitungsmodus beenden.**
6. Um die Vorlage auf die Standardversion (zertifiziert) zurückzusetzen, wählen Sie aus **Bearbeiten** Und verwenden **Weitere Aktionen** Menü zum Auswählen **Zurück zu „zertifiziert“** .

Services überwachen und Probleme untersuchen

Operatoren verwenden Service-Observability Dient zur Überwachung der Integrität ihrer Services und zur Selektierung und Verwaltung von Incidents. Sie können Leistungsmetriken aus externen APM-Systemen (Application Performance Management) im Kontext eines Anwendungsservice und der zugehörigen CIs anzeigen.

Übersicht über die Verwendung Service-Observability

Service-Observability Kann Metriken aus einer APM-Instanz im Kontext eines Service anzeigen. Zusammen mit Metriken für den Service und Informationen zu zugehörigen CIs, Service-Observability Kann Entitäten im Zusammenhang mit dem Service ableiten, z. B. einen Host oder eine Datenbank, und ihre Metriken anzeigen. Diese Funktionalität bietet einem Betreiber einen ganzheitlicheren Überblick darüber, was sich auf die Leistung auswirken könnte.

Die **Übersicht** Auf der Registerkarte „Servicedetails“ werden allgemeine Leistungsmetriken für den Service und andere kontextbezogene Informationen wie offene Warnungen oder Incidents angezeigt, die sich auf den Service auswirken. Die **Erkennbarkeit** Auf der Registerkarte werden detailliertere Metriken aus dem APM für den Service zusammen mit Metriken für abgeleitete Entitäten angezeigt, die durch Datenzuordnungen gefunden werden, die während des Setups konfiguriert wurden. Außerdem werden Informationen zu CIs angezeigt, die sich auf diese abgeleiteten Entitäten beziehen. Anstatt zu einem externen Tool wechseln zu müssen, kann ein Operator diese externen Metriken im Kontext von anzeigen Service Operations-Arbeitsbereich(SOW).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die allgemeine Serviceintegrität an

  In **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW, Zeigen Sie die allgemeine Serviceintegrität und zugehörige Informationen wie Warnungen und Changes an.

- Zeigen Sie Serviceintegritätsmetriken an

  In **Erkennbarkeit** Auf der Registerkarte können Sie detailliertere Servicemetriken sowie Metriken aus zugehörigen von APM überwachten Entitäten wie Datenbanken und Hosts anzeigen.

Zeigen Sie die allgemeine Serviceintegrität an

Zeigen Sie die allgemeine Serviceintegrität und zugehörige Ereignisse wie Warnungen und Changes mit an **Übersicht** Registerkarte auf der Seite „Servicedetails“ in SOW.

Vorbereitungen

- Für Version 1,5 muss ein Service aktiviert sein. Weitere Informationen finden Sie unter Teams und Services aktivieren.
- Eine Datenzuordnung muss konfiguriert werden. Weitere Informationen finden Sie unter Erstellen und verwalten Sie Datenzuordnungen.

Erforderliche Rolle: Operator [snc_SOW_svcobs.Manager]

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie benachrichtigt wurden, dass bei einem Service Leistungsprobleme auftreten, können Sie Ihre Untersuchung mit beginnen **Übersicht** Registerkarte auf der Seite „Servicedetails“.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
   Sie können auf die Seite „Servicedetails“ von diesen Seiten in zugreifen SOW:
   - **Services** Liste: Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard** : Wählen Sie einen Service im Dashboard aus, und wählen Sie aus **Servicedetails** .
   - **Liste** : Navigieren Sie zu **Anwendungsservices** > **Services** Und wählen Sie einen Service aus.
   - **Express-Liste** Warnung: Wählen Sie einen Service aus **Betroffene Services** Spalte.

   Die Seite „Servicedetails“ wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Informationen zu Fehlermeldungen in Diagrammen finden Sie unter Diagrammfehler status.

2. Verwenden Sie die Diagramme im Abschnitt „Übersicht“, um festzustellen, wo möglicherweise Leistungsprobleme auftreten.
   Der Abschnitt „Übersicht“ zeigt die Standardmetriken für Rate, Fehler und Dauer (ROT) zusammen mit Metriken für Schlüsseltransaktionen an, die im Service gefunden wurden. Bewegen Sie den Mauszeiger über eine Metrik, um weitere Details anzuzeigen.

   Hinweis: Wenn mehr als ein Service mit demselben Namen gefunden wird, wählen Sie mithilfe von einen einzelnen Service aus **Alle Services** Dropdown-Menü.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie den Zeitraum mithilfe der Zeitauswahl.
4. Verwenden Sie die anderen Diagramme auf der Seite, um zugehörige Informationen zum Service anzuzeigen, z. B. aktuelle Changes, offene Incidents und Trends für Incidents und Warnungen.
   Diese Diagramme helfen zu erklären, ob wiederkehrende Incidents oder Warnungen durch Leistungsprobleme im Service verursacht werden können. Detaillierte Informationen zur Verwendung dieser Seite finden Sie in den entsprechenden Übersichtsvorlagen für Ihren APM-Lieferanten, die in beschrieben werden Service-Observability Vorlagen.

Nächste Maßnahme

Um detailliertere Metriken und Metriken für zugehörige Entitäten anzuzeigen, wählen Sie aus **Erkennbarkeit** Registerkarte. Weitere Informationen finden Sie unter Zeigen Sie Serviceintegritätsmetriken an.

Zeigen Sie Serviceintegritätsmetriken an

Zeigen Sie detaillierte Metriken für einen Service sowie Informationen und Metriken aus zugehörigen Entitäten, z. B. Datenbanken und Hosts, auf der an **Erkennbarkeit** Registerkarte in SOW.

Warum und wann dieser Vorgang ausgeführt wird

Die **Erkennbarkeit** Auf der Registerkarte „Servicedetails“ werden Metriken für zugehörige Entitäten angezeigt, die aus externen APM-Instanzen (Application Performance Management) abgeleitet wurden, sodass Sie zugehörige Metriken anzeigen können, ohne dass Sie die verlassen müssen ServiceNow Plattform.

Die Metriken sind nach den folgenden Entitätstypen gruppiert:

- Anwendungsmetriken: Metriken, die den Anwendungsservices zugeordnet sind
- Computermetriken: Metriken, die den Hosts des Service zugeordnet sind
- Datenbanken: Metriken, die den vom Service verwendeten Datenbanken zugeordnet sind

Angenommen, Sie haben Metriken von New Relic Wird verwendet, um Services, Datenbanken und Hosts zu überwachen. Sagen Sie, dass Sie auch ein Problem mit haben Zur Kasse Service und möchten Leistungsinformationen und -Metriken im Zusammenhang mit diesem Service anzeigen. Service-Observability Kann Ihnen den Service, die Datenbank und die Host-Metriken im Zusammenhang mit diesem Service anzeigen, die von stammen New Relic, Zusammen mit zugehörigen CI-Informationen aus dem ServiceNow Plattform. Jeder Entitätstyp hat ein eigenes Dashboard, und jede Metrik und zugehörige CI-Informationen hat ein eigenes Diagramm.

Vorbereitungen

- Für Version 1,5 muss ein Service aktiviert sein. Weitere Informationen finden Sie unter Teams und Services aktivieren.
- Eine Datenzuordnung muss konfiguriert werden. Weitere Informationen finden Sie unter Erstellen und verwalten Sie Datenzuordnungen.

Erforderliche Rolle: Operator [snc_SOW_svcobs.Manager]

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
   Sie können auf die Seite „Servicedetails“ von diesen Seiten in zugreifen SOW:
   - **Services** Liste: Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard** : Wählen Sie einen Service im Dashboard aus, und wählen Sie aus **Servicedetails** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Liste** : Navigieren Sie zu **Anwendungsservices** > **Services** Und wählen Sie einen Service aus.
- **Express-Liste** Warnung: Wählen Sie einen Service aus **Betroffene Services** Spalte.

Die Seite „Servicedetails“ wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

Trouble?
Informationen zu Fehlermeldungen in Diagrammen finden Sie unter Diagrammfehler status.

2. Wählen Sie aus **Erkennbarkeit** Registerkarte.
Die **Erkennbarkeit** Auf der Registerkarte werden die zugehörigen Metriken und CI-Informationen angezeigt, die für den Service verfügbar sind. Verwenden Sie den Navigationsbereich, um die Entitäts-Dashboards anzuzeigen.

> **Hinweis:** Wenn für eine Entität keine Navigationsoptionen angezeigt werden, wurden die Metriken für diese Entität nicht erkannt oder zugeordnet.

3. Wählen Sie eine Entität aus, um ihr Dashboard anzuzeigen.
Mit den Diagrammen können Sie Folgendes tun:
   - Zeigen Sie Metriken für eine einzelne Entität an, indem Sie auswählen **Alle [Entitätstyp]** Dropdown-Liste und Auswahl einer Entität.

     > **Hinweis:** Wenn mehr als eine Entität Metriken zurückgegeben hat, zeigen Diagramme mehrere Zeilen mit einer Zeile für jede Entität an.

   - Zeigen Sie Metriken aus einem anderen Zeitraum mithilfe der Zeitauswahl an. Der Standardzeitraum ist die letzte Stunde.
   - Aktualisieren Sie die Diagramme auf den aktuellen Zeitraum der letzten Stunde, indem Sie auswählen **Aktualisieren** Schaltfläche.
   - Bewegen Sie den Mauszeiger über einen Punkt, um detaillierte Informationen anzuzeigen.

Detaillierte Informationen zur Verwendung dieser Seite finden Sie in den entsprechenden Observability-Vorlagen für Ihren APM-Lieferanten, die in beschrieben werden Service-Observability Vorlagen.

Service-Observability – Referenz

Referenzthemen enthalten zusätzliche Informationen zur Verwaltung und Verwendung Service-Observability.

Mit Service-Observability installierte Komponenten

Bei der Aktivierung des Service-Observability-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Operator-/Vorgangsmanager [snc_SOW_svcobs.Manager]	Selektiert Incidents in SOW. Zeigt grundlegende Integritätsmetriken für einen Service und detailliertere	• sn_sow_srm.srm_responder • connection_admin • evt_mgmt_Connector_instance_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Servicemetriken aus zugehörigen Entitäten an.	
Service-Observability administrator [sn_SOW_svcobs.admin]	Konfiguriert Datenquellen und fügt Datenzuordnungen hinzu. Passt Dashboard-Vorlagen an.	• sn_SOW_srm.srm_admin • connection_admin • evt_mgmt_Connector_instance_write • sn_sow_itsm_admin.sow_admin_user

Anwendungen speichern Installiert

Folgendes wird installiert, wenn Sie installieren Service-Observability.

Store-Anwendung [Plugin]	Beschreibung
Service-Observability-Benutzeroberfläche [sn_Service_obs_ui]	Die Registerkarten Übersicht und Beobachtungsfähigkeit auf der Seite „Servicedetails“ von SOW.
Service Reliability Management	Service Reliability Management Und Service-Observability Zeigen Sie Serviceleistungsmetriken zusammen an, um einen ganzheitlichen Überblick über die Serviceintegrität zu erhalten.
Platform Analytics	Ermöglicht die Anpassung der Dashboards.

Installierte Tabellen

Tabelle	Beschreibung
Dashboard-Fragmente [sn_SOW_svcobs_Dashboard_Fragments]	Enthält die Definitionen von Dashboards im JSON-Format.
Konfigurationszuordnung für die Service-zu-Daten-Zuordnung [sn_SOW_svcobs_svc_to_config_Map]	Ordnet Datenzuordnungskonfigurationen mit einem registrierten Service über die Tabelle „CMDB-Gruppe enthält Konfigurationselement“ [cmdb_Group_contains_ci] zu.
Datenzuordnungskonfigurationen [sn_SOW_svcobs_Mapping_config]	Definiert eine Datenzuordnungskonfiguration für einen Service.
Konfigurationsregeln für Datenzuordnung [sn_SOW_svcobs_Mapping_config_rules]	Definiert eine einzelne Tag-basierte Zuordnungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Observability-Datenquelle [sn_SOW_svcobs_Data_Source]	Definiert eine Drittpartei-APM-Lieferantendatenquelle (eine `http_connections`), die zum Abrufen von Telemetrie für Services verwendet werden kann.
Datensätze der Service Observability-Entität [sn_SOW_svcobs_Entity_Records]	Zeichnet Konfigurationselemente und unbekannte überwachte Objekte für Entitäten auf, die in Dashboards angezeigt werden.
Service-Observability-PA-Dashboards sn_SOW_svcobs_PA_Dashboards	Enthält Referenzinformationen für anwenderdefinierte Dashboards.

Domain Separation und Service-Observability

Domänentrennung wird für Service-Observability unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domänentrennung und Service-ObservabilityÜbersicht

Domänentrennung ist in allen Aspekten der Anwendung Synthetische Überwachung vorhanden. Benutzer, die zu einer bestimmten Domäne gehören, sehen nur die Daten, die in ihrer eigenen Domäne vorhanden sind.

So funktioniert Domain Separation in Service-Observability

Wenn Daten in durch Domänen getrennt sind Service-Observability, Anwender können die Erkennbarkeitsdaten nur in ihrer eigenen Domäne konfigurieren und anzeigen. Standardmäßig werden alle Benutzer und Datensätze auf die übergeordnete Domäne festgelegt, es sei denn, der Administrator weist sie einer bestimmten Domäne zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie definieren die domänengetrennte Umgebung, wenn Sie Ihre Dateneingaben konfigurieren. Alle relevanten Datensätze und Datenverarbeitungen in Service-Observability Der Programm-Flow befindet sich in derselben Domäne wie die Dateneingabe. Der Domänenname einer Dateneingabe wird in der Spalte Domäne angezeigt, die in den Tabellen in Ihrer Instanz angezeigt wird.

Service-Observability Verwaltet alle Aspekte der Daten, z. B. die Datenzuordnungen und die in Dashboards angezeigten Daten. Wenn eine Eigenschaft geändert wird, wirkt sich der neue Wert nur auf neue Quellen in der spezifischen Domäne aus.

Zugehörige Informationen

Domänentrennung für Service Provider

APM-Lieferantenentitätszuordnungen für Service-Observability

Verstehen Sie, wie Service-Observability Ordnet Service-, Host- und Datenbankentitäten Ihren APM-Lieferantenressourcen (Application Performance Management) zu.

Service-Observability Zeigt Metriken Ihres APM-Lieferanten für Services, Hosts und Datenbanken in den Observability-Dashboards basierend auf den Schlüssel-Wert-Paaren in an Von Ihnen erstellte Zuordnungsregeln Während der Konfiguration. Die folgenden Abschnitte zeigen, wie APM-spezifische Ressourcen den Entitäten zugeordnet werden.

Amazon CloudWatch Entitätszuordnung

Ressourcen werden mit AWS zurückgegeben `GetResources` API.

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	**AWS-Ressource**
Anwendung	API-Gateway –HTTP	API-Gateway-HTTP-APIs
	API-Gateway –REST	API-Gateway-REST-APIs
	ELB	Lastenausgleichsmodule der ELB-Anwendung
	Lambda	Lambda-Funktionen
Berechnen	Host	EC2-Instanzen
Datenbanken	RDS	RDS-Datenbankinstanzen

Azure Entitätszuordnung

Ressourcen werden mit Azure zurückgegeben `ResourceGraph` API.

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Azure **Ressource**
Anwendung	Service	• `Microsoft.Compute/ cloudServices` • `Microsoft.Web/ Sites`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Azure **Ressource**
Berechnen	Host	Microsoft.Compute/virtualMachines
Datenbanken	MySQL	• Microsoft.DBforMySQL/Server • Microsoft.DBforMySQL/flexibleServer
	PostgreSQL	• Microsoft.DBforPostgreSQL/Server • Microsoft.DBforPostgreSQL/flexibleServer

Datadog Entitätszuordnung

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Datadog **Ressource**
Anwendung	Service	Entitäten, die von der Softwarekatalog-API zurückgegeben werden: Entitäten auflisten
Berechnen	Host	Hosts, die von der API „Hosts: Hosts auflisten“ zurückgegeben werden
Datenbanken	MySQL	Datenbanken, die durch Filtern von zurückgegeben werden mysql.net.max_connections Metrik, gefiltert nach dem angegebenen Schlüssel-Wert-Paar in der Datenzuordnung. **Hinweis:** Wenn Ihre Datenbanken diese Metrik nicht ausgeben, werden sie nicht zugeordnet.
	PostgreSQL	Datenbanken, die durch Filtern von zurückgegeben werden postgresql.Verbindungen Metrik, gefiltert nach dem angegebenen Schlüssel-Wert-Paar in der Datenzuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

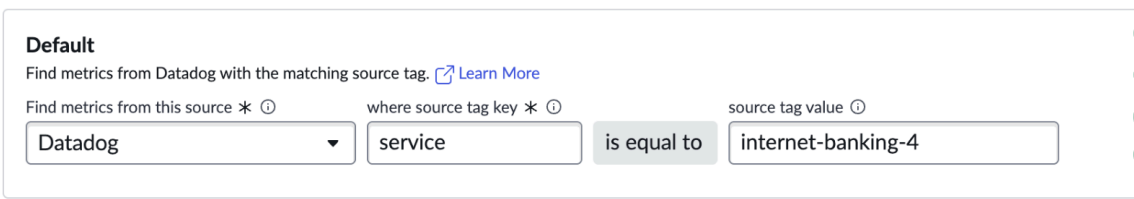
Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Datadog **Ressource**
		Hinweis: Wenn Ihre Datenbanken diese Metrik nicht ausgeben, werden sie nicht zugeordnet.

Hinweiselemente:

- Serviceentitäten: Die `Softwarekatalog-Listenentitäten` Die API gibt nur Daten für Services zurück, die Metadaten enthalten. Wenn Sie Services zuordnen möchten, die keine Metadaten enthalten, müssen Sie mit eine Zuordnung erstellen `Service` Als Tag und der Name des Service als Wert.

  Angenommen, Sie haben einen Service namens `internet-Banking-4` Die Sie in einer Zuordnung verwenden möchten und keine Metadaten enthält. Sie richten die Zuordnung wie in diesem Screenshot gezeigt ein.

  Datadog-Zuordnung, wenn keine Metadaten vorhanden sind

- Standard-Dashboard-Vorlagen: Die Diagramme „Anforderungen“, „Fehler“ und „Latenz“ in den Dashboard-Vorlagen „Übersicht“ und „Observability“ werden mit erstellt Datadog `Trace.http.Request` Nachverfolgungsmetrik. Wenn ein Service diese Metrik nicht ausgibt, werden keine Daten gefunden. Sie können die Vorlage anpassen, um eine andere Ablaufverfolgungsmetrikabfrage zu verwenden. Weitere Informationen finden Sie unter Passen Sie Dashboard-Vorlagen für Service Observability an.

Dynatrace Entitätszuordnung

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Service-Observability **Ressource**
Anwendung	Service	Services
Berechnen	Host	Hosts
Datenbanken	MySQL	MySQL-Datenbankinstanzen
	PostgreSQL	PostgreSQL-Datenbankinstanzen

New Relic Entitätszuordnung

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Service-Observability **Ressource**
Anwendung	Service	APM-Anwendungsservices

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Service-Observability **Ressource**
Berechnen	Host	Hosts
Datenbanken	MySQL	MySQL-Datenbankinstanzen
	PostgreSQL	PostgreSQL-Datenbankinstanzen

SolarWinds Entitätszuordnung

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	SolarWinds **Ressource**
Anwendung	Service	APM-Anwendungsservices
Berechnen	Host	Hosts

Splunk Entitätszuordnung

Ressourcen werden mit zurückgegeben Splunk Metrikzeitreihen-Metadaten-API. Service-Observability Sucht nach übereinstimmenden Schlüssel-Wert-Paaren in anwenderdefinierten Eigenschaften und greift dann auf Suchdimensionen zurück.

Die zurückgegebene Nutzlast wird dann nach dem Vorhandensein einer bestimmten Metrik in den Metadaten gefiltert, die einem Entitätstyp entspricht.

Service-Observability **Entitätskategorie**	Service-Observability **Entitäts-Dashboard**	Splunk **Eigenschaft oder Dimension**	Splunk **Zum Filtern verwendete Metrik**
Anwendung	Service	• Eigenschaft: `sf_Service` • Dimension-Fallback: `service.name`	`sf_metric:Service.Request`
Berechnen	Host	• Eigenschaft: `host.name` • Dimension-Fallback: `Host.ID`	`sf_metric:Disk.summary_usage`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Observability Entitätskategorie	Service-Observability Entitäts-Dashboard	Splunk Eigenschaft oder Dimension	Splunk Zum Filtern verwendete Metrik
Datenbanken	MySQL	• Eigenschaft: mysql.instance.name • Dimension-Fallback: mysql.instance.endpoint	sf_metric:mysql.Threads
	PostgreSQL	Nicht unterstützt	

Erweiterte Abfrageunterstützung für AWS und Azure

Erfahren Sie, wie Sie erweiterte Abfragen für erstellen Service-Observability Dashboard-Diagramme.

Erweiterte Abfragen in Service-Observability Unterstützt die meisten lieferantenspezifischen Abfragesprachen. Kopieren Sie einfach eine Abfrage aus dem APM-Diagramm, und fügen Sie sie in das Feld Erweiterte Abfrage in ein Service-Observability. Abfragen an AWS und Azure müssen jedoch JSON-formatiert sein und den in diesem Thema beschriebenen Richtlinien entsprechen.

Erweiterte AWS-Abfragen

Auf Daten aus AWS wird mit zugegriffen `MetricData abrufen` API. Abfragen können entweder eine direkte Anforderung im JSON-Format an diese API oder im Format eines sein `DashboardBody` Metrik-Widget. Sie können beispielsweise die Widget-Darstellung für ein Diagramm verwenden, das in einem AWS CloudWatch-Dashboard vorhanden ist.

Example: Direkte Anforderung von GetMetricData

Das folgende Beispiel zeigt einen `MetricData abrufen` JSON-Abfrage für ein Diagramm, das die durchschnittliche CPU-Auslastung für eine ELB-Instanz anzeigt.

```
{

  "StartTime": 1637061900, // can be replaced with “${START}”
  "EndTime": 1637074500, // can be replaced with “${END}”
  "MetricDataQueries": [
     {
        "Expression": "SELECT AVG(CPUUtilization) FROM SCHEMA(\"AWS/EC2\",
InstanceId)",
        "Id": "q1",
        "Period": 300,
        "Label": "Cluster CpuUtilization"
     },
     {
        "Id": "m1",
        "Label": "Unhealthy Behind Load Balancer",
        "MetricStat": {
           "Metric": {
              "Namespace": "AWS/ApplicationELB",
              "MetricName": "UnHealthyHostCount",
              "Dimensions": [
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                {
                   "Name": "LoadBalancer",
                   "Value": "app/EC2Co-EcsEl-EXAMPLE69Q/fdd2210e799e4376" // can be
 replaced with “${ENTITIES}” or “${ENTITIES_ELB}”
                }
             ]
          },
          "Period": 300,
          "Stat": "Average"
       }
    }
  ]
}
```

Example: Kopierte Quelle für ein einzelnes Objekt in einem AWS CloudWatch-Dashboard

Dieses Beispiel zeigt das JSON, das direkt aus einem einzelnen Objekt in der Widgets-Liste in der Quellansicht für ein CloudWatch-Dashboard kopiert wurde.

```
{
 "type": "metric",
 "x": 9,
 "y": 0,
 "width": 15,
 "height": 5,
 "properties": {
  "view": "timeseries",
  "metrics": [
   [ "AWS/ApplicationELB", "RequestCountPerTarget", "TargetGroup",
"targetgroup/api-tg/1e3dc9z72fe21ca2", "AvailabilityZone", "us-west-1a" ],
   ["...", "targetgroup/api-tg-cs/82a1db5f950073e1", ".", "." ]
  ],
  "region": "us-west-1"
 }
}
```

Beide Abfragetypen können Vorlagenvariablen verwenden, um eine Reihe von Entitäten oder die in der Anwenderoberfläche ausgewählte Start- und Endzeit darzustellen. Anstatt beispielsweise nach einer einzelnen ELB-Instanz abzufragen, können Sie ersetzen Wert Feld für Lastenausgleichsmodul Dimension mit ${ENTITY_ELB} . Die Abfrage wird für jede ELB-Instanz ausgeführt, die dem ausgewählten Service in zugeordnet ist Service-Observability UI. Das Diagramm zeigt für jede Zeitreihe eine Zeitreihe an.

Hinweis: JSON-Objekte, die aus der Quelle eines CloudWatch-Dashboards kopiert wurden, enthalten keine expliziten Zeitfelder. Die Werte aus der Zeitauswahl in Service-Observability UI wird automatisch verwendet.

Vorlagenvariablen

AWS-Feld	Vorlagenvariable
Dimensionen[n].Wert	• ENTITÄTEN • ENTITÄTEN_HOST • ENTITÄTEN_LAMBDA • ENTITÄTEN_API_GATEWAY_HTTP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlagenvariablen (Fortsetzung)

AWS-Feld	Vorlagenvariable
	• ENTITÄTEN_API_GATEWAY_REST • ENTITÄTEN_ELB • ENTITÄTEN_RDS Die Dimensionen[n].Wert Feld muss ein Ressourcenbezeichner-Schlüssel sein.
Startzeit	START
Endzeit	ENDE

Erweiterte Azure-Abfragen

Sie führen eine erweiterte Abfrage für ein Azure-basiertes Diagramm aus, indem Sie die Quelle aus der Azure-UI kopieren und in einfügen **Erweiterte Abfrage** Feld.

So kopieren Sie die Quelle:

1. Exportieren Sie das Dashboard in der Azure-UI, und laden Sie es herunter.
2. Kopieren Sie die JSON für ein einzelnes Diagramm. Diagramme befinden sich unter Eigenschaften.Objektive[i].Teile[j].metadata.settings.content.options.chart .
3. Fügen Sie die JSON in das Abfragefeld ein. Die JSON muss mindestens Folgendes enthalten:

```
```
{
“metrics”: [
  “name”: string,
  “resourceMetadata”: {
    “id”: string
    }
  ]
}
```
```

Die id Das Feld muss entweder eine Azure-Ressourcen-ID oder ein sein Vorlagenvariable .

Service-Observability Vorlagenvariablen

Machen Sie sich mit den Vorlagenvariablen vertraut, die Sie beim Bearbeiten in Ihren Abfragen verwenden können Service-Observability Dashboards und Diagramme.

Sie können die folgenden Vorlagenvariablen in Ihrer Abfrage verwenden. Mit Variablen kann die Abfrage für mehrere Services, Hosts und Datenbankinstanzen sowie für den Zeitraum verwendet werden, der derzeit für das Dashboard ausgewählt ist.

Hinweis: Amazon CloudWatch Verwendet geringfügig andere Vorlagenvariablen. Weitere Informationen finden Sie unter Erweiterte Abfrageunterstützung für AWS und Azure.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlagenvariablen

Variable	Beschreibung
{$ENTITIES_HOST}	Gibt Metriken für den ausgewählten Host zurück
{$ENTITIES_MYSQL}	Gibt Metriken für die ausgewählte MySQL-Instanz zurück
{$ENTITIES_POSTGRESQL}	Gibt Metriken für die ausgewählte PostgreSQL-Instanz zurück
{$ENTITIES_SERVICE}	Gibt Metriken für den ausgewählten Service zurück.
{$ENTITÄTEN}	Gibt Metriken für die ausgewählte Entität zurück; entweder Service, Host oder Datenbank.
{$START_TIME}	Gibt Metrikzeitreihen anhand der ausgewählten Startzeit zurück.
{$END_TIME}	Gibt Metrikzeitreihen anhand der ausgewählten Endzeit zurück.

Beispielanfrage

Angenommen, Sie verwenden NewRelic und erstellen eine Datenzuordnung, die den Schlüssel zuordnet `Service` Auf den Wert `Checkout-Service` .

Eine einfache Abfrage, die mithilfe der Abfrage erstellt wurde generator Könnte wie folgt aussehen:

```
rate(count(apm.service.transaction.duration), 1 minute
```

Es würde den Kurs der Transaktionen für zurückgeben `Checkout-Service` Service.

Stattdessen können Sie eine vollständige Lieferantenabfrage wie diese verwenden:

```
SELECT rate(count(apm.service.transaction.duration), 1 minute)
 as 'Web throughput' FROM Metric WHERE (entity.guid =
 'NDc2NDMyNXxBUE18QVBQTElDQVRJT058MTA3NjIyODQwMw') AND (transactionType =
 'Web') LIMIT MAX SINCE 30 minutes ago TIMESERIES UNTIL now
```

Es würde die Dauer für den hartcodierten zurückgeben `NDc2NDMyNXxBUE18QVBQTElDQVRJT058MTA3NjIyODQwMw` Entität aus den letzten 30 Minuten.

Um eine Abfrage zu erstellen, die die Zeitreihen für einen ausgewählten Service zu einem beliebigen Zeitpunkt zurückgibt, können Sie die Entität und die Zeiten durch Vorlagenvariablen ersetzen:

```
SELECT average(convert(apm.service.transaction.duration, unit, 'ms')) as metricValue,
 average(convert(apm.service.transaction.duration, unit, 'ms')) - 100 as loop FROM Metric
 WHERE entity.guid IN (${ENTITIES}) FACET entity.guid, entity.name SINCE ${START} UNTIL
 ${END} TIMESERIES LIMIT 25
```

Service-Observability Vorlagen

Zeigen Sie die Vorlagen für Ihren APM-Lieferanten (Application Performance Management) an, um die von bereitgestellten Standard-Dashboards zu verstehen Service-Observability.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Informationen zum Anpassen dieser Vorlagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon CloudWatch Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen Amazon CloudWatch Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

Amazon CloudWatch Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden Amazon CloudWatch **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Aufrufe	Aggregatrate der Transaktionen über den Service.	AWS
Fehler	Anzahl der Transaktionen, die einen Fehler aufweisen.	AWS
Dauer	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	AWS

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige Konfigurationselemente (Configuration Items, CIs) angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Alle Aktive Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon CloudWatch Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der Amazon CloudWatch Registerkarte der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboards

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

API-Gateway –HTTP

Diagramm	Beschreibung	Datenquelle
Anforderungsanzahl	Aggregierte Rate der Transaktionen über den Service, pro Minute.	AWS
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	AWS
4xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 4xx.	AWS
5xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 5xx.	AWS

API-Gateway –REST

Diagramm	Beschreibung	Datenquelle
Anforderungsanzahl	Aggregierte Rate der Transaktionen über den Service, pro Minute.	AWS
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	AWS
4xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 4xx.	AWS
5xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 5xx.	AWS

ELB

Diagramm	Beschreibung	Datenquelle
Anforderungsanzahl	Aggregierte Rate der Transaktionen über den Service, pro Minute.	AWS

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ELB (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	AWS
4xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 4xx.	AWS
5xx-Fehler	Anzahl der zurückgegebenen Fehler mit einem Status von 5xx.	AWS

Lambda

Diagramm	Beschreibung	Datenquelle
Fehler	Anzahl der von der Lambda-Funktion gemeldeten Fehler.	AWS
Dauer	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	AWS
Aufrufe	Anzahl der von diesem Service ausgeführten Lambda-Aufrufe.	AWS

Dashboards berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der von diesem Service verbrauchten Host-Verarbeitungsleistung.	AWS
Disk Write Bytes (Laufwerk-Schreibbytes)	Anzahl der Bytes, die von diesem Service in die Datenbank geschrieben wurden.	AWS
Disk Read Bytes (Laufwerk-Lesebytes)	Anzahl der von diesem Service aus der Datenbank gelesenen Bytes.	AWS
Netzwerk In Byte	Menge des eingehenden Netzwerkverkehrs in Byte für diesen Service.	AWS
Netzwerk Aus Bytes	Menge des ausgehenden Netzwerkverkehrs in Byte für diesen Service.	AWS
Alle EC2-VM-Instanzen	Informationen für alle EC2-VM-Instanzen, die der Service aktiv verwendet. Wählen Sie einen Link aus, um detailliertere Informationen anzuzeigen.	CMDB
Alle Aktiven Server	Informationen für alle Server, die der Service aktiv verwendet. Wählen Sie einen Server-Link aus, um detailliertere Informationen anzuzeigen.	CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenbank-Dashboards

In diesem Dashboard werden Metriken für RDS-Datenbanken angezeigt, die sich auf den Service beziehen.

RDS

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der von diesem Service verbrauchten Verarbeitungsleistung der Datenbank.	AWS
Freier Arbeitsspeicher	Menge des in dieser Datenbank verfügbaren Arbeitsspeichers in Byte.	AWS
Freier Speicher	Menge des in dieser Datenbank verfügbaren Speichers in Byte.	AWS
Aktuelle Verbindungen	Anzahl der Verbindungen von diesem Service zur Datenbank.	AWS
Leselatenz	Zeit in Millisekunden, die für den Abschluss des Lesevorgangs aus der Datenbank benötigt wird.	AWS
Schreiblatenz	Zeit in Millisekunden, die für den Abschluss des Schreibvorgangs aus der Datenbank benötigt wird.	AWS
Alle RDS-Instanzen	Informationen für alle Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

Azure Vorlagen für überwachen Service-Observability

Zum Erstellen verwendete Vorlagen AzureÜberwachen Sie Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

Azure Registerkarte „Überwachungsübersicht“ für Service-Observability

Informationen, die auf angezeigt werden AzureÜberwachen **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Anforderungen	Aggregatrate der Transaktionen über den Service.	Azure
Antwortzeit	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Azure
HTTP 5xx	Anzahl der zurückgegebenen Fehler mit einem Status von 5xx.	Azure

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige Konfigurationselemente (Configuration Items, CIs) angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Alle aktiven Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

Azure Registerkarte „Beobachtungsfähigkeit überwachen“ für Service-Observability

Dashboard und Diagramme auf der Azure Registerkarte „Observability überwachen“ der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Service

Diagramm	Beschreibung	Datenquelle
Anforderungen	Aggregatrate der Anforderungen über den Service.	Azure
HTTP 4xx	Anzahl der Transaktionen, die eine HTTP 4xx-Antwort haben.	Azure
Antwortzeit	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Azure
Daten Aus	Volumen des ausgehenden Netzwerkverkehrs von diesem Service in Byte.	Azure
HTTP 2xx	Anzahl der Transaktionen, die eine HTTP 2xx-Antwort haben.	Azure

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Daten In	Volumen in Byte des eingehenden Netzwerkverkehrs an diesen Service.	Azure

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
Prozentsatz Des Verfügbaren Arbeitsspeichers	Prozentsatz des für den Service verfügbaren Arbeitsspeichers.	Azure
CPU %	Prozentsatz der verbrauchten Host-Verarbeitungsleistung.	Azure
VM Cached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter gecachter Bandbreite)	Prozentsatz der zwischengespeicherten Bandbreite der virtuellen Maschine, die der Service verbraucht.	Azure
Alle aktiven VM-Instanzen	Informationen für alle virtuellen Computer (VM), die der Service aktiv verwendet. Wählen Sie einen VM-Link aus, um weitere Informationen anzuzeigen.	CMDB
Alle Aktiven Server	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Diese Dashboards zeigen Metriken für Datenbanken an, die sich auf den Service beziehen.

MySQL

Diagramm	Beschreibung	Datenquelle
Speicher %	Prozentsatz des Speichers, der derzeit vom Service verbraucht wird.	Azure
CPU %	Prozentsatz der CPU, die derzeit vom Service verbraucht wird.	Azure
Arbeitsspeicher %	Prozentsatz des Arbeitsspeichers, der derzeit vom Service verbraucht wird.	Azure
Aktive Verbindungen	Anzahl der Verbindungen, die derzeit vom Service verwendet werden.	Azure
Abgebrochene Verbindungen	Anzahl der Verbindungen aus dem Service, die von der Datenbank beendet wurden	Azure
MySQL-Betriebszeit	Gesamtzeit in Sekunden, die diese MySQL-Instanz seit ihrem letzten Neustart ausgeführt wurde.	Azure

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Langsame Abfragen	Anzahl der Abfragen, deren Ausführung länger dauert als der angegebene Schwellenwert. Dieser Schwellenwert wird normalerweise durch definiert `Long_query_time` Parameter in MySQL.	Azure

PostgreSQL

Diagramm	Beschreibung	Datenquelle
Speicher %	Prozentsatz des Speichers, der derzeit vom Service verbraucht wird.	Azure
CPU %	Prozentsatz der CPU, die derzeit vom Service verbraucht wird.	Azure
Arbeitsspeicher %	Prozentsatz des Arbeitsspeichers, der derzeit vom Service verbraucht wird.	Azure
Aktive Verbindungen	Anzahl der Verbindungen, die derzeit vom Service verwendet werden.	Azure
Abgebrochene Verbindungen	Anzahl der Verbindungen aus dem Service, die von der Datenbank beendet wurden	Azure
Erfolgreiche Verbindungen	Anzahl der erfolgreichen Verbindungen vom Service zur Datenbank.	Azure
Deadlocks	Anzahl der vom Service aufgetretenen Deadlocks.	Azure
Ist Datenbank Aktiv	`1` Wenn die Datenbank aktiv ist, `0` Wenn ausgefallen ist.	Azure
Alle PostgreSQL-Instanzen	Informationen aller Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

Datadog Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen Datadog Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

Datadog Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden Datadog**Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Abschnitt „KPIs“

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Anforderung	Aggregatrate der Transaktionen über den Service.	Datadog

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Fehler	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	Datadog
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Datadog

Transaktionsdiagramme

Die Transaktionsdiagramme zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen werden durch die Systemkonfiguration Ihres Application Performance Management (APM) bestimmt.

Diagrammname	Beschreibung	Datenquelle
Anforderungen	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog
Fehler	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige CIs angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Aktuelle offene Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

Datadog Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der Datadog Registerkarte „Erkennbarkeit“ der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Service-KPIs

Diagramm	Beschreibung	Datenquelle
Anforderungen	Aggregatrate der Anforderungen über den Service.	Datadog
Fehler	Anzahl der Transaktionen, die einen Fehler aufweisen.	Datadog
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Datadog

Top-Transaktionen

Diagramm	Beschreibung	Datenquelle
Anforderungen	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog
Fehler	Jede Zeile stellt die Anzahl der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Datadog

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Host-Verarbeitungsleistung.	Datadog
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den der Host verwendet.	Datadog
Datenträgerauslastung	Prozentsatz des verwendeten Datenträgerspeichers.	Datadog
Alle Aktiven Server	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB
Alle aktiven VM-Instanzen	Informationen für alle virtuellen Computer (VM), die der Service aktiv verwendet. Wählen Sie einen VM-Link aus, um weitere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Diese Dashboards zeigen Metriken für Datenbanken an, die sich auf den Service beziehen.

MySQL

Diagramm	Beschreibung	Datenquelle
Höchstzahl an Verbindungen	Maximale Anzahl gleichzeitiger Verbindungen, die mit dem MySQL-Datenbankserver hergestellt werden können.	Datadog
Fehlgeschlagene Verbindungen	Anzahl der fehlgeschlagenen Versuche, eine Verbindung zum MySQL-Server herzustellen.	Datadog
Langsame Abfragerate	Anzahl der Datenbankabfragen, die vom APM als langsam kategorisiert wurden.	Datadog
Daten Werden Gelesen	Anzahl der Lesevorgänge, die für die MySQL-Datenbank ausgeführt werden.	Datadog
Daten-Schreibvorgänge	Anzahl der Schreibvorgänge, die für die MySQL-Datenbank ausgeführt werden.	Datadog
Cache-Auslastung	Prozentsatz des Cache-Speichers, der von der MySQL-Datenbank verwendet wird.	Datadog
Alle MySQL-Instanzen	Informationen für alle Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

PostgreSQL

Diagramm	Beschreibung	Datenquelle
Verbindungen	Gesamtzahl der Verbindungen zum Datenbankserver, einschließlich aller verbindungsstatus wie aktiv, inaktiv und andere.	Datadog

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Verwendete Verbindungen	Anzahl der Verbindungen mit der Datenbank, die von diesem Service verwendet werden.	Datadog
Aktive Wartende Abfragen	Anzahl der Abfragen in der Warteschlange, die auf die Ausführung warten.	Datadog
Deadlocks	Anzahl der vom Service aufgetretenen Deadlocks.	Datadog
Rollbacks	Anzahl der vom Service zurückgesetzten Transaktionen.	Datadog
Puffertreffer	Gibt an, wie oft Datenträgerblöcke im Puffer-Cache gefunden wurden, sodass kein Lesen erforderlich war.	Datadog
Alle PostgreSQL-Instanzen	Informationen aller Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

Dynatrace Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen Dynatrace Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

Dynatrace Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden Dynatrace **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Abschnitt „KPIs“

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Kurs	Aggregatrate der Transaktionen über den Service.	Dynatrace
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	Dynatrace
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Dynatrace

Diagramme der Schlüsseltransaktionen

Die Transaktionsdiagramme zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen werden durch die Systemkonfiguration Ihres Application Performance Management (APM) bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Dynatrace
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Dynatrace
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Dynatrace

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige CIs angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Aktuelle offene Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

Dynatrace Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der Dynatrace Registerkarte „Erkennbarkeit“ der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Grundlegende Servicemetriken

Diagramm	Beschreibung	Datenquelle
Kurs	Aggregatrate der Transaktionen über den Service.	Dynatrace
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	Dynatrace
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Dynatrace
Client-Fehlerrate	Fehlerrate der Service-Clients.	Dynatrace
Client-Durchsatz	Rate der Clientanforderungen für diesen Service.	Dynatrace
Client-Antwortzeit	Antwortzeit für Clientanforderungen für diesen Service, in Millisekunden.	Dynatrace
DB-Verbindungen insgesamt	Anzahl der Datenbanken, mit denen dieser Client Verbindungen hat.	Dynatrace
DB-Verbindungsfehler	Anzahl der Fehler, die der Client beim Versuch, auf Datenbanken zuzugreifen, erhalten hat.	Dynatrace
Zeit, die für Datenbankaufrufe aufgewendet wurde	Dauer der Anforderungen an Datenbanken in Millisekunden.	Dynatrace

Servicetransaktionen

Diagramm	Beschreibung	Datenquelle
Schlüsselanforderungsanzahl	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Dynatrace
Schlüsselanforderungsfehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Dynatrace
Antwortzeit Der Schlüsselanforderung	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen	Dynatrace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicetransaktionen (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
	Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Host-Verarbeitungsleistung.	Dynatrace
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den der Host verwendet.	Dynatrace
Festplattenauslastung	Prozentsatz des verwendeten Datenträgerspeichers.	Dynatrace
Alle Aktiven Server	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB
Alle aktiven VM-Instanzen	Informationen für alle virtuellen Computer (VM), die der Service aktiv verwendet. Wählen Sie einen VM-Link aus, um weitere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Diese Dashboards zeigen Metriken für Datenbanken an, die sich auf den Service beziehen.

MySQL

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Verarbeitungsleistung der Datenbank.	Dynatrace
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den die Datenbank verwendet.	Dynatrace
Verfügbarkeit	Prozentsatz der Zeit, die die Datenbank verfügbar ist.	Dynatrace
Verbindungen	Anzahl der Verbindungen zur Datenbank.	Dynatrace
Langsame Abfragen	Anzahl der Datenbankabfragen, die vom APM als langsam kategorisiert wurden.	Dynatrace
Alle MySQL-Instanzen	Informationen für alle Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

PostgreSQL

Diagramm	Beschreibung	Datenquelle
Geplante Prüfpunkte	Durchschnittliche Anzahl der durchgeführten geplanten Prüfpunkte.	Dynatrace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Puffer, die für Prüfpunkt geschrieben wurden	Durchschnittliche Anzahl der während Prüfpunkten geschriebenen Puffer.	Dynatrace
Vom Hintergrundschreiber geschriebene Puffer	Durchschnittliche Anzahl der vom Hintergrundautor geschriebenen Puffer.	Dynatrace
Puffer Zugewiesen	Durchschnittliche Anzahl der zugeteilten Puffer.	Dynatrace
Prüfpunkt-Schreibzeit	Zeit in Millisekunden, die für das Schreiben von Dateien auf den Datenträger aufgewendet wurde.	Dynatrace
Alle PostgreSQL-Instanzen	Informationen aller Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

New Relic Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen New Relic Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

New Relic Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden New Relic **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Abschnitt „KPIs“

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Kurs	Aggregatrate der Transaktionen über den Service.	New Relic
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	New Relic
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	New Relic

Transaktionsdiagramme

Die Transaktionsdiagramme zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen werden durch die Systemkonfiguration Ihres Application Performance Management (APM) bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige CIs angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Aktuelle offene Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

New Relic Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der Registerkarte New Relic Observability der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Grundlegende Servicemetriken

Diagramm	Beschreibung	Datenquelle
Kurs	Aggregierte Rate der Transaktionen über den Service, pro Minute.	New Relic
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	New Relic
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	New Relic
Zeit, die für Datenbankaufrufe aufgewendet wurde	Dauer der Anforderungen an Datenbanken in Millisekunden.	New Relic
Datenbankdurchsatz	Rate der Datenbankanforderungen für diesen Service, pro Minute.	New Relic
In Datenbankabfragen aufgewendete Zeit	Zeit, die für die Abfrage der Datenbank aufgewendet wurde, in Millisekunden.	New Relic

Servicetransaktionen

Diagramm	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	New Relic

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Host-Verarbeitungsleistung.	New Relic
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den der Host verwendet.	New Relic
Festplattenauslastung	Prozentsatz des verwendeten Datenträgerspeichers.	New Relic
Alle Aktiven Server	Informationen für alle Server, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Diese Dashboards zeigen Metriken für Datenbanken an, die sich auf den Service beziehen.

MySQL

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Verarbeitungsleistung der Datenbank.	New Relic
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den die Datenbank verwendet.	New Relic
Verfügbarkeit	Prozentsatz der Zeit, die die Datenbank verfügbar ist.	New Relic
Verbindungen	Anzahl der Verbindungen zur Datenbank.	New Relic
Langsame Abfragen	Anzahl der Datenbankabfragen, die vom APM als langsam kategorisiert wurden.	New Relic
Alle MySQL-Instanzen	Informationen für alle Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

PostgreSQL

Diagramm	Beschreibung	Datenquelle
Geplante Prüfpunkte	Durchschnittliche Anzahl der durchgeführten geplanten Prüfpunkte.	New Relic
Puffer, die für Prüfpunkt geschrieben wurden	Durchschnittliche Anzahl der während Prüfpunkten geschriebenen Puffer.	New Relic
Vom Hintergrundschreiber geschriebene Puffer	Durchschnittliche Anzahl der vom Hintergrundautor geschriebenen Puffer.	New Relic
Puffer Zugewiesen	Durchschnittliche Anzahl der zugeteilten Puffer.	New Relic
Prüfpunkt-Schreibzeit	Zeit in Millisekunden, die für das Schreiben von Dateien auf den Datenträger aufgewendet wurde.	New Relic
Alle PostgreSQL-Instanzen	Informationen aller Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SolarWinds Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen SolarWinds Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

SolarWinds Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden SolarWinds **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Abschnitt „KPIs“

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Kurs	Aggregatrate der Transaktionen über den Service.	SolarWinds
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	SolarWinds
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	SolarWinds

Transaktionsdiagramme

Die Transaktionsdiagramme zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen werden durch die Systemkonfiguration Ihres Application Performance Management (APM) bestimmt.

Diagrammname	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	SolarWinds
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	SolarWinds
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	SolarWinds

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige CIs angezeigt, die sich auf den Service auswirken könnten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Aktuelle offene Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

SolarWinds Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der SolarWinds Registerkarte „Erkennbarkeit“ der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Grundlegende Servicemetriken

Diagramm	Beschreibung	Datenquelle
Kurs	Aggregierte Rate der Transaktionen über den Service, pro Minute.	SolarWinds
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	SolarWinds
Zeit, die für Datenbankaufrufe aufgewendet wurde	Dauer der Anforderungen an Datenbanken in Millisekunden.	SolarWinds
In Datenbankabfragen aufgewendete Zeit	Zeit, die für die Abfrage der Datenbank aufgewendet wurde, in Millisekunden.	SolarWinds
Datenbankdurchsatz	Rate der Datenbankanforderungen für diesen Service pro Minute.	SolarWinds

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der verbrauchten Host-Verarbeitungsleistung.	SolarWinds
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den der Host verwendet.	SolarWinds
Festplattenauslastung	Prozentsatz des verwendeten Datenträgerspeichers.	SolarWinds
Alle Aktiven Server	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB
Alle aktiven VM-Instanzen	Informationen für alle VM-Instanzen, die der Service aktiv verwendet. Wählen Sie einen VM-Link aus, um detailliertere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Datenbankmetriken werden derzeit für nicht unterstützt SolarWinds.

Splunk Vorlagen für Service-Observability

Zum Erstellen verwendete Vorlagen Splunk Dashboards in Service-Observability. Sie können diese Vorlagen nach Bedarf bearbeiten.

Siehe Passen Sie Dashboard-Vorlagen für Service Observability an Weitere Informationen finden Sie unter

Splunk Registerkarte „Übersicht“ für Service-Observability

Informationen, die auf angezeigt werden Splunk **Übersicht** Registerkarte der Seite „Servicedetails“ in SOW.

Abschnitt „KPIs“

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Diagrammname	Beschreibung	Datenquelle
Kurs	Aggregatrate der Transaktionen über den Service.	Splunk
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	Splunk
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Splunk

Diagramme der Schlüsseltransaktionen

Die Diagramme „Schlüsseltransaktionen“ zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen werden durch die Systemkonfiguration Ihres Application Performance Management (APM) bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk

Abschnitt mit kontextbezogenen Informationen

Die Tabelle „aktuelle Changes“ zeigt Änderungen am System an, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Konfigurationselementen in CMDB.

Abschnitt „Statusindikatoren“

Im Abschnitt „Statusindikatoren“ werden Diagramme für zugehörige CIs angezeigt, die sich auf den Service auswirken könnten.

Diagrammname	Beschreibung	Datenquelle
SLO Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in konfiguriert Service Reliability Management(SRM). Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die eine Beziehung zum ausgewählten Service haben.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Auftreten von Warnungen, die sich auf diesen Service auswirken, im letzten Monat.	CMDB
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Alle aktiven Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

Splunk Registerkarte „Erkennbarkeit“ für Service-Observability

Dashboard und Diagramme auf der Splunk Registerkarte „Erkennbarkeit“ der Seite „Servicedetails“ in SOW.

Anwendungs-Dashboard

In diesem Dashboard werden Leistungsmetriken für den ausgewählten Service angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Dashboards angepasst wurden, spiegeln sie möglicherweise nicht die auf dieser Seite angezeigten Informationen wider.

Service-KPIs

Diagramm	Beschreibung	Datenquelle
Kurs	Aggregierte Rate der Transaktionen über den Service, pro Minute.	Splunk
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	Splunk
Latenz	Aggregierte Dauer der Transaktionen über den Service, in Millisekunden.	Splunk

Top-Servicetransaktionen

Diagramm	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion über den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	Splunk

Dashboard berechnen

In diesem Dashboard werden Metriken für Hosts angezeigt, die sich auf den Service beziehen.

Host

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozentsatz der CPU, die derzeit vom Service verbraucht wird.	Splunk
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, der derzeit vom Service verbraucht wird.	Splunk

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Host (Fortsetzung)

Diagramm	Beschreibung	Datenquelle
Festplattenauslastung	Prozentsatz des Festplattenspeichers, der derzeit vom Service verbraucht wird.	Splunk
Alle Aktiven Server	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB
Alle aktiven VM-Instanzen	Informationen für alle VM-Instanzen, die der Service aktiv verwendet. Wählen Sie einen Host-Link aus, um detailliertere Informationen anzuzeigen.	CMDB

Datenbank-Dashboards

Diese Dashboards zeigen Metriken für Datenbanken an, die sich auf den Service beziehen.

MySQL

Diagramm	Beschreibung	Datenquelle
Abfragen Pro Sekunde	Anzahl der Abfragen pro Sekunde, die der Service an die Datenbank sendet.	Splunk
Rate Der Zeilensperren	Häufigkeit, mit der Zeilensperren von Transaktionen aus diesem Service festgestellt werden.	Splunk
Pufferpool Nutzung	Verwendung des Pufferpools für den Zugriff auf zwischengespeicherte Daten durch diesen Service.	Splunk
Tabellen-E/A-Wartezeit	Zeit in Millisekunden Dass die Datenbank auf Eingabe-/Ausgabevorgänge für Tabellen wartet, die von diesem Service gesendet werden.	Splunk
Threads	Anzahl der von diesem Service verwendeten Threads	Splunk
Betriebszeit	Zeit in (?) Dass die Datenbank seit dem letzten Neustart ausgeführt wurde.	CMDB

Service-Observability Formular „Datenzuordnung“

Feldbeschreibungen für das Formular „Observability-Datenzuordnung“. Verwenden Sie dieses Formular, um aktivierte Services in zuzuordnen Service-Observability An Metriken aus Ihrer APM-Instanz (Application Performance Monitoring). Jeder Service kann nur einmal zugeordnet werden, kann jedoch Ausnahmen enthalten, um alle zugehörigen Entitäten einzubeziehen.

Feld	Beschreibung
Zuordnungsname	Name für die Zuordnung. Der Name sollte beschreibend sein, damit Anwender verstehen, woher die Daten stammen.
Services	Für diese Zuordnung zu verwendender Service. Jeder Service kann nur einmal zugeordnet werden. Für Version 1.5.0 von Service-Observability, Services müssen aktiviert sein, um zugeordnet zu werden. Informationen zum Aktivieren eines Service finden Sie unter Teams und Services aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standard	
Metriken aus dieser Quelle suchen	Vorhandene Datenverbindung zur Verwendung für Metriken. Informationen zum Hinzufügen einer Verbindung finden Sie unter Verbinden Sie einen Service-Observability Datenquelle.
wobei Quell-Tag-Schlüssel	Tag-Schlüssel, den Sie dem aktivierten Service zuordnen möchten. Wenn Sie mehr als ein Tag zur Darstellung eines Service verwenden, können Sie eine Ausnahme erstellen. Zum Beispiel verwenden die meisten Tags `Service_Name` Mit Ausnahme von Datenbankmetriken, die verwenden `Service` .
Quell-Tag-Wert	Wert, der den Servicenamen darstellt. Werte können Zeichenfolgen oder eine Variable sein, die Felder im CI für den Service darstellt. Sie können Variablen für Ihre APM-Daten als Wert verwenden, um mehrere Entitäten gleichzeitig zuzuordnen. Beispiel: Wenn Ihre APM-Daten verwenden `$Service_Name` Variable und geben Sie diese als ein **Quell-Tag-Wert** , Alle Services, die diesen Wert verwenden, werden zugeordnet.
Ausnahmen	
Für Entitätstyp	Entität, die einen anderen Schlüssel oder Wert als der Standardwert verwendet.
Metriken aus dieser Quelle suchen	Vorhandene Datenverbindung zur Verwendung für Metriken. Informationen zum Hinzufügen einer Verbindung finden Sie unter Verbinden Sie einen Service-Observability Datenquelle.
wobei Quell-Tag-Schlüssel	Tag-Schlüssel, den Sie dem aktivierten Service für diese Entität zuordnen möchten.
Quell-Tag-Wert	Wert, der den Servicenamen darstellt. Werte können Zeichenfolgen oder eine Variable sein, die Felder im CI für den Service darstellt.

Diagrammfehler status

Machen Sie sich mit den verschiedenen fehlerstatus vertraut, in denen sich die Diagramme befinden Service-Observability Wird möglicherweise angezeigt und wie sie behoben werden können.

Fehlermeldung	Beheben
Richten Sie die Zuordnung der Erkennbarkeitsdaten dieses Service ein	Die Observability-Zuordnung wurde nicht von einem Administrator für den Service konfiguriert. Weitere Informationen finden Sie unter Erstellen und verwalten Sie Datenzuordnungen.
Datenzuordnung ist nicht konfiguriert	Die Observability-Zuordnung wurde nicht von einem Administrator für den Service konfiguriert. Weitere Informationen finden Sie unter Erstellen und verwalten Sie Datenzuordnungen.
Authentifizierung fehlgeschlagen	Service-Observability Verbindung zur Datenquelle kann nicht hergestellt werden. Weitere Informationen finden Sie unter Verbinden Sie einen Service-Observability Datenquelle.
Keine Ergebnisse gefunden	Für das Diagramm wurden keine Metriken gefunden.
Ein Fehler ist aufgetreten.	Die Verbindung mit der Datenquelle war erfolgreich, die APM-Instanz (Application Performance Management) hat jedoch nicht geantwortet. Dieser

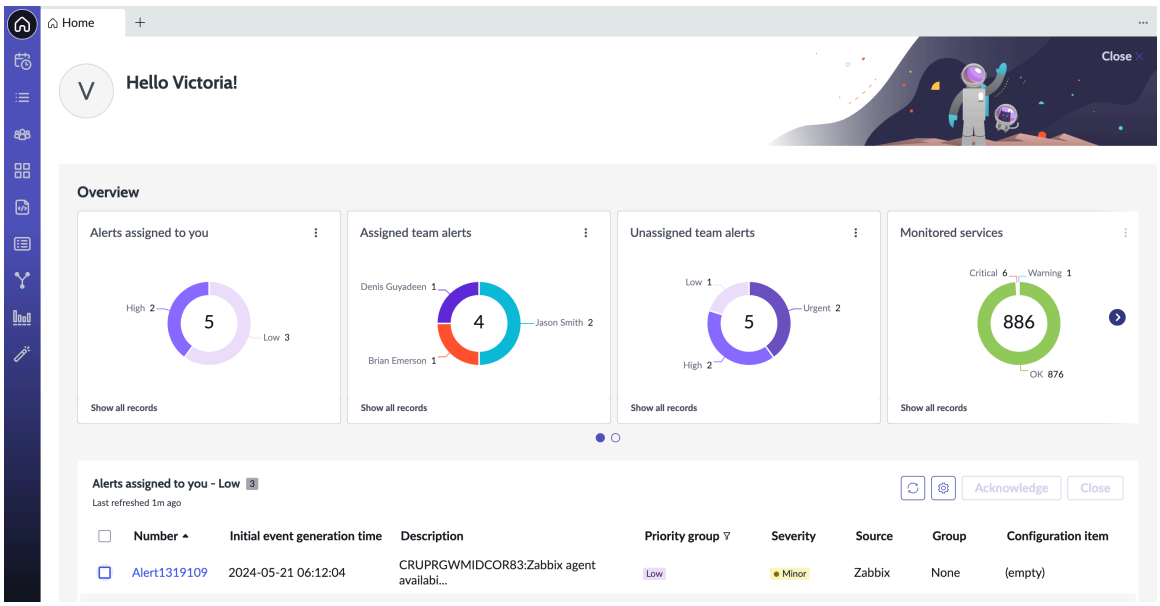
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Beheben
	Fehler kann auf eine Verbindungszeitüberschreitung auf der APM-Seite zurückzuführen sein.
Keine betroffenen Systeme gefunden (Diagramm „Betroffene Systeme“ auf der Übersichtsseite)	Nur Services, die in Ihrer Servicezuordnung gefunden wurden, können angezeigt werden. Aktualisieren Sie Ihre Servicezuordnung, um alle Services einzubeziehen, die in das Diagramm aufgenommen werden sollen. Weitere Informationen finden Sie unter Service-Mapping.
Ziele einrichten (SLO-Fehlerbudget-Diagramm auf der Übersichtsseite)	SLOs wurden für nicht konfiguriert Service Reliability Management. Weitere Informationen finden Sie unter Erstellen Sie SLOs, SLIs und Fehlerbudgetrichtlinien.

Service Operations-Arbeitsbereich für ITOM

ServiceNow® Service Operations-Arbeitsbereich(SOW) ist ein konfigurierbarer Arbeitsbereich zur Optimierung IT Operations Management(ITOM) Workflows, die eine einheitliche Experience für mehrere IT-Betriebsprozesse bieten. Konfigurierbar und anwenderfreundlich konsolidiert es verschiedene Aufgaben in einer einzigen Oberfläche, was eine nahtlose Navigation und einfachen Zugriff auf Tools und Informationen ermöglicht.

Durch die Zentralisierung von Workflows verbessert es die Zusammenarbeit, erleichtert ein effizientes Aufgabenmanagement und bietet Echtzeiteinblicke durch verschiedene Metriken. Sehr anpassbar, ermöglicht es Ihnen, den Arbeitsbereich an Ihre spezifischen Anforderungen anzupassen und die Produktivität und Workflow-Effizienz zu optimieren. Mit einem umfassenden Satz von Funktionen, einschließlich Automatisierungs- und Zusammenarbeitstools, Service Operations-Arbeitsbereich Ermöglicht Anwendern die effektivere Arbeit über verschiedene Workflows hinweg, wodurch die Produktivität unternehmensweit gesteigert wird. Es ist skalierbar, um sich ändernden Geschäftsanforderungen zu entsprechen, und stellt einen kontinuierlichen Support für IT-Umgebungen aller Größen sicher, bietet erstklassige Services und fördert die operative Exzellenz.



Für Informationen zu Abonnements für ITOM Service Operations-Arbeitsbereich, Überprüfen Sie ITOM-Integrität Abonnement um Abonnement für ITOM-Integrität .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

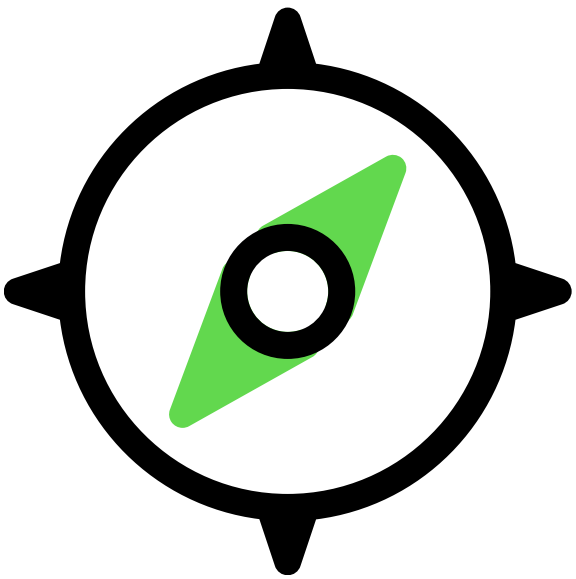
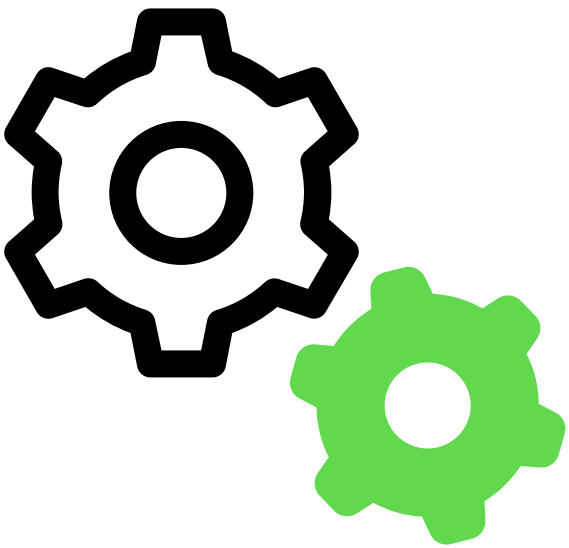
Beim Einrichten von Service Operations-Arbeitsbereich, Es ist wichtig, beides zu konfigurieren IT Operations Management(ITOM) Für die Verwaltung von Warnungen und IT Service Management(ITSM) Für die Lösung von Incidents und die Bereitstellung von Services. Dieses integrierte Setup stellt den Zugriff auf das gesamte Funktionsumfang sicher und erleichtert ein umfassendes Management des IT-Betriebs und der Servicequalität.

Um mehr über zu erfahren ITSM Funktionen, siehe Service Operations-Arbeitsbereich for ITSM .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Erste Schritte

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Service Operations-Arbeitsbereich Konzepte und Funktionen	Konfigurieren Sie die Umgebung, Tools und den Anwenderzugriff

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden

Erfahren Sie, wie Service Desk-Mitarbeiter verwenden können Service Operations-Arbeitsbereich

Referenz

Rufen Sie Details zu ab Service Operations-Arbeitsbereich Komponenten wie Rollen und abhängige Anwendungen

Problembehandlung und Hilfe

Kontakt Kundenservice und Support

Service Operations-Arbeitsbereich für ITOM erkunden

Erfahren Sie, wie Service Operations-Arbeitsbereich Für ITOM Optimiert den gesamten Lebenszyklus von Warnungen, einschließlich Warnungserstellung, Benachrichtigung, Gruppierung, Analyse Untersuchung, Lösung und Abschluss.

Übersicht über Service Operations-Arbeitsbereich

Service Operations-Arbeitsbereich Für ITOM Bietet leistungsstark AIOps-Experience-Fähigkeiten, d. h. Express-Liste, Integrations Launchpad, Warnungsautomatisierung , Und AIOps-Dashboards, die jeweils einen einzigartigen Wert bieten.

Express-Liste

Express-Liste Revolutioniert das Warnungsmanagement durch die Bereitstellung einer konsolidierten Plattform für effiziente Selektierung, Ursachenanalyse (RCA) und Warnungskorrektur. Mit Echtzeitaktualisierungen, dynamischer Filterung und einem intuitiven Vorschaubereich können Anwender ihre Warnungs-Workflows mühelos verwalten und sofort handeln – mit beispielloser Leichtigkeit und Geschwindigkeit.

Integrations-Launchpad

Integrations Launchpad Bietet einen Hub nahtloser Verbindungen zu verschiedenen externen Tools und Services, wodurch das Onboarding neuer Datenquellen vereinfacht wird. Dies optimiert den Integrationsprozess, sodass Anwender ihre vorhandenen mühelos nutzen können ITOMÖkosystem innerhalb von ServiceNow Plattform. Das Integrations-Launchpad verbessert den Datenaustausch und die plattformübergreifende Zusammenarbeit und steigert die Effizienz und Produktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsautomatisierung

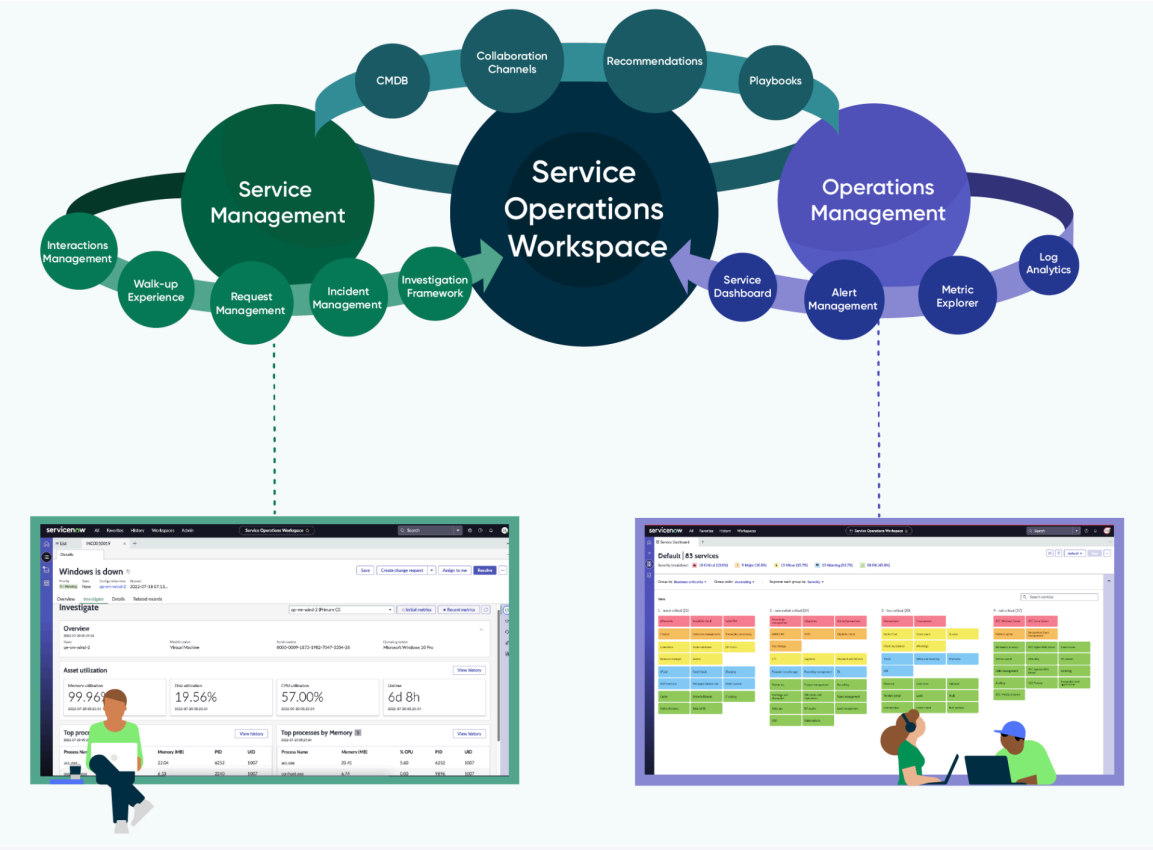
Die Warnungsautomatisierung bietet wichtige Unterstützung, wenn Unternehmen in komplexen IT-Infrastrukturen und steigenden Datenvolumina navigieren. Die manuelle Warnungsbehandlung ist fehleranfällig und ineffizient, was den Bedarf an automatisierten Systemen unterstreicht. Durch die Nichtberücksichtigung irrelevanter oder falsch positiver Warnungen durch die Automatisierung von Warnungen und durch die Verwendung von Warnungsanreicherung, Gruppierung und Antwort optimieren diese Systeme die Reaktion auf Warnungen, reduzieren menschliche Fehler und stellen konsistente, rechtzeitige Aktionen sicher.

AIOps – Dashboards

AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten und Einblicke. Benutzer können Leistungskennzahlen (KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontexte für die IT-Umgebung insgesamt gewinnen. Diese anpassbaren Dashboards ermöglichen Anwendern umsetzbare Einblicke, erleichtern datengesteuerte Entscheidungen und stellen proaktive Antworten auf potenzielle Probleme sicher.

Beim Einrichten von Service Operations-Arbeitsbereich, Es ist wichtig, beides zu konfigurieren IT Operations Management(ITOM) Für die Verwaltung von Warnungen und IT Service Management(ITSM) Für die Lösung von Incidents und die Bereitstellung von Services. Dieses integrierte Setup stellt den Zugriff auf das gesamte Funktionsumfang sicher und erleichtert ein umfassendes Management des IT-Betriebs und der Servicequalität.

Weitere Informationen finden Sie unter Service Operations-Arbeitsbereich für ITSM erkunden .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer-Experience in Service Operations-Arbeitsbereich

1. Tagesbeginn: Der Betreiber überprüft zunächst eine Übersicht über Warnungen und Metriken im Service Operations-Arbeitsbereich, um die Arbeit zu priorisieren.
2. Warnungspriorität: Der Operator priorisiert Warnungen basierend auf SLAs, Prioritätsstufe und Dringlichkeit.
3. Warnungsuntersuchung: Der Operator untersucht Warnungen detailliert und nutzt Verlaufsdaten und Trends.
4. Auf Warnungsinformationen zugreifen: Der Operator greift auf alle zugehörigen Informationen von der Warnungsdatensatzseite zu, um eine umfassende Ansicht zu erhalten.
5. Warnungen lösen: Mithilfe maßgeschneiderter Empfehlungen löst der Betreiber Warnungen effizient.
6. Beratung durch Fachexperten (SME): Bei komplexen Aufgaben oder Aufgaben mit hoher Priorität wendet sich der Betreiber an KMU oder verwendet automatisierte Tools.
7. Zusammenarbeit: Der Betreiber arbeitet direkt aus der Warnung mit Teammitgliedern und Stakeholdern zusammen, gibt Einblicke und koordiniert Antworten.
8. Change-Anforderungen oder Wartung initiieren: Um zukünftige Vorkommen zu verhindern, initiiert der Betreiber Change-Anforderungen oder Wartungsaktivitäten, um die Ursachen zu beheben und langfristige Lösungen zu implementieren.

Anwender

Rollentitel [Name]	Beschreibung
Administrator [evt_mgmt_admin]	Konfiguriert und richtet ein Ereignismanagement Eigenschaften und Regeln.
Operator [evt_mgmt_operator]	Verwaltet Warnungen, einschließlich Schließen und Bestätigen.
Anwender [evt_mgmt_user]	Verwaltet den Lebenszyklus von Warnungen, einschließlich der Ausführung grundlegender Vorgänge wie Anzeigen und Bestätigen.

Vorteile

Vereinheitlichen Sie die Experience für mehrere Workflows

Konsolidieren Sie verschiedene IT-Betriebs-Workflows in einer einzigen, intuitiven Oberfläche, um ein nahtloses Aufgabenmanagement in verschiedenen IT-Betriebsbereichen zu ermöglichen, wodurch die Effizienz verbessert und die Komplexität reduziert wird.

Geben Sie automatisierte Empfehlungen an

Verbessern Sie die Effizienz und Entscheidungsfindung mit automatisierten Empfehlungen, die auf Operator-Aktionen zugeschnitten sind.

Bieten Sie Echtzeiteinblicke

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bieten Sie Analytics- und Berichterstellungsfunktionen in Echtzeit für jeden integrierten Workflow, um fundierte Entscheidungen und proaktive Problemlösungen zu ermöglichen, indem Sie wichtige Leistungsmetriken überwachen und den Betriebsstatus in Echtzeit nachverfolgen.

Zielgerichtete Experience

Bieten Sie dynamische und minimale Inhalte basierend auf der aktuellen Aufgabe an, wobei die nächste Aufgabe mit minimalen Klicks zugänglich ist. Gewähren Sie Zugriff auf zugehörige Warnungen, um schnellere Antwortzeiten zu unterstützen.

Passen Sie die Konfigurierbarkeit an

Ermöglichen Sie Organisationen, den Arbeitsbereich an bestimmte Anforderungen und Einstellungen anzupassen und die Produktivität zu optimieren, indem relevante Daten und Tools für jeden Workflow angezeigt werden.

Steigern Sie die Produktivität

Ermöglichen Sie Anwendern, effizienter über mehrere Workflows hinweg zu arbeiten, indem Routineaufgaben automatisiert werden, Zugriff auf relevante Informationen gewährt und die Zusammenarbeit erleichtert wird, wodurch die Produktivität unternehmensweit gesteigert wird.

Nahtlose Skalierung

Passen Sie Änderungen an Arbeitsauslastung, Anforderungen und betrieblicher Komplexität für alle integrierten Workflows an, um sicherzustellen, dass sich entwickelnde IT-Umgebungen unabhängig von der Größe des Unternehmens weiterhin unterstützt werden.

Zugehörige Informationen

Liste der Arbeitsbereiche

Service Operations-Arbeitsbereich Für ITOM Anwenderoberfläche

Erkunden Sie die Oberfläche, um zu verstehen, wie ein Betreiber Aufgaben priorisieren und Lösungen anbieten kann.

Zugriff Service Operations-Arbeitsbereich

Öffnen Sie den Arbeitsbereich, indem Sie zu navigieren **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.

Homepage

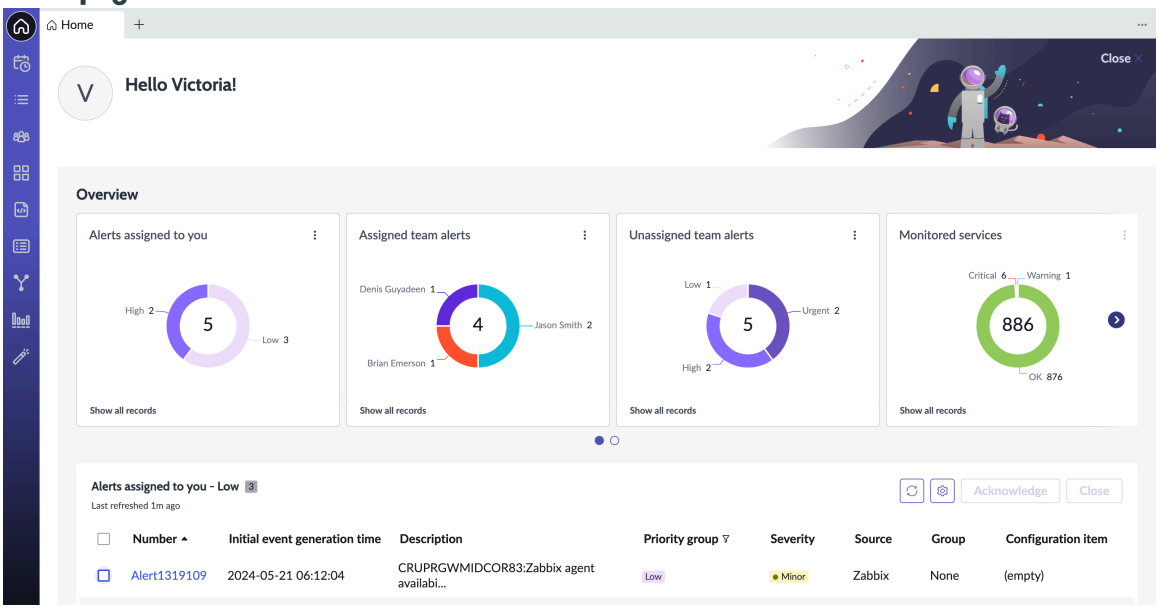
Um auf Informationen auf der Homepage zuzugreifen, wählen Sie das Startsymbol ( ).

Die Homepage bietet Bedienern einen umfassenden Snapshot der aktuellen Betriebslandschaft. Der Abschnitt „Übersicht“ enthält wichtige Einblicke, einschließlich Warnungen, die dem Operator zugewiesen sind, teambasierte Warnungen, nicht zugewiesene Teamwarnungen, überwachte Services und offene Warnungen. Dieser Abschnitt „Ihnen zugewiesene Warnungen“ enthält Operatoren spezifische Details zu Warnungen, die auf ihre Verantwortlichkeiten zugeschnitten sind. Zu den Informationen gehören die Warnungsnummer, die Zeit der Generierung des ersten Ereignisses, die Beschreibung, die Prioritätsgruppe, der Schweregrad, die Quelle, Gruppe, Konfigurationselement, Status, Knoten, Metrikname, und Zeitstempel der letzten Aktualisierung. Beide Abschnitte optimieren den Betrieb, indem sie Betreibern einen kurzen Überblick und personalisierte Einblicke in Warnungen bieten, die für ihre Verantwortlichkeiten relevant sind, wodurch eine schnelle Priorisierung und proaktive Lösung kritischer Probleme erleichtert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage

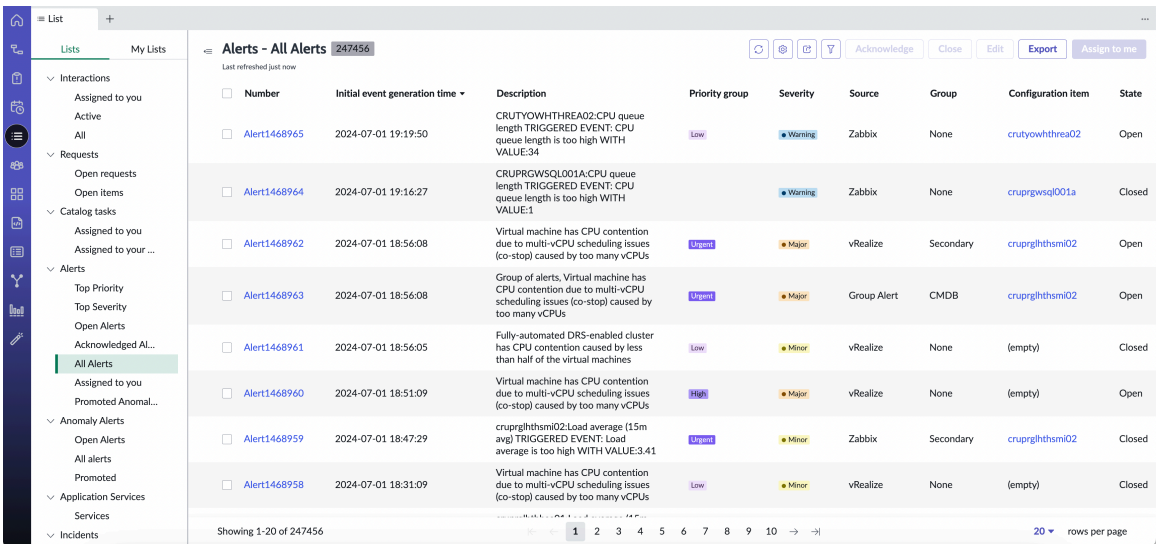


Listen-Seite

Um auf Informationen zu Warnungen aus der Liste zuzugreifen, wählen Sie das Listensymbol ( ).

Die **Listen** Auf der Registerkarte werden vordefinierte Listen angezeigt, während **Meine Listen** Auf der Registerkarte können Anwender eigene Listen für ein personalisiertes Aufgabenmanagement erstellen und anpassen. Detaillierte Anweisungen zum Erstellen einer Liste finden Sie unter Erstellen Sie eine Liste in Service Operations-Arbeitsbereich Für ITOM.

Listenseite



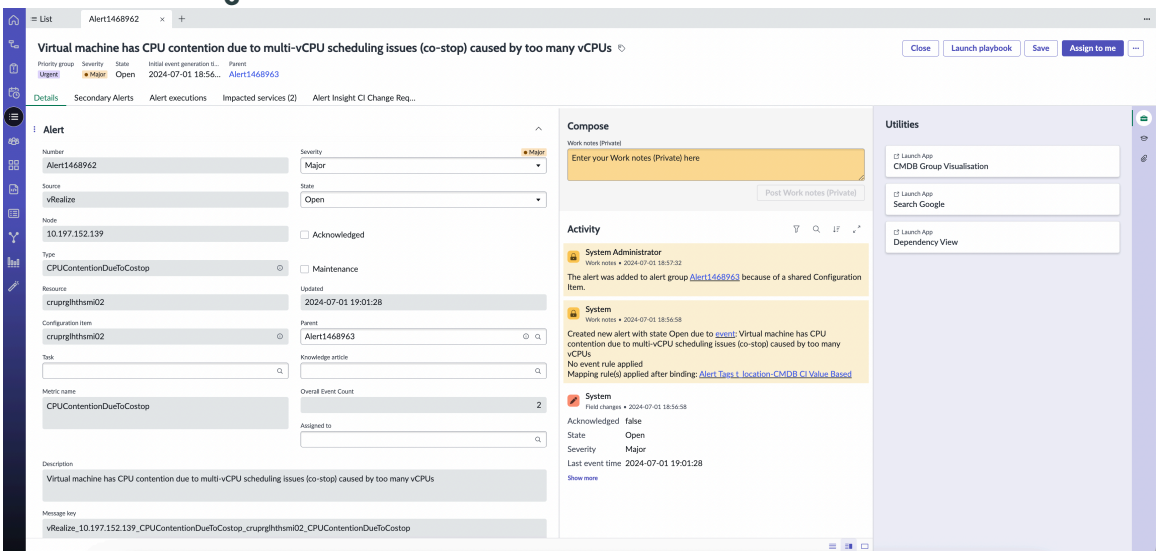
Datensatzansicht

Greifen Sie auf detaillierte Informationen für jede Warnung zu, indem Sie ihre Warnungsnummer auswählen, um den Datensatz zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite mit Warnungsdetails

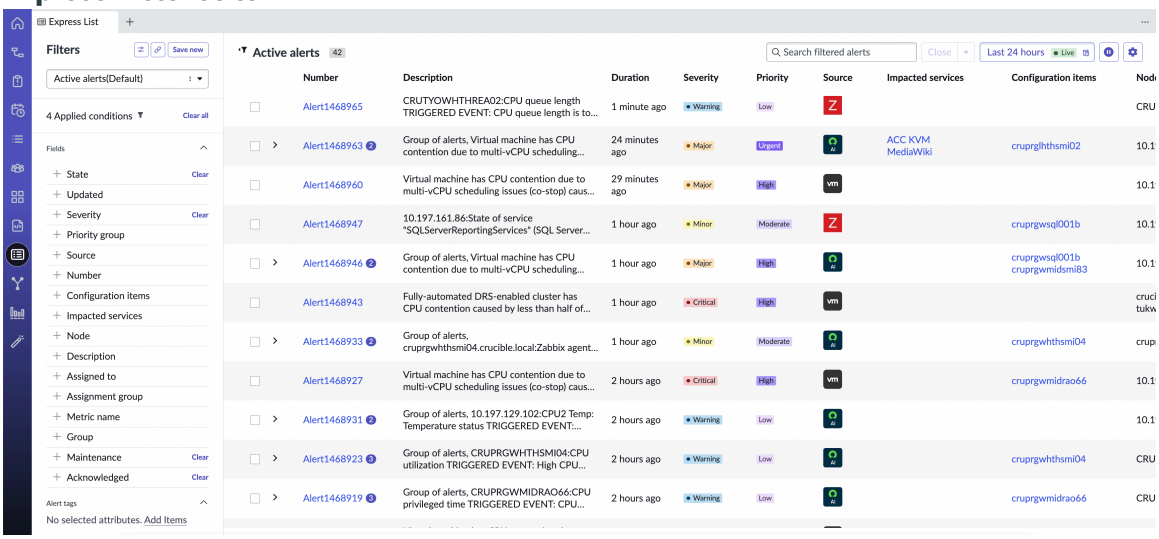


Express-Liste

Die Express-Liste bietet schnelle Warnungsinformationen für effiziente Überwachung, Lösung, Auswirkungsbewertung, Nachverfolgung und Incident-Reporting.

Um auf Informationen in der Express-Liste zuzugreifen, wählen Sie das Symbol für die Express-Liste ( ).

Express-Listenseite



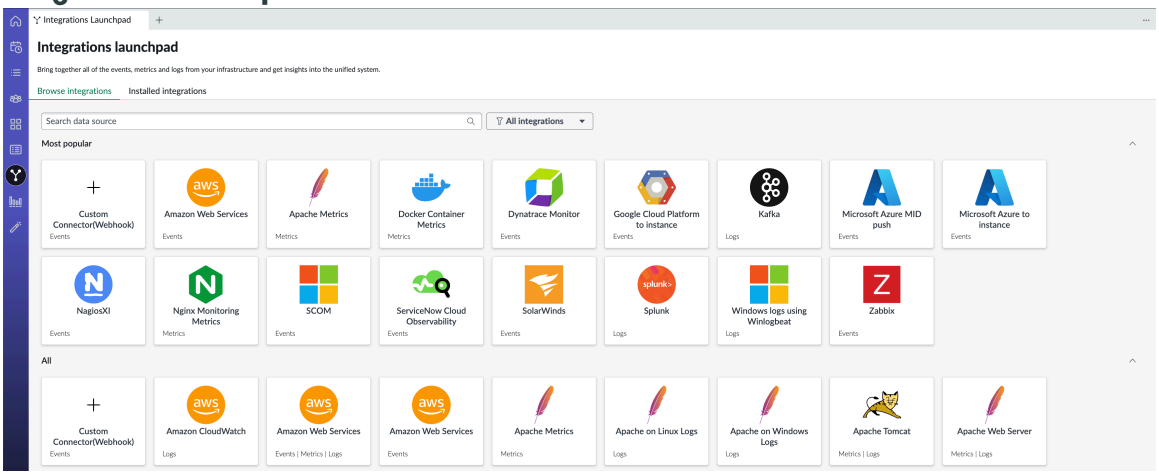
Integrations Launchpad

Die Integrations Launchpad Konsolidiert Ereignisse, Metriken und Protokolle aus Ihrer Infrastruktur, um Einblicke in ein einheitliches System zu erhalten.

Um auf Informationen zu zuzugreifen Integrations Launchpad, Wählen Sie aus Integrations Launchpad Symbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrations Launchpad Seite

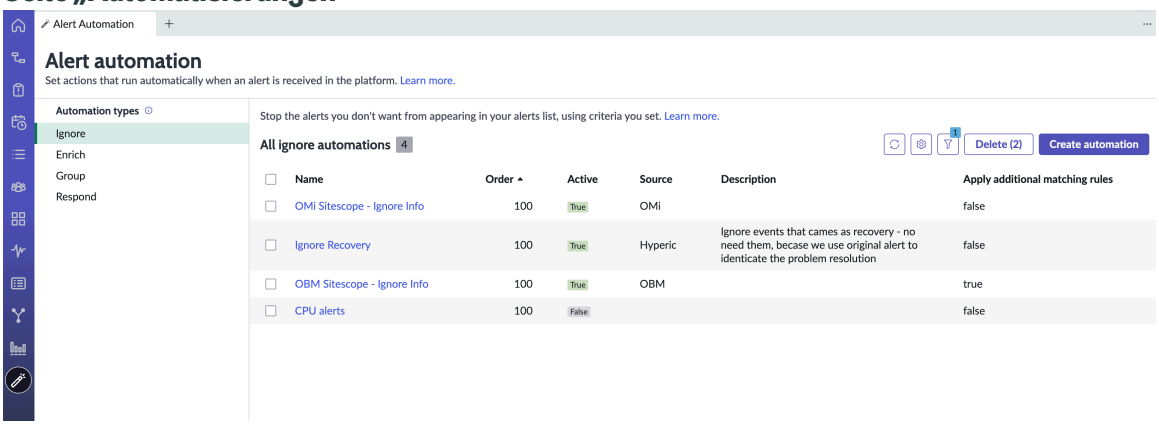


Warnungsautomatisierung

Automatisierungen optimieren Prozesse und ermöglichen zeitnahe Antworten auf potenzielle Probleme, indem Warnungen ignoriert, bereichert, gruppiert und auf Warnungen reagiert werden. Sie reduzieren manuelle Eingriffe, senken das Fehlerrisiko und befreien IT-Teams, um sich auf strategische Aufgaben zu konzentrieren, wodurch die Systemzuverlässigkeit und die Kundenzufriedenheit verbessert werden.

Um auf Informationen zu Automatisierungen zuzugreifen, wählen Sie das Symbol für Warnungsautomatisierungen ( ).

Seite „Automatisierungen“



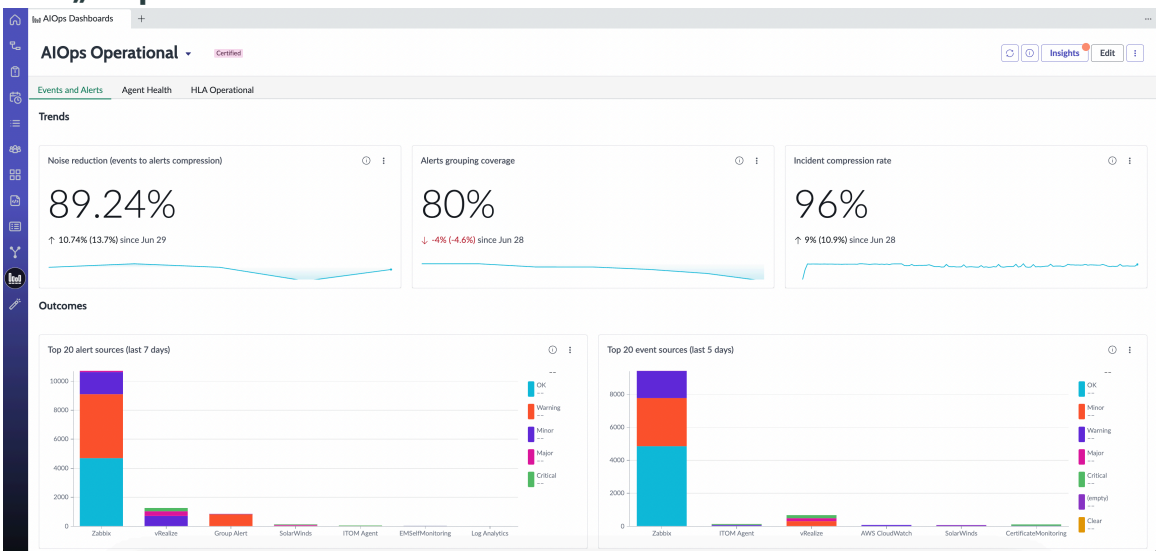
AIOps – Dashboards

Die AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten. Sie können KPIs überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontexte in der IT-Umgebung gewinnen, um proaktive Antworten auf Probleme zu ermöglichen.

Um auf Informationen in Dashboards zuzugreifen, wählen Sie das AIOps-Dashboards-Symbol ( )

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „AIOps-Dashboards“



Service Operations-Arbeitsbereich für ITOM konfigurieren

Konfigurieren Service Operations-Arbeitsbereich Für ITOM Damit Sie IT-Warnungsvolumina effizient verwalten und den Arbeitsbereich anpassen können, um die Servicebereitstellung und die operative Transparenz zu verbessern.

Die Service Operations-Arbeitsbereich Für ITOM Ist ein zentralisierter Hub zur Optimierung IT Operations Management Indem Sie sich auf die Verarbeitung und Lösung von Warnungen konzentrieren. Durch die Nutzung dieses Arbeitsbereichs können Administratoren den Prozess der Überwachung, Selektierung und Lösung von Warnungen optimieren und so die Servicebereitstellung und die betriebliche Effizienz verbessern.

Hinweis: Die Installation der AIOps-Experience-Anwendung [sn_SOW_aiops] bietet Ihnen die Möglichkeit Service Operations-Arbeitsbereich Für ITOM.

Wenn Sie Informationen zu Abonnements für wünschen ITOM Service Operations-Arbeitsbereich, Überprüfen Sie ITOM-Integrität Abonnement um Abonnement für ITOM-Integrität .

Beim Einrichten von Service Operations-Arbeitsbereich, Es ist wichtig, beides zu konfigurieren IT Operations Management(ITOM) Für die Verwaltung von Warnungen und IT Service Management(ITSM) Für die Lösung von Incidents und die Bereitstellung von Services. Dieses integrierte Setup stellt den Zugriff auf das gesamte Funktionsumfang sicher und erleichtert ein umfassendes Management des IT-Betriebs und der Servicequalität.

Um mehr über zu erfahren ITSM Konfigurationen, siehe Service Operations-Arbeitsbereich für ITSM konfigurieren .

Installieren Service Operations-Arbeitsbereich Für ITOM Anwendung

Sie können installieren AIOps-Experience[sn_SOW_aiops] abzurufende Anwendung Service Operations-Arbeitsbereich Für ITOM Wenn Sie die Administratorrolle innehaben.Die Anwendung enthält Demodaten und installiert die zugehörigen ServiceNow® Store-Anwendungen, falls sie nicht bereits installiert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfen Sie AIOps-Experience Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.
- Service Operations Workspace bietet Unterstützung für Domänentrennung. Details finden Sie unter Domain Separation und Ereignismanagement.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit dem Plugin „AIOps-Experience“ [sn_SOW_aiops] installiert.

- Rollen
- Plugins

Weitere Informationen finden Sie unter Mit AIOps-Experience installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der AIOps-Experience [sn_SOW_aiops].

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. **Wahlweise:** Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind die Beispieldatensätze, die Anwendungsfunktionen für allgemeine Anwendungsfälle beschreiben. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.
6. Wählen Sie **Installieren** aus.

Passen Sie an Service Operations-Arbeitsbereich Für ITOM Homepage

Sie können die Daten anpassen, die auf Unterseiten der Homepage angezeigt werden, die im Basissystem verfügbar ist. Für alle visuellen Stiländerungen müssen Sie eine Kopie dieser Zielseite erstellen und sie bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Begrüßungstext auf der Zielseite ändern

Passen Sie die Header-Nachricht an, die Teil des Begrüßungstexts auf der Homepage ist. Dadurch wird eine personalisiertere Anwender-Experience geschaffen, die Besuchern das Gefühl gibt, willkommen und geschätzt zu werden, und sie können auch dazu beitragen, den richtigen Ton und den richtigen Kontext für die dargestellten Informationen festzulegen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Das Daten-Broker-Serverskript „Service Desk-Mitarbeiterschicht abrufen“ ruft die SOWServiceDeskAgentShift-Skripteinbindungen auf, um die Schichtinformationen im Begrüßungstext anzuzeigen.

Während der Anzeigetext für die Standardzielseite angepasst werden kann, können Sie visuelle Stiländerungen am Text nur vornehmen, wenn Sie eine Kopie der Zielseite erstellen.

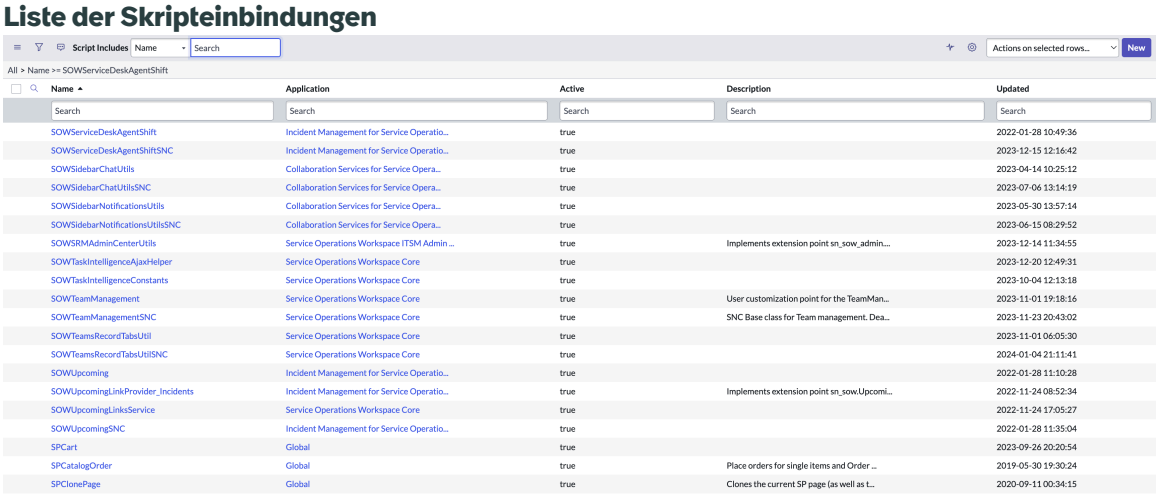
Angenommen, Sie sind bis Montag, 21. März in Rufbereitschaft. Sie können Ihre Begrüßungen entsprechend Ihrem Rufbereitschaftsstatus aktualisieren.

Header

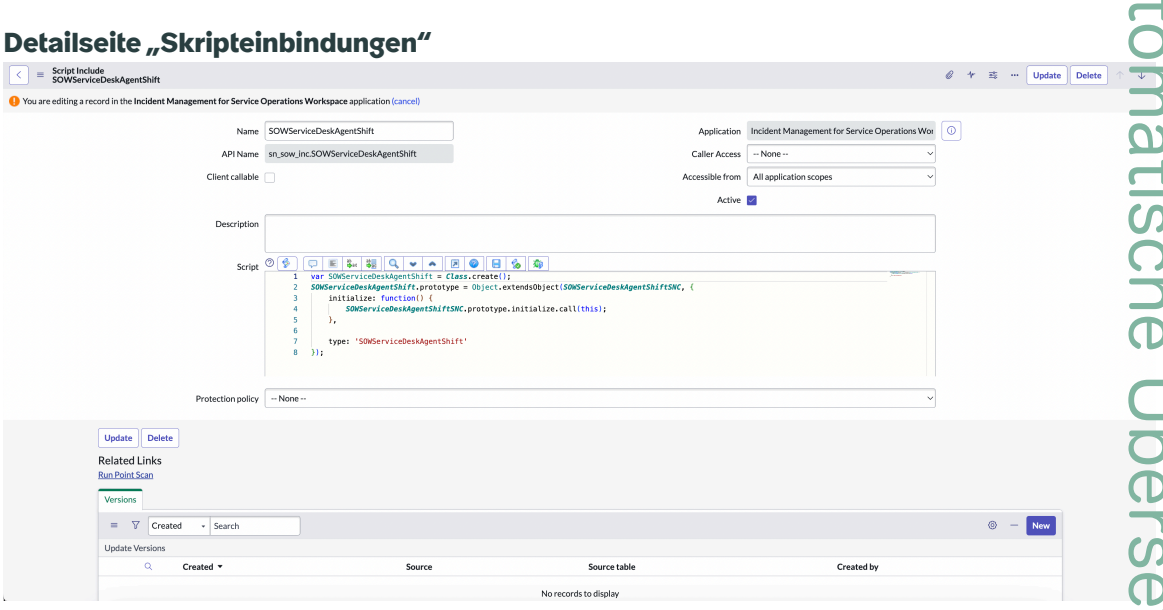
Prozedur

1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich Admin Center** > **Übersicht**an.
2. Wählen Sie auf der Registerkarte **Übersicht** im Abschnitt **Ersteinrichtung** die Option **Zielseite konfigurieren**.
3. Wählen Sie im Formular „Zielseite“ neben **Begrüßungen** die Option **Konfigurieren**.
   Das Formular „Skripteinbindungen“ wird für SOWServiceDeskAgentShift angezeigt, das intern SOWServiceDeskAgentShiftSNC aufruft.
4. Kopieren Sie den Wert des Felds **Skript** von SOWServiceDeskAgentShiftSNC.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**an.
   b. Öffnen Sie in der Liste der Skripteinbindungen den Eintrag „SOWServiceDeskAgentShiftSNC“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Kopieren Sie den Wert des Felds **Skript**.



5. Bearbeiten Sie das Skript SOWServiceDeskAgentShift.

a. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**an.

b. Öffnen Sie in der Liste der Skripteinbindungen den Eintrag „SOWServiceDeskAgentShift“.

c. Fügen Sie den Wert des Felds **Skript** ein, den Sie aus SOWServiceDeskAgentShiftSNC kopiert haben.

```
initialize: function() {
  this.PLUGINS = {
    ON_CALL: "com.snc.on_call_rotation",
    SHIFT_PLANNING: "com.sn_shift_planning"
  };
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  this.DAYS_AHEAD = gs.getProperty('com.snc.on_call_rotation.upcoming_rota_days', 30);
  this.DATE_FORMAT = gs.getDateFormat();
  this.TIME_FORMAT = gs.getTimeFormat();
  this.WFO_SCHEMA_IDENTIFIER = 'readInTimezone';
  this.WFO_ONCALL_TYPE_IDENTIFIER = 'oncallAPIReadInTimezone';
  this.WEEK_DAY_FORMAT = 'EEEE';
  this.FORMAT = {
    SERVICE_DESK_HEADER: 'SERVICE_DESK_HEADER'
  };
  this.DATE_TIME_FORMAT_FULL = "full";
 },


 getUpcomingShift: function(userId, outputFormat, wfoShift) {
  var upcomingShifts, gd = new GlideDate();
  var from = gd.getDisplayValueInternal();
  gd.addDaysLocalTime(this.DAYS_AHEAD);
  var to = gd.getDisplayValueInternal();
  var mayBeWFOUser = userId == gs.getUserID() ?
gs.hasRole("sn_shift_planning.agent") : true;
  if (GlidePluginManager.isActive(this.PLUGINS.SHIFT_PLANNING) && mayBeWFOUser
&& wfoShift)
    upcomingShifts = this.getWFOShifts(from, to, userId);
  var isWFOResponseValid = Array.isArray(upcomingShifts) && upcomingShifts.length >
0;
  if (!isWFOResponseValid && GlidePluginManager.isActive(this.PLUGINS.ON_CALL))
    upcomingShifts = this.getOnCallShifts(from, to, userId);
  return this.getFormattedShift(upcomingShifts, outputFormat);
 },


 getWFOShifts: function(from, to, userId) {
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  var smUtil = new sn_shift_planning.ScheduleManagerUtil();
  var defaultEventCategories = [
    smUtil.WORK_CATEGORY_SYS_ID,
    smUtil.ON_CALL_CATEGORY_SYS_ID
  ];
  var params = {
    "assignmentGroups": "",
    "individualAgents": userId,
    "startDate": from,
    "endDate": to,
    "published": true,
    "eventCategories": defaultEventCategories,
    "filter": {
      "sn_shift_planning_agent_schedule": {
        "event": ["8d03fd9b0f310010717cc562ff767e4a",
"936319993bd02010e81a4ee1f3efc419"]
      }
    }
  };
  var upcomingShifts = [];
  try {
    var agentScheduleRESTAPIUtils = new
sn_shift_planning.AgentScheduleRESTAPIUtils();
    var spans = agentScheduleRESTAPIUtils.retrieveAgentSchedulesFromParams(params);
    if (spans && spans.shiftData && spans.shiftData.user && spans.shiftData.user.data &&
spans.shiftData.user.data.length > 0 && spans.shiftData.user.data[0].schedules) {
      var schedules = spans.shiftData.user.data[0].schedules,
        arrayUtil = new global.ArrayUtil();
      for (var schedule in schedules)
        upcomingShifts = arrayUtil.union(upcomingShifts, schedules[schedule]);
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    }
  } catch (e) {
    gs.error("SOWServiceDeskAgentShiftSNC: Error fetching WFO shifts");
  }

  return upcomingShifts;
 },

 getOnCallShifts: function(from, to, userId) {
  var onCallCommon = new global.OnCallCommon();
  var onCallGroups = onCallCommon.getMyGroups();
  var spans = new global.OCRotationV2(null,
global.OCRotationV2.DEFAULT_FORMAT_OPTION).setStartDate(from).setEndDate(to).set
UserIds(userId).setGroupIds(onCallGroups).getSpans();
  var upcomingShifts = [];
  for (var i = 0; i < spans.length; i++)
    if ((spans[i].type == "roster" || spans[i].type == "override") && spans[i].user_id ==
userId)
      upcomingShifts.push(spans[i]);
  return upcomingShifts;
 },

 getFormattedShift: function(upcomingShifts, outputFormat) {
  if (gs.nil(upcomingShifts))
    return;
  switch (outputFormat) {
    case this.FORMAT.SERVICE_DESK_HEADER:
      return this.getServiceDeskFormattedShift(upcomingShifts);
    default:
      return upcomingShifts;
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  }

},



getServiceDeskFormattedShift: function(upcomingShifts) {

  var response = {

    shiftText: "",

    nearestShift: {}

  };

  var startAttr = "start",

    endAttr = "end",

    isOnCall = true;

  var dateFormat = 'EEEE, MMM dd',

    timeFormat = 'hh:mm a';

  var isWFOSchema = Array.isArray(upcomingShifts) && upcomingShifts.length > 0 &&
this.WFO_SCHEMA_IDENTIFIER in upcomingShifts[0];

  if (isWFOSchema)

    startAttr = "scheduledStartTime", endAttr = "scheduledEndTime";

  response.nearestShift = this.getNearestShift(upcomingShifts, startAttr, endAttr);

  if (response.nearestShift) {

    if (isWFOSchema) {

      if (response.nearestShift.schedule && !(this.WFO_ONCALL_TYPE_IDENTIFIER in
response.nearestShift.schedule))

        isOnCall = false;

    }

    if (isOnCall) {

      if (response.nearestShift.isCurrent) {

        if (response.nearestShift.roster_name)

          response.shiftText = gs.getMessage("You are on-call until {0}
as {1}", [this.getFormattedDateTime(response.nearestShift[endAttr]),
response.nearestShift.roster_name]);

        else
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        response.shiftText = gs.getMessage("You are on-call until {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

      } else {

        if (response.nearestShift.roster_name)

          response.shiftText = gs.getMessage("Your next on-call shift starts on
{0} as {1}", [this.getFormattedDateTime(response.nearestShift[startAttr]),
response.nearestShift.roster_name]);

        else

          response.shiftText = gs.getMessage("Your next on-call shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

      }

    } else {

      if (response.nearestShift.isCurrent) {

        response.shiftText = gs.getMessage("Your shift ends on {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

      } else

        response.shiftText = gs.getMessage("Your next shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

    }

  }



  return response;

},



getNearestShift: function(upcomingShifts, startAttr, endAttr) {

  if (gs.nil(upcomingShifts) || gs.nil(startAttr) || gs.nil(endAttr))

    return;

  var nearestShift;

  upcomingShifts.sort(function(shift_1, shift_2) {

    var gdt1 = new GlideDateTime();

    gdt1.setDisplayValueInternal(shift_1[startAttr]);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    var gdt2 = new GlideDateTime();
    gdt2.setDisplayValueInternal(shift_2[startAttr]);
    return GlideDateTime.subtract(gdt2, gdt1).getNumericValue();
  });
  var currentDateTime = new GlideDateTime(),
    startDateTime = new GlideDateTime(),
    endDateTime = new GlideDateTime();
  for (var i = 0; i < upcomingShifts.length; i++) {
    startDateTime.setDisplayValueInternal(upcomingShifts[i][startAttr] + "");
    endDateTime.setDisplayValueInternal(upcomingShifts[i][endAttr] + "");
    if (currentDateTime.onOrBefore(endDateTime)) {
      nearestShift = upcomingShifts[i];
      if (currentDateTime.onOrAfter(startDateTime))
        nearestShift.isCurrent = true;
      else
        nearestShift.isCurrent = false;
      break;
    }
  }
  return nearestShift;
},


getFormattedDateSpan: function(date, dateFormat, timeFormat) {
  var formattedDate = this.getFormattedDate(date, dateFormat);
  var dateAmPmTime = this.getFormattedTime(date, timeFormat);
  return formattedDate + " " + dateAmPmTime;
},


getFormattedDate: function(inputDate, format) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  var date = new GlideDateTime();
  date.setDisplayValueInternal(inputDate);
  format = !format ? this.DATE_FORMAT : format;
  var gd = date.getLocalDate();
  return gd.getByFormat(format);
 },

 getFormattedTime: function(inputDate, format) {
  var date = new GlideDateTime();
  date.setDisplayValueInternal(inputDate);
  format = !format ? this.TIME_FORMAT : format;
  var gt = date.getLocalTime();
  return gt.getByFormat(format);
 },

 getFormattedDateTime: function(date) {
  var dateTime = new GlideDateTime();
  dateTime.setDisplayValueInternal(date);
  return dateTime.getDisplayValueLang(this.DATE_TIME_FORMAT_FULL);
 },

 endsToday: function(inputDate) {
  var inputGdt = new GlideDateTime();
  inputGdt.setDisplayValueInternal(inputDate);
  return new GlideDateTime().getLocalDate().getValue() ==
inputGdt.getLocalDate().getValue();
 },

 endingTomorrow: function(inputDate) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  var inputGdt = new GlideDateTime();

  inputGdt.setDisplayValueInternal(inputDate);

  var tomorrowDateTime = new GlideDateTime();

  tomorrowDateTime.addDaysLocalTime(1);

  return tomorrowDateTime.getLocalDate().getValue() ==
inputGdt.getLocalDate().getValue();

 },
```

d. Bearbeiten Sie den folgenden Teil des Skripts wie erwähnt.

```
    if (isOnCall) {

      if (response.nearestShift.isCurrent) {

        if (response.nearestShift.roster_name)

          response.shiftText = gs.getMessage("You are on-call until {0}
as {1}", [this.getFormattedDateTime(response.nearestShift[endAttr]),
response.nearestShift.roster_name]);

        else

          response.shiftText = gs.getMessage("You are on-call until {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

      } else {

        if (response.nearestShift.roster_name)

          response.shiftText = gs.getMessage("Your next on-call shift starts on
{0} as {1}", [this.getFormattedDateTime(response.nearestShift[startAttr]),
response.nearestShift.roster_name]);

        else

          response.shiftText = gs.getMessage("Your next on-call shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

      }

    } else {

      if (response.nearestShift.isCurrent) {

        response.shiftText = gs.getMessage("Your shift ends on {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

      } else

        response.shiftText = gs.getMessage("Your next shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    }
```

6. Wählen Sie **Aktualisieren**.

Ändern Sie die Karten der ersten Ebene in Service Operations-Arbeitsbereich Für ITOM Abschnitt „Übersicht“

Passen Sie die Daten an, die auf den Karten der ersten Ebene im Abschnitt Übersicht angezeigt werden, indem Sie verschiedene Parameter konfigurieren, z. B. Headerbezeichnung, Datenquelle, Metrik, Gruppierungsfeld und viewAllQuery. Dies ermöglicht eine maßgeschneidertere und relevantere Anzeige von Informationen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie zu **sys_ux_client_script_include.list**.
2. Wählen Sie in der Liste „UX-Client-Skripteinbindungen“ die Definition SowEMLandingPageUtilsSNC für Client-Skripteinbindungen aus.
3. Bearbeiten Sie im Formular „UX-Client-Skript-Einbeziehung“ das Feld **Skript**.
   Beispiel:

```
}
 };
 const labelMap = {
    'em_alert': {
       'alerts_assigned_to_you': {
          '1': 'Alerts assigned to you - Urgent',
          '2': 'Alerts assigned to you - High',
          '3': 'Alerts assigned to you - Moderate',
          '4': 'Alerts assigned to you - Low'
       },
       'open_alerts': {
          '1': 'Open alerts - Urgent',
          '2': 'Open alerts - High',
          '3': 'Open alerts - Moderate',
          '4': 'Open alerts - Low'
       },
       'team_alerts_assigned': 'Assigned team alerts - to ',
       'team_alerts_unassigned': {
          '1': 'Unassigned team alerts - Urgent',
          '2': 'Unassigned team alerts - High',
          '3': 'Unassigned team alerts - Moderate',
          '4': 'Unassigned team alerts - Low'
       }
    }
```

4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Kopie von Service Operations-Arbeitsbereich Für ITOM Zielseite

Nehmen Sie visuelle Stiländerungen an den Unterseiten auf der Homepage vor. Dies verbessert die allgemeine Anwender-Experience, indem eine konsistente und visuell

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ansprechende Oberfläche bereitgestellt wird, die Navigation verbessert und sichergestellt wird, dass wichtige Informationen leicht zugänglich und ansprechend sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder ui_Builder_admin

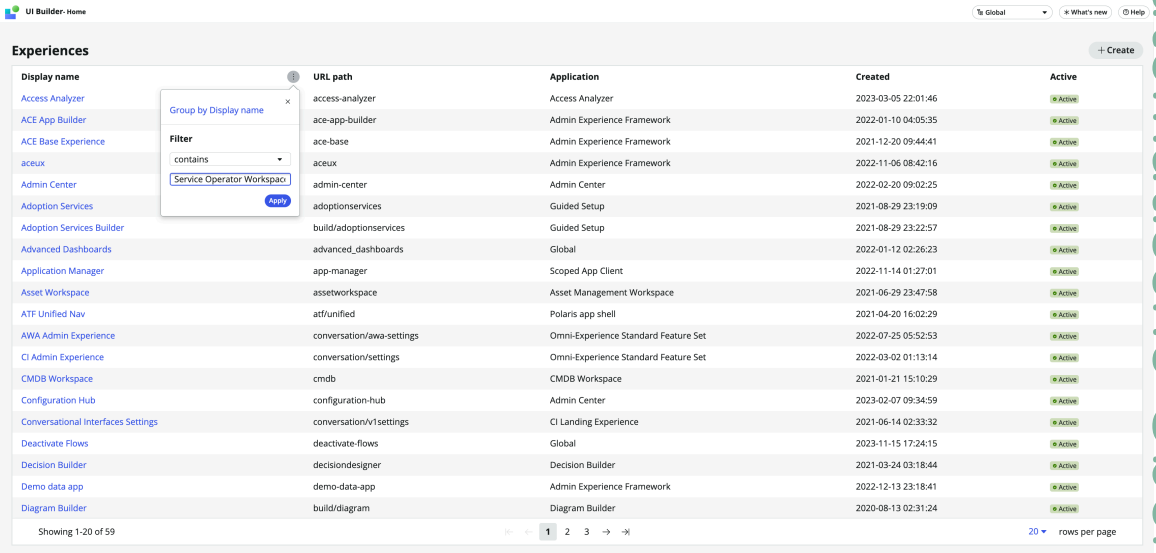
Warum und wann dieser Vorgang ausgeführt wird

Eine Seite ist Inhalt, der sich unter einer bestimmten URL befindet. Wenn ein Anwender die URL öffnet, wird ihm basierend auf der von Ihnen festgelegten Zielgruppe, den Bedingungen und der Reihenfolge eine andere Variante dieser Seite angezeigt.

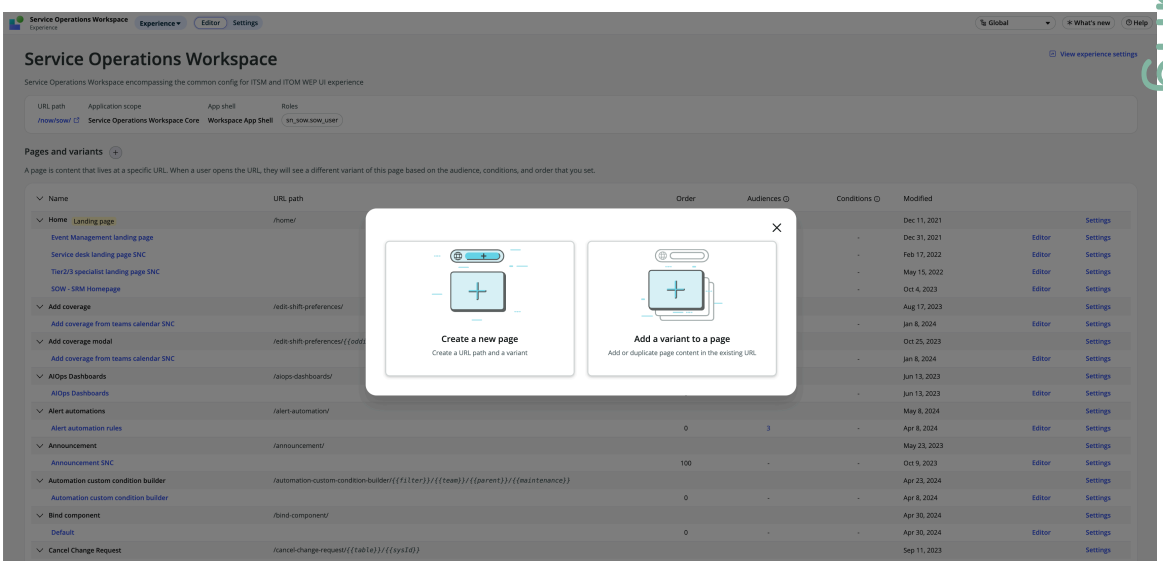
Prozedur

1. Navigieren zu **Alle** > **Now-Experience-Framework** > **UI Builder**an.
2. Von **Anzeigename** Feld, filtern und suchen **Service Operations-Arbeitsbereich** .

   Die Seite „Experiences“ wird geöffnet.



3. Öffnen **Service Operations-Arbeitsbereich** Indem Sie es auswählen.
4. Neben **Seiten und Varianten** , Wählen Sie das Plus-Symbol (⊕).

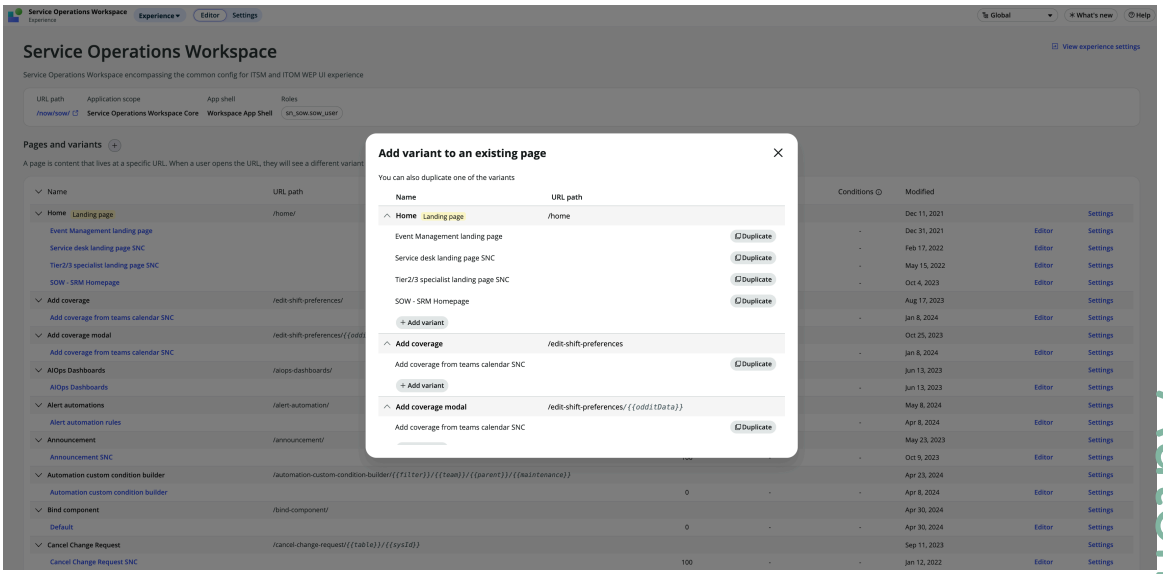


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie Aus **Fügen Sie einer Seite eine Variante hinzu** .

   Das Fenster Variante zu vorhandener Seite hinzufügen wird geöffnet.



6. Um einen doppelten Seiteninhalt im vorhandenen URL-Pfad zu erstellen, wählen Sie aus **Duplikat** Und befolgen Sie die Schritte.

Öffnen Sie Ihre konfigurierbare Arbeitsbereich-Experience in UI Builder

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen
Erforderliche Rolle: ui_builder_admin oder admin

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**an.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnis
Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Zu umleiten Service Operations-Arbeitsbereich Homepage

Ermöglichen Sie eine schnelle Aufgabenpriorisierung, indem Sie Service Desk-Mitarbeiter sofort nach der Anmeldung bei zur Homepage leiten ServiceNow Instanz. Dies verbessert die Workflow-Effizienz, indem Service Desk-Mitarbeitern sofortigen Zugriff auf wichtige Tools und Informationen gewährt wird, was die rechtzeitige Lösung kritischer Aufgaben und Probleme erleichtert.

Vorbereitungen
Stellen Sie sicher, dass der Wert von *`glide.login.home property`* auf `/now/nav/ui/home` gesetzt ist. Diese Eigenschaft gibt die Standard-Homepage an, die bei der Anmeldung angezeigt wird.

Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie Aus **Alle** Und suchen Sie dann nach `sys_properties.list` .
2. Fügen Sie die Eigenschaft *`sn_sow.service_desk_groups`* hinzu.
3. In **Wert** Feld die sys_ID der Anwendergruppe eingeben, zu der der Operator gehört.

   Hinweis: Wenn Sie mehrere Service Desk-Gruppen angeben möchten, fügen Sie im Feld Wert eine kommagetrennte Liste von Gruppen-sys_IDs hinzu.

4. Wählen Sie **Aktualisieren**.

Öffnen Sie Ihre konfigurierbare Workspace-Experience in UI Builder

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen
Erforderliche Rolle: ui_builder_admin oder admin

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**an.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnis
Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Service Operations-Arbeitsbereich

Die Service Operations-ArbeitsbereichÜberwacht Services in Ihrem Ereignismanagement Umgebung, mit der Sie ihren Status überprüfen und diejenigen identifizieren können, die von einer suboptimalen Leistung bedroht sind. Dadurch können Sie Probleme umgehend beheben.

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Sie können konfigurieren Service Operations-Arbeitsbereich Um bis zu 24 Stunden angemeldet zu bleiben. Weitere Informationen finden Sie unter Verwalten Sie Anwendersitzungen .

Zeigen Sie Informationen zur Integrität des Anwendungsservice in an Service Operations-Arbeitsbereich

Überwachen Sie die Integrität von Services, und filtern Sie die Informationen, die Sie anzeigen möchten, sodass Sie sich auf die relevantesten Daten konzentrieren und schnell fundierte Entscheidungen treffen können.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol aus: .

Automatische Übersetzung

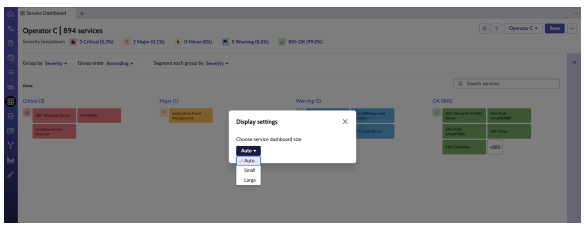
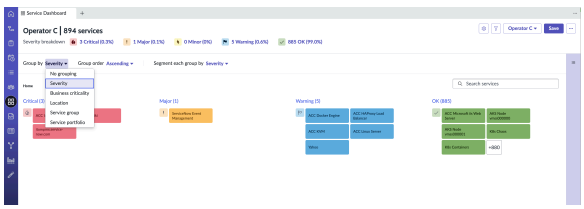
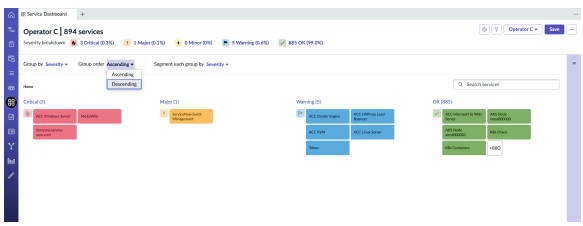
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Seite „Service-Dashboard“ wird angezeigt.

Hinweis: Die Anwendungsservices, die im Service-Dashboard angezeigt werden, sind diejenigen, die der Liste Impact Filter Services hinzugefügt wurden. Weitere Informationen finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

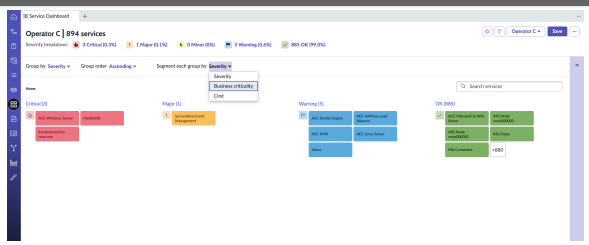
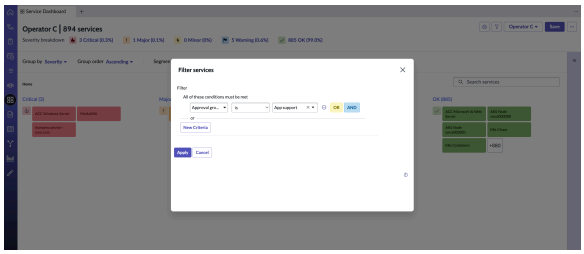
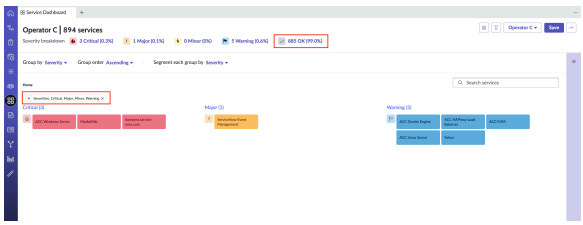
3. Führen Sie die folgenden Aktionen nach Bedarf aus.

Funktionen und Aktionen

Features	Aktionen
Vergrößern oder verkleinern Sie die Kacheln.	a. Wählen Sie das Symbol für die Anzeigeeinstellungen ( ) aus. b. Von **Anzeigeeinstellungen** Popup-Fenster: Wählen Sie die Größe aus. 
Gruppieren Sie Services nach ausgewählten Kriterien	Wählen Sie den Pfeil neben aus **Gruppieren Nach** Und wählen Sie dann die Kriterien aus, nach denen Sie Services gruppieren möchten. 
Gruppenreihenfolge	Wählen Sie den Pfeil neben aus **Gruppenreihenfolge** Und wählen Sie dann die Kriterien aus, nach denen Sie Services gruppieren möchten. 
Jede Gruppe segmentieren nach	Segmentieren Sie jede Gruppe nach Schweregrad, Geschäftsrelevanz und Kosten, um sie basierend auf diesen Attributen in unterschiedliche Gruppen zu kategorisieren und zu organisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Features	Aktionen
	
Filterinformationen	Filtern Sie die im Dashboard angezeigten Informationen, um sicherzustellen, dass Sie sich für eine effektive Überwachung auf relevante Daten konzentrieren. ○ Um einen globalen Filter festzulegen, wählen Sie das Filtersymbol ( ) Und legen Sie die globale Filterbedingung fest, fügen Sie Filterbedingungen hinzu, und wählen Sie dann aus **Anwenden** .  ○ Um einen Schweregrad aus der Anzeige auszuschließen, wählen Sie ihn im aus **Schweregradaufgliederung** Menüband. Herausgefilterte Schweregrade werden abgeblendet angezeigt. Um einen gedämpften Schweregrad auf der Anzeige wiederherzustellen, wählen Sie ihn einfach erneut aus. 

Erstellen Sie eine Anwenderansicht in Service Operations-Arbeitsbereich

Erstellen und passen Sie eine Anwenderansicht in an Service Operations-Arbeitsbereich Um die Anzeige von Informationen im gewünschten Format zu ermöglichen.

Vorbereitungen

Hinweis: Die Betreiber-Arbeitsbereich Die Schnittstelle ist nur für Kunden verfügbar, die von einem Release vor aktualisiert haben Utah Release. Neue Kunden ab Utah Release kann verwenden Service Operations-Arbeitsbereich Für ITOM, Die eine erweiterte UI für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

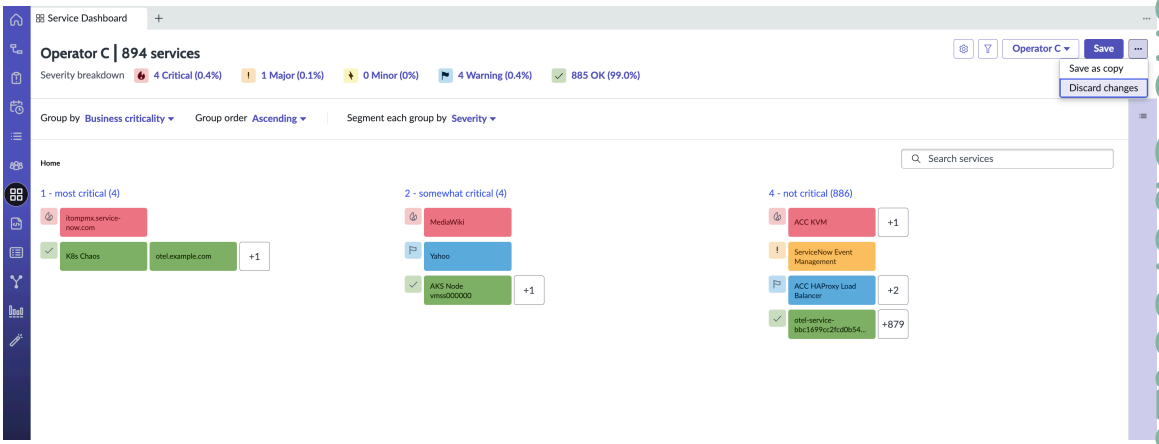
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol aus: .
   Die Seite „Service-Dashboard“ wird angezeigt.

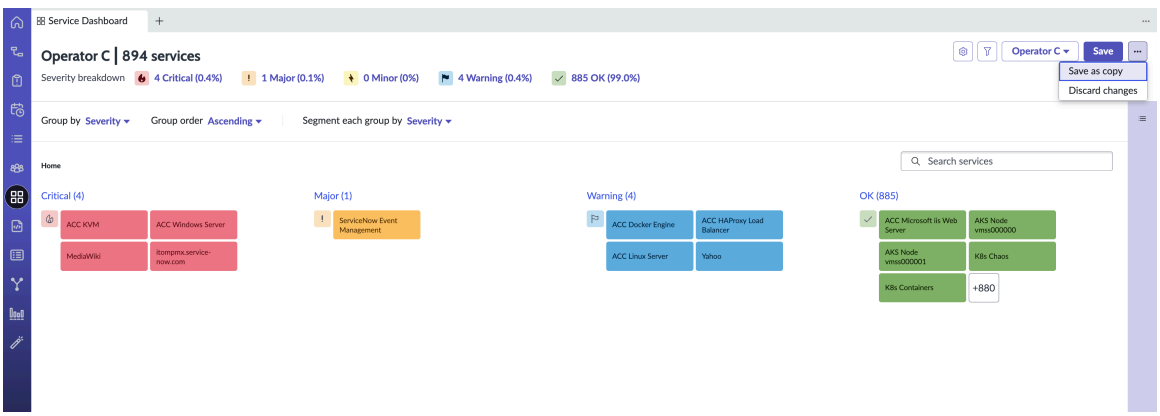
   Hinweis: Die Anwendungsservices, die im Service-Dashboard angezeigt werden, sind diejenigen, die der Liste Impact Filter Services hinzugefügt wurden. Weitere Informationen finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

3. So können Sie das Aussehen des Dashboards anpassen: Wählen Sie Ausgabekriterien aus den Filtern **Gruppieren nach**, **Gruppenreihenfolge** bzw. **Jede Gruppe segmentieren nach**, oder wählen Sie die relevante **Schweregradaufgliederung** aus.
   Auswählen **Servicegruppe** > **Alle** In **Gruppieren nach** Filter zeigt alle Servicegruppen an.
4. Konfigurieren Sie die Informationen, die für die Ansicht angezeigt werden sollen, indem Sie auf das Symbol für Filter-Services ( ) klicken und einen globalen Filter festlegen.
   Beispielsweise können Sie einen Filter so konfigurieren, dass nur die Services angezeigt werden, die einem bestimmten Benutzer zugewiesen sind.

   Hinweis: Um Ihre Änderungen zu verwerfen und den zuletzt gespeicherten Status der Ansicht wiederherzustellen, wählen Sie das Symbol „Weitere Aktionen“ ( ), und wählen Sie **Änderungen verwerfen**.



5. Speichern Sie Ihre neue Ansicht, indem Sie auf das Symbol „weitere Aktionen“ ( ) Neben **Speichern** Schaltfläche und wählen Sie aus **Als Kopie speichern** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

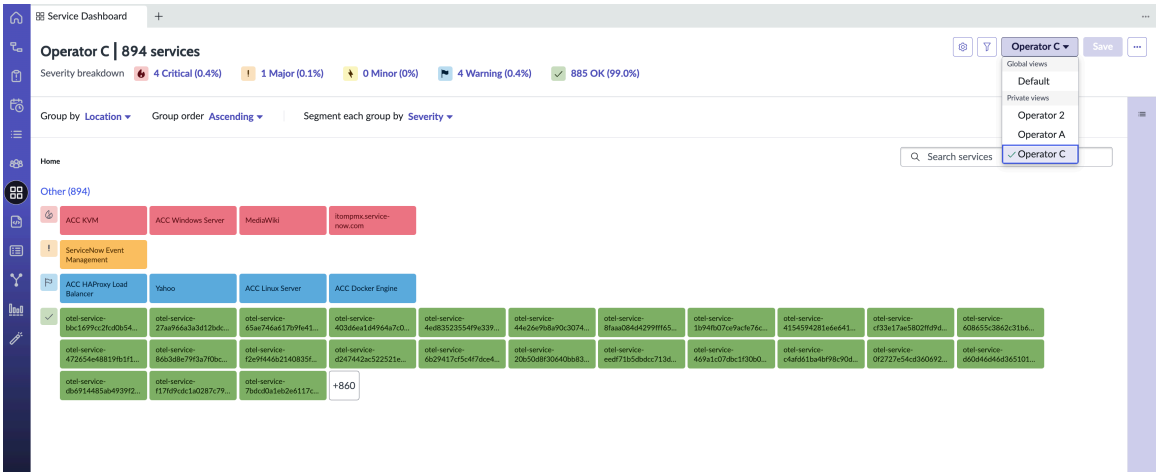
6. Im Dialogfeld „Als Kopie speichern“ geben Sie den Namen Ihrer Ansicht in das Feld **Ansichtsname** ein.

   Die Ansicht wird als gespeichert **Private Ansicht** (Nur für den angemeldeten Anwender sichtbar) und ist zur Verwendung verfügbar.

   Ansichten werden in die folgenden Kategorien gruppiert:

   - **Globale Ansichten**: Für alle Benutzer sichtbar. Nur ein Ereignismanagement Administrator kann globale Ansichten erstellen.
   - **Private Ansichten**: Nur für den angemeldeten Benutzer sichtbar.

   Hinweis: Sie können zwischen verschiedenen Ansichten wechseln, indem Sie eine Ansicht aus der Liste neben auswählen **Speichern** Schaltfläche.



Löschen Sie eine Anwenderansicht in Service Operations-Arbeitsbereich

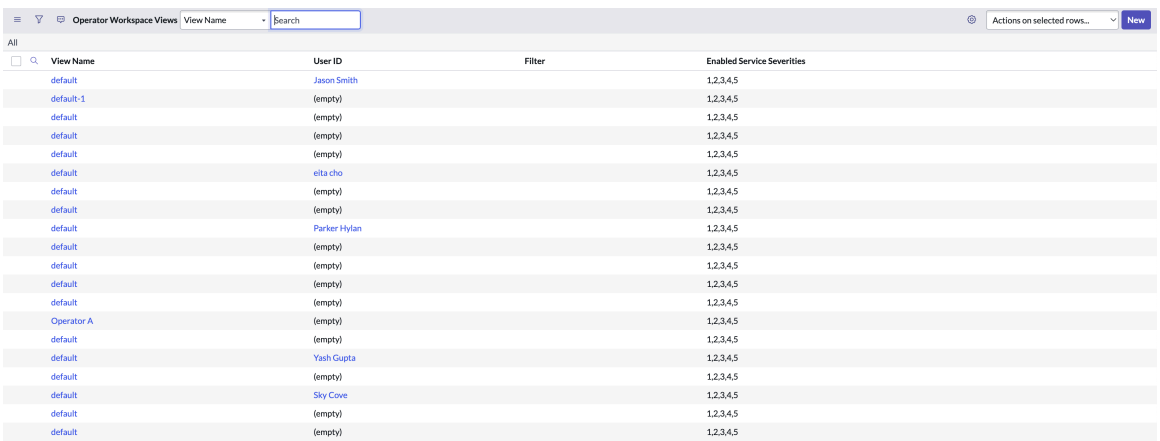
Löschen Sie einen Service Operations-Arbeitsbereich Anwenderansicht, die Sie nicht mehr benötigen. Sie führen diese Aktion über das Menü Ereignismanagement außerhalb von Service Operations-Arbeitsbereich aus.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

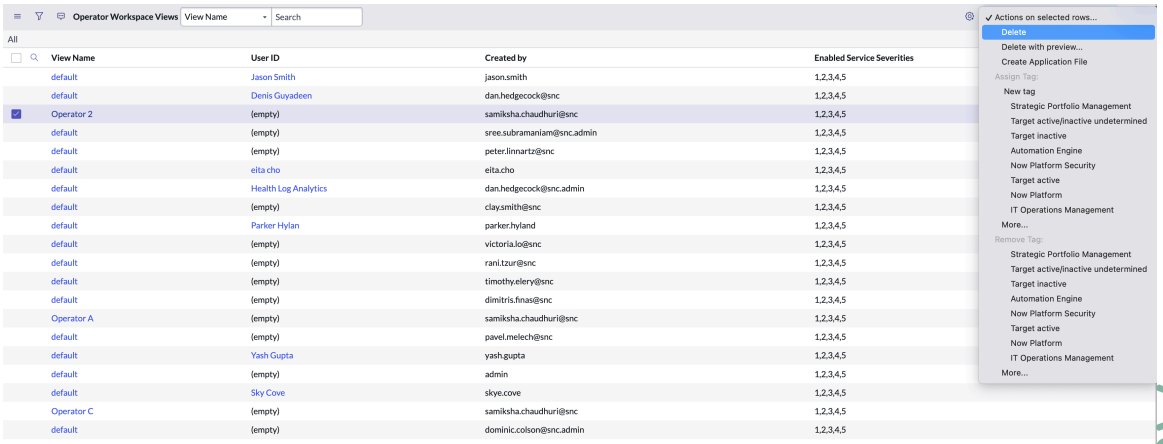
1. In Ihrem Ereignismanagement Instanz im Navigationsbereich suchen nach `noc_user_view.list`.
   Die Seite „Ansichten des Operator-Arbeitsbereichs“ wird geöffnet.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Aktivieren Sie das Kontrollkästchen neben der Ansicht, die Sie löschen möchten.
3. In **Aktionen für ausgewählte Zeilen** Liste, wählen Sie aus **Löschen** .



Zeigen Sie Anwendungsservicedetails in an Service Operations-Arbeitsbereich

Zeigen Sie umfassende Informationen zu einem Anwendungsservice an, einschließlich Name, Geschäftsrelevanz, Besitzstand, Prozess- und Betriebsstatus, datenverkehrsbasierte Discovery-Details, Discovery-Status und relevante Kommentare. Dies ermöglicht eine gründliche Analyse des aktuellen Status und der Nutzung des Anwendungsservice, bietet Klarheit in Bezug auf Besitz und Relevanz und erleichtert eine effektive Priorisierung von Ressourcen und Aktionen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_Operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

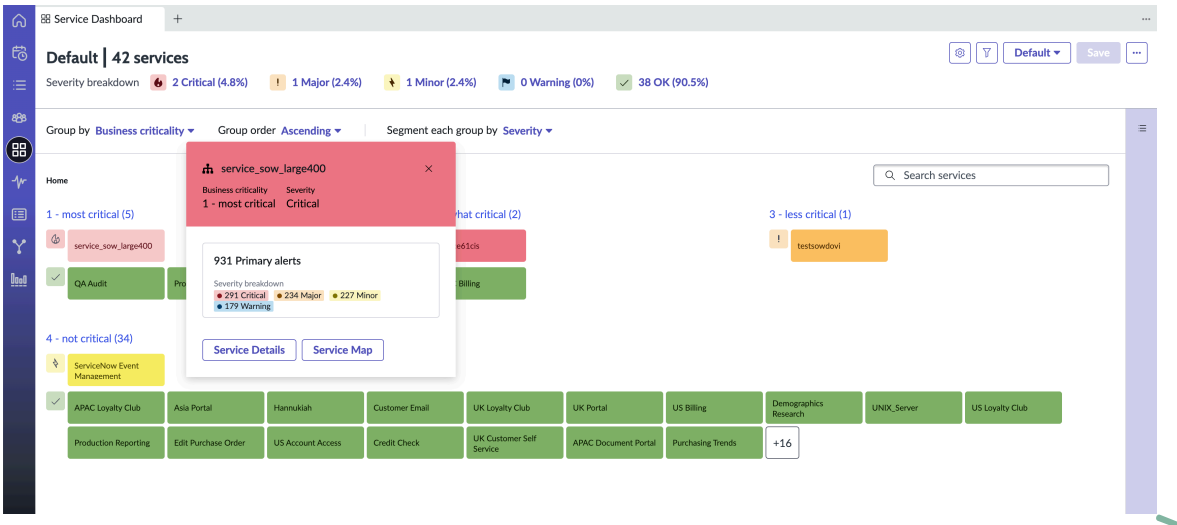
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol aus: .
   Die Seite „Service-Dashboard“ wird angezeigt.

   Hinweis: Die Anwendungsservices, die im Service-Dashboard angezeigt werden, sind diejenigen, die der Liste Impact Filter Services hinzugefügt wurden. Weitere Informationen finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftsrelevanz und der Schweregrad eines Service angezeigt.

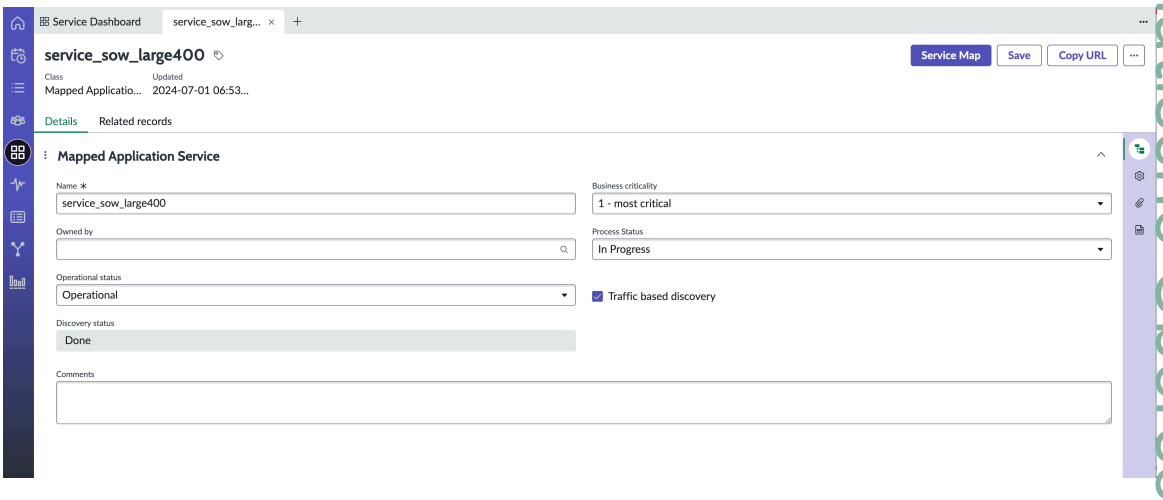
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Servicedetails** aus.
   Standardmäßig ist **Details** Registerkarte ist ausgewählt.

   Die Detailseite enthält umfassende Informationen zu einem Anwendungsservice.



   Weitere Informationen zu diesen Feldern finden Sie unter Detailseite für Anwendungsservice.

Primäre Warnungen anzeigen, die einem Service zugeordnet sind

Zeigen Sie die einem Service zugeordneten primären Warnungen an, um Probleme mit dem Service zu beheben.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

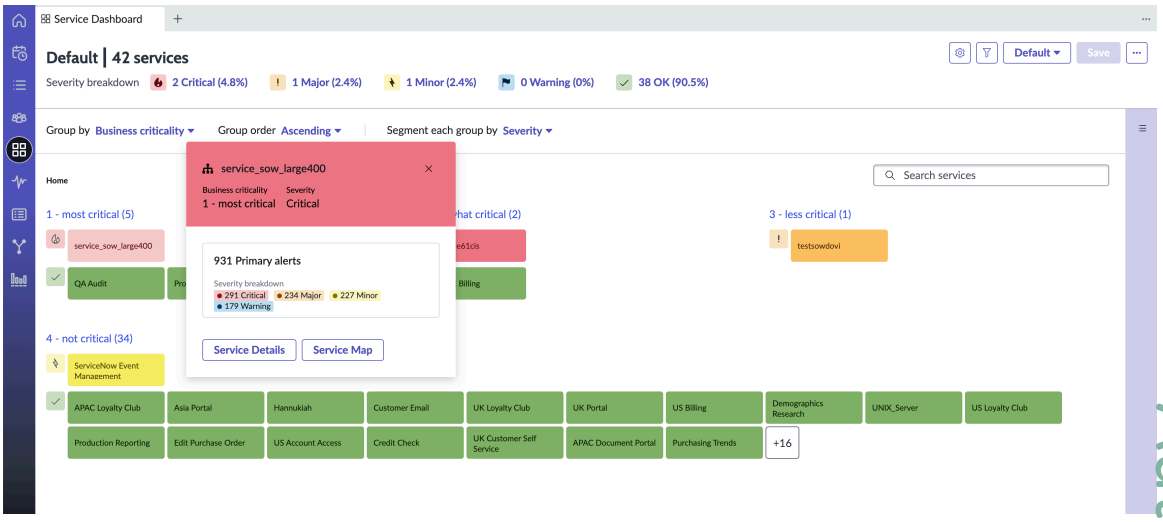
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol aus: .
   Die Seite „Service-Dashboard“ wird angezeigt.

> **Hinweis:** Die Anwendungsservices, die im Service-Dashboard angezeigt werden, sind diejenigen, die der Liste Impact Filter Services hinzugefügt wurden. Weitere Informationen finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

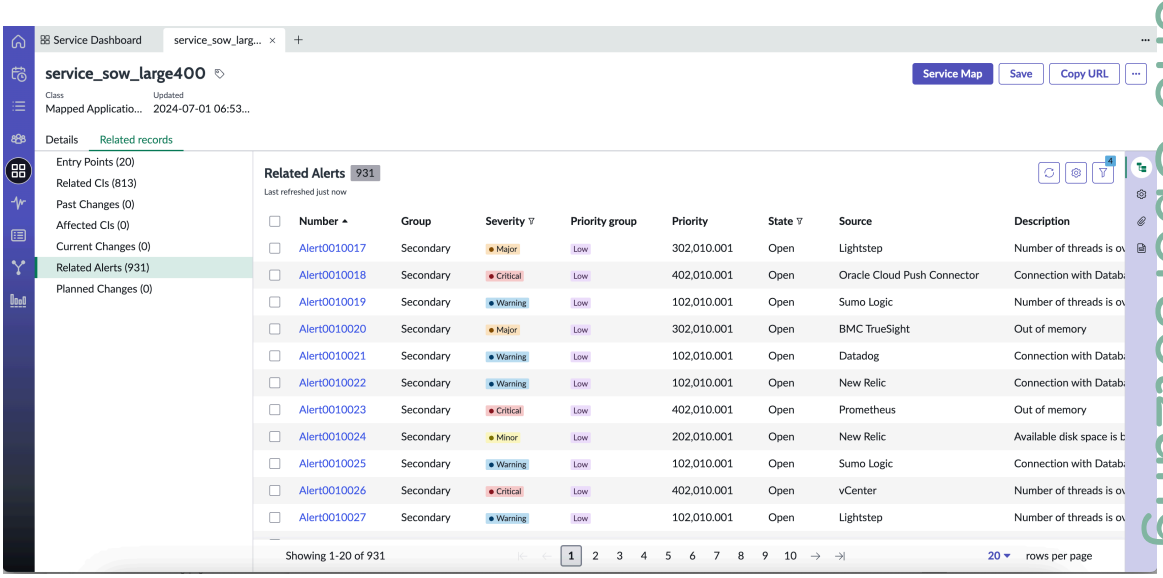
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftsrelevanz und der Schweregrad eines Service angezeigt.



4. Wählen Sie **Servicedetails** aus.
   Standardmäßig ist **Details** Registerkarte ist ausgewählt.
5. Wählen Sie aus **Zugehörige Datensätze** Registerkarte.
6. Wählen Sie im linken Bereich aus **Zugehörige Warnungen** .



Zeigen Sie Details zu einer Warnung an, indem Sie ihre Nummer im auswählen **Nummer** Spalte.

Erstellen Sie eine Liste in Service Operations-Arbeitsbereich Für ITOM

Passen Sie Listen in an Service Operations-Arbeitsbereich Indem Sie neue Listen erstellen, ihre Reihenfolge ändern, ihren Inhalt ändern oder Listen nach Bedarf löschen. Diese Flexibilität ermöglicht es Betreibern, Informationen nach ihren spezifischen Anforderungen zu organisieren, was die Navigation erleichtert, den Zugriff auf relevante Daten beschleunigt und das Workflow-Management optimiert.

Vorbereitungen

Erforderliche Rolle: itil

Automatische Übersetzung

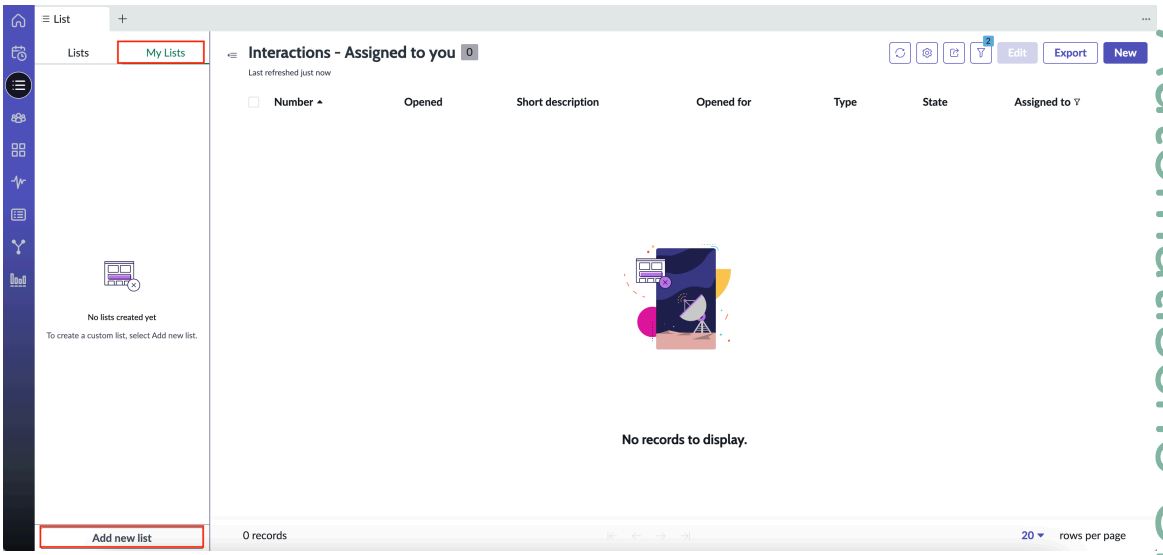
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie anwenderdefinierte Gruppierungen von Datensätzen, die unter aufgeführt sind **Listen** Registerkarte, z. B. Incidents, die an ein bestimmtes Unternehmen gebunden sind. Passen Sie vorhandene Listen an, oder erstellen Sie neue, die ausschließlich unter sichtbar sind **Meine Listen** Registerkarte für personalisierte Organisation.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie **Neue Liste hinzufügen**.



5. Erstellen Sie eine Liste, indem Sie sie entweder auf einer vorhandenen Liste basieren oder eine neue erstellen.
   - Um die Liste auf Grundlage einer vorhandenen Liste anzulegen, wählen Sie **Mit vorhandener beginnen** aus.
   - Um eine neue Liste zu erstellen, wählen Sie **Selbst erstellen** aus.
6. Füllen Sie im Formular die Felder aus.
   Weitere Informationen zu den Feldern finden Sie unter Erstellen Sie Listenfelder.
7. Wählen Sie **Erstellen** aus.
   Die Liste wird in angezeigt **Meine Listen** Registerkarte.

Benennen Sie eine Liste in um Service Operations-Arbeitsbereich Für ITOM

Benennen Sie eine Liste um, um ihren Inhalt oder Zweck besser widerzuspiegeln. Diese Anpassung ermöglicht es Operatoren, Listennamen an ihrer Workflow-Terminologie auszurichten und so die Klarheit und Anwenderfreundlichkeit zu verbessern.

Vorbereitungen

Erforderliche Rolle: itil

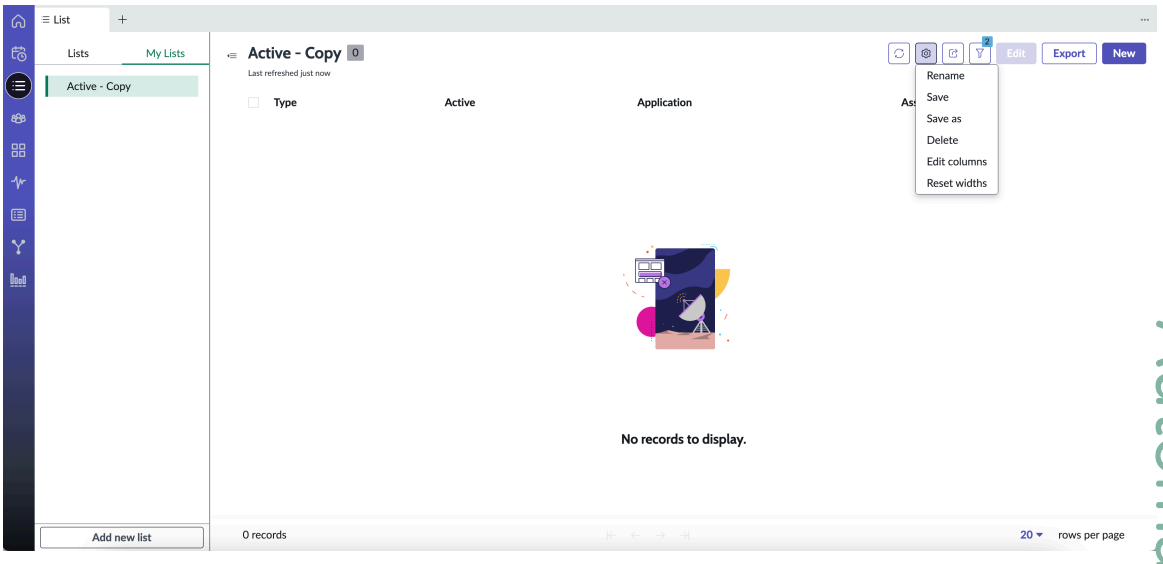
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie die Liste aus, die Sie umbenennen möchten.
5. Wählen Sie das Einstellungssymbol ( ) Und dann auswählen **Umbenennen** .



6. In **Umbenennen** Popup-Fenster im **Titel** Feld umbenennen Sie den Namen der Liste, und wählen Sie aus **Speichern** .
   Die Liste wird umbenannt.

Liste in neu anordnen Service Operations-Arbeitsbereich Für ITOM

Ordnen Sie Listen neu an, um Informationen zu priorisieren und die Workflow-Organisation zu verbessern.

Vorbereitungen

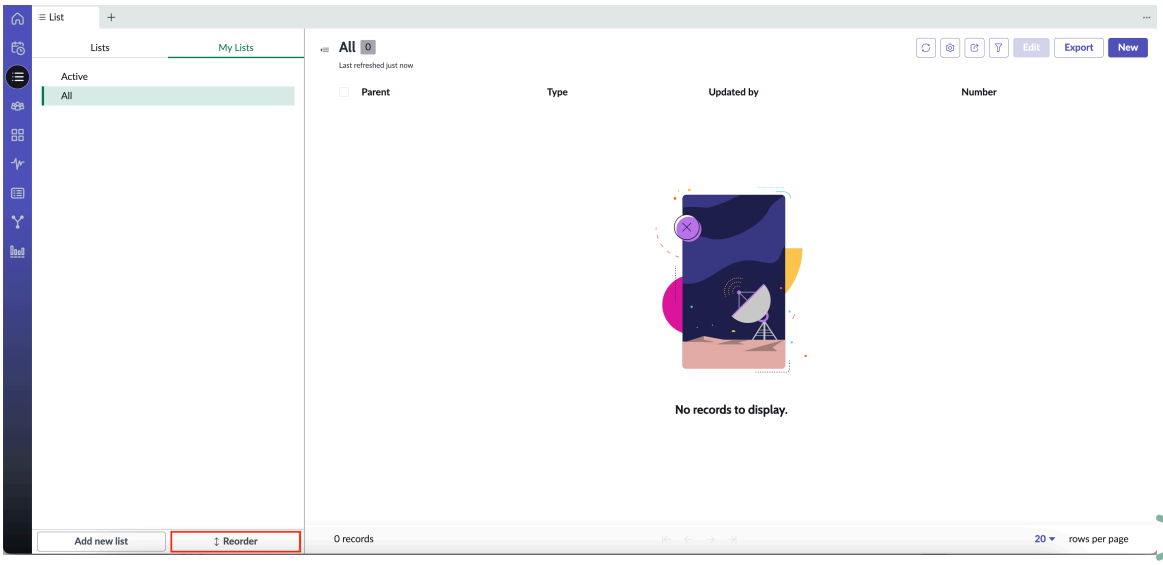
Erforderliche Rolle: itil

Prozedur

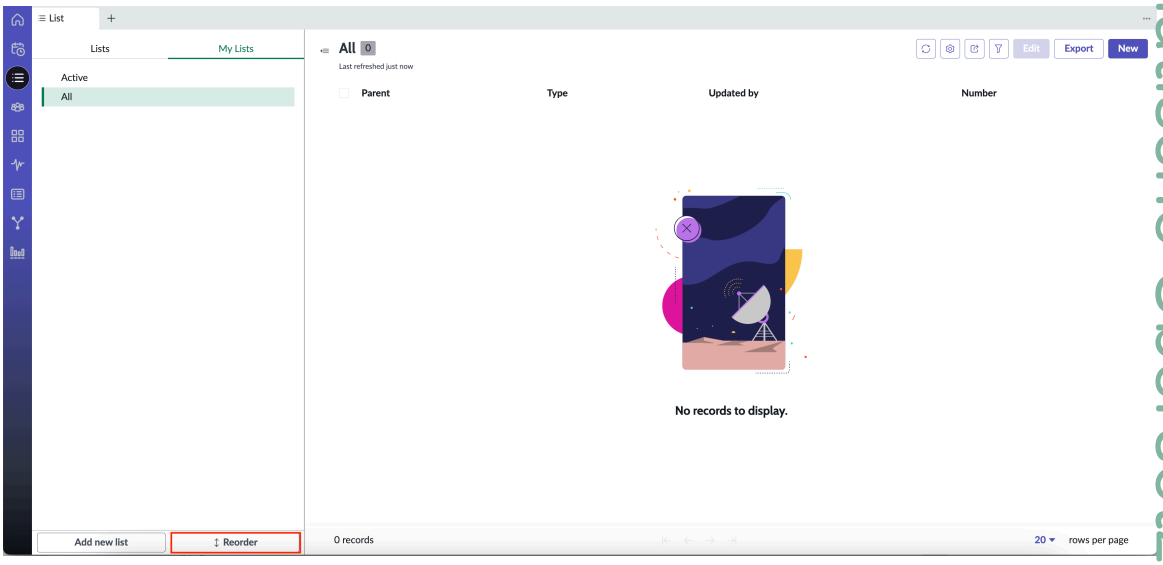
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .
3. Wählen Sie die Registerkarte **Meine Listen** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Liste aus, die Sie neu anordnen möchten.
5. Wählen Sie Aus **Neu Anordnen** Zum Anpassen der Position der Liste.



Löschen Sie eine Liste in Service Operations-Arbeitsbereich Für ITOM

Löschen Sie eine Liste, um Datensätze effizient zu verwalten, Ihren Arbeitsbereich zu deklarieren und organisierte Informationen zu verwalten.

Vorbereitungen

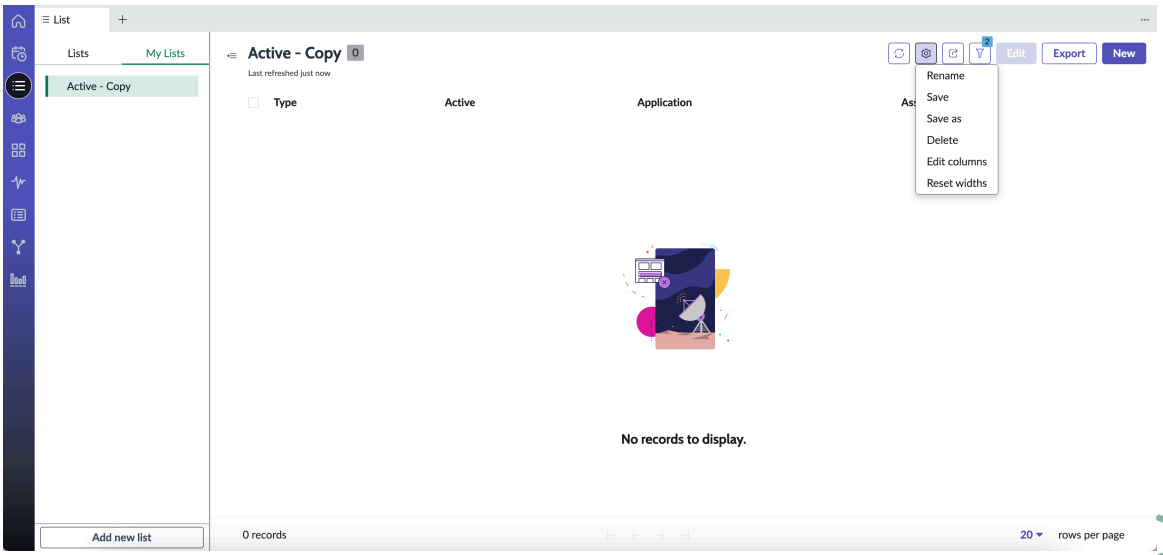
Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie die Liste aus, die Sie löschen möchten.
5. Wählen Sie das Einstellungssymbol ( ) Und dann auswählen **Löschen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie im Bestätigungs-Popup-Fenster aus **Löschen** .
   Die Liste wird gelöscht.

Zeigen Sie die einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich

Visualisieren Sie Beziehungen zwischen Konfigurationselementen (Configuration Items, CIs) und Warnungen mit Echtzeitaktualisierungen und detaillierten Auswirkungspfaden. Verbessern Sie die Problembehandlung und das proaktive Management, indem Sie schnell Ursachen und Abhängigkeiten für erkannte Services und Anwendungsservices identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_Operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die erweiterte Servicezuordnung in Service Operations-Arbeitsbereich Zeigt den betroffenen Pfad einer Warnung an, damit Sie ihre Auswirkungen auf einen Service schnell bewerten können. Sie können direkt über das Service-Dashboard, über den Vorschaubereich oder über einen betroffenen Service in der Express-Liste auf die erweiterte Servicezuordnung zugreifen.Die Servicezuordnung verfügt über mehrere Anzeigemodi:

- Für einen Service mit bis zu 60 CIs werden unabhängig vom Warnungsstatus alle CIs angezeigt.
- Für einen Service mit mehr als 60 CIs ohne Warnungen werden in der Zuordnung bis zu 60 CIs angezeigt.
- Für einen Service mit mehr als 60 CIs mit Warnungen zeigt die Karte den betroffenen Pfad der letzten Warnung mit dem höchsten Schweregrad an.

Sie können unabhängig von Warnungen auch eine breitere Ansicht der Servicetopologie in der Servicezuordnung für bis zu 250 CIs untersuchen. Wählen Sie für eine breitere Ansicht aus **Löschen** Und wählen Sie einen Modus mit bis zu 60 oder bis zu 250 Knoten aus.

Hinweis: Administratoren können die Legacy-Servicezuordnung weiterhin verwenden, um die Verbreitung des Schweregrads zu verwalten. Greifen Sie auf die Karte zu, indem Sie zu navigieren **Services** > **Anwendungsservices**an.

Automatische Übersetzung

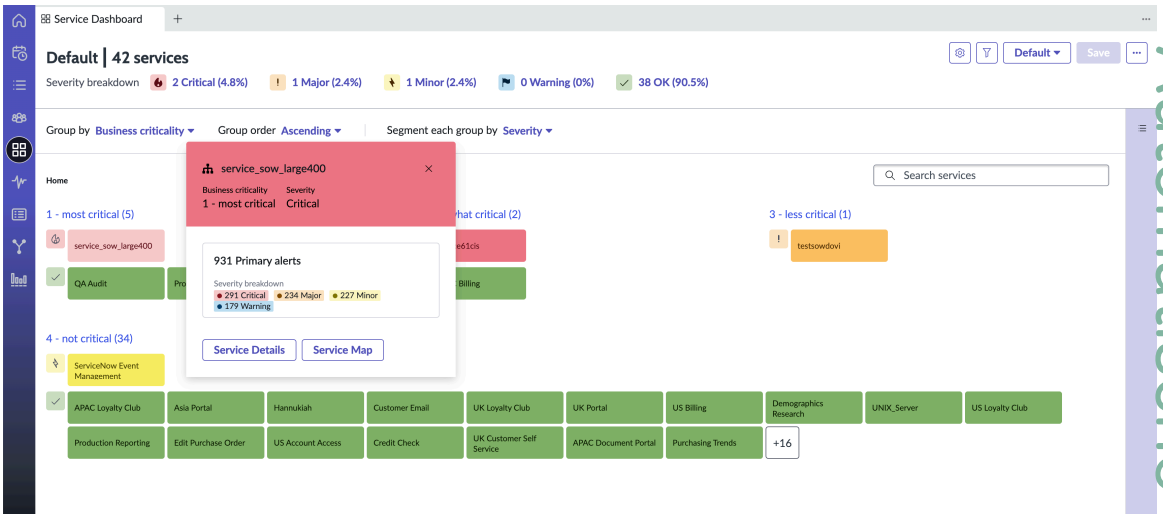
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol aus: .
   Die Seite „Service-Dashboard“ wird angezeigt.

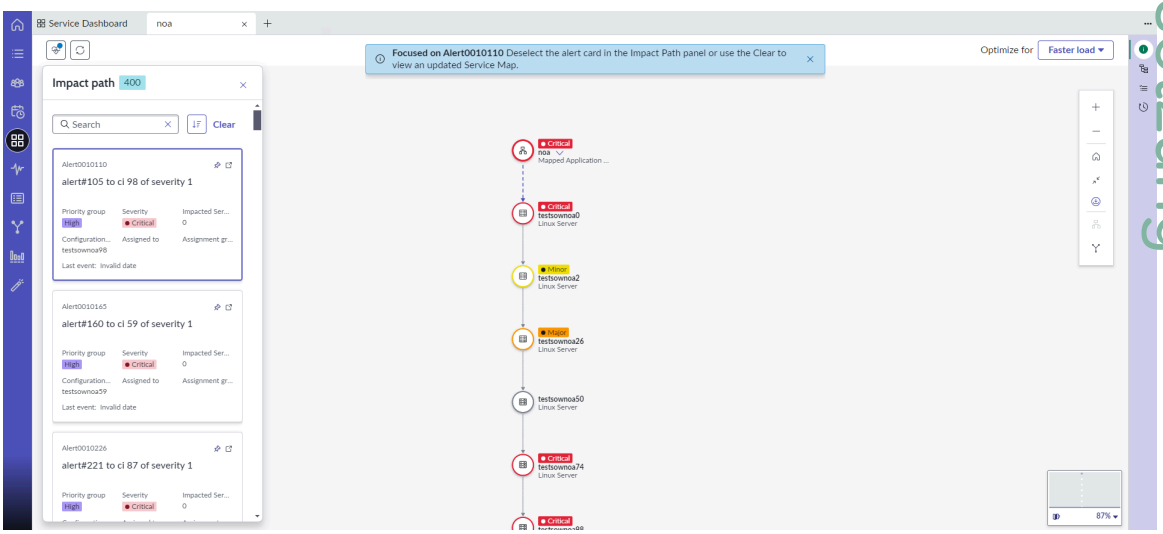
   Hinweis: Die Anwendungsservices, die im Service-Dashboard angezeigt werden, sind diejenigen, die der Liste Impact Filter Services hinzugefügt wurden. Weitere Informationen finden Sie unter Fügen Sie Anwendungsservices für die Auswirkungsberechnung hinzu.

3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftsrelevanz und der Schweregrad eines Service angezeigt.



4. Wählen Sie Aus **Servicezuordnung** .

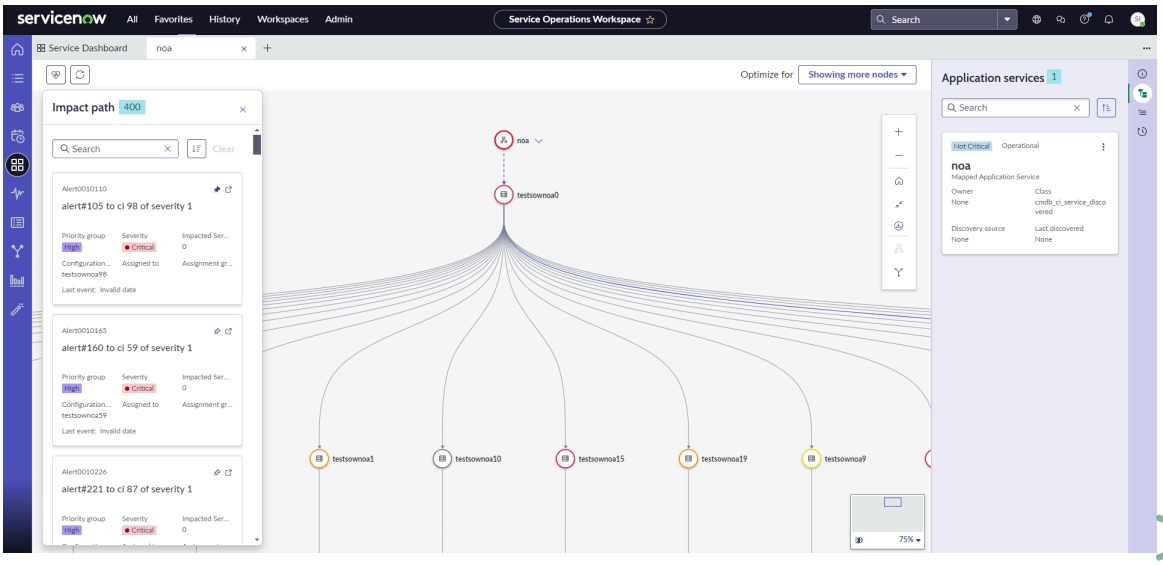
   Die Anwendungszuordnung wird zusammen mit den CI-Beziehungen angezeigt.



   Hinweis: Je nach Größe des Service zeigt die einheitliche Übersicht entweder die vollständige Zuordnung (wenn sie bis zu 60 CIs enthält) oder einen Auswirkungspfad, der zur kritischsten Warnung führt (für Karten mit mehr als 60 CIs). Bei großen Karten können Sie weitere CIs anzeigen, indem Sie die vorhandene Auswahl löschen und zu navigieren **Weitere Knoten werden angezeigt** Optimierungsoption.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

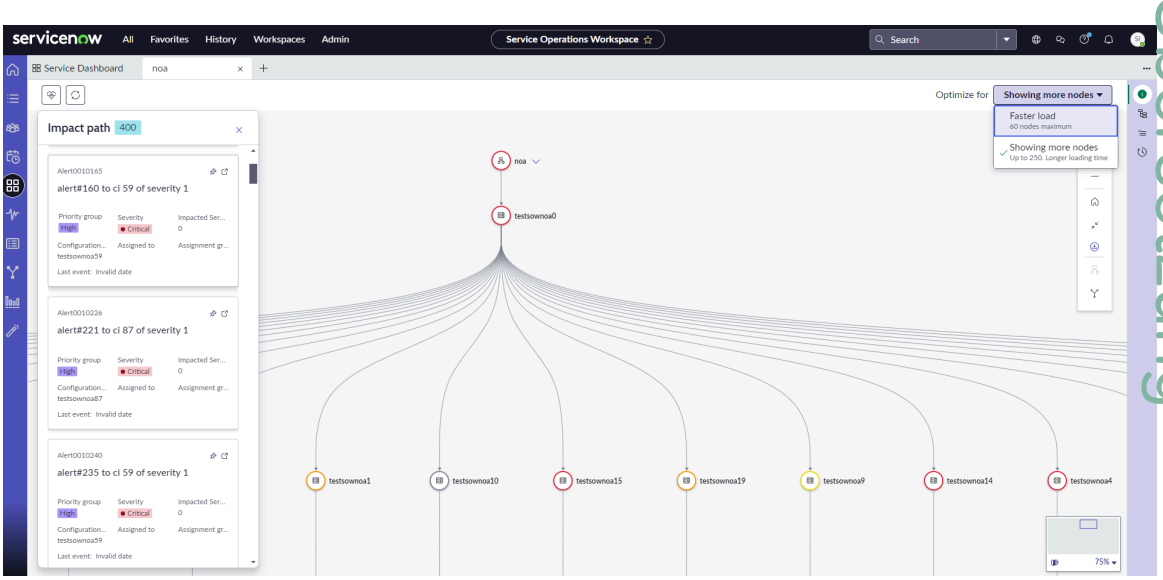


Wenn der Auswirkungspfadbereich geschlossen ist, können Sie ihn öffnen, indem Sie das Auswirkungspfadsymbol ( ).

5. Navigieren Sie zwischen Warnungen, indem Sie eine Warnungskarte auswählen.

Alternativ können Sie die Suchfunktion verwenden, um eine Warnung nach Beschreibung, CI oder Warnungsnummer zu suchen und sich auf ihren Auswirkungspfad zu konzentrieren.

Wenn Sie eine Warnungskachel auswählen, wird die einheitliche Übersicht für diese Warnung angezeigt. Um zur vollständigen Zuordnung für den Service zurückzukehren, wählen Sie aus **Löschen** .

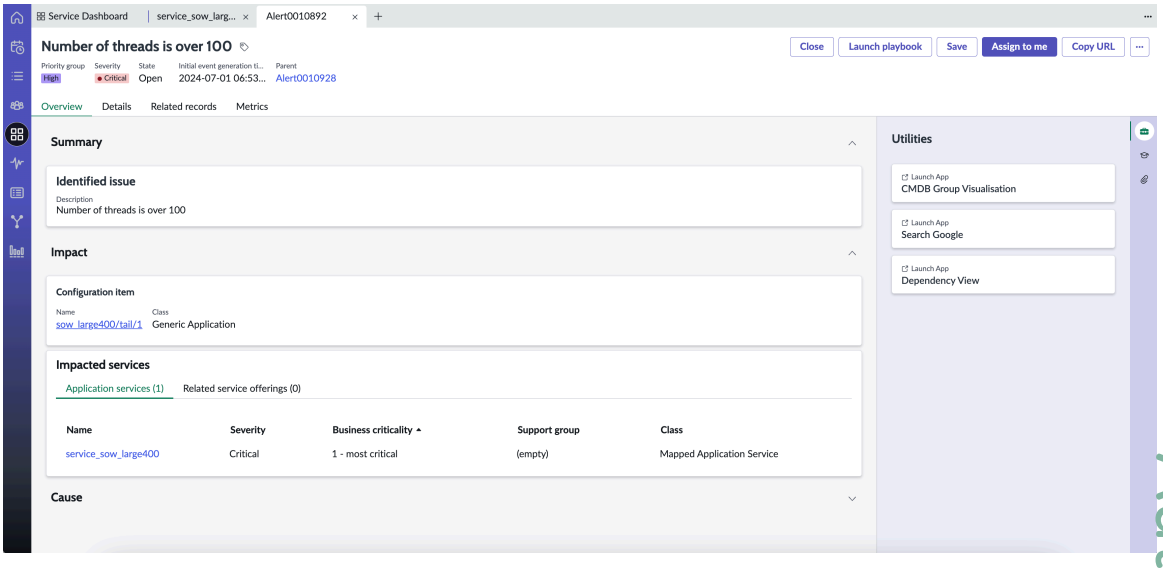


6. Um Warnungsdetails anzuzeigen, wählen Sie das Symbol „Datensatzformular öffnen“ ( ) Auf der Warnungskarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Seite mit den Warnungsdetails wird geöffnet.



Konfigurieren Sie die Einstellungen für die automatische Aktualisierung für Warnungslisten

Richten Sie Einstellungen für die automatische Aktualisierung von Warnungslisten ein, um Aktualisierungen in Echtzeit und eine nahtlose Überwachung sicherzustellen. Dies verbessert die Genauigkeit und Aktualität der angezeigten Informationen, ermöglicht schnellere Reaktionszeiten und verbessert die Zuverlässigkeit und Leistung des Systems insgesamt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden Warnungen in den Warnungslisten automatisch aktualisiert, immer wenn eine Aktion für eine Warnung ausgeführt wird. Sie können die Zeit in Sekunden konfigurieren, nach der die Warnungsliste nach einer Aktion aktualisiert wird. Sie können auch die automatische Aktualisierung deaktivieren oder konfigurieren, wie oft die Warnungsliste aktualisiert wird. Das ist nützlich, wenn ständig viele Warnungen verarbeitet werden, um ein zu häufiges Aktualisieren zu verhindern.

Hinweis: Legen Sie die Berechtigungen der Leserolle auf die Ereignismanagement-Benutzer (evt_mgmt_user) fest. Andernfalls ist die Eigenschaft nicht verfügbar.

Prozedur

1. Navigieren Sie zu **Alle** Und geben Sie im Suchfeld ein `sys_properties_list.do` .

   Das Fenster Systemeigenschaften wird geöffnet.

2. Suchen Sie nach den folgenden Eigenschaften, und konfigurieren Sie ihre Werte nach Bedarf.

Eigenschaften, um die Aktualisierung der Warnungsliste zu konfigurieren

Eigenschaft	Beschreibung
evt_mgmt.ai_refresh_time_to_wait_after_manual_action	Aktualisierungszeit der Warnungsliste (in Millisekunden), nachdem eine manuelle Aktion für die Warnung ausgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Wenn mehrere Aktionen nacheinander ausgeführt wurden, beginnt die Aktualisierungszeit neu nach der letzten Aktion. Dadurch wird sichergestellt, dass die Warnungsliste den aktuellen Status widerspiegelt und nach Anwenderinteraktionen umgehend aktualisiert wird.
evt_mgmt.ai_refresh_time_interval	Wenn innerhalb des definierten Zeitintervalls (5000 Millisekunden) eine Warnungsaktualisierung empfangen wird, erfolgt während dieses Zeitraums keine sofortige Aktualisierung für Aktualisierungen. Stattdessen führt das System am Ende des Zeitintervalls eine weitere Aktualisierung durch, um sicherzustellen, dass die Warnungsliste die neuesten verfügbaren Informationen widerspiegelt.
evt_mgmt.disable_lists_auto_refresh	Deaktiviert den automatischen Aktualisierungsprozess der Warnungslisten. Sie können eine neue Liste auf der Seite **Automatische Aktualisierung von Warnungslisten** erstellen, indem Sie im Navigationsbereich *em_alert_lists_auto_refresh.list* eingeben. Um eine automatische Aktualisierung der Liste zu verhindern, deaktivieren Sie die Option **Aktualisierung aktivieren**.

Warnungsmetriken konfigurieren

Konfigurieren Sie die Metriken, für die Sie sichtbar sein möchten Service Operations-Arbeitsbereich Warnungen oder verwenden Sie die mit dem Basissystem konfigurierten Metriken, um sich auf relevante Daten zu konzentrieren, um die Fehlerbehebung zu beschleunigen.

Vorbereitungen
Stellen Sie sicher, dass das Plugin „Metrik Intelligence“ (sn_metrics_ng) installiert ist.

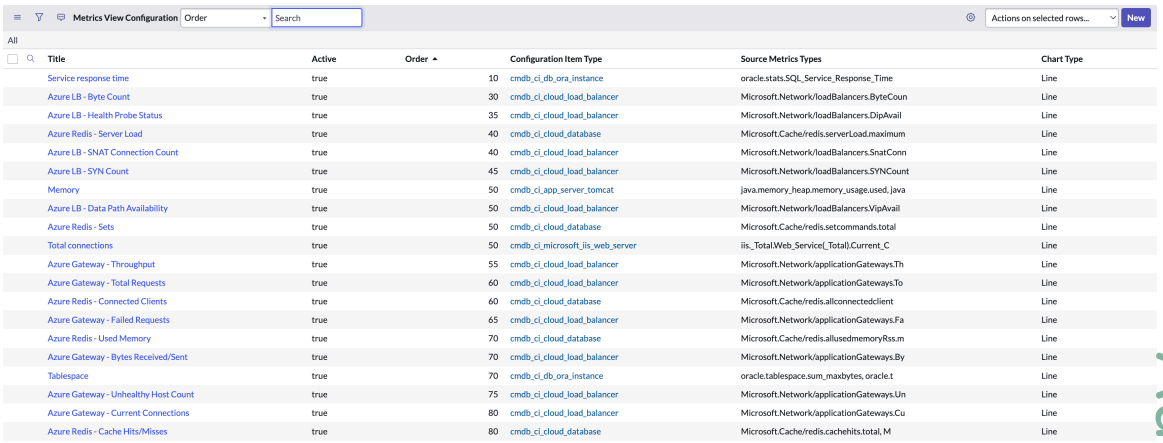
Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Konfiguration der Metrikansicht**an.



Title	Active	Order	Configuration Item Type	Source Metrics Types	Chart Type
Service response time	true	10	cmdb_ci_db_ora_instance	oracle.stats.SQL_Service_Response_Time	Line
Azure LB - Byte Count	true	30	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.ByteCoun	Line
Azure LB - Health Probe Status	true	35	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.DipAvail	Line
Azure Redis - Server Load	true	40	cmdb_ci_cloud_database	Microsoft.Cache/redis.serverLoad.maximum	Line
Azure LB - SNAT Connection Count	true	40	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.SnatConn	Line
Azure LB - SYN Count	true	45	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.SYNCount	Line
Memory	true	50	cmdb_ci_app_server_tomcat	java.memory_heap.memory_usage.used, java	Line
Azure LB - Data Path Availability	true	50	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.VipAvail	Line
Azure Redis - Sets	true	50	cmdb_ci_cloud_database	Microsoft.Cache/redis.setcommands.total	Line
Total connections	true	50	cmdb_ci_microsoft_iis_web_server	iis_Total.Web_Service(_Total).Current_C	Line
Azure Gateway - Throughput	true	55	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Th	Line
Azure Gateway - Total Requests	true	60	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.To	Line
Azure Redis - Connected Clients	true	60	cmdb_ci_cloud_database	Microsoft.Cache/redis.allconnectedclient	Line
Azure Gateway - Failed Requests	true	65	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Fa	Line
Azure Redis - Used Memory	true	70	cmdb_ci_cloud_database	Microsoft.Cache/redis.allusedmemoryRss.m	Line
Azure Gateway - Bytes Received/Sent	true	70	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.By	Line
Tablespace	true	70	cmdb_ci_db_ora_instance	oracle.tablespace.sum_maxbytes, oracle.t	Line
Azure Gateway - Unhealthy Host Count	true	75	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Un	Line
Azure Gateway - Current Connections	true	80	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Cu	Line
Azure Redis - Cache Hits/Misses	true	80	cmdb_ci_cloud_database	Microsoft.Cache/redis.cachehits.total, M	Line

2. Wählen Sie auf der Seite „Konfiguration der Metrikansicht“ die Option **Neu** aus.
3. Füllen Sie im Formular die Felder aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Formularfelder „Konfiguration der Metrikansicht“.
4. Wählen Sie **Absenden**.

Zeigen Sie die CI-Integrität in an Metric Explorer

Zeigen Sie die Integrität und Leistung des CI einer Warnung mit an Metric Explorer, Um Problembereiche im CI zu beheben.

Vorbereitungen

Alle Plugins im Zusammenhang mit Ereignismanagement, Metrikdaten, Und Metric Explorer, Sind erforderlich.

Erforderliche Rollen:

- Um in Metric Explorer auf Metrikdaten-Metriken zugreifen zu können, sind die Rollen workspace_agent und itil erforderlich.
- Zum Konfigurieren des Metrikensatzes, der in Metric Explorer für eine Klasse angezeigt wird, ist die Rolle admin oder evt_mgmt_admin erforderlich.

Warum und wann dieser Vorgang ausgeführt wird

Metric Explorer Zeigt Folgendes an Metrikdaten Daten:

- Diagramme, Kontrollgrenzen und Zusammenfassungen für Schlüsselmetriken für Konfigurationselemente (Configuration Items, CIs) an einem einzigen Ort.
- Zusammenfassung von Metriken für CIs mit Ressourcen in einer einzigen konsolidierten Zeitreihe
- Möglichkeiten für Administratoren zur Konfiguration, welche Metriktypen für jede CI-Klasse angezeigt werden

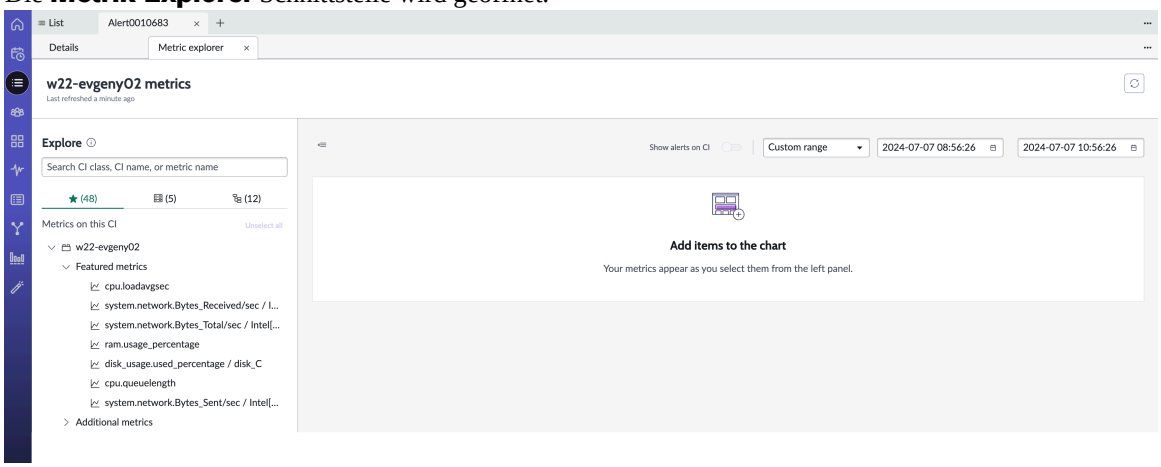
Metriken werden nur für Warnungen angezeigt, die ein CI enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .
3. Auswahlvorgang **Listen** > **Alerts** > **Alle Warnungen**an.
   Die Seite Warnungen – alle Warnungen wird geöffnet.
4. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird in einer separaten Registerkarte geöffnet, auf der angezeigt wird **Übersicht** Registerkarte.
5. Wählen Sie die Registerkarte **Metriken** aus.
6. Wählen Sie aus **Metrik-Explorer** Schaltfläche.
   Die **Metrik-Explorer** Schnittstelle wird geöffnet.



Hinweis: Sie können auch auf zugreifen **Metriken** Unterregisterkarte und **Metrik-Explorer** Schaltfläche beim Auswählen eines CI.

7. Wählen Sie im Abschnitt „Erkunden“ Metriken aus, um die Metriken im Diagrammformat anzuzeigen **Anwenderdefiniertes Diagramm** Abschnitt.
   Metriken werden gemäß den folgenden Unterregisterkarten aufgeteilt:

Unterregisterkarten des Abschnitts „Durchsuchen“

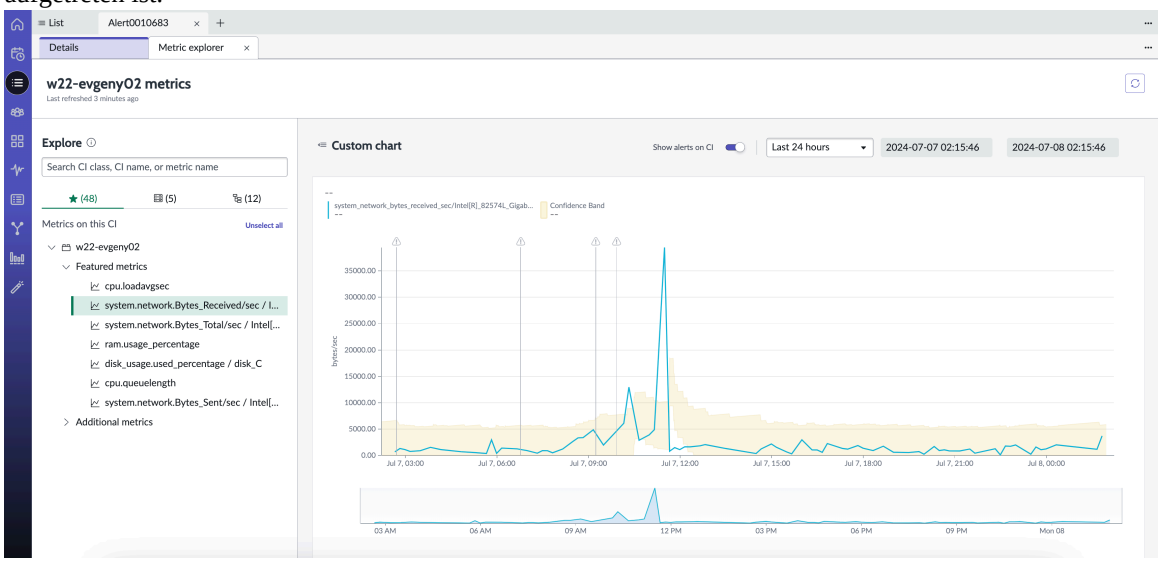
Unterregisterkarte	Beschreibung
★	Zeigt Metriken für das aktuelle CI an.
	Zeigt Metriken für andere CIs auf demselben Host an.
	Zeigt Metriken zu Einstiegspunkten an, die sich auf den Service beziehen, auf den sich das CI auswirkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterregisterkarte	Beschreibung
	Hinweis: Bei der Arbeit mit großen Mengen von Einstiegspunkten (100K oder mehr) kann das Sammeln von Einstiegspunktmetriken zu einer Verschlechterung des Systems führen. Um dies zu verhindern, erstellen Sie `sn_disable_selection_entry_point`Eigenschaft (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) Und legen Sie sie auf fest **Wahr** Zum Deaktivieren der Metriksammlung für Einstiegspunkte.

8. In **Anwenderdefiniertes Diagramm** Konfigurieren Sie einen Zeitbereich, für den Sie die angezeigten Metriken anzeigen möchten.
9. Benennen Sie Warnungen im anwenderdefinierten Diagramm, indem Sie aktivieren **Warnungen für CI anzeigen** Option.

   Ein Warnungssymbol (⚠) Wird oben im Diagramm an dem Punkt angezeigt, an dem die Warnung aufgetreten ist.



Zeigen Sie Trends der Warnungsmetrik in an Service Operations-Arbeitsbereich

Zeigen Sie die Metriken für eine Warnung an, und passen Sie den Zeitbereich an, um die Trends für die Warnung oder das zugehörige Konfigurationselement (Configuration Item, CI) anzuzeigen, wodurch eine genauere Analyse und eine rechtzeitige Entscheidungsfindung ermöglicht werden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Metrik Intelligence“ (sn_metrics_ng) installiert ist.

Konfigurieren Sie die Metriken, die für die Warnung angezeigt werden sollen, wie in Warnungsmetriken konfigurieren beschrieben.

Erforderliche Rolle: evt_mgmt_admin

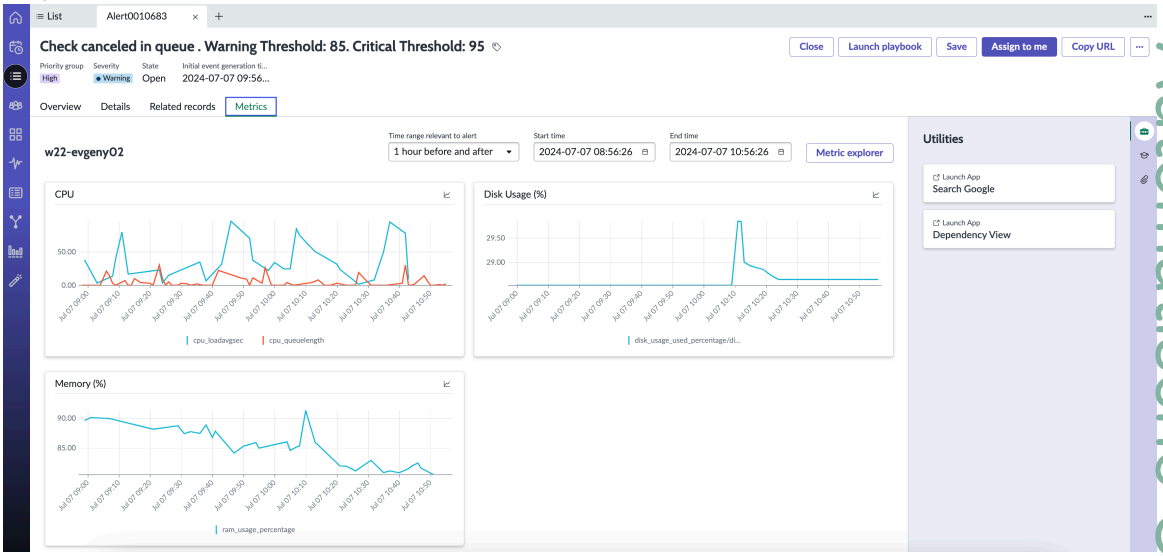
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

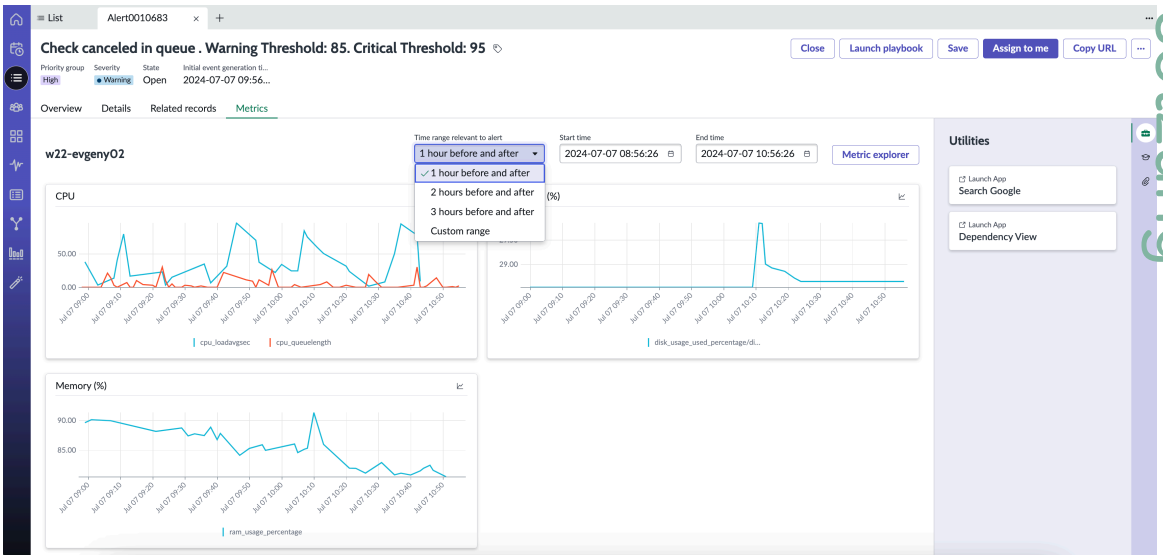
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol aus: .
3. Auswahlvorgang **Listen** > **Alerts** > **Alle Warnungen**an.
   Die Seite Warnungen – alle Warnungen wird geöffnet.
4. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird in einer separaten Registerkarte geöffnet, auf der angezeigt wird **Übersicht** Registerkarte.
5. Wählen Sie die Registerkarte **Metriken** aus.

Registerkarte „Metriken“



6. Konfigurieren Sie in den Feldern über den Metrikdiagrammen den Zeitbereich für die Metriken der Warnung.



Um die Metrikanzeige anzupassen, konfigurieren Sie die folgenden Eigenschaften auf der **Systemeigenschaften** > **Alle Eigenschaften** Seite:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

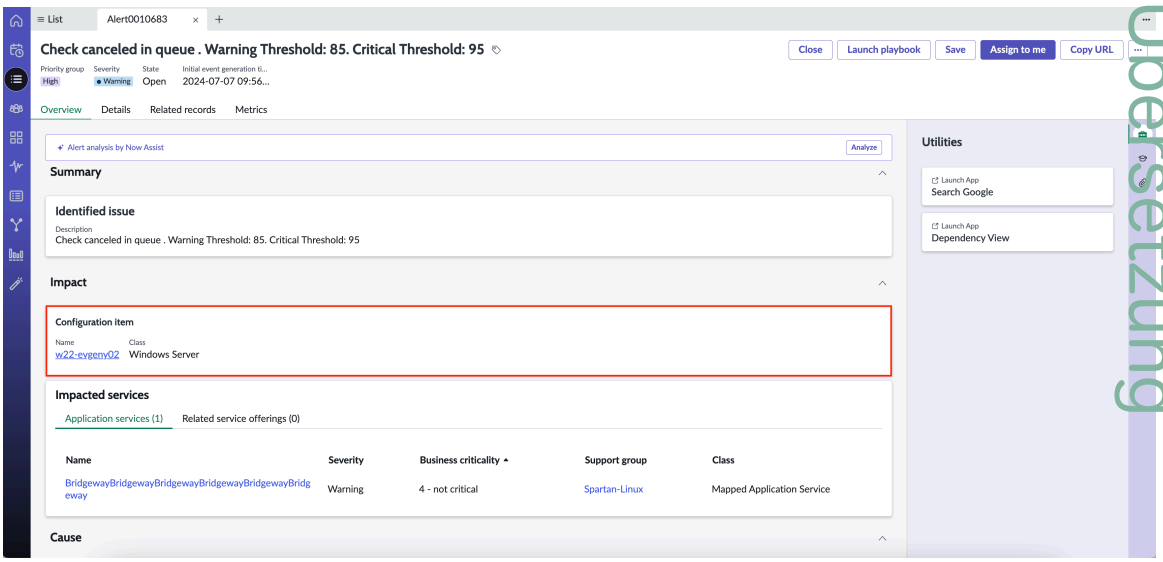
- `ws_metric.widgets_number_limit`: Geben Sie die Anzahl der Widgets/Datensätze an, die auf der Registerkarte „Metriken“ angezeigt werden können.
- `ws_metric.datasets_per_widget_limit`: Geben Sie die Anzahl der Diagramme/Datensätze an, die in einem Diagramm angezeigt werden dürfen.

Feldname	Beschreibung
Relevanter Zeitbereich für Warnung	Dauer für die Berechnung von Metriken rund um die Warnung.
Startzeit	Startdatum und -Uhrzeit für Metrikberechnungen.
Endzeit	Enddatum und -Uhrzeit für Metrikberechnungen.

7. Wählen Sie einen Parameter unter einem Diagramm aus, um die Daten des angegebenen Parameters im Diagramm auszublenden.
8. **Wahlweise:** Wählen Sie aus **Explorer Für Einblicke** Schaltfläche zum Anzeigen von Metriken durch Ziehen und Ablegen auf eine Zeitleiste.
9. Wählen Sie **Speichern**.
10. **Wahlweise:** Zeigen Sie einen Zeitbereich für das CI einer Warnung an.

    a. Wählen Sie die Registerkarte **Übersicht** aus.

    b. Unter dem Abschnitt Auswirkung auf auf auf der **Konfigurationselement** Wählen Sie den Link zum CI aus, der unter angezeigt wird **Name** Feld.



    c. Wählen Sie die Registerkarte **Metriken** aus.

    d. Wählen Sie **Speichern**.

Bereitschaftsplanung in Service Operations-Arbeitsbereich Für ITOM

ITOM Service Operations-Arbeitsbereich Unterstützt die Erstellung und Verwaltung Ihrer Rufbereitschaftsschichten und -Zeitpläne. Der Rufbereitschaftszeitplan bestimmt, wer zu einem bestimmten Zeitpunkt Rufbereitschaft hat. Erfahren Sie, wie Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rufbereitschaftskalender und Eskalationsrichtlinien konfigurieren, um eine rechtzeitige Reaktion auf kritische Probleme zu gewährleisten, Ausfallzeiten zu reduzieren und die Servicekonkontinuität zu gewährleisten. Die Optimierung dieser Prozesse verbessert die Teambereitschaft, minimiert Unterbrechungen und verbessert die Serviceverlässlichkeit.

Erste Schritte mit der Bereitschaftsplanung

Um die Bereitschaftsplanung für Warnungen zu aktivieren, integrieren Sie zuerst die Warnungstabelle [em_Alert] in die Liste „Konfiguration der Auslöserregeltabelle“. Weitere Informationen finden Sie unter Fügen Sie eine Warnungstabelle hinzu, um die Bereitschaftsplanung für zu aktivieren Service Operations-Arbeitsbereich Für ITOM.

Teams in Service Operations-Arbeitsbereich

Verwenden Sie das Teams-Menü ( ) in Service Operations-Arbeitsbereich, um alle Teams anzuzeigen. Wählen Sie eine Teamkarte aus, um den Zeitplan eines Teams anzuzeigen und zu verwalten und um Eskalationsrichtlinien und Teameinstellungen für eine ausgewählte Schicht zu definieren. Diese Funktion stellt sicher, dass Ihr Team weiß, wer Rufbereitschaft hat und verantwortlich ist, sodass Sie sicher sein können, dass kritische Warnungen oder Incidents bestätigt werden. Informationen zum Erstellen einer Schicht finden Sie unter Erstellen Sie Rufbereitschaftsschicht für Ihr Team .

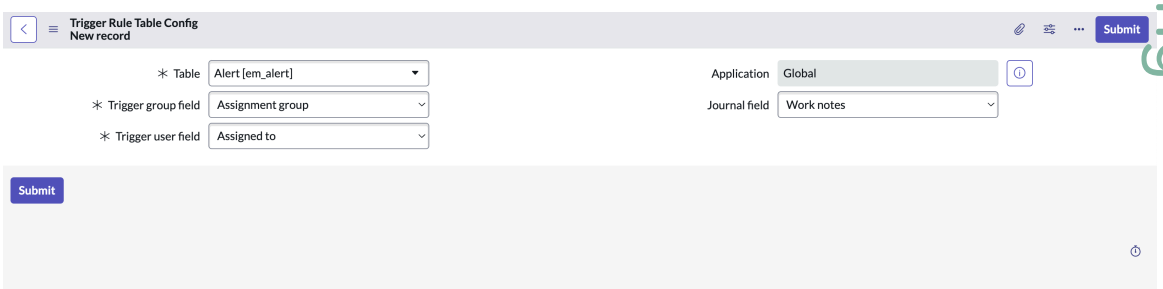
Fügen Sie eine Warnungstabelle hinzu, um die Bereitschaftsplanung für zu aktivieren Service Operations-Arbeitsbereich Für ITOM

Aktivieren Sie die Bereitschaftsplanung, indem Sie die Warnungstabelle [em_Alert] in die Liste „Konfiguration der Auslöserregeltabelle“ integrieren. Dies ermöglicht die Erstellung von Schichten und die Implementierung von Eskalationsauslösern und -Richtlinien, um sicherzustellen, dass Teams schnell auf Warnungen reagieren und die betriebliche Kontinuität aufrechterhalten können.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie zu **Alle** Und geben Sie im Suchfeld ein `Trigger_rule_table_cfg.list` .
   Die Seite „Konfigurationen der Auslöserregel-Tabelle“ wird geöffnet.
2. Füllen Sie die Felder im Formular mit den folgenden Werten aus.



   - In **Tabelle** Feld auswählen **Warnung [em_Alert]** .
   - In **Auslösergruppe** Feld auswählen **Zuweisungsgruppe** .
   - In **Auslöseranwender** Feld auswählen **Zugewiesen an** .
   - In **Journal** Feld auswählen **Arbeitsnotizen** .
3. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Erstellen Sie Rufbereitschaftsschicht für Ihr Team .

Service Operations-Arbeitsbereich für ITOM verwenden

Service Operations-Arbeitsbereich Für ITOM Bietet eine einheitliche Plattform, die verschiedene Anwendungen integriert und sich auf ein optimiertes Warnungsmanagement spezialisiert hat. Verwalten Sie IT Operations-Workflows nahtlos, während Sie Warnungen effizient verarbeiten, um optimale Leistung und Produktivität sicherzustellen.

Beim Einrichten von Service Operations-Arbeitsbereich, Es ist wichtig, beides zu konfigurieren IT Operations Management(ITOM) Für die Verwaltung von Warnungen und IT Service Management(ITSM) Für die Lösung von Incidents und die Bereitstellung von Services. Dieses integrierte Setup stellt den Zugriff auf das gesamte Funktionsumfang sicher und erleichtert ein umfassendes Management des IT-Betriebs und der Servicequalität.

Für weitere Informationen zu den Aufgaben in ITSM, Siehe Service Operations-Arbeitsbereich for ITSM .

Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM

Die Integrations Launchpad Zeigt alle an Ereignismanagement Connector-Integrationen, mit denen Anwender Ereignisse von externen oder internen Geräten abrufen oder veröffentlichen können. Dieser zentrale Hub vereinfacht Ereignismanagement Durch Konsolidierung von Integrationsoptionen an einem Ort.

Die Integrations Launchpad Optimiert den Prozess der Verwaltung und Verwendung von Ereignis-Connectors, verbessert die betriebliche Effizienz und stellt eine nahtlose Integration von Ereignisdaten aus verschiedenen externen Quellen sicher. Diese Zentralisierung hilft Anwendern, die Kontrolle und Transparenz über ihre zu verbessern EreignismanagementÖkosystem.

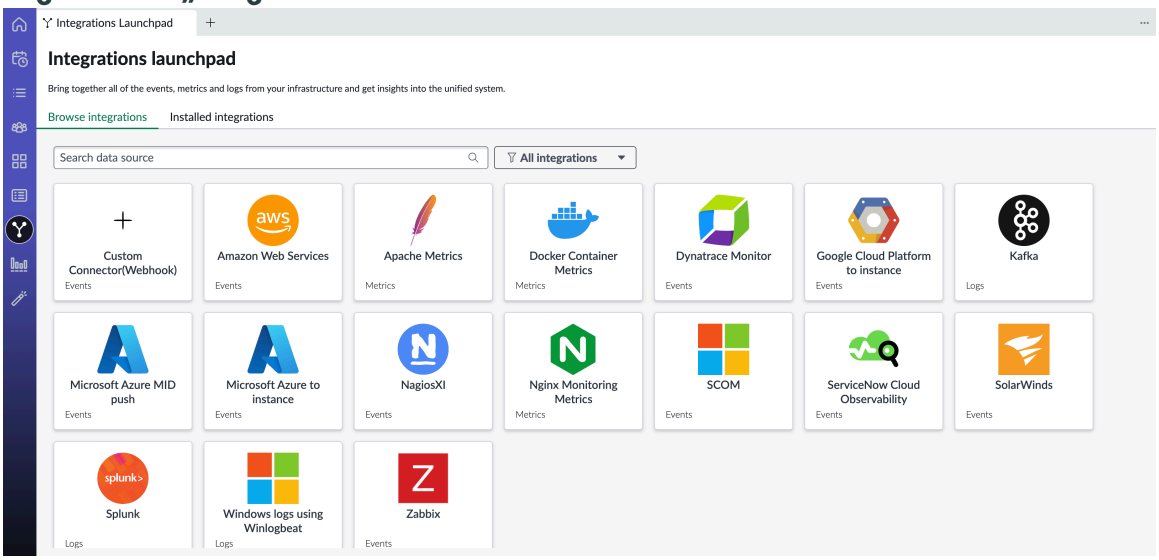
Registerkarte „Integrationen durchsuchen“

Zeigt alle Pull-, Push- und anwenderdefinierten Connector-Integrationen an, einschließlich Connectors, die über verfügbar sind ServiceNow Store und Drittparteien. Diese Registerkarte bietet folgende Funktionen:

- Suchfeld: Hilft Ihnen, durch Eingabe von Stichwörtern schnell eine bestimmte Datenquelle zu finden, was die Effizienz verbessert und Zeit spart.
- Liste „alle Integrationen“: Organisiert Integrationen in Kategorien wie alle Integrationen, Ereignisse (Push, Pull, anwenderdefiniert), Metriken (ACC-M), und Protokolle (HLA). Diese Kategorisierung erleichtert Anwendern das Durchsuchen der Liste und die Auswahl des relevanten Integrationstyps, den sie benötigen.

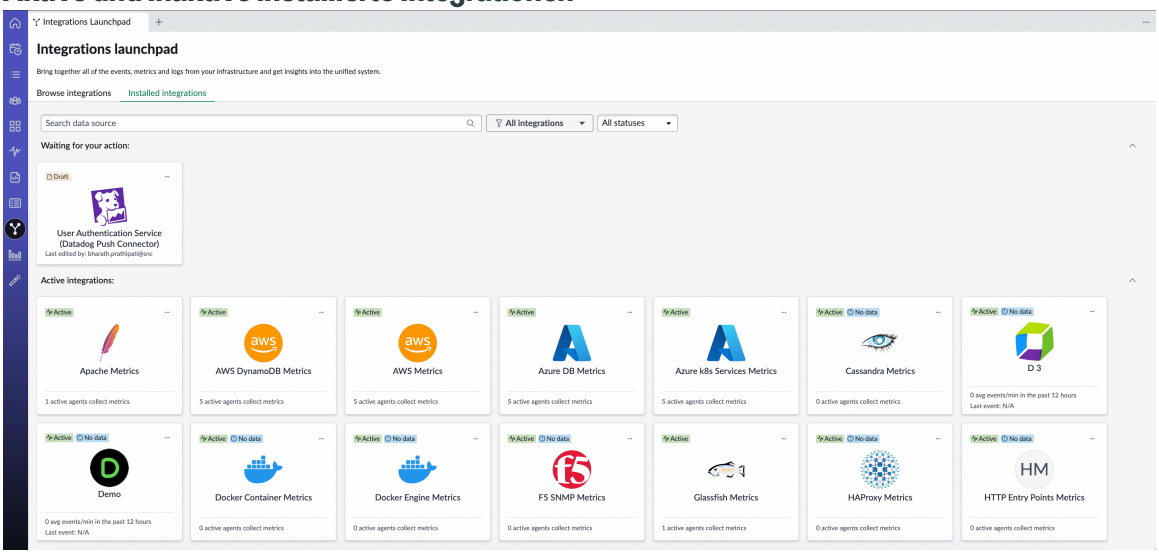
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Integrationen durchsuchen“



Registerkarte „installierte Integrationen“

Aktive und inaktive installierte Integrationen



Listet alle anwenderkonfigurierten Integrationen auf, sowohl aktiv als auch inaktiv. Diese Registerkarte bietet folgende Funktionen:

- Suchfeld: Hilft Anwendern, durch Eingabe von Stichwörtern schnell eine bestimmte Datenquelle zu finden, was die Effizienz verbessert und Zeit spart.
- Liste „alle Integrationen“: Organisiert Integrationen in Kategorien wie alle Integrationen, Ereignisse (Push, Pull, anwenderdefiniert), Metriken (ACC-M), und Protokolle (HLA). Diese Kategorisierung erleichtert Anwendern das Durchsuchen der Liste und die Auswahl des relevanten Integrationstyps, den sie benötigen.
- Liste „alle Status“: Ermöglicht das Filtern von Integrationen nach ihrem Status – alle Status, aktiv, Inaktiv, Entwurf oder keine Daten. Dies hilft Anwendern, Integrationen basierend auf ihrem aktuellen Status schnell zu identifizieren und zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsstatus und -Beschreibung

Status	Beschreibung
Alle Status	Alle Integrationsstatus
Aktiv	Aktive Integrationen, die erfolgreich installiert wurden
Inaktiv	Inaktive Integrationen, die erfolgreich installiert wurden
Entwurf	In Bearbeitung befindliche Integrationen mit einer Konfiguration, die gestartet, aber nicht abgeschlossen wurde
Keine Daten	Integrationen, die erfolgreich ohne Daten installiert wurden

Konfigurieren Sie einen Ereignis-Pull-Connector

Konfigurieren Sie Ereignis-Pull-Connectors, die ein Skript, eine Connector-Definition und eine Connector-Instanz erfordern, um Ereignisse von externen Geräten abzurufen. Diese Connectors automatisieren den Datenabrufprozess und stellen die nahtlose Integration externer Ereignisse in Ihr System für eine effiziente Überwachung und Verwaltung sicher.

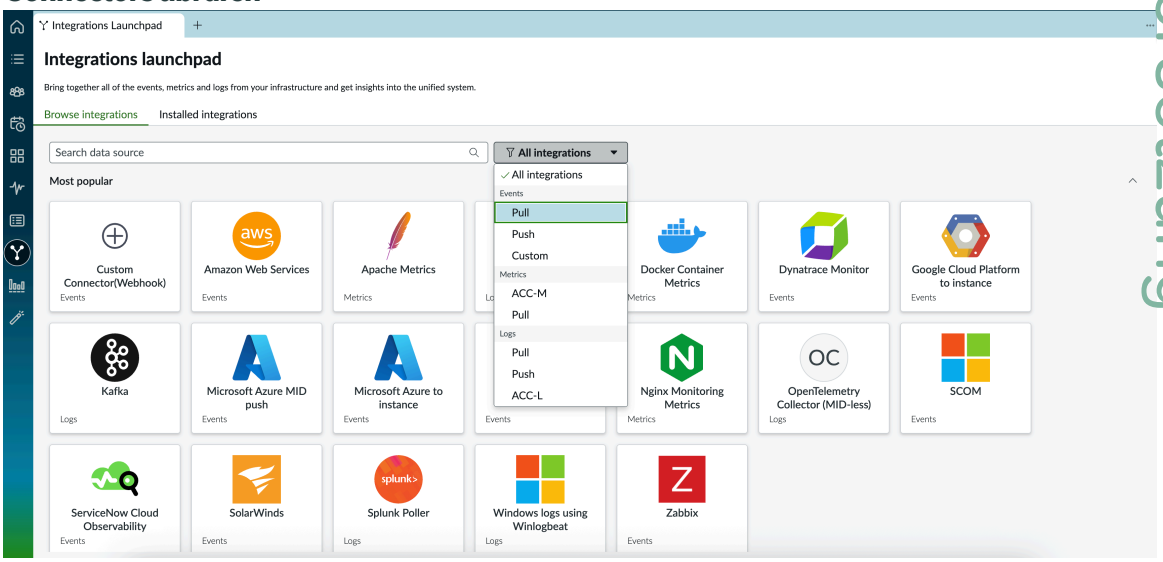
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen Durchsuchen** Wählen Sie die Registerkarte aus **Alle Integrationen** Dropdown-Liste, und wählen Sie aus **Abrufen** .
   Nur Pull-Connector-Kacheln werden angezeigt.

Connectors abrufen

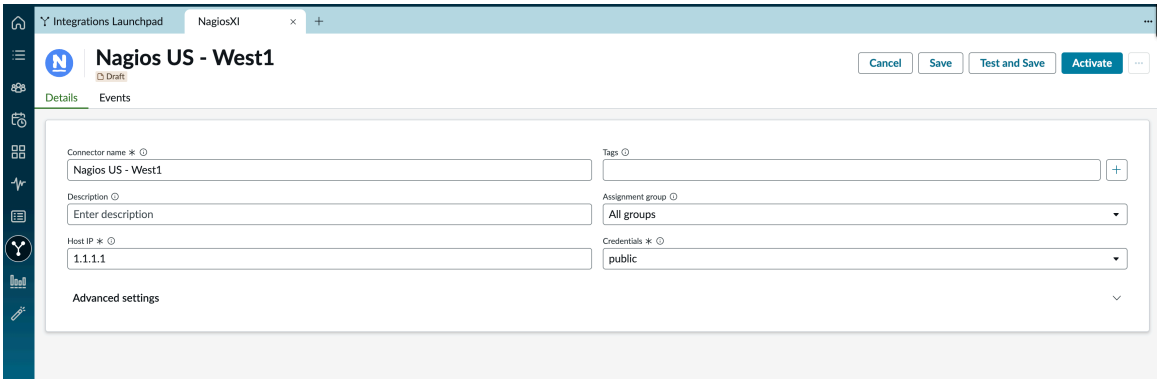


4. Wählen Sie eine Pull-Connector-Kachel aus.
   Wenn ein Popup-Menü geöffnet wird, wählen Sie die Daten aus, die von diesem Connector verfolgt werden sollen, und wählen Sie aus **Fahren Sie Fort** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailseite für Connectors abrufen



5. In **Details** Registerkarte im **Connector-Name** Feld einen eindeutigen Namen für den Connector-Typ eingeben.
6. **Wahlweise:** In **Tags** Geben Sie Tags ein, um Connectors dieses Typs im zu finden und zu identifizieren Express-Liste.

   Um zusätzliche Tags hinzuzufügen, wählen Sie das Plus-Symbol ( ) Neben **Tags** Feld. Das Fenster Tags hinzufügen wird geöffnet.

   a. In **Schlüssel** Feld einen Tag-Schlüssel eingeben.

   b. In **Wert** Feld einen Tag-Wert eingeben.

   c. Wählen Sie **Hinzufügen**.
7. **Wahlweise:** In **Beschreibung** Geben Sie kurze Informationen zu diesem Connector ein.
8. **Wahlweise:** Von **Zuweisungsgruppe** Wählen Sie in der Dropdown-Liste die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Connectors verantwortlich ist.
9. In **Host-IP** Geben Sie die IP-Adresse ein, die zur Auswahl des entsprechenden verwendet wird MID-Server Für die Kommunikation mit dem Ereignisquellhost.
   Sie können den Hostnamen anstelle der Host-IP verwenden.
10. Von **Anmeldeinformationen** Wählen Sie in der Dropdown-Liste die gültigen Anmeldeinformationen für den Zugriff auf den Ereignisquellhost aus.
    Um neue Anmeldeinformationen zu erstellen, wählen Sie aus **Erstellen Sie neue Anmeldeinformationen** Und fahren Sie mit dem Prozess fort.
11. **Wahlweise:** Wenn Sie Konfigurationen an bestimmte Anforderungen anpassen möchten, wählen Sie aus **Erweiterte Einstellungen** Und füllen Sie das Formular aus.

Feld	Beschreibung
Verbundener MID-Server	Legen Sie fest, ob das System die optimale auswählen soll MID-Server Oder wählen Sie ein bestimmtes aus MID-Server Selbst. Führen Sie nur aus, wenn Sie Änderungen an vornehmen müssen MID-Server Andernfalls lassen Sie es leer, und lassen Sie das System das Optimum auswählen MID-Server.
Zeitplan für Eventsammlung (Sekunden)	Geben Sie die Häufigkeit in Sekunden ein, die angibt, wie oft das System nach neuen Ereignissen aus der externen Ereignisquelle suchen soll. Der Wert darf nicht niedriger sein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	als die minimale Zeitplaneigenschaft, die standardmäßig 120 Sekunden beträgt.
Protokoll	Definiert das Kommunikationsprotokoll, das zum Abrufen von Ereignissen von externen Geräten verwendet wird.
Schweregrad_by_State_type	Bestimmt den Schweregrad, der Ereignissen basierend auf ihrem Statustyp zugewiesen ist.
time_zone	Gibt die Zeitzone an, die für die Aufzeichnung und Anzeige von Ereigniszeitstempeln verwendet wird.
offset_min	Legt den Zeitversatz für den Ereignisabruf fest, um eine genaue Synchronisierung sicherzustellen.
Port	Überprüfen Sie die Standardwerte für Ihren Connector-Typ, z. B. Portdetails oder Zeitformate, und ändern Sie sie nach Bedarf. Standardwerte aus Ihrem Connector sind ausgefüllt. Gibt die Portnummer an, die für die Kommunikation mit externen Geräten verwendet wird.
max_fetch_interval_min	Begrenzt das maximale Intervall zwischen Ereignisabrufvorgängen.
initial_sync_in_days	Legt die Dauer für den anfänglichen Synchronisierungsprozess beim Abrufen von Verlaufsdaten fest.

12. **Wahlweise:** Testen Sie den Connector, bevor Sie ihn aktivieren, indem Sie auswählen **Testen und speichern** .
13. Wählen Sie aus, um den Connector zu speichern **Speichern** .
14. Wählen Sie aus, um den Pull-Connector zu aktivieren **Aktivieren** .
    Der Pull-Connector ist aktiviert, und seine Kachel wird in angezeigt **Installierte Integrationen** Registerkarte.

Nächste Maßnahme

Um die erfolgreiche Konfiguration des Pull-Connectors und den Flow der Ereignisse in das System zu bestätigen, wählen Sie aus **Zugehörige Ereignisse** Registerkarte. Wenn das Setup erfolgreich ist, fahren Sie mit fort **Fügen Sie Automatisierung hinzu** Dient zum Einrichten einer Warnungsautomatisierung. Für Details zu **Zugehörige Ereignisse** Registerkarte, siehe Überprüfen Sie die Integrations- und Konfigurationsintegrität Informationen zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich Für ITOM.

Konfigurieren Sie einen Ereignis-Push-Connector

Integrieren Sie einen Ereignis-Push-Connector, um eine Verbindung zu einer externen Ereignisquelle herzustellen und Ereignisinformationen an Ihren zu übermitteln ServiceNow Instanz.

Vorbereitungen

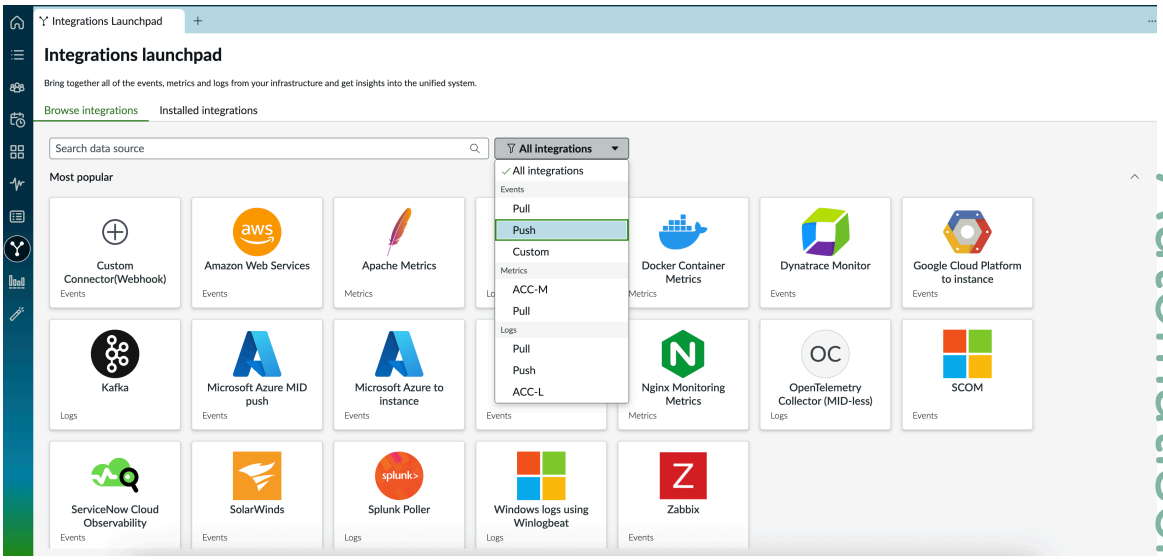
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

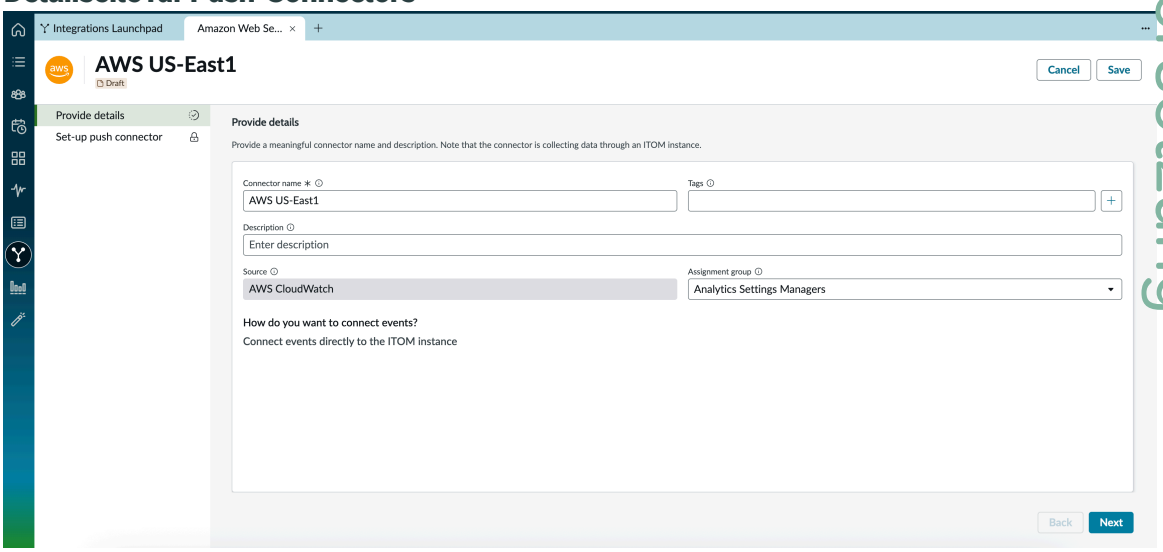
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen Durchsuchen** Wählen Sie die Registerkarte aus **Alle Integrationen** Dropdown-Liste, und wählen Sie aus **Veröffentlichen** .
   Nur Push-Connector-Kacheln werden angezeigt.

Push-Connectors



4. Wählen Sie eine Kachel vom Typ Push-Connector aus.
5. Geben Sie Details zum Connector-Typ auf der an **Geben Sie Details an** Bildschirm.

Detailseite für Push-Connectors



   a. In **Connector-Name** Feld einen eindeutigen Namen für den Connector-Typ eingeben.

   b. **Wahlweise:** In **Tags** Geben Sie Tags ein, um Connectors dieses Typs im zu finden und zu identifizieren Express-Liste.
   Um zusätzliche Tags hinzuzufügen, wählen Sie das Pluszeichen neben aus **Tags** Feld. Das Fenster Tags hinzufügen wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. In **Schlüssel** Feld einen Tag-Schlüssel eingeben.

ii. In **Wert** Feld einen Tag-Wert eingeben.

iii. Wählen Sie **Hinzufügen**.

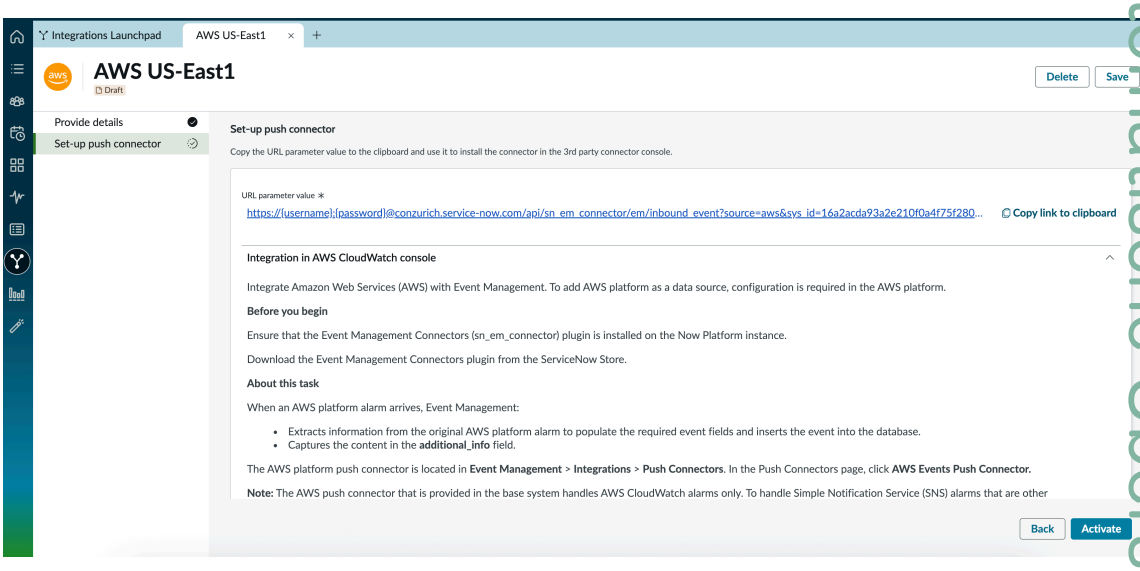
c. **Wahlweise:** In **Beschreibung** Geben Sie Informationen ein, um diesen Connector-Typ zu identifizieren.

d. Überprüfen Sie, ob der Lieferantenname in **Quelle** Feld ist korrekt.

e. **Wahlweise:** Von **Zuweisungsgruppe** Wählen Sie in der Dropdown-Liste die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Push-Connectors verantwortlich ist.

f. Wählen Sie **Weiter**.

Der Connector wird im Entwurfsmodus gespeichert, und der Prozess geht zum Abschnitt Push-Connector einrichten über.



6. In **URL-Parameterwert** Feld auswählen **In Zwischenablage kopieren** Dient zum Kopieren des automatisch generierten URL-Parameterwerts in die Zwischenablage.

   Diese URL wird von dem Code generiert, der von abhängt ServiceNow Instanz- und Connector-Typ zum Empfangen von Ereignissen vom Drittanbieter-Connector. Durch das Einfügen der URL in Ihre Drittanbieter-Connector-Konfiguration wird ein Webhook erstellt, mit dem Ereignisse an gesendet werden können ServiceNow Instanz.

7. Wählen Sie Aus **Aktivieren** Und wählen Sie dann aus **OK** .

8. In **Details** Zeigen Sie die Connector-Details und den URL-Link an, und befolgen Sie die Schritt-für-Schritt-Anweisungen, um Ihren Drittanbieter-Connector mit zu integrieren Ereignismanagement.
   Der Connector wird gespeichert, und eine Benachrichtigung wird gesendet, nachdem der Connector aktiv ist.

Nächste Maßnahme

Um die erfolgreiche Konfiguration des Pull-Connectors und des Flows von Ereignissen in das System zu bestätigen, wechseln Sie zu **Zugehörige Ereignisse** Registerkarte. Wenn das Setup erfolgreich ist, fahren Sie mit fort **Fügen Sie Automatisierung hinzu** Dient zum Einrichten einer Warnungsautomatisierung. Für Details zu **Zugehörige Ereignisse** Registerkarte, siehe Überprüfen Sie die Integrations- und Konfigurationsintegrität Informationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich Für ITOM.

Konfigurieren Sie einen anwenderdefinierten Ereignis-Connector

Authentifizieren Sie Ihren anwenderdefinierten Ereignis-Connector als Datenquelle, um die Übertragung von Ereignisinformationen an Ihren zu ermöglichen ServiceNow Instanz. Definieren Sie den anwenderdefinierten Connector, indem Sie seine Details und Zuordnungsfelder angeben. Dadurch können die extrahierten Informationen aus den Ereignisnachrichten Ihres anwenderdefinierten Connectors die erforderlichen Ereignisfelder ausfüllen. Erstellen Sie abschließend eine URL für den anwenderdefinierten Connector-Webhook, und geben Sie sie an.

Vorbereitungen

- Stellen Sie sicher, dass Ereignismanagement Plugin „Connectors“ (sn_em_Connector) ist auf installiert ServiceNow AI Platform Instanz. Weitere Informationen finden Sie unter Konfigurieren Ereignismanagement Connectors.
- Stellen Sie sicher, dass die Konfigurationselemente für die von Ihrem anwenderdefinierten Connector verwalteten Hosts in vorhanden sind ServiceNow AI Platform Instanz. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder Cloud-Discovery erkannt werden. Weitere Informationen finden Sie unter Auf Cloud-Umgebungen für ITOM-Produkte zugreifen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Um mit der Übertragung von Ereignisinformationen an Ihren zu beginnen ServiceNow-Instanz müssen Sie festlegen ServiceNow AI Platform Instanz als REST-Endpunkt mit einem Standard-Webhook in Ihrem anwenderdefinierten Connector.

Indem Sie Connector-Details und Zuordnungsfelder bereitstellen, definieren Sie den anwenderdefinierten Connector. Die extrahierten Informationen aus den Ereignisnachrichten des anwenderdefinierten Connectors füllen dann die erforderlichen Ereignisfelder aus und fügen das Ereignis in die Datenbank ein.

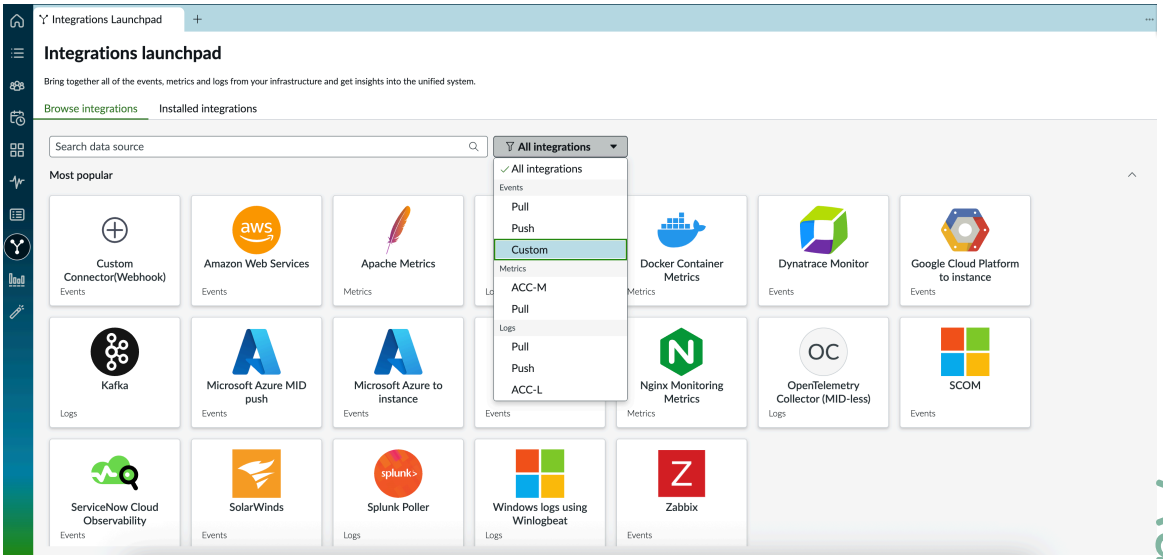
Die URL wird vom Code basierend auf generiert ServiceNow Instanz und der anwenderdefinierte Connector. Verwenden Sie diese URL, um einen Webhook zu erstellen, mit dem Ihr anwenderdefinierter Connector Ereignisse an den senden kann ServiceNow Instanz.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen Durchsuchen** Wählen Sie die Registerkarte aus **Alle Integrationen** Dropdown-Liste, und wählen Sie aus **Anwenderdefiniert** .
   Nur anwenderdefinierte Connector-Kacheln werden angezeigt.

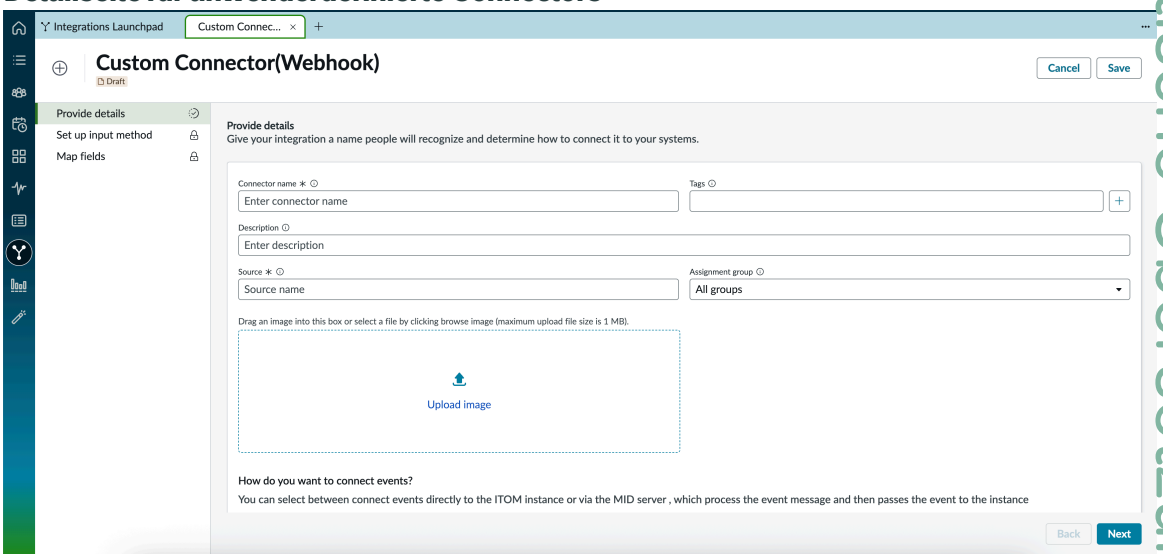
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Connectors



4. Wählen Sie eine Kachel vom anwenderdefinierten Connector-Typ aus.
5. Auf der **Geben Sie Details an** Seite, geben Sie die Details für den Connector an.

Detailseite für anwenderdefinierte Connectors



a. In **Connector-Name** Geben Sie einen eindeutigen Integrationsnamen für den Connector ein.

b. **Wahlweise:** In **Tags** Geben Sie Tags ein, um Connectors dieses Typs im zu finden und zu identifizieren Express-Liste.

   Um zusätzliche Tags hinzuzufügen, wählen Sie das Plus-Symbol ( ) Neben **Tags** Feld. Das Fenster Tags hinzufügen wird geöffnet.

   i. In **Schlüssel** Feld einen Tag-Schlüssel eingeben.

   ii. In **Wert** Feld einen Tag-Wert eingeben.

   iii. Wählen Sie **Hinzufügen**.

c. **Wahlweise:** In **Beschreibung** Geben Sie kurze Informationen zu diesem Connector ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. In **Quelle** Geben Sie den Lieferanten ein, der zum Sammeln von Ereignissen aus der externen Ereignisquelle verwendet wird.

Die **Quelle** Feld identifiziert den Connector und dient als Bezeichner, um die Quelle von Ereignissen und Warnungen zu erkennen, sobald der Connector aktiv ist.

e. Wahlweise: Von **Zuweisungsgruppe** Wählen Sie in der Dropdown-Liste die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Connectors verantwortlich ist.

6. Wahlweise: Ziehen Sie ein Bild, oder laden Sie es hoch, um es in Ihrer Connector-Kachel anzuzeigen.

- Ziehen Sie ein Bild in das Feld.
- Navigieren Sie zur Bilddatei, indem Sie auswählen **Bild hochladen** Und wählen Sie dann die Datei aus.

Die maximale Größe der Upload-Datei beträgt 1 MB.

7. Legen Sie fest, ob Sie Ereignisse direkt mit verbinden möchten ITOM Instanz oder über ein MID-Server.

- Zum Senden von Ereignissen direkt an ITOM Instanz, wählen Sie aus **Direkt zur ITOM-Instanz** .
- Zum Senden von Ereignissen über einen MID-Server, Das das Ereignis verarbeitet und dann an die Instanz übergibt, wählen Sie aus **Über den MID-Server** .

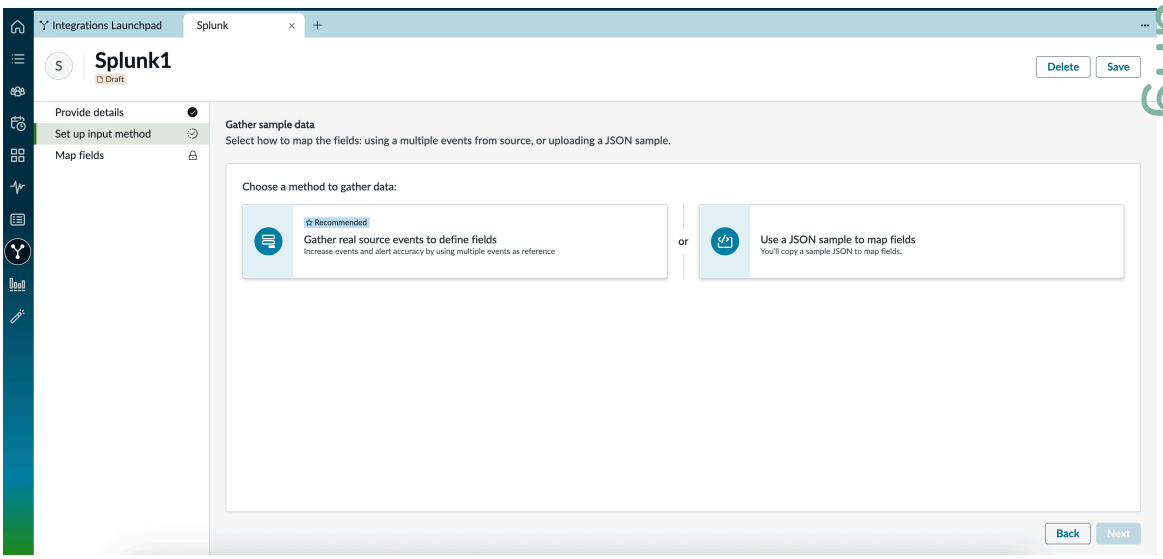
  Wenn ein MID-Server Ist vorhanden, aus **Wählen Sie MID-Server aus** Wählen Sie ein verfügbares Feld aus MID-Server Mit einem Ereignis-Listener verbunden.

  Wenn Sie erstellen müssen MID-Server, Und wählen Sie dann eine der folgenden Optionen aus.

  - **MID-Webservererweiterung konfigurieren**
  - **MID-Webservice-Ereignis konfigurieren – Collector-Kontext**

  Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren und MID-WebService-Event-Sammlerkontext konfigurieren.

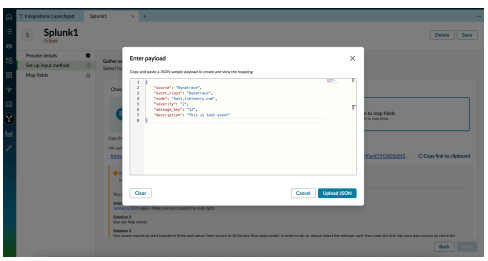
8. Wählen Sie **Weiter**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Auf der **Richten Sie die Eingabemethode ein** Wählen Sie eine Methode zum Sammeln von Ereignisdaten aus.

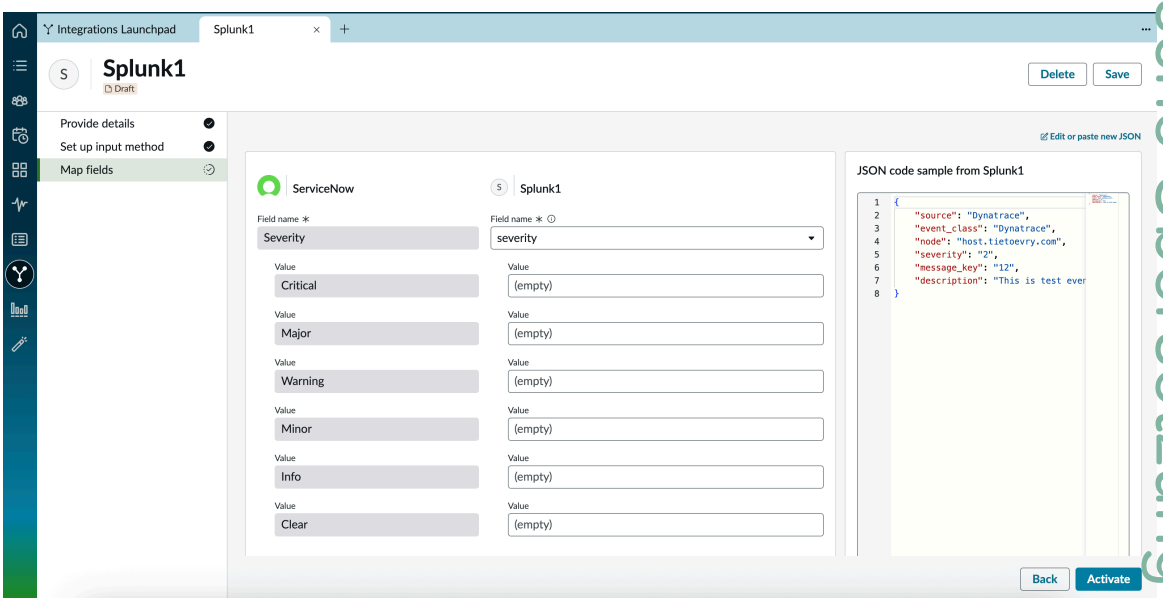
Methode	Beschreibung
Sammeln Sie echte Quellereignisse, um Felder zu definieren	**a.** Wählen Sie Aus **Erfassen Sie echte Quellereignisse, um Felder zu definieren** . **Hinweis:** Indem Sie Ereignisse aus echten Quellen aus Ihrem anwenderdefinierten Connector erfassen, erhöhen Sie die Genauigkeit von Ereignissen und Warnungen, indem Sie mehrere Ereignisse als Referenz zum Definieren der Felder verwenden. **b.** Wählen Sie Aus **In Zwischenablage kopieren** Und kopieren Sie die URL. **c.** Fügen Sie die URL in das Webhook-Setup Ihres anwenderdefinierten Connectors ein, um einen Webhook zu erstellen, mit dem Ihr anwenderdefinierter Connector Ereignisse an senden kann ServiceNow Instanz. Geben Sie Ihre Anmeldeinformationen für die Standardauthentifizierung in die Webhook-Konfiguration des Überwachungssystems ein (z. B. Anwendername und Passwort). Mit dem Webhook kann Ihr anwenderdefinierter Connector Ereignisse an die Instanz senden. **d.** Wählen Sie Aus **Überprüfen Sie auf Ereignisse** . Die Anzahl der Ereignisse wird angezeigt. Das Ereignis erstellt JSON-Dateien, die Sie nach der Auswahl durchsuchen können **Als Nächstes** .
JSON-Beispiel für die Zuordnung von Feldern verwenden	**a.** Wählen Sie Aus **Verwenden Sie ein JSON-Beispiel, um Felder zuzuordnen** . **Hinweis:** Wählen Sie diese Option nur aus, wenn Sie ein Beispiel-JSON haben. **b.** In **Geben Sie die Nutzlast ein** Dialogfeld kopieren und fügen Sie Ihre JSON-Beispielnutzlast ein, um die Zuordnung zu erstellen und anzuzeigen, um die Felder zuzuordnen.  **c.** Wählen Sie Aus **JSON hochladen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Beschreibung
	d. Wählen Sie Aus **Bearbeiten oder fügen Sie neu es JSON ein** Zum Bearbeiten der JSON, die Sie hochgeladen haben, oder zum Einfügen einer neuen. **e.** Wählen Sie Aus **In Zwischenablage kopieren** Und kopieren Sie die URL. **f.** Fügen Sie die URL in das Webhook-Setup Ihres anwenderdefinierten Connectors ein, um einen Webhook zu erstellen, mit dem Ihr anwenderde–finierter Connector Ereignisse an senden kann ServiceNow Instanz. Geben Sie Ihre Anmeldein–formationen für die Standardauthentifizierung in die Webhook-Konfiguration des Überwachungs–systems ein (z. B. Anwendername und Pass–wort). Mit dem Webhook kann Ihr anwender–definierter Connector Ereignisse an die Instanz senden.

10. Wählen Sie **Weiter**.
    Die Seite wird geöffnet, auf der Sie Felder zuordnen können.



11. Auf der **Felder zuordnen** Seite geben Sie in der Spalte Connector-Feldnamen mindestens einen Wert ein, der den in aufgeführten Schweregradwerten zugeordnet ist ServiceNow **Schweregrad** Feldspalte.

12. Auf der **Felder zuordnen** Seite geben Sie in der Spalte Connector-Feldnamen mindestens einen Wert ein, der den in aufgeführten Schweregradwerten zugeordnet ist ServiceNow **Schweregrad** Feldspalte.

    Sie können den Schweregradwert aus dem JSON-Codebeispiel eingeben. Um einen Schweregradwert festzulegen, müssen Sie mit der Nutzlast Ihres anwenderdefinierten Connectors und den Typen des unterstützten Schweregrads vertraut sein. Die Schweregradwerte der empfangenen Ereignisse müssen mit den generierten Ereignissen in Ihrem System übereinstimmen.

    Aktivieren Sie das System, Ereignisse korrekt aus eingehenden Daten zu erstellen, indem Sie die Felder in Ihrem JSON-Codebeispiel dem zuordnen ServiceNow Felder. Die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad Und **Nachrichtenschlüssel** Informationen werden automatisch ausgefüllt, um Zeit und Aufwand zu sparen. Die **Nachrichtenschlüssel** Stellt den richtigen Bezeichner für die Ereignisse bereit, um sicherzustellen, dass die Deduplizierung ordnungsgemäß funktioniert und keine redundanten Warnungen generiert werden.

13. **Wahlweise:** Um mehrere JSON-Dateien anzuzeigen, wählen Sie den Pfeil über dem JSON-Beispiel aus.
14. **Wahlweise:** Im Abschnitt „andere Felder“ in Ihr Connector Spalte: Geben Sie anwenderdefinierte Ereignisparameter an, die optional sind, aber zusätzliche Informationen zum Ereignis bereitstellen. Wenn Sie die optionalen Informationen nicht angeben möchten, lassen Sie das Feld leer.

    a. In **Beschreibung** Feld eine aussagekräftige Warnungsbeschreibung eingeben.

    b. In **Metrikname** Geben Sie einen Metriknamen ein, mit dem Sie Ereignisse den Leistungsmetriken oder KPIs zuordnen können, die die Warnung ausgelöst haben.

    c. In **Knoten** Feld einen Knotenwert eingeben, der für die CI-Bindung verwendet werden soll.

    d. In **Ereigniszeit** Geben Sie die Erstellungszeit des anwenderdefinierten Connector-Ereignisses ein. Wenn die Ereigniszeit nicht zugeordnet ist, verwendet das System die standardmäßige Ereigniszeit.

    e. In **Einstellungen für Ereigniszeit** Feld das Zeitformat und die Ereigniszeitzone auswählen.
    - **Zeitformat** : Ein GlideDateTime-Feld im UTC- oder GMT-Format mit einer maximalen Länge von 40 Zeichen.
    - **Zeitzone** : Zeiten werden in Coordinated Universal Time (UTC) gespeichert und global basierend auf der Systemzeitzone angezeigt.

15. Aktivieren und speichern Sie den Connector, indem Sie auswählen **Aktivieren** Und wählen Sie dann aus **OK** Im Bestätigungs-Popup-Fenster.
    Sie können die Connector-Details in anzeigen **Details** Registerkarte und Ihre Feldzuordnungen auf der **Feldzuordnung** Registerkarte.

Ergebnis

Nachdem der Connector aktiviert wurde, werden Ereignisse von Ihrer anwenderdefinierten Connector-Konsole in die übertragen ServiceNow Instanz. Das Plugin extrahiert Informationen aus der ursprünglichen anwenderdefinierten Connector-Ereignisnachricht, um die erforderlichen Ereignisfelder auszufüllen, und fügt das Ereignis in die Datenbank ein. Um die Ereignisse in anzuzeigen ServiceNow AI Platform Instanz, navigieren Sie zu alle Ereignisse. Weitere Informationen finden Sie unter Events anzeigen.

Nächste Maßnahme

Um sicherzustellen, dass der Prozess erfolgreich abgeschlossen wurde und Ereignisse in das System fließen, zeigen Sie die zugehörigen Ereignisse im an **Zugehörige Ereignisse** Registerkarte. Wenn das Setup erfolgreich ist, fahren Sie mit fort **Fügen Sie Automatisierung hinzu** Dient zum Einrichten einer Warnungsautomatisierung. Informationen zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich Für ITOM.

Konfigurieren Sie einen Metrik-Pull-Connector

Konfigurieren Sie Metrik-Pull-Connectors, die ein Skript, eine Connector-Definition und eine Connector-Instanz erfordern, um Metriken aus externen Quellen abzurufen. Diese Connectors automatisieren den Datenabrufprozess und stellen die nahtlose Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

externer Metriken in Ihr System für eine effiziente Überwachung und Leistungsanalyse sicher.

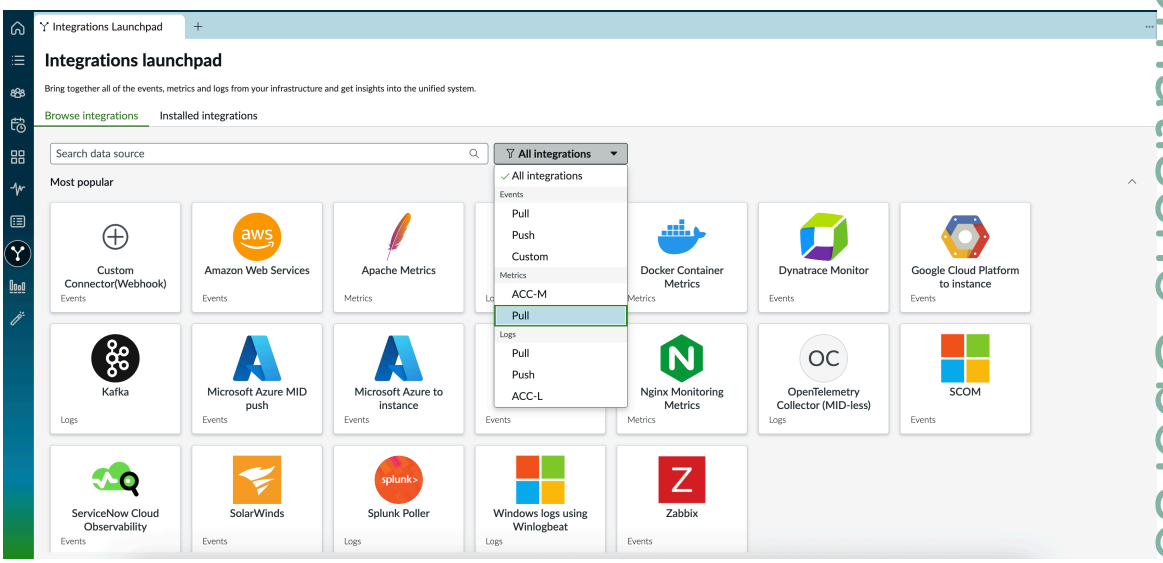
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Die neue UI zum Konfigurieren des Metrik-Pull-Connectors ist derzeit nur für den SolarWinds Metric Connector verfügbar. Für alle anderen Metrik-Connectors verwendet die Konfiguration weiterhin die UI der Plattformtabelle.

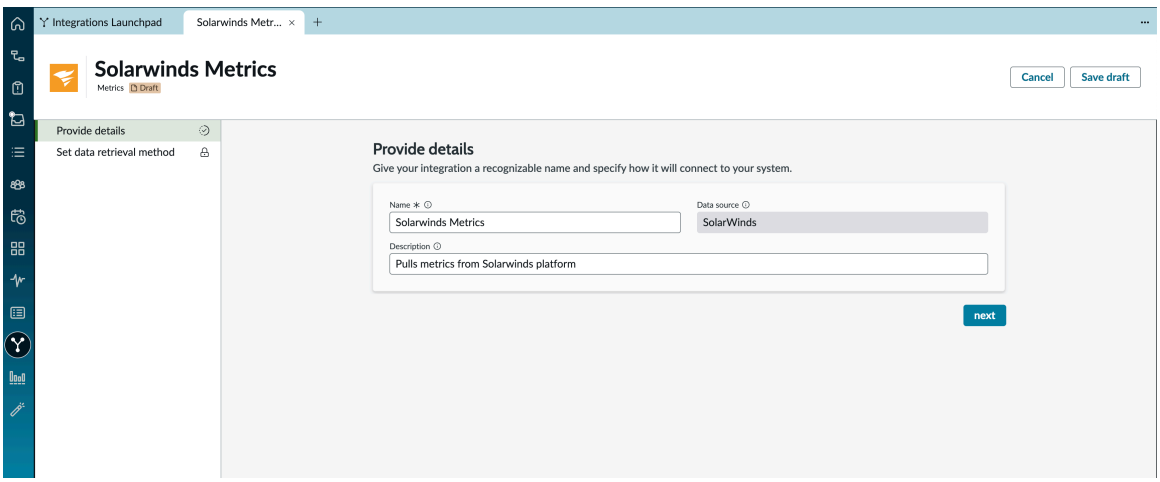
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen Durchsuchen** Wählen Sie die Registerkarte aus **Alle Integrationen** Dropdown-Liste, und wählen Sie aus **Metriken** > **Abrufen**an.



Nur Metrik-Pull-Connector-Kacheln werden angezeigt.

4. Wählen Sie eine Pull-Connector-Kachel aus.
Wenn ein Popup-Menü geöffnet wird, wählen Sie die Daten aus, die von diesem Connector verfolgt werden sollen, und wählen Sie aus **Fahren Sie Fort** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In **Geben Sie Details an** Geben Sie die folgenden Informationen ein, und wählen Sie aus **Als Nächstes** .
   - In **Name** Feld einen eindeutigen Namen für den Connector-Typ eingeben.
   - In **Datenquelle** Feld, wird die externe Quelle zum Abrufen von Metriken basierend auf dem von Ihnen ausgewählten Kacheltyp automatisch ausgefüllt.
   - In **Beschreibung** Geben Sie kurze Informationen zu diesem Connector ein.
6. In **Legen Sie die Datenabrufmethode fest** Geben Sie die folgenden Informationen ein:
   - In **Host-IP** Geben Sie die IP-Adresse ein, die zur Auswahl des entsprechenden verwendet wird MID-Server Für die Kommunikation mit dem Ereignisquellhost.
   - Von **Anmeldeinformationen** Wählen Sie in der Dropdown-Liste die gültigen Anmeldeinformationen für den Zugriff auf den Ereignisquellhost aus.
   - In **Zeitplan für Metriksammlung (Sekunden)** Feld das Zeitintervall (in Sekunden) eingeben, in dem der Connector Metriken vom Quellhost abruft.
   - In **MID-Server** Wählen Sie ein aus MID-Server Die Metrikdaten aus externen Tools sammelt und sicher an sendet ServiceNow.

     Wenn keine verfügbar sind, stellen Sie sicher, dass eines installiert ist, ausgeführt wird und über die erforderlichen Fähigkeiten verfügt.

     Hinweis: Sie können mehrere MID-Server auswählen. Das System weist zufällig eine als primäre zu und verwendet die anderen als Sicherungen.
7. **Wahlweise:** Wenn Sie Konfigurationen an bestimmte Anforderungen anpassen möchten, wählen Sie aus **Erweiterte Einstellungen** Und füllen Sie das Formular aus.

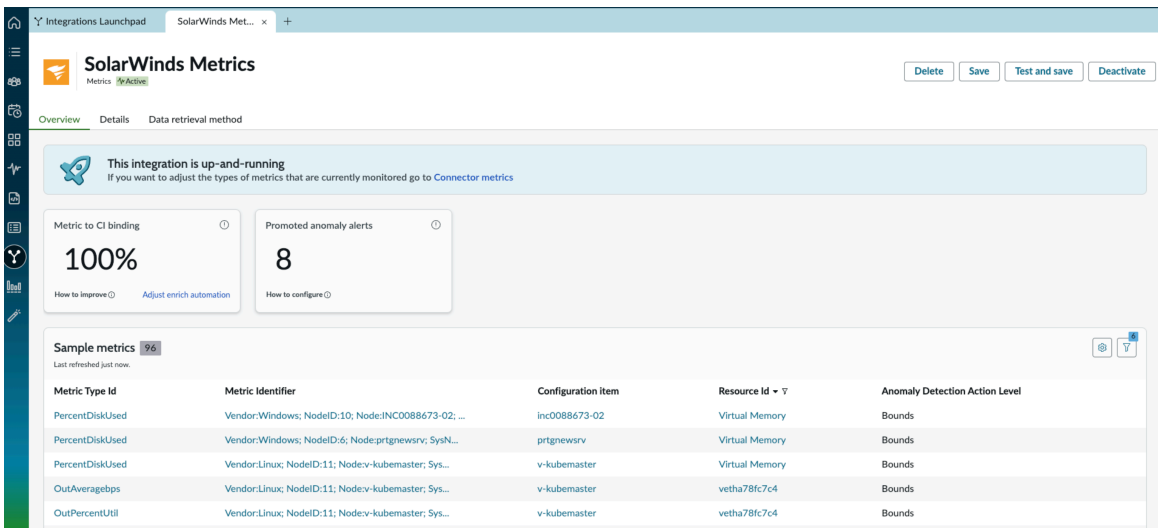
Feld	Beschreibung
Max. Zeilen pro Abfrage	Häufigkeit in Sekunden, die angibt, wie oft das System nach neuen Metriken aus der externen Ereignisquelle suchen soll. Der Wert darf nicht niedriger sein als die minimale Zeitplaneigenschaft, die standardmäßig 120 Sekunden beträgt.
Max. Abrufintervall (Minuten)	Begrenzt das maximale Intervall zwischen Ereignisabrufvorgängen.
Offset (in Minuten)	Legt den Zeitversatz für den Ereignisabruf fest, um eine genaue Synchronisierung sicherzustellen.
Port	Gibt die Portnummer an, die für die Kommunikation mit externen Geräten verwendet wird. (Optional) Überprüfen Sie die Standardwerte für Ihren Connector-Typ, z. B. Portdetails oder Zeitformate, und ändern Sie sie nach Bedarf. Standardwerte aus Ihrem Connector sind ausgefüllt.
Protokoll	Definiert das Kommunikationsprotokoll, das zum Abrufen von Ereignissen von externen Geräten verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Debugging	○ Debuggen: Stellt detaillierte Protokolle für die Fehlerbehebung bereit. ○ Protokollnutzlast: Zeigt Rohprotokolldaten an. Verwenden Sie nur zum Debugging, da es schnell gefüllt werden kann MID-Server Protokolle.

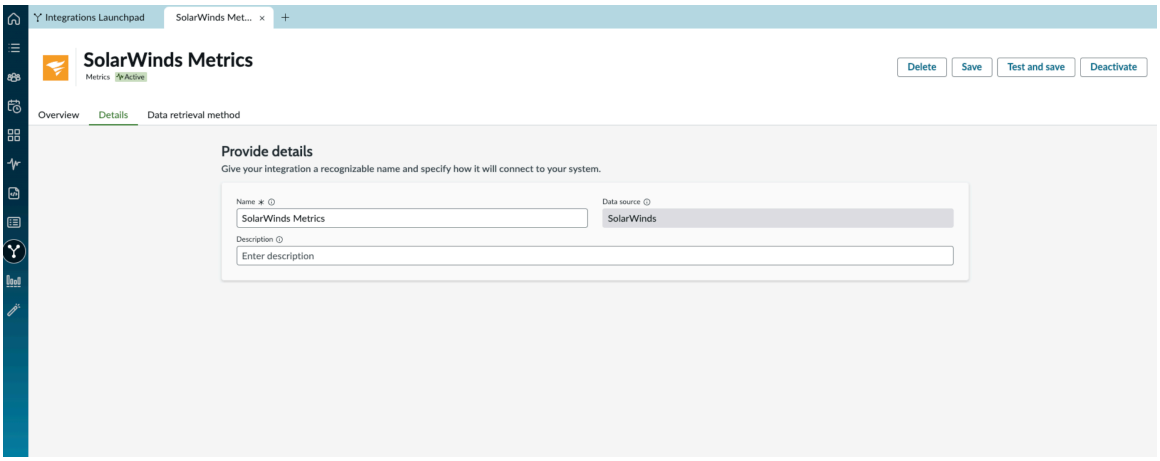
8. **Wahlweise:** Testen Sie den Connector, bevor Sie ihn aktivieren, indem Sie auswählen **Testen und speichern** .
9. Wählen Sie aus, um den Connector zu speichern **Speichern** .
10. Wählen Sie aus, um den Pull-Connector zu aktivieren **Aktivieren** .
    Der Connector für Metrik-Abruf ist aktiviert, und seine Kachel wird in angezeigt **Installierte Integrationen** Registerkarte. Wenn Sie die Kachel öffnen, finden Sie die **Übersicht** , **Details** , Und **Datenabrufmethode** Registerkarten.

    Die **Übersicht** Mit der Registerkarte können Sie überprüfen, ob der Connector ausgeführt wird und Daten erfasst. Es bietet auch Optionen zur Verbesserung der Systemeinstellungen, z. B. das Verfeinern von Warnungsdefinitionen oder die Verbesserung von Bindungskonfigurationen.

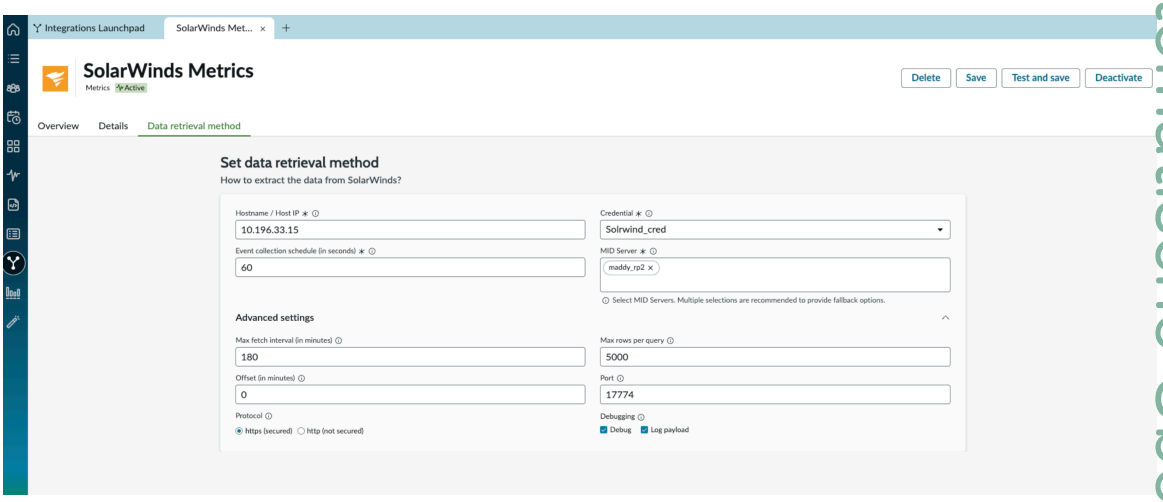


Die **Details** Auf der Registerkarte können Sie die allgemeinen Informationen des Connectors (z. B. Name oder Beschreibung) aktualisieren und alle während des Vorgangs aufgetretenen Fehler anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die **Datenabrufmethode** Die Registerkarte enthält die Connector-Einstellungen (z. B. Host, Port und Anmeldeinformationen) und kann zusätzliche Details zu Problemen wie enthalten MID-Server Fehler.



Überprüfen Sie die Integrations- und Konfigurationsintegrität

Überprüfen Sie Ihre Ereignisse, um sicherzustellen, dass Warnungen wie beabsichtigt erstellt werden. Starten Sie diesen Prozess, indem Sie den Integritätsstatus Ihrer Integration überprüfen. Dies bietet nützliche Statistiken, um hervorzuheben, wo Sie Verbesserungen vornehmen können, um Warnungen mit relevantem Geschäftskontext zu ergänzen, sie für eine bessere Reduzierung des Rauschens zu gruppieren, kritische Warnungen umgehend zu eskalieren und Ihr Team über schnelle Reaktion und Lösung zu benachrichtigen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

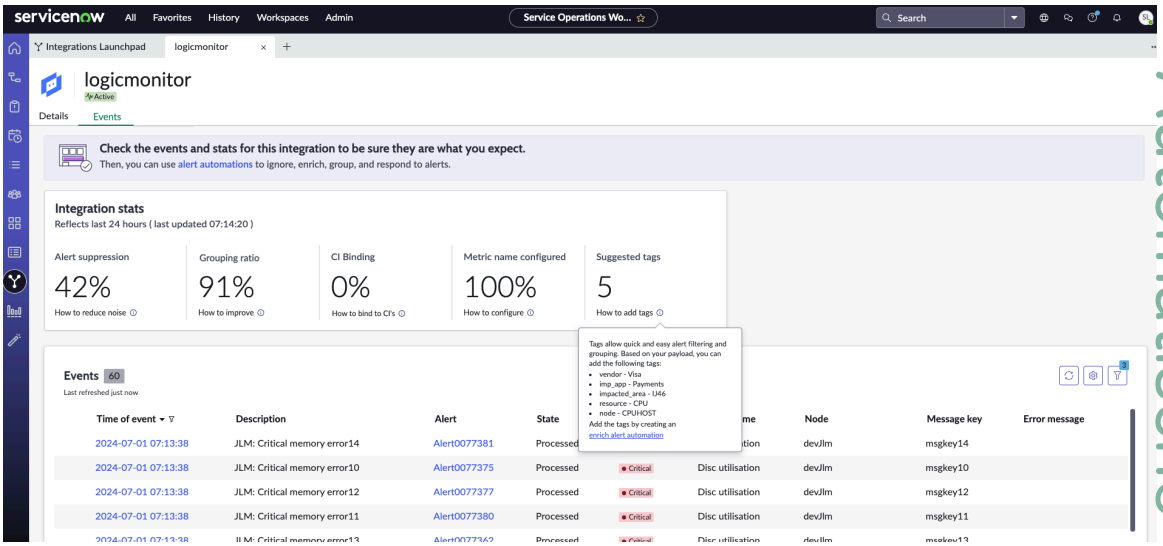
Integritätsstatusmetriken geben an, wie effektiv Warnungsautomatisierungen Kontext hinzufügen und Rauschen reduzieren, wodurch Operatoren die durchschnittliche Zeit bis zur Reparatur (MTTR) senken können. Überprüfen Sie beim Hinzufügen einer neuen Integration diese Metriken, bewerten Sie die Raten, und entwickeln Sie neue Regeln, um die Reduzierung von Rauschen und die Gesamtsystemleistung weiter zu verbessern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. In **Integrationen Durchsuchen** Wählen Sie die Registerkarte aus **Alle Integrationen** Dropdown-Liste, und wählen Sie aus **Abrufen** Oder **Veröffentlichen** Nach Bedarf.
4. Wählen Sie eine Kachel vom Typ „Pull“, „Push“ oder „anwenderdefinierter Connector“ aus.
   Wenn ein Popup-Menü geöffnet wird, wählen Sie die Daten aus, die von diesem Connector verfolgt werden sollen, und wählen Sie aus **Fahren Sie Fort** .
5. Wählen Sie die Registerkarte **Events** aus.



6. Zeigen Sie im Abschnitt „Integritätsstatus“ die Daten für Warnungen und die zugehörigen Attribute an.

Warnungsattribute

Warnungsattribut	Beschreibung
Warnungsunterdrückung	Das Unterdrückungsverhältnis gibt den Anteil der erstellten Warnungen an empfangenen Ereignissen an. Die Reduzierung unerwünschter Warnungen kann durch Deduplizierung oder Ignorieren erreicht werden. ○ Deduplizierung: Der **Message_key** Das Feld ist ein eindeutiger Bezeichner für eine Warnung im Quellüberwachungssystem. Es wird für die Deduplizierung und die Erkennung von Warnungsfluktuationen verwendet. Wenn das Quellereignis keine zuverlässigen eindeutigen Werte bereitstellt, können Sie den Standardwert verwenden oder eigene erstellen. Wenn der Nachrichtenschlüssel nicht definiert ist, ist der Standardnachrichtenschlüssel <Source + Node + Type + Resource + Metric Name>. Die Richtlinie dient dazu, dass die Ereignisquelle automatisch ausfüllt <Source + Node + Type + Resource + Metric Name>Felder und generieren Sie den Nachrichtenschlüssel. Diese Praxis erleichtert eine bessere Verteilung der Ereignisverarbeitung auf Instanz-Worker und Knoten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsattribut	Beschreibung
	Wenn das Quellereignis keine Werte für diese Felder bereitstellt, stellen Sie sicher, dass sie mit Transformationsregeln ausgefüllt werden. Diese Aktion, die sich nicht auf die Ereignisverarbeitung auswirkt, ist für die Deduplizierung wichtig. Füllen Sie so viele dieser Felder wie möglich aus, bevor Sie das Ereignis an die Instanz senden. Dadurch wird die Verteilung von Ereignissen auf Prozessormitarbeiter verbessert, was zu einem verbesserten Durchsatz und einer verbesserten Skalierbarkeit führt. Weitere Informationen zur Deduplizierung finden Sie unter Ereignismanagement-Konfigurationspräferenzen. Informationen zum Festlegen des Nachrichtenschlüssels in Ihrer anwenderdefinierten Connector-Integration finden Sie unter Konfigurieren Sie einen anwenderdefinierten Ereignis-Connector. ○ Warnungsereignisregeln ignorieren: Filtern Sie Warnungen mit niedriger Qualität heraus, indem Sie eine erstellen Automatisierung ignorieren .
Warnungs-Komprimierungsrate	Wenn Sie Warnungen gruppieren, ist eine hohe Komprimierungsrate wünschenswert, da dies bedeutet, dass weniger Warnungen für Ihr Betriebsteam verbleiben, um sie zu überprüfen und zu bearbeiten. Dies kann zu einer verbesserten Teameffizienz führen. Die Komprimierungsrate wird berechnet als 1 – (Anzahl der Warnungsgruppen + Anzahl der nicht gruppierten Warnungen) / Gesamtzahl der Warnungen. Informationen zur Warnungszusammenfassung finden Sie unter Warnungsgruppierung. Eine Möglichkeit, Ihre Warnungskomprimierungsrate zu verbessern, besteht darin, eine neue Gruppierungsautomatisierung zu definieren.
CI-Bindung	Der Prozentsatz der Warnungen, die erfolgreich an ein Konfigurationselement (CI) in Ihrer CMDB gebunden sind, ist entscheidend. Ziel ist, dass diese Zahl bei oder nahe 100 % liegt, um die Warnungsgruppierung, die Ursachenanalyse, die Zuweisung und vieles mehr zu verbessern. Um einen Host, einen Computer oder ein beliebiges Gerät mit einer IP zu binden, füllen Sie aus **Knoten** Feld mit einem eindeutigen Hostnamen, FQDN, IP oder MAC-Adresse. Dies kann innerhalb der Integration selbst oder durch Erstellen einer Bereicherungsautomatisierung erfolgen. Für komplexere Szenarien können Sie die knotenbasierte Bindung mithilfe von Ereignisregeln überschreiben. Weitere Informationen zur CI-Bindung finden Sie unter Warnungen werden an CIs gebunden.
Metrikname wurde konfiguriert	Zeigt den Prozentsatz der Warnungen an, für die ein Metrikname definiert ist. Es ist wichtig, fast 100 % anzustreben, da es standardmäßig in unserem automatisierten Korrelationsalgorithmus verwendet wird. Dies kann innerhalb der Integration selbst oder durch Erstellen eines erreicht werden Bereichern Sie die Automatisierung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsattribut	Beschreibung
Vorgeschlagene Tags	Stellt vorgeschlagene Warnungs-Tags basierend auf der Integrationsnutzlast bereit. Warnungs-Tags sind strukturierte Felder, die Sie definieren können, um das Filtern und Gruppieren von Warnungen zu erleichtern. Die Tags werden in gespeichert *sn_itom_integ_app_recommendation_tags_suggestion*, Und nur die 5 beliebtesten Tags werden angezeigt. Wenn Sie die Ergebnisse des Vorschlagsmechanismus verfeinern möchten, können Sie die Eigenschaft verwenden *sn_itom_integ_app.evt_mgmt_tag_suggestion_ignore_keys*, Die eine Liste von Kleinbuchstaben oder Stichwörtern anzeigt, getrennt durch Kommas, die beim Scannen zusätzlicher Warnungsinformationen auf Tag-Vorschläge ignoriert werden sollen. Der Standardwert ist Zeit.

7. Stellen Sie im Abschnitt „Ereignisse“ sicher, dass Ihre Ereignisse wie erwartet Warnungen generieren.

   Überprüfen Sie, ob Warnungsfelder und -Tags korrekt ausgefüllt sind, um das Lesen und Filtern der Warnungen zu erleichtern Express-Liste. Bestätigen Sie, dass die Schweregradwerte den Erwartungen Ihres Betriebsteams entsprechen und dass Felder und Tags quellenübergreifend einem standardisierten Format entsprechen, um die Gruppierung zu erleichtern.

   Durch die Überprüfung der Warnungsgenerierung können Sie sicher sein, dass Ihr System ordnungsgemäß konfiguriert ist, um bemerkenswerte Vorkommnisse zu erkennen und zu benachrichtigen. Informationen zu den Feldern im Abschnitt „Ereignisse“ finden Sie unter Integrations- und Konfigurationsintegritätsereignisfelder.

Nächste Maßnahme
Nachdem Sie nun Warnungen aus den Ereignissen bestätigt haben, können Sie den Warnungsautomatisierungsprozess initiieren, indem Sie auswählen **Fügen Sie Automatisierung hinzu** . Dadurch gelangen Sie zum Schritt „Automatisierung ignorieren“, in dem Sie irrelevante oder falsch positive Warnungen ignorieren können. Fahren Sie anschließend mit dem Anreichern, Gruppieren und Automatisieren von Antworten fort. Dieser Prozess umfasst die Umwandlung von Rohwarnungen in ein Format, das für verständlich ist ServiceNow, Gruppierung der Warnungen und Eskalation einer Warnung, um eine sofortige Antwort des entsprechenden Teams oder einer Person sicherzustellen. Weitere Informationen zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich Für ITOM.

Aktivieren Sie die Integration

Mit „Integration aktivieren“ können Sie eine zuvor deaktivierte Connector-Integration aktivieren und ihre Funktionalität wiederherstellen. Diese Funktion hilft Ihnen, Daten-Flow- und Integrationsaktivitäten nahtlos fortzusetzen und so Kontinuität und effizientes Ereignismanagement sicherzustellen, ohne die Integration neu konfigurieren zu müssen.

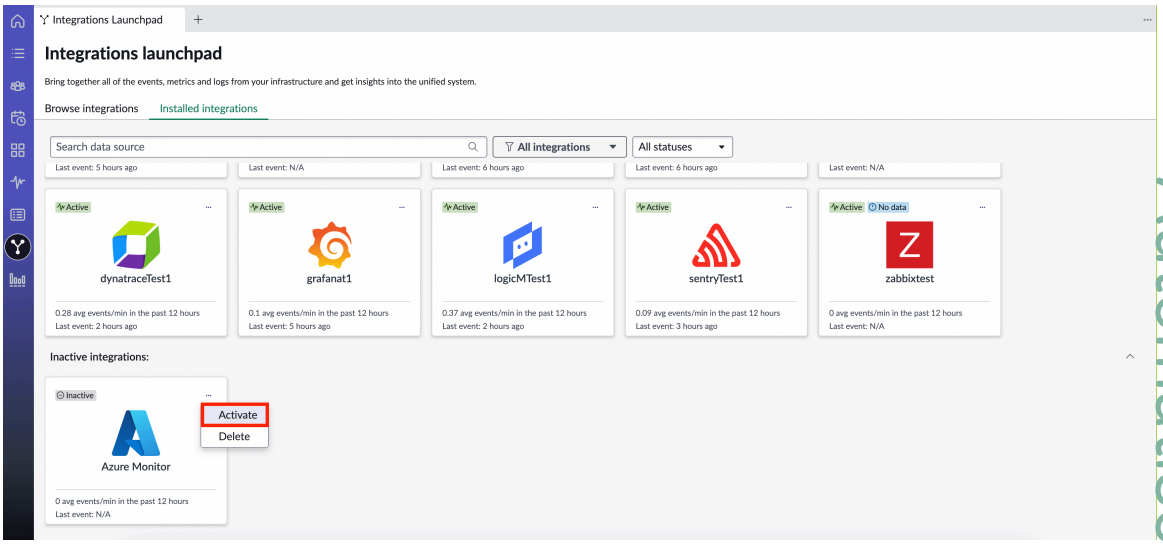
Vorbereitungen
Stellen Sie sicher, dass die Integration deaktiviert ist.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. Wählen Sie aus **Installierte Integrationen** Registerkarte.
4. Wählen Sie für die Integration, die Sie aktivieren möchten, das Ellipsen-Symbol (•••) Und dann auswählen **Aktivieren** .



Die ausgewählte Integration wird aktiviert, und ihr Status wird als angezeigt **Aktiv** Auf der Installationskachel.

Deaktivieren Sie die Integration

Mit „Integration deaktivieren“ können Sie eine aktive Connector-Integration vorübergehend deaktivieren, ohne sie zu löschen. Diese Funktion hilft Ihnen, Integrationen effektiver zu verwalten, indem der Datenfluss bei Bedarf angehalten wird, unnötige Ereignisverarbeitung reduziert und die Systemleistung verbessert wird.

Vorbereitungen

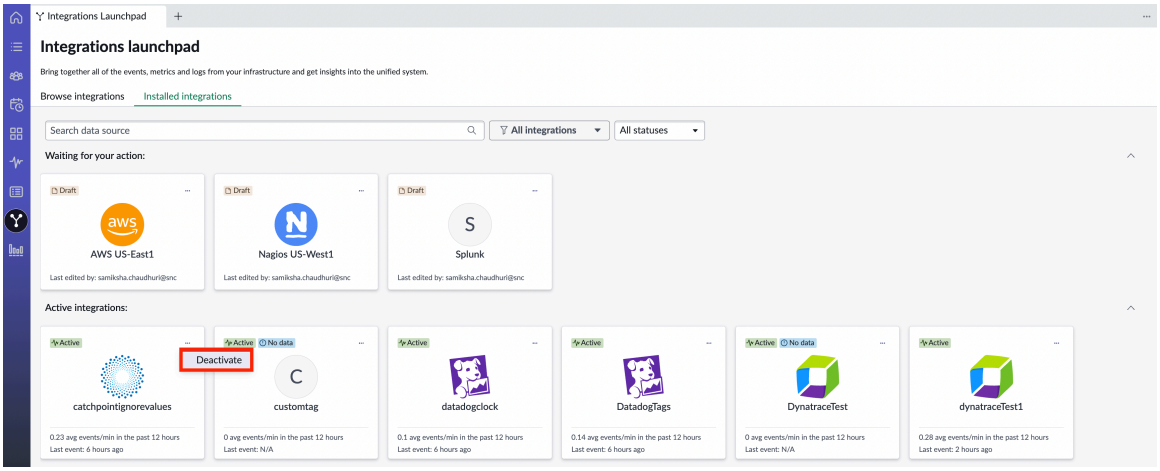
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. Wählen Sie aus **Installierte Integrationen** Registerkarte.
4. Wählen Sie für die Integration, die Sie deaktivieren möchten, das Ellipsen-Symbol (•••) Und dann auswählen **Deaktivieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die ausgewählte Integration ist deaktiviert, und ihr Status wird als angezeigt **Inaktiv** Auf der Installationskachel.

Löschen Sie die Integration

Mit „Integration löschen“ können Sie eine Connector-Integration dauerhaft aus Ihrem System entfernen. Diese Funktion hilft Ihnen, ein sauberes und organisiertes System zu verwalten, indem nicht verwendete oder veraltete Integrationen eliminiert werden, Ressourcen freigesetzt und potenzielles Kabelgewirr reduziert wird.

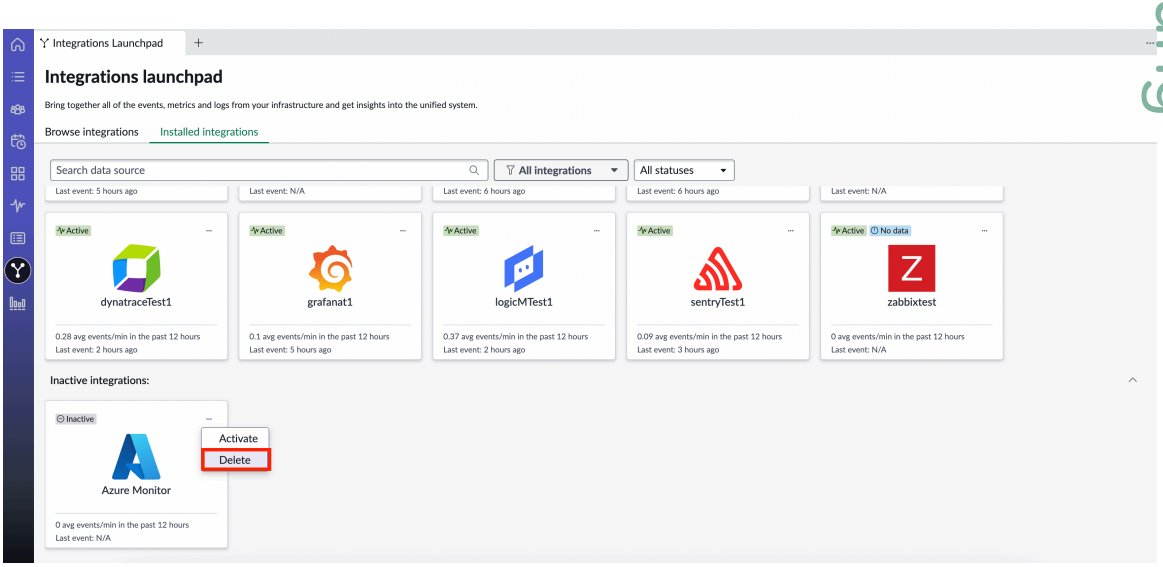
Vorbereitungen

Stellen Sie sicher, dass die Integration deaktiviert ist.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie im linken Bereich das Symbol Integrations Launchpad: .
3. Wählen Sie aus **Installierte Integrationen** Registerkarte.
4. Wählen Sie für die Integration, die Sie löschen möchten, das Symbol Ellipsen (•••) Und dann auswählen **Löschen** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die Integration wird gelöscht.

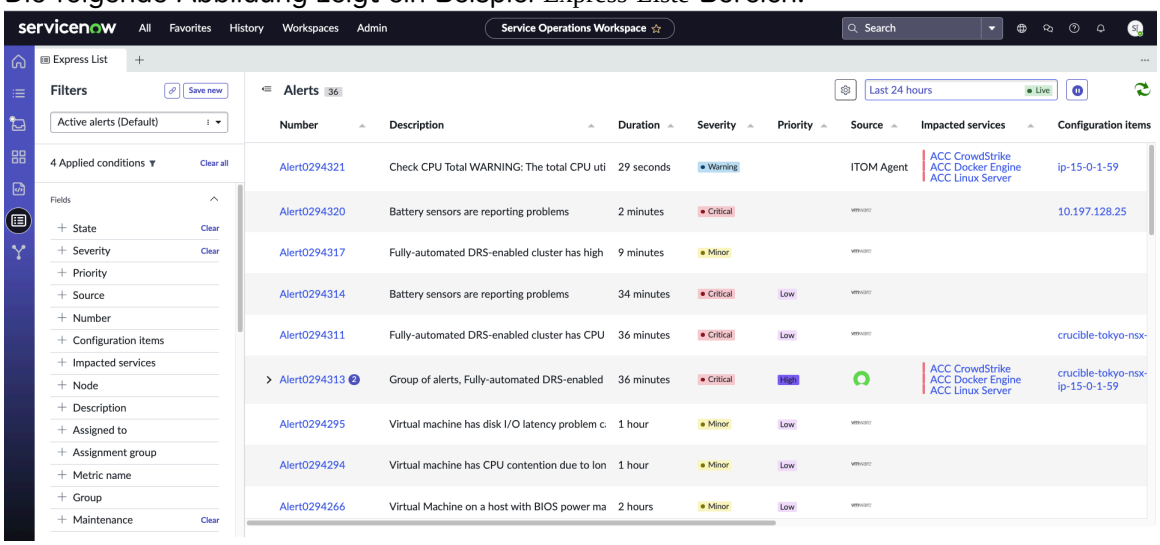
Express-Liste In Service Operations-Arbeitsbereich Für ITOM

Die ServiceNow Ereignismanagement Express-Liste Die Funktion hilft Ihnen, Integritätsprobleme im Rechenzentrum im zu identifizieren Service Operations-Arbeitsbereich. Es bietet eine Liste von schnellen Informationen zu Warnungen, damit Sie Systeme und Services effizienter überwachen,Warnungen lösen, die Auswirkung auf Warnungen bewerten,Probleme nachverfolgen und Incidents melden können.

Einführung in das Ereignismanagement Express-Liste

Die Express-Liste Die sortierbare Warnungsliste des Bereichs reduziert die Anzahl der Klicks, die für den Zugriff auf Warnungsinformationen erforderlich sind. Wenn Sie das Kontrollkästchen einer Warnung aktivieren, wird ein Vorschaubereich geöffnet, in dem Sie Daten anzeigen können, die bei der Priorisierung, der Auswirkungsrealisierung und der Ursachenanalyse hilfreich sind. Sie können einfach ändern Express-Liste Bereich, um die Anzeige einzugrenzen, indem Sie eine Liste der bereitgestellten Felder verwenden, zusätzliche Warnungsinformationen anzeigen und übereinstimmende Warnungen herausfiltern oder anzeigen. Sie können auch den angezeigten Zeitbereich ändern.

Die folgende Abbildung zeigt ein Beispiel Express-Liste Bereich.



Express-Liste – Vorteile

Die Express-Liste Mit dem Bereich können Operatoren die folgenden Aktionen effizienter ausführen:

- **Überwachungssysteme oder Anwendungsservices** . Überwachung der Leistung und Fähigkeit von Computersystemen, um Diskrepanzen zu erkennen.
- **Warnungen werden gelöst** . Arbeiten an Diskrepanzen, um Probleme zu beheben und das effiziente Funktionieren der IT-Infrastruktur zu fördern.
- **Nachverfolgung von Problemen** . Nachverfolgung und Dokumentation von Fehlern und Lösungen im Detail und Meldung von Incidents.
- **Melden von Incidents** . Eskalation komplexer Probleme an das Management, andere IT-Ressourcen, Drittparteien oder Lieferanten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsinformationen, die in angezeigt werden Express-Liste Vorschaubereich

Die Express-Liste Im Vorschaubereich werden zusätzliche Warnungsinformationen im angezeigt Express-Liste Bereich. Mit diesen Informationen können Sie eine Bewertung durchführen, die bei der Lösung von Incidents hilft, ohne mehrere Warnungsformulare öffnen zu müssen.

Die **Info** Auf der Registerkarte im Vorschaubereich werden die folgenden Informationen für eine ausgewählte Warnung angezeigt:

- Warnungsnummer (Link)
- Status
- Dauer
- Konfigurationselemente (mit Links)
- Metrikname
- Knoten
- Ressource
- Quelle
- Zugewiesen an
- Zuweisungsgruppe
- Letztes Update
- Betroffene Services

  Weitere Informationen finden Sie unter Zeigen Sie Daten zu betroffenen Services im Vorschaubereich in an Express-Liste.

- Zusätzliche Information
- Anwenderdefiniertes Feld

Sie können zusätzliche Warnungsinformationen anzeigen, indem Sie eines der verknüpften Elemente auswählen.

Die **Warnungen in Gruppe** Auf der Registerkarte im Vorschaubereich werden Warnungsinformationen für eine ausgewählte Warnungsgruppe angezeigt. Informationen für jede Warnung werden in einer Kachel mit zusätzlichen Optionen für jede Warnung in der Gruppe angezeigt.

Jede Kachel zeigt die folgenden Warnungsinformationen an:

- Warnungsnummer (Link)
- Status
- Schweregrad
- Konfigurationselemente
- Dauer
- Metrikname

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anpassen des Zeitbereichs der Warnungsanzeige

Sie können den Zeitbereich der angezeigten Warnungen bestimmen. Der Standardzeitbereich ist die letzten 24 Stunden. Die Liste wird weiterhin mit neuen Warnungen aktualisiert, bis Sie das Anhaltesymbol ( ). Wenn Sie oben rechts die aktuelle Bereichseinstellung auswählen, wird ein Dialogfeld mit Optionen für Datums- und Zeitbereich angezeigt:

- Alle Zeit: Die letzten 90 Tage
- Letzte 24 Stunden
- Letzte Woche
- Letzte 12 Stunden
- Letzte Stunde
- Letzte 15 Minuten
- Anwenderdefiniert: Ermöglicht Ihnen die Auswahl eines Datums- und Zeitbereichs aus dem Popup-Kalender.

Standardzeitbereiche können von Ihrem Administrator mit der Systemeigenschaft sn_SOW_em.evt_mgmt.Express_list.all_time_days definiert werden.

Zugehörige Informationen

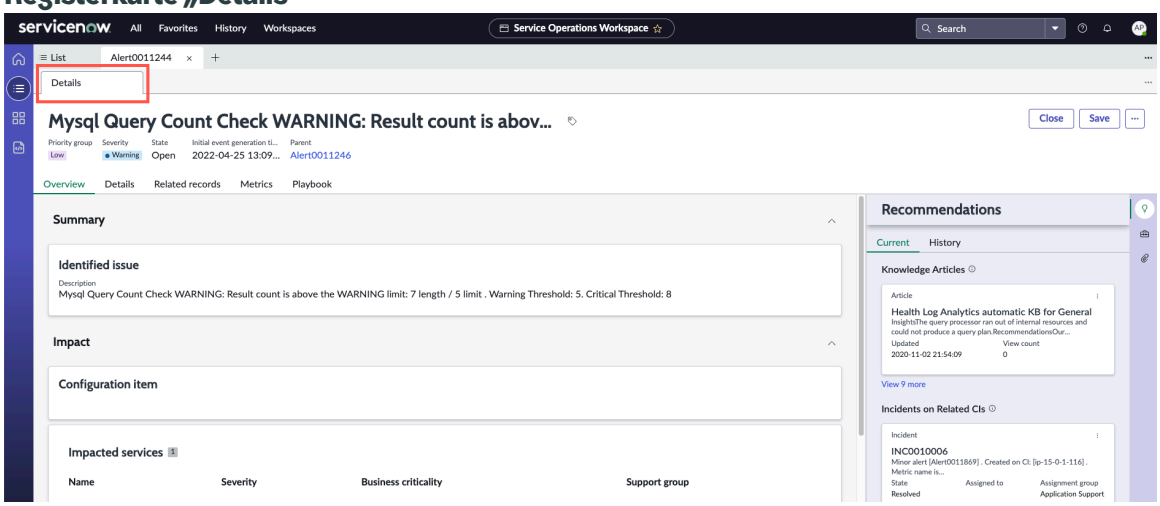
Von verwendete Rollen Express-Liste

Warnungen in Service Operations-Arbeitsbereich

Auf der Benutzeroberfläche von Service Operations-Arbeitsbereich wird eine Warnungsliste mit weiteren Details zu bestimmten Warnungen angezeigt.

Wenn Sie in der Warnungsliste auf eine Warnung klicken, wird die Registerkarte **Details** der ausgewählten Warnung angezeigt, und im Warnungstitel wird das Problem angezeigt, das die Warnung verursacht hat (das identifizierte Problem). Auf der resultierenden Seite werden nur die für die Warnung relevanten Unterregisterkarten angezeigt. Beispielsweise wird die Option **Warnungen in Gruppe** nur für Warnungsgruppen auf der Registerkarte **Zugehörige Datensätze** angezeigt.

Registerkarte „Details“



In der folgenden Tabelle werden die Bereiche im Warnungsformular beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereiche im Warnungsformular

Funktion	Beschreibung
Kopfzeile	Der Header enthält die folgenden Details: • Beschreibung: Der Text aus dem Feld **Beschreibung** der Warnung wird angezeigt. • Prioritätsgruppe: Die Prioritätsgruppe, zu der die Warnung gehört. • Schweregrad: Der Schweregrad der Warnung. • Status: Der Status der Warnung. • Generierungszeit des ersten Events: Datum und Uhrzeit der Generierung des ersten Ereignisses. • Übergeordnet: Die primäre Warnung in der Gruppe (nur relevant für untergeordnete Warnungen in einer Gruppe). • Gruppe: Gruppentyp, zu dem die Warnung gehört (nur relevant für Warnungen in einer Gruppe). • Aufgabe: Nummer des Incidents, dem die Warnung zugeordnet ist. Die angezeigten Informationen variieren je nach Warnungstyp.
Registerkarte Übersicht	Wenn Sie eine Warnung mit zugewiesenem CI anzeigen, wird diese Registerkarte beim Auswählen der Warnung geöffnet. Die angezeigten Informationen variieren je nach Typ der Warnung (gruppiert, sekundär oder primär). Wenn Sie die App Health Log Analytics installiert haben, gehören Health Log Analytics-Warnungen und komponentenbasierte Warnungen zu den Warnungstypen.

Weisen Sie Warnungen in zu Express-Liste

Weisen Sie Warnungen in zu Express-Liste An sich selbst, an eine andere Person oder an eine Zuweisungsgruppe, um die Arbeitsauslastung Ihrer Organisation auszugleichen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

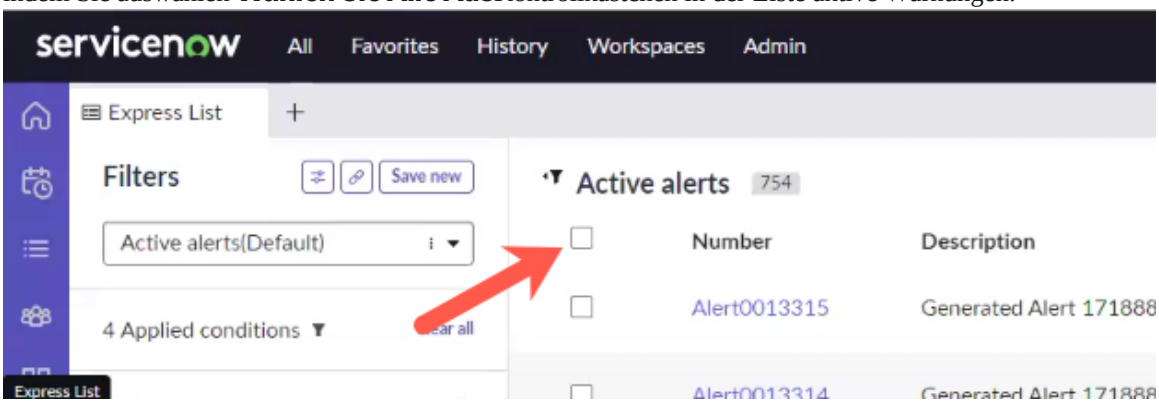
Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

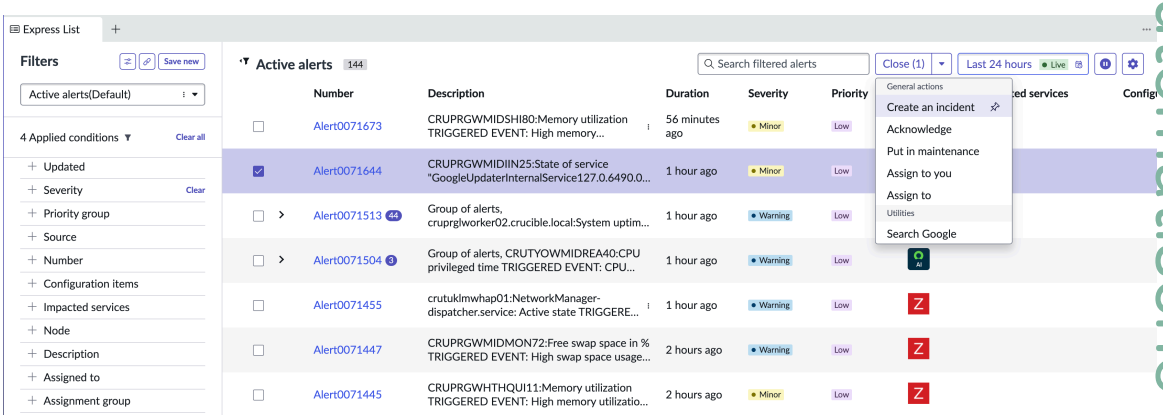
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie das Kontrollkästchen neben der Warnungsnummer, die Sie zuweisen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie auswählen **Wählen Sie Alle Aus**Kontrollkästchen in der Liste aktive Warnungen.



4. Wählen Sie aus **Schließen** Dropdown-Liste.



5. Führen Sie eine der folgenden Aktionen aus.

Zuweisung	Aktionen
Selbst	Wählen Sie Aus **Ihnen zuweisen** Und wählen Sie dann aus **OK** .
Jemand anderes	**a.** Wählen Sie Aus **Zuweisen an** . **b.** Wählen Sie den Namen der Person aus, der Sie die Warnung zuweisen möchten **Zugewiesen an** Feld. **c.** (Optional) Geben Sie Informationen zur Zuweisung oder Warnung in ein **Arbeits notizen** Feld. **d.** Wählen Sie aus **Weisen Sie <num ber>-Warnungen zu** Schaltfläche.
Zuweisungsgruppe	**a.** Wählen Sie Aus **Zuweisen an** . **b.** Wählen Sie den Namen der Gruppe aus der aus **Zuweisungsgruppe** Feld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisung	Aktionen
	c. Wählen Sie den Namen der Person aus, der Sie die Warnung zuweisen möchten **Zugewiesen an** Feld. **d.** (Optional) Geben Sie Informationen zur Zuweisung oder Warnung in ein **Arbeits notizen** Feld. **e.** Wählen Sie aus **Weisen Sie <num ber>-Warnungen zu** Schaltfläche.

Ergebnis

Die zugewiesene Person wird in angezeigt **Zugewiesen an** Spalte und die Zuweisungsgruppe werden in angezeigt **Zuweisungsgruppe** Spalte in Express-Liste Bereich.

Express-Liste-Tastenkürzel

Verwenden Sie Tastenkombinationen, um schnell allgemeine Aktionen in auszuführen Express-Liste.

Navigationsverknüpfungen

Aktion	Tastenkombination
Wechseln Sie zur vorherigen/nächsten Zeile	Pfeil nach oben/unten
Fokus zwischen anklickbaren Elementen verschieben	Registerkarte
Fokus zwischen anklickbaren Elementen nach hinten verschieben	Umschalt + Tabulatortaste

Aktionsverknüpfungen

Aktion	Tastenkombination
Öffnen Sie einen Warnungsdatensatz	Option/Alt + R
Bestätigen Sie eine Warnung	Option/Alt + K
Weisen Sie sich selbst eine Warnung zu	Option/Alt + Y
Warnungen schließen	Option/Alt + X
Incident erstellen	Option/Alt + I
Freitext durchsuchen	Option/Alt + S
Live-Updates anhalten/neu starten	Option/Alt + L
Öffnen/schließen Sie den Vorschaubereich	Eingabe

Auswahlverknüpfungen

Aktion	Tastenkombination
Eine ausgewählte Gruppe von Warnungen erweitern/reduzieren	Leertaste
Wählen Sie mehrere benachbarte Warnungszeilen aus	Umschalt + Pfeil nach oben/unten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswahlverknüpfungen (Fortsetzung)

Aktion	Tastenkombination
Wählen Sie mehrere separate Warnungszeilen aus	Befehl/Steuerung + Pfeil nach oben/unten
Aktivieren Sie einen ausgewählten Link oder eine ausgewählte Schaltfläche	Eingabe

Hinweis: Die Informationen in diesem Abschnitt sind auch als produktinterne Hilfe im Hilfebereich für verfügbar Express-Liste.

Verwenden Sie einen zugewiesenen Express-Liste Anzeigen

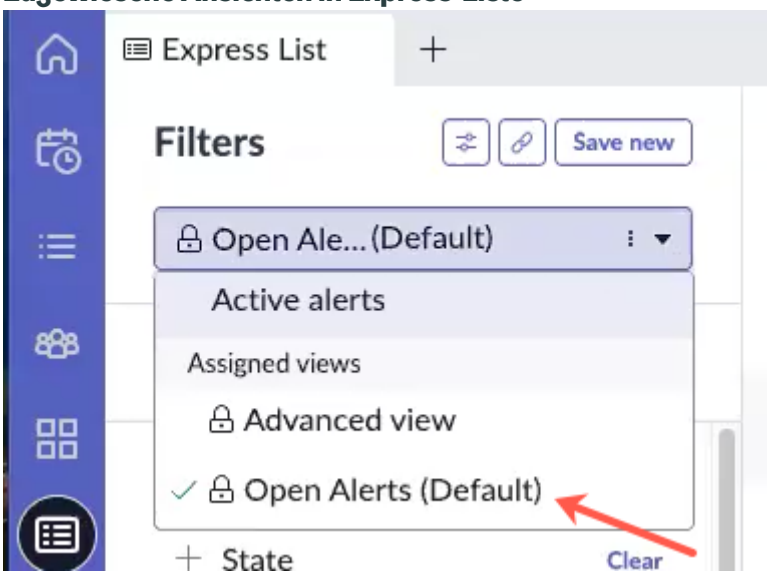
Arbeiten Sie mit Express-Liste Ansicht, die Ihnen von zugewiesen wurde Ereignismanagement administrator, um sicherzustellen, dass Sie sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie in der Dropdown-Liste im Bereich Filter eine aus Express-Liste Ansicht, die Ihnen zugewiesen wurde.
   Ihre Standardansicht ist als Standard markiert.

Zugewiesene Ansichten in Express-Liste



Hinweis: Die Ereignismanagement der administrator hat Ihnen möglicherweise mehr als eine Ansicht zugewiesen. Sie können zwischen Ihren Ansichten wechseln und Ansichten ändern und speichern, die nicht Ihre Standardansicht sind. Sie können Ihre Standardansicht in keiner Ihrer zugewiesenen Ansichten ändern, freigeben oder Einstellungen überschreiben.

Im Bereich Filter werden die vordefinierten Filter aufgelistet. Die Express-Liste Tabelle zeigt die Spalten an, die für die ausgewählte Ansicht konfiguriert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Wird Konfiguriert Express-Liste Ansichten für Anwender und Anwendergruppen

Hinzufügen oder ändern Express-Liste Spalten

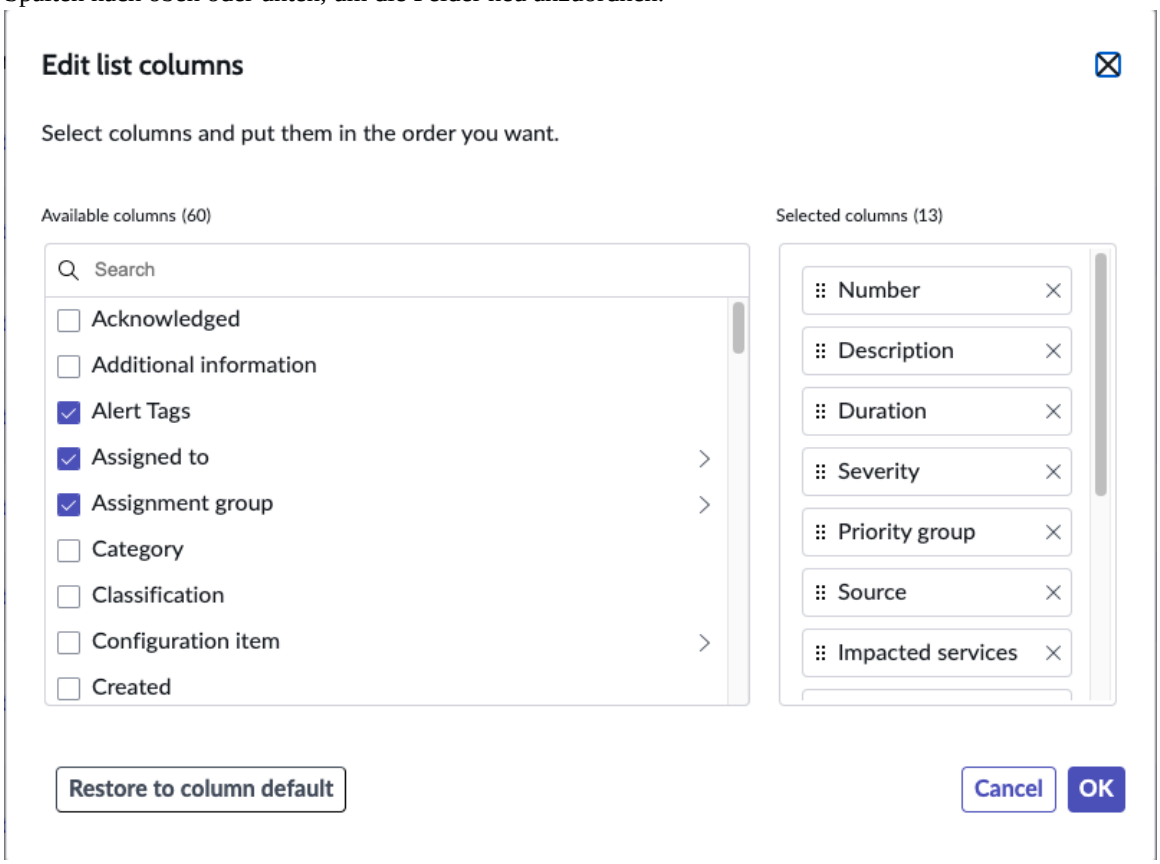
Fügen Sie Spalten zu hinzu Ereignismanagement Express-Liste Anzeigen, um die Liste der angezeigten Warnungen zu fokussieren oder die vorhandenen angezeigten Spalten zu ändern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Bearbeiten Sie die Standardspalten im Bereich.
   a. Wählen Sie das Zahnradsymbol ( ).
   b. In **Verfügbare Spalten** Liste die gewünschten Spalten auswählen.
   c. In **Ausgewählte Spalten**Liste, ziehen Sie ausgewählte Spalten nach oben oder unten, um die Felder neu anzuordnen.



   d. **Wahlweise:** Wählen Sie Aus **Auf Spaltenstandard zurücksetzen** Um die Spalten in den Standardstatus zurückzuversetzen.
   e. Wählen Sie **OK**.
4. **Wahlweise:** Ändern Sie die Spaltenbreite, die Reihenfolge und die Sortierrichtung direkt in Express-Liste Bereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Spaltenbreite	Zeigen Sie auf die rechte Seite der Spalte, bis der bi-direktionale Pfeil angezeigt wird, und ziehen Sie die Spalte auf die gewünschte Breite.
Spaltenreihenfolge	Wählen Sie den Spaltenheader aus, und ziehen Sie ihn an die gewünschte Position.
Spaltensortierung	Wählen Sie den Spaltenheader und dann den Pfeil aus. Die Pfeilrichtung gibt die Sortierreihenfolge an. Jede Auswahl des Pfeils ändert die Sortierrichtung.

Ergebnis

Das Layout wird automatisch in der Tabelle „Anwendereinstellung“ [sys_user_preferences] gespeichert. Wenn Sie die Liste erneut öffnen, werden die gleichen Spalten und die gleiche Reihenfolge angezeigt.

Fügen Sie anwenderdefinierte Felder zu hinzu Express-Liste Vorschaubereich

Fügen Sie anwenderdefinierte Felder aus der Tabelle „Warnung“ [em_Alert] zu hinzu Express-Liste Infovorschaubereich zum Nachverfolgen von Warnungsinformationen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften**an.
2. In **Systemeigenschaften** Liste, wählen Sie aus **evt_mgmt.Express_list.custom_fields** .

   Wenn eine Meldung zum Anwendungsbereich angezeigt wird, wählen Sie aus **Hier** Um den Datensatz bearbeiten zu können.

3. In **Wert** Feld den anwenderdefinierten Namen aus der Warnungstabelle [em_Alert] eingeben.
   Wenn Sie mehr als ein Feld angeben möchten, trennen Sie die Feldnamen durch Kommas.
4. Wählen Sie **Aktualisieren**.
5. **Wahlweise:** Zeigen Sie die anwenderdefinierten Felder im Vorschaubereich an:
   a. Wählen Sie in der primären Navigation die aus Express-Liste Symbol ( ).
   b. Wählen Sie eine Zeile oder das Informationssymbol am Anfang einer Zeile aus.

Ergebnis

Auf der Registerkarte Info im Vorschaubereich werden die anwenderdefinierten Felder am unteren Rand der Feldliste angezeigt.

Bestätigen Sie die angezeigten Warnungen in Express-Liste

Bestätigen Sie Warnungen, die Sie angezeigt haben, um Unordnung in zu entfernen Express-Liste Bereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

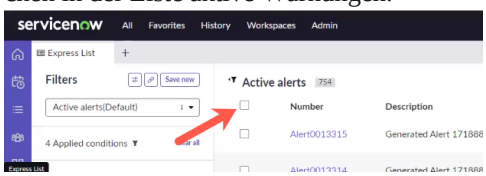
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Bestätigen, um anzugeben , dass die Warnung bekannt ist und vorübergehend ignoriert werden kann. Verwenden Sie Bestätigen nicht, um eine Warnung mit einem Handlungsbedarf zu versehen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Bestätigen Sie die ausgewählten Warnungen.
   Sie können Warnungen unabhängig davon bestätigen, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnungsgruppe ausgewählt ist.

Standort	Aktion
Die Express-Liste Bereich	**a.** In Express-Liste Wählen Sie die zu bestäti–gende Warnung aus. Sie können mehr als eine Warnungszeile auswählen. **Hinweis:** Sie können die Aktion für bis zu 1.000 Warnungen gleichzei-tig ausführen, indem Sie auswählen **Wählen Sie Alle Aus**Kontrollkäst-chen in der Liste aktive Warnungen.  Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Chevron-Symbol ( ) Am Anfang der Warnungsgruppenzeile. **b.** Von **Schließen** Dropdown-Liste oben rechts in der Warnungsliste auswählen **Bestätigen** .
Die Express-Liste Vorschaubereich für Gruppen-warnungen	**a.** Aktivieren Sie ein Kontrollkästchen für eine Warnungsgruppenzeile. **b.** In **Warnungen in Gruppe** Wählen Sie eine Warnungskachel aus. **c.** Wählen Sie das Symbol weitere Aktionen ( ). **d.** Wählen Sie Aus **Bestätigen** .

Ergebnis

Die Warnung wird bestätigt, und ihr Status wird oben im Vorschaubereich angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingehende Warnungen überwachen

Sie können eingehende Warnungen in überwachen Service Operations-Arbeitsbereich. Sie können Warnungen auch auf der Oberfläche Ereignismanagement überwachen und verwalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Zeigen Sie die Warnungsinformationen an.

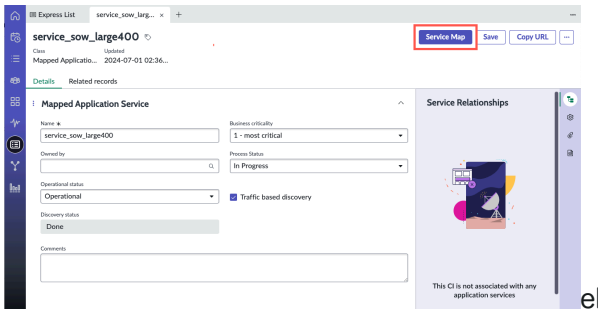
Spaltenüberschriften Warnungen

Spaltenüberschrift	Beschreibung
Nummer	Eindeutige ID, die von Ereignismanagement generiert wird, um die Warnung zu identifizieren.
Gruppe	Ein Eintrag in dieser Spalte gibt an, dass die zugeordnete Warnung ein Mitglied einer Warnungsgruppe ist. Warnungen, die keinen Eintrag in dieser Spalte haben, sind nicht gruppierte Warnungen. ○ **Automatisiert**: Werden automatisch durch Warnungszusammenfassung zusammengefasst. Eine virtuelle Warnung wird der Gruppe als primäre Warnung der Gruppe hinzugefügt. ○ **Regelbasiert** : Warnungsgruppe, die als Ergebnis einer anwenderkonfigurierten Korrelationsregel erstellt wurde. ○ **Manuell**: Diese Warnung ist ein Mitglied einer Warnungsgruppe, die beim Klicken mit der rechten Maustaste auf eine Warnung und als sekundäre Einstellung für die ausgewählte primäre Warnung gebildet wird. ○ **CMDB**: CIs ohne Verlaufsdaten, die durch Warnungszusammenfassung basierend auf CI-Beziehungen in der CMDB aggregiert wurden. ○ **Sekundär**: Diese Warnung ist eine Komponente einer Warnungsgruppe. Die Warnung an der Spitze der Gruppe wird als primäre Warnung bezeichnet. Wenn **Korrelierte Warnungen** ausgewählt ist, werden die sekundären Warnungen, die sich unter der primären Warnung befinden, nicht angezeigt, wodurch die Warnungsliste übersichtlicher und leichter zu überprüfen ist. ○ **Keine** : Diese Warnung ist eine nicht gruppierte Warnung. Damit eine nicht gruppierte Warnung Mitglied einer Gruppe wird, klicken Sie mit der rechten Maustaste darauf, und wählen Sie im Thema **Zu Gruppen hinzufügen** aus. Wählen Sie die Warnung aus, und klicken Sie auf **Ausgewählte hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenüberschrift	Beschreibung
	○ **Text** : Diese Warnung ist Mitglied einer Warnungsgruppe, die basierend auf der Ähnlichkeit ihres Texts oder ihrer Beschreibung erstellt wurde. ○ **Log Analytics** : Diese Warnung ist Mitglied einer Log Analytics-Warnungsgruppe. ○ **Komponentenbasiert** : Diese Warnung ist Mitglied von Log Analytics Gruppe, die basierend auf den betroffenen IT-Komponenten oder -Services erstellt wurde. ○ **Tag-Cluster** : Diese Warnung ist Mitglied einer Warnungsgruppe, die basierend auf allgemeinen Tags oder Bezeichnungen erstellt wurde, die ihnen zugewiesen sind. ○ **Netzwerkverkehr** : Diese Warnung ist Mitglied einer Warnungsgruppe, die basierend auf Netzwerkverkehrsverbindungen zwischen Prozessen von Host-CIs erstellt wurde. ○ **Gemischt** : Diese Warnung ist Mitglied einer Gruppierungsmethode, die Warnungen mithilfe mehrerer Gruppierungsstrategien, z. B. CMBD-basierte Gruppierung und Tag-basierte Gruppierung, in einer einzigen, zusammenhängenden Gruppe kombiniert.
Schweregrad	Der Schweregrad des Events. Der Wert für dieses Feld wird aus dem Event kopiert, es sei denn, das Event schließt die Warnung. In diesem Fall wird der vorherige Schweregrad für die Berichterstellung beibehalten. ○ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ○ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ○ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ○ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ○ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Gibt an, welche Warnungen zuerst behandelt werden sollen. Die Priorität wird für alle offenen Warnungen berechnet, woraufhin diese einer von vier Prioritätskategorien zugeordnet werden.
Priorität	Wert, der als Leitfaden für die Priorität der Warnung dient, basierend auf einer Anzahl von kumulierten Kategorien. Beispielsweise Warnungsstatus und geschäftliche Relevanz.
Quelle	Eventüberwachungssoftware, die das Event generiert hat, z. B. SolarWinds oder SCOM. Optional können Sie eine Beschreibung eingeben, z. B. Gruppenwarnung. Dieses Feld hat eine maximale Länge von 100.
Beschreibung	Die Warnungsbeschreibung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenüberschrift	Beschreibung
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, die dem Ereignis zugeordnet ist, z. B. IBM-ASSET. Dieses Feld hat eine maximale Länge von 100.
Konfigurationselement	JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: {„Name“: „SAP ORA01“, „Typ“: „Oracle“}. Der CI-Bezeichner, der das Event generiert hat, wird im Feld **Zusätzliche Informationen** angezeigt. Dieses Feld hat eine maximale Länge von 1000. Klicken Sie auf das , um die Warnung in der Abhängigkeitsansicht zu öffnen.
Betroffene Services	Listet die von dieser Warnungsgruppe betroffenen Services auf. Wählen Sie einen betroffenen Service aus, um den zugehörigen Datensatz anzuzeigen. **Hinweis:** Sie können in auf die Servicezuordnung zugreifen Service Operations-Arbeitsbereich Direkt im Formular Betroffener Service durch Auswahl **Servicezuordnung** . Die Servicezuordnung zeigt den betroffenen Pfad von Warnungen an, sodass Sie ihre Auswirkungen auf den Service schnell bewerten können. Weitere Informationen finden Sie unter Zeigen Sie die einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich.  el-imp-service-open-map.png
Metrikname	Eindeutiger Name, der beschreibt, welche Metriken erfasst werden und für welche die Warnung erstellt wurde.
Reserviert	Zeigt an, ob sich die von der Warnung betroffene Ressource in Wartung befindet. Gültige Werte sind `true` oder `false`.
Aufgabe	Die entsprechende Aufgabe für die Warnung, z. B. Incident, Change oder Problem.
Übergeordnet	Verweis auf übergeordnete Warnung.
Generierungszeit des ersten Events	Zeit des ersten Ereignisses im Remote-System

Nächste Maßnahme

Wenn Operational Intelligence aktiviert ist, klicken Sie mit der rechten Maustaste auf eine Warnung, und klicken Sie dann auf **Metriken anzeigen**, um den integrierten Explorer für Einblicke und die Dependency Views-Zuordnung für das CI zu öffnen, das der Warnung zugeordnet ist.

Zugehörige Informationen

- Metrikdaten
- Warnungsinformationen anzeigen
- Warnungsgruppierungstypen und Erstellungsmethoden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließen Sie eine Warnung in Express-Liste

Schließen Sie Warnungen manuell direkt aus Express-Liste Oder aus dem Vorschaubereich, ohne darauf zu warten, dass sie automatisch geschlossen werden, wenn Sie die Ursache bereits kennen oder das Problem behoben haben.

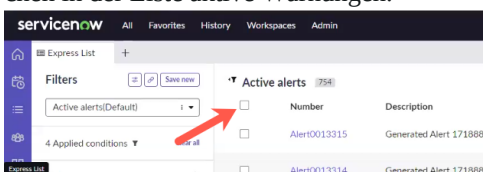
Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Schließen Sie ausgewählte Warnungen.
   Sie können Warnungen unabhängig davon schließen, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnungsgruppe ausgewählt ist.

Standort	Aktion
Die Express-Liste Bereich	**a.** In Express-Liste Wählen Sie die Warnung aus. Sie können mehr als eine Warnungszeile auswählen. **Hinweis:** Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie auswählen **Wählen Sie Alle Aus**Kontrollkästchen in der Liste aktive Warnungen.  Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Chevron-Symbol ( ) Am Anfang der Warnungsgruppenzeile. **b.** Von **Schließen** Dropdown-Liste oben rechts in der Warnungsliste auswählen **Warnung schließen** .
Die Express-Liste Vorschaubereich für Gruppenwarnungen	**a.** Wählen Sie eine Warnungsgruppenzeile aus. **b.** In **Warnungen in Gruppe** Wählen Sie eine Warnungskachel aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standort	Aktion
	c. Wählen Sie das Symbol weitere Aktionen (⋮). **d.** Wählen Sie Aus **Warnung schließen** .

Ergebnis
Die Warnung wird geschlossen, und ihr Status wird oben im Vorschaubereich angezeigt.

Erstellen Sie einen Incident aus einer Warnung in Express-Liste

Erstellen Sie einen Incident aus einer Warnung direkt aus der Express-Liste Bereich, der Ihnen Zeit und Aufwand für die Navigation zum Incident-Datensatz spart.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Erstellen Sie einen Incident aus einer ausgewählten Warnung.
   a. In Express-Liste Wählen Sie die Warnung aus.

      Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Chevron-Symbol (›) Am Anfang der Warnungsgruppenzeile.

   b. Von **Schließen** Wählen Sie in der Dropdown-Liste unter Korrekturaktionen die Option aus **Incident Erstellen** .

   Aus der ausgewählten Warnung wird ein Incident erstellt, und eine Bestätigungsnachricht wird angezeigt.
4. **Wahlweise:** Zeigen Sie einen erstellten Incident an, indem Sie auswählen **Incident anzeigen** In der Bestätigungsnachricht.

Erstellen Sie einen Incident mit Now Assist In Express-Liste

Erstellen Sie mit einen Incident mit einer visuell lesbaren, KI-generierten Beschreibung Now Assist.

Vorbereitungen
Derzeit ist diese Funktion für verfügbar CMDB, Log Analytics, Tag-basierte und komponentenbasierte Warnungen.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie aus Express-Liste Symbol ( ) In der linken Navigationsleiste.
3. Erstellen Sie einen Incident aus einer ausgewählten Warnung.

   a. In Express-Liste Wählen Sie die Warnung aus.

   Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Chevron-Symbol ( ) Am Anfang der Warnungsgruppenzeile.

   b. Von **Schließen** Wählen Sie in der Dropdown-Liste unter Korrekturaktionen die Option aus **Incident mit Now Assist erstellen** .

   Aus der ausgewählten Warnung wird ein Incident mit einer visuell lesbaren, KI-generierten Beschreibung erstellt, und eine Bestätigungsmeldung wird angezeigt.

4. **Wahlweise:** Zeigen Sie den erstellten Incident an, indem Sie auswählen **Incident anzeigen** In der Bestätigungsnachricht oder im Warnungsvorschaubereich.

Schalten Sie die Warnungen eines CI in stumm Express-Liste

Schalten Sie die Warnungen eines CI in stumm Express-Liste Um zu vermeiden, dass beim Ersetzen oder Aktualisieren des CI Warnungen ausgegeben werden.

Vorbereitungen

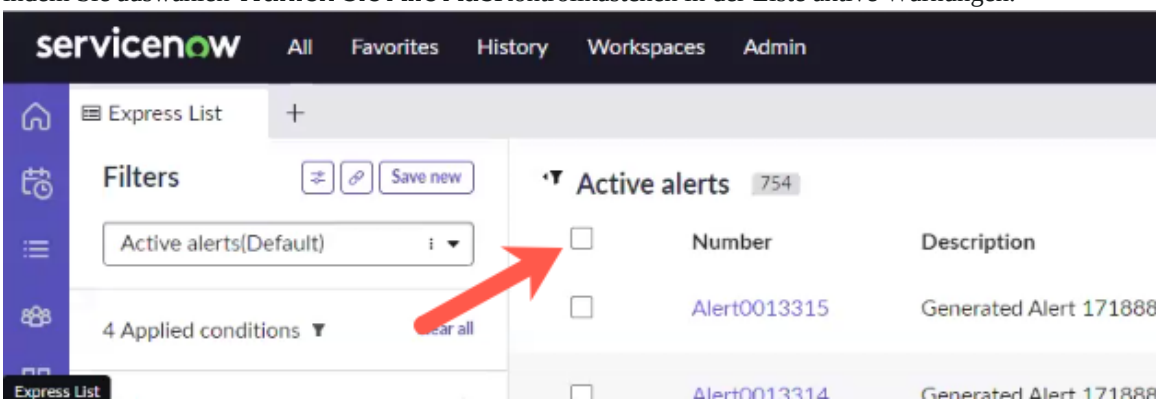
Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie das Kontrollkästchen Warnungszeile.

   Hinweis: Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie auswählen **Wählen Sie Alle Aus**Kontrollkästchen in der Liste aktive Warnungen.



4. Von **Schließen** Dropdown-Liste auswählen **In Wartung setzen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Warnungen werden für die Konfigurationselemente dieser Warnung stummgeschaltet.

Warnungen in den Status „Wartung“ versetzen

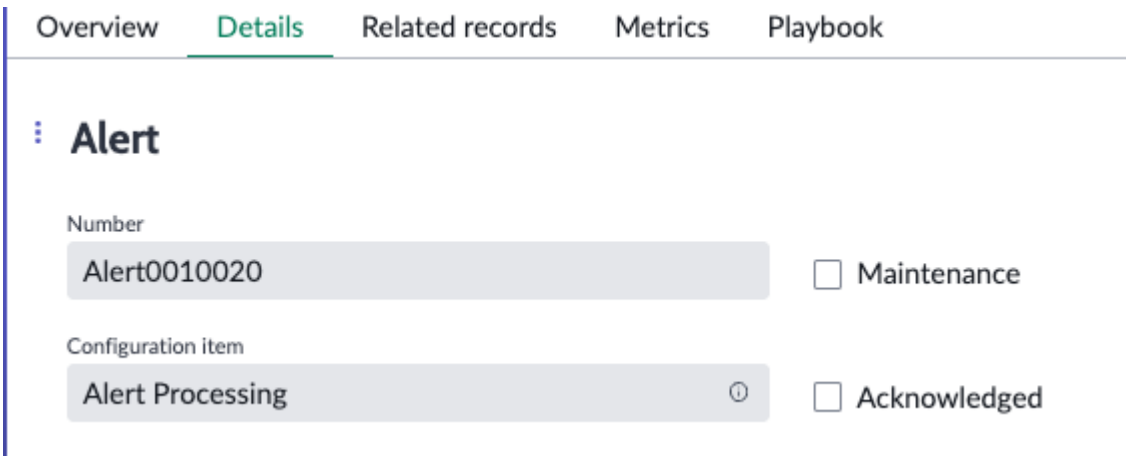
Indem Sie eine Warnung in den Status „Wartung“ versetzen, geben Sie an, dass verschiedene Probleme mit den CIs der Warnung behandelt werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Filtern Sie mit **Aktive Warnungen** .
4. Wählen Sie eine Warnung aus.



5. Aktivieren Sie auf der Unterregisterkarte **Details** das Kontrollkästchen **Wartung**, um die Warnung in den Status „Wartung“ zu versetzen.
6. Klicken Sie auf **Speichern**.

Warnungen in den Status „Bestätigt“ versetzen

Indem Sie eine Warnung in den Status „Bestätigt“ versetzen, geben Sie an, dass Probleme mit der Warnung behoben werden müssen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

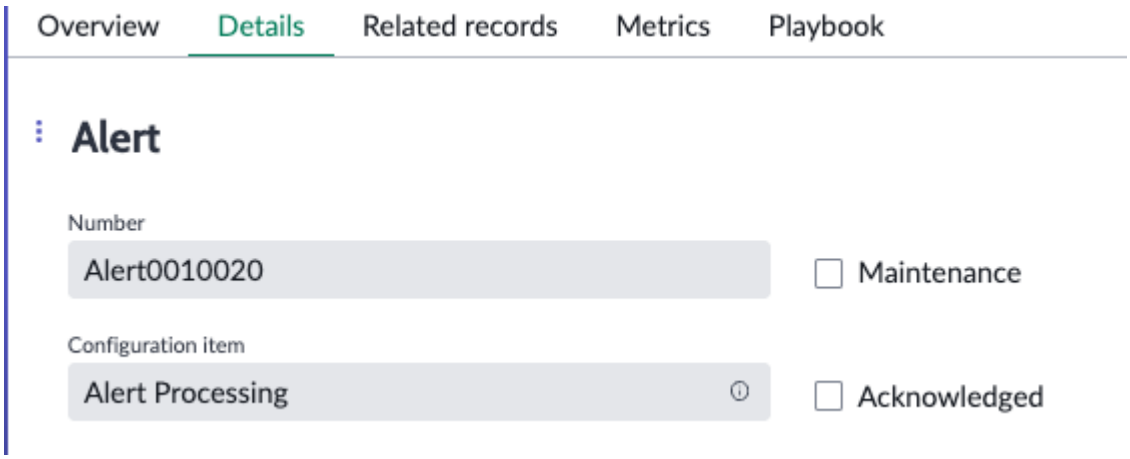
Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Filtern Sie mit **Aktive Warnungen** .
4. Wählen Sie eine Warnung aus.



5. Aktivieren Sie auf der Unterregisterkarte **Details** das Kontrollkästchen **Bestätigt**, um die Warnung in den Status „Bestätigt“ zu versetzen.
6. Klicken Sie auf **Speichern**.

Korrigieren Sie eine Warnung in Express-Liste

Führen Sie eine Korrekturaktion aus, um ein Problem manuell in einer Warnung direkt über zu beheben Express-Liste Bereich.

Vorbereitungen

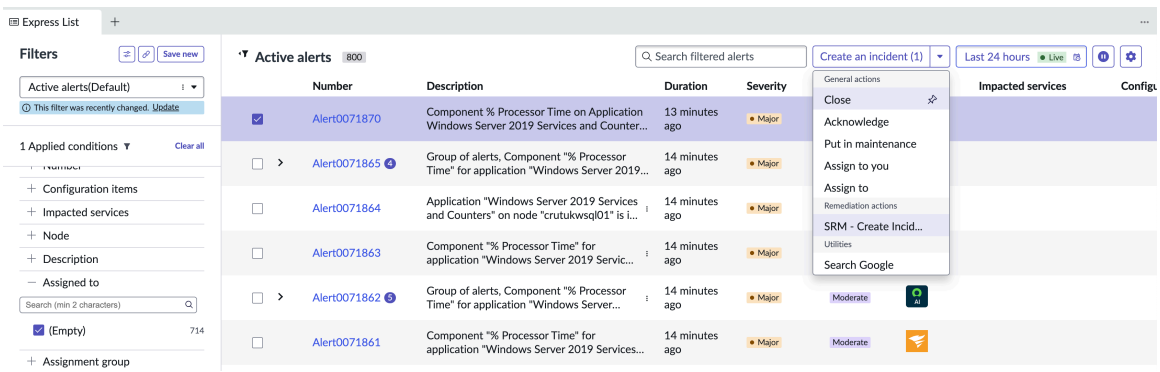
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
4. Wählen Sie die Korrekturaktion für die Warnung aus **Schließen** Dropdown-Liste.

Hinweis: Wenn die Liste leer ist, sind keine Korrekturaktionen verfügbar.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Metriken für eine Warnung an

Durch das Anzeigen von Metriken können Sie Verlaufsdaten im Zusammenhang mit dem CI einer Warnung verstehen.

Vorbereitungen

- Installieren Sie das Plugin Operational Intelligence (com.snc.sa.metric).
- Konfigurieren Sie die Metriken, die für die Warnung angezeigt werden sollen, wie in Warnungsmetriken konfigurieren beschrieben.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie eine Warnung aus, um sie zu öffnen.
4. Klicken Sie auf die Unterregisterkarte **Metriken**.
   Die konfigurierten Metriken werden auf der Seite angezeigt.

   Um die Metrikanzeige anzupassen, konfigurieren Sie die folgenden Eigenschaften auf der **Systemeigenschaften** > **Alle Eigenschaften** Seite:

   - `ws_metric.widgets_number_limit`: Geben Sie die Anzahl der Widgets/Datensätze an, die auf der Registerkarte „Metriken“ angezeigt werden können.
   - `ws_metric.datasets_per_widget_limit`: Geben Sie die Anzahl der Diagramme/Datensätze an, die in einem Diagramm angezeigt werden dürfen.

5. Wählen Sie in der Liste **Zeitbereich relativ zur Warnung** den Zeitbereich aus, für den die Metriken zur Warnung angezeigt werden sollen:
   - 1 Stunde vorher und nachher (Standardeinstellung)
   - 3 Stunden davor und danach
   - 5 Stunden davor und danach
   - Benutzerdefinierter Bereich (zum Konfigurieren eines benutzerdefinierten Zeitraums für die Metriken)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf einen Parameter unter einem Diagramm, um die Daten des Parameters im Diagramm auszublenden.
7. **Wahlweise:** Klicken Sie auf die Schaltfläche **Explorer für Einblicke**, um Metriken anzuzeigen, indem Sie sie mittels Drag-and-Drop auf der Zeitleiste ablegen.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Zeigen Sie Details zur Auswirkung und Ursache einer Warnung in an Express-Liste

Zeigen Sie Informationen zu einer Warnung auf der Registerkarte „Übersicht“ der Warnung in Express-Liste an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird in einer separaten Registerkarte geöffnet, auf der angezeigt wird **Übersicht** Registerkarte.
4. Zeigen Sie Warnungsinformationen auf der Registerkarte **Übersicht** an.

Registerkarte Übersicht

Abschnitt	Beschreibung
Zusammenfassung	Enthält eine Beschreibung der ausgewählten Warnung und beschreibt, warum der Sachverhalt als Problem betrachtet wird.
Auswirkung	Listet das Konfigurationselement und alle von der Warnung betroffenen Services auf. Die Kachel **Betroffene Services** enthält die folgenden untergeordneten Registerkarten: ○ **Anwendungsservices:** Die von der Warnung betroffenen Anwendungsservices. Weitere Informationen zu Anwendungsservices finden Sie unter Anwendungsservices . ○ **Related service offerings (Zugehörige Serviceangebote):** Die Serviceangebote, die mit den von der Warnung betroffenen Anwendungsservices verbunden sind. Anwendungsservices und die zugehörigen Serviceangebote werden auf einer Viele-zu-viele-Basis angezeigt. Das heißt: Mehrere Serviceangebote können sich auf einen oder mehrere Anwendungsservice(s) beziehen, und mehrere Anwendungsservices können sich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Beschreibung
	auf ein oder mehrere Serviceangebot(e) beziehen.
Ursache	Listet die Protokolleigenschaften mit Informationen auf, die zum Warnungsproblem beitragen, sowie wahrscheinliche Ursachen für die Warnung.

Zeigen Sie die Abhängigkeitsansichtszuordnung für CMDB-Warnungen in der Express-Liste an

Die Zuordnung „Abhängigkeitsansichten“ bietet Einblicke in die Gruppierung von Warnungen und unterstützt sowohl die Problembehandlung als auch die proaktive Verwaltung. Zeigt die verbindenden CIs zwischen CMDB-Warnungen innerhalb einer Gruppe an. Auch wenn ein CI nicht Teil der Gruppe ist, wird es auf der Karte angezeigt, wenn es eine Verbindung zu anderen Warnungs-CIs innerhalb der Gruppe herstellt.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user, evt_mgmt_Operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation entweder das Listensymbol ( ) Oder Express-Liste Symbol (.
3. Wählen Sie für eine Warnung, für die Sie die CI-Abhängigkeitsansicht anzeigen möchten, in den Spalten Konfigurationselemente das Konfigurationselement aus.
4. Wählen Sie im Fenster „Konfigurationselemente“ die Option aus **Öffnen Sie Die Abhängigkeitsansicht** .
   Sie können die Abhängigkeitsansicht der CMDB-Warnungen anzeigen.

Zeigen Sie Metrikdaten für Anomaliewarnungen im Vorschaubereich in an Express-Liste

Zeigen Sie Visualisierungen für Anomaliewarnungen an, um Anomalien mithilfe von Metrikdaten zu untersuchen, ohne sich von zu entfernen Express-Liste Vorschaubereich.

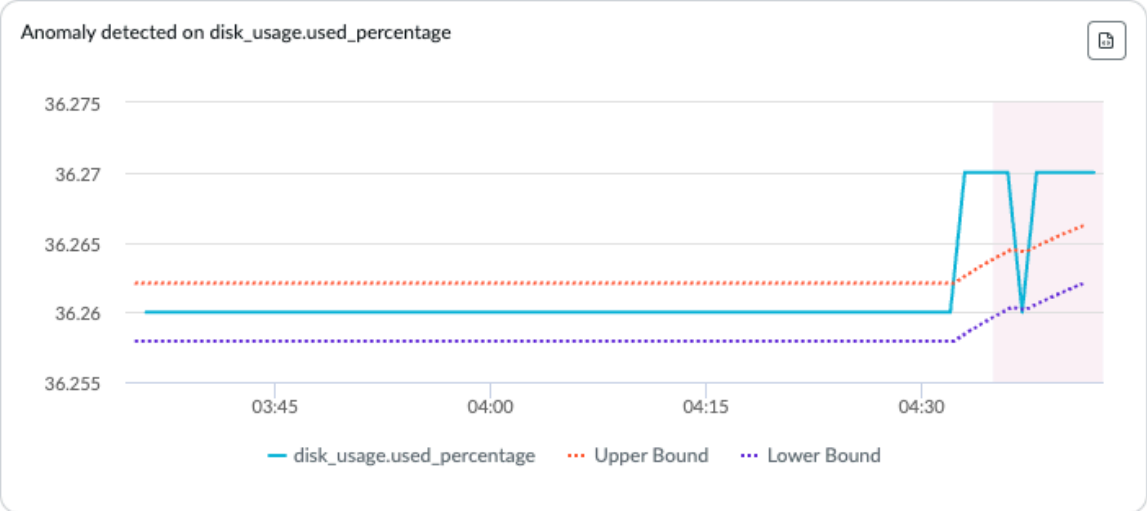
Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie in der Liste aktive Warnungen das Kontrollkästchen für eine Anomaliewarnung.
   Informationen in **Beschreibung** Spalte kann Ihnen helfen, zu bestimmen, welche Warnungen Anomaliewarnungen sind. Beispielsweise kann eine Warnungsbeschreibung warnen, wenn Werte sich den konfigurierten Schwellenwerten nähern oder diese überschreiten, oder Metriken oberhalb oder unterhalb einer definierten Grenze.
4. Wählen Sie im Vorschaubereich die Registerkarte Info aus.
   Je nachdem, wie die Metrikanomalie konfiguriert ist, wird eines von zwei Diagrammen angezeigt.

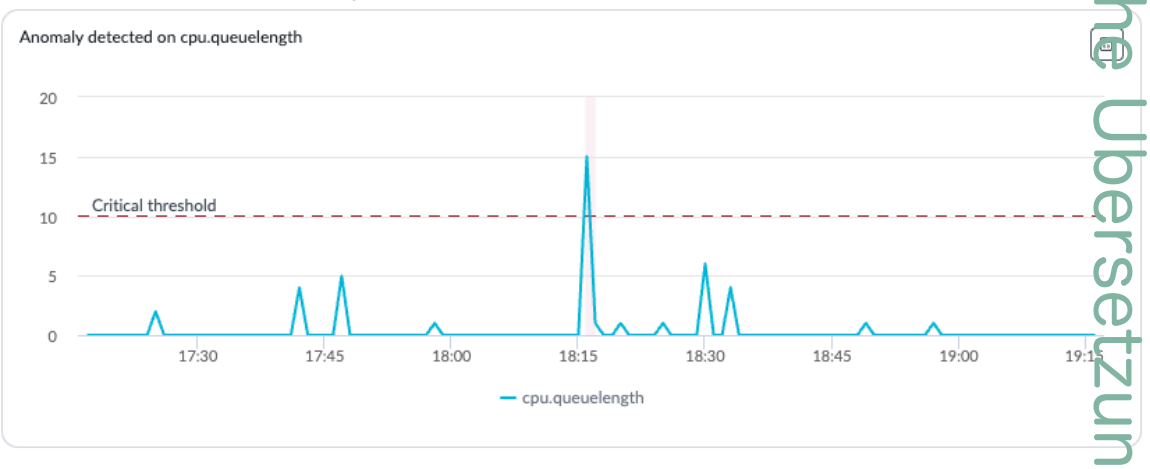
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn das Statistikmodell „Metrik Intelligence“ zum Erkennen von Anomalien verwendet wird, wird das Anomaliewarnungsdiagramm basierend auf Modellen für maschinelles Lernen mit Ober- und Untergrenzen angezeigt.



Weitere Informationen finden Sie unter Metrikdaten verstehen.

- Wenn Schwellenwerte von Administratoren konfiguriert werden, zeigt das Warnungsdiagramm der statischen Schwellenwertmetrik Anomalien an, die mithilfe der konfigurierten Schwellenwerte definiert



wurden.

Hinweis:

Die Rohdaten, die für das Metrikdiagramm im Vorschaubereich verwendet werden, sind nur sieben Tage lang verfügbar. Wenn ältere Warnungen ausgewählt sind und die Rohdaten nicht mehr verfügbar sind, wird kein Diagramm angezeigt.

Weitere Informationen finden Sie unter Metrikregeln erstellen.

5. **Wahlweise:** Überprüfen Sie die umgebenden Metrikdaten, indem Sie auswählen **In Metrik-Explorer öffnen** Symbol ( ) Im Informationsbereich.

(Optional) Die **Metrik** Auf der Registerkarte wird der Metrik-Explorer im Zeitrahmen der Anomalie angezeigt. Bei einer offenen Warnung wird das Diagramm Stunde vor und nach dem letzten Zeitpunkt der Ereignisgenerierung angezeigt. Für eine geschlossene Warnung wird das Diagramm eine Stunde vor und nach dem ersten Ereignis angezeigt,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das eine Warnung erstellt hat. Wenn keine Daten vorhanden sind, wird das Diagramm nicht angezeigt.

Weitere Informationen finden Sie unter Metric Explorer.

Anzeigen Log Analytics Anomaliewarnungsdiagramme im Vorschaubereich in Express-Liste

Zeigen Sie Visualisierungen für an Health Log Analytics Anomaliewarnungen auf dem Express-Liste Vorschaubereich, um Verhaltenszeiträume zu identifizieren, die von den erwarteten Bereichen abweichen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie in der Liste aktive Warnungen das Kontrollkästchen für Log Analytics Basierte Warnung. Diese Option ist nur für einzelne Warnungen oder die zugrunde liegenden einzelnen Warnungen innerhalb einer Gruppe verfügbar.
4. Wählen Sie im Vorschaubereich die Registerkarte Info aus.
   Ein Diagramm mit einer visuellen Darstellung der Anomalie wird angezeigt.
5. **Wahlweise:** Wählen Sie den Parameter aus, um Anomaliedaten innerhalb dieses Zeitraums zu visualisieren:
   - **Ereignisse pro Minute** – Die Standardeinstellung, die die erkannte Anomalie anzeigt.
   - **Tag her**
   - **Woche her**
6. **Wahlweise:** Überprüfen Sie relevante Protokolle im Kontext, indem Sie das Symbol in umgebenden Protokollen öffnen ( ) Im Informationsbereich.
   Die **Umgebende Protokolle** Auf der Registerkarte wird die Liste der Protokollzeilen angezeigt, die eine Minute vor und eine Sekunde nach generiert wurden Log Analytics Warnung. Weitere Informationen finden Sie unter Wie Health Log Analytics Warnungen generiert.

Zeigen Sie Daten zu betroffenen Services im Vorschaubereich in an Express-Liste

Zeigen Sie im Vorschaubereich zusätzliche Informationen zu betroffenen Services an, die an Warnungen gebunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie in der Liste aktive Warnungen ein Kontrollkästchen für Warnungen.
4. Öffnen Sie im Vorschaubereich die Registerkarte Info.
5. Bewegen Sie den Mauszeiger über den Abschnitt „Betroffene Services“, um Informationssymbole anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie das entsprechende Symbol aus, um zusätzliche Informationen zu einem betroffenen Service anzuzeigen.

Symbole für betroffene Serviceinformationen

Symbol	Name	Beschreibung
ⓘ	Info	Zeigt den Schweregrad, die Geschäftsrelevanz und eine Kurzbeschreibung des betroffenen Service an. In diesem Popup können Sie die Servicezuordnung in öffnen Service Operations-Arbeitsbereich Durch Auswahl von **Zeigen Sie die Servicezuordnung an** . Die Servicezuordnung zeigt den betroffenen Pfad von Warnungen an, sodass Sie ihre Auswirkungen auf den Service schnell bewerten können. Weitere Informationen finden Sie unter Zeigen Sie die einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich. Wenn für diesen Service Metrikdaten vorhanden sind, können Sie den Metrik-Explorer aus dem Popup öffnen, indem Sie auswählen **Zeigen Sie zugehörige Metriken an** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbol	Name	Beschreibung
	Kontaktperson/Gruppe	Zeigt den Namen des Besitzers des betroffenen Service und die ihm zugewiesene Supportgruppe an.

Zeigen Sie Daten zu Konfigurationselementen im Vorschaubereich in an Express-Liste

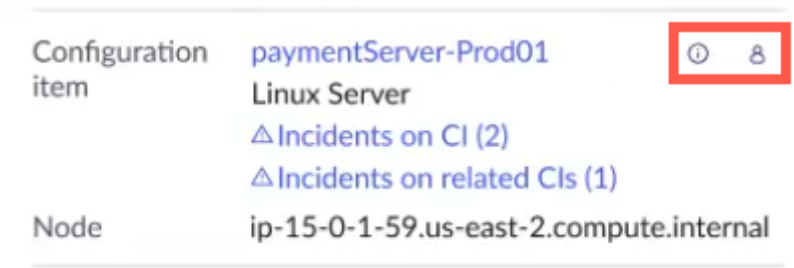
Zeigen Sie zusätzliche Details zu Konfigurationselementen (CIs) an, die an Warnungen in gebunden sind Express-Liste Vorschaubereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Aktivieren Sie in der Liste aktive Warnungen ein Kontrollkästchen für Warnungen.
4. Öffnen Sie im Vorschaubereich die Registerkarte Info.
5. Bewegen Sie den Mauszeiger über den Abschnitt „Konfigurationselement“, um Informationssymbole anzuzeigen.



6. Zeigen Sie zusätzliche Informationen zu einem CI an, indem Sie das entsprechende Symbol auswählen.

Symbole für Konfigurationselementinformationen

Symbol	Name	Beschreibung
	Info	Zeigt die Klasse, die IP-Adresse, den Standort und die Umgebung des CI an.
	Kontaktperson/Gruppe	Zeigt den Namen des Besitzers des CI, die ihm zugewiesene Supportgruppe und Avatare der einzelnen Teammitglieder an.

7. **Wahlweise:** Zeigen Sie an, wie das aktuelle CI mit anderen CIs verbunden ist, indem Sie auswählen **Zeigen Sie die CI-Topologie an** Im Bereich „zusätzliche Informationen“.
   Die **Abhängigkeitsansicht** Karte wird geöffnet. Die Zuordnung stellt die Beziehungen zwischen CIs visuell dar, sodass Sie verstehen, wie verschiedene Komponenten miteinander verbunden sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Blenden Sie geschlossene Warnungen in aus Express-Liste

Wählen Sie aus, ob die geschlossenen Warnungen in einer Warnungsgruppe sowie die offenen Warnungen im Vorschaubereich und in der Linkansicht angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie in der Liste aktive Warnungen eine Warnungsgruppe aus.

   Im Vorschaubereich wird die Standardanzeige angezeigt:

   - Auf der Registerkarte Warnungen und der Zeitleistenansicht werden nur die offenen Warnungen angezeigt. Die geschlossenen Warnungen sind ausgeblendet.
   - Die Linkansicht zeigt die Attribute offener und geschlossener Warnungen an.
4. Ändern Sie auf der entsprechenden Registerkarte die Anzeige.

   Im Vorschaubereich auf der Registerkarte Warnungen:

   a. Zeigen Sie sowohl die offenen als auch die geschlossenen Warnungen an, indem Sie wechseln **Schließen Sie Warnungen aus** Wechseln Sie zur Position Geschlossen.

   b. (Optional) Sortieren Sie die angezeigten Warnungen nach Zeit oder Schweregrad, indem Sie das Sortiersymbol ( ) Und dann das entsprechende Menüelement auswählen.

Hinweis: Wenn Sie den Umschalter wechseln oder die Warnungen in der Zeitleistenansicht sortieren, wird die Registerkarte Warnungen an Ihre Auswahl angepasst.

In Linkansicht: Zeigen Sie nur die Attribute offener Warnungen an, während Sie die der geschlossenen Warnungen ausblenden, indem Sie wechseln **Blenden Sie Attribute geschlossener Warnungen aus** Wechseln Sie zur offenen Position.

Zeigen Sie eine Warnungsanalyse von an Now Assist In Express-Liste

Zeigen Sie eine von erstellte Warnungsanalyse an Now Assist Generative KI verwenden. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, damit Sie die Warnung effektiver untersuchen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basiert, CMDB, Log Analytics, Gemischt Und auf Netzwerkdatenverkehr basierende Warnungsgruppen. Für alle anderen Warnungsgruppentypen Now Assist für ITOM Analysiert nur die übergeordnete Warnung.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Neben der Warnung.
4. Im Vorschaubereich **Info** Wählen Sie die Registerkarte aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

6. **Wahlweise:** Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Warnungsanalysesymbole

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Fall wird aus einer Warnung generiert

Aktivieren Sie eine schnelle Lösung, indem Sie Fälle aus Warnungen entweder manuell oder automatisch generieren.

Kundenservice-Management bietet Integration mit ITOM Ereignismanagement. Diese Integration ermöglicht Ihnen, die Kunden-Experience zu verbessern, indem Sie Strukturen aufbrechen, die zwischen den Prozessen und Systemen bestehen, die von Front-Line-Kundenservice- und Back-Office-Betriebsteams verwendet werden. Indem Sie proaktiv Probleme überwachen und Fälle erstellen, können Sie Kundenprobleme besser korrelieren und so schneller Antworten liefern.

Mit der Integration zwischen den Anwendungen Kundenservice-Management und Ereignismanagement können Sie für die von einer Warnung betroffene Kunden-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installationsbasis einen Fall erstellen. Weitere Informationen finden Sie unter Erstellen Sie manuell einen proaktiven Fall aus einer Warnung . Sie können auch eine Warnungsregel aktivieren, um automatisch einen proaktiven Fall aus einer Warnung zu erstellen, wenn ein Incident erstellt wird. Weitere Informationen finden Sie unter Aktivieren Sie eine Warnungsregel, um automatisch einen proaktiven Fall aus einer Warnung zu erstellen .

Entfernen Sie Warnungen aus einer Warnungsgruppe in Express-Liste

Entfernen Sie sekundäre Warnungen aus einer Warnungsgruppe direkt aus dem Express-Liste Oder im Vorschaubereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und hat keine Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Entfernen Sie eine sekundäre Warnung aus einer Warnungsgruppe.
   Sie können Warnungen aus einer Gruppe entfernen, unabhängig davon, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnungsgruppe ausgewählt ist.

Standort	Aktion
Die Express-Liste Bereich	**a.** Wählen Sie in der Liste aktive Warnungen das Chevron-Symbol ( ) Am Anfang einer oder mehrerer Warnungsgruppenzeilen, um die in der Gruppe enthaltenen Warnungen anzuzeigen. **b.** Wählen Sie eine oder mehrere sekundäre Warnungen aus. **c.** Von **Schließen** Dropdown-Liste oben rechts in der Liste auswählen **Aus Gruppe entfernen** . **Hinweis:** Wenn Sie versuchen, die einzige sekundäre Warnung aus einer Warnungsgruppe zu entfernen und dadurch die Gruppierung der Gruppe aufzuheben, wird eine Meldung angezeigt, mit der Sie die Aktion rückgängig machen können.
Die Express-Liste Vorschaubereich für eine Gruppe von Warnungen	**a.** In **Warnungen in Gruppe** Wählen Sie eine Warnungskachel aus. **b.** Wählen Sie das Symbol weitere Aktionen ( ). **c.** Wählen Sie Aus **Aus Gruppe entfernen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

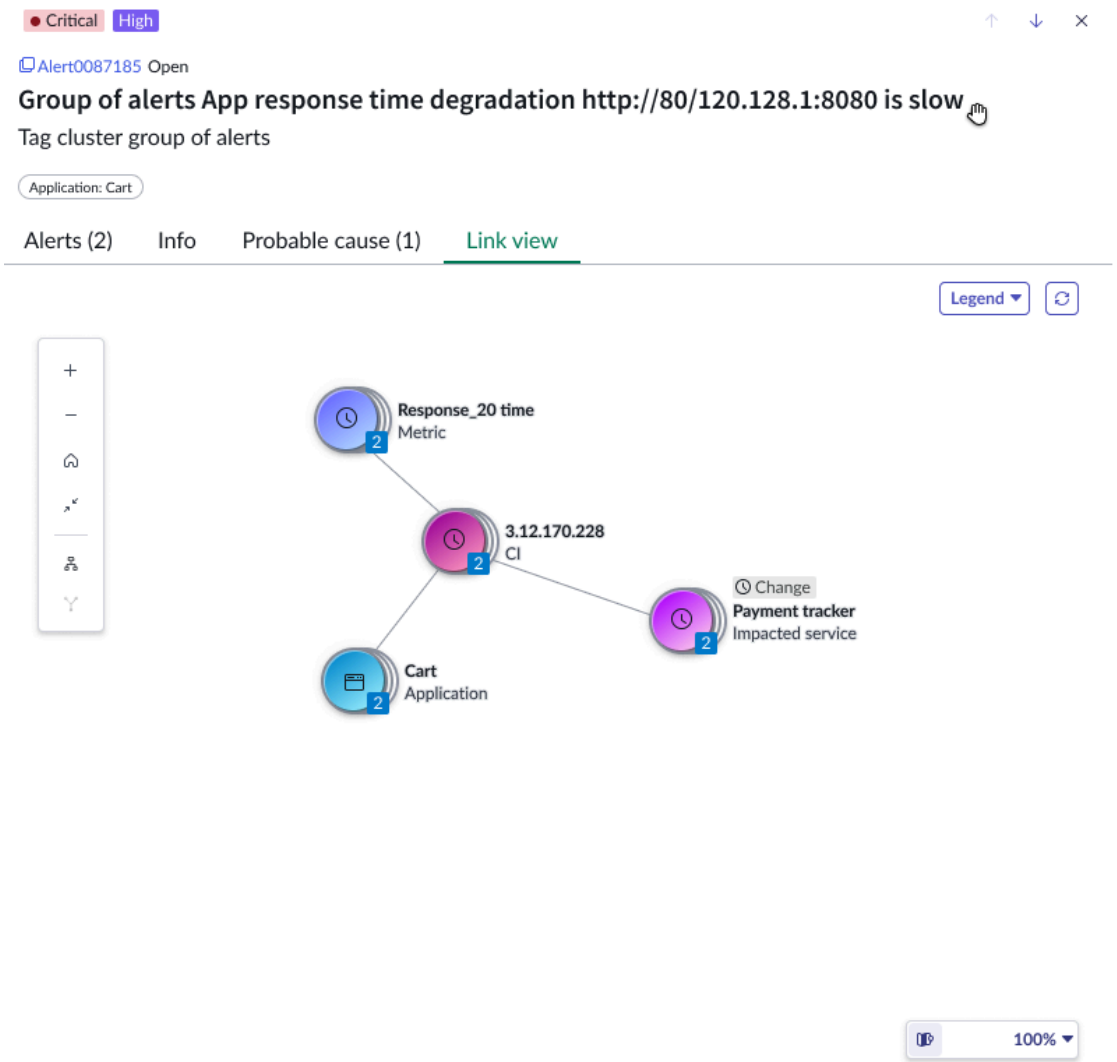
Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste

Verschaffen Sie sich ein besseres Verständnis der Beziehungen zwischen Warnungen in Warnungsgruppen in der Express-Liste Mithilfe der Linkansicht. Die Linkansicht bietet eine visuelle Darstellung der Beziehungen zwischen den Warnungen in einer Gruppe.

Wenn Ereignismanagement Generiert eine Warnungsgruppe. Die Verknüpfungsansicht zeigt, wie die Attribute der Warnungen in der Gruppe verknüpft sind. Die farbigen Tags stellen dar c Konfiguration ich Tems (CIs) und andere Umgebungselemente in Bezug auf die Warnungen.

Die in der Linkansicht angezeigten Informationen sind verfügbar, ohne dass ein ausgefüllter erforderlich ist Configuration Management Database (CMDB). Wenn jedoch CMDB Ist ausgefüllt, bietet die Linkansicht zusätzlichen Wert, indem die wahrscheinliche Ursache der Warnungen und der Service angegeben werden, auf den sich die Warnungsgruppe auswirkt.

Beispiel für eine Warnungsgruppe in der Linkansicht



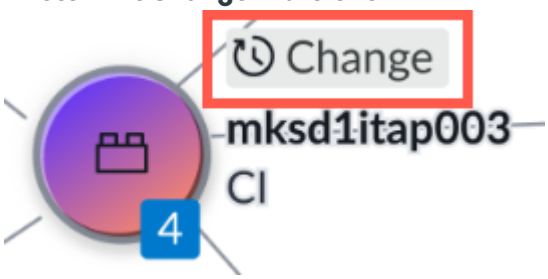
Sie können sich auf Ihre Interessenbereiche konzentrieren, indem Sie die Knoten in der Linkansicht an verschiedene Positionen ziehen. Wenn Sie eine Warnungsgruppe aktualisieren, werden neu angeordnete Knoten wieder an ihrer ursprünglichen Position angezeigt. Daher wird die Linkansicht nicht automatisch aktualisiert, sondern wartet darauf, dass Sie dies manuell tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn sich eine Warnung für ein CI auf einen Service in auswirkt Configuration Management Database (CMDB), Die Linkansicht zeigt den betroffenen Service an, sodass Sie ihn für eine schnelle Selektierung auf einen Blick anzeigen können.

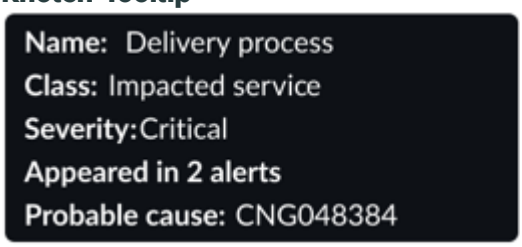
Ein gestapelter Knoten gibt an, dass mehrere Knoten für dasselbe Tag zugeordnet wurden. Wenn dasselbe Schlüssel-Wert-Paar in mehr als einer Warnung angezeigt wird, wird der entsprechende Knoten mit einem Abzeichen angezeigt. Wenn beispielsweise dasselbe Schlüssel-Wert-Paar in zwei Warnungen angezeigt wird, zeigt das Abzeichen auf dem Knoten die Zahl 2 an, wie auf dem Zahlungstracker-Knoten in der Beispiel-Warnungsgruppenfigur zu sehen ist. Wenn ein Knoten kein Abzeichen hat, wird das Schlüssel-Wert-Paar angezeigt S In nur einer Warnung. Eine aktive Change-Anforderung, eine wahrscheinliche Ursache der Warnung, wird durch ein Change-Abzeichen markiert.

Knoten mit Change-Abzeichen



Die Legende der Linkansicht listet die Bedeutung der verwendeten Symbole und Farben auf Aktiviert Sie können zwischen dem Ausblenden und Anzeigen von Tags-Typen umschalten, um Rauschen zu reduzieren. Darüber hinaus beschreibt die Legende die Bedeutung der verschiedenen Zeilen, die die Warnungsattribute verknüpfen. Attribute, die durch eine durchgezogene Linie verknüpft sind, teilen eine oder mehrere Warnungen, während Attribute, die durch eine gepunktete Linie verknüpft sind, durch Gruppierungskriterien korreliert werden. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in Express-Liste Link-Ansicht. Wenn Sie den Mauszeiger über einen Knoten bewegen, wird ein Tooltip angezeigt, der den Namen des Tags, seine Klasse, seinen Schweregrad, die Anzahl der Warnungen, in denen sie aufgetreten sind, und ob die Warnung primär oder sekundär ist oder die wahrscheinliche Ursache der Warnung, falls zutreffend.

Knoten-Tooltip



Derzeit wird die Linkansicht für mehrere Warnungsgruppen unterstützt. Weitere Informationen finden Sie unter Die folgenden Themen :

- Anzeigen von Links zwischen Warnungen in Tag-basierten Warnungsgruppen
- Anzeigen von Links zwischen Warnungen in regelbasierten Warnungsgruppen
- Anzeigen von Links zwischen Warnungen in CMDB-basierten Warnungsgruppen
- Anzeigen von Links zwischen Warnungen in auf Netzwerkdatenverkehr basierenden Warnungsgruppen
- Anzeigen von Links zwischen Warnungen in Protokoll Analytics-basierten Warnungsgruppen
- Anzeigen von Links zwischen Warnungen in gemischten Warnungsgruppen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

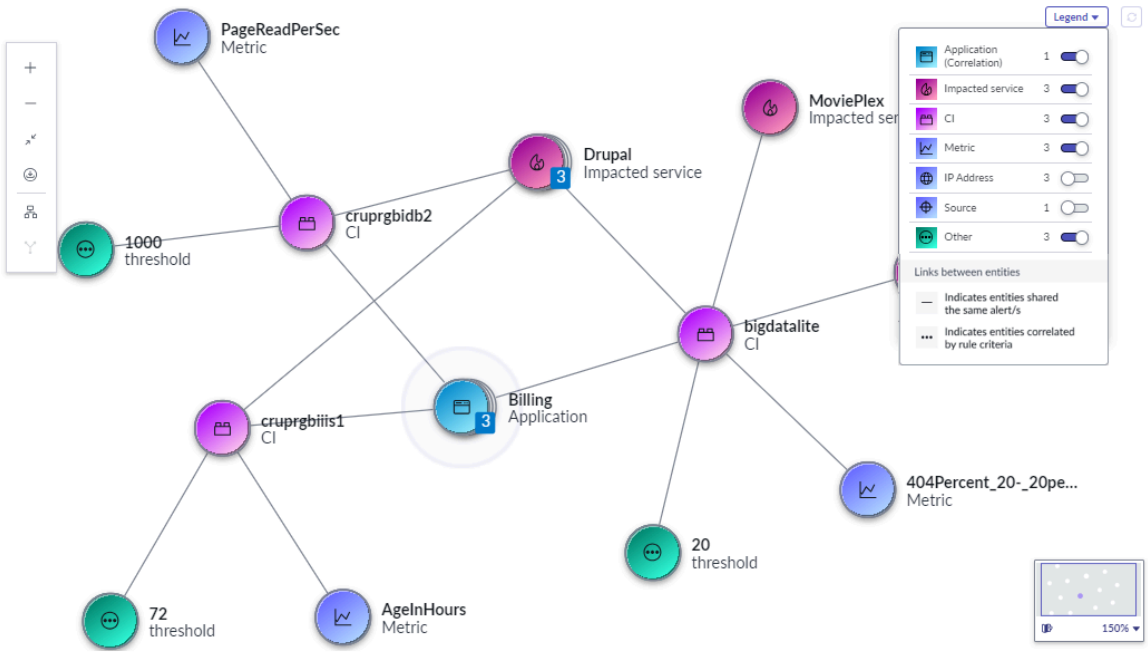
Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Anzeigen von Links zwischen Warnungen in Tag-basierten Warnungsgruppen

Zeigen Sie die Verbindungen zwischen Warnungen in einer Tag-basierten Warnungsgruppe in an Express-Liste Mithilfe der Linkansicht. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

Wenn Sie Warnungs-Tags und festgelegt haben Ereignismanagement Hat basierend auf Tag-basierten Regeln eine Warnungsgruppe generiert. Die Linkansicht bietet eine visuelle Darstellung der Beziehungen zwischen den Warnungen in der Gruppe. Die farbigen Tags in der Ansicht stellen Konfigurationselemente (Configuration Items, CIs) und andere Umgebungselemente in Bezug auf die Warnungen dar.

Beispiel für eine Tag-basierte Warnungsgruppe in der Linkansicht



In diesem Beispiel ist das definierende Tag für die Korrelation, Anwendung, mit den Tags der relevanten CIs verknüpft. Eine Korrelation kann jedoch durch ein beliebiges Tag oder eine Kombination aus zwei Tags definiert werden, z. B. Ressourcen- und Metrikname. Wenn das definierende Tag in der Linkansicht fehlt, basierte die Korrelation auf Informationen, die in der Ansicht nicht dargestellt werden, z. B. die Beschreibung. Jeder CI-Knoten ist weiter mit den Tags verknüpft, die in derselben Warnung wie dieses CI angezeigt wurden.

In einer Warnungsgruppe, die aus Tag-Regeln generiert wurde, bedeuten Knoten, die durch eine gestrichelte Linie verbunden sind, eine ungefähre Fuzzy-Übereinstimmung. Dies bedeutet, dass die Knoten korreliert wurden, wenn die Übereinstimmung mit der Tag-Regel nicht exakt war, aber geschlossen genug war, um signifikant zu sein. Dies kann beispielsweise passieren, wenn ein Standort, eine E-Mail-Adresse oder ein IP-Muster ähnlich genug waren, um als Übereinstimmung zu qualifizieren.

Die Legende der Linkansicht listet die Bedeutung der Symbole und Farben auf, die zur Darstellung der Tags und ihrer Anzahl eindeutiger Knoten verwendet werden. In der Legende werden Definierende Tags als Korrelation markiert. Sie können zwischen dem Ausblenden und Anzeigen von Tag-Typen umschalten, um Rauschen zu reduzieren. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in Express-Liste Link-Ansicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste

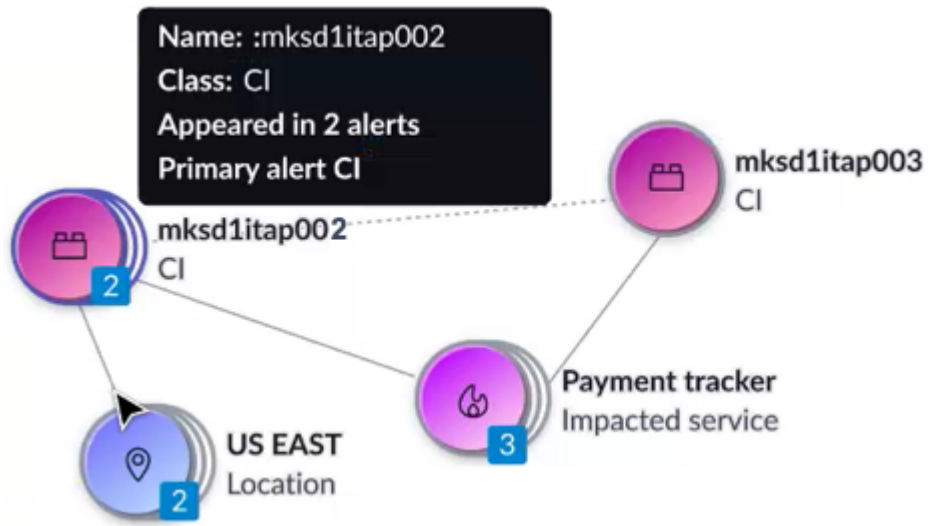
Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Anzeigen von Links zwischen Warnungen in regelbasierten Warnungsgruppen

Zeigen Sie die Verbindungen zwischen Warnungen in einer regelbasierten Warnungsgruppe in an Express-Liste Mithilfe der Linkansicht. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

Wenn Sie Warnungsregeln und festgelegt haben Ereignismanagement Hat basierend auf diesen Regeln eine Warnungsgruppe generiert. Die Linkansicht bietet eine visuelle Darstellung der Beziehungen zwischen den Warnungen in der Gruppe. Die farbigen Tags in der Ansicht stellen Konfigurationselemente (Configuration Items, CIs) und andere Umgebungselemente in Bezug auf die Warnungen dar.

Beispiel für eine regelbasierte Warnungsgruppe in der Linkansicht



Regelbasierte Warnungsgruppen bestehen aus einer primären Warnung und einer oder mehreren sekundären Warnungen. Die primäre Warnung wird direkt generiert und in der Linkansicht als Startknoten dargestellt. Sekundäre Warnungsknoten sind mit dem Startknoten durch eine gestrichelte Linie verbunden, was darauf hinweist, dass sie nicht dieselbe Warnung teilen, sondern anhand von Regelkriterien korreliert werden. Eine durchgezogene Linie zwischen Knoten gibt an, dass die verbundenen Knoten dieselbe Warnung oder mehrere Warnungen teilen.

Wenn sich eine Warnung für ein CI auf einen Service in auswirkt Configuration Management Database (CMDB), Die Linkansicht zeigt den betroffenen Service an, sodass Sie ihn für eine schnelle Selektierung auf einen Blick anzeigen können. Wenn Sie den Mauszeiger über einen Knoten bewegen, wird ein Tooltip angezeigt, der den Namen des Tags, seinen Typ, die Anzahl der Warnungen, in denen es aufgetreten ist, und ob es sich um eine primäre oder sekundäre Warnung handelt.

Zugehörige Informationen

Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Automatische Übersetzung

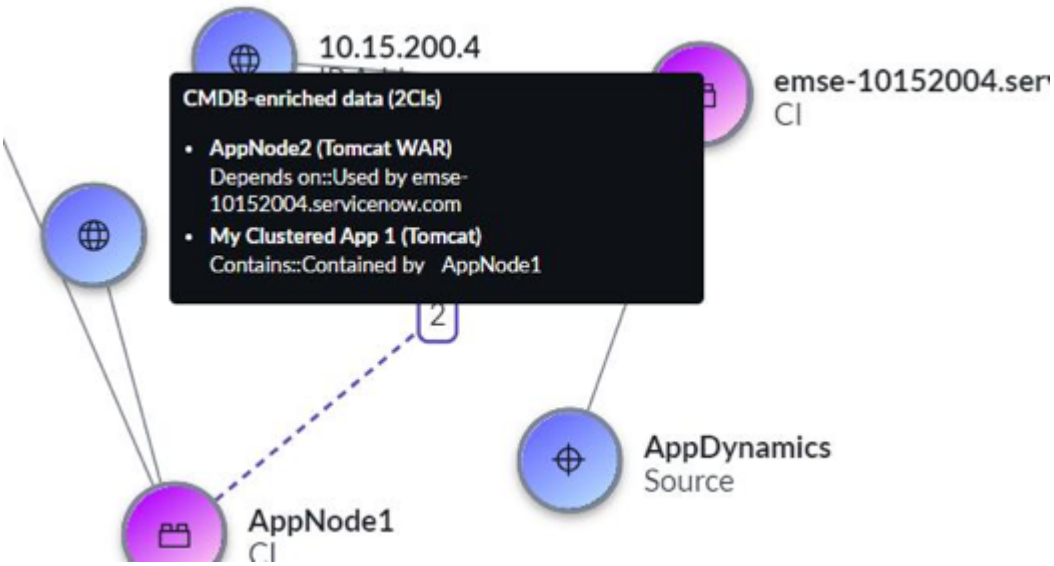
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen von Links zwischen Warnungen in CMDB-basierten Warnungsgruppen

Zeigen Sie die Verbindungen zwischen Warnungen in Warnungsgruppen in an Express-Liste Die basierend auf der Nähe von Konfigurationselementen (Configuration Items, CIs) in erstellt wurden Configuration Management Database (CMDB). Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

Wenn Warnungen für CIs in der Nähe zueinander im angezeigt werden CMDB Topologie tritt innerhalb eines bestimmten Zeitrahmens auf, Ereignismanagement Generiert eine CMDB-basierte Warnungsgruppe. Ereignismanagement Korreliert CIs in einer Servicezuordnung, wenn sie durch maximal drei andere CIs getrennt sind. Die farbigen Tags in der Linkansicht bieten eine visuelle Darstellung der CIs und anderer Umgebungselemente in Bezug auf die Warnungen in der Gruppe.

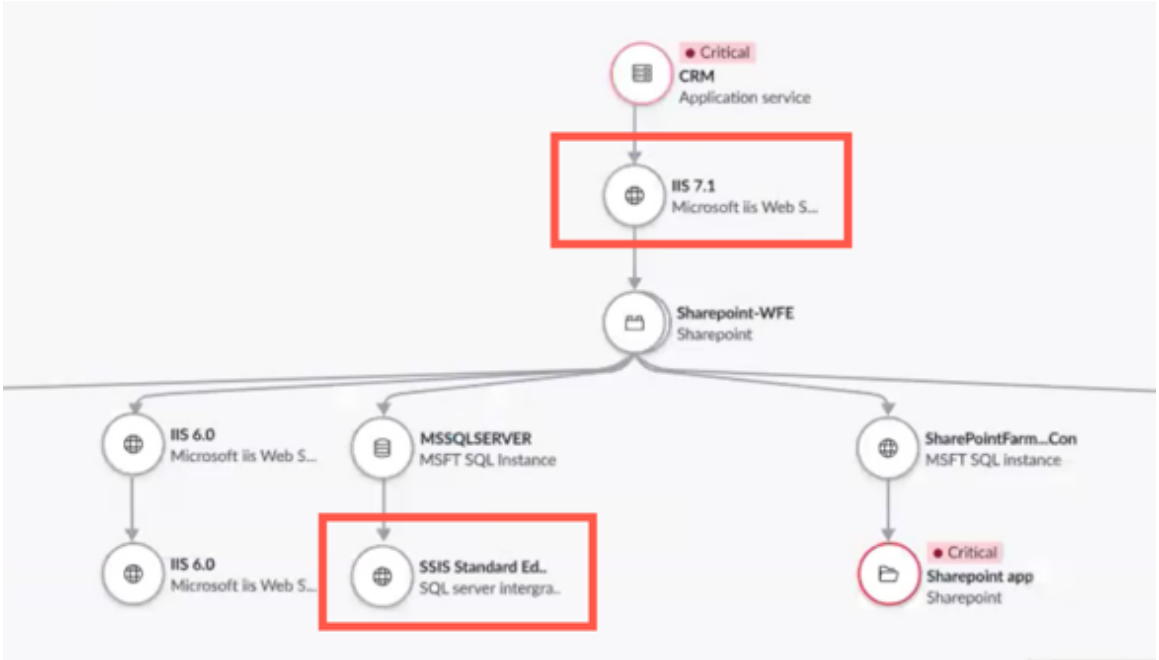
Beispiel für CMDB-basierte Warnungsgruppe in der Linkansicht



In dieser Beispiel-Link-Ansicht einer CMDB-basierten Warnungsgruppe gibt die gestrichelte Linie mit der Zahl 2 zwischen den CIs an, dass die CIs nicht direkt verbunden sind, sondern in der Servicezuordnung im durch zwei CIs getrennt sind CMDB Topologie. Das Beispiel CMDB Die Servicezuordnung zeigt auch korrelierte CIs, getrennt durch zwei CIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Servicezuordnung mit korrelierten CIs



Zugehörige Informationen

Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Anzeigen von Links zwischen Warnungen in auf Netzwerkdatenverkehr basierenden Warnungsgruppen

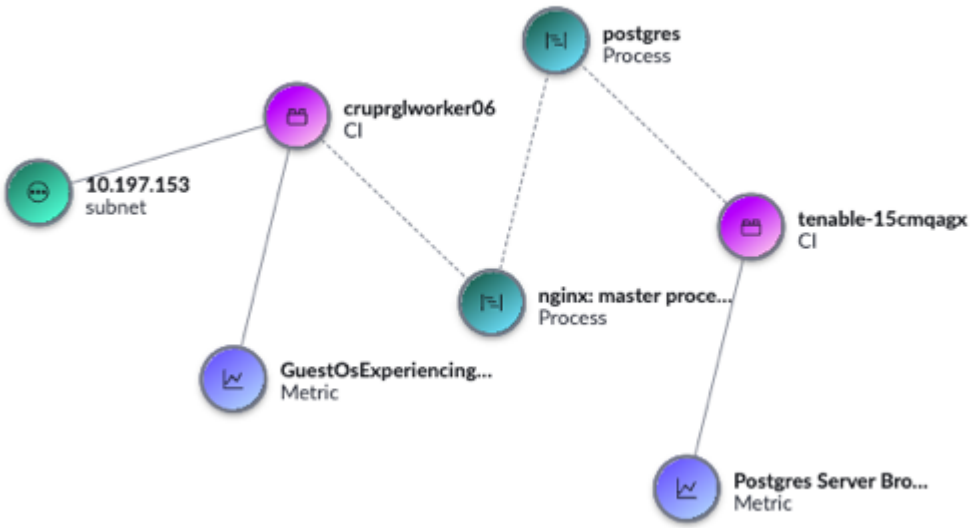
Zeigen Sie die Verbindungen zwischen Warnungen in auf Netzwerkdatenverkehr basierenden Warnungsgruppen in an Express-Liste Mithilfe der Linkansicht. Netzwerkdatenverkehrsbasierte Warnungsgruppen werden erstellt, indem Netzwerkdatenverkehrsverbindungen zwischen Prozessen auf Hosts analysiert werden.

Durch ML-Service-Mapping identifizierte Servicekandidaten , Gruppieren Sie Warnungen basierend auf Netzwerkverkehrsverbindungen zwischen Prozessen. Die Linkansicht zeigt eine kontextbezogene Ansicht von Netzwerk-Incidents basierend auf diesen Gruppen direkt verbundener Prozesse. Servicekandidaten sind potenzielle Sammlungen von Prozessen in Ihrer IT-Umgebung, die basierend auf ihren Netzwerkverbindungen und Interaktionen identifiziert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine auf Netzwerkverkehr basierte Warnungsgruppe in der Linkansicht



In dieser Beispiel-Link-Ansicht einer auf Netzwerkverkehr basierenden Warnungsgruppe zeigen die gestrichelten Linien an, dass verbundene Prozesse für die CIs ausgeführt werden. Attribute, die durch eine durchgezogene Linie verknüpft sind, teilen eine oder mehrere Warnungen.

Zugehörige Informationen

Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Anzeigen von Links zwischen Warnungen in Protokoll Analytics-basierten Warnungsgruppen

Verwenden Sie die Linkansicht in der Express-Liste, um zu sehen, warum Warnungen in einer Protokoll Analytics-basierten Warnungsgruppe durch die Visualisierung freigegebener Attribute korreliert werden.

Die Linkansicht für Protokoll-Analytics-basierte Warnungsgruppen zeigt die Verbindungen zwischen komponentenbasierten Warnungen an. Jede komponentenbasierte Warnung kann mehrere Host-Konfigurationselemente (CIs) umfassen. Eine Komponente stellt einen logischen Teil einer Serviceinstanz dar, in der die Warnung erkannt wurde. Komponenten können aus mehreren CIs bestehen, die dieselbe Funktion ausführen, z. B. aus mehreren redundanten Hosts. Weitere Informationen finden Sie unter Typen von Health Log Analytics Warnungen.

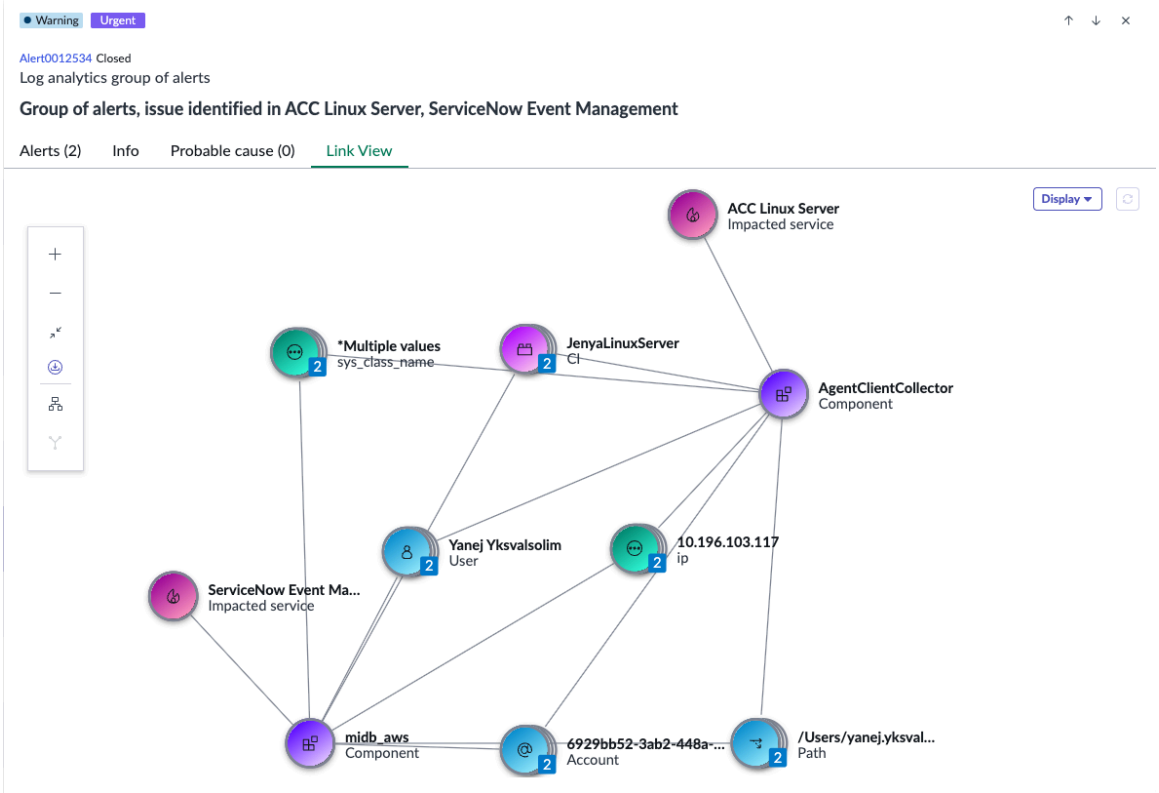
Die farbigen Tags in der Linkansicht stellen Attribute der Warnungen dar, z. B. Hosts, Anwender oder Korrelationsindikatoren, die aus den Protokollen extrahiert wurden. Die Linien verbinden Attribute, die dieselbe Warnung teilen. Diese Visualisierung hilft Ihnen, die Beziehungen zwischen verschiedenen Warnungen in der Gruppe anhand ihrer freigegebenen Attribute zu verstehen.

Log Analytics-basierte Gruppen enthalten häufig mehrere Korrelationsattribute innerhalb einer einzigen Gruppe. Mit der Linkansicht können Sie untersuchen, warum erkannte Anomalien in verschiedenen Komponenten zu einer Gruppe korreliert wurden. Durch die Bearbeitung der Attributanzeige können Sie die Beziehungen zwischen Warnungen besser verstehen, die gemeinsame Attribute aufweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Protokoll-Analytics-basierte Warnungsgruppe in der Linkansicht

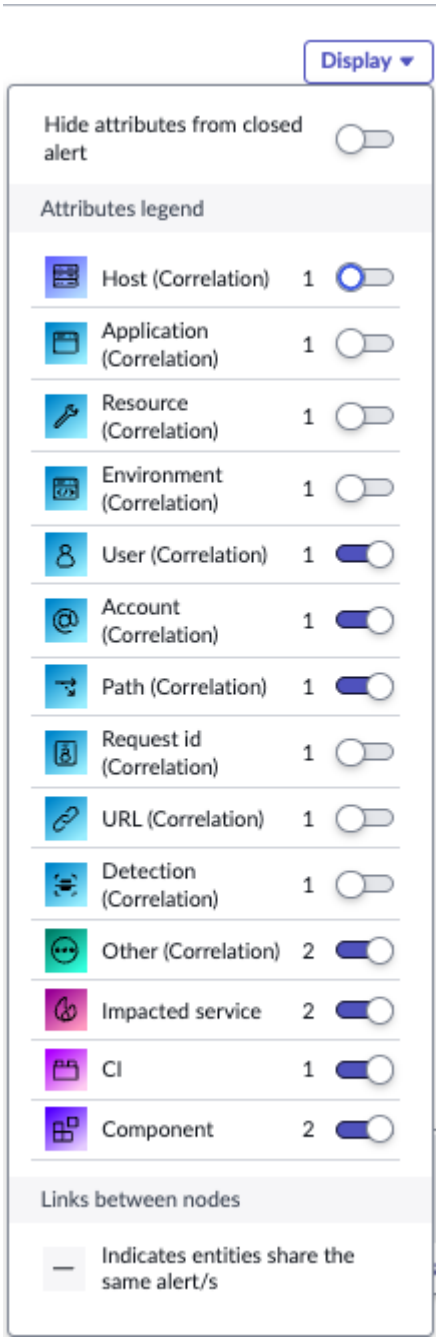


In dieser Beispiel-Linkansicht wird für jede untergeordnete Warnung in der Log Analytics-Warnungsgruppe ein Komponentenattribut angezeigt. Andere Attribute zeigen Verbindungen zwischen den Komponentenwarnungen an.

Die Legende der Linkansicht listet die Bedeutung der Symbole auf, die zur Darstellung der Attribute verwendet werden. Sie können zwischen dem Ausblenden und Anzeigen von Attributtypen umschalten, um Rauschen zu reduzieren. Eine Beschreibung der einzelnen Attribute finden Sie unter Attribute in Express-Liste Link-Ansicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Anzeigen von Links zwischen Warnungen in gemischten Warnungsgruppen

Zeigen Sie die Verbindungen zwischen Warnungen in gemischten Warnungsgruppen in an Express-Liste Mithilfe der Linkansicht. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

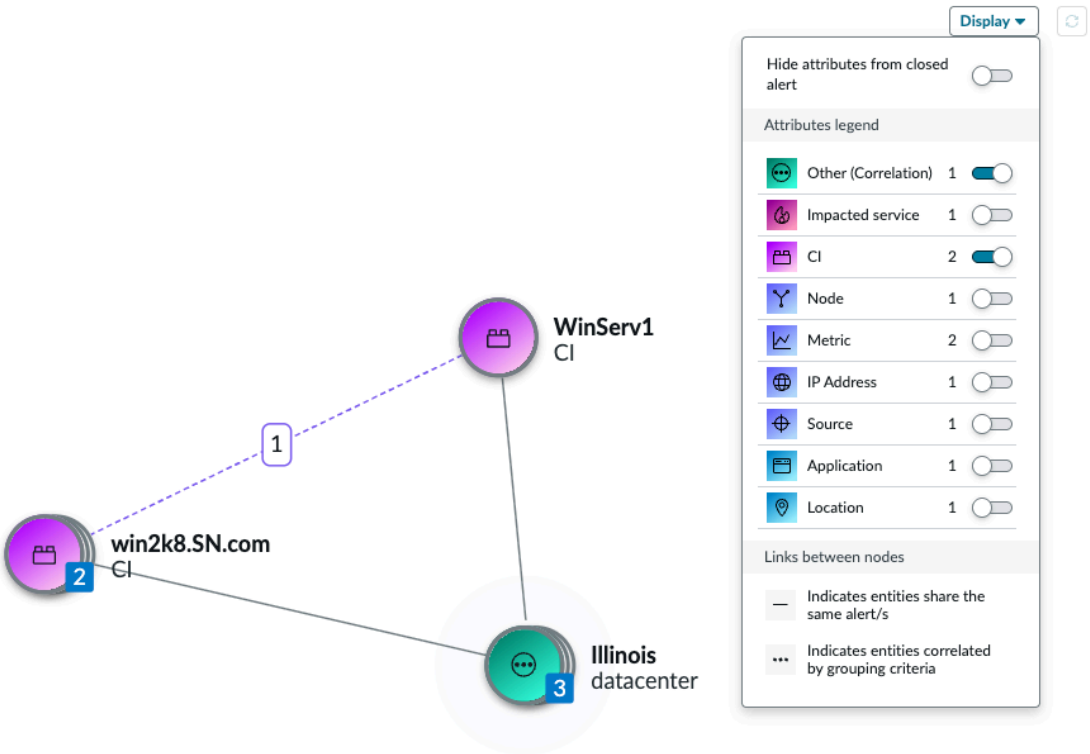
Die Linkansicht für gemischte Warnungsgruppen zeigt die Verbindungen zwischen Warnungen in Gruppen an, die verschiedene Warnungsgruppenstrategien kombinieren, um eine einzige zusammenhängende Gruppe zu bilden. Weitere Informationen finden Sie unter Gemischte Warnungsgruppierung.

Informationen zum Anzeigen, wie verschiedene Warnungsgruppen in der Linkansicht visualisiert werden, finden Sie in der Beschreibung der Linkansicht für die relevanten Warnungsgruppentypen. Derzeit bestehen gemischte Gruppen aus Tag-Cluster-Warnungsgruppen und CMBD-basierten Warnungsgruppen. Weitere Informationen zur Linkansicht für diese Gruppen finden Sie unter Anzeigen von Links zwischen Warnungen in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-basierten Warnungsgruppen, Und Anzeigen von Links zwischen Warnungen in CMDB-basierten Warnungsgruppen.

Beispiel für gemischte Warnungsgruppe in der Linkansicht



In dieser Beispiel-Link-Ansicht einer gemischten Warnungsgruppe gibt die gestrichelte Linie mit der Zahl 1 zwischen den CIs an, dass die CIs nicht direkt verbunden sind, sondern durch ein CI in der Servicezuordnung in getrennt sind CMDB Topologie. Das Beispiel zeigt auch das definierende Attribut für die Korrelation, das Rechenzentrum, das mit den relevanten CIs verknüpft ist.

Die Linkansicht **Anzeige** Legende listet die Bedeutung der Symbole auf, die zur Darstellung der Tags verwendet werden, und ihre Anzahl eindeutiger Knoten. In der Legende werden Definierende Tags als Korrelation markiert. Sie können zwischen dem Ausblenden und Anzeigen von Tag-Typen umschalten, um Rauschen zu reduzieren. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in Express-Liste Link-Ansicht.

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Wenn eine Warnungsgruppe generiert wird, können Sie besser verstehen, wie die Warnungen in der Gruppe verknüpft werden, indem Sie eine visuelle Darstellung ihrer Beziehungen in der Linkansicht anzeigen.

Vorbereitungen

Für eine Übersicht über die Linkansicht in Express-Liste, Siehe Anzeigen von Links zwischen Warnungen in Warnungsgruppen in Express-Liste.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation die aus Express-Liste Symbol ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie in den Feldern im interaktiven Filterbereich aus **Gruppe** Und dann das Kontrollkästchen für die Warnungsgruppen, die Sie anzeigen möchten.

   Hinweis: Derzeit wird die Linkansicht für Tag-basierte, regelbasierte, CMDB-basierte und auf Netzwerkverkehr basierende Warnungsgruppen unterstützt.

   - **Tag-Cluster**
   - **Regelbasiert**
   - **CMDB**
   - **Netzwerkverkehr**

4. In **Aktive Warnungen** Liste die Beschreibung einer Warnungsgruppe auswählen.
   Der Vorschaubereich wird für geöffnet **Warnungen in Gruppe** Registerkarte, die alle korrelierten Warnungen in der ausgewählten Gruppe auflistet.
5. Navigieren Sie zu **Link-Ansicht** .
6. Zeigen Sie die Beziehungen zwischen allen Warnungen in der ausgewählten Gruppe an.
7. **Wahlweise:** Führen Sie die folgenden optionalen Aufgaben aus.

Aufgabe	Aktion
Konzentrieren Sie sich auf einen Bereich von Interesse	Wählen Sie einen oder mehrere Knoten aus, und ordnen Sie sie in der Linkansicht neu an, indem Sie sie an eine neue Position ziehen. **Hinweis:** Nach dem Aktualisieren der Warnungsgruppe werden die Knoten wieder an ihrer ursprünglichen Position angezeigt.
Aktualisieren Sie die Warnungsgruppe	Wählen Sie Aus **Aktualisieren** . Wenn Sie die Warnungsgruppe aktualisiert haben, werden neu angeordnete Knoten wieder an ihrer ursprünglichen Position angezeigt. Neu hinzugefügte Knoten sind als Neu markiert. **Hinweis:** Die **Aktualisieren** Die Schaltfläche ist aktiviert, wenn neue Daten für die Warnungsgruppe verfügbar sind. Die Linkansicht wird nicht automatisch aktualisiert.
Zeigen Sie die Bedeutung von Symbolen und Farben an	Wählen Sie die Legende der Link-Ansicht aus. (Optional) Die Legende gibt auch die Anzahl der eindeutigen Knoten an, die pro Tag angezeigt werden. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in Express-Liste Link-Ansicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

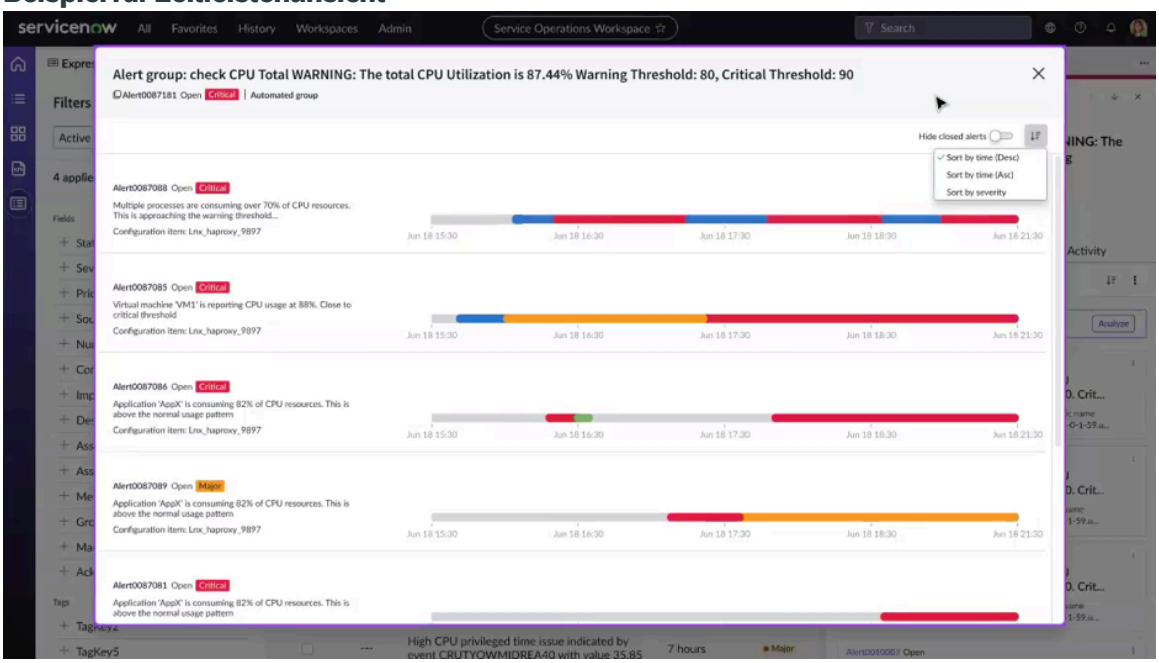
Aufgabe	Aktion
Reduzieren Sie das Rauschen	Wechseln Sie in der Legende der Linkansicht zwischen dem Ausblenden und Anzeigen eines Tag-Typs.
Zeigen Sie Informationen zu einer Warnung an	Bewegen Sie den Mauszeiger über einen Knoten, um einen Tooltip mit Informationen anzuzeigen.

Untersuchen chronologischer Daten zu Warnungen in einer Warnungsgruppe in Express-Liste

Visualisieren Sie die chronologische Sequenz von Ereignissen innerhalb einer Warnungsgruppe in Express-Liste Mit der Zeitleistenansicht. Diese Funktion bietet einen umfassenden Überblick darüber, wann die Warnungen aufgetreten sind, ihren Schweregrad ändert sich und andere relevante Daten für eine effiziente Selektierung und eine durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR).

In der Zeitleistenansicht wird jede Warnung durch einen Balken dargestellt, sodass Sie schnell die Reihenfolge des Auftretens, Schweregradübergänge und den Abschlussstatus erkennen können. Die Zeitleiste beginnt mit der Erstellung der ersten Warnung und erstreckt sich bis zum aktuellen Moment.

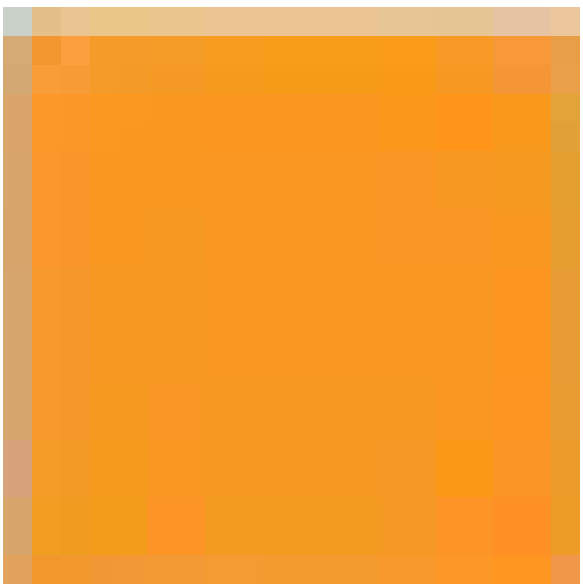
Beispiel für Zeitleistenansicht



In den Balken werden Standardfarben für den Schweregrad verwendet, wobei graue Segmente Zeiträume vor der Erstellung von Warnungen oder nach deren Schließung anzeigen. Wenn Sie den Mauszeiger über einen Schweregradbalken bewegen, wird ein Tooltip mit wichtigen Warnungsdetails angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

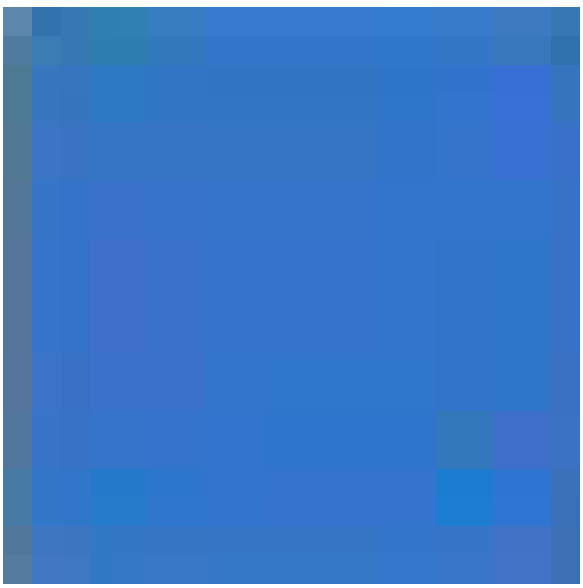
Schweregradbereich nach Farbe in der Zeitleistenansicht

Farbe	Schweregrad
	Kritisch
	Schwerwiegend

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

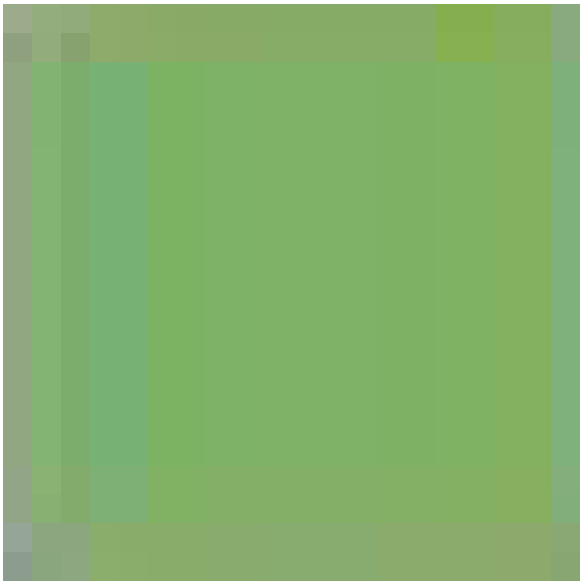
Schweregradbereich nach Farbe in der Zeitleistenansicht (Fortsetzung)

Farbe	Schweregrad
	Kleiner
	Warnung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregradbereich nach Farbe in der Zeitleistenansicht (Fortsetzung)

Farbe	Schweregrad
	OK

Der Titel der Zeitleistenansicht für eine Warnungsgruppe fasst Beschreibung, Nummer, Status, Schweregrad und Gruppierungstyp der Gruppe zusammen. von der primären Warnung abgeleitet. Detaillierte Informationen wie Warnungsnummer, Status, Schweregrad, eine kurze Beschreibung und zugehöriges Konfigurationselement (CI) oder Knoten, falls verfügbar, werden für jede Warnung innerhalb der Gruppe angezeigt.

Zugehörige Informationen

Zeigen Sie eine Zeitleiste der Warnungen in einer Warnungsgruppe an

Zeigen Sie eine Zeitleiste der Warnungen in einer Warnungsgruppe an

Erhalten Sie Einblicke in die Reihenfolge der Ereignisse im Zusammenhang mit einem Problem, indem Sie chronologische Informationen zu den Warnungen in einer Warnungsgruppe in anzeigen Express-Liste.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation die aus Express-Liste Symbol ( ).
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol (Für eine Warnung.
4. Wählen Sie auf der Registerkarte Warnungen im Vorschaubereich aus **Zeitleistenansicht** .
5. Analysieren Sie die in der Zeitleistenansicht bereitgestellten Informationen.
6. **Wahlweise:** Sortieren Sie die angezeigten Warnungen nach aufsteigender oder absteigender Zeit oder nach Schweregrad.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie das Sortiersymbol ( ).

b. Wählen Sie im Popup-Menü die bevorzugte Sortieroption aus.

7. Wahlweise: Zeigen Sie geschlossene Warnungen an, oder blenden Sie sie aus, indem Sie umschalten **Schließen Sie Warnungen aus** Schieberegler.

Zugehörige Informationen

Untersuchen chronologischer Daten zu Warnungen in einer Warnungsgruppe in Express-Liste

Suchen Sie Warnungsdatensätze in Express-Liste Freitextsuche wird verwendet

Führen Sie eine Freitextsuche nach Warnungsdatensätzen in einer gefilterten Liste von Warnungen durch.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ereignismanagement Durchsucht die Warnungen, die derzeit in angezeigt werden Express-Liste Basierend auf den Filtern und dem Zeitbereich, den Sie festgelegt haben. Es wird in den folgenden vordefinierten Feldern gesucht, auch wenn sie nicht sichtbar sind: Metrikname, Knoten, Warnungsnummer, Warnungs-Tags und Beschreibung. Der von Ihnen eingegebene Text wird als einzelne Zeichenfolge und nicht als einzelne Wörter behandelt.

Die Ergebnisse entsprechen sowohl den von Ihnen angewendeten Filtern als auch der Zeichenfolge, die Sie im Suchfeld eingegeben haben. In den resultierenden Warnungsdatensätzen wird die gesamte Zeichenfolge hervorgehoben, nach der Sie gesucht haben, und die verfügbaren Filter zeigen die Anzahl der Datensätze an, die der Zeichenfolge entsprechen. Aktuelle Suchvorgänge werden gespeichert und können über das Suchfeld aufgerufen werden.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.

2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .

3. Geben Sie im Feld Suche den Freitext ein, nach dem gesucht werden soll.
Die Freitextzeichenfolge muss zwischen 3 und 50 Zeichen lang sein. Bei der Suche wird die Groß-/Kleinschreibung nicht beachtet.

4. Wählen Sie das Häkchensymbol aus Oder drücken Sie **Geben Sie Ein** Um die Suche durchzuführen.

Führen Sie Aktionen aus, um Warnungsprobleme in zu lösen Service Operations-Arbeitsbereich Für ITOM

Lösen Sie das zugrunde liegende Problem einer Warnung, indem Sie vordefinierte Korrekturaufgaben ausführen, um eine schnellere Problemlösung und eine konsistente Lösung sicherzustellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.

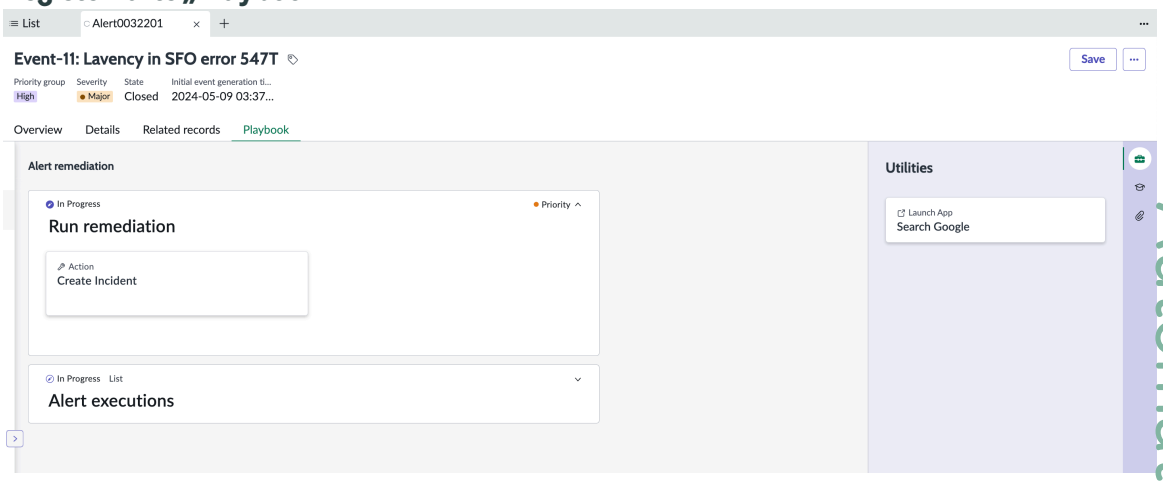
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird in einer separaten Registerkarte geöffnet, auf der angezeigt wird **Übersicht** Registerkarte.
4. Wählen Sie Aus **Starten Sie das Playbook** .
5. Wählen Sie die Registerkarte **Playbook** aus.
   Die **Führen Sie die Korrektur aus** Die Karte zeigt die verfügbaren Korrekturaktionen an.

Registerkarte „Playbook“



6. Wählen Sie die Kachel aus, die der Aktion entspricht, die Sie ausführen möchten.
   Die ausgewählte Aktion wird im angezeigt **Warnungsausführungen** Karte.

Ergebnis

Wenn die Aktion abgeschlossen ist, wird sie unter dem Abschnitt „Warnungs-Fehlerkorrektur“ auf der Karte **Abgeschlossen** angezeigt.

Starten Sie eine Webanwendung für eine Warnung in Service Operations-Arbeitsbereich Für ITOM

Starten Sie eine Webanwendung, die in einer Warnungsverwaltungsregel konfiguriert wurde, um schnell auf die erforderlichen Tools zuzugreifen und die Reaktionszeiten und Effizienz zu verbessern.

Vorbereitungen

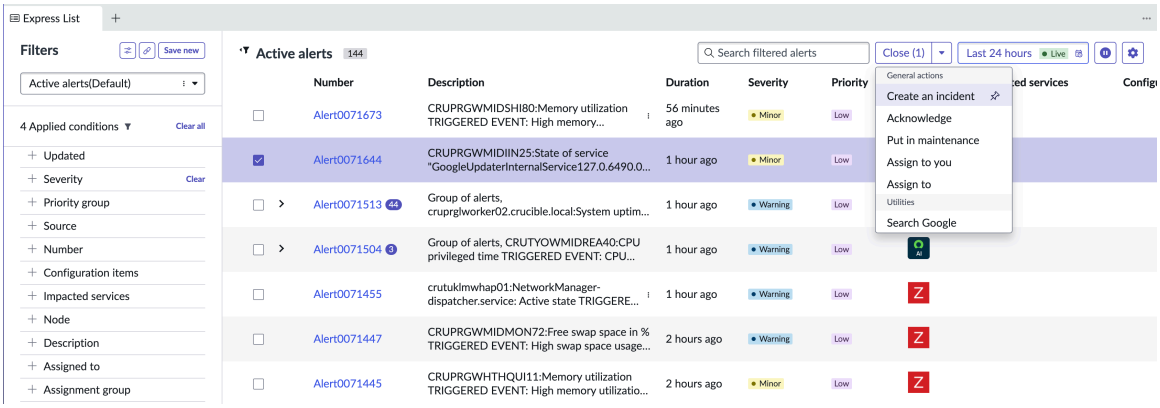
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.

   Die Warnung wird auf einer separaten Registerkarte geöffnet, auf der die untergeordnete Registerkarte **Übersicht** angezeigt wird. Im rechten Bereich die **Dienstprogramme** Die Registerkarte ist standardmäßig ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie im Abschnitt Dienstprogramme die Webanwendung aus, um die App zu starten.

Filtern der Warnungsanzeige in Express-Liste Bereich

Filter helfen Ihnen, verschiedene Ansichten kategorisierter Warnungen zu erstellen und eine gezielte Liste von Warnungen zu erstellen, auf die Sie sich konzentrieren und priorisieren können, was Zeit spart und Ablenkungen minimiert.

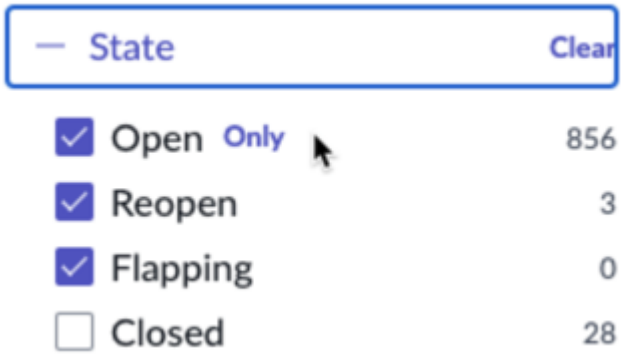
Mit den Feldern im interaktiven Filterbereich auf der linken Seite können Sie verschiedene Ansichten im erstellen Express-Liste Bereich. Standardfilter:

- Status
- Schweregrad
- Priorität
- Quelle
- Anzahl
- Konfigurationselement
- Anzahl der betroffenen Services
- Knoten
- Beschreibung
- Zugewiesen an
- Zuweisungsgruppe
- Metrikname
- Gruppe
- Wartung

Sie können interaktiv anzeigen, was passiert, wenn Sie eines der Felder hinzufügen oder entfernen. Die Zahlen neben jedem Attribut geben die Anzahl der zurückgegebenen Warnungen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In Express-Liste Filterbereich können Sie die folgenden Aktionen ausführen:

- Fügen Sie der Standardfilterliste Filter hinzu, oder entfernen Sie Filter aus dieser Liste, um sich auf die angewendeten Filter zu konzentrieren. Die häufigsten Filter sind Status, Priorität, CI und betroffene Services.
- Fügen Sie Warnungs-Tags hinzu, oder entfernen Sie sie. Mit Tags können Sie Warnungen einfach identifizieren und gruppieren, ohne dass eine Discovery erforderlich ist oder auf die CMDB zugegriffen werden muss.
- Filtern Sie nach Zeichenfolgen-, Zahlen- oder Datumsattributen.
- Speichern, löschen, zuweisen als Standard, oder geben Sie das Filterlayout frei.
- Filtern oder zeigen Sie Warnungen an, die einer ausgewählten Warnung entsprechen.

Filtern Sie Express-Liste Mit Attributen anzeigen

Filtern Sie Express-Liste Zeigen Sie mithilfe von interaktiven nach Text-, Zahlen- und Datumsattributen an Express-Liste Filterbereich. Erstellen Sie eine gezielte Liste von Warnungen, auf die Sie sich konzentrieren und priorisieren möchten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

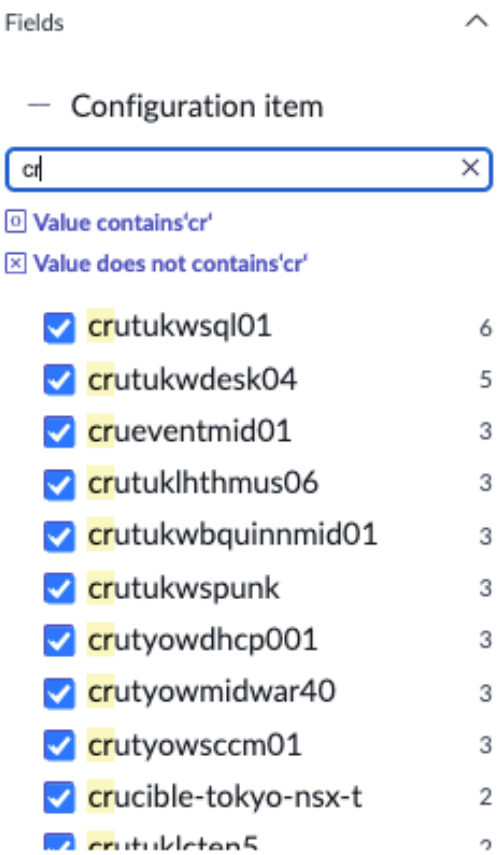
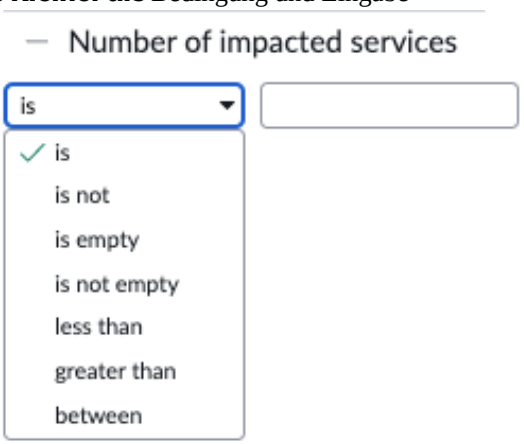
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Wählen Sie im Bereich Filter auf der linken Seite aus, ob je nach Filtertyp nach Text-, Zahlen- oder Datumsattributen gefiltert werden soll.

Filterattributtyp	Aktion
Text	Suchen Sie Elemente nach Namen, indem Sie die ersten Zeichen eingeben, um die Elemente anzuzeigen, die mit diesen Zeichen beginnen. Wählen Sie dann die Werte aus, die Sie

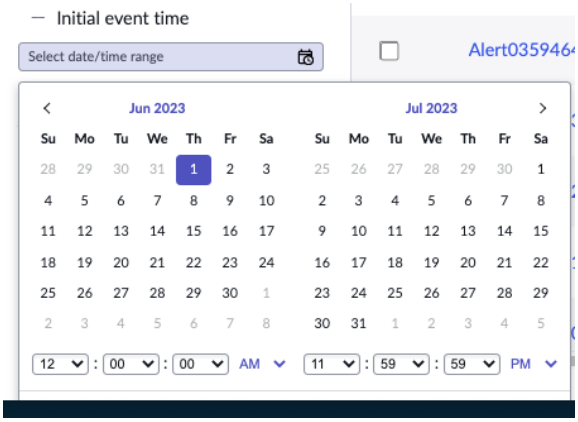
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterattributtyp	Aktion
	in anzeigen möchten Express-Liste Bereich. 
Anzahl der betroffenen Services	Geben Sie eine Bedingung ein, um Warnungen entsprechend der Anzahl der Warnungen für den ausgewählten Filter anzuzeigen. Um beispielsweise Warnungen mit weniger als 10 betroffenen Services anzuzeigen, wählen Sie aus **Kleiner als** Bedingung und Eingabe  10.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterattributtyp	Aktion
Datum	Zeigen Sie Warnungen gemäß dem ausgewählten Datums- und Zeitbereich im Pop-up-Kalender an Express-Liste Bereich. 

Filtern Sie Express-Liste Durch Hinzufügen oder Entfernen von Feldern anzeigen

Fügen Sie Felder zu hinzu, oder entfernen Sie Felder aus Express-Liste Bereichsfilter mithilfe des interaktiven Filterbereichs. Verwenden Sie Filterung, um verschiedene Ansichten kategorisierter Warnungen zu erstellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

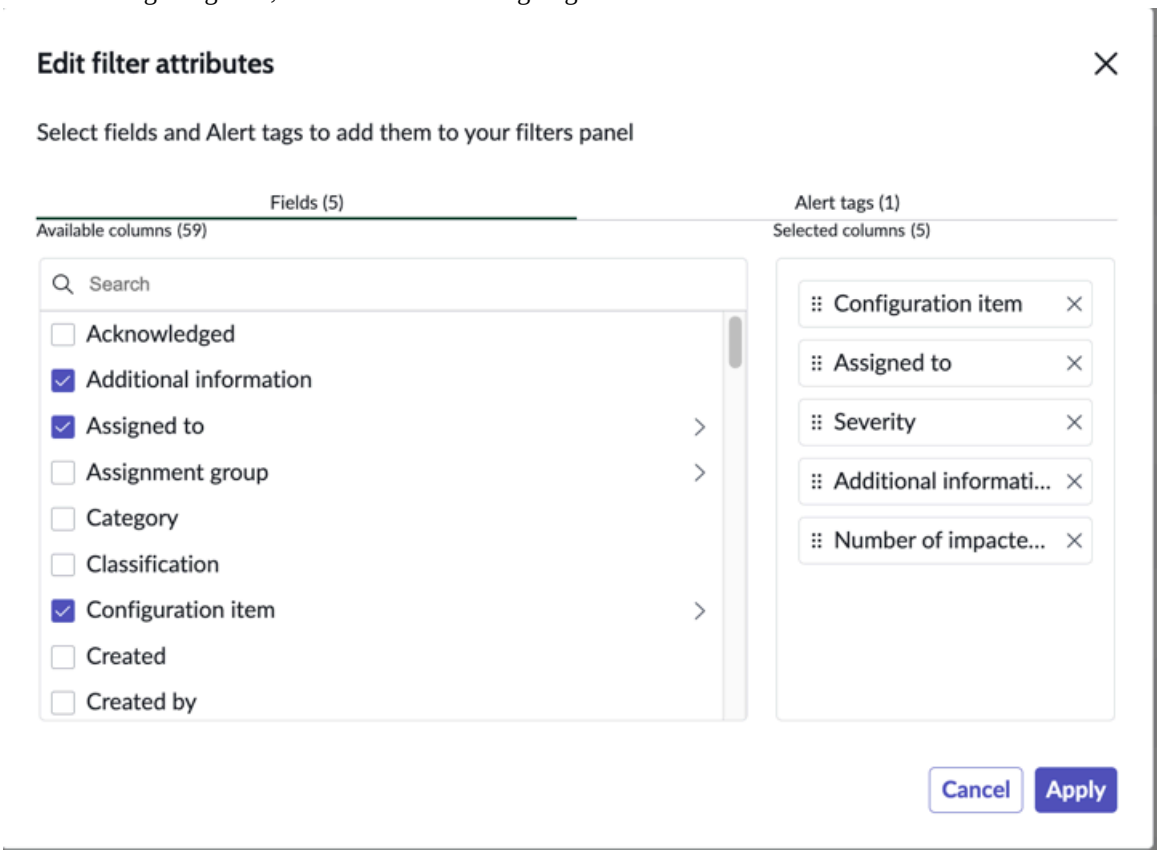
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Wählen Sie im linken Filterbereich das Symbol Filterattribute bearbeiten ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In **Bearbeiten Sie Filterattribute**Dialogfeld wählen Sie Felder oder Warnungs-Tags aus, die Ihrem Filter hinzugefügt werden sollen.



Die **Felder** Die Registerkarte wird standardmäßig angezeigt und zeigt die Anzahl der ausgewählten Felder an.

Die Anzahl der verfügbaren Felder wird oben in der Spalte neben angezeigt **Verfügbare Spalten** .

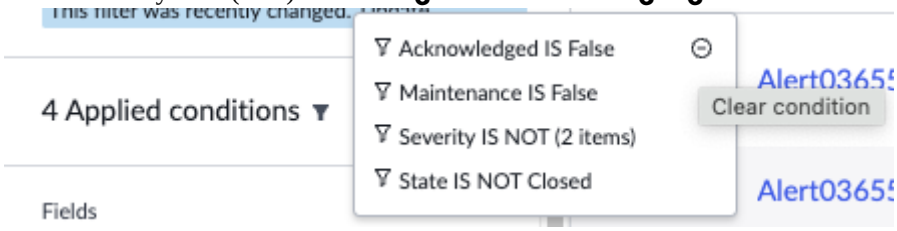
Die ausgewählten Felder werden in der rechten Spalte angezeigt. Die Anzahl der ausgewählten Spalten wird oben in der Spalte neben angezeigt **Ausgewählte Spalten** .

5. **Wahlweise:** Suchen Sie ein bestimmtes Feld, indem Sie seinen Namen in eingeben **Suchen** Feld.
6. **Wahlweise:** Ordnen Sie die Reihenfolge der ausgewählten Spalten neu an, indem Sie sie in der rechten Spalte nach oben oder unten ziehen.
7. **Wahlweise:** Entfernen Sie eine Spalte, indem Sie auswählen **X** Neben dem Namen.
8. Wählen Sie **Übernehmen**.
9. **Wahlweise:** Löschen Sie einen Filter, indem Sie auswählen **Löschen** Neben diesem Filternamen. **Löschen** Wird nur angezeigt, wenn Sie eines der Attribut-Kontrollkästchen des ausgewählten Filters aktiviert oder deaktiviert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. **Wahlweise:** Zeigen Sie die angewendeten Bedingungen an, indem Sie das Filtersymbol ( ) Neben **Angewendete Bedingungen**.



11. **Wahlweise:** Entfernen Sie eine Bedingung, indem Sie auswählen **Bedingung löschen** ( )-Symbol.

Ergebnis

Alle ausgewählten Felder werden in angezeigt **Filter** Bereich in **Felder** Spalte.

Kategorisieren Sie Warnungen, die in angezeigt werden Express-Liste

Erstellen Sie verschiedene Ansichten von Warnungen, indem Sie Tags in hinzufügen Express-Liste Damit Sie Warnungen einfach identifizieren und gruppieren können, ohne dass eine Discovery erforderlich ist oder auf die CMDB zugegriffen werden muss.

Vorbereitungen

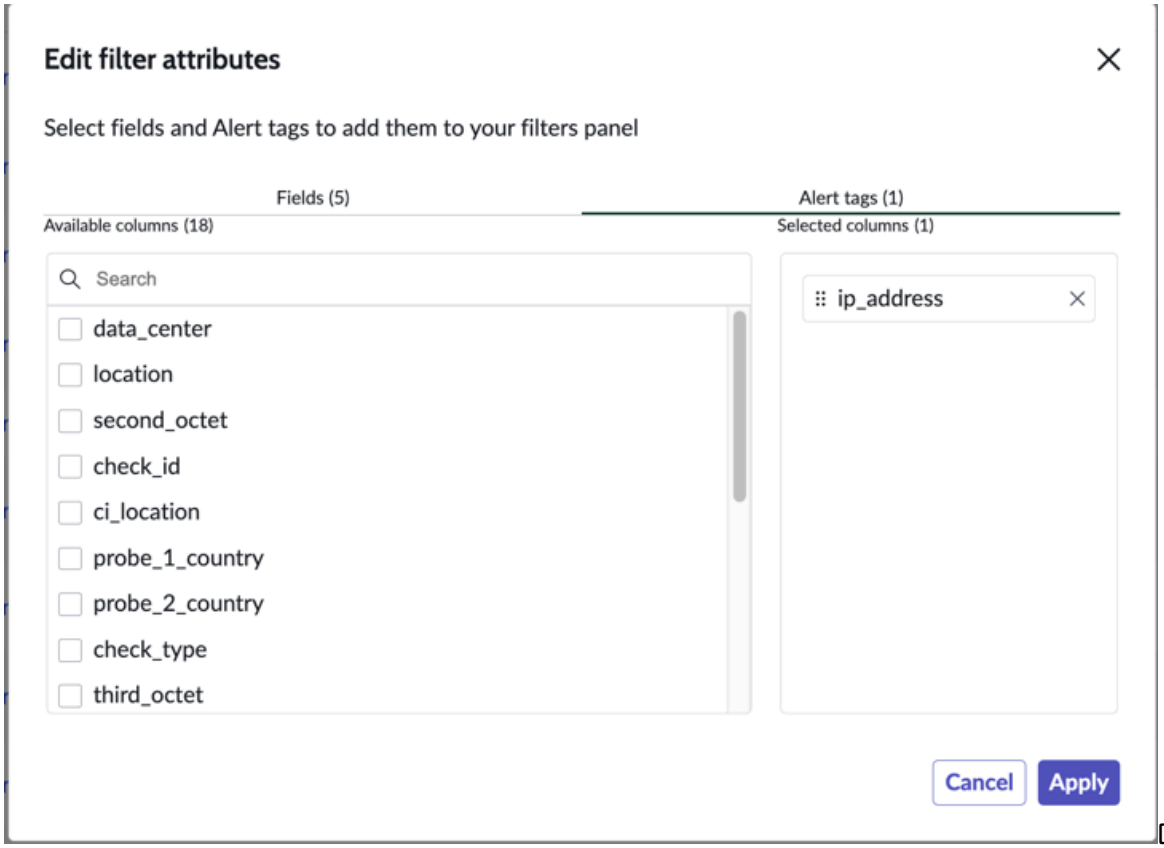
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Wählen Sie im linken Filterbereich die aus **Bearbeiten Sie Filterattribute** Symbol ( ).
4. In **Bearbeiten Sie Filterattribute** Wählen Sie das Dialogfeld aus **Warnungs-Tags** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die **Warnungs-Tags** Der Registerkartentitel zeigt die Anzahl der ausgewählten Warnungs-Tags an.

In der linken Spalte wird die Anzahl der verfügbaren Tags in angezeigt **Verfügbare Spalten** Spaltentitel.

Die ausgewählten Tags werden in der rechten Spalte angezeigt. Die Anzahl der ausgewählten Tags wird in angezeigt **Ausgewählte Spalten** Spaltentitel.

5. **Wahlweise:** Suchen Sie ein bestimmtes Tag, indem Sie seinen Namen in eingeben **Suchen** Feld.
6. **Wahlweise:** Ordnen Sie die ausgewählten Tags neu an, indem Sie sie in der rechten Spalte nach oben oder unten ziehen.
7. **Wahlweise:** Heben Sie die Auswahl eines Tags auf, indem Sie (**X**) Daneben.
8. Wählen Sie **Übernehmen**.

Ergebnis

Alle ausgewählten Tags werden in angezeigt **Filter** Bereich unter **Warnungs-Tags** Registerkarte.

Filtern oder zeigen Sie übereinstimmende Warnungen an

Erstellen Sie verschiedene Ansichten von kategorisierten Warnungen in Express-Liste Indem Warnungen angezeigt oder herausgefiltert werden, die einer ausgewählten Warnung entsprechen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Klicken Sie mit der rechten Maustaste auf eine Warnungszeile.
4. Übereinstimmende Warnungen abgleichen oder herausfiltern.
   - Zeigen Sie übereinstimmende Warnungen an, indem Sie auswählen **Übereinstimmungen Anzeigen** Aus dem Kontextmenü.
   - Filtern Sie übereinstimmende Warnungen heraus, indem Sie auswählen **Herausfiltern** Aus dem Kontextmenü.

Speichern Sie einen anwenderdefinierten Filter in Express-Liste

Speichern Sie Ihre anwenderdefinierte Ansicht kategorisierter Warnungen in Express-Liste Um erneut zu verwenden, geben Sie sie frei, oder legen Sie sie als Standardansicht fest. Durch das Speichern Ihrer anwenderdefinierten Ansicht werden alle Filter, Tags und Bedingungen gespeichert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_Operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Sobald Sie einen Filter eingerichtet haben, den Sie wiederverwenden, als Standardansicht festlegen oder für andere freigeben möchten, speichern Sie den Filter.
   Weitere Informationen zum Filtern von finden Sie Express-Liste Warnungsanzeige, siehe die folgenden Themen:
   - Filtern Sie Express-Liste Mit Attributen anzeigen
   - Filtern Sie Express-Liste Durch Hinzufügen oder Entfernen von Feldern anzeigen
   - Filtern oder zeigen Sie übereinstimmende Warnungen an

   a. In Express-Liste Wählen Sie aus **Speichern Sie neu** .
   b. In **Neuen Filter speichern** Dialogfeld in **Filtername** Feld einen Namen für den Filter eingeben.
   c. **Wahlweise:** Machen Sie diesen Filter zum Standardfilter, indem Sie auswählen **Als Standard festlegen** .
   d. Wählen Sie Aus **Speichern** Zum Speichern des Filters.
4. **Wahlweise:** Geben Sie einen gespeicherten Filter frei, indem Sie den zugehörigen Link kopieren, um ihn an andere zu senden.
   a. In **Filter** Wählen Sie den Filter aus der Dropdown-Liste aus.
   b. Wählen Sie das Symbol Link in Zwischenablage kopieren ( ).
5. **Wahlweise:** Legen Sie einen gespeicherten Filter als Standardfilter fest.
   a. In **Filter** Wählen Sie den Filter aus der Dropdown-Liste aus.
   b. Wählen Sie aus M Erz A Symbol „ctions“ ( ) Und wählen Sie aus **Als Standard festlegen** .
6. **Wahlweise:** Löschen Sie einen gespeicherten Filter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. In **Filter** Wählen Sie den Filter aus der Dropdown-Liste aus.

b. Wählen Sie aus M Erz A Symbol „ctions“ (⋮) Und wählen Sie aus **Löschen Sie den Filter** .

Anzeigen einer Warnungsgruppenanalyse nach Now Assist In Express-Liste

Zeigen Sie eine Analyse der Warnungsgruppen in an Express-Liste, Generiert von Now Assist Mit KI. Die Analyse hilft Ihnen, die Art der Warnungsgruppe besser zu verstehen, warum die Warnungen in der Gruppe korreliert wurden und wie Sie im Korrekturprozess fortfahren.

Die KI-gesteuerte Warnungsgruppenanalyse bietet eine vereinfachte, visuell lesbare Beschreibung der Gruppe und technische Informationen, damit Sie sie effizienter untersuchen können. Die bereitgestellten Informationen basieren auf Beschreibungen und Konfigurationselementdetails (Configuration Item, CI), die sich auf die einzelnen Warnungen in der Gruppe beziehen. Die Warnungsgruppenanalyse wird für die folgenden Warnungsgruppentypen unterstützt:

Tag-basierte Warnungsgruppen

Tags helfen beim Kategorisieren von Warnungen basierend auf allgemeinen Attributen, z. B. betroffenen Systemen oder Services. Warnungen in Tag-basierten Warnungsgruppen teilen bestimmte Tags, was Ähnlichkeiten bei den Problemen anzeigt. Die Warnungsanalyse für diese Gruppen zeigt die freigegebenen Tags, die zum Korrelieren der Warnungen in der Gruppe verwendet wurden. Außerdem erhalten Sie Einblicke in die Gründe, warum diese Warnungen gruppiert wurden. Darüber hinaus bietet die Analyse Vorschläge für eine Vorgehensweise basierend auf den Ähnlichkeiten zwischen den Tags.

CMDB-Warnungsgruppen

Wenn eine Warnung für ein CI in erstellt wird Configuration Management Database (CMDB), Ereignismanagement Sucht in nach Warnungen für andere CIs, die eng damit verbunden sind CMDB Topologie. Eine enge topologische Beziehung zwischen CIs deutet auf eine Interdependenz zwischen Komponenten in der IT-Infrastruktur hin und trägt zur Warnungskorrelation bei. Wenn eine Beziehung zwischen CIs gefunden wird, wird ein CMDB Warnungsgruppe wird gebildet. Die Warnungsanalyse für CMDB Warnungsgruppen erklären die Art der Gruppe und den Grund ihrer Bildung sowie die Beziehungen zwischen den CIs. Es enthält auch technische Informationen, mit denen Sie entscheiden können, welche Warnungen Ihre Untersuchung konzentrieren sollen.

Log Analytics-Warnungsgruppen

Wenn Ereignismanagement Identifiziert mehrere Log Analytics Warnungen, die sich auf wichtige Weise beziehen, werden in einem gruppiert Log Analytics Gruppe. Das System generiert einen Log Analytics Gruppieren, wenn Log Analytics Warnungen teilen eine oder mehrere Beziehungen im Zusammenhang mit Zeit, Metadaten, Nachrichtentext und Trend. Die Warnungsanalyse für Log Analytics Warnungsgruppen basieren auf der Analyse der von bereitgestellten Anomalieinformationen Health Log Analytics, Und in den Beschreibungen, CIs und Tags der Warnungen in der Gruppe.

Auf Netzwerkdatenverkehr basierende Warnungsgruppen

Die auf Netzwerkverkehr basierte Warnungsgruppierungsmethode gruppiert Warnungen, indem Netzwerkverkehrsverbindungen zwischen Prozessen auf Hosts analysiert werden. Es nutzt Servicekandidaten, die von ML Service Mapping identifiziert wurden, um die Warnungen zu gruppieren. Die Warnungsanalyse für auf Netzwerkverkehr basierende Warnungsgruppen enthält eine Beschreibung aller Warnungen in der Gruppe und der Verbindungen zwischen ihnen.

Gemischte Warnungsgruppen

Die gemischte Gruppierungsmethode kombiniert Warnungen mithilfe mehrerer Gruppierungsstrategien, z. B. CMDB-Basierte Gruppierung und Tag-basierte Gruppierung in einer einzigen, zusammenhängenden Gruppe. Diese Methode nutzt die Stärken jeder Strategie,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um Warnungsrauschen zu reduzieren, die Warnungskorrelation zu verbessern und die wahre Ursache von Incidents hervorzuheben.

Zeigen Sie eine Warnungsgruppenanalyse nach an Now Assist In Express-Liste

Zeigen Sie eine von erstellte Warnungsgruppenanalyse an Now Assist Generative KI verwenden. Die Analyse bietet eine vereinfachte, visuell lesbare Beschreibung der Warnungsgruppe und technische Informationen, damit Sie sie effizienter untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basiert, CMDB, Log Analytics, Gemischt, Und auf Netzwerkdatenverkehr basierende Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste die aus Express-Liste Symbol ( ).
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Neben einer Warnungsgruppe, um den Vorschaubereich anzuzeigen.
4. Im Vorschaubereich **Info** Wählen Sie die Registerkarte aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden unabhängig von der in den Warnungsbeschreibungen verwendeten Sprache in Englisch bereitgestellt.

6. **Wahlweise:** Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Warnungsanalysesymbole

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Zugehörige Informationen

Anzeigen einer Warnungsgruppenanalyse nach Now Assist In Express-Liste

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisieren Sie eine Warnungsbeschreibung in Express-Liste Basierend auf einem Now Assist Analysezusammenfassung

Aktualisieren Sie Warnungsbeschreibungen in Warnungsgruppen oder einzelnen Warnungen in Express-Liste, In eine visuell lesbare Zusammenfassung, die von generiert wurde Now Assist.

Warum und wann dieser Vorgang ausgeführt wird

Das Aktualisieren der Warnungsbeschreibung ist für die Warnungstypen verfügbar:

- Tag-basierte Warnungsgruppe.
- CMDB Korrelationswarnungsgruppe.
- Warnungsgruppe für Korrelation des Netzwerkverkehrs.
- Log Analytics – einzelne Warnungen und Warnungsgruppen.
- Gemischte Warnungsgruppe.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste die aus Express-Liste Symbol ( ).
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Einer Warnung.
4. Im Vorschaubereich **Info** Wählen Sie die Registerkarte aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Überprüfen Sie die visuell lesbare, KI-generierte Zusammenfassung in der Warnungsanalyse.

   Hinweis: Die Warnungsanalyse wird unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

6. Im Vorschaubereich **Info** Wählen Sie die Registerkarte aus **Aktualisieren Sie die Beschreibung** Dient zum Aktualisieren der Beschreibung basierend auf dem Zusammenfassungsinhalt der Warnungsgruppe. Der KI-generierte Zusammenfassungsinhalt ersetzt die ursprüngliche Beschreibung der Warnungsgruppe.

Von verwendete Rollen Express-Liste

Detaillierte Informationen zu allen Rollen, die auf zugreifen können Express-Liste-Funktion in Service Operations-Arbeitsbereich.

Rollentitel	Beschreibung	Enthält Rollen
Ereignismanagement-Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.	• evt_mgmt_user • template_editor_global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel	Beschreibung	Enthält Rollen
	Hinweis: Seien Sie bei der Rolle „evt_mgmt_admin“ vorsichtig, da sie auf die Administratorrolle hochgestuft werden kann.	
Ereignismanagement-Operator [evt_mgmt_operator]	In Kombination mit den Berechtigungen „evt_mgmt_user“ können auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Incidents und Ausführen von Korrekturen aktiviert werden.	evt_mgmt_user
Ereignisteamoperator [evt_Team_Operator]	Verwaltet Ereignismanagement Vorgänge in einem bestimmten Team, wie in definiert **Zuweisungsgruppe** Feld. Mit dieser Rolle kann der Operator Warnungen ausschließlich für sein zugewiesenes Team lesen und schreiben. Darüber hinaus kann der Betreiber Konfigurationsänderungen für sein Team vornehmen, einschließlich Updates für Warnungsautomatisierung und Integrations Launchpad. **Hinweis:** Die Rolle „evt_Team_Operator“ muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keiner Gruppe zugeordnet ist, denen Warnungen zugewiesen sind, kann der Operator keine Warnungen sehen.	
Ereignismanagement-Anwender [evt_mgmt_user]	Hat schreibgeschützten Zugriff auf alle Ereignismanagement Funktionen. Die enthaltene itil-Rolle gewährt Zugriff auf die Verwaltung von Incidents, die aus Warnungen erstellt werden. Kann nur anzeigen Express-Liste.	ITIL
Ereignismanagement-Integrator [evt_mgmt_integration]	Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel	Beschreibung	Enthält Rollen
	mit externen Ereignisquellen zu integrieren.	

Warnungsautomatisierung in Service Operations-Arbeitsbereich Für ITOM

Die Warnungsautomatisierung ist wichtig, da Organisationen mit einer steigenden Anzahl von Warnungen und komplexen IT-Infrastrukturen zu kämpfen haben. Die manuelle Warnungsverarbeitung ist langsam, fehleranfällig und ineffizient, was den Bedarf an automatisierten Systemen unterstreicht. Automatisierung kann die durchschnittliche Zeit bis zur Lösung von Warnungen verbessern, die Servicezuverlässigkeit verbessern und die Mitarbeiterressourcen besser skalieren.

Warnungsautomatisierungen unterstützen auch die Rollen des zentralen Administrators und des verteilten Teams. Dadurch können qualifizierte Teams sich selbst bedienen und eigene Warnungsautomatisierungen erstellen. Sie können beispielsweise Site Reliability Engineers (SREs) Zugriff gewähren. Mitglieder von Teams können Automatisierungen für ihr eigenes Team und ihre eigenen Warnungen verwalten, ohne andere Teams zu beeinträchtigen.

Für Anwender, die mit unserer klassischen Experience vertraut sind, bietet die Warnungsautomatisierung eine einfachere Anwenderoberfläche und eine bessere Teamunterstützung für Ereignisregeln, Tag-basierte Clustering-Definitionen und Warnungsverwaltungsregeln. Einige erweiterte Funktionen sind derzeit nur für Administratoren in der klassischen Experience verfügbar. Diese beiden Experiences verwenden dieselben Back-End-Tabellen. Sie können die Experience verwenden, die am bequemsten ist, und Änderungen in einer aktualisieren auch die andere.

https://player.vimeo.com/video/1068873181?h=b03003c9bf&badge=0&autopause=0&player_id=0&app_id=58479

Warnungsautomatisierungstypen

Derzeit Service Operations-Arbeitsbereich ITOM Stellt die folgenden Automatisierungstypen bereit.

1. Automatisierung ignorieren : Reduzieren Sie irrelevante oder falsch positive Warnungen, verwalten Sie die Warnungsermüdung effizient, indem Sie laute Benachrichtigungen herausfiltern, und ermöglichen Sie Teams, sich auf kritische Probleme zu konzentrieren.
2. Bereichern Sie die Automatisierung : Verbessern Sie Rohwarnungen mit kontextbezogenen Informationen, um sie informativer und umsetzbarer zu machen. Vereinfacht ausgedrückt: Dazu werden die durch Überwachungstools generierten Rohereignisse in ein gemeinsames Standardformat umgewandelt, um die automatisierte Gruppierung und Antwort zu erleichtern.
3. Gruppenautomatisierung : Gruppieren Sie mehrere zugehörige Warnungen in einer einzigen primären Warnung, um Warnungsrauschen zu reduzieren und die Ursache zu identifizieren.
4. Reagieren Sie auf Automatisierung : Antworten Sie automatisch auf Warnungen, indem Sie die entsprechenden Stakeholder benachrichtigen, eskalieren Sie sie nach Bedarf, oder führen Sie Korrekturmaßnahmen aus. Bestimmen Sie, wie und wann Warnungen basierend auf Schweregrad oder Typ eskaliert werden. Integrieren Sie Systeme von Drittparteien, um Fälle und Benachrichtigungen zu erstellen oder Korrekturaktionen auszuführen.

Prozessablauf für Warnungsautomatisierung

Sie können damit beginnen, Warnungen oder Ereignisse von Überwachungssystemen an zu senden ServiceNow Integrations-Launchpad verwenden. Hier stellen Administratoren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungen her ServiceNow Und Überwachungstools. Diese Integrationen ermöglichen die Erfassung überwachter Daten und generieren Ereignisse aus Drittparteiquellen.

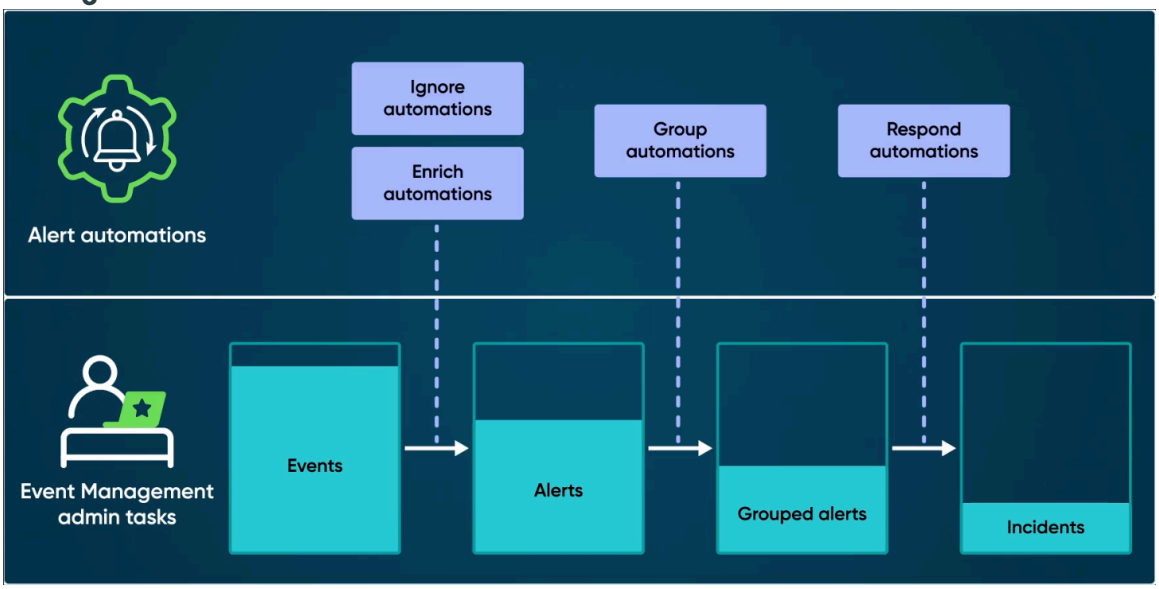
Wenn Warnungen von empfangen werden ServiceNow, Warnungsautomatisierungen werden in der auf der Seite angezeigten Reihenfolge ausgeführt. Zuerst ignorieren wir Warnungen, um das Rauschen zu reduzieren. Als Nächstes ergänzen wir Warnungen mit zusätzlichem Kontext und gruppieren die Warnungen dann anhand des hinzugefügten Kontexts. Schließlich reagieren wir auf Warnungen, indem wir Korrekturen eskalieren oder ausführen. Für jeden Typ können mehrere Automatisierungen vorhanden sein. Jede Automatisierung wird basierend auf bestimmten Auslöserbedingungen ausgeführt und führt bestimmte Aktionen aus. Warnungen werden nur automatisiert, wenn sie empfangen werden. Wir wenden keine Automatisierungen auf vergangene Warnungen an.

In der Warnungsanreicherungsphase fügen Administratoren erforderliche Felder hinzu oder extrahieren sie aus Warnungen, um wichtige Informationen für eine schnelle Lösung bereitzustellen. Dadurch wird sichergestellt, dass Warnungen alle relevanten Details enthalten, die für eine effektive Reaktion auf Incidents erforderlich sind. Administratoren fügen Warnungen Kontext hinzu, indem sie sie ändern und normalisieren. Dies verbessert die Korrelation von Warnungen, wodurch es einfacher wird, Muster und potenzielle Bedrohungen zu identifizieren.

Die angereicherten und verfassten Warnungen werden dann basierend auf vordefinierten Kriterien gruppiert, wobei zugehörige Warnungen konsolidiert werden. Dies reduziert die Ermüdung von Warnungen und erleichtert eine effiziente Korrektur. Schließlich lösen eskalierte Warnungen Benachrichtigungen an Stakeholder über verschiedene Kanäle aus, um eine rechtzeitige Kommunikation und Reaktion auf kritische Warnungen sicherzustellen.

Das folgende Diagramm zeigt diesen Prozess-Flow.

Warnungsautomatisierung: Reduzierung von Rauschen und Verbesserung der Lösungszeit



Dieser umfassende Warnungsautomatisierungsprozess kann Warnungsrauschen reduzieren, die durchschnittliche Zeit bis zur Lösung (MTTR) verbessern, die Serviceverlässlichkeit verbessern und die Mitarbeiterproduktivität steigern.

Automatisierung „Ignorieren“ erstellen

Die Automatisierung ignorieren optimiert den Prozess der Nichtberücksichtigung irrelevanter oder falsch positiver Warnungen aus Überwachungssystemen, wodurch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Warnungsermüdung effizient verwaltet wird, indem unnötige Benachrichtigungen herausgefiltert werden. Dadurch können sich Teams auf kritische Probleme konzentrieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird
Automatisierungen ignorieren filtern Warnungen aus Quellüberwachungssystemen heraus, die bestimmten Bedingungen entsprechen. Separat, Ereignismanagement Ignoriert Warnungen, die ein doppeltes Nachrichtenschlüsselfeld haben oder deren Schweregrad ist **Löschen** .

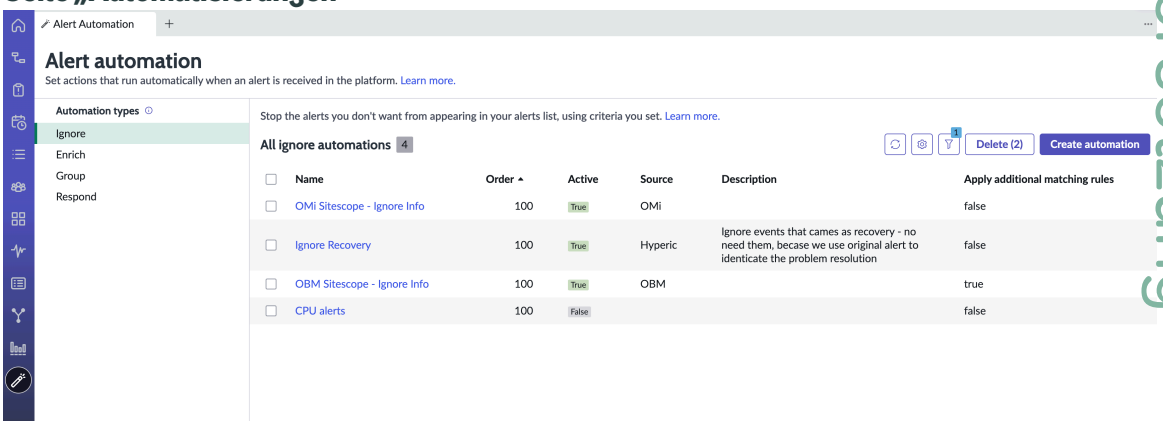
Für Anwender, die mit dem Klassiker vertraut sind Ereignismanagement Experience – Automatisierungen ignorieren bieten eine einfachere Schnittstelle mit erweiterter Teamunterstützung für den Ereignisfilterabschnitt von Ereignisregeln.

Hinweis: Das Ignorieren von Warnungen vor dem Anreichern verbessert die Leistung und vereinfacht den Verarbeitungs-Flow. Der Bedingungsfilter in Automatisierungen ignorieren gilt nur für das ursprüngliche Ereignis, nicht für das angereicherte. Durch Anreicherungsautomatisierungen kann verhindert werden, dass Automatisierungen ignoriert werden, wenn **Führen Sie keine anderen Anreicherungswarnungsautomatisierungen aus** Ist auf „falsch“ festgelegt, gelten sie für dieselbe Quelle, haben eine niedrigere Reihenfolge und entsprechen den Filterbedingungen. Um Konflikte zu vermeiden, ist es am besten, dies beim Erstellen von Ergänzungen oder Ereignisregeln zu berücksichtigen.

Prozedur

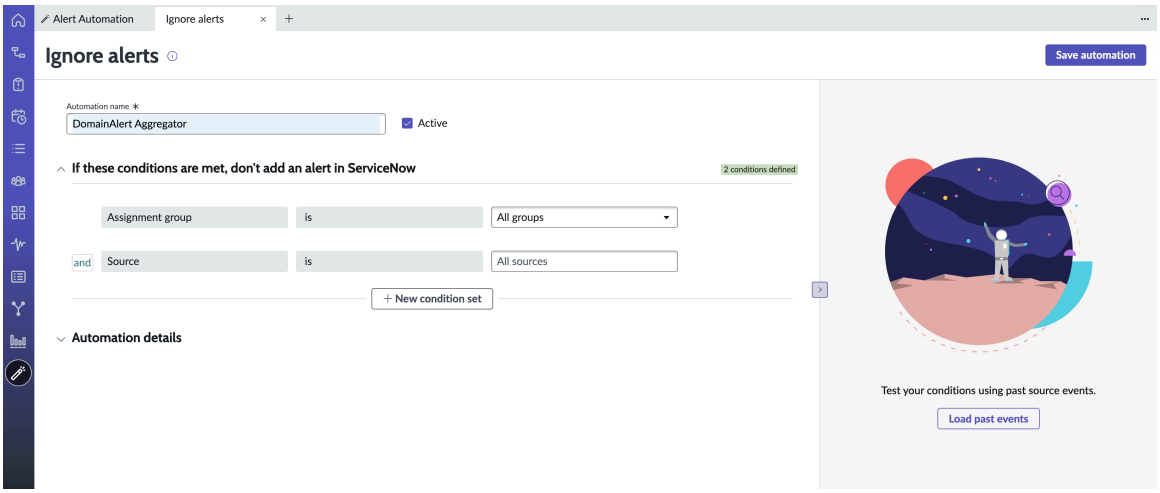
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Warnungsautomatisierung ( ).
3. Auf der Seite Warnungsautomatisierung unter **Automatisierungstypen** , Wählen Sie aus **Ignorieren** . Die Seite Warnungen ignorieren wird angezeigt.

Seite „Automatisierungen“



4. Wählen Sie Aus **Automatisierung erstellen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. In **Automatisierungsname** Feld den Namen der Automatisierung zum Ignorieren von Warnungen eingeben.
6. Aktivieren Sie die Automatisierung, indem Sie aktivieren **Aktiv** Umschalter.
7. In **Wenn diese Bedingungen erfüllt sind, fügen Sie keine Warnung in ServiceNow hinzu** Richten Sie Filterkriterien ein, um die Ereignisse zu identifizieren, die Sie erfassen möchten.
   a. Von **Zuweisungsgruppe** Feldmenü die Zuweisungsgruppe auswählen, um zu bestimmen, welche Warnungen des Teams die Automatisierung auslösen.

      Die **Zuweisungsgruppe** Stellt ein bestimmtes Team dar, das für die Verarbeitung bestimmter Warnungen verantwortlich ist. Durch Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung gezielt und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

      Hinweis:

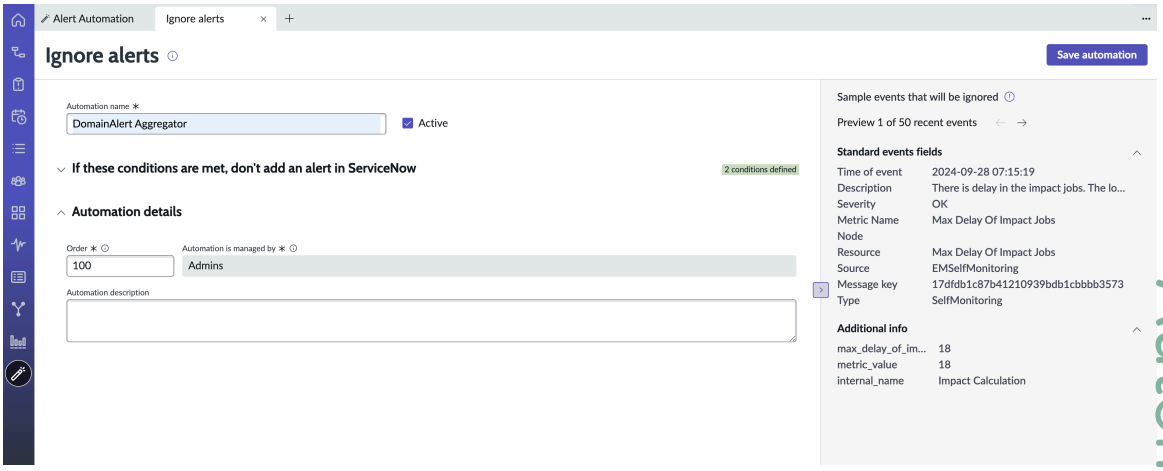
      - Wenn Sie mit einer Administratorrolle (evt_mgmt_admin) bei der Instanz angemeldet sind, sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie auswählen **Alle Gruppen** Um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
      - Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
      - Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

   b. Von **Quelle** Feldmenü: Wählen Sie das Überwachungstool aus, aus dem die Warnung generiert wird.
   c. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit den Operatoren ODER oder UND hinzu.

      Um einen weiteren Satz von Bedingungen hinzuzufügen, wählen Sie aus **+ neuer Bedingungssatz** . Sie können auch manuell ein Feld mit zusätzlichen Informationen hinzufügen, wenn es nicht in der Dropdown-Liste angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Um sicherzustellen, dass Sie die richtigen Ereignisse ignorieren, oder um Beispiele für Felder anzuzeigen, die zum Festlegen der Bedingungen verwendet werden können, wählen Sie aus **Laden Sie vergangene Ereignisse** .
   Sie können eine Vorschau der Details einiger vergangener Ereignisse anzeigen.
9. In **Automatisierungsdetails** Geben Sie eine Beschreibung der Reihenfolge und Automatisierung an.



   a. In **Reihenfolge** Feld die Automatisierungsreihenfolge eingeben.

      Hinweis: Automatisierungen werden in der Reihenfolge vom niedrigsten zum höchsten ausgeführt.

      Die **Automatisierung wird von verwaltet** Das Feld zeigt das Team oder die Zuweisungsgruppe an, die diese Automatisierung besitzt, bearbeitet und löschen kann. Die Zuweisungsgruppe ist mit der in definierten Gruppe identisch **Wenn diese Bedingungen erfüllt sind** Abschnitt.

   b. In **Automatisierungsbeschreibung** Geben Sie eine kurze Beschreibung der Automatisierung ein.
10. Wählen Sie Aus **Automatisierung speichern** .
    Eine Benachrichtigung wird angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Automatisierung ignorieren wird im angezeigt **Warnungen ignorieren** Seite, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

Nächste Maßnahme

Sie können Rohereignisse in ein verständliches Format umwandeln, indem Sie erstellen Erstellen Sie eine Anreicherungsautomatisierung.

Erstellen Sie eine Anreicherungsautomatisierung

Die Ergänzung von Warnungen umfasst die Umwandlung von Rohereignissen aus Überwachungstools in ein Standardformat, was die automatisierte Gruppierung und Reaktion unterstützt. Dies umfasst das Extrahieren von Feldern aus langen Warnungsnutzlasten oder das Verfassen in ein standardisiertes Format. Darüber hinaus können Sie Tags erstellen, bei denen es sich um Metadaten handelt, die Warnungen hinzugefügt werden, um das Filtern und Gruppieren zu erleichtern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

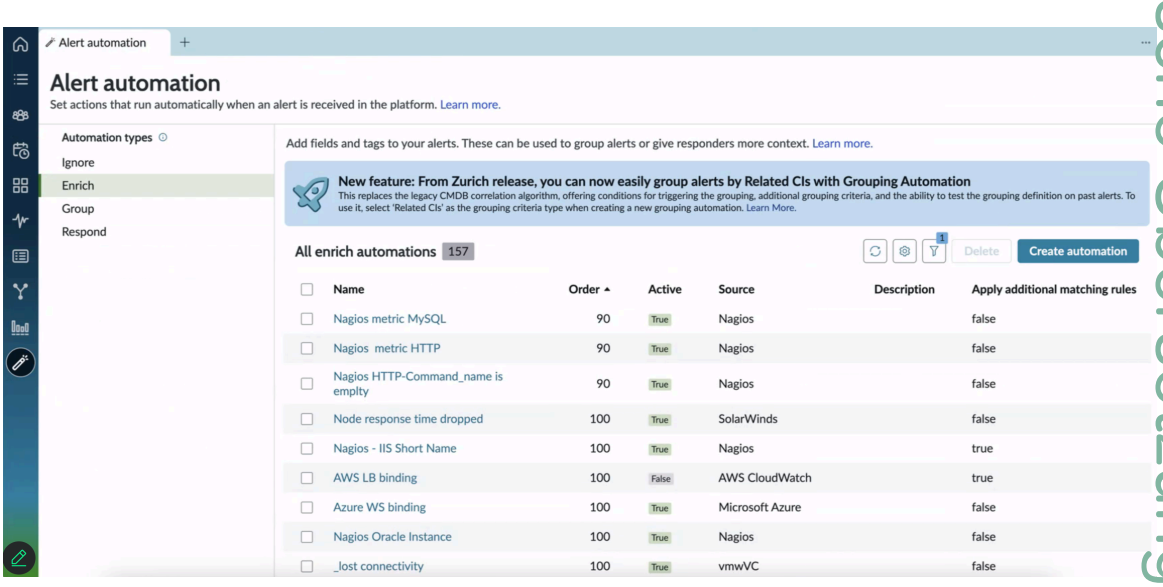
Warum und wann dieser Vorgang ausgeführt wird

Beim Extrahieren werden Werte aus Ereignisnutzlastfeldern übernommen und in Warnungsausgabefelder platziert, während beim Verfassen mehrere Warnungsfelder in einem zusammengefasst werden. Weitere Informationen finden Sie unter Warnungsfelder werden extrahiert und verfasst.

Für Anwender, die mit dem Klassiker vertraut sind Ereignismanagement Mit Experience, Anreicherung von Automatisierungen werden Ereignisregeln erstellt, jedoch mit einer einfacheren Schnittstelle und besserer Teams-Unterstützung. Ereignisregeln bieten einige erweiterte Funktionen wie Schwellenwerte und CI-Identifizierung mit IRE, die in Anreicherungsautomatisierungen noch nicht verfügbar sind. Administratoren können Warnungen auch mit Ereignisfeldzuordnungsregeln ergänzen. Durch das Ändern von Warnungswerten wird eine Ereignisfeldzuordnungsregel mit dem Zuordnungstyp erstellt **Feld zuordnen und Wert umwandeln (einzelnes Feld)** . Diese Regel ist mit der Ereignisregel verknüpft und wird gleichzeitig ausgeführt, was eine optimierte Zuordnung und Transformation von Ereignisdaten ermöglicht, um Warnungen anzureichern.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Warnungsautomatisierung ( ).
3. Auf der Seite Warnungsautomatisierung unter **Automatisierungstypen** , Wählen Sie aus **Bereichern** . Die Seite „Warnungen anreichern“ wird angezeigt.



4. Wählen Sie Aus **Automatisierung erstellen** .
   Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert.
5. In **Automatisierungsname** Geben Sie den Namen der Automatisierung für die Ergänzung von Warnungen ein.
6. In **Wenn diese Bedingungen erfüllt sind** Richten Sie Filterkriterien ein, um die Warnungen zu identifizieren, die Sie anreichern möchten.

   Die Bedingung wird anhand des vom Quellüberwachungssystem empfangenen Rohereignisses ausgewertet und berücksichtigt keine angereicherten Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Von **Zuweisungsgruppe** Feldmenü die Zuweisungsgruppe auswählen, um zu bestimmen, welche Warnungen des Teams die Automatisierung auslösen.

Die **Zuweisungsgruppe** Stellt ein bestimmtes Team dar, das für die Verarbeitung bestimmter Warnungen verantwortlich ist. Durch Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung gezielt und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

Hinweis:

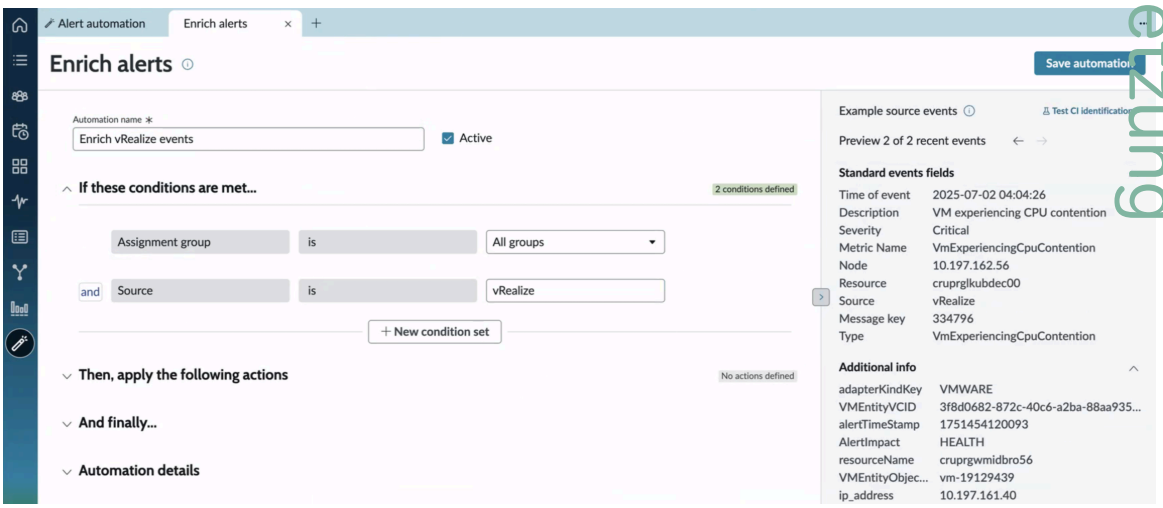
- Wenn Sie mit einer Administratorrolle (evt_mgmt_admin) bei der Instanz angemeldet sind, sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie auswählen **Alle Gruppen** Um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
- Wenn Sie ein Teamoperator sind, sind nur die Gruppen verfügbar, denen Sie angehören.
- Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

b. Von **Quelle** Feldmenü: Wählen Sie das Überwachungstool aus, aus dem die Warnung generiert wird.

c. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit den Operatoren ODER oder UND hinzu.

Um einen weiteren Satz von Bedingungen hinzuzufügen, wählen Sie aus **+ neuer Bedingungssatz** . Sie können auch manuell ein Feld mit zusätzlichen Informationen hinzufügen, wenn es nicht in der Dropdown-Liste angezeigt wird.

Hinweis: Wählen Sie Aus **Laden Sie vergangene Ereignisse** Dient zum Anzeigen vorheriger Ereignisse beim Erstellen der Automatisierung.



7. In **Wenden Sie dann die folgenden Aktionen an** Wählen Sie die Automatisierungsaktionen aus, die von dieser Automatisierung ausgelöst werden.
Sie müssen mindestens eine Aktion auswählen.

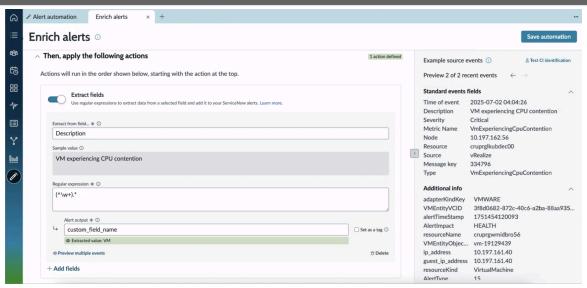
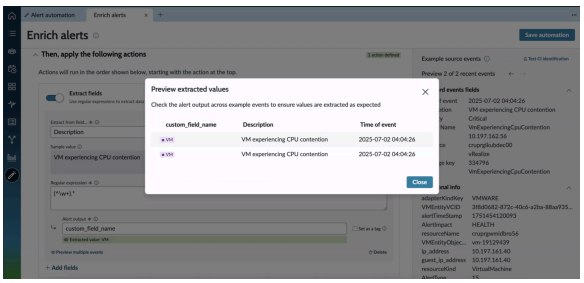
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

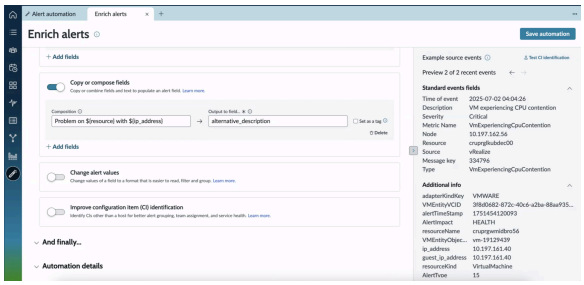
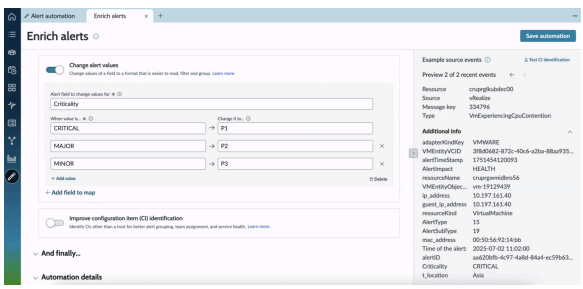
- **Extrahieren Sie Warnungsfelder** : Ruft Warnungsfeldwerte aus der Ereignisnutzlast ab und platziert sie in ein Warnungsausgabefeld.
- **Kopieren oder verfassen Sie Felder** : Führt verschiedene Warnungsfelder, Tags und Texte zusammen, um eine zusammengesetzte Warnungsausgabe zu generieren.
- **Warnungswerte ändern** : Ordnet den aktuellen Wert von Warnungsfeldern angegebenen neuen Werten zu.
- **Verbessern Sie die Identifizierung des Konfigurationselements (Configuration Item, CI)** : Identifiziert andere CIs als einen Host, um die Warnungsgruppierung, die Teamzuweisung und die Serviceintegrität zu verbessern.

Option	Aktion
Warnungsfelder extrahieren	**a.** Aktivieren Sie **Extrahieren Sie Warnungsfelder** Umschalter. **b.** Von **Quelleingabefeld** Menü einen Wert auswählen. Im Menü werden die Standard-Ereignisfelder, zusätzliche Informationen und Tags angezeigt. Der Feldwert wird dann angezeigt. Sie können auch manuell einen Feldnamen eingeben, der nicht angezeigt wird, und Ihren eigenen Wert hinzufügen. Im Bereich Beispielquellenereignisse wird ein Beispiel für aktuelle Ereignisse in Ihrem System angezeigt. Wenn keine Ereignisse angezeigt werden, können Sie ein Ereignis erstellen, siehe Event-Regel erstellen oder bearbeiten. **c.** In **Regulärer Ausdruck** Erstellen Sie einen regulären Ausdruck, um den Wert zu extrahieren, den Sie extrahieren möchten. **Hinweis:** Sie können Text mit Formatkonventionen für reguläre Ausdrücke (regulärer Ausdruck) verfassen. Verwenden Sie eine oder mehrere Erfassungsgruppen mit Klammern, um Teile der Eingabe zu extrahieren. Erfassungsgruppen im regulären Ausdruck werden Warnungsausgaben basierend auf der Reihenfolge zugewiesen, in der sie angezeigt werden. Der reguläre Ausdruck muss mit der gesamten Eingabe übereinstimmen. Berücksichtigen Sie daher, Ihren regulären Ausdruck mit zu umgeben `.*` An jedem Ende Beispiel: `(\W+).acme.com.*` Erfasst den Hostnamen in einem vollqualifizierten Domänennamen. Der Parser für die Engine für reguläre Ausdrücke ist mit Perl-kompatiblen regulären Ausdrücken (PCRE) kompatibel. **d.** In **Warnungsausgabe** Feld auswählen Sie ein Warnungsfeld oder ein Warnungs-Tag aus. Sie können auch manuell einen neuen Feldnamen eingeben. Wenn Sie ein Warnungs-Tag hinzufügen möchten, wählen Sie aus **Als Tag festlegen** Kontrollkästchen. **Tipp:** Erstellen Sie Warnungs-Tags, die quellenübergreifend freigegeben werden können, um das Filtern und Gruppieren zu erleichtern, z. B. die sofort einsatzbereiten Tags.

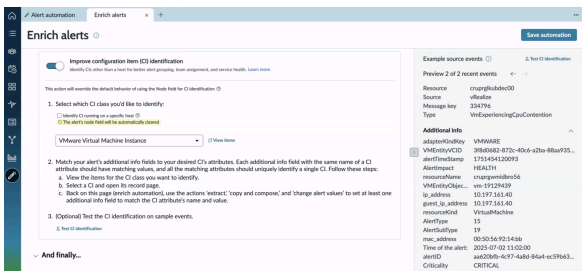
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	 **e.** Wählen Sie Aus **Vorschau mehrerer Ereignisse anzeigen** Um sicherzustellen, dass der reguläre Ausdruck (regulärer Ausdruck) allgemein genug ist, um Werte für viele Beispiele korrekt zu extrahieren. **Hinweis:** Diese Option ist nur verfügbar, wenn Beispielquellenereignisse verfügbar sind und mit dem Filter für reguläre Ausdrücke abgeglichen werden.  Um zusätzliche Felder für die Extraktion einzubeziehen, wählen Sie aus **+ Felder hinzufügen** .
Felder kopieren oder verfassen	**a.** Aktivieren Sie **Kopieren oder verfassen Sie Felder** Umschalter. **b.** Von **Quelleingabefeld** Menü, wählen Sie Warnungsfelder und/oder Warnungs-Tags aus, geben Sie manuell einen Feldnamen ein, oder fügen Sie sogar Freitext hinzu. Warnungsfelder werden in angezeigt ${field} Syntaxformat. **c.** In **Warnungsausgabe** Ein vorhandenes Warnungsfeld oder Warnungs-Tag auswählen oder ein Warnungsfeld manuell eingeben. Die **Warnungsausgabe** Das Feld ist eine angereicherte Warnung, die die zusammengesetzten Warnungsdaten enthält. Um die Gruppierung zu erleichtern, können Sie ein Tag aus dem Menü auswählen. Wenn Sie den neuen Feldnamen als Tag für die Gruppierung verwenden möchten, wählen Sie aus **Als Tag festlegen** Kontrollkästchen.

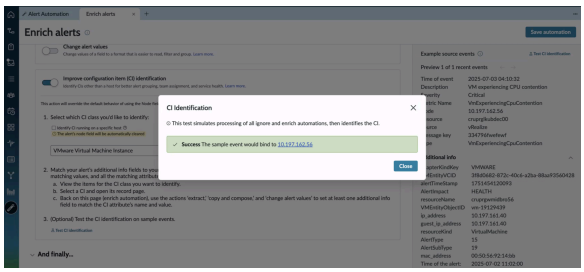
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Tipp: Erstellen Sie Warnungs-Tags, die quellenübergreifend freigegeben werden können, um das Filtern und Gruppieren zu erleichtern, z. B. die sofort einsatzbereiten Tags.  Um zusätzliche Warnungsdatenzusammensetzungen zu erstellen, wählen Sie aus **+ Felder hinzufügen** .
Warnungswerte ändern	**a.** Aktivieren Sie **Warnungswerte ändern** Umschalter. **b.** In **Warnungsfeld** , Geben Sie das Feld in der Warnung ein, für das Sie Werte zuordnen möchten. **c.** In **Von-Wert** Feld den ursprünglichen Wert in das Warnungsfeld eingeben, das Sie ändern möchten. **d.** In **Bis Wert** Feld den neuen Wert eingeben, der den ursprünglichen Wert im Warnungsfeld ersetzt. Um weitere Feldwerte hinzuzufügen, wählen Sie aus **+ Wert hinzufügen** Und um weitere Felder zur Zuordnung hinzuzufügen, wählen Sie aus **+ Feld zu Zuordnung hinzufügen** . 
Identifizierung von Konfigurationselementen (CI) verbessern	Mit dieser Option können Sie ändern, wie Warnungen an ein Konfigurationselement (Configuration Item, CI) gebunden oder verknüpft werden, um sicherzustellen, dass Warnungen mit den richtigen IT-Komponenten verknüpft sind, um die Transparenz zu verbessern und Probleme schneller zu lösen. Die standardmäßige und häufigste Methode zum Binden von Warnungen an CIs basiert auf **Knoten** Feld. Dies funktioniert sofort, ohne dass eine Konfiguration erforderlich ist. Verwenden Sie es, indem Sie ausfüllen **Knoten** Feld in Ihrer Warnung mit dem Namen eines CI, dem vollqualifizierten Domänennamen (FQDN), der IP- oder MAC-Adresse. Dies unterstützt Host-CIs, einschließlich Computer, Betriebssysteme

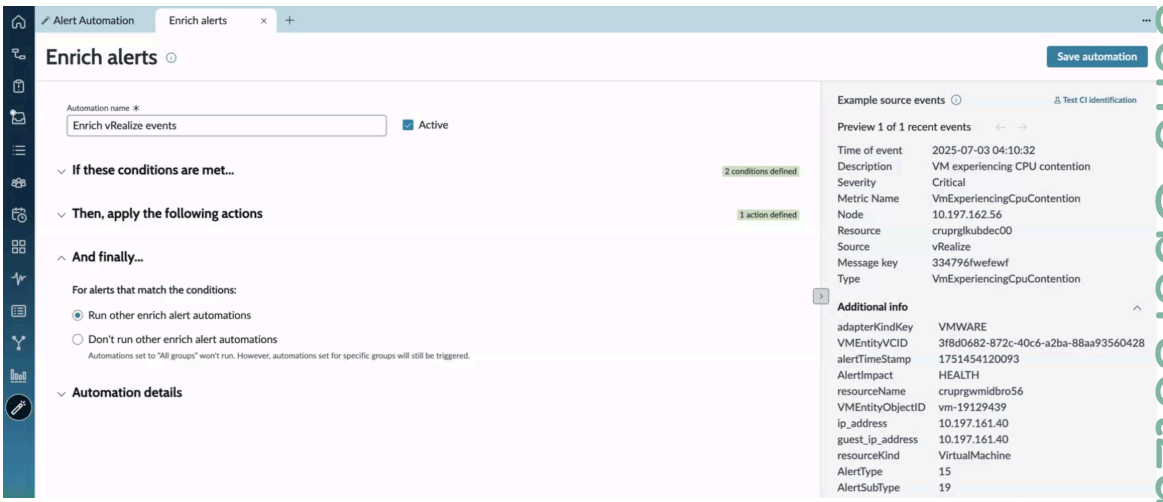
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	(OS), Switches, Router oder beliebige CI-Typen oder Klas–sen, die die Tabelle [cmdb_ci_Hardware] erweitern. Sie können diese Aktion aktivieren, um die CI-Identifizierung für andere Arten von CIs wie Prozesse oder Serviceinstan–zen zu verbessern. Das System sucht basierend auf dem ausgewählten CI-Typ in der entsprechenden CMDB-Tabelle nach einem übereinstimmenden CI. Wenn Sie beispielsweise VMware Virtual Machine Instance als CI-Klasse auswählen, sucht das System anhand von Details aus dem Ereignisregel–datensatz, insbesondere dem nach einem übereinstimmenden Datensatz in der Tabelle [cmdb_ci_vmware_instance] **Zusätzli che Informationen** Felder.  **a.** Wählen Sie aus **Identifizieren Sie das CI, das auf einem be stimmten Host ausgeführt wird** Kontrollkästchen, um anzu–geben, dass das CI auf einem bestimmten Host ausgeführt wird. Stellen Sie sicher, dass **Knoten** Das Feld in der Warnung ist korrekt ausgefüllt, um ein Host-CI zu identifizieren. Das CI, das Sie identifizieren, muss über einen verfügen Wird auf ausgeführt Beziehung zum Host-CI oder der BE Dem Host zuge-ordnet . **Hinweis:** Außerdem, wenn der Wert ist **Knoten** In **War nungsausgabe** Feld des Abschnitts „Felder extrahieren“ oder in **Ausgabe an Feld** Wählen Sie im Abschnitt Felder kopie-ren oder verfassen aus, und wählen Sie dann aus **Identifizieren Sie das CI, das auf einem bestimmten Host ausgeführt wird** Kontrollkästchen. **b.** Wählen Sie die zu bindende CI-Klasse aus. Wählen Sie Aus **Zeigen Sie Elemente an** Um die Liste der CIs dieses Typs und ihrer Attributwerte anzuzeigen. **c.** Stellen Sie sicher, dass mindestens ein CI-Attribut in vor–handen ist **Zusätzliche Informationen** Feld der Warnung. Anweisungen zum Ausfüllen dieser Felder finden Sie unter Legen Sie zusätzliche Informationsfelder so fest, dass sie dem CI-Attri-butformat entsprechen. Das System versucht, Werte aus dem abzugleichen **Zusätzliche Informationen** Feld der Warnung mit der CI-Tabelle. Wenn eine Übereinstimmung gefunden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	wird, wird die Warnung an das entsprechende CI gebun–den. **d.** Wählen Sie Aus **CI-Identifizierung testen** Zum Testen der CI-Identifizierung bei Beispielereignissen.  Weitere Informationen zur CI-Bindung finden Sie unter Warnungen werden an CIs gebunden.

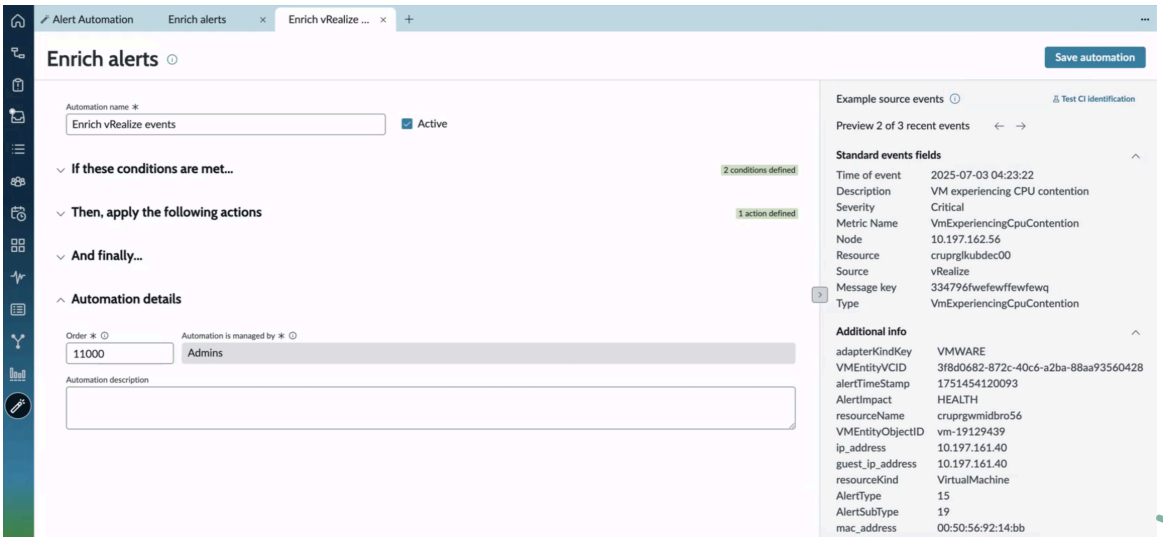
8. In **Und schließlich** Um nach der Ausführung dieser Automatisierung weitere Ergänzungsautomatisierungen mit denselben Filterbedingungen auszuführen, wählen Sie aus **Führen Sie andere Anreicherungswarnungsautomatisierungen aus** .



Wenn Sie auswählen **Führen Sie keine anderen Anreicherungswarnungsautomatisierungen aus** , Zusätzliche Automatisierungen dieses Typs werden nicht mehr ausgeführt, nachdem diese Automatisierung einmal ausgeführt wurde. Wenn die Automatisierung von einem Administrator verwaltet wird, wird die Ausführung von Automatisierungen im Besitz des Administrators beendet, aber weiterhin Automatisierungen im Besitz anderer Zuweisungsgruppen ausgeführt.

9. In **Automatisierungsdetails** Geben Sie eine Beschreibung der Reihenfolge und Automatisierung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. In **Reihenfolge** Feld die Automatisierungsreihenfolge eingeben.

> **Hinweis:** Automatisierungen werden in der Reihenfolge vom niedrigsten zum höchsten ausgeführt. Stellen Sie sicher, dass keine Ergänzungsautomatisierungen mit einer niedrigeren Ordnungsnummer vorhanden sind, die übereinstimmende Bedingungen und aufweisen **Wenden Sie zusätzliche Automatisierungen dieses Typs an** Auf „falsch“ festlegen. Andernfalls kann dies verhindern, dass nachfolgende Automatisierungen ausgeführt werden.

Die **Automatisierung wird von verwaltet** Das Feld zeigt das Team oder die Zuweisungsgruppe an, die diese Automatisierung besitzt, bearbeitet und löschen kann. Die Zuweisungsgruppe ist mit der in definierten Gruppe identisch **Wenn diese Bedingungen erfüllt sind** Abschnitt.

b. In **Automatisierungsbeschreibung** Geben Sie eine kurze Beschreibung der Automatisierung ein.

10. Wählen Sie Aus **Automatisierung speichern** .
Eine Benachrichtigung wird angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Anreicherungsautomatisierung wird auf der Seite „Warnungen anreichern“ angezeigt, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

Nächste Maßnahme

Sie können Warnungen effektiver verwalten, indem Sie ähnliche Warnungen mithilfe von gruppieren Gruppenautomatisierung erstellen.

Zugehörige Informationen

Warnungsfelder werden extrahiert und verfasst

Warnungsfelder werden extrahiert und verfasst

Extrahieren und Verfassen sind Möglichkeiten, um zu verwalten, was in der Warnungsausgabe angezeigt wird, wodurch das Filtern, Gruppieren und Lesen einfacher wird. Mit der Warnungsautomatisierung können Sie Werte aus dem Warnungsfeld der Ereignisnutzlast extrahieren und in einem Warnungsausgabefeld platzieren. Durch das Verfassen können Sie mehrere Warnungsfelder in einem einzelnen Ausgabefeld zusammenführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

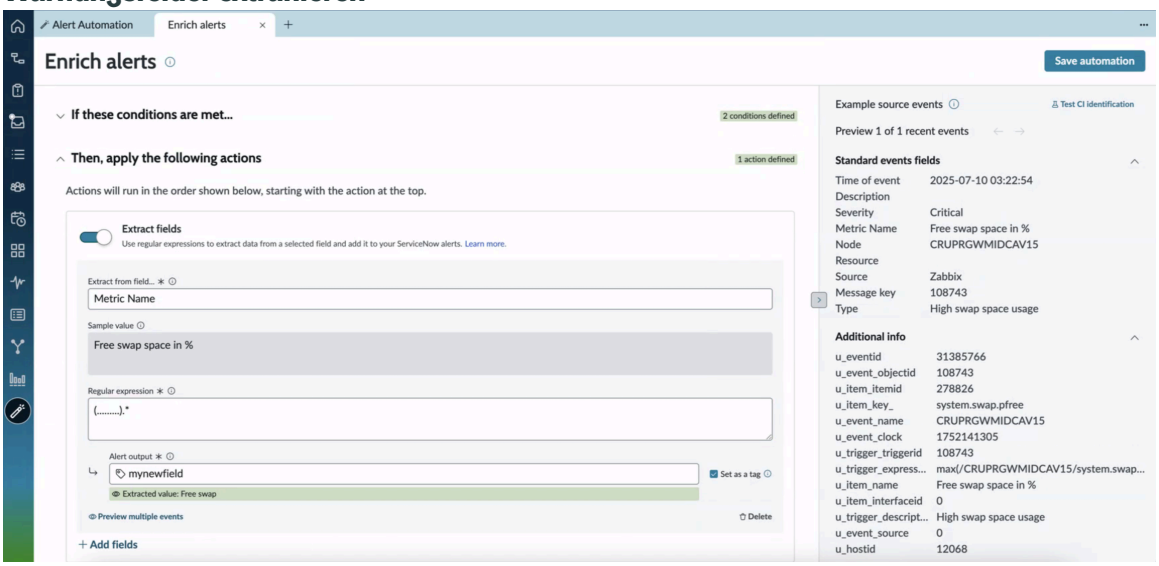
Warnungsfelder werden extrahiert

Warnungsbenachrichtigungen enthalten häufig relevanten Kontext, der in Ereignisnutzlasten verborgen ist. Indem Sie Warnungsausgaben mit Werten aus der vorhandenen Nutzlast ergänzen, können Sie die Bedeutung von Warnungen besser verstehen und die entsprechenden Schritte für die Lösung bestimmen. Beispielsweise enthält ein Hostname normalerweise wichtige Informationen wie Service, Knoten, Cluster, Rechenzentrum und Domäne. Um den Wert für ein Cluster-Tag basierend auf eingehenden Hostdaten automatisch hinzuzufügen, können Sie nur die Clusterdaten extrahieren.

Verwenden Sie beim Extrahieren von Warnungsfeldern reguläre Ausdrücke (regulärer Ausdruck), um Wertformeln zu erstellen. Mit dem regulären Ausdruck können Sie die relevanten Teile der Nutzlast genau identifizieren und erfassen, wodurch aussagekräftige und umsetzbare Warnungsbenachrichtigungen erstellt werden können.

Hinweis: Sie können Text mit Formatkonventionen für reguläre Ausdrücke (regulärer Ausdruck) verfassen. Verwenden Sie eine oder mehrere Erfassungsgruppen mit Klammern, um Teile der Eingabe zu extrahieren. Erfassungsgruppen im regulären Ausdruck werden Warnungsausgaben basierend auf der Reihenfolge zugewiesen, in der sie angezeigt werden. Der reguläre Ausdruck muss mit der gesamten Eingabe übereinstimmen. Berücksichtigen Sie daher, Ihren regulären Ausdruck mit zu umgeben `.*` An jedem Ende Beispiel: `(\W+).acme.com.*` Erfasst den Hostnamen in einem vollqualifizierten Domänennamen. Der Parser für die Engine für reguläre Ausdrücke ist mit Perl-kompatiblen regulären Ausdrücken (PCRE) kompatibel.

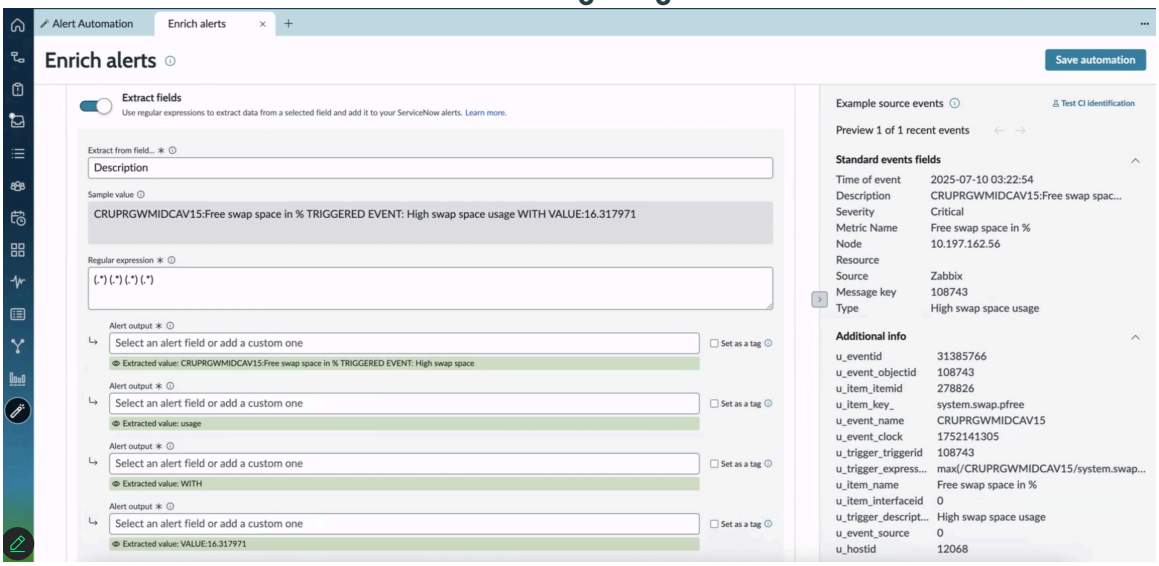
Warnungsfelder extrahieren



Wenn Sie mehrere Erfassungsgruppen mit Klammern verwenden, wird jeder extrahierte Wert in einem separaten Ausgabefeld angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Extrahieren Sie das Feld für mehrere Warnungsausgaben



Zeigen Sie eine Vorschau der Warnungsausgabe für Beispielereignisse an, um sicherzustellen, dass die Werte wie erwartet extrahiert werden, indem Sie auswählen **Vorschau mehrerer Ereignisse anzeigen** .

Hinweis: Diese Option ist nur verfügbar, wenn Beispielquellenereignisse verfügbar sind und mit dem Filter für reguläre Ausdrücke abgeglichen werden.

Beispiel: Warnungsfelder werden extrahiert

Angenommen, Sie müssen nur sechs Buchstaben aus einem bestimmten Feld eines Ereignisses extrahieren und in einem neuen Warnungsfeld mit dem Namen anzeigen `Mynewfield` . Sie möchten dieses neue Warnungsfeld auch zur späteren Verwendung in der Warnungsgruppierung kennzeichnen. So können Sie dies erreichen:

- **Quelleingabefeld** : Wählen Sie das Ereignisfeld aus, aus dem Sie Daten extrahieren möchten. In diesem Fall lautet das Feld **Metrikname** .
- **Regulärer Ausdruck** : Verwenden Sie einen regulären Ausdruck, um das bestimmte benötigte Teil aus dem Wert des ausgewählten Felds zu extrahieren. Beispiel: Wenn **Metrikname** Feldwert enthält „Freier Swap-Platz in %“, und Sie möchten „Freier Swap“ extrahieren. Ihr regulärer Ausdruck muss (.....).*.
- **Warnungsausgabe** :
  - Wählen Sie ein vorhandenes Warnungsfeld oder ein vorhandenes Warnungs-Tag aus, oder geben Sie manuell einen neuen Feldnamen ein. In diesem Fall geben wir einen neuen Feldnamen ein `Mynewfield` .
  - Festlegen `Mynewfield` Als Tag zur späteren Verwendung in der Tag-basierten Gruppierung. Beachten Sie das Tag, das vor dem Feldnamen angezeigt wird.

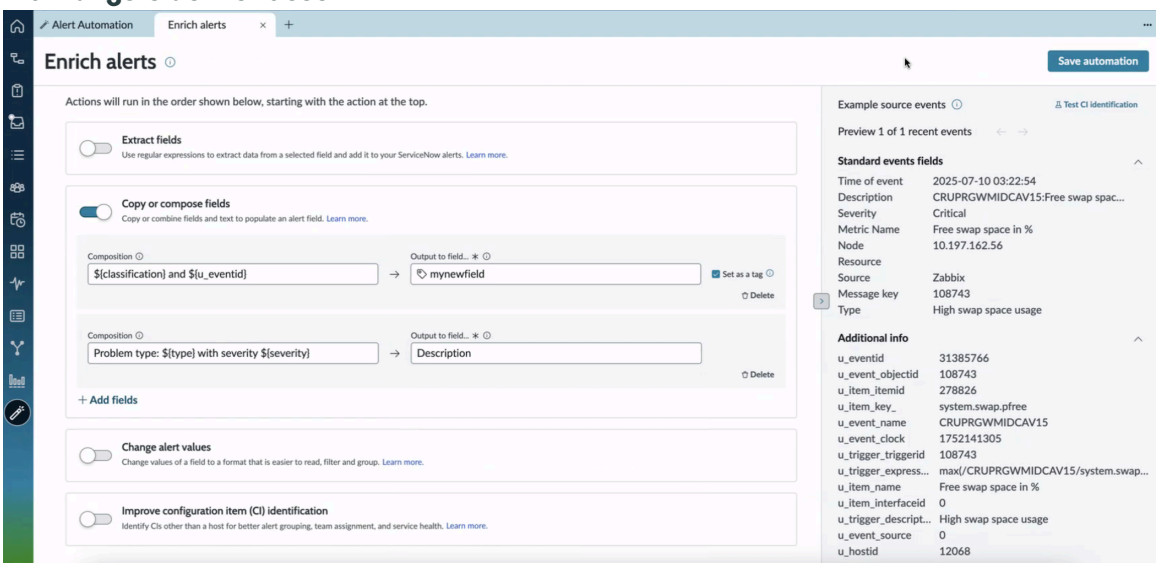
  Nachdem der reguläre Ausdruck auf den Wert des ausgewählten Felds angewendet wurde (in diesem Fall die **Metrikname** Feldwert), überprüfen Sie das extrahierte Wort, das unter angezeigt wird **Warnungsausgabe** Feld. Beispielsweise sollte „Free Swap“ angezeigt werden, wenn der reguläre Ausdruck korrekt übereinstimmt.
- **Vorschau mehrerer Ereignisse anzeigen** : Durch die Vorschau mehrerer Ereignisse können Sie überprüfen, ob der reguläre Ausdruck Daten aus einer Reihe von Beispielereignissen genau extrahiert. Dies hilft bei der Bestimmung, ob Anpassungen am regulären Ausdruck erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsfelder werden erstellt

Beim Erstellen einer Warnungsausgabe können Sie Felder, Tags oder Freitext auswählen oder manuell eingeben, die eingeschlossen werden sollen. Diese Daten können leicht gelesen, gefiltert und gruppiert werden, um die Verwaltung und das Verständnis der Warnungen zu verbessern.

Warnungsfelder verfassen



Beispiel: Warnungsfelder werden verfasst

Angenommen, Sie möchten zwei Eingabefelder haben, die Daten verfassen und in zwei verschiedenen Warnungsausgabefeldern anzeigen. In einem Szenario soll der Quellwert aus einem vorhandenen Warnungsfeld zusammen mit einem neuen Feld stammen, das den zusammengesetzten Wert in einem neuen Warnungsausgabefeld anzeigt. Sie planen auch, das neue Warnungsausgabefeld zur späteren Verwendung in der Tag-basierten Gruppierung zu kennzeichnen. Im anderen Szenario kombinieren Sie vorhandene Felder mit Freitext, und wählen Sie die Warnungsausgabe aus, die in einem vorhandenen Warnungsfeld angezeigt werden soll. So können Sie dies erreichen:

- Szenario 1:

1. **Quelleingabefeld** : Wählen Sie ein vorhandenes Warnungsfeld aus, und fügen Sie den Text „und“ hinzu, und geben Sie dann ein anderes Feld ein **u_eventid** . Beispiel: ${classification} und ${u_eventid}.

   Beachten Sie, dass Warnungsfelder in angezeigt werden `${field}` Syntaxformat. Sie können auch den Feldnamen aus der Dropdown-Liste auswählen, und die Syntax wird automatisch hinzugefügt.

2. **Warnungsausgabe** : Geben Sie den Namen des neuen Warnungsfelds ein, in dem Sie die Werte aus den Eingabefeldern anzeigen möchten. Nennen wir es beispielsweise `Mynewfield` .

   Festlegen `Mynewfield` Als Tag zur späteren Verwendung in der Tag-basierten Gruppierung. Beachten Sie das Tag, das vor dem Feldnamen angezeigt wird.

- Szenario 2:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. **Quelleingabefeld** : Wählen Sie vorhandene Warnungsfelder aus, und fügen Sie den gewünschten Freitext ein, damit sie im Warnungsausgabefeld angezeigt werden sollen. Beispiel: Problemtyp: ${type} mit Schweregrad ${severity}.

   Warnungsfelder werden in angezeigt `${field}` Syntaxformat. Sie können auch den Feldnamen aus dem Dropdown-Feld auswählen, und die Syntax wird automatisch hinzugefügt.

2. **Warnungsausgabe** : Wählen Sie ein vorhandenes Warnungsfeld aus, in dem Sie die Werte aus den Eingabefeldern anzeigen möchten. Wählen Sie beispielsweise aus **Beschreibung** .

Legen Sie zusätzliche Informationsfelder so fest, dass sie dem CI-Attributformat entsprechen

Legen Sie zusätzliche Informationsfelder in Warnungen so fest, dass sie dem Feld- und Wertformat von CI-Attributen in CI-Datensätzen entsprechen. Dies stellt eine genaue Bindung von Warnungen zu CI sicher, verbessert die Warnungsnachverfolgung und reduziert den manuellen Aufwand.

Vorbereitungen

Stellen Sie sicher, dass Sie sich auf der Seite „Warnungen anreichern“ und im befinden **Verbessern Sie die Identifizierung des Konfigurationselements (Configuration Item, CI)** Umschalter ist aktiviert.

Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

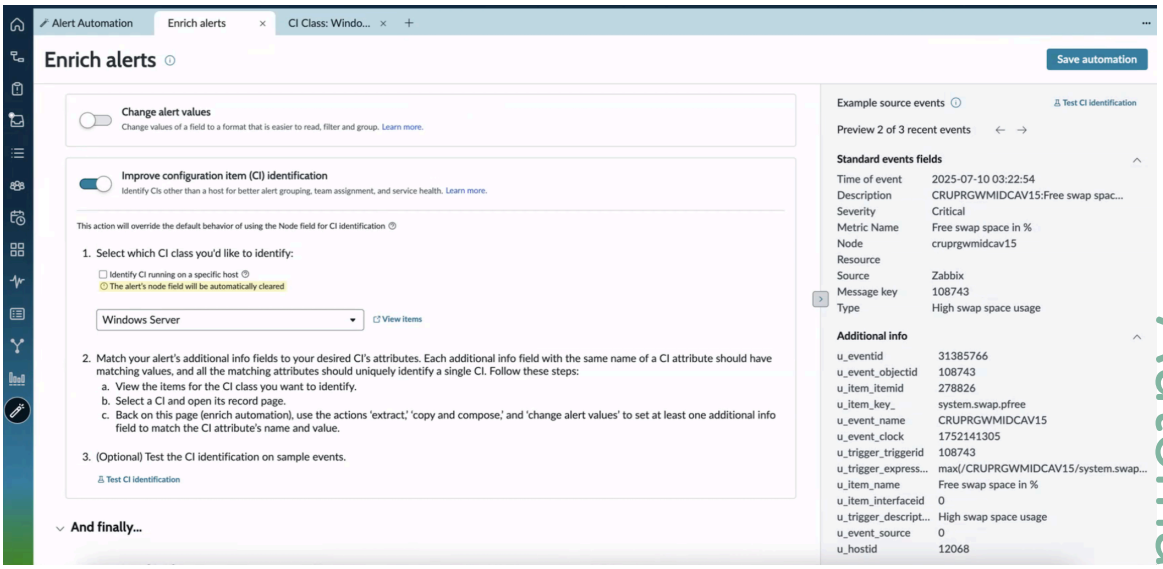
Warum und wann dieser Vorgang ausgeführt wird

Das System versucht, den abzugleichen **Zusätzliche Informationen** Felder der Warnung mit Attributen in der CI-Tabelle. Wenn genau ein übereinstimmendes CI gefunden wird, wird die Warnung mit diesem CI verknüpft. Damit die CI-Identifizierung erfolgreich ist, fügen Sie neue Felder hinzu, oder stellen Sie sicher, dass Ihre Warnung zusätzliche Informationsfelder enthält, die dem Spaltennamen für CI-Attribute entsprechen. Verwenden Sie beispielsweise den Spaltennamen **ip_address** Anstelle der Spaltenbezeichnung **IP-Adresse** . Jeder übereinstimmende Schlüsselname muss übereinstimmende Werte aufweisen. Wenn Ihre Warnung übereinstimmende Felder enthält, die Sie nicht für die Bindung verwenden möchten, kopieren Sie sie in ein anderes Feld, und löschen Sie dann das ursprüngliche Feld.

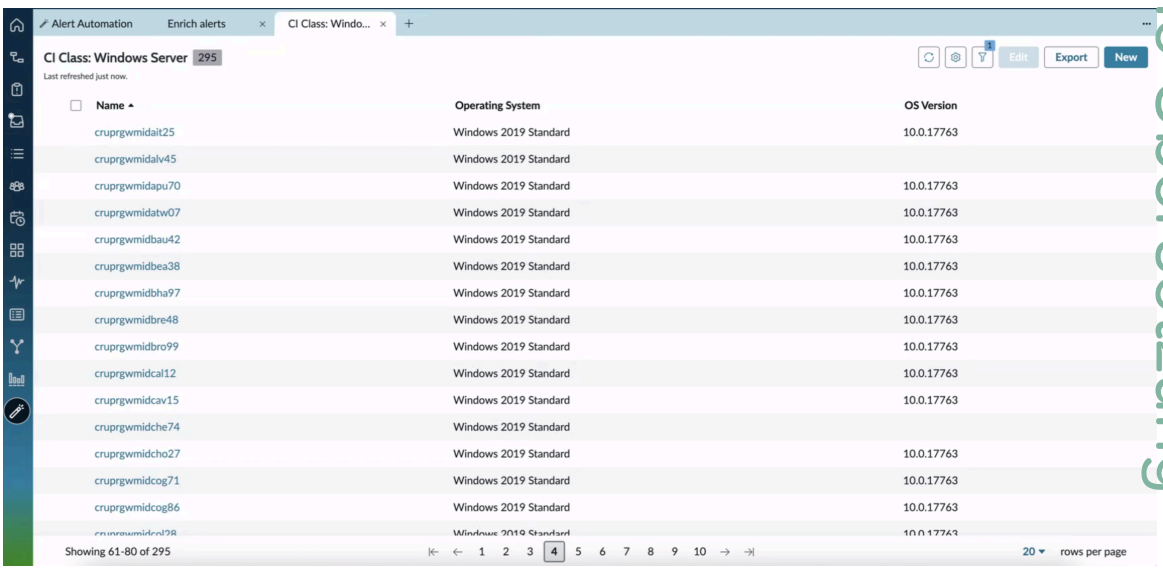
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Unter **Verbessern Sie die Identifizierung des Konfigurationselements (Configuration Item, CI)** , In **Wählen Sie aus, welche CI-Klasse Sie identifizieren möchten** Wählen Sie die CI-Klasse aus.



2. Wählen Sie Aus **Zeigen Sie Elemente an** Neben **Wählen Sie aus, welche CI-Klasse Sie identifizieren möchten** Feld zum Öffnen der Liste der CIs der ausgewählten CI-Klasse.

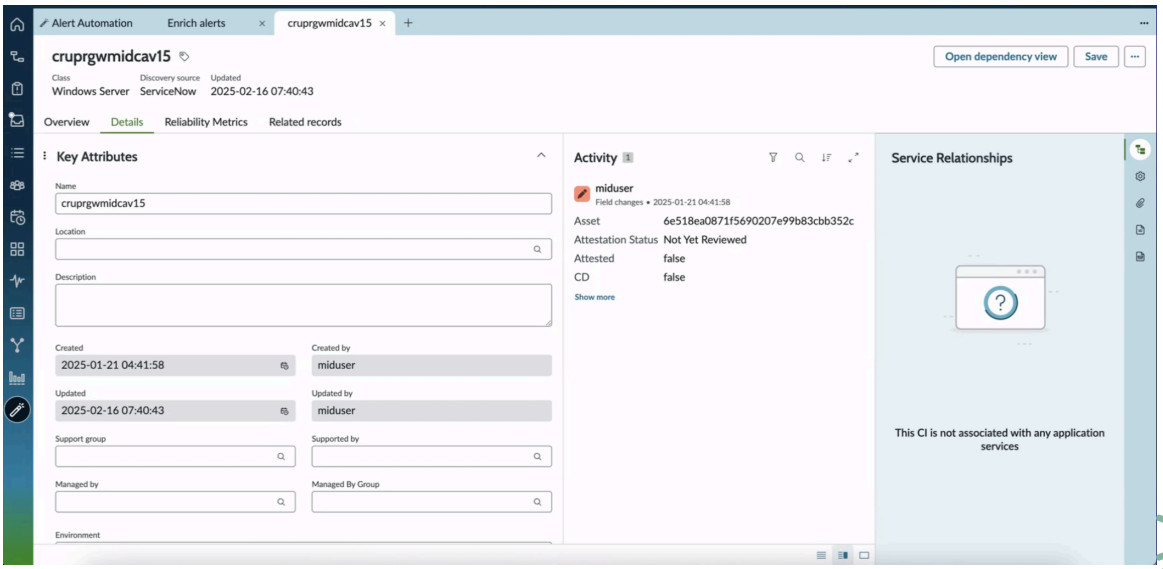


3. Wählen Sie einen CI-Namen aus, um seine Details oder Datensatzseite zu öffnen.

   Mindestens ein Feld und der entsprechende Wert auf der CI-Detailseite müssen in angezeigt werden **Zusätzliche Informationen** Feld der Warnung.

Automatische Übersetzung

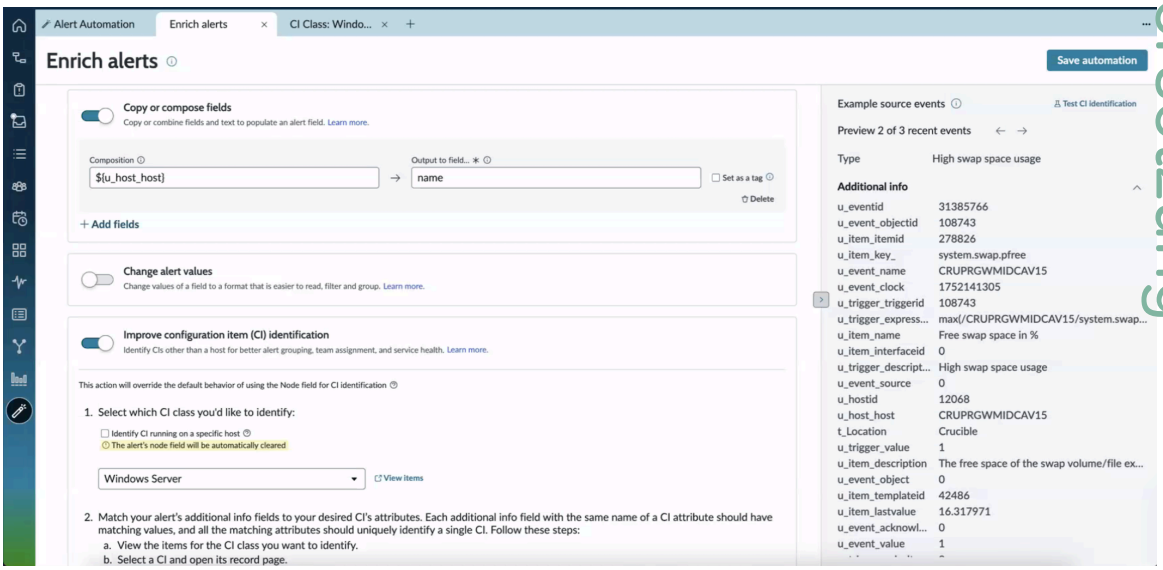
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Verwenden Sie auf der Seite Warnungen anreichern **Felder extrahieren** , **Felder kopieren oder verfassen** , Und **Warnungswerte ändern** Zum Festlegen von mindestens einem **Zusätzliche Informationen** Feld in Ihrer Warnung, um genau dem Feld- und Wertformat der CI-Attribute im CI-Datensatz zu entsprechen.

   Beispiel: Angenommen, die CI-Datensatzseite hat **Name** Feld mit dem Wert **CRUPRGWMIDCAV15** . Um diese Felder und ihre Werte in einzubeziehen **Zusätzliche Informationen** Feld der Warnung: Legen Sie die Felder wie in der Abbildung angezeigt fest.

   Ordnen Sie zu `${u_Host_Host}` Feld zu einem neuen Feld namens **Name** . Dieses Feld wird zu hinzugefügt **Zusätzliche Informationen** Und wird für die CI-Identifizierung während der Bindungsphase verwendet.



Gruppenautomatisierung erstellen

Die Gruppierungsautomatisierung hilft Ihnen, Warnungen effektiver zu verwalten, indem ähnliche Warnungen zusammen erfasst werden. Dies erleichtert das Anzeigen von Mustern, die schnelle Identifizierung von Problemen und die effiziente Reaktion. Indem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie Warnungen auf diese Weise organisieren, können Sie Warnungsrauschen reduzieren, Ursachen identifizieren und sie den entsprechenden Teams zuweisen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird

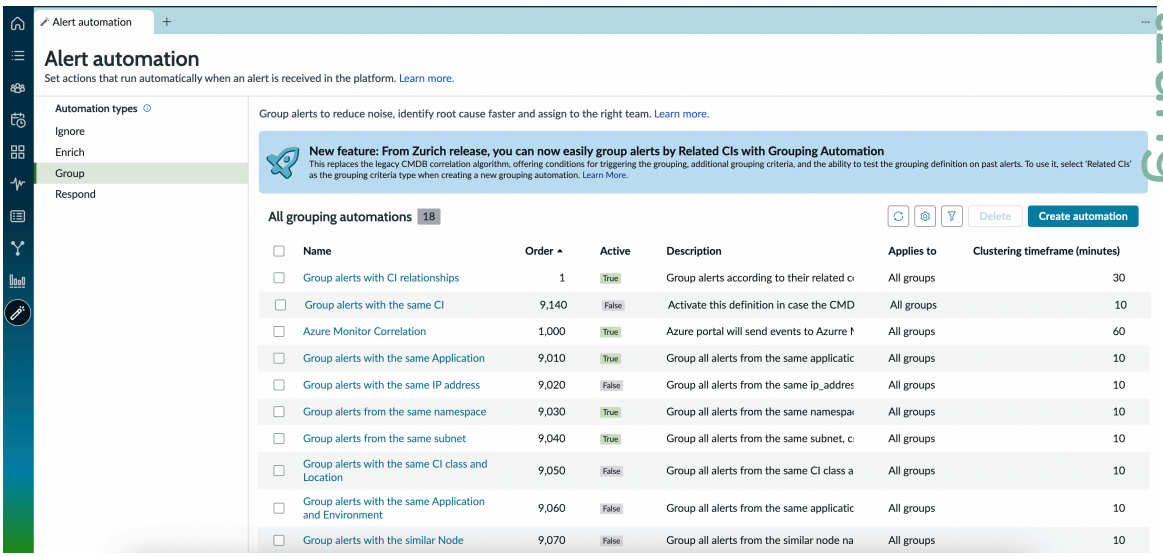
Die Gruppierung dieser Methode ist am nützlichsten, wenn Warnungen allgemeine Daten oder Tags teilen, z. B. einen Knoten oder einen Standort. Sie können Felder oder Tags verwenden, die über eine Anreicherungsautomatisierung ausgefüllt werden. Dies ist die beste Möglichkeit, Warnungen zu gruppieren, wenn Ihre CMDB oder Servicezuordnungen unausgereift sind. Dies ergänzt unsere anderen Gruppierungsalgorithmen, einschließlich Warnungskorrelationsregeln, CMDB, ML und textbasierte Gruppierung. Warnungen werden mit ihrer ersten Übereinstimmung gruppiert, und Sie können die Prioritätsreihenfolge dieser Algorithmen über die Systemeigenschaft steuern. Informationen zur Reihenfolge der Korrelationslogik finden Sie unter Konfigurieren Sie die logische Reihenfolge der Warnungskorrelation.

Die Warnungsautomatisierung bietet auch eine Simulationsfunktion, mit der Sie testen können, wie viele Warnungsgruppen gebildet werden, wie viele nicht gruppiert sind, und wie hoch die Komprimierungsrate ist. Eine höhere Komprimierungsrate bedeutet, dass Ihr Team produktiver ist und möglicherweise die Ursachen schneller identifizieren kann. Überlegen Sie jedoch, ob die Gruppen korrekt, operativ korrekt und den richtigen Teams zugewiesen sind. Sie können die Gruppenkriterien anpassen, bis Sie mit den resultierenden Gruppen zufrieden sind.

Für Anwender, die mit dem Klassiker vertraut sind Ereignismanagement Experience bietet diese Funktion eine einfachere Schnittstelle mit verbesserter Teamunterstützung zum Erstellen von Tag-basierten Warnungs-Clustering-Definitionen.

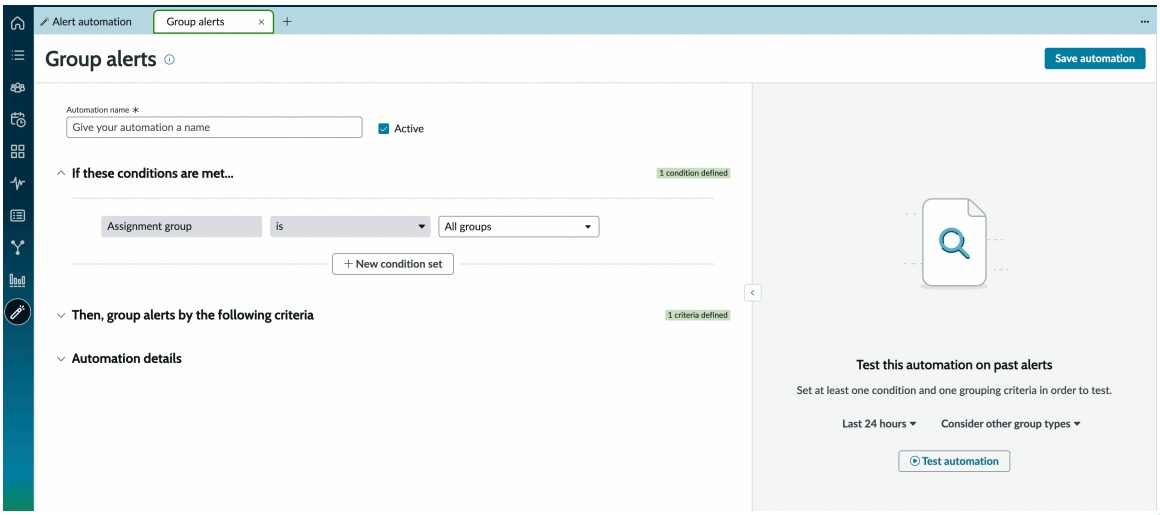
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Warnungsautomatisierung ( ).
3. Auf der Seite Warnungsautomatisierung unter **Automatisierungstypen** , Wählen Sie aus **Gruppe** .
   Die Seite Gruppenwarnungen wird angezeigt.



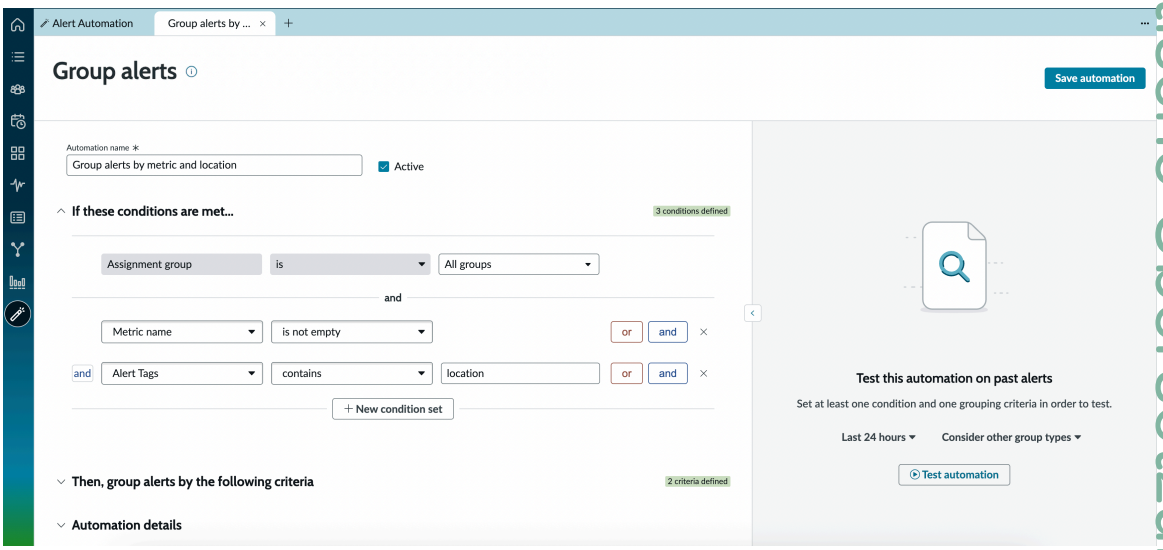
4. Wählen Sie Aus **Automatisierung erstellen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. In **Automatisierungsname** Feld den Namen der Automatisierung für die Gruppierung von Warnungen eingeben.
Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert.

6. In **Wenn diese Bedingungen erfüllt sind** Richten Sie Filterkriterien ein, um die Warnungen zu identifizieren, die Sie gruppieren möchten.



a. Von **Zuweisungsgruppe** Feldmenü die Zuweisungsgruppe auswählen, um zu bestimmen, welche Warnungen des Teams die Automatisierung auslösen.

Die **Zuweisungsgruppe** Stellt ein bestimmtes Team dar, das für die Verarbeitung bestimmter Warnungen verantwortlich ist. Durch Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung gezielt und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie mit einer Administratorrolle (evt_mgmt_admin) bei der Instanz angemeldet sind, sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie auswählen **Alle Gruppen** Um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
- Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
- Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

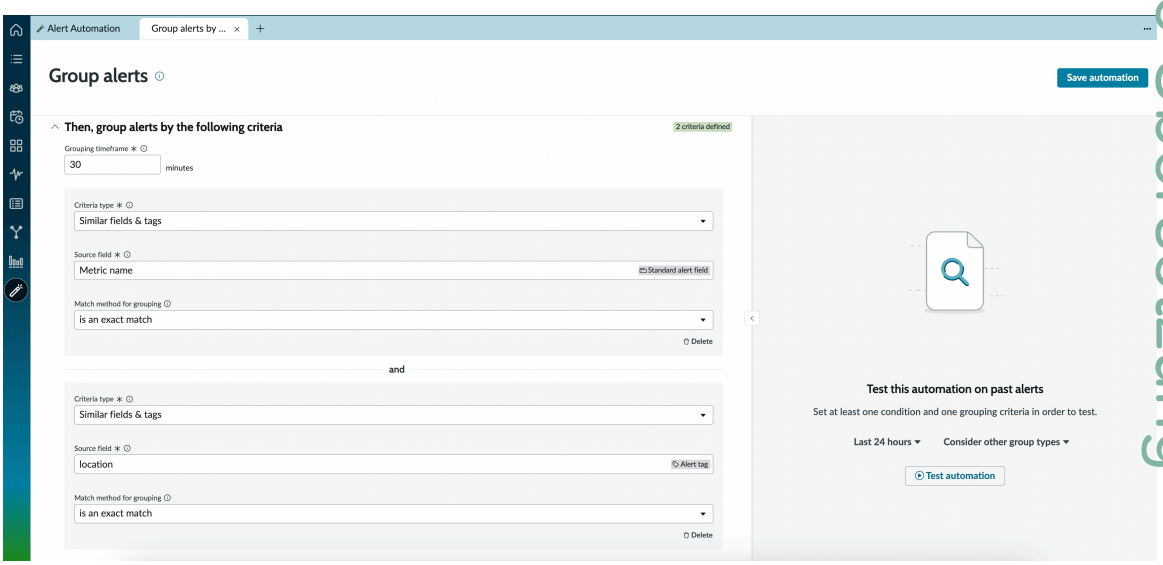
b. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit den Operatoren ODER oder UND hinzu. Sie müssen neben der Zuweisungsgruppe mindestens einen weiteren Filter hinzufügen.

Tipp: Wählen Sie einen spezifischeren Filter aus, um die Leistung zu verbessern.

Um einen weiteren Satz von Bedingungen hinzuzufügen, wählen Sie aus **+ neuer Bedingungssatz** . Sie können auch manuell ein Feld mit zusätzlichen Informationen hinzufügen, wenn es nicht in der Dropdown-Liste angezeigt wird.

Hinweis: Wählen Sie Aus **Laden Sie vergangene Ereignisse** Dient zum Anzeigen vorheriger Ereignisse beim Erstellen der Automatisierung.

7. In **Gruppieren Sie dann Warnungen nach den folgenden Kriterien** Führen Sie die folgenden Schritte aus.



a. In **Gruppierungszeitrahmen** Feld die Dauer (in Minuten) angeben, während der Warnungen gesammelt und gruppiert werden müssen.

b. In **Kriterientyp** Menü auswählen, wie Sie die Warnungen gruppieren möchten.

Derzeit gibt es zwei Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ähnliche Felder und Tags: Gruppieren Sie Warnungen nach ähnlichen Feldern und Tags.
- Zugehörige CIs: Gruppieren Sie Warnungen gemäß CI-Beziehungen (Konfigurationselement) (untergeordnete/übergeordnete/gleichgeordnete Elemente), Containment und anwendbaren Flows.

c. In **Quellfeld** Menü die Quelle auswählen, aus der die Warnungen gruppiert werden sollen.

> **Hinweis:** Sie können manuell einen Feldnamen hinzufügen und den Typ des Felds auswählen. Zu den verfügbaren Optionen gehören zusätzliches Informationsfeld, Warnungs-Tag und CI-Tag. Mit dieser Flexibilität können Sie die erfassten Informationen an Ihre spezifischen Anforderungen anpassen.

d. In **Übereinstimmungsmethode für Gruppierung** Wählen Sie eine der folgenden Optionen aus: Gruppieren Sie Warnungen basierend auf einer genauen Übereinstimmung, einer Fuzzy-Übereinstimmung oder einer Musterübereinstimmung.

Wenn Sie im Feld Gruppierung einen Wert für die Fuzzy-Übereinstimmungsmethode auswählen, wird die verwendet **Ähnlichkeitsschwellenwert (Prozentsatz)** Feld wird sichtbar. Warnungen werden gruppiert, wenn ihre Ähnlichkeit den angegebenen Prozentsatz basierend auf der Bearbeitungsentfernung größer oder gleich ist.

Wenn Sie beispielsweise Warnungen aus den USA, CA und den USA, NY haben und die Warnungen nach Ländern gruppieren möchten, legen Sie fest **Quelle** Feld in USA. Wenn **Übereinstimmungsmethode für Gruppierung** Ist eine Fuzzy-Übereinstimmung und der **Ähnlichkeitsschwellenwert (Prozentsatz)** Bei 50 % werden Warnungen gruppiert, wenn sie mindestens 50 % ähnlich sind, d. h., sie teilen das Land „USA“ als gemeinsames Attribut.

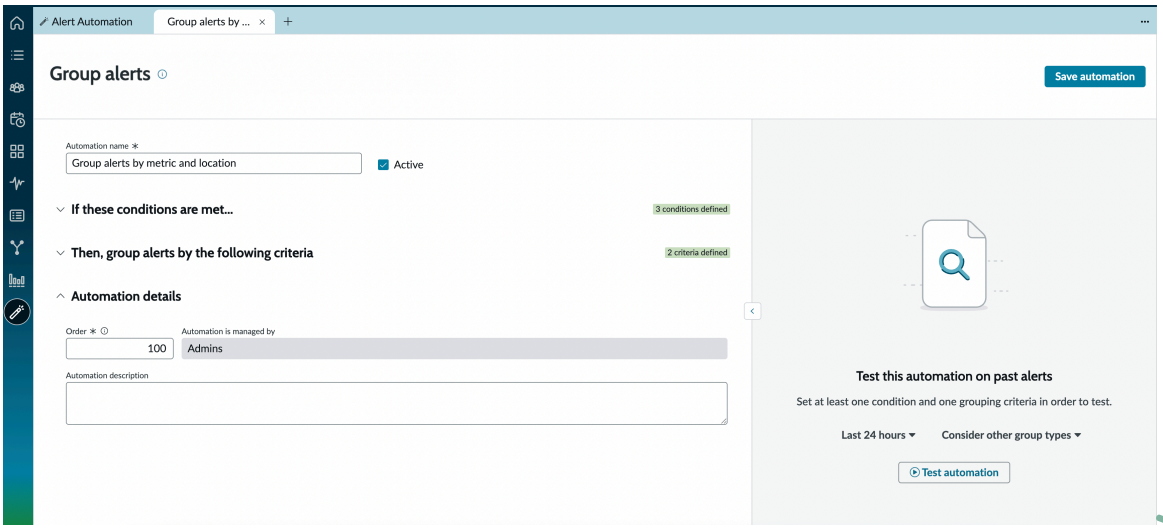
e. Wenn Sie im Feld Gruppierung einen Wert für die Musterübereinstimmungsmethode auswählen, wird der **Musterübereinstimmung** Feld wird sichtbar. Warnungen werden gruppiert, wenn das angegebene Muster übereinstimmt. Weitere Informationen finden Sie unter Musterabgleich .

Verwenden Sie Sternchen (*) in der Suchzeichenfolge, um eine beliebige Anzahl von Zeichen oder ein Fragezeichen (?) abzugleichen. Zum Abgleichen eines einzelnen Zeichens. Alles andere in der Suchzeichenfolge stimmt mit sich selbst überein. Verwenden Sie beispielsweise „HTTP-Fehler 5??“. Zum Abgleichen aller HTTP 500-Fehler.

Um zusätzliche Felder für die Gruppierung einzubeziehen, wählen Sie aus **+ Kriterien hinzufügen** .

8. In **Automatisierungsdetails** Geben Sie eine Beschreibung der Reihenfolge und Automatisierung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. In **Reihenfolge** Feld die Automatisierungsreihenfolge eingeben.

> **Hinweis:** Warnungen werden basierend auf der ersten Übereinstimmung gruppiert und in der Reihenfolge von der niedrigsten bis zur höchsten Zahl ausgeführt. Die **Automatisierung wird von verwaltet** Das Feld zeigt das Team oder die Zuweisungsgruppe an, die diese Automatisierung besitzt, bearbeitet und löschen kann. Die Zuweisungsgruppe ist mit der in definierten Gruppe identisch **Wenn diese Bedingungen erfüllt sind** Abschnitt.

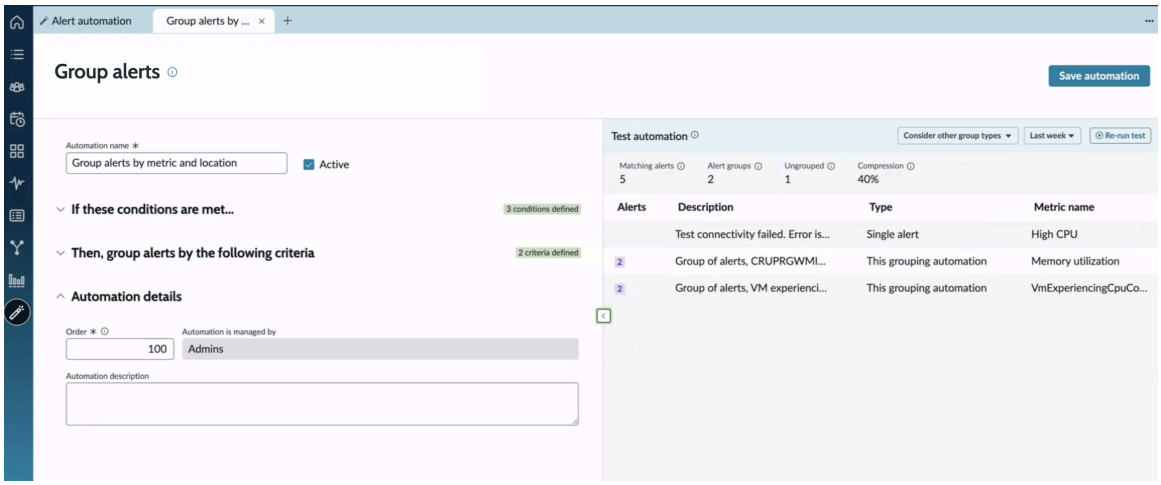
b. In **Automatisierungsbeschreibung** Geben Sie eine kurze Beschreibung der Automatisierung ein.

9. Um zu testen, ob die Warnungsgruppierung ordnungsgemäß funktioniert, navigieren Sie zu **Testen Sie diese Automatisierung für vergangene Warnungen** Wählen Sie in der Dropdown-Liste den Zeitrahmen für die Simulation aus, wählen Sie aus, ob Sie andere Gruppierungstypen berücksichtigen möchten, und wählen Sie dann aus **Automatisierung testen** .

> **Hinweis:** Von **Berücksichtigen Sie andere Gruppentypen** Menü können Sie entweder auswählen **Nur diese Automatisierung** Oder **Berücksichtigen Sie andere Gruppentypen** . Auswählen **Nur diese Automatisierung** Ignoriert andere Warnungsgruppentypen bei der Auswahl **Berücksichtigen Sie andere Gruppentypen** Enthält alle Automatisierungen der Warnungsgruppierung, z. B. tagbasierte, automatisierte, textbasierte und CMDB-basierte Warnungsgruppierung.

Während der Simulation werden sowohl die gruppierten Warnungen als auch die nicht gruppierten Warnungen für den angegebenen Zeitrahmen angezeigt. Wenn Warnungen gruppiert sind, wird die Anzahl der gruppierten Warnungen angezeigt. Sie können diese Zahl auswählen, um die gruppierten Warnungen anzuzeigen. Darüber hinaus werden bei Auswahl einer einzelnen Warnung die Details dieser spezifischen Warnung angezeigt. Sie können auch alle Warnungsgruppierungsbedingungen oder Feldwerte ändern und den Prozess erneut initiieren, indem Sie auswählen **Test erneut ausführen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Header des Abschnitts „Testautomatisierung“ zeigt auch Folgendes an: Übereinstimmende Warnungen, Warnungsgruppen, nicht gruppierte Warnungen und Komprimierung.

- **Übereinstimmende Warnungen** : Die Gesamtzahl der übereinstimmenden Warnungen vor der Gruppierung, die den für diese Automatisierung definierten Bedingungen entsprechen.
- **Warnungsgruppen** : Die Anzahl der Gruppen, die mehr als eine Warnung enthalten, die den Automatisierungsbedingungen entspricht. Die kleinere Zahl in Klammern stellt die Anzahl der von dieser Automatisierung erstellten Gruppen dar.
- **Gruppierung Aufgehoben** : Die Anzahl der Warnungen, die den Automatisierungsbedingungen entsprechen und nicht gruppiert bleiben.
- **Komprimierung** : Die prozentuale Reduzierung der Gesamtzahl der durch Gruppierung erzielten Warnungen, berechnet als 1 – (Warnungsgruppen + nicht gruppiert) / Gesamtzahl der Warnungen. Sie können die Komprimierungsrate verbessern, indem Sie Ihre Warnungen in zugehörige Probleme gruppieren. Die kleinere Zahl in Klammern gibt den Prozentsatz der übereinstimmenden Warnungen an, die durch diese Automatisierung komprimiert werden.
- Wenn der Kriterientyp ist **Zugehörige CIs** :
  - Die **Öffnen Sie die CIs-Abhängigkeitszuordnung** Der Link wird im Abschnitt „Testautomatisierung“ angezeigt.
  - Die **Konfigurationselement** Feld wird angezeigt.

Im Abschnitt „Testautomatisierung“ werden drei Schlüsselspalten angezeigt: **Beschreibung** , **Typ** , Und **Zeit** . Die **Beschreibung** Die Spalte enthält die Details der Warnungsgruppe. Vor **Beschreibung** Spalte, eine Zahl gibt die Gesamtzahl der Warnungen an, die in dieser Gruppe enthalten sind. **Typ** Gibt die Kategorie der Gruppierung an, z. B. diese Gruppierungsautomatisierung, andere Gruppierungsautomatisierung, CMDB-Gruppe oder einzelne Warnung usw. Auswählen **Andere Gruppierungsautomatisierung** Leitet Sie zur entsprechenden Automatisierungsseite weiter, die die Gruppe generiert hat. Darüber hinaus die **Zeit** Spalte zeigt an, wann der Test durchgeführt wurde.

Wichtig: Sie können die Simulation von Warnungen für Ihre Test- und Produktionsinstanz ausführen. Die Testautomatisierung simuliert die Automatisierung mit bis zu 200 aktuellen Warnungen, die den angegebenen Bedingungen entsprechen. Berücksichtigt nur Gruppen, bei denen alle Warnungen die Bedingungen für diese Automatisierung erfüllen, obwohl während der tatsächlichen Laufzeit zusätzliche Gruppierungsalgorithmen angewendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wählen Sie Aus **Automatisierung speichern** .
    Eine Benachrichtigung wird angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Gruppenautomatisierung wird auf der Seite „Gruppenwarnungen“ angezeigt, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

Nächste Maßnahme

Sie können Warnungen eskalieren, die schnellere Antworten von Teams oder Einzelpersonen benötigen, indem Sie implementieren Reagieren Sie auf Automatisierung .

Erstellen Sie die Antwortautomatisierung

Reagieren Sie automatisch auf Warnungen, indem Sie die entsprechenden Stakeholder benachrichtigen, sie je nach Schweregrad und Typ eskalieren oder andere Antwortaktionen ausführen. Dieser Prozess stellt sicher, dass Warnungen schnell und effektiv verwaltet werden.

Vorbereitungen

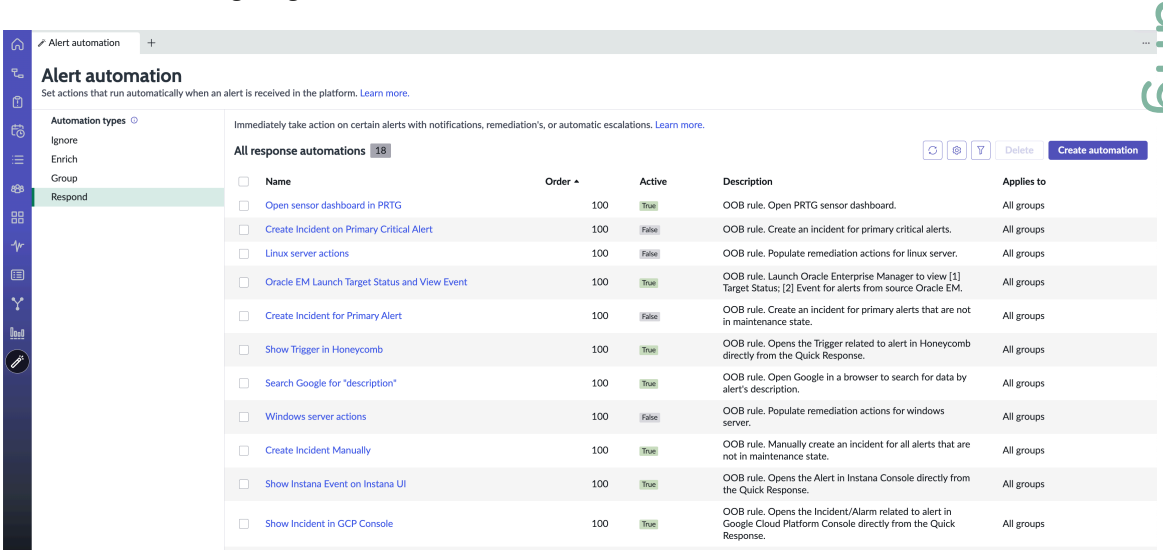
Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

Warum und wann dieser Vorgang ausgeführt wird

Für Anwender, die mit dem Klassiker vertraut sind Ereignismanagement Experience bietet dies eine einfache Schnittstelle mit erweiterter Teamunterstützung zum Erstellen von Antwortautomatisierungen oder Warnungsverwaltungsregeln. Warnungsverwaltungsregeln oder Antwortautomatisierungen sind konfigurierbare automatisierte Aktionen, die als Reaktion auf Warnungen ausgelöst werden, die bestimmten Bedingungen entsprechen und IT-Teams helfen, Probleme schneller und mit minimalem manuellem Aufwand zu lösen. Diese erweiterten Funktionen sind derzeit nur für Administratoren und andere Personas verfügbar, die im Abschnitt „erforderliche Rolle“ erwähnt werden.

Prozedur

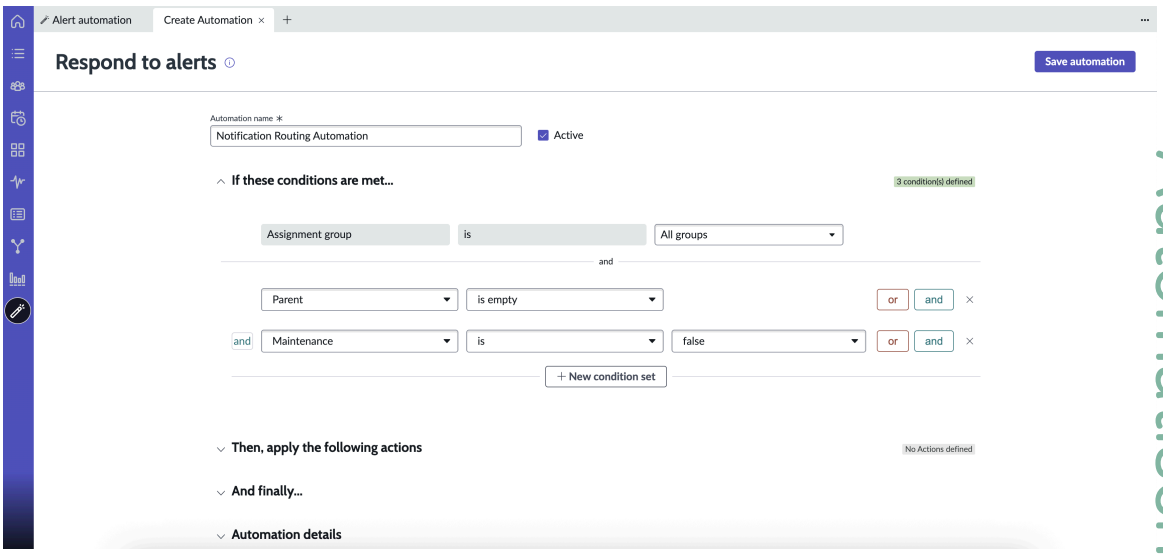
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Warnungsautomatisierung ( ).
3. Wählen Sie auf der Seite Warnungsautomatisierungen die Option aus **Antworten Sie** .
4. Wählen Sie Aus **Automatisierung erstellen** .
   Die Seite Antworten wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In **Automatisierungsname** Feld den Namen der Automatisierung eingeben.
   Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert.
6. In **Wenn diese Bedingungen erfüllt sind** Erstellen Sie Filterkriterien, um die Warnungen zu identifizieren, die Sie erfassen möchten.

> **Wichtig:** Sie können Antwortautomatisierungen auf primäre Warnungen beschränken, um zu verhindern, dass sekundäre Warnungen von unnötigem Rauschen überfordert werden. Stellen Sie sicher, dass diese Automatisierungen nur auf Warnungen angewendet werden, die CIs zugeordnet sind, die derzeit nicht gewartet werden.



a. Von **Zuweisungsgruppe** Feldmenü die Zuweisungsgruppe auswählen, um zu bestimmen, welche Warnungen des Teams die Automatisierung auslösen.

   Die **Zuweisungsgruppe** Stellt ein bestimmtes Team dar, das für die Verarbeitung bestimmter Warnungen verantwortlich ist. Durch Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung gezielt und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

   Hinweis:

   - Wenn Sie mit einer Administratorrolle (evt_mgmt_admin) bei der Instanz angemeldet sind, sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie auswählen **Alle Gruppen** Um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
   - Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
   - Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

b. Für **Übergeordnet** Feldwert: Wählen Sie aus, ob die Warnung, für die Sie eine Antwort erhalten möchten, unter einer übergeordneten Warnung gruppiert ist.

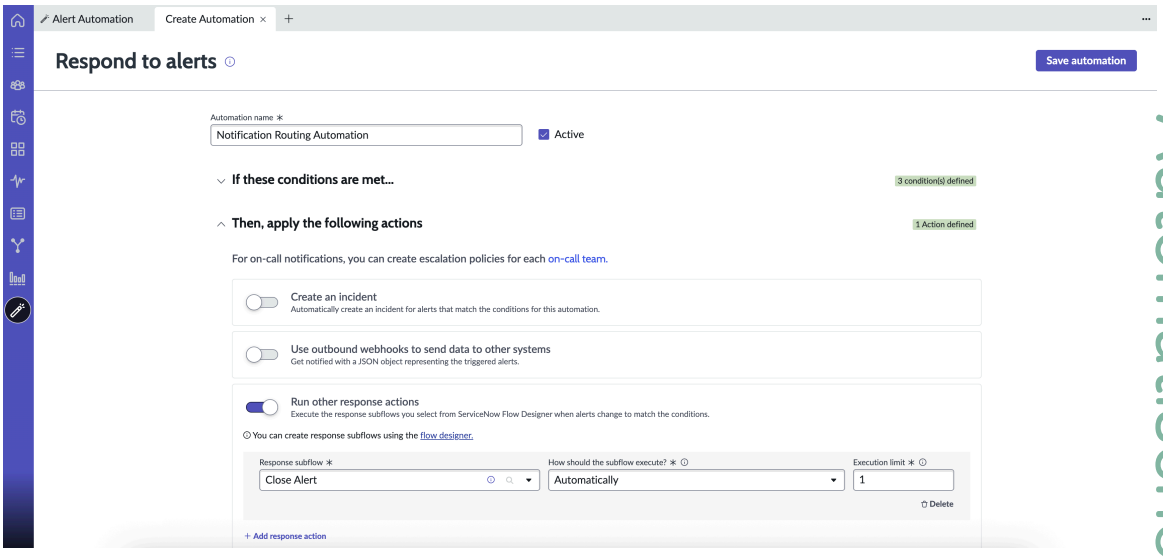
c. Für **Wartung** Feldwert: Wählen Sie aus, ob die Warnung, für die Sie eine Antwort erhalten möchten, gewartet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Um einen weiteren Satz von Bedingungen hinzuzufügen, wählen Sie aus **+ neuer Bedingungssatz** . Sie können auch manuell ein Feld mit zusätzlichen Informationen hinzufügen, wenn es nicht in der Dropdown-Liste angezeigt wird.

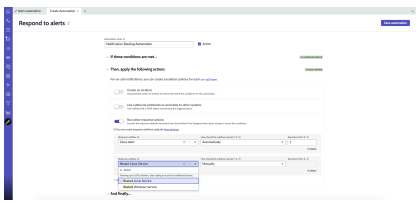
Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit den Operatoren ODER oder UND hinzu.

7. In **Wenden Sie dann die folgenden Aktionen an** Wählen Sie mindestens eine der drei Automatisierungsaktionen aus, die von der Automatisierung ausgelöst werden können.

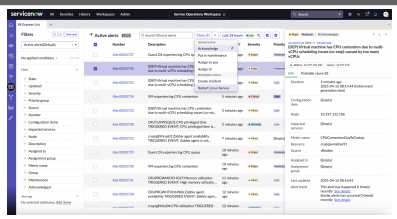


Aktion	Beschreibung
Incident erstellen	Erstellt einen Incident für die Warnungen, die dem angegebenen Filter entsprechen. Details zum Zuordnen der Warnungsfelder zu den Incident-Feldern finden Sie unter Warnungsfeldzuordnung auf der Antwortseite. Um zusätzliche Felder in den Incident einzubeziehen, wählen Sie aus **+ Hinzufügen** .
Ausgehende Webhooks verwenden, um Daten an andere Systeme zu senden	Sendet Benachrichtigungen über ausgehende Webhooks an andere Systeme. Diese Fähigkeit kann beispielsweise verwendet werden, um eine Chat-Benachrichtigung zu senden, einen Fall zu erstellen oder ein externes Runbook auszulösen, um das Problem zu beheben. Weitere Informationen zum Konfigurieren eines ausgehenden Webhooks finden Sie unter Parameter für ausgehenden Webhook. Um eine zusätzliche Eigenschaft zu erstellen, wählen Sie aus **+ Eigenschaft hinzufügen** . Die Eigenschaft kann ein beliebiges

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

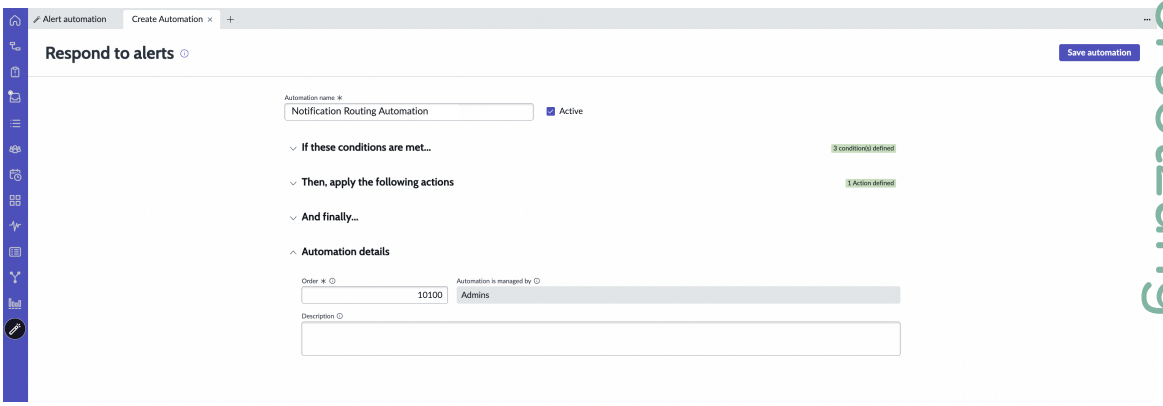
Aktion	Beschreibung
	anwenderdefiniertes Schlüssel-Wert-Paar sein, das Sie in die Webhook-Nutzlast aufnehmen möchten, z. B. „Inhaltstyp: Anwendung/JSON“ oder „Autorisierung: Bearer-<token>“.
Andere Antwortaktionen ausführen	Führt ausgewählte Subflows aus aus Workflow-Studio Für Warnungen, die der angegebenen Bedingung entsprechen. Sie können beispielsweise auswählen Sofort einsatzbereite Subflows Um Services neu zu starten. Sie können auch eigene erstellen Anwenderdefinierte Subflows , Mit Hunderten von Integrationen, die in Integration Hub verfügbar sind.  **a.** In **Antwort-Subflow** Wählen Sie den Subflow aus. Klicken auf das Informationssymbol (ⓘ) Führt Sie zum Workflow des Subflows. Wenn Sie beispielsweise auf das Informationssymbol (ⓘ) Neben „Warnung schließen“ wird der Workflow „Warnung schließen“ geöffnet. **Schließen Sie den Warnungs-Workflow** **b.** In **Wie soll der Subflow ausgeführt werden?** Feld auswählen **Automatisch** , **Manuell** Oder **Automatisch und manuell** . **Hinweis:** Wenn Sie einen Subflow mit dem Ausführungstyp auswählen **Manuell** Oder **Automatisch und manuell** , Und speichern Sie dann die Automatisierung, wird sie in angezeigt Express-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Beschreibung
	 **c.** In **Ausführungslimit** Feld angeben, wie oft der Subflow maximal ausgeführt werden kann. Nach Erreichen des Grenzwerts wird der Subflow nicht mehr ausgeführt. Um eine weitere Antwortaktion hinzuzufügen, wählen Sie aus **+ Antwortaktion hinzufügen** .

Hinweis: Wenn Sie nicht mindestens eine Aktion auswählen, wird die Automatisierung deaktiviert.

8. In **Und schließlich** Um nach der Ausführung dieser Automatisierung weitere Antwortautomatisierungen mit denselben Filterbedingungen auszuführen, wählen Sie aus **Führen Sie andere Antwortautomatisierungen aus** .
   Wenn Sie auswählen **Führen Sie keine Antwortautomatisierungen aus** , Zusätzliche Automatisierungen dieses Typs werden nicht mehr ausgeführt, nachdem diese Automatisierung einmal ausgeführt wurde. Wenn die Automatisierung von einem Administrator verwaltet wird, wird die Ausführung von Automatisierungen im Besitz des Administrators beendet, aber weiterhin Automatisierungen im Besitz anderer Zuweisungsgruppen ausgeführt.
9. In **Automatisierungsdetails** Geben Sie eine Beschreibung der Reihenfolge und Automatisierung an.



   Informationen zu den Feldern „Automatisierungsdetails“ finden Sie unter #unique_2206.
10. Wählen Sie Aus **Automatisierung speichern** .

    Eine Benachrichtigung wird angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt.

    Die von Ihnen erstellte Antwortautomatisierung wird auf der Seite „alle Antwortautomatisierungen“ angezeigt, auf der Sie die vorhandenen Automatisierungen anzeigen, bearbeiten oder löschen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Löschen Sie eine Automatisierung

Löschen Sie eine Automatisierung, um eine automatisierte Warnungsverarbeitungsregel dauerhaft aus Ihrem System zu entfernen.

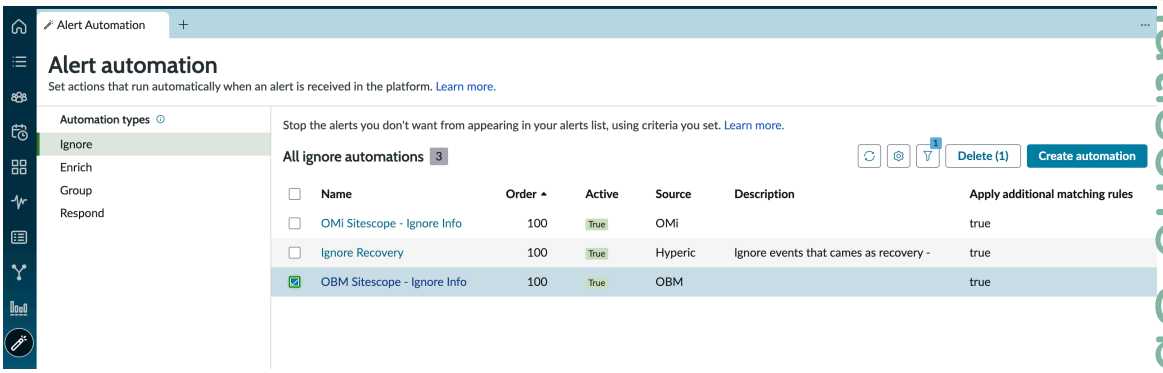
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_Team_Operator oder srm_Responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der primären Navigation das Symbol Warnungsautomatisierung ( ).
3. Auf der Seite Warnungsautomatisierung unter **Automatisierungstypen** , Wählen Sie den Automatisierungstyp aus, den Sie löschen möchten, z. B. Ignorieren, Anreichern, Gruppe oder Antworten.

   Die Seite für diesen Automatisierungstyp wird geöffnet und zeigt alle vorhandenen Automatisierungen an.
4. Um eine Automatisierung zu löschen, aktivieren Sie das Kontrollkästchen neben ihrem Namen, und wählen Sie dann aus **Löschen** .



5. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die Warnung wird endgültig gelöscht.

AIOps-Dashboards in Service Operations-Arbeitsbereich Für ITOM

Die AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten. Sie können Leistungskennzahlen (Key Performance Indicators, KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontexte für die IT-Umgebung insgesamt gewinnen. Diese Dashboards bieten umsetzbare Einblicke, die proaktive Antworten auf potenzielle Probleme erleichtern.

Wichtige Vorteile der Verwendung der AIOps-Dashboards:

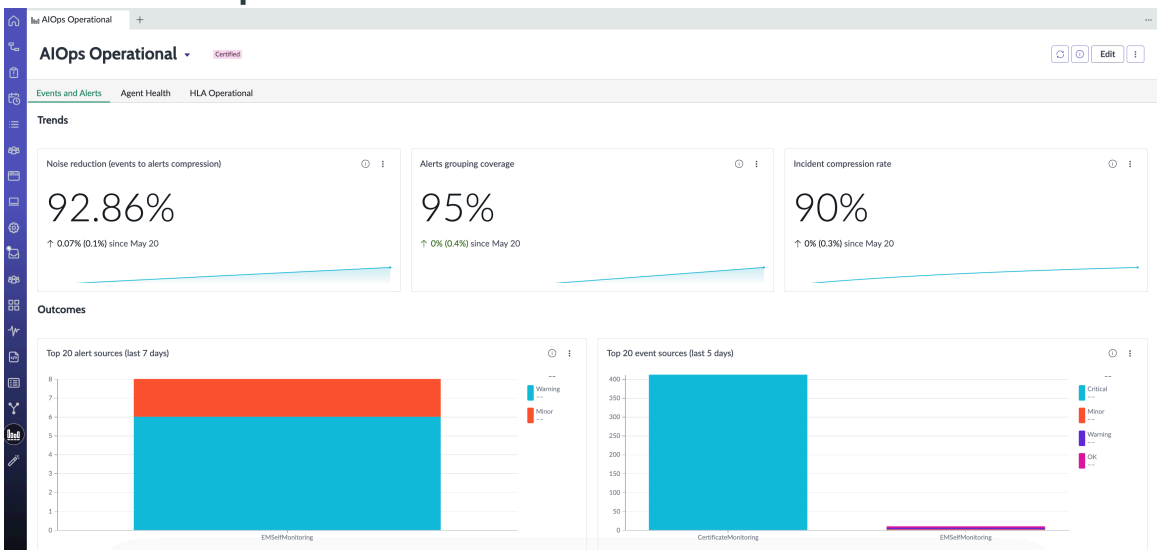
- Konfigurieren Sie die Dashboards, um sich auf die Metriken und Daten zu konzentrieren, die für Ihre Rolle am relevantesten sind.
- Profitieren Sie von interaktiven visuellen Darstellungen kritischer Betriebsdaten.
- Überwachen Sie KPIs, Serviceintegritätsmetriken und andere wichtige Leistungsdaten auf einen Blick.
- Nutzen Sie aus der Datenanalyse abgeleitete umsetzbare Einblicke für eine bessere Entscheidungsfindung.

Hinweis: Wenn Sie eine Reihe von Dashboards öffnen, wird das zuletzt aufgerufene Dashboard in dieser Kategorie angezeigt.

Automatische Übersetzung

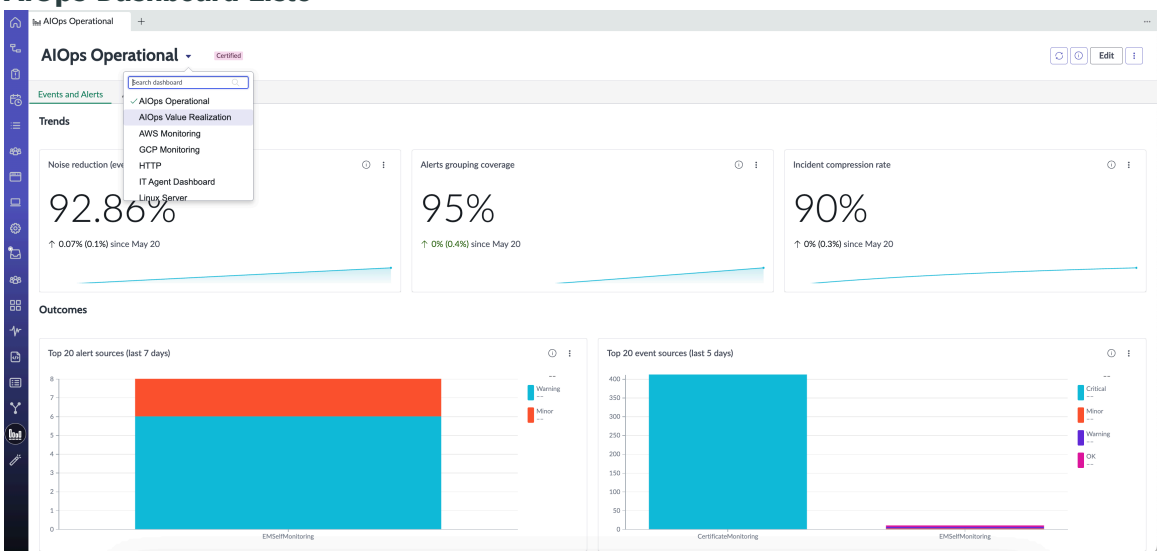
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Startseite des AIOps-Dashboards



Um operative AIOps-Dashboards anzuzeigen, z. B. die AIOps-Wertrealisierung, wählen Sie die Liste „AIOps operativ“ und dann den Namen des Dashboards aus.

AIOps-Dashboard-Liste



AIOps 360-Übersichts-Dashboard

Das AIOps 360-Übersichts-Dashboard bietet eine einheitliche Ansicht von Wert und Leistung im gesamten IT-Betrieb, sodass Teams die Effizienz nachverfolgen, die Warnungsverarbeitung überwachen und Automatisierungsergebnisse bewerten können. Es verbessert die Transparenz in AIOps-Auswirkungen, unterstützt fundierte Entscheidungen und fördert schnellere, intelligentere Vorgänge.

Voraussetzungen

Stellen Sie sicher, dass Ereignismanagement Anwendung ist installiert.

Erforderliche ServiceNow AI Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Greifen Sie auf das AIOps 360-Übersichts-Dashboard zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ), dann von **AIOps betriebsbereit** Dropdown-Menü auswählen **AIOps 360-Übersicht** .

Aufgliederungen

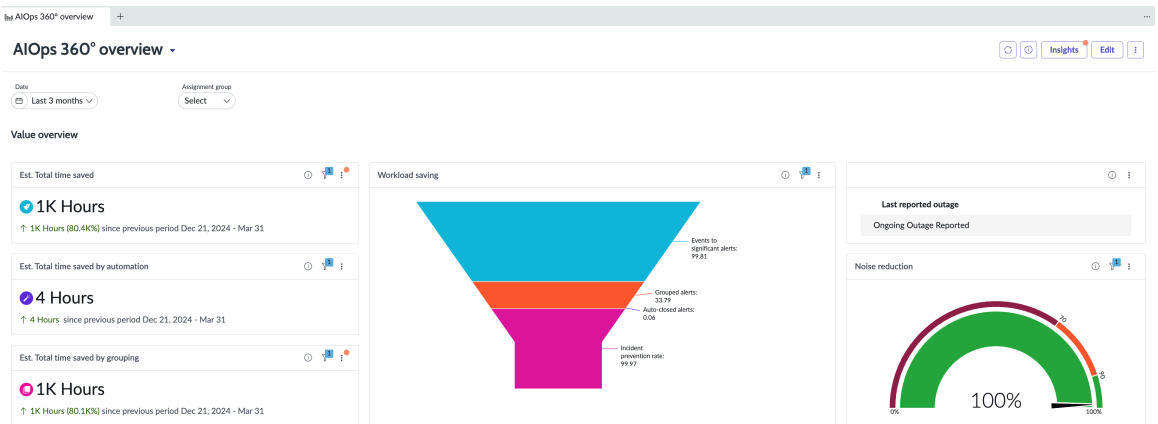
Im AIOps 360-Übersichts-Dashboard sind folgende Aufgliederungen verfügbar:

- Wertübersicht
- Leistungsübersicht

Abschnitt „Wertübersicht“

Verwenden Sie Filter wie **Datum** Und **Zuweisungsgruppe** Dient zum Anpassen der Dashboard-Ansicht und zum Fokussieren auf bestimmte Zeiträume und Teams. Dies hilft Ihnen, Trends zu erkennen, Bereiche mit Verbesserungspotenzial zu identifizieren und datengesteuerte Entscheidungen zu treffen, die auf Ihre betrieblichen Anforderungen zugeschnitten sind.

Im Abschnitt „Wertübersicht“ werden die Gesamtauswirkungen von AIOps auf die betriebliche Effizienz hervorgehoben. Es zeigt, wie viel manueller Aufwand durch Automatisierung und intelligente Warnungsgruppierung reduziert wurde. Sie spiegelt auch den Grad der Geräuschreduzierung, den Ausfallverlauf und die Gesamteinsparungen bei der Arbeitsauslastung wider und vermittelt ein klares Bild der realisierten Zeit- und Kostenvorteile.



Metriken	Beschreibung
Est. Zeitersparnis gesamt	Summe der Zeitersparnisse durch Warnungsautomatisierung und Warnungsgruppierung, berechnet in Stunden.
Est. Gesamtzeit durch Automatisierung eingespart	Zeitersparnis basierend auf der Anzahl der ausgeführten Warnungsautomatisierungsregeln multipliziert mit der durchschnittlichen Lösungszeit pro Warnung, berechnet in Stunden. Die durchschnittliche Lösungszeit kann von Administratoren in angepasst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Beschreibung
	werden **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an. Verwenden Sie *sn_aiops_dashboard.ITOM.Dashboard.Avg_time_saved_* zum Abrufen der tatsächlichen durch die Automatisierung eingesparten Zeit in Minuten, wie vom Indikator „Automatisierungszeit gespeichert“ verwendet. Standardmäßig ist sie auf 5 Minuten festgelegt.
Est. Gesamtzeit durch Gruppierung eingespart	Zeitersparnis basierend auf der Anzahl der gruppierten Warnungen vs. Der Zeit, die für die individuelle Selektierung jeder Warnung erforderlich ist, berechnet in Stunden. Die durchschnittliche Lösungszeit kann von Administratoren in angepasst werden **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an. Verwenden Sie *sn_aiops_dashboard.ITOM.Dashboard.MTTR_for_time_s* zum Definieren der MTTR (in Minuten), die bei der Berechnung der Zeitersparnis für die Warnungsgruppierung verwendet wird. Standardmäßig ist sie auf 5 Minuten festgelegt.
Arbeitsauslastungsspeicherung	Misst die Reduzierung des manuellen Aufwands durch Filtern, Gruppieren, Automatisieren von Warnungsabschlüssen und verhindern von Incident-Eskalationen. • Ereignisse zu signifikanten Warnungen: Prozentsatz der Ereignisse, die herausgefiltert und nicht in Warnungen konvertiert wurden, reduziert durch AIOps-Einstellungen wie Automatisierungen ignorieren. • Gruppierte Warnungen: Prozentuale Reduzierung der Anzahl eigenständiger Warnungen aufgrund von Gruppierungsregeln, die in Automatisierungen der Warnungsgruppierung definiert sind. • Automatisch geschlossene Warnungen: Prozentsatz der Warnungen, die automatisch durch Antwortautomatisierung, Aktionen zum Löschen von Ereignissen oder als Teil der Warnungsgruppenlösung geschlossen wurden.

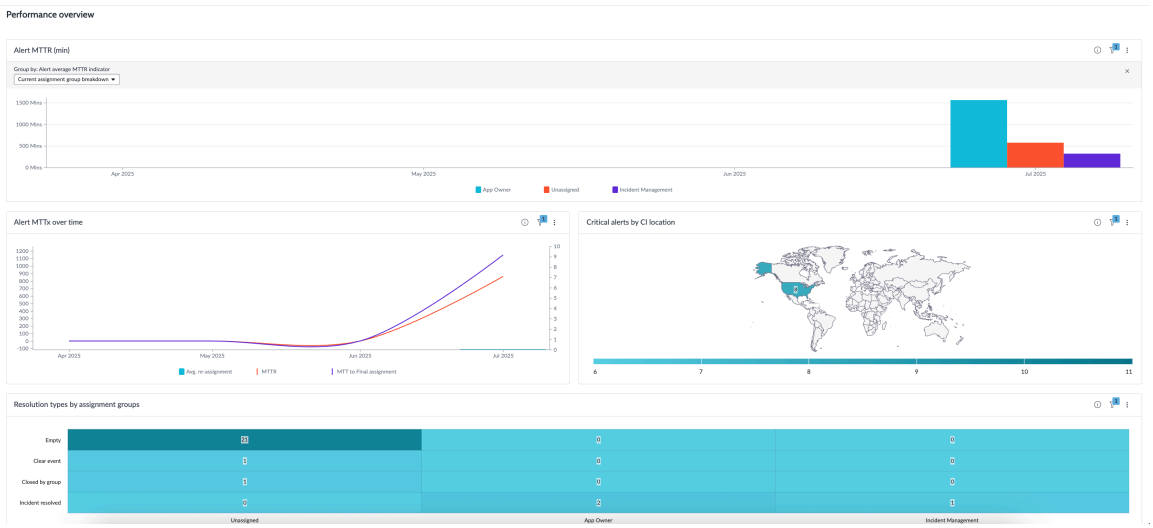
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Beschreibung
	• Incident-Präventionsrate: Prozentsatz der Warnungen, die erfolgreich gelöst wurden, ohne dass eine Eskalation zu Incidents erforderlich ist.
Letzter gemeldeter Ausfall	Letztes Datum eines schwerwiegenden Ausfalls (z. B. CMDB) Auswirkungen auf einen Service oder Server basierend auf gemeldeten Ausfällen für alle Klassen, die von cmdb_ci_Service oder cmdb_ci_Server geerbt wurden.
Rauschreduzierung	Prozentuale Effektivität beim Ignorieren doppelter und bedeutungsloser Ereignisse. Der typische Kundenwert überschreitet 90 %.

Abschnitt „Leistungsübersicht“

In diesem Abschnitt wird erläutert, wie effektiv Warnungen und Incidents behandelt werden. Sie umfasst Metriken wie Lösungszeiten über Gruppen hinweg, Trends bei Erkennung und Reaktion, Automatisierungsnutzung und Verteilung des Lösungsbesitzes. Es hilft, Leistungslücken zu identifizieren, Verbesserungen nachzuverfolgen und Reaktionsstrategien im gesamten Unternehmen zu optimieren.



Metriken	Beschreibung
Warnungs-MTTR	Lösungszeit für Warnungen nach Zuweisungsgruppe, um langsamere Teams zu identifizieren und SLAs durchzusetzen. Kann auch über das Dropdown-Menü Gruppierung nach Schweregrad gruppiert werden.
Warnungs-MTTx im Laufe der Zeit	MTTR (Durchschnittliche Zeit bis zur Lösung), MTTA (Durchschnittliche Zeit bis zur endgültigen Gruppenzuweisung) und durchschnittliche Anzahl von Gruppenneuzuweisungen, die im Laufe der Zeit nachverfolgt werden. Gibt die Effizienz der Zuweisung und die Fähigkeit an, Warnungen innerhalb einer einzelnen Gruppe zu lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Beschreibung
Kritische Warnung nach CI-Standort	Kritische Warnungen auf einer geografischen Karte basierend auf dem physischen oder logischen Standort von Configuration Items (CIs). Hilft, wiederkehrende Hotspots für retrospektive Analysen zu identifizieren und regionale Trends zu erkennen.
Lösungstypen nach Zuweisungsgruppen	Abschlussgründe durch Top-Zuweisungsgruppen, Hervorhebung von Automatisierungsabschlüssen (innerhalb von 10 Minuten nach der Ausführung), um eine schnelle Lösung zu fördern, und Zeitschwellenwertabschlüsse (nach dem Intervall für automatisches Schließen), die auf unbeaufsichtigte Warnungen hinweisen. Berücksichtigen Sie die Anzahl der Warnungen, die automatisch geschlossen werden, wenn sie ihre Zeitgrenze erreichen. Diese Zahl kann zeigen, ob Ihr Team nicht in der Lage ist, alle Warnungen zu lösen oder zu schließen, sodass einige nicht behandelt werden.

Hinweis: Wenn Sie mit beginnen Zurich, Einige Diagramme, Diagramme oder Metriken im Dashboard werden möglicherweise leer oder nur begrenzte Daten angezeigt. Dies wird erwartet, wenn keine Verlaufsdaten oder nur einige Wochen oder Monate Daten verfügbar sind. Während Ihr System weiterhin Warnungen sammelt und verarbeitet, wird das Dashboard im Laufe der Zeit mit umfassenderen Einblicken gefüllt.

Informationen zur Trichtervisualisierung finden Sie unter Erstellen Sie eine Trichtervisualisierung.

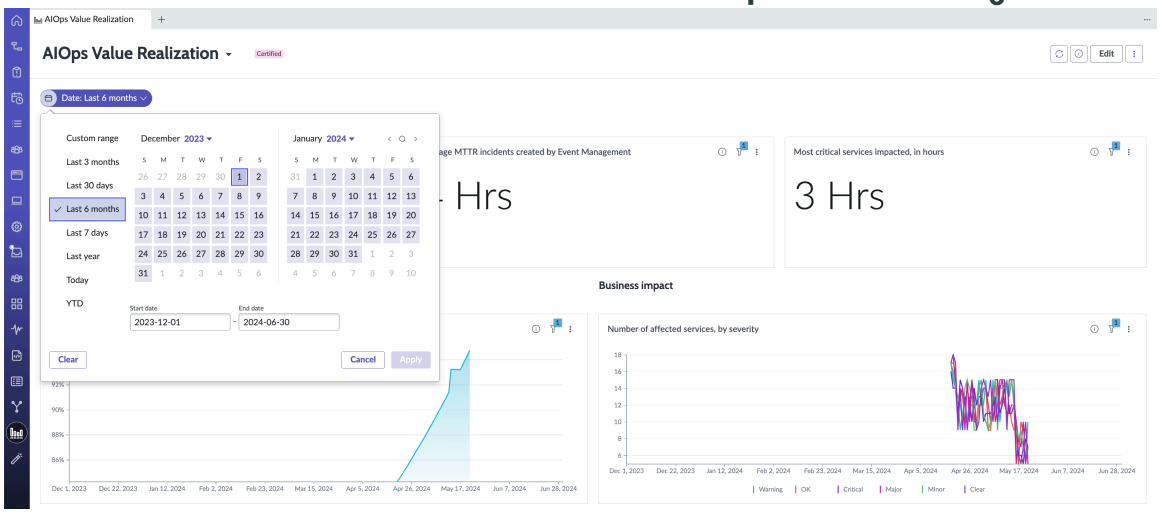
Dashboard für AIOps-Wertrealisierung

Das Dashboard „AIOps-Wertrealisierung“ verwendet Performance Analytics Bietet umfassenden Einblick in die Geschäftsergebnisse von Warnungen, Ereignissen und Incidents. Es enthält Metriken wie die Reduzierung von Rauschen (Komprimierung von Ereignissen zu Warnungen), die durchschnittliche MTTR für Incidents, die vom Ereignismanagement erstellt wurden[var.event-mgmt], und die wichtigsten Services, die von Stunden betroffen sind.

Das Dashboard „AIOps-Wertrealisierung“ enthält eine Kalenderfunktion, mit der Anwender verschiedene Datumsbereiche auswählen können, z. B. anwenderdefinierte Daten, die letzten 3 Monate, die letzten 30 Tage, die letzten 6 Monate, die letzten 7 Tage, das letzte Jahr, heute und das Jahr bis heute (seit Jahresbeginn). Sie können ein anwenderdefiniertes Start- und Enddatum angeben und diese Auswahl anwenden, um Berichte speziell für den ausgewählten Datumsbereich anzuzeigen. Diese Funktion erleichtert eine maßgeschneiderte Analyse und Berichterstellung basierend auf bestimmten Zeiträumen des Interesses.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswahl des Datumsbereichs des Dashboards für die AIOps-Wertrealisierung

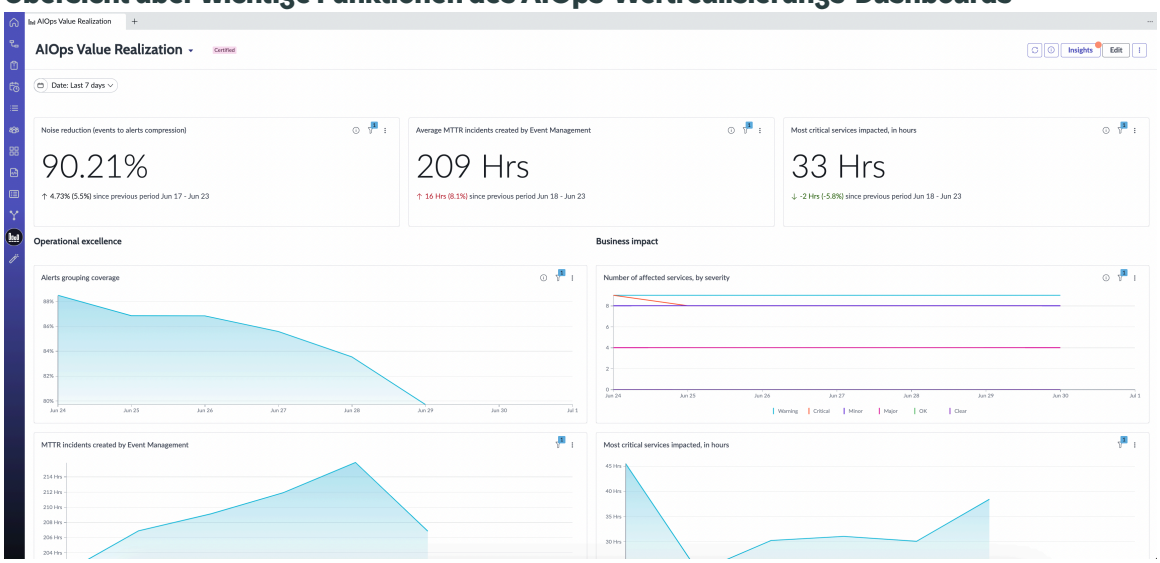


Das Dashboard „AIOps-Wertrealisierung“ bietet wichtige Einblicke und Metriken, die für die betriebliche Effizienz und die Bewertung der Geschäftsauswirkungen von entscheidender Bedeutung sind. Es umfasst Funktionen wie die Reduzierung von Rauschen, um die Konzentration auf kritische Probleme zu verbessern, indem die Konvertierungen von Ereignis zu Warnung reduziert werden. Die Nachverfolgung der durchschnittlichen MTTR für Incidents und die Messung von Ausfallzeiten bei kritischen Services tragen dazu bei, die betriebliche Effizienz zu verbessern und Lösungen zu priorisieren. Kategorisiert in die Abschnitte „operative Exzellenz“ und „Geschäftsauswirkung“ bietet das Dashboard detaillierte Abdeckung für die Gruppierung von Warnungen, die schnelle Lösung kritischer Incidents, die von Anwendern gemeldet werden, und die Quantifizierung der Serviceauswirkungen nach Schweregrad, um die Betriebsstabilität zu optimieren.

Führen Sie den Auftrag [PA EM] Verlaufsdatensammlung einmal aus, um die teilweise Erfassung von Verlaufsdaten zu aktivieren Ereignismanagement Daten:

1. Navigieren zu **Alle** > **Performance Analytics** > **Datenerfasser** > **Aufträge**an.
2. Wählen Sie [PA EM] Verlaufsdatensammlung aus.
3. Wählen Sie **Jetzt ausführen**.

Übersicht über wichtige Funktionen des AIOps-Wertrealisierungs-Dashboards



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Stellen Sie sicher, dass Ereignismanagement Anwendung ist installiert.

Erforderliche ServiceNow AI Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf das Dashboard „AIOps-Wertrealisierung“ zu

Verwenden Sie zum Öffnen des Dashboards eine der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Wert** > **Wertrealisierung**an.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ), dann von **AIOps betriebsbereit** Dropdown-Menü auswählen **AIOps-Wertrealisierung** .

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
evt_mgmt_admin oder admin	Bearbeiten Sie das Dashboard, und gewähren Sie Ansichts- und Freigabeberechtigungen.
evt_mgmt_operator oder admin	Zeigen Sie das Dashboard an, und überprüfen Sie Datensatzdetails, um die Geschäftsauswirkungen von Warnungen, Ereignissen und Incidents zu visualisieren und nachzuverfolgen.

Aufgliederungen

Im Dashboard „AIOps-Wertrealisierung“ sind folgende Aufgliederungen verfügbar:

- Operative Exzellenz
- Geschäftsauswirkung

Berichte

Titel	Typ	Beschreibung
Reduzierung des Datenrauschens (Ereignisse zu Warnungskomprimierung)	Liniendiagramm	Die Komprimierungsrate von Ereignissen bis zur Warnungserstellung: Eine höhere Zahl gibt an, dass weniger Warnungen erstellt werden.
Durchschnittliche von erstellte MTTR-Incidents Ereignismanagement	Liniendiagramm	Die durchschnittliche durchschnittliche Zeit bis zur Reparatur (MTTR) eines von erstellten Incidents

Automatische Übersetzung

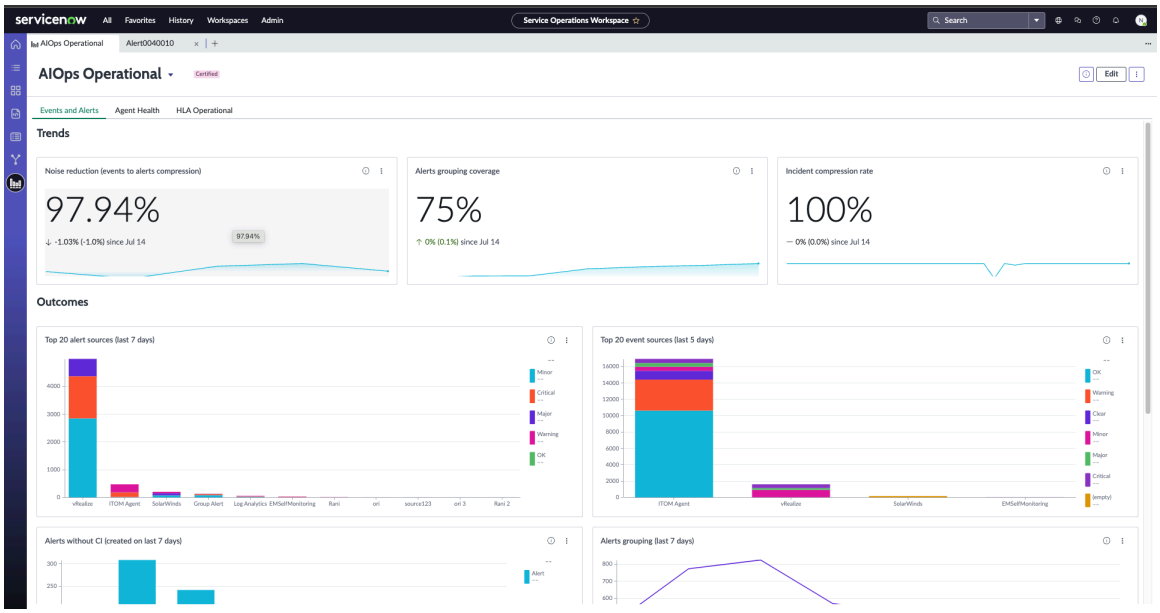
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		Ereignismanagement: Eine niedrigere Zahl zeigt eine höhere Effizienz Ihres IT-Teams an.
Die meisten betroffenen Services in Stunden	Liniendiagramm	Die Gesamtzeit, die die kritischsten Business-Services Ihrer Organisation betroffen sind: Eine höhere Zahl gibt an, dass mehr Zeit kritische Services von offenen Warnungen betroffen sind.
Warnungsgruppierungsabdeckung	Liniendiagramm	Der Prozentsatz der Gesamtzahl der gruppierten Warnungen: Eine höhere Zahl gibt an, dass weitere Warnungen innerhalb einer Warnungsgruppe korreliert und gruppiert werden.
Anzahl der betroffenen Services nach Schweregrad	Liniendiagramm	Die Anzahl der von Warnungen betroffenen Services, gruppiert nach Schweregrad, z. B. die Anzahl der Services, bei denen pro Tag kritische Probleme auftreten.
Anzahl der neuen P1-Incidents in überwachten Services, die von Anwendern erstellt wurden	Liniendiagramm	Die Anzahl der Incidents, die für von überwachte Services erstellt wurden Ereignismanagement: Eine niedrigere Zahl gibt an, dass weniger Anwender von einem Serviceausfall oder einer Verschlechterung der Leistung betroffen sind.

Ereignis- und Warnungs-Dashboard

Das Dashboard „Ereignis und Warnung“ verwendet Performance Analytics Um Echtzeiteinblick in Ereignisse und Warnungen in zu bieten Ereignismanagement, Zeigt wichtige Trends, Ergebnisse und die am stärksten betroffenen Konfigurationselemente. Es hebt Metriken wie die Reduzierung von Rauschen, die Abdeckung von Warnungsgruppierungen und die häufigsten Warnungsquellen hervor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Führen Sie den Auftrag [PA EM] Verlaufsdatensammlung einmal aus, um die teilweise Erfassung von Verlaufsdaten zu aktivieren Ereignismanagement Daten:

1. Navigieren zu **Alle** > **Performance Analytics** > **Datenerfasser** > **Aufträge**an.
2. Wählen Sie [PA EM] Verlaufsdatensammlung aus.
3. Wählen Sie **Jetzt ausführen**.

Voraussetzungen

Stellen Sie sicher, dass Ereignismanagement Anwendung ist installiert.

Erforderliche ServiceNow AI Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf zu Ereignisse und Warnungen Dashboard

Verwenden Sie zum Öffnen des Dashboards eine der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **Ereignisse und Warnungen**an.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ).

  Standardmäßig ist **Ereignisse und Warnungen** Registerkarte ist ausgewählt.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
evt_mgmt_admin oder admin	Bearbeiten Sie das Dashboard, und gewähren Sie Ansichts- und Freigabeberechtigungen.
evt_mgmt_operator oder admin	Zeigen Sie das Dashboard und die Details der darin enthaltenen Datensätze an, um Ereignisse, Warnungen, Trends, Ergebnisse und die am stärksten betroffenen Konfigurationselemente in Ihrer Organisation zu visualisieren und nachzuverfolgen.

Aufgliederungen

Im Dashboard „Ereignis und Warnung“ sind folgende Aufgliederungen verfügbar:

- Trends
- Ergebnisse

Berichte

Titel	Typ	Beschreibung
Reduzierung des Datenrauschens (Ereignisse zu Warnungskomprimierung)	Liniendiagramm	Die Komprimierungsrate von Ereignissen bis zur Warnungserstellung. Je höher die Zahl, desto weniger Warnungen werden erstellt.
Warnungsgruppierungsabdeckung	Liniendiagramm	Der Prozentsatz der Warnungen, die im Laufe der Zeit zu gruppierten Warnungen aggregiert wurden.
Incident-Komprimierungsrate	Liniendiagramm	Der Prozentsatz der aus Warnungen erstellten Incidents.
Top-20-Warnungsquellen (letzte 7 Tage)	Balkendiagramm	Die Anzahl der Warnungen pro Quelle, kategorisiert nach Schweregrad in den letzten 7 Tagen.
Top-20-Ereignisquellen (letzte 5 Tage)	Balkendiagramm	Die Anzahl der Ereignisse pro Quelle, kategorisiert nach Schweregrad in den letzten 5 Tagen.
Warnungen ohne CI (in den letzten 7 Tagen erstellt)	Liniendiagramm	Die Anzahl der Warnungen ohne CI-Bindung, die in den letzten 7 Tagen erstellt wurden.
Warnungsgruppierung (letzte 7 Tage)	Balkendiagramm	Die Verteilung der gruppierten Warnungen in den letzten 7 Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

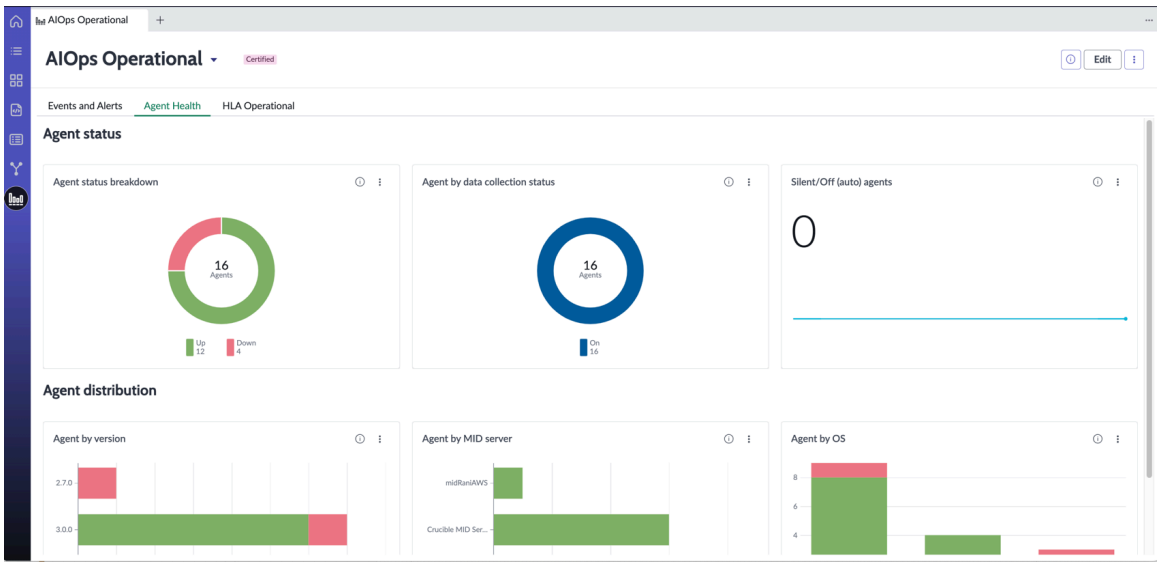
Am stärksten betroffene Konfigurationselemente

Der Abschnitt „Konfigurationselemente mit den meisten Auswirkungen“ im Dashboard „Ereignis und Warnung“ bietet einen umfassenden Überblick über die Konfigurationselemente (Configuration Items, CIs), die am stärksten von dem Problem betroffen sind. In diesem Abschnitt werden wichtige Details aufgelistet, z. B. der Name jedes CI, die Anzahl der zugehörigen Warnungen, ihre Klassifizierung (z. B. Anwendungsservice) und der Standort. Darüber hinaus werden der Besitzer und die Supportgruppe identifiziert, die für jedes CI verantwortlich sind, wodurch eine gezielte und effiziente Lösung von Incidents ermöglicht wird. Durch die Hervorhebung der am stärksten betroffenen CIs hilft dieser Abschnitt bei der Priorisierung kritischer Assets und Ressourcen und stellt sicher, dass die wichtigsten Probleme umgehend behoben werden, um die Systemstabilität und -Leistung zu gewährleisten.

Dashboard „Agent-Integrität“

Das Dashboard „Mitarbeiterintegrität“ bietet Einblick in den Status und die Verteilung der in Ihrem System installierten Service Desk-Mitarbeiter. Sie können damit schnell die Anzahl der bereitgestellten Service Desk-Mitarbeiter und ihre Verteilung bewerten, sodass Sie Ihre Arbeit effizienter priorisieren können.

Das folgende Beispiel zeigt die Service Desk-Mitarbeiter in Ihrem System, die derzeit aktiv sind, welche Service Desk-Mitarbeiter für die Erfassung von Daten konfiguriert sind und welche Service Desk-Mitarbeiter die Datenerfassung gestoppt haben, da sie ihren CPU-Schwellenwert (Silent/Off) erreicht haben. Außerdem werden die Service Desk-Mitarbeiter entsprechend ihrer Version, ihrem Betriebssystem und ihrer verbundenen Version angezeigt MID-Server.



Voraussetzungen

Die Anwendung Agent Client Collector muss installiert sein.

Erforderliche ServiceNow AI Platform-Rollen

Ein Anwender muss über die Rolle „Agent_Client_Collector_admin“ verfügen, um alle Widgets im Dashboard anzuzeigen.

Greifen Sie auf zu Ereignisse und Warnungen Dashboard

Verwenden Sie zum Öffnen des Dashboards eine der folgenden Methoden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **Agenten-Integrität**an.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ) Und dann auswählen **Service Desk-Mitarbeiter-Integrität** Registerkarte.
- Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (August 2024 Store), können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** Und verwenden Sie das erweiterte Dashboard.

Anwendungsfall

Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden, finden Sie im Anwendungsfall in der folgenden Tabelle.

Dashboard-Anwendungsfall

Anwender	Dashboard-Verwendung
Administrator	Transparenz des Status der Service Desk-Mitarbeiter.

Aufgliederungen

Folgende Aufgliederungen sind in der Agent-Integrität verfügbar:

- Agent-Status: Der Status der Service Desk-Mitarbeiter, die derzeit in Ihrem System bereitgestellt werden.
- Agent-Verteilung: Die Verteilung der Service Desk-Mitarbeiter nach Versionsnummer des Service Desk-Mitarbeiters MID-Server Dem der Service Desk-Mitarbeiter zugewiesen ist, und das Betriebssystem, an dem der Service Desk-Mitarbeiter arbeitet.

Berichte

Titel	Typ	Beschreibung
Aufgliederung des Agentenstatus	Kreisdiagramm	In Ihrem System bereitgestellte Agents, die aktiv und ausgefallen sind. Wählen Sie die entsprechende Farbe im Widget aus, um eine Liste der Service Desk-Mitarbeiter anzuzeigen.
Agent nach Status der Datensammlung	Kreisdiagramm	In Ihrem System bereitgestellte Agents mit aktivierter und deaktivierter Datensammlung. Wählen Sie die entsprechende Farbe im Widget aus, um eine Liste von Service Desk-Mitarbeitern mit aktivierter oder deaktivierter Datensammlung anzuzeigen.
Agenten stummschalten/ deaktivieren (automatisch)	Liniendiagramm	Service Desk-Mitarbeiter, die die Datenerfassung nach dem Überschreiten

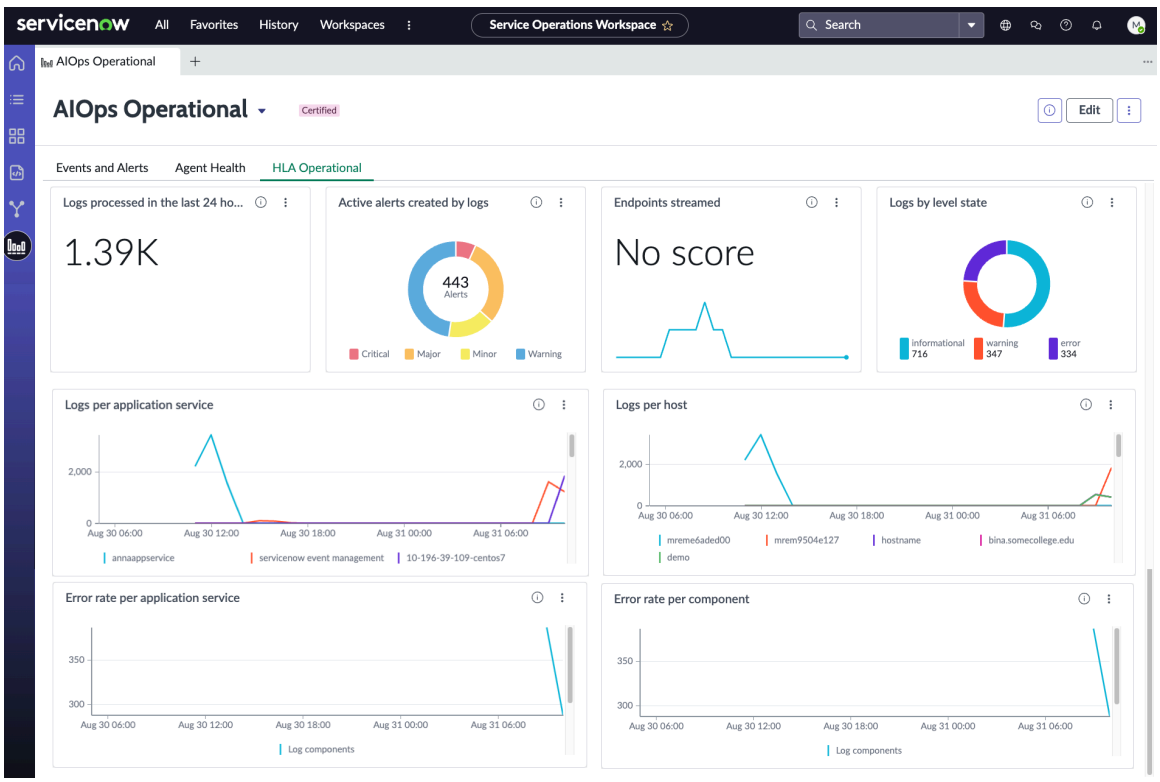
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		des Schwellenwerts für die CPU-Auslastung automatisch beendet haben. Der Schwellenwert für die CPU-Auslastung ist in konfigurierbar acc.yml Konfigurationsdatei. Weitere Informationen zu finden acc.yml Konfigurationsdatei, siehe Konfigurationsdateioptionen.
Agent nach Version	Balkendiagramm	Aufgliederung der bereitgestellten Agents nach Versionsnummern.
Service Desk-Mitarbeiter nach `MID-Server`	Balkendiagramm	Aufgliederung der bereitgestellten Agents gemäß `MID-Server`Sie sind zugewiesen.
Agent nach Betriebssystem	Balkendiagramm	Aufgliederung der bereitgestellten Agents nach den Betriebssystemen, an denen sie arbeiten.

Dashboard „HLA-Betrieb“

Die Health Log Analytics Wird für das operative Dashboard verwendet Performance Analytics Damit Sie Protokolldaten, Warnungen und Fehlerquoteninformationen in überwachen können Service Operations-Arbeitsbereich Und behandeln Probleme, wenn sie im System auftreten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Stellen Sie sicher, dass Health Log Analytics Anwendung ist installiert.

Erforderliche ServiceNow AI Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf das Dashboard „HLA-Betrieb“ zu

Verwenden Sie zum Öffnen des Dashboards eine der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **HLA – Operativ**an.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ), zeigen Sie dann das Dashboard „HLA-Betrieb“ an.

Anwendungsfälle

Die folgenden Anwendungsfälle veranschaulichen, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten.

Anwender	Dashboard-Verwendung
evt_mgmt_admin	Bearbeitet das Dashboard und erteilt Ansichts- und Freigabeberechtigungen
evt_mgmt_Operator oder evt_mgmt_admin	Überwacht das Dashboard, um HLA-Protokoll- und Warnungsdaten, Fehlerraten und andere relevante Informationen zu visualisieren und nachzuverfolgen.

Aufgliederungen

Im Dashboard „HLA-Betrieb“ sind folgende Aufgliederungen verfügbar:

- HLA-Übersicht
- Fehlerrate

Berichte

Titel	Typ	Beschreibung
Verarbeitete Protokolle	Balkendiagramm	Die Anzahl der Protokolle, die im ausgewählten Zeitraum verarbeitet und analysiert wurden. Standardmäßig visualisiert das Dashboard Protokolldaten, die in den letzten 24 Stunden erfasst wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
Von Protokollen erstellte aktive Warnungen	Tabelle	Detaillierte Daten zu allen derzeit aktiven Warnungen.
Endpunkte gestreamt	Liniendiagramm	Die Anzahl der Endpunkte (IPs, Netzwerke und Geräte), die in gestreamt werden Health Log Analytics, Nach Anwendungsservice.
Protokolle nach Ebenenstatus	Balkendiagramm	Der Schweregrad der Protokolle für die Streaming-Quellen.
Protokolle pro Anwendungsservice	Liniendiagramm	Die Anzahl der Protokolle, die für jeden Anwendungsservice im ausgewählten Zeitraum gestreamt wurden. Überwachen Sie diese Daten, um sicherzustellen, dass Protokolldaten wie erwartet für jeden Anwendungsservice gestreamt werden.
Protokolle pro Host	Liniendiagramm	Die Anzahl der verarbeiteten Protokolle für jeden Host im ausgewählten Zeitraum. Überwachen Sie diese Daten, um Hosts zu erkennen, die mehr oder weniger Daten als erwartet protokollieren.
Fehlerrate pro Anwendungsservice	Liniendiagramm	Die Anzahl der Protokolle mit Fehlern für jeden Anwendungsservice, der im ausgewählten Zeitraum analysiert wurde. Überwachen Sie diese Daten, um die Fehler weiter zu untersuchen. **Hinweis:** Health Log Analytics Erstellt automatisch Warnungen für Fehleranomalien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
Fehlerrate pro Komponente	Liniendiagramm	Die Anzahl der Protokolle mit Fehlern für jede Komponente, die im ausgewählten Zeitraum analysiert wurde. Überwachen Sie diese Daten, um sicherzustellen, dass die Fehlerquote für jede Komponente normal ist.

Datenvisualisierung in ITOM

Gewinnen Sie mit der Datenvisualisierung in IT Operations Management schneller Einblicke (ITOM). Visualisieren Sie Metriken, Protokolle, Ereignisse und Warnungen über intuitive Dashboards und Diagramme, um Trends zu identifizieren, die Leistung zu überwachen und Probleme proaktiv zu lösen.

Jeder mit Zugriff auf Daten kann eine Visualisierung dieser Daten in einem Dashboard erstellen, dessen Eigentümer er ist.

Erstellen Sie eine Trichtervisualisierung

Eine Trichtervisualisierung zeigt, wie Daten sequenzielle Phasen durchlaufen, und hilft Ihnen, Abgaben oder Engpässe bei jedem Schritt zu identifizieren. Verwenden Sie es, um Konvertierungen, Workflows oder Prozessabschlussraten nachzuverfolgen. Sie können einem vorhandenen Dashboard oder einem neuen Dashboard eine Trichtervisualisierung hinzufügen.

Vorbereitungen

Erforderliche Rolle: Report_user, admin oder VIZ_Creator

Stellen Sie sicher, dass Sie über eine Administratorrolle oder Berechtigung des Dashboard-Besitzers verfügen, um das Dashboard zu bearbeiten.

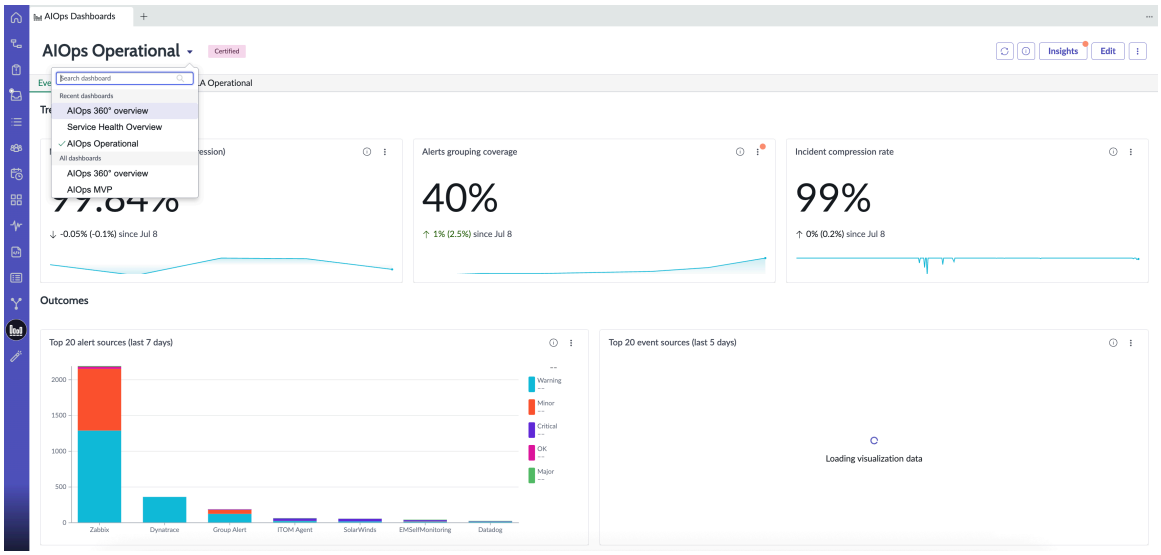
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie über die entsprechende Rolle verfügen, können Sie Trichterberichte in einem Dashboard hinzufügen und bearbeiten. Die **Bearbeiten** Die Schaltfläche ist in den ITOM-Dashboards nur verfügbar, wenn der Anwender zum Bearbeiten berechtigt ist. Weitere Informationen zum Erstellen von Dashboards finden Sie unter Allgemeine Dashboard-Aufgaben im Inline-Editor .

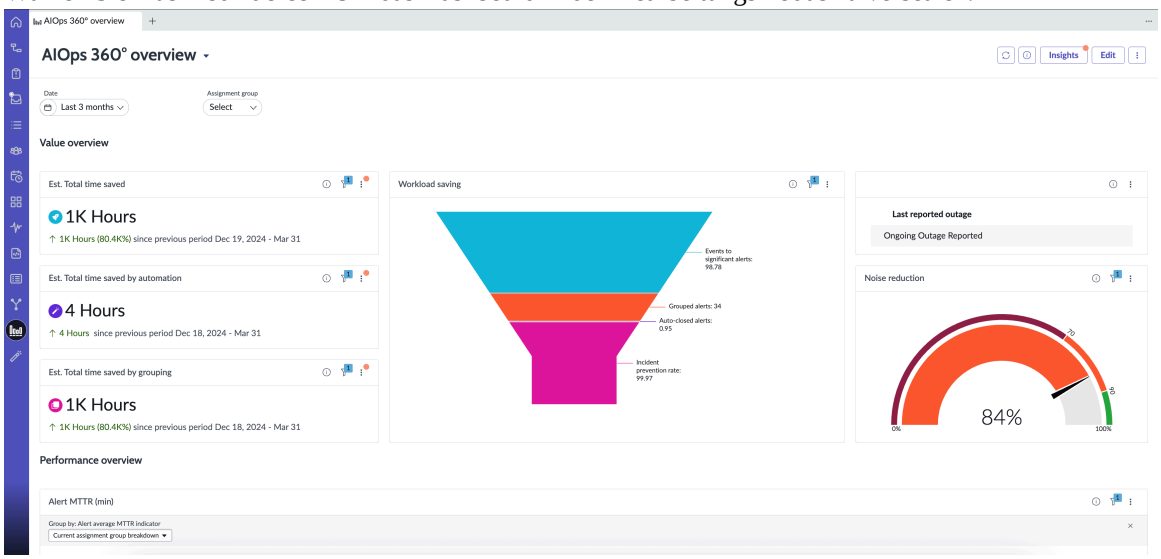
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Symbol AIOps-Dashboards ( ).
2. Wählen Sie in der Dashboard-Auswahl aus **AIOps 360-Übersicht** .

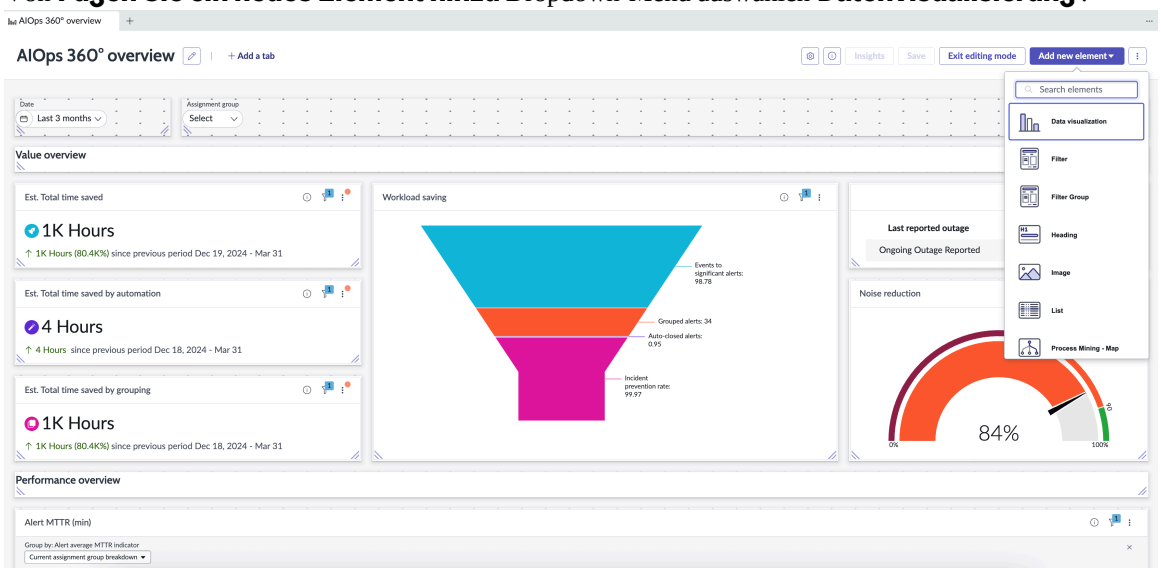
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie Aus **Bearbeiten** Um das Dashboard in den Bearbeitungsmodus zu versetzen.



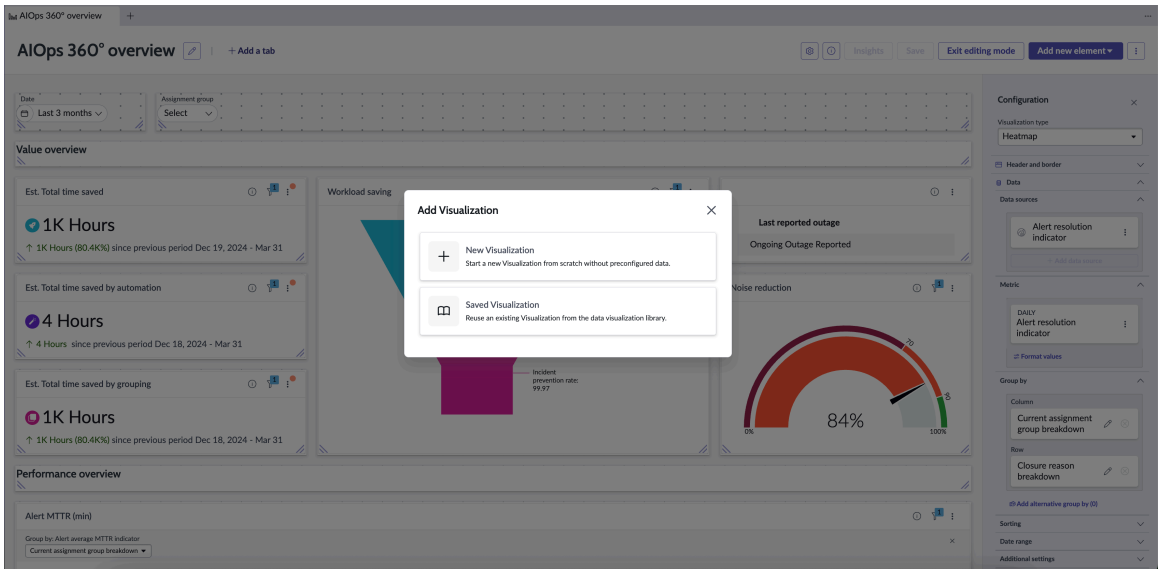
4. Von **Fügen Sie ein neues Element hinzu** Dropdown-Menü auswählen **Datenvisualisierung** .



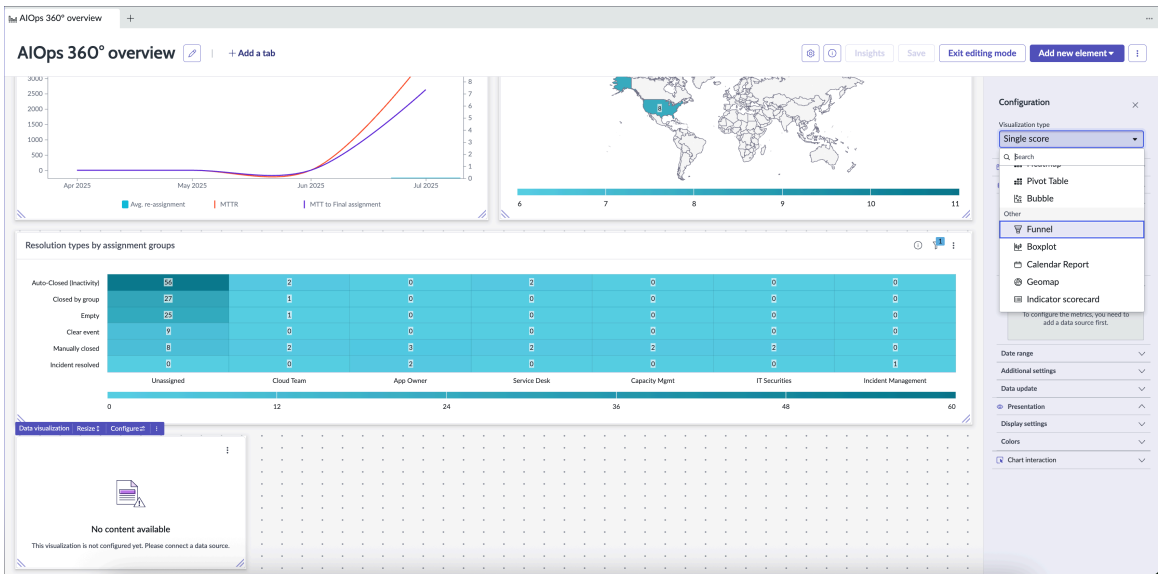
5. Wählen Sie im Fenster „Visualisierung hinzufügen“ die Option aus **Neue Visualisierung** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Von **Visualisierungstyp** Feld auswählen **Trichter** .



Hinweis: Die **Trichter** Der Visualisierungstyp ist derzeit nur für Kunden verfügbar, die über verfügen ITOM Plugin installiert.

7. Unter **Datenquellen** , Wählen Sie aus **+ Datenquelle hinzufügen** .
   Für stehen zwei Arten von Datenquellen zur Verfügung **Trichter** Visualisierungstyp: Tabelle und Indikator. Visualisierungen basierend auf Tabellendaten zeigen einen Snapshot des Status dieser Daten. Indikatorvisualisierungen spiegeln Daten im Zeitverlauf basierend auf Datensammlungsaufträgen wider. Sie können Trichterphasen mit Indikatoren auf eine der folgenden Arten konfigurieren:

   Sie können Trichterphasen mit Indikatoren auf eine der folgenden Arten konfigurieren:

   - Option 1: Verwenden Sie einen einzelnen Indikator oder eine einzelne Tabelle mit einer Aufgliederung

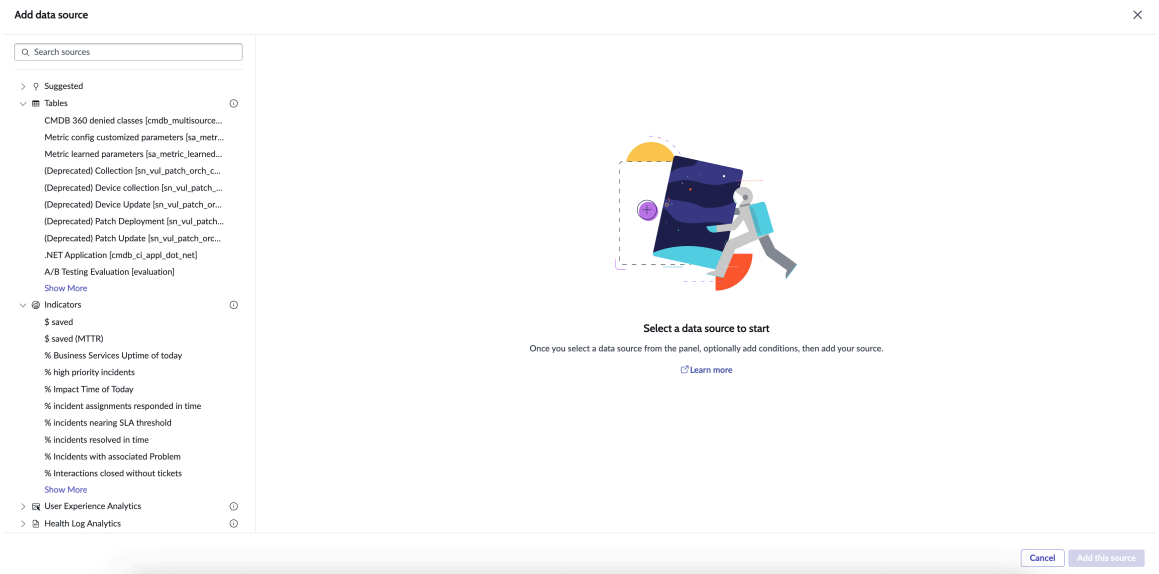
     Wählen Sie einen einzelnen Indikator oder eine einzelne Tabelle aus, und definieren Sie dann die Aufgliederung mithilfe des Felds Gruppieren nach. Die Aufgliederungswerte werden als Trichterphasen verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie nur einen Indikator ohne Aufgliederung auswählen, wird in der Visualisierung ein Fehler angezeigt: Ungültige Konfiguration. Ein Wert für „Gruppieren nach“ muss ausgewählt werden, damit die Visualisierung gerendert wird.

- Option 2: Mehrere Indikatoren ohne Aufgliederung verwenden

  Wählen Sie mehrere Indikatoren aus, ohne eine Aufgliederung festzulegen. In diesem Fall stellt der Wert jedes Indikators eine Phase im Trichter dar.



8. Wählen Sie die erforderliche Datenquelle aus, und wählen Sie aus **Fügen Sie diese Quelle hinzu** .

   Wenn Sie eine Tabellen- oder Indikatordatenquelle für eine Trichtervisualisierung auswählen, finden Sie in den folgenden Themen die verfügbaren Datenkonfigurationsoptionen:

   - Tabellendatenoptionen für Trichtervisualisierungen
   - Indikatordatenoptionen für Trichtervisualisierungen

9. Wählen Sie **Speichern**.

Tabellendatenoptionen für Trichtervisualisierungen

Wenn Sie eine Tabellendatenquelle für die Trichtervisualisierung auswählen, sind die folgenden Datenkonfigurationsoptionen verfügbar.

Datenkonfigurationsoptionen

Feld	Beschreibung
Vordefinierte Bedingungen	Voreingestellte Filter zur schnellen Eingrenzung von Daten basierend auf allgemeinen Kriterien.
+ anwenderdefinierte Bedingungen hinzufügen	Anwenderdefinierte Filter basierend auf anwenderdefinierten Kriterien.
Header und Rahmen	
Kopfzeile anzeigen	Der Visualisierungsheader, einschließlich Titel und Symbole.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenkonfigurationsoptionen (Fortsetzung)

Feld	Beschreibung
Header-Trennzeichen anzeigen	Option zum Anzeigen einer Zeile, die den Header vom Rest der Komponente trennt.
Diagrammtitel	Text, der als Titel des Diagramms angezeigt wird.
Beschreibung	Optionaler Erklärungstext, der unter dem Titel angezeigt wird.
Titel umbrechen	Option zum Umbrechen langer Titel in mehrere Zeilen.
Rand anzeigen	Option für die Einstellung der Rahmensichtbarkeit für den Widget-Container.
Header-Hintergrundfarbe	Einstellung der Hintergrundfarbe für den Headerbereich.
Daten	
Datenquellen	Verfügbare Eingaben, die der Visualisierung Daten liefern.
Metrik	
Bezeichnung	Anwenderdefinierter Name für die ausgewählte Metrik. Standardmäßig stimmt die Bezeichnung mit dem Datenquellennamen überein.
Eine Zusammenfassung auswählen	Zusammenfassungstyp, der auf die Metrik angewendet wird (z. B. Summe, Durchschnitt). Die Standardeinstellung ist Anzahl und zeigt die Anzahl der ausgewählten Datensätze an. **Hinweis:** Wählen Sie Aus **Eindeutige Anzahl** Dient zum Zählen nur eindeutiger Datensätze. Wenn Sie beispielsweise einen Bericht von Anwendern mit einer oder mehreren Rollen aus einer Liste generieren, zählen Sie jeden Anwender nur einmal. Ohne diese Option werden Anwender mit mehreren Rollen mehrmals gezählt.
Feld	Quellfeld aus dem Datensatz für die ausgewählte Metrik. **Hinweis:** Die Daten werden in einem Format angezeigt, das dem Feldtyp entspricht. Beispiel: Ein Ganzzahlfeld wie **Priorität** Wird als Zahl angezeigt. Ein Feld für die Dauer wie **Geschäftsdauer** Aus der Tabelle [Incident] wird in Tagen, Stunden und Minuten angezeigt. Wenn Funktionsfelder im Berichtsdesigner für die Tabelle erstellt wurden, sind sie in der Dropdown-Liste verfügbar. Weitere Informationen finden Sie unter Bericht zu Funktionsfeldern .
Werte formatieren	Formatierungsstil für die Anzeige von Metrikwerten. Wählen Sie diese Option aus, um das Dialogfeld Formatierungswerte zu öffnen. Weitere Informationen finden Sie unter Wertformatierung in Berichten .
Gruppe	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenkonfigurationsoptionen (Fortsetzung)

Feld	Beschreibung
Feld für Incident	Feld, das speziell zum Gruppieren von Incident-Daten verwendet wird.
Maximale Anzahl Gruppen	Beschränken Sie die Anzahl der in der Visualisierung angezeigten Gruppen.
Andere anzeigen	Option zum Gruppieren überschüssiger Daten in einem **Andere** Kategorie.
Datenaktualisierung	
Filter nachverfolgen	Folgt Filtern, die auf Seitenebene festgelegt sind. Wenn diese Option ausgewählt ist, spiegelt die Visualisierung Arbeitsbereichsfilter wider. Wenn diese Option nicht ausgewählt ist, ignoriert die Visualisierung alle Filter auf Seitenebene.
Filtersymbol anzeigen	Option zum Anzeigen des Filtersymbols und der Anzahl der Filter, die sich auf die Visualisierung auswirken. Wenn das Kontrollkästchen nicht aktiviert ist, werden das Symbol und die Filteranzahl ausgeblendet.
Aktualisieren Sie, nachdem Sie X Min. Abwesend waren	Auslöser basierend auf der Zeit außerhalb des Dashboards innerhalb desselben Arbeitsbereichs, einschließlich der Platform Analytics-Experience. Definiert die Anzahl der Minuten, nach denen die Visualisierung automatisch aktualisiert wird, wenn Sie zurückkehren. Verwechseln Sie diese Einstellung nicht mit **Geplante Wiederholung** In Inline-Dashboards, wodurch das gesamte Dashboard nur aktualisiert wird, solange es geöffnet bleibt.
Infonachrichten	
Anwenderdefinierte Nachricht festlegen, wenn keine Daten vorhanden	Anwenderdefinierter Text, der angezeigt wird, wenn keine Daten für die Visualisierung verfügbar sind.
Farben	
Farbtyp festlegen	Farbschema, das auf verschiedene Datenwerte oder -Bereiche angewendet wird.
Diagramminteraktion	Im Diagramm unterstützte Anwenderaktionen, z. B. Zeigen oder Auswählen.

Indikatordatenoptionen für Trichtervisualisierungen

Wenn Sie eine Indikatordatenquelle für die Trichtervisualisierung auswählen, sind die folgenden Datenkonfigurationsoptionen verfügbar.

Sie können entweder einen einzelnen Indikator auswählen und verwenden **Gruppieren nach** Feld zum Berechnen von Phasenwerten oder Auswählen mehrerer Indikatoren ohne Aufgliederung, wobei der Wert jedes Indikators eine Trichterphase darstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenkonfigurationsoptionen

Feld	Beschreibung
Aufgliederung	Bietet eine Möglichkeit, Daten mithilfe von Feldern wie Warnungsschweregrad oder Warnungsstatus zu segmentieren. Jede Bedingung enthält einen **Aufgliederung** Feld, ein **Operator** , Und **Element** Der den Zielwert definiert. Alle Bedingungen werden mit der Logik UND angewendet, d. h. Daten müssen jedes angegebene Kriterium erfüllen, um in die Visualisierung aufgenommen zu werden.
Header und Rahmen	
Kopfzeile anzeigen	Option für die Sichtbarkeitseinstellung für den Widget-Header.
Header-Trennzeichen anzeigen	Option zum Anzeigen einer Trennlinie unter dem Header.
Diagrammtitel	Text, der als Titel des Diagramms angezeigt wird.
Beschreibung	Optionaler Erklärungstext, der unter dem Titel angezeigt wird.
Titel umbrechen	Option zum Umbrechen langer Titel in mehrere Zeilen.
Rand anzeigen	Option für die Einstellung der Rahmensichtbarkeit für den Widget-Container.
Header-Hintergrundfarbe	Einstellung der Hintergrundfarbe für den Headerbereich.
Daten	
Datenquellen	Verfügbare Eingaben, die der Visualisierung Daten liefern.
Metrik	
Bezeichnung	Anwenderdefinierter Name für die ausgewählte Metrik. Standardmäßig stimmt die Bezeichnung mit dem Datenquellennamen überein.
Eine Zusammenfassung auswählen	Zusammenfassungstyp, der auf die Metrik angewendet wird (z. B. Summe, Durchschnitt). Die Standardeinstellung ist Anzahl und zeigt die Anzahl der ausgewählten Datensätze an. **Hinweis:** Wählen Sie Aus **Eindeutige Anzahl** Dient zum Zählen nur eindeutiger Datensätze. Wenn Sie beispielsweise einen Bericht von Anwendern mit einer oder mehreren Rollen aus einer Liste generieren, zählen Sie jeden Anwender nur einmal. Ohne diese Option werden Anwender mit mehreren Rollen mehrmals gezählt.
Feld	Quellfeld aus dem Datensatz für die ausgewählte Metrik. **Hinweis:** Die Daten werden in einem Format angezeigt, das dem Feldtyp entspricht. Beispiel: Ein Ganzzahlfeld wie **Priorität** Wird als Zahl angezeigt. Ein Feld für die Dauer wie **Geschäftsdauer** Aus der Tabelle [Incident] wird in Tagen, Stunden und Minuten angezeigt. Wenn Funktionsfelder im Berichtsdesigner für die Tabelle erstellt wurden, sind sie in der Dropdown-Liste

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenkonfigurationsoptionen (Fortsetzung)

Feld	Beschreibung
	verfügbar. Weitere Informationen finden Sie unter Bericht zu Funktionsfeldern .
Werte formatieren	Formatierungsstil für die Anzeige von Metrikwerten. Wählen Sie diese Option aus, um das Dialogfeld Formatierungswerte zu öffnen. Weitere Informationen finden Sie unter Wertformatierung in Berichten .
Gruppe	
Feld für Incident	Feld, das speziell zum Gruppieren von Incident-Daten verwendet wird.
Maximale Anzahl Gruppen	Beschränken Sie die Anzahl der in der Visualisierung angezeigten Gruppen.
Andere anzeigen	Option zum Gruppieren überschüssiger Daten in einem **Andere** Kategorie.
Datenaktualisierung	
Filter nachverfolgen	Folgt Filtern, die auf Seitenebene festgelegt sind. Wenn diese Option ausgewählt ist, spiegelt die Visualisierung Arbeitsbereichsfilter wider. Wenn diese Option nicht ausgewählt ist, ignoriert die Visualisierung alle Filter auf Seitenebene.
Filtersymbol anzeigen	Option zum Anzeigen des Filtersymbols und der Anzahl der Filter, die sich auf die Visualisierung auswirken. Wenn das Kontrollkästchen nicht aktiviert ist, werden das Symbol und die Filteranzahl ausgeblendet.
Aktualisieren Sie, nachdem Sie X Min. Abwesend waren	Auslöser basierend auf der Zeit außerhalb des Dashboards innerhalb desselben Arbeitsbereichs, einschließlich der Platform Analytics-Experience. Definiert die Anzahl der Minuten, nach denen die Visualisierung automatisch aktualisiert wird, wenn Sie zurückkehren. Verwechseln Sie diese Einstellung nicht mit **Geplante Wiederholung** In Inline-Dashboards, wodurch das gesamte Dashboard nur aktualisiert wird, solange es geöffnet bleibt.
Infonachrichten	
Anwenderdefinierte Nachricht festlegen, wenn keine Daten vorhanden	Anwenderdefinierter Text, der angezeigt wird, wenn keine Daten für die Visualisierung verfügbar sind.
Farben	
Farbtyp festlegen	Farbschema, das auf verschiedene Datenwerte oder -Bereiche angewendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenkonfigurationsoptionen (Fortsetzung)

Feld	Beschreibung
Diagramminteraktion	Im Diagramm unterstützte Anwenderaktionen, z. B. Zeigen oder Auswählen.

Log Analytics in Service Operations-Arbeitsbereich für ITOM

Zeigen Sie die Warnungen an, und behandeln Sie sie Health Log Analytics Generiert in Service Operations-Arbeitsbereich.

Auf der Übersichtsregisterkarte Maßnahmen für Log Analytics-Warnungen ergreifen

Starten Sie Log Analytics Warnungskorrekturprozess von **Übersicht** Registerkarte in Service Operations-Arbeitsbereich. Diese Registerkarte enthält Informationen zu den Warnungen, Protokolldaten, die dem anomalen Verhalten zugeordnet sind, CIs, die die auslösende Metrik generiert haben, und Services, die von den Warnungen betroffen sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Prozedur

1. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.
2. Wählen Sie die entsprechende Liste in der Unterliste „Warnungen“ aus, und navigieren Sie zu der gewünschten Warnung oder Gruppe.

   Alle von generierten Warnungen Health Log Analytics Haben den Wert **Log Analytics** In **Quelle** Spalte. Durch den Wert in der Spalte **Gruppe** wird die Art der Log Analytics-Warnung identifiziert. Unter Typen von Health Log Analytics Warnungen finden Sie eine detailliertere Beschreibung der einzelnen Arten von Warnungen oder Gruppen.

   Tipp: Um die Vorschau einer Warnung in der Liste anzuzeigen, klicken Sie auf das zugehörige Info-Symbol ( ).

3. Wählen Sie die Warnungsnummer aus.

   Die Registerkarte **Übersicht** wird angezeigt.

4. Zeigen Sie den Abschnitt der Registerkarte **Übersicht** an, der die Informationen enthält, die Sie benötigen.

   Eine Beschreibung der Abschnitte und Karten finden Sie unter Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics.

   Hinweis: Da in einigen Abschnitten der Registerkarte **Übersicht** nur ein Teil der Informationen zu sehen ist, enthalten viele Abschnitte einen Link, über den Sie andere oder vollständigere Informationen aufrufen können.

5. **Wahlweise:** Führen Sie vordefinierte Korrekturaufgaben aus, um Warnungsprobleme zu lösen.
   a. Wählen Sie Aus **Starten Sie das Playbook** .
   b. Wählen Sie die Registerkarte **Playbook** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Führen Sie die Korrektur aus** Die Karte zeigt die verfügbaren Korrekturaktionen an.

c. Wählen Sie die Kachel aus, die der Aktion entspricht, die Sie ausführen möchten.
Wenn die Aktion abgeschlossen ist, wird sie in angezeigt **Abgeschlossen** Karte.

Abschnitte und Karten auf der Registerkarte Übersicht für eine komponentenbasierte Warnung in Health Log Analytics

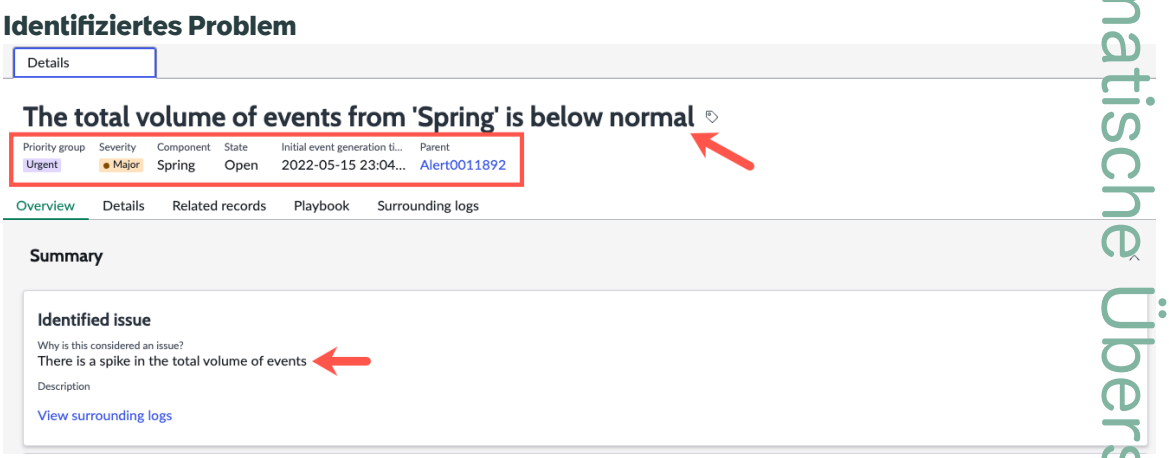
Die Registerkarte **Übersicht** in Service Operations-Arbeitsbereich hilft Ihnen, komponentenbasierte Warnungen zu verstehen.

Eine detaillierte Beschreibung von Komponentenbasierte Warnungen finden Sie unter Typen von Health Log Analytics Warnungen.

Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.



Wählen Sie **Umgebende Protokolle anzeigen** aus, um Protokollnachrichten anzuzeigen, die für die Warnung relevant sind. Weitere Informationen finden Sie unter Analysieren Sie Protokollzeilen, die eine Anomalie in umgeben Health Log Analytics.

Abweichung

Auf dieser Karte wird die anomale Aktivität dargestellt, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

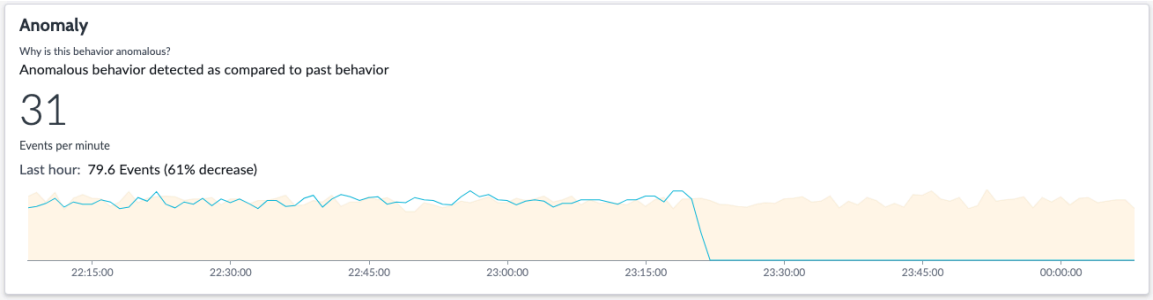
  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Das Abfallen des Metrikwerts (Ereignisse pro Minute) ist deutlich sichtbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Karte „Abweichung“



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Typen von anomalem Verhalten in Health Log Analytics.

Auswirkung

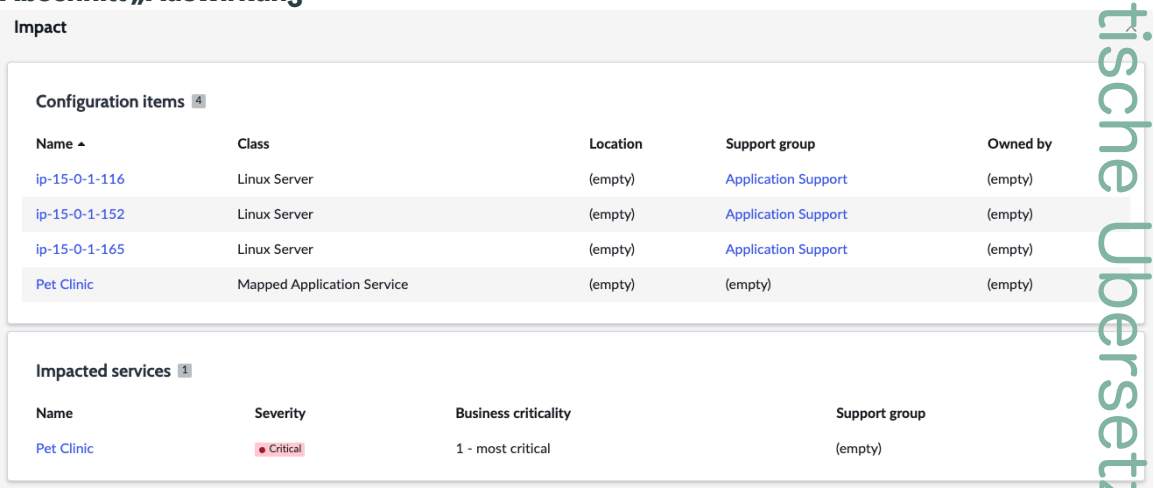
Konfigurationselemente

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

Betroffene Services

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

Abschnitt „Auswirkung“



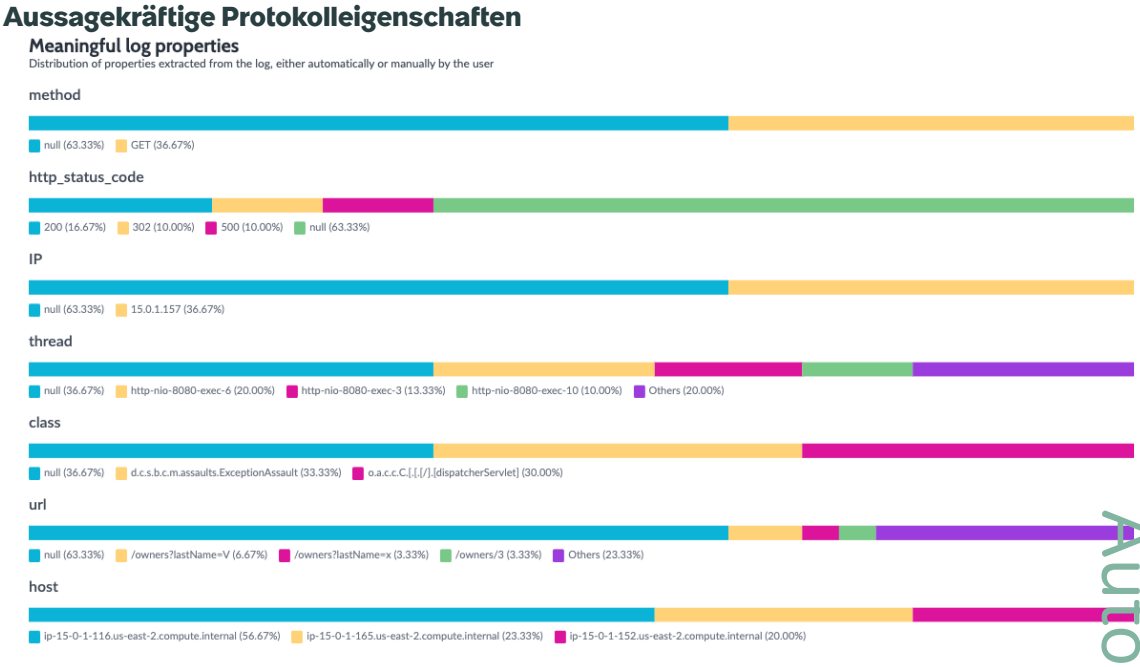
Ursache

Aussagekräftige Protokolleigenschaften

Auf dieser Karte zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Abschnitte und Karten auf der Registerkarte Übersicht für einen Log Analytics Gruppieren Sie in Health Log Analytics

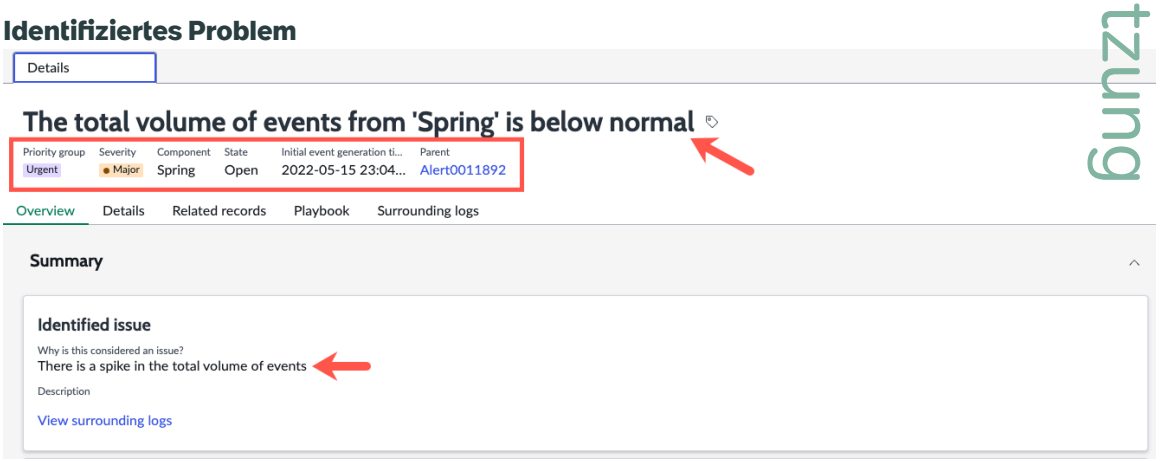
Mithilfe der Registerkarte **Übersicht** in Service Operations-Arbeitsbereich können Sie Log Analytics-Gruppen korrekt interpretieren.

Eine detaillierte Beschreibung von Log Analytics-Gruppen finden Sie unter Typen von Health Log Analytics Warnungen.

Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.



Wählen Sie **Korrelationen anzeigen** aus, um die Liste der Korrelationen anzuzeigen, die sich auf die Log Analytics-Warnungen beziehen.

Liste „Korrelationen“

Automatische Übersetzung

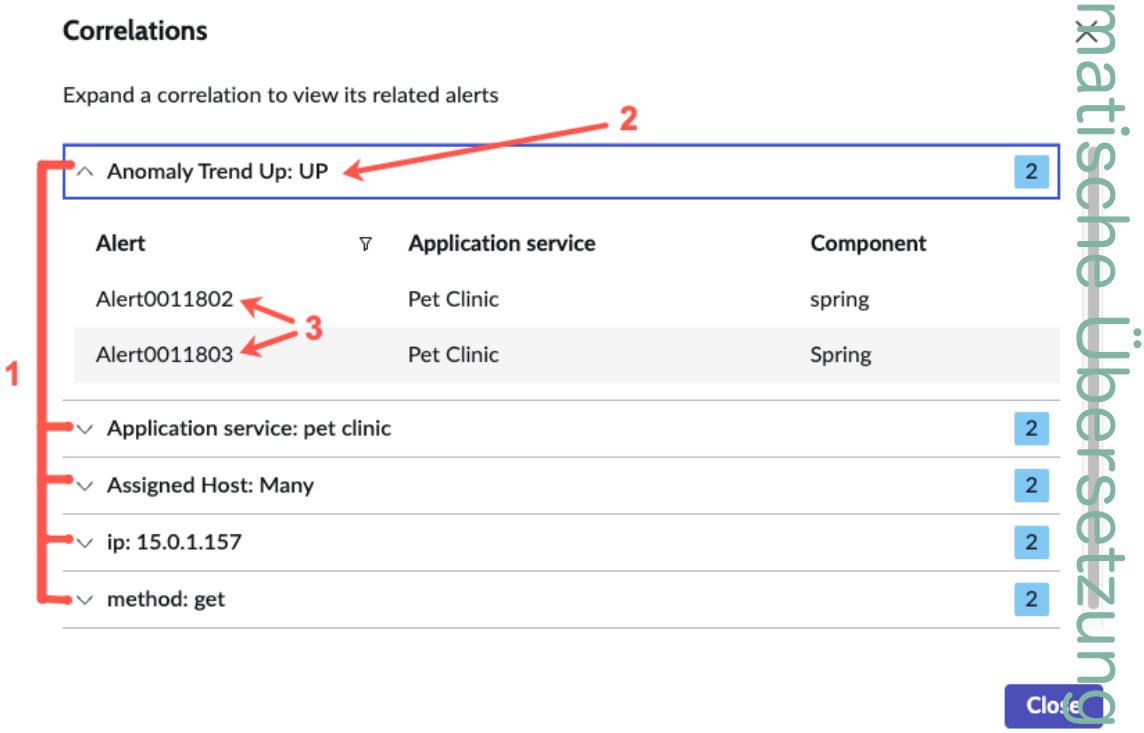
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der ersten Analyse werden Warnungen bewertet. Jede Korrelation in Protokolldaten einer Warnung mit einer anderen Warnung trägt zur Punktzahl einer Warnung bei. Je höher die Punktzahl, desto wahrscheinlicher ist es, dass die Warnung als Log Analytics-Warnung in einer eingeschlossen wird Log Analytics-Gruppe.

Die folgenden Arten von Daten werden berücksichtigt, wenn untersucht wird, ob Warnungen miteinander in Beziehung stehen:

- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Korrelationen



1. Liste der Korrelationen: Die erste Korrelation in der Liste wird erweitert, um die einzelnen korrelierten Log Analytics-Warnungen und anzuzeigen ProtokollkorrelatorDie die Warnungen teilen.
2. Eine Person Protokollkorrelator: Der Bezeichner für eine Gruppe korrelierter Log Analytics-Warnungen. Die Warnungen werden nach den Daten oder Metadaten der Protokollzeile gruppiert, die in mehreren Warnungen identisch sind (z. B. IP-Adresse, Hostname oder Benutzername). Die Zahl in dem blauen Quadrat ist die Anzahl der miteinander in Beziehung stehenden Warnungen.
3. Protokollieren Sie Analytics-Warnungen, die korreliert sind.

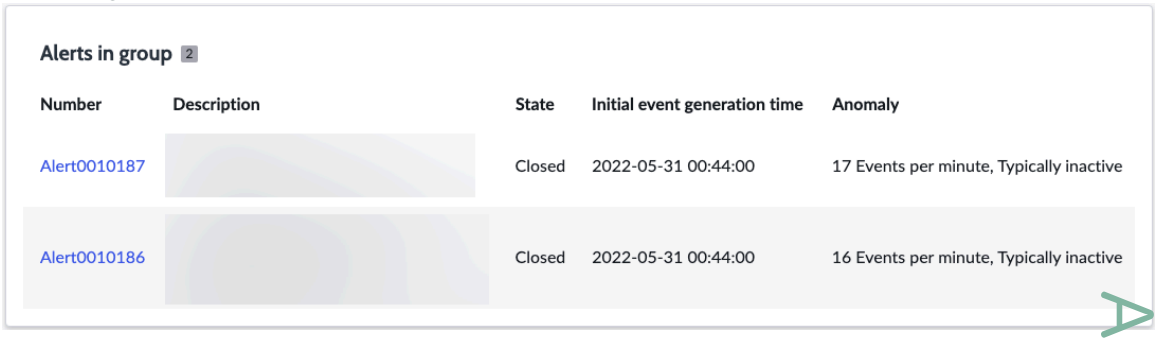
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen in Gruppe

Für eine Log Analytics-Warnung zeigt die Karte Warnungen in Gruppe die Log Analytics-Warnungen an, die unter der Log Analytics-Warnung gruppiert sind. Wählen Sie eine Log Analytics-Warnung aus, um ihre Details anzuzeigen.

Warnungen in Gruppe



Wählen Sie **Alle anzeigen** aus, um die Liste aller Log Analytics-Warnungen in der Gruppe und relevante Informationen zu ihnen anzuzeigen. Sie können die Liste „Warnungen in Gruppe“ auch anzeigen, indem Sie die Registerkarte **Zugehörige Datensätze** und dann **Warnungen in Gruppe** auswählen. Weitere Informationen finden Sie unter Zeigen Sie an Log Analytics Warnungen in einem Log Analytics Gruppieren Sie in Health Log Analytics

Auswirkung

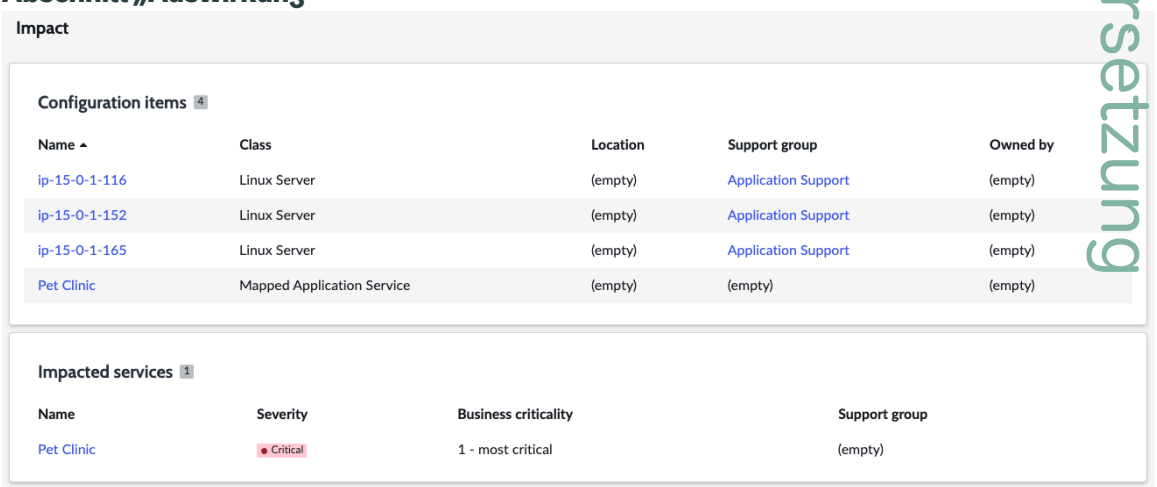
Konfigurationselemente

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

Betroffene Services

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

Abschnitt „Auswirkung“



Zeigen Sie an Log Analytics Warnungen in einem Log Analytics Gruppieren Sie in Health Log Analytics

Zeigen Sie eine Liste aller an Log Analytics Warnungen in einem Log Analytics-GruppeAuf der **Zugehörige Datensätze** Registerkarte.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

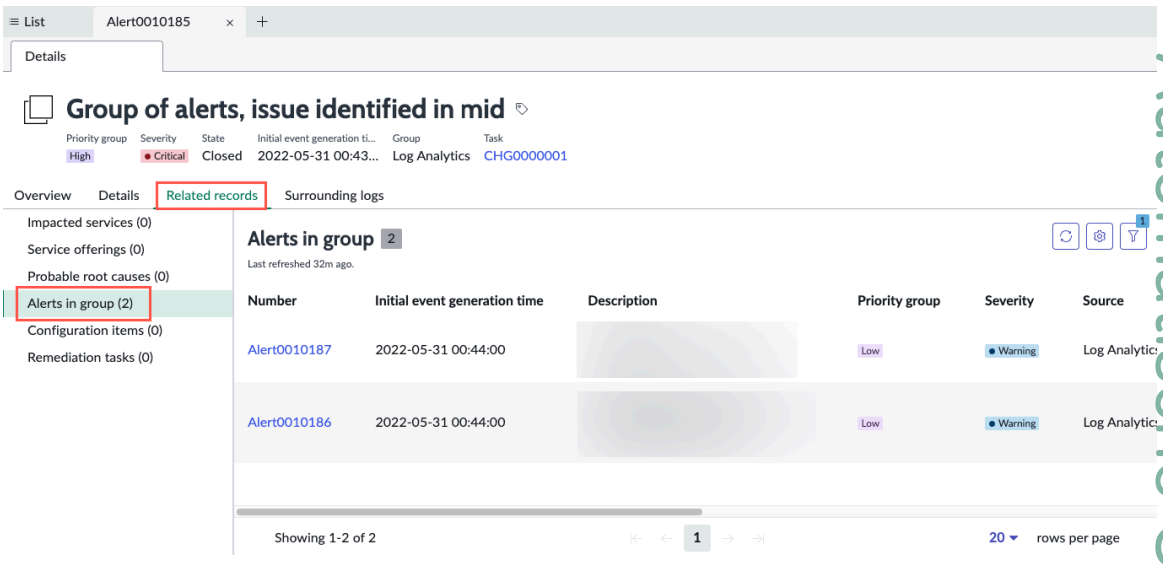
Für eine detaillierte Beschreibung von Log Analytics Gruppen und Log Analytics Warnungen, siehe Typen von Health Log Analytics Warnungen.

Prozedur

1. Auf der **Übersicht** Registerkarte für ein Log Analytics Warnung, wechseln Sie zu **Warnungen in Gruppe** Karte und wählen Sie aus **Alle anzeigen** Link.

   Der Abschnitt **Warnungen in Gruppe** auf der Registerkarte **Zugehörige Datensätze** wird angezeigt.

Abschnitt „Warnungen in Gruppe“ auf der Registerkarte „Zugehörige Datensätze“



2. Für jeden Log Analytics Warnung in Log Analytics-Gruppe, Die in der Tabelle beschriebenen Informationen sind verfügbar.

Warnungen in Gruppe

Spalte	Beschreibung
Nummer	Die Nummer der Warnung. Wählen Sie die Nummer aus, um detaillierte Informationen zu einer Warnung anzuzeigen. Dieses Feld wird automatisch festgelegt.
Generierungszeit des ersten Ereignisses	Die Zeit, zu der das Ereignis, von dem die Warnung generiert wurde, zuerst aufgetreten ist. **Hinweis:** Dies ist die Verarbeitungszeit des ServiceNow-Systems, nicht die Zeit des Quellsystems.
Gruppe	Typ der Gruppe, zu der die Warnung gehört: Eine eigenständige Log Analytics-Warnung oder ein Komponentenbasierte Warnung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Beschreibung	Anomales Muster oder anomale Metrik, die die Generierung der Warnung verursacht haben.
Schweregrad	Schweregradwert für die Warnung. Verfügbare Werte: ○ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. ○ **Schwerwiegend**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert. ○ **Gering**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor. ○ **Warnung**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. ○ **Info**: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. ○ **Löschen oder Gelöst**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Prioritätsgruppe, die die Reihenfolge angibt, in der Warnungen gelöst werden sollen. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Dringend** ○ **Hoch** ○ **Mittel** ○ **Niedrig** Der Wert der Prioritätsgruppe ist wichtiger als der Schweregrad allein. Beispielsweise sollte eine Warnung mit hoher Priorität und niedrigem Schweregrad vor einer Warnung mit niedriger Priorität und hohem Schweregrad behandelt werden. Informationen zur Berechnung der Priorität finden Sie unter Warnungspriorität.
Status	Verarbeitungsstatus der Warnung. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	○ **Erneut öffnen**: Eine zuvor geschlossene Warnung wurde erneut geöffnet und erfordert Ihre Aufmerksamkeit. ○ **Flatternd**: Die Warnung erhält identische Events, die mit hoher Häufigkeit aus derselben Quelle eintreffen. Dieser Status kann dazu führen, dass eine Warnung aus dem Status „Geschlossen“ erneut geöffnet wird, was zu einer Anhäufung von Changes mit den Status „Offen“ und „Geschlossen“ führt. ○ **Geschlossen**: Die Warnung wurde geschlossen und erfordert keine weitere Aktion. Sie schließen eine Warnung, wenn sie behoben wurde.
Konfigurationselement	CI in der CMDB. Das CI wird von der Warnung angewendet.
Knoten	Knotenfeld, das in der Protokollnachricht empfangen wurde. Das in der Protokollnachricht beschriebene Event ist auf diesem Knoten aufgetreten. Oft ist der Knoten der Name des CI, das der Warnung zugeordnet ist. Zum Beispiel ein Computername, eine IP-Adresse, ein FQDN oder eine MAC-Adresse.
Quelle	Alle Health Log Analytics-Warnungen haben den Wert **Log Analytics** In **Quelle** Spalte, die angibt, dass die Health Log Analytics-App die Warnung generiert hat.
Metrikname	Name der Metrik, deren anomales Verhalten zu der Warnung geführt hat. Zum Beispiel die *`I/O request`*Wenn die E/A-Anforderung länger als 15000 ms dauerte.
Aktualisiert	Zeitpunkt der letzten Aktualisierung der Informationen oder des Status der Warnung.

Informationen auf der Registerkarte Übersicht für einen Log Analytics Warnung in Health Log Analytics

Mithilfe der Registerkarte **Übersicht** in Service Operations-Arbeitsbereich können Sie Log Analytics-Warnungen korrekt interpretieren.

Eine detaillierte Beschreibung von Log Analytics-Warnungen finden Sie unter Typen von Health Log Analytics Warnungen.

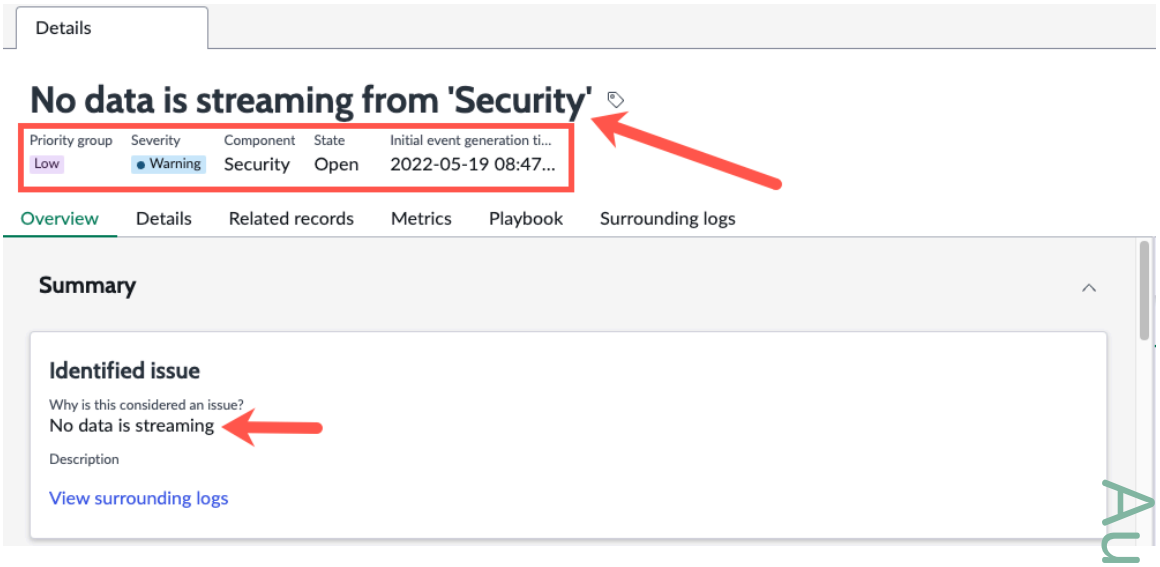
Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifiziertes Problem



Wählen Sie **Umgebende Protokolle anzeigen** aus, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Analysieren Sie Protokollzeilen um die Anomalie, um die Ursache zu finden.

Abweichung

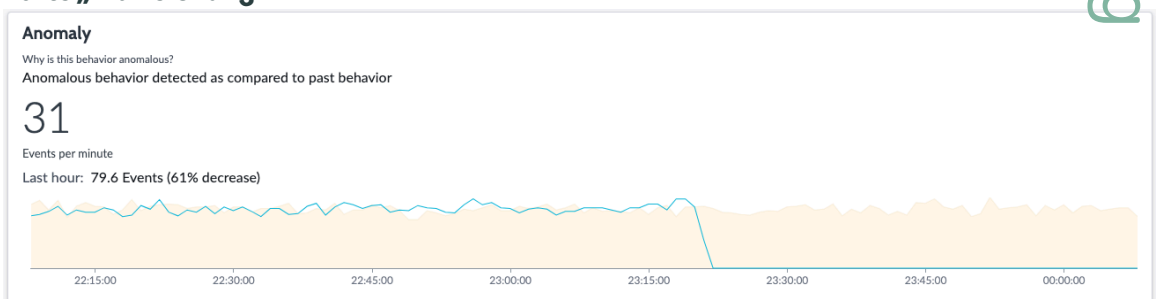
Auf dieser Karte wird die anomale Aktivität dargestellt, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Das Abfallen des Metrikwerts (Ereignisse pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Typen von anomalem Verhalten in Health Log Analytics.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkung

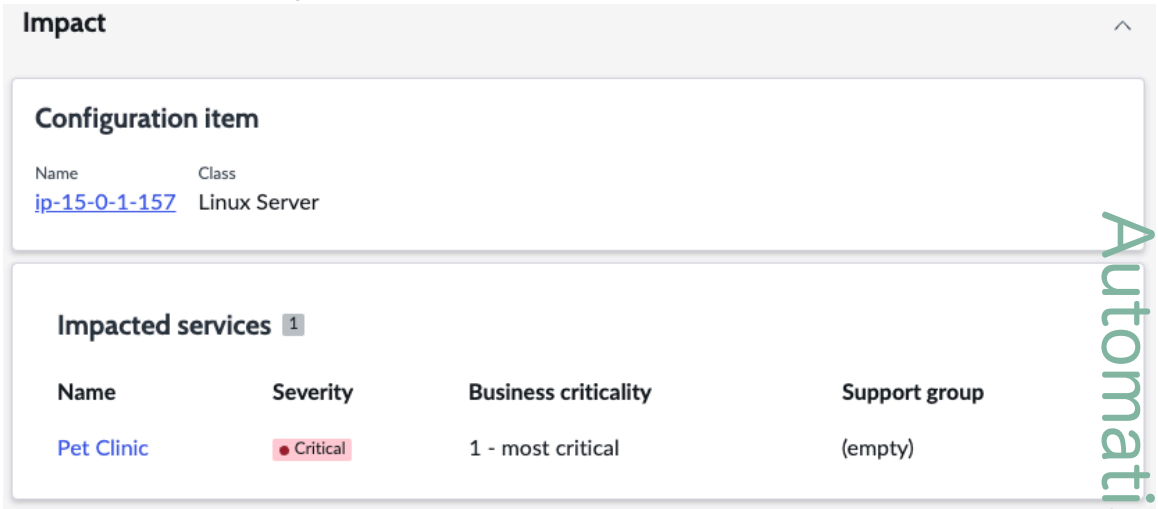
Konfigurationselemente

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

Betroffene Services

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

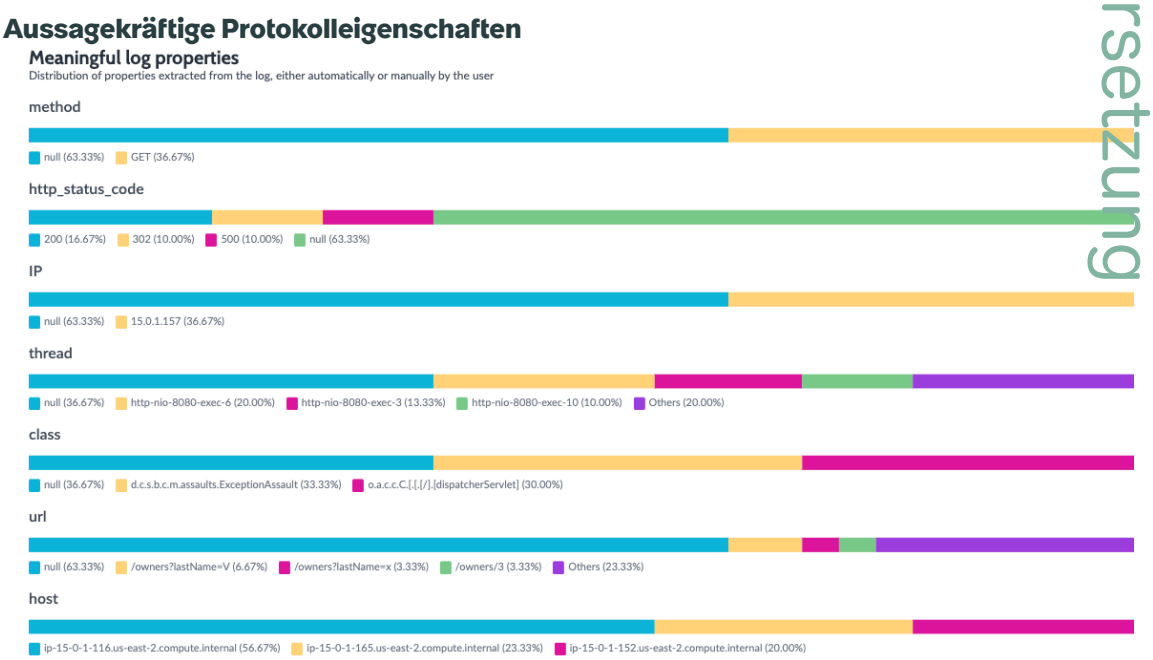
Abschnitt „Auswirkung“



Ursache

Aussagekräftige Protokolleigenschaften

Auf dieser Karte zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analyse der Protokolle um eine Anomalie, um die Ursache der Warnung in zu finden Health Log Analytics

Wenn Health Log Analytics eine Anomalie identifiziert, gibt die Anzeige der die Anomalie umgebenden Protokolle Hinweise auf den Status fehlerhafter Systeme. Diese Informationen können Ihnen helfen, die Ursache einer Warnung einzugrenzen.

Beim Anzeigen von Log Analytics Warnung, die **Umgebende Protokolle** Auf der Registerkarte werden die Protokollzeilen aufgelistet, die eine Minute vor und eine Sekunde nach dem Auftreten der Anomalie generiert wurden. Die Protokollzeilen beziehen sich auf die Metrik oder das Muster, die die Warnung ausgelöst hat. Die Liste wird nach der entsprechenden Komponente gefiltert.

Protokolle, die unmittelbar vor der Anomalie generiert wurden, können auf Warnzeichen oder Bedingungen verweisen, die zu dem Problem geführt haben. Durch die Überprüfung dieser Protokolle können Sie die Sequenz der Ereignisse nachverfolgen, die zur Anomalie geführt haben, um zu verstehen, was schief gelaufen ist. Protokolle, die direkt nach der Anomalie erstellt wurden, können Ihnen helfen, die Auswirkungen des Ereignisses zu bewerten, indem analysiert wird, wie das System reagiert hat und ob andere Komponenten betroffen waren. Die Zeitleiste der Protokolle um die Anomalie kann helfen, zu klären, was das Problem verursacht haben könnte, z. B. eine Konfigurationsänderung oder ein Software-Update.

Sie können den Zeitbereich der angezeigten Protokollzeilen ändern, z. B. um Protokolle von mehr als einer Minute vor der Anomalie oder mehr als einer Sekunde danach zu untersuchen.

Hinweis: Protokolle, die die Anomalie umgeben, werden aufbewahrt und sind nach Erstellung der Warnung 30 Tage lang verfügbar. Diese Protokolle werden vom System nicht gelöscht, wenn der globale Aufbewahrungszeitraum der Protokolle abgelaufen ist. Wenn der Aufbewahrungszeitraum abgelaufen ist, sind die umgebenden Protokolle nur auf der Registerkarte **Umgebende Protokolle** und nicht im Protokoll-Viewer verfügbar.

Health Log Analytics Ermöglicht Ihnen das grafische Anzeigen der anomalen Protokolldaten im Protokoll-Viewer, auf den über zugegriffen wird Service Operations-Arbeitsbereich. Der Protokoll-Viewer zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und einer Minute nach an Log Analytics Warnung und listet die zugehörigen Protokollzeilen auf. Er zeigt automatisch die Abfrage im Zusammenhang mit der Anomalie, der ausgewählten Komponente und dem entsprechenden Zeitfilter an. Weitere Informationen finden Sie unter Überprüfen der Protokolle, die mit einer Warnung im Protokoll-Viewer in verbunden sind Health Log Analytics.

Zugehörige Informationen

Analysieren Sie Protokollzeilen, die eine Anomalie in umgeben Health Log Analytics

Analysieren Sie Protokollzeilen, die eine Anomalie in umgeben Health Log Analytics

Zeigen Sie die Protokollzeilen um eine Anomalie an, um die Ursache einer Log Analytics-Warnung zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereich eine Log Analytics-Warnung.
2. Wählen Sie die Registerkarte **Umgebende Protokolle** aus, und überprüfen Sie die Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Registerkarte wird die Liste der Protokollzeilen angezeigt, die eine Minute vor und eine Sekunde nach der Log Analytics-Warnung erzeugt wurden. Eine Erklärung der Informationen auf der Registerkarte finden Sie unter Felder der Registerkarte „umgebende Protokolle“.

3. **Wahlweise:** Zeigen Sie mit einer der folgenden Methoden einen anderen Zeitraum der Protokollzeilen an:
   - Aktualisieren Sie den Zeitbereich relativ zur Warnung auf einen vorgegebenen Zeitbereich in der Liste **Bereich auswählen**.
   - Geben Sie mithilfe der Zeitauswahl eine **Startzeit** oder **Endzeit** an.
4. **Wahlweise:** Um die anomalen Protokolldaten als Funktion der Zeit grafisch anzuzeigen, wählen Sie **Protokoll-Viewer** aus.
   Weitere Informationen finden Sie unter Überprüfen der Protokolle für eine Warnung im Protokoll-Viewer in Health Log Analytics.

Überprüfen der Protokolle für eine Warnung im Protokoll-Viewer in Health Log Analytics

Die **Protokoll-Viewer** Auf der Registerkarte können Sie die Protokolle für eine Warnung nach Zeitstempel oder Zeitbereich durchsuchen und die Anomaliehäufigkeit innerhalb eines bestimmten Zeitraums visualisieren. Durch das Anpassen der angezeigten Daten und das Anpassen der Zeitfilter können Sie das Framework, in dem die Anomalie aufgetreten ist, besser verstehen und so die Ursache schneller finden.

Der Protokoll-Viewer zeigt alle Daten an, die mit verbunden sind Log Analytics Warnung. Zeigt die Abfrage, die sich auf die Anomalie, die ausgewählte Komponente und den entsprechenden Zeitfilter bezieht. Sie können die angezeigten Daten personalisieren und den Zeitbereich manuell anpassen, ohne die anderen Einstellungen zu beeinträchtigen. Die angewendeten Filter werden in angezeigt **Filter** Bereich. Sie können Filter nach Bedarf hinzufügen oder entfernen, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Die **Protokoll-Viewer** Zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und einer Minute nach an Log Analytics Warnung und listet die zugehörigen Protokolldaten auf. Diese Informationen helfen Ihnen, Trends zu identifizieren, die vor und nach dem Ereignis führen, und bieten Kontext für die Ursachenanalyse.

Während Sie die Protokolle für eine Warnung im analysieren **Protokoll-Viewer** , Sie können die Abfrage ändern, um die Suche zu optimieren, nützliche Suchen zu speichern und für andere freizugeben. Für eine Beschreibung der Informationen, die in angezeigt werden **Protokoll-Viewer** Tabelle, siehe Protokollbetrachter-Tabellenfelder.

Sie können die folgenden Aufgaben auf ausführen **Protokoll-Viewer** :

- Zeigen Sie Protokolldaten für eine Warnung in an Health Log Analytics

  Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

- Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics

  Optimieren Sie die Suchabfrage, um die Ursachen des Problems zu bestimmen, und speichern und nützliche Suchen freigeben zu können.

- Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics

  Verwenden Sie eine gespeicherte Suche. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

- Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics

  Wenden Sie Filter an, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics

  Fügen Sie Spalten in der Tabelle hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Wenn Sie eine wichtige Metrik in den Protokolldaten erkennen, können Sie sie verwenden, um eine neue zu definieren Log Analytics Warnungsregel. Weitere Informationen finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

Zugehörige Informationen

Analyse der Protokolle um eine Anomalie, um die Ursache der Warnung in zu finden Health Log Analytics

Zeigen Sie Protokolldaten für eine Warnung in an Health Log Analytics

Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokolllinien und der zugehörigen Protokolldaten im Protokoll-Viewer an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Registerkarte mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. **Wahlweise:** Personalisieren Sie die angezeigten Daten und ihre Darstellung im Protokoll-Viewer.
   - Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics, um nur die Daten anzuzeigen, die Sie anzeigen möchten.
   - Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics, indem Sie Spalten hinfügen oder entfernen.

   Diese Funktionen werden unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .
3. Analysieren Sie protokollbasierte Anomalien und den hinzugefügten Kontext, um die durchschnittliche Zeit bis zur Reparatur (MTTR) zu verkürzen.
   Angenommen, Sie finden eine Protokollzeile mit Fehlern in einer Konfigurationsdatei. Auf der Karte **Anomalie** zeigt eine plötzliche Spitze im Diagramm an, wo die Konfigurationsdatei die Fehler generiert. Auf der Karte **Aussagekräftige Protokolleigenschaften** können Sie aus den Protokollen extrahierte zusätzliche Schlüssel-Wert-Paare anzeigen und die betroffenen Anwendungsservices und die zugehörigen Serviceangebote auf der Karte **Betroffene Services** herausfinden. Um den Kontext zu vergrößern, sollten Sie die Protokolle untersuchen, die die Anomalie umgeben, nach der Konfigurationsdatei suchen und den Zeitrahmen ermitteln, in dem die Probleme aufgetreten sind.

Nächste Maßnahme

Verwenden Sie zusätzliche Funktionen im Protokoll-Viewer, um Ihre Suche zu verfeinern oder Warnungen zu definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie die Suchabfrage, um die Suche zu optimieren und nützliche Suchen zu speichern. Weitere Informationen finden Sie unter Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics.
- Wenn Sie in den Protokolldaten wichtige Beziehungen entdecken, wählen Sie **Warnung definieren**, um die Art der Warnung zu definieren, die von den Daten ausgelöst werden soll. Anweisungen dazu finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

Zugehörige Informationen

Überprüfen der Protokolle für eine Warnung im Protokoll-Viewer in Health Log Analytics

Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics

Definieren, speichern und teilen Sie Suchen nach Protokolldaten, um die Ursachen von Log Analytics-Warnungen zu ermitteln.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Definieren Sie eine Suche.
   a. Wählen Sie auf Auswahlsymbol ( ), und wählen Sie **Neue Suche** aus.
   b. Legen Sie die Werte der Suchparameter in den Suchfeldern fest.

Suchfelder

Suchfeld	Beschreibung
Abfrage	Suchabfrage. **Tipp:** Der Protokoll-Viewer nutzt die Suchmaschine Elasticsearch. Sie können daher im Feld **Abfrage** beliebige unterstützte Suchbegriffstrukturen verwenden.
Komponente	Logische Komponente von Service Instanz , die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Zeitbereich	Zeitbereich, der beim Anzeigen der zurückgegebenen Daten auf die X-Achse angewendet werden soll. Die von Ihnen angegebene Einstellung wird in den Feldern **Start time** (Startzeit) und **End time** (Endzeit)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchfeld	Beschreibung
	angezeigt. Verwenden Sie eine der folgenden Methoden: ▪ Wählen Sie einen Zeitraum aus der Liste aus. ▪ Klicken Sie auf **Benutzerdefinierter Bereich**, um über die Auswahl für Datum und Uhrzeit einen Bereich anzugeben. **Hinweis:** Sie können die Einstellungen in den Feldern **Startzeit** und **Endzeit** manuell ändern. Der ausgewählte Zeitraum, der in **Bereich auswählen** angezeigt wird, ändert sich dann zu „Benutzerdefinierter Bereich“. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store . **Hinweis:** Gespeicherte Suchen enthalten keine Einstellungen für den Zeitbereich.

c. Klicken Sie auf **Search** (Suchen).

Das System gibt die vollständige Liste der Protokollzeilen zurück, die den Suchwerten entsprechen. Die Informationen werden im Diagramm „Ergebnisse im Zeitverlauf“ angezeigt.

3. Wahlweise: Speichern Sie die Suche.
Die gespeicherte Suche enthält die ausgewählten Filter. Weitere Informationen zu Filtern finden Sie unter Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics.

Hinweis: Gespeicherte Suchen enthalten keine Einstellungen für den Zeitbereich.

a. Wählen Sie **Save As** (Speichern unter).

b. Geben Sie im Feld **Search name** (Suchname) einen eindeutigen und beschreibenden Namen für die Suche ein, und klicken Sie dann auf **Save** (Speichern).

Hinweis: Wenn Sie Health Log Analytics Anwendung, Version 20.0.11 – Juli 2021, und Health Log Analytics Viewer-Anwendung, Version 20.0.4 – Juli 2021, verfügbar über ServiceNow Store verwenden, können Sie eine Warnungsregel definieren, ohne die Suche zu speichern. Weitere Informationen finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.

4. Wahlweise: Geben Sie die gespeicherte Suche für eine Zuweisungsgruppe frei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Freigeben**.

b. Wählen Sie eine Zuweisungsgruppe aus der Liste aus.

c. Wählen Sie **Speichern**.

Zugehörige Informationen

Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics

Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics

Verwenden oder ändern Sie eine gespeicherte Protokolldatensuche in Health Log Analytics

Verwenden Sie eine gespeicherte Suche nach Protokolldaten, um die Ursachen einer Warnung besser zu verstehen. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

Vorbereitungen

Hinweis: Wenn Sie nicht der Besitzer der gespeicherten Suche sind, speichern Sie die Suche unter einem anderen Namen. Anschließend können Sie Suchwerte aktualisieren, Ihre Änderungen speichern und die Suche für andere freigeben.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:

- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
- Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .

2. Verwenden Sie eine gespeicherte Suche.

a. Wählen Sie auf Auswahlsymbol ( ), und wählen Sie **Suche laden** aus.

b. Wählen Sie im Dialogfeld „Suche laden“ den Namen der zu ladenden Suche aus.
Das System gibt die vollständige Liste der Protokollzeilen zurück, die den Suchwerten entsprechen, und zeigt die Informationen im Diagramm mit den Ergebnisse im Zeitverlauf an.

3. Wahlweise: Aktualisieren Sie die gespeicherte Suche.

a. Klicken Sie auf das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine Suchen verwalten** aus.

b. Ändern Sie die Einstellungen.

Formular „Meine Suchen verwalten“

Feld	Beschreibung
Name	Name der gespeicherten Suche.
Abfrage	Suchabfrage. (Optional) Der Protokoll-Viewer nutzt die Elasticsearch-Such-Engine. Sie können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	daher im Feld **Query** (Abfrage) beliebige unterstützte Suchbegriffstrukturen verwenden.
Zuweisungsgruppe	Zuweisungsgruppen, die auf die Suche zugreifen können. Die Mitglieder der Gruppen können die Suche verwenden.
Filter	Spaltenfilter im Standardformat (`field1=value1, field2=value2, field3=value3, ...`).
Aktualisiert	Datum und Uhrzeit der Aktualisierung der Suche. (Optional) Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store.

Um Änderungen an den Suchwerten rückgängig zu machen, wählen Sie das Auswahlsymbol ( ) und dann **Änderungen verwerfen** aus. Die Änderungen, die Sie an den Suchwerten vorgenommen haben, werden verworfen. Sie können die Sucheinstellungen weiterhin aktualisieren.

c. Speichern Sie die aktualisierte Suche.

i. Wählen Sie **Speichern unter** aus.

ii. Geben Sie im Feld **Search name** (Suchname) einen eindeutigen und beschreibenden Namen für die Suche ein, und klicken Sie dann auf **Save** (Speichern).

Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics

Wenden Sie Filter auf an **Protokoll-Viewer** Um nur die gewünschten Daten anzuzeigen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store.

Prozedur

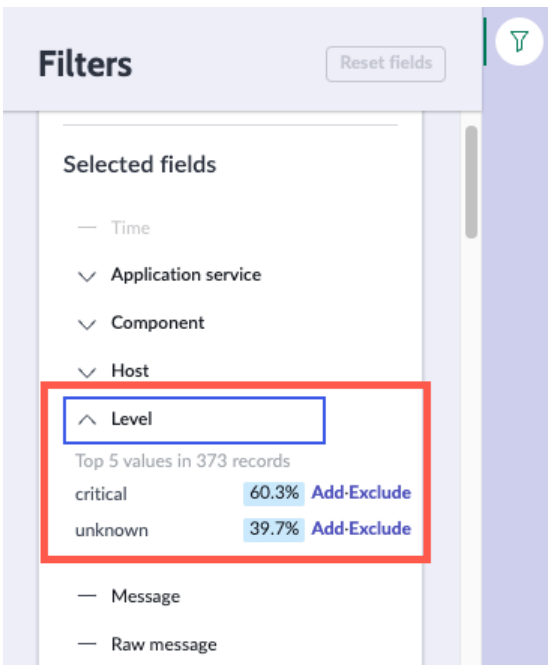
1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:

- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
- Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .

2. Definieren Sie eine Suche, und führen Sie diese aus.
Weitere Informationen finden Sie unter Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics.

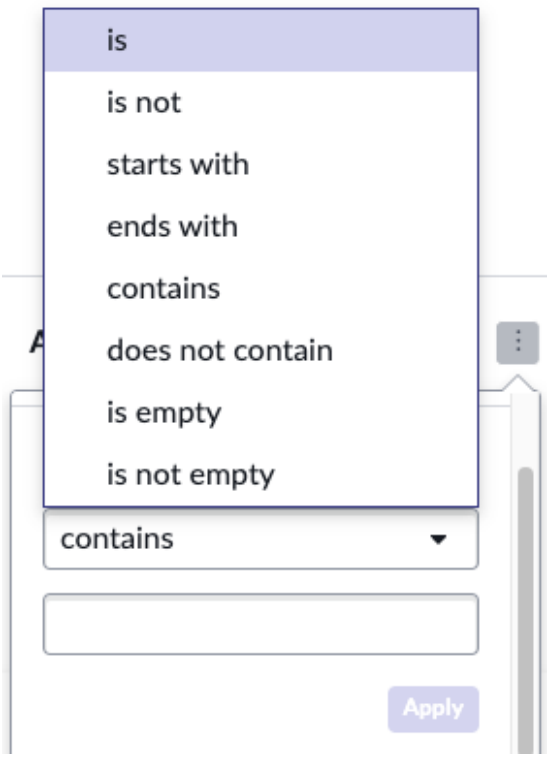
3. Filtern Sie die Suchergebnisse auf eine der folgenden Arten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Filter mithilfe der Feldliste hinzufügen	**a.** Wählen Sie das Filtersymbol ( ) aus. Die Liste ausgewählte Felder enthält die Felder, die derzeit als Spalten in angezeigt werden **Protokoll-Viewer** Tabelle. Standardmäßig enthält die Tabelle die folgenden Spalten: Anwendungsservice, Komponente, Host, Ebene, Nachricht, Rohnachricht und Zeit. Die Liste „Verfügbare Felder“ enthält alle verbleibenden Felder, die vom System aus dem Protokoll extrahiert wurden. **b.** Wählen Sie ein Feld in der Liste aus. **Hinweis:** Mit der Suchoption können Sie nach einem bestimmten Feld suchen. Die fünf wichtigsten Werte, die das System in den Datensätzen für dieses Feld gefunden hat, werden zusammen mit dem Prozentsatz ihrer Häufigkeit angezeigt.  **c.** Definieren Sie einen Filter für einen Wert im Feld. ▪ Um nur Daten anzuzeigen, die einen Wert enthalten, wählen Sie **Hinzufügen**. Um beispielsweise den Filter **[Ebene][ist][kritisch]** festzulegen, wählen Sie **Hinzufügen** für den Wert „kritisch“ im Feld „Ebene“ aus.

Automatische Übersetzung

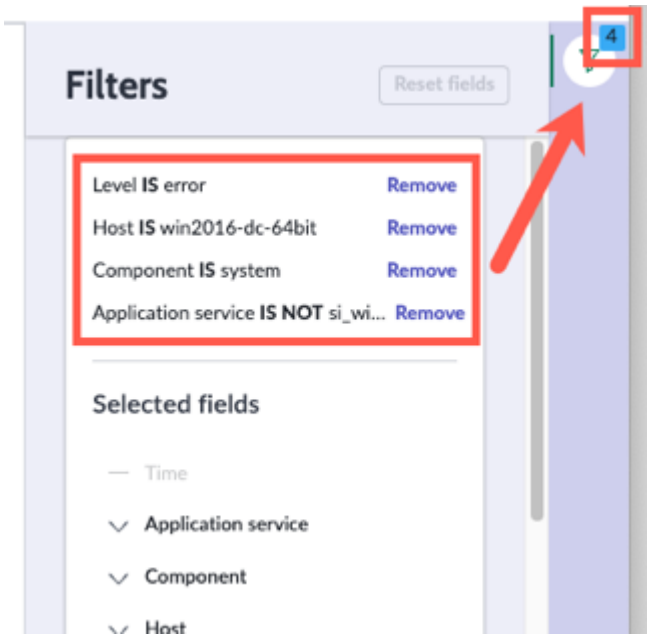
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	▪ Um negative Filter zu erstellen, die Daten ausschließen, die einen bestimmten Wert enthalten, wählen Sie **Ausschließen**. Um beispielsweise den Filter **[Ebene][ist nicht][kritisch]** festzulegen, wählen Sie **Ausschließen** für den Wert „kritisch“ im Feld „Ebene“ aus.
Fügen Sie Filter aus hinzu Protokoll-Viewer Tabelle	**a.** Wählen Sie in einem Spaltenheader das Symbol „Weitere Aktionen“ (⋮). **b.** Wählen Sie im Dialogfeld den Operator aus, und geben Sie die Filterbedingungen für das Feld an.  **c.** Wählen Sie **Übernehmen**. Ein Filtersymbol im Spaltenheader zeigt an, dass ein Filter für dieses Feld gilt.

Der angewendete Filter wird oben im Bereich **Filter** angezeigt. Die Gesamtanzahl der angewendeten Feldwertfilter im Symbol **Filter** wird angepasst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. **Wahlweise:** Entfernen Sie einen Filter auf eine der folgenden Arten.
   - Im Bereich **Filter**:
     a. Suchen Sie den Filter, den Sie entfernen möchten.
     b. Wählen Sie **Entfernen**.
   - In einem Spaltenheader:
     a. Wählen Sie das Symbol „Weitere Aktionen“ (⋮).
     b. Wählen Sie den Filter aus, den Sie entfernen möchten.
     c. Wählen Sie **Filter entfernen**.

Passen Sie die Tabelle „Protokoll-Viewer“ in an Health Log Analytics

Fügen Sie der Tabelle **Protokoll-Viewer** Spalten hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Prozedur
1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Wählen Sie das Filtersymbol ( ), um den Bereich **Filter** anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste „Ausgewählte Felder“ enthält die Felder, die derzeit als Spalten in der Tabelle **Protokoll-Viewer** angezeigt werden. Standardmäßig enthält die Tabelle die folgenden Spalten: Anwendungsservice, Komponente, Host, Ebene, Nachricht, Rohnachricht und Zeit. Die Felder „Verfügbar“ enthalten alle verbleibenden Felder, die das System aus dem Protokoll extrahiert hat.

In Service Operations-Arbeitsbereich Log Analytics Anwendung, Version 21.2.7 – November 2022 und höher, verfügbar über ServiceNow Store , Die Spalte Protokollnachricht wird hinzugefügt, und die Spalte Rohnachricht wird standardmäßig nicht mehr angezeigt. Sie können der Tabelle die Spalte „Rohnachricht“ hinzufügen, indem Sie sie aus der auswählen **Filter** Bereich.

3. Fügen Sie der Tabelle **Protokoll-Viewer** Spalten hinzu, oder entfernen Sie Spalten.
   - Um der Tabelle eine Spalte hinzuzufügen, wählen Sie das gleichnamige Feld in der Liste „Verfügbare Felder“ und dann das Symbol zum Hinzufügen ( ) aus.

     Das hinzugefügte Feld wird als Spalte in der Tabelle angezeigt. Es wird jetzt in der Liste „Ausgewählte Felder“ aufgeführt.
   - Um eine Spalte aus der Tabelle zu entfernen, wählen Sie das gleichnamige Feld in der Liste „Ausgewählte Felder“ und dann das Symbol zum Entfernen ( ) aus.

     Die entsprechende Spalte wird aus der Tabelle entfernt. Das entfernte Feld wird der Liste „Verfügbare Felder“ hinzugefügt.

     Wenn Sie die Daten nach bestimmten Werten in einem Feld gefiltert haben, werden diese Daten auch dann angezeigt, wenn das Feld nicht mehr ausgewählt ist. Weitere Informationen zum Filtern von Daten finden Sie unter Filtern Sie Suchergebnisse im Protokoll-Viewer in Health Log Analytics.

     Hinweis: Die Spalte „Zeit“ kann nicht aus der Tabelle entfernt werden.

4. **Wahlweise:** Passen Sie die maximale Anzahl von Zeichen pro Feld in der Tabelle an.
   a. Navigieren zu **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Systemeigenschaften**an.
   b. Öffnen Sie den Eigenschaftendatensatz `sn_occ.log_viewer.max.characters`.
   c. Bearbeiten Sie den Standardwert im Feld **Wert**.
   d. Wählen Sie **Aktualisieren**.

Ergebnis

Die Tabelle **Protokoll-Viewer** zeigt die benutzerdefinierte Ansicht ab der laufenden Sitzung solange an, bis Sie die Einstellungen ändern.

Hinzufügen, Ändern oder Löschen Log Analytics Warnungsregeln in Health Log Analytics

Fügen Sie eine Warnungsregel hinzu, ändern oder löschen Sie sie, die eine Warnung für eine angegebene Metrik generiert.

Weitere Informationen finden Sie unter Verwenden Sie Warnungsregeln, um zu steuern, wann Health Log Analytics Generiert Warnungen.

Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics

Definieren Sie ein Log Analytics Warnungsregel, wenn Protokolldaten angezeigt werden, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Definieren Sie eine Suche, und führen Sie diese aus.
   Weitere Informationen finden Sie unter Definieren, speichern und teilen Sie eine Suche nach Protokolldaten in Health Log Analytics.
3. Wenn eine Suche Protokolldaten zurückgibt, die eine Warnung generieren sollten, klicken Sie auf **Speichern** oder **Speichern unter**, um die Suche zu speichern.

   Hinweis: Wenn Sie Health Log Analytics Anwendung, Version 20.0.11 – Juli 2021, und Health Log Analytics Viewer-Anwendung, Version 20.0.4 – Juli 2021, verfügbar über ServiceNow Store verwenden, müssen Sie diesen Schritt nicht ausführen.

4. Greifen Sie auf das Formular zum Erstellen einer Warnungsregel zu, indem Sie oben rechts auf der Registerkarte **Protokoll-Viewer** die Option **Warnung definieren** auswählen.
5. Geben Sie im Formular den Namen und die Beschreibung für die Warnungsregel an.
   Der Name wird auf der Anomaliekarte für generierte Warnungen angezeigt.
6. Bestimmen Sie, ob die Regel Warnungen generiert, wenn die Schwellenwertbedingungen in den Protokolldaten erfüllt sind, indem Sie das Feld **Status** festlegen.
   Um die Regel zu aktivieren, wählen Sie **Aktiviert**aus.
7. Wenn Sie installiert haben Health Log Analytics Anwendung, Version 20.0.11 - Juli 2021, Legen Sie fest Schweregradwert für die von dieser Warnungsregel generierte Warnung.
   - **Niedrig**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit.
   - **Mittel**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor.
   - **Hoch**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert.
   - **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme.
8. Wenn Sie die Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, und die Anwendung Health Log Analytics Viewer, Version 20.0.4 - Juli 2021, installiert haben, geben Sie die Details für die Abfrage ein.

Abfragedetails

Feld	Beschreibung
Ihre Abfrage	Die Abfrage, nach der in den Protokolldaten gesucht werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig ist dies die Abfrage, die im Protokoll-Viewer definiert wurde. Sie können die Abfrage ändern, indem Sie Suchanforderungen hinzufügen. Um nach allen Abfragen zu suchen, geben Sie ein Sternchen (*) an.
Aktive Filter	Die für die Abfrage im Protokoll-Viewer definierten Filter. Sie können die Filter löschen.
Komponente	Die Komponente, für die diese Warnungsregel gilt. Standardmäßig ist dies die Komponente, die im Protokoll-Viewer definiert wurde. Sie können eine andere Komponente auswählen, indem Sie in der Komponentenzeile das Suchsymbol ( ) wählen und dann die erforderliche Komponente aus der Liste auswählen.

9. Füllen Sie die Felder aus, die sich auf den Schwellenwert beziehen, der die Warnungsregel auslöst.

Schwellenwert

Feld	Beschreibung
Operator	Mathematischer Vergleichsoperator, der festlegt, wie die Trefferanzahl eine Warnung dieser Art auslöst. Dieses Feld wird automatisch auf „Größer als“ festgelegt.
Trefferanzahl	Anzahl der übereinstimmenden Protokolleinträge, die als Auslöser für eine solche Warnung dienen.
Zeitraum	Zeitraum, über den die Trefferanzahl gemessen wird. Die Zeit wird in den Einheiten gemessen, die durch den Wert **Time unit** (Zeiteinheit) vorgegeben wird.
Time unit (Zeiteinheit)	Einheiten des Zeitraums. Dieses Feld wird automatisch auf Minuten gesetzt.
Persistenz	Zeitraum, über den die angegebene Trefferanzahl pro Zeiteinheit bestehen bleiben muss, um eine Warnung dieser Art auszulösen. Dieses Feld wird automatisch auf 1 Minute gesetzt.

10. Wählen Sie **Speichern**.

Ändern Sie A Log Analytics Warnungsregel in Health Log Analytics

Ändern Sie einen Log Analytics Warnungsregel, die Sie definiert haben.

Vorbereitungen

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Öffnen Sie eine definierte Warnung.
   a. Wählen Sie oben rechts auf der Registerkarte **Protokoll-Viewer** das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine definierten Warnungen verwalten** aus.
   b. Wählen Sie in der Tabelle **Definierte Warnungen** die Warnungsregel aus, die Sie ändern möchten.
3. Aktualisieren Sie im Formular die Einstellungen.
   Eine Beschreibung der Einstellungen finden Sie unter Fügen Sie ein hinzu Log Analytics Warnungsregel in Health Log Analytics.
4. Wählen Sie **Speichern** aus, um die Änderungen zu speichern.

Löschen Sie einen Log Analytics Warnungsregel in Health Log Analytics

Löschen Sie einen Log Analytics Warnungsregel, die Sie definiert haben, wenn sie nicht mehr erforderlich ist.

Vorbereitungen

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Öffnen Sie eine definierte Warnung.
   a. Wählen Sie oben rechts auf der Registerkarte **Protokoll-Viewer** das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine definierten Warnungen verwalten** aus.
   b. Wählen Sie in der Tabelle **Definierte Warnungen** die Warnung aus, die Sie löschen möchten.
3. Wählen Sie **Löschen**.

Zuweisen einer Warnung in eine höhere oder niedrigere Bedeutung Health Log Analytics

Bezeichnen Sie eine Warnung als aussagekräftig oder unbedeutend, oder stellen Sie die normale Wichtigkeit der Metrik wieder her, die an der Generierung beteiligt ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Markieren Sie eine Warnung in als signifikant Health Log Analytics

Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. In Service Operations-Arbeitsbereich, Öffnen Sie ein Log Analytics Warnung und dann auswählen **ML-Feedback anwenden** > **Als signifikant markieren**an.
2. Bestätigen Sie die Aktion im Dialogfeld.

   Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

3. **Wahlweise:** Stellen Sie die signifikante Warnung wieder her.
   Wenn Sie nicht mehr möchten, dass die signifikante Warnung besonders behandelt wird, können Sie die normale Relevanz der Warnungsmetrik wiederherstellen. Weitere Informationen finden Sie unter Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics.

Schalten Sie eine unwichtige Warnung in stumm Health Log Analytics

Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie eine Warnung stummschalten, die auf der Stichwortmetrik oder der Musterschweregradmetrik basiert, schaltet das System die Metrik im dominanten Muster stumm. Das dominante Muster ist das Hauptmuster, das die Anomalie hervorruft.
Nur für die angegebene Quelle werden bei anomalem Verhalten für die Metrik, die der stummgeschalteten Warnung zugeordnet ist, keine Warnungen mehr generiert. Sie können auch die Metrik stummschalten, die einer unwichtigen Warnung für alle Komponenten des Anwendungsservice zugeordnet ist. Eine Komponente kann mehrere CIs sein, die dieselbe Funktion ausführen.

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereich die Log Analytics-Warnung, die Sie nicht mehr sehen möchten.
2. Auswahlvorgang **ML-Feedback anwenden**
3. Schalten Sie die Metrik, die der Warnung zugeordnet ist, stumm, indem Sie einen der folgenden Schritte ausführen:
   - Wählen Sie Aus **Warnungsmetrik stummschalten** Dient zum Stummschalten der Metrik nur für die angegebene Quelle.
   - Wählen Sie Aus **Warnungsmetrik für alle Komponenten stummschalten** Zum Stummschalten der Metrik für alle Komponenten des Anwendungsservice.
4. Bestätigen Sie die Aktion im Dialogfeld.

   Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Stellen Sie die stummgeschaltete Warnung wieder her.
   Wenn Sie nicht mehr möchten, dass die stummgeschaltete Warnung besonders behandelt wird, können Sie die normale Relevanz der Warnungsmetrik wiederherstellen. Weitere Informationen finden Sie unter Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics.

Zugehörige Informationen

Zeigen Sie die Liste der stummgeschalteten Metriken in an Health Log Analytics

Verringern Sie die Empfindlichkeit gegenüber ähnlichen Anomalien in Health Log Analytics

Machen Sie die Anomalieerkennung weniger empfindlich auf Anomalien wie die, die den aktuellen Auslöser ausgelöst haben Log Analytics Warnung.

Vorbereitungen

Hinweis: Diese Funktionalität ist für Kundenwarnungen und Warnungen hinsichtlich neuer Signale nicht verfügbar.

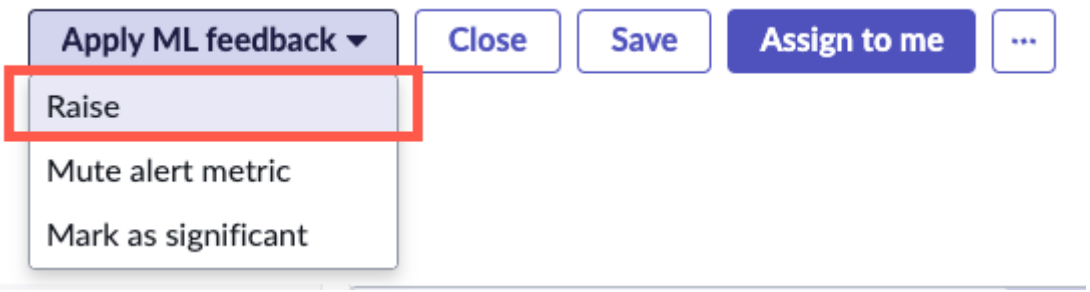
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch Auswahl der Option „Raise“ (Erhöhen) wird der Rückmeldungsschwellenwert für die Generierung von Warnungen erhöht, wenn von Health Log Analytics zukünftige Anomalien identifiziert werden, die derjenigen ähneln, die zu dieser Warnung geführt hat.

Prozedur

1. In Service Operations-Arbeitsbereich, Öffnen Sie ein Log Analytics Warnung und dann auswählen **ML-Feedback anwenden** > **Erhöhen**an.



2. Bestätigen Sie die Aktion im Dialogfeld.

   Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

3. **Wahlweise:** Stellen Sie die normale Sensitivität gegenüber Anomalien wie derjenigen wieder her, durch die diese Warnung ausgelöst wurde.

   a. Wählen Sie beim Anzeigen der Warnung **Feedback entfernen** aus.

   b. Bestätigen Sie die Aktion im Dialogfeld.

Stellen Sie die normale Wichtigkeit einer Warnungsmetrik in wieder her Health Log Analytics

Stellen Sie die normale Signifikanz der Metrik wieder her, die an der Generierung einer Log Analytics-Warnung beteiligt ist. Verwenden Sie diese Option, wenn eine Warnung nicht mehr besonders behandelt werden soll, die stummgeschaltet, als signifikant markiert oder deren Sensitivität gegenüber ähnlichen Anomalien verringert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Beim Anzeigen von Log Analytics Warnung in Service Operations-Arbeitsbereich, Wählen Sie aus **ML-Feedback wiederherstellen** .
2. Bestätigen Sie die Aktion im Dialogfeld.

Ergebnis

Die Metrik, die der Warnung zugeordnet ist, nimmt wieder ihre normale Relevanz an.

Dashboards für die Echtzeitvisualisierung von Protokolldaten in Health Log Analytics

Health Log Analytics ermöglicht Ihnen die Erstellung von Protokolldaten-Dashboards und -visualisierungen in Echtzeit für eine verbesserte Datenüberwachung und eine schnellere Identifizierung von Abweichungen.

Protokolldaten-Dashboards und -visualisierungen können Ihnen ein allgemeines visuelles Verständnis wichtiger Probleme vermitteln, wenn sie im System auftreten. Die Health Log Analytics-Datenquelle Ihrer Wahl wird dazu verwendet, die für die Visualisierung bereitgestellten Daten zu erfassen. Die Protokolldaten werden direkt aus den gespeicherten Protokollen übernommen, sodass Sie Dashboards für jeden Aspekt der Daten erstellen können, der Sie interessiert. Durch die Visualisierung der Komponenten, von denen Protokolle generiert werden, erhalten Sie beispielsweise einen Hinweis auf die Anzahl der vollständig integrierten Komponenten.

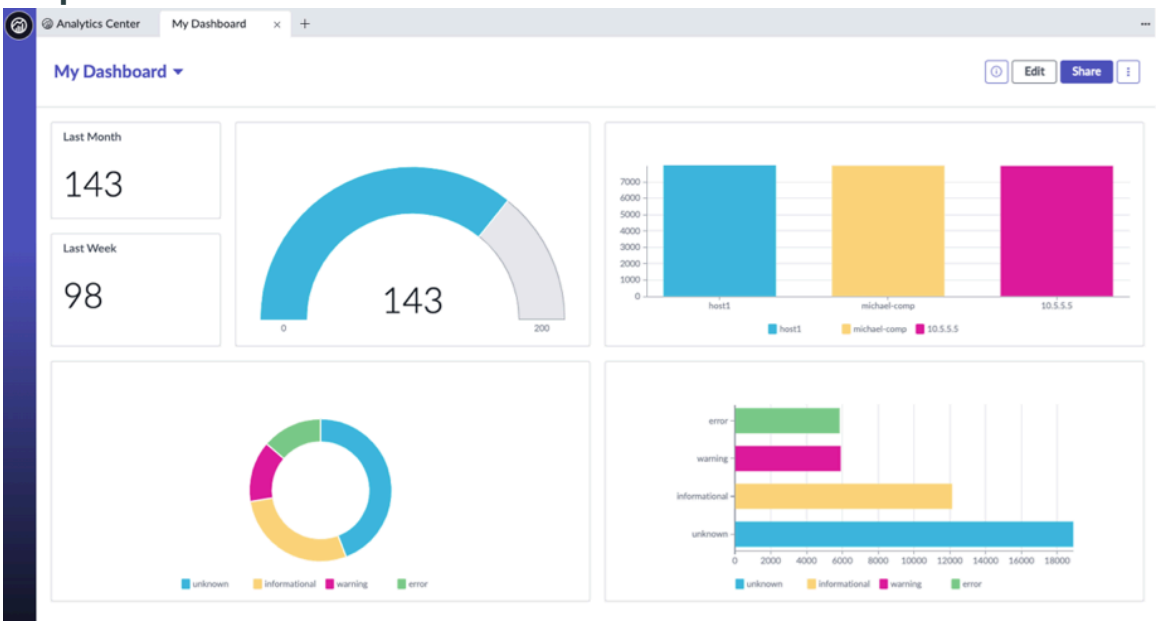
Die Daten können in verschiedenen Arten von Grafiken und Diagrammen dargestellt werden. Sie können den Zeitbereich und die anderen Einstellungen der Visualisierung nach Bedarf anpassen.

Diese Funktionalität wird in unterstützt Service Operations-Arbeitsbereich Log Analytics Anwendung, Version 21.2.7 – November 2022 und höher, und hat eine Abhängigkeit vom Platform Analytics-Arbeitsbereich, der über verfügbar ist ServiceNow Store .

Als Alternative zum Definieren Ihres eigenen Dashboards können Sie die AIOps-Dashboards verwenden, die umfassende Visualisierungen kritischer Betriebsdaten bieten. Weitere Informationen finden Sie unter AIOps-Dashboards in Service Operations-Arbeitsbereich Für ITOM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für ein Protokolldaten-Dashboard



Erstellen Sie Protokolldaten-Dashboards und Visualisierungen in Health Log Analytics

Erstellen Sie Dashboards und Visualisierungen für Health Log Analytics-Protokolldaten in Echtzeit, um Probleme leichter zu identifizieren und zu verstehen.

Vorbereitungen

Diese Funktionalität wird in unterstützt Service Operations-Arbeitsbereich Log Analytics Anwendung, Version 21.2.7 – November 2022 und höher, und hat eine Abhängigkeit vom Platform Analytics-Arbeitsbereich, der über verfügbar ist ServiceNow Store .

Detaillierte Informationen zum Erstellen und Arbeiten mit Dashboards finden Sie unter Dashboards im Analytics Center .

Hinweis: Als Alternative zum Definieren Ihres eigenen Dashboards können Sie die AIOps-Dashboards verwenden, die umfassende Visualisierungen kritischer Betriebsdaten bieten. Weitere Informationen finden Sie unter AIOps-Dashboards in Service Operations-Arbeitsbereich Für ITOM.

Erforderliche Rolle: evt_mgmt_operator oder viz_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Platform Analytics-Arbeitsbereich**an.
2. Wählen Sie auf der Seite Analytics Center die Registerkarte **Dashboards** aus.
   Auf dieser Registerkarte können Sie alle Dashboards anzeigen, für die Sie in Ihrer Instanz Zugriffsrechte haben. Sie können die Dashboard-Kacheln filtern, um die Anzahl der sichtbaren Elemente zu begrenzen.

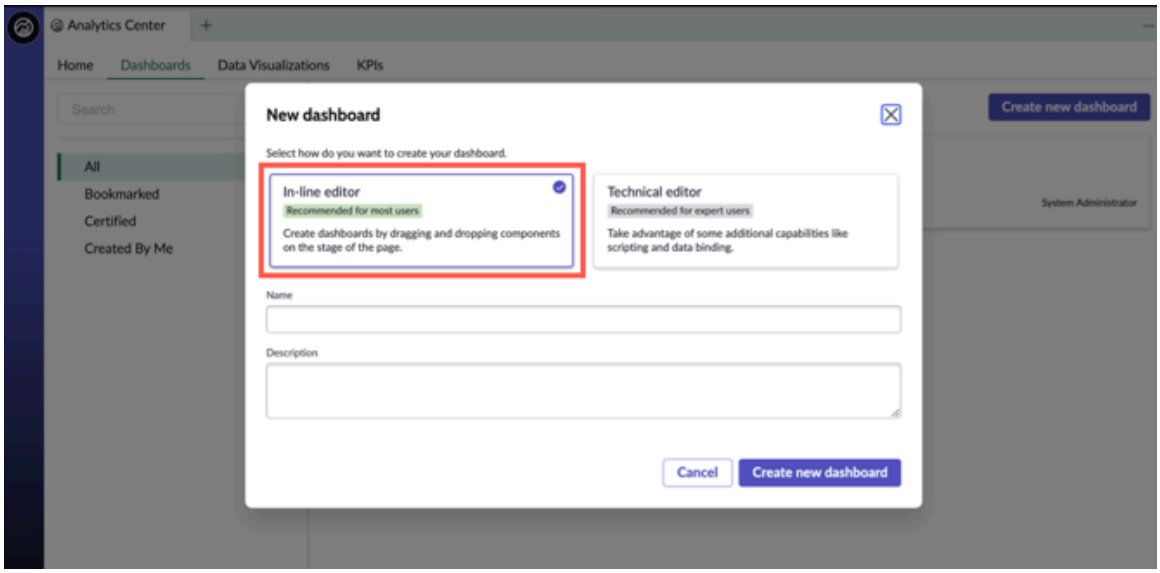
   Hinweis: Wenn Sie ein vorhandenes Dashboard verwenden möchten, wählen Sie das Dashboard hier aus, um es zu öffnen. Erstellen Sie andernfalls ein Dashboard, wie im weiteren Verlauf dieses Verfahrens beschrieben.

3. Erstellen Sie ein Dashboard.
   a. Wählen Sie **Neues Dashboard erstellen** aus.
   b. Wählen Sie im Dialogfeld „Neues Dashboard“ die Option **Inline-Editor** aus, und geben Sie einen Namen und eine optionale Beschreibung für das Dashboard an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Vom Inline-Editor wird Ihre Arbeit nicht automatisch gespeichert. Achten Sie darauf, dass Sie die Arbeit regelmäßig speichern.



c. Wählen Sie **Neues Dashboard erstellen** aus.

4. Fügen Sie dem Dashboard ein Element hinzu.
Es stehen verschiedene Elemente zur Verfügung, mit denen Sie die Informationen im Dashboard organisieren und ausfüllen können. Weitere Informationen finden Sie unter Analytics Center-Dashboard-Elemente .

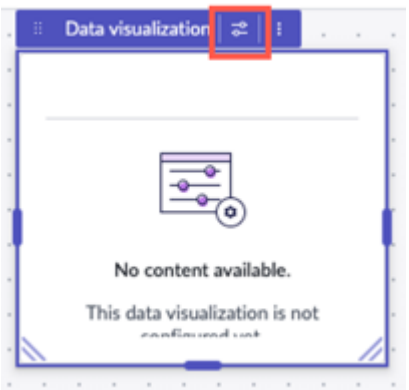
a. Wählen Sie **Neues Element hinzufügen** aus.

b. Wählen Sie aus den verfügbaren Elementen die Option **Datenvisualisierung** aus.
Das Element **Datenvisualisierung** wird im Dashboard angezeigt und kann dort bearbeitet werden.

Hinweis: Sie können auf die Ecken des Elements klicken und daran ziehen, um die Größe zu ändern.

5. Bearbeiten Sie das Element.

a. Wählen Sie auf dem Element das Symbol für Einstellungen aus:



Das Konfigurationsfenster wird geöffnet.

Automatische Übersetzung

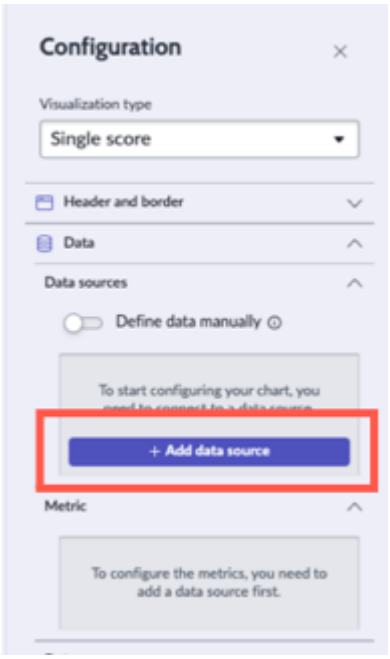
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie aus der Liste **Visualisierungstyp** den Typ der visuellen Darstellung aus, die Sie für die Protokolldaten wünschen.
Sie können aus verschiedenen Arten von Grafiken und Diagrammen auswählen.

Detaillierte Informationen finden Sie unter Datenvisualisierungen im Analytics Center .

c. Wählen Sie im Abschnitt „Daten“ die Option **+ Datenquelle hinzufügen** aus.

Die Health Log Analytics-Datenquelle, die Sie auswählen, wird dazu verwendet, die für die Visualisierung bereitgestellten Protokolldaten zu erfassen.



d. Wählen Sie aus Health Log Analytics Datenquelle für Protokollkomponenten.

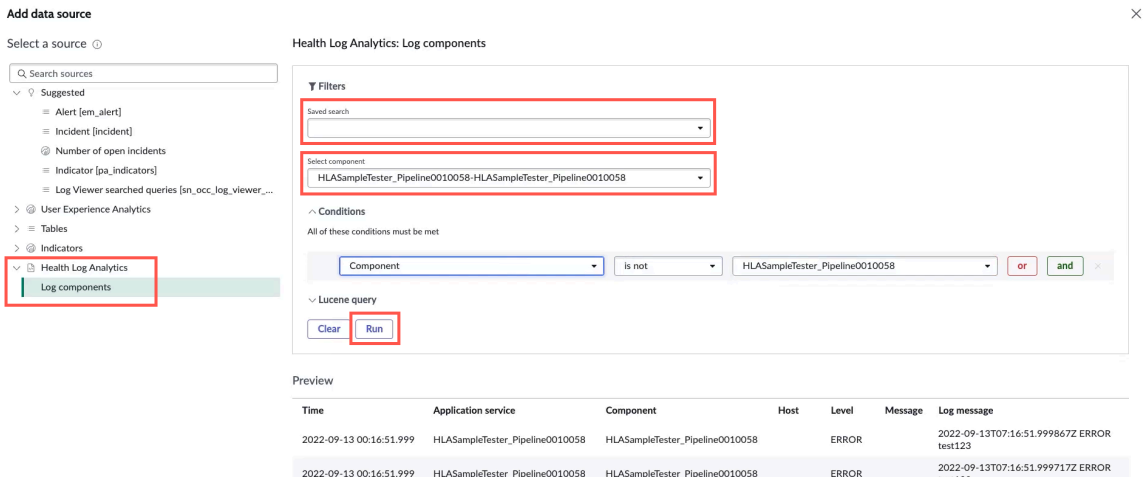
e. Wählen Sie die erforderliche Datenquelle aus diesen Optionen aus:

- Gespeicherte Suchen: Eine Liste aller Suchvorgänge, die Sie im Protokoll-Viewer gespeichert haben.
- Komponente auswählen: Eine Liste aller Komponenten, an die Daten gestreamt werden Health Log Analytics.

f. Verwenden Sie Bedingungen, eine Lucene-Abfrage oder beides, um das Datensegment anzugeben, an dem Sie interessiert sind, und wählen Sie dann aus **Ausführen** .

Automatische Übersetzung

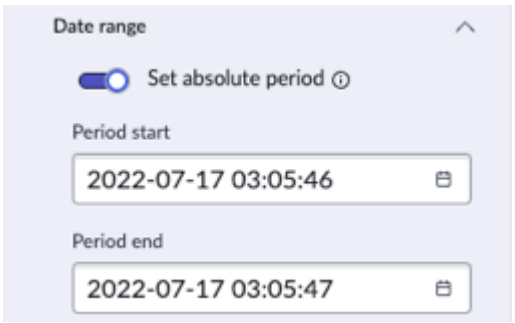
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Wählen Sie **Diese Quelle hinzufügen** aus, um die ausgewählte Health Log Analytics-Datenquelle hinzuzufügen.
Die angegebene Visualisierung wird in angezeigt **Datenvisualisierung** Element.

h. Wahlweise: Legen Sie feste Start- und Enddaten fest, um den Zeitbereich der angezeigten Daten anzupassen.

(Optional)



i. Wählen Sie im Abschnitt „Datumsbereich“ die Option **Absoluten Zeitraum festlegen** aus.

ii. Geben Sie das Start- und Enddatum für den absoluten Zeitraum in den entsprechenden Kalendern an.

i. Wahlweise: Passen Sie die anderen Einstellungen der Visualisierung nach Bedarf an.

(Optional) Um detaillierte Informationen zu den Einstellungen für alle Visualisierungstypen zu erhalten, wählen Sie den Link für den entsprechenden Typ in aus Datenvisualisierungen im Analytics Center .

j. Wahlweise: Fügen Sie nach Bedarf weitere Elemente hinzu.

k. Wählen Sie **Speichern** aus, um die Änderungen zu speichern, und setzen Sie die Bearbeitung fort.

l. Wählen Sie **Bearbeitungsmodus beenden** aus, um die Bearbeitung zu beenden und das Dashboard anzuzeigen.

Zugehörige Informationen

Geben Sie ein frei Platform Analytics Dashboard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie visualisierte Protokolldaten in einem vordefinierten Dashboard in Health Log Analytics

Verwenden Sie Visualisierungen, um Protokolldaten im integrierten operativen Dashboard in zu überwachen Service Operations-Arbeitsbereich Log Analytics Und behandeln Probleme, wenn sie im System auftreten.

Vorbereitungen

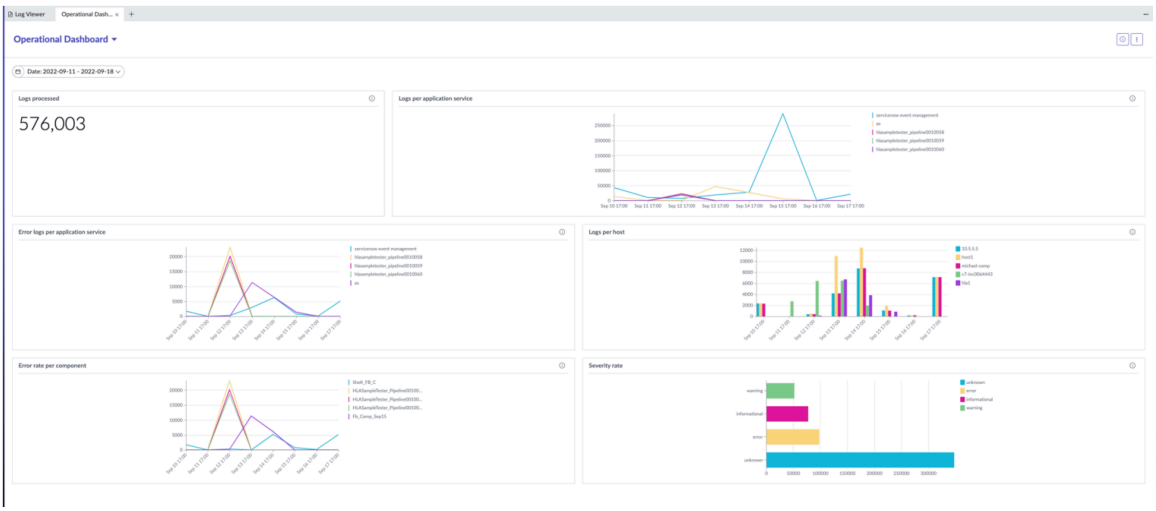
Erforderliche Rolle: evt_mgmt_operator oder viz_admin

Wichtig: Ab dem Vancouver-Release ist diese Funktion veraltet und durch AIOps ersetzt Dashboard „HLA-Betrieb“. Weitere Informationen zu AIOps-Dashboards finden Sie unter AIOps-Dashboards in Service Operations-Arbeitsbereich Für ITOM. Sie können auch ein anwenderdefiniertes Dashboard nach Ihren Anforderungen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Protokolldaten-Dashboards und Visualisierungen in Health Log Analytics.

Prozedur

1. Öffnen Sie **Protokoll-Viewer** Mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** Und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Beim Anzeigen von Protokolleinträgen für eine Warnung auf dem **Umgebende Protokolle** Wählen Sie die Registerkarte aus **Protokoll-Viewer** .
2. Wählen Sie das Auswahlsymbol oben rechts im aus **Protokoll-Viewer** Registerkarte und wählen Sie dann aus **Verwalten Sie meine Dashboards** Aus der Dropdown-Liste.
   Die **Operatives Dashboard** Die Registerkarte wird angezeigt.

   Standardmäßig visualisiert das Dashboard Protokolldaten, die in den letzten 24 Stunden erfasst wurden.



3. **Wahlweise:** Ändern Sie den Zeitbereich, für den Daten angezeigt werden, indem Sie den erforderlichen Bereich aus auswählen **Datum** Dropdown-Liste.
   Sie können einen anwenderdefinierten Bereich angeben, indem Sie auswählen **Anwenderdefiniert** Und wählen Sie dann die erforderlichen Start- und Enddaten aus.
4. Überwachen Sie die visualisierten Protokolldaten, und verwenden Sie sie, um Probleme zu identifizieren und zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard für Vorgänge

Name	Beschreibung	Verwendung der Daten
Verarbeitete Protokolle	Die Anzahl der Protokolle, die im ausgewählten Zeitraum verarbeitet und analysiert wurden.	Stellen Sie sicher, dass die Protokolldaten wie erwartet gestreamt werden.
Protokolle pro Anwendungsservice	Die Anzahl der Protokolle, die für jeden Anwendungsservice im ausgewählten Zeitraum gestreamt wurden.	Stellen Sie sicher, dass Protokolldaten wie erwartet für jeden Anwendungsservice gestreamt werden.
Fehlerrate pro Anwendungsservice	Die Anzahl der Protokolle mit Fehlern für jeden Anwendungsservice im ausgewählten Zeitraum. **Hinweis:** Health Log Analytics Erstellt automatisch Warnungen für Fehleranomalien.	Identifizieren Sie Fehler in den Protokollen.
Protokolle pro Host	Die Anzahl der verarbeiteten Protokolle für jeden Host im ausgewählten Zeitraum.	Identifizieren Sie Hosts, die mehr oder weniger Daten protokollieren als erwartet.
Fehlerrate pro Komponente	Die Anzahl der Protokolle mit Fehlern für jede Komponente im ausgewählten Zeitraum.	Stellen Sie sicher, dass die Komponenten eine normale Fehlerrate aufweisen.
Schweregrad	Die Schweregradstufe-Rate der Protokolle für die Streaming-Quellen.	Stellen Sie sicher, dass die Raten für Kritisch- und Fehlerniveaus den Erwartungen entsprechen.

KB-Artikel einer Log Analytics-Warnung hinzufügen

Fügen Sie Ihren eigenen KB-Artikel (Knowledge Base) einer Warnung hinzu, die von Health Log Analytics generiert wurde. Sie können beispielsweise zusätzliche Informationen angeben, die zur Lösung des zugrunde liegenden Problems beitragen können.

Vorbereitungen

Diese Funktion wird in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, und in der Anwendung Health Log Analytics Viewer, Version 21.0.0 – Dezember 2021 und später, unterstützt. Diese Anwendungen sind im ServiceNow Store verfügbar.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie eine Log Analytics-Warnung.
   a. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.
   b. Wählen Sie die entsprechende Liste in der untergeordneten Liste „Warnungen“ aus, und navigieren Sie zu der gewünschten Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Liste **Alle Warnungen** weisen alle von Health Log Analytics generierten Warnungen in der Spalte **Quelle** den Wert **Log Analytics** auf.

c. Wählen Sie die Warnungsnummer aus.

2. Wählen Sie oben rechts auf der Registerkarte **Details** das Symbol für weitere Aktionen ( ) und dann in der Liste die Option **Create KB article for this issue** (KB-Artikel für dieses Problem erstellen) aus.
3. Füllen Sie die Felder des Formulars aus.

Formular „Neues Wissen erstellen“

Feld	Beschreibung
Knowledge Base	Die Knowledge Base, in der der neue KB-Artikel gespeichert wird. Standardmäßig ist dieser Wert die Health Log Analytics-Knowledge Base.
Workflow	(Schreibgeschützt) Der Status des KB-Artikels. Wenn Sie den Artikel veröffentlichen, ändert sich sein Status automatisch von „Entwurf“ in „Veröffentlicht“.
Kategorie	Die Kategorie der Komponente, die die Warnung verursacht hat.
Kurzbeschreibung	Zusammenfassung des KB-Artikels.
Artikeltext	Inhalt des KB-Artikels.

4. Wählen Sie **Speichern**.
5. Wenn der Inhalt des Artikels endgültig ist, wählen Sie **Veröffentlichen** aus.

Ergebnis

Der KB-Artikel wird der ausgewählten Warnung hinzugefügt. Sie können den artikel in suchen und anzeigen Agent Assist Seitenbereich. Health Log Analytics Verwendet Ihren artikel auch, um ähnliche Warnungen mit derselben Ereignis-ID-Eigenschaft oder demselben Warnungsmuster zu verbessern.

Service Operations-Arbeitsbereich Für ITOM Referenz

Referenzthemen enthalten zusätzliche Informationen zu ServiceNow Service Operations-Arbeitsbereich.

Mit AIOps-Experience installierte Komponenten

Bei der Aktivierung von werden verschiedene Arten von Komponenten installiert AIOps-Experience[sn_SOW_aiops] Anwendung, einschließlich Anwenderrolle und Plugins.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
evt_mgmt_user	Verwaltet den Warnungslebenszyklus und führt grundlegende Vorgänge wie das Anzeigen von Warnungen aus.	ITIL
evt_mgmt_operator	Verwaltet Warnungen, einschließlich Aufgaben wie Schließen und Bestätigen.	evt_mgmt_user
evt_Team_Operator	Verwaltet Ereignismanagement Vorgänge in einem bestimmten Team, wie in definiert **Zuweisungsgruppe** Feld. Mit dieser Rolle kann der Operator Warnungen ausschließlich für sein zugewiesenes Team lesen und schreiben. Darüber hinaus kann der Betreiber Konfigurationsänderungen für sein Team vornehmen, einschließlich Updates für Warnungsautomatisierung und das Integrations-Launchpad. **Hinweis:** Die Rolle „evt_Team_Operator“ muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keiner Gruppe zugeordnet ist, denen Warnungen zugewiesen sind, kann der Operator keine Warnungen sehen.	sn_sow_alert_rules.automation_create_nonglobal sn_sow_alert_rules.automation_delete_nonglobal
evt_mgmt_admin	Konfiguriert und richtet ein Ereignismanagement Eigenschaften und Regeln.	evt_mgmt_user und evt_mgmt_Operator

Installierte Plugins

Plugin	Beschreibung
Ereignismanagement [com.glideapp.itom.snac]	Bietet serviceorientierte Verfügbarkeit und überwacht Ereignisse über eine intuitive Konsole.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin	Beschreibung
Performance Analytics – Premium [Com.snc.PA.em]	Bietet sofort einsatzbereite Leistungskennzahlen (Key Performance Indicators, KPIs), um Ereignismanagementprozesse zu überwachen und zu verbessern. Beachten Sie, dass die Aktivierung dieses Plugins in Produktionsinstanzen möglicherweise eine separate erfordert Performance Analytics Lizenz.
Performance Analytics – Inhaltspaket – Ereignismanagement [com.snc.pa.premium]	Enthält sofort einsatzbereite Leistungskennzahlen (Key Performance Indicators, KPIs). Die Aktivierung dieses Plugins in Produktionsinstanzen erfordert möglicherweise eine separate Performance Analytics Lizenz.

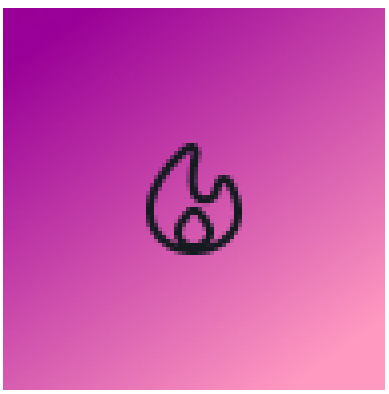
Informationen zur Rückkehr zum Verfahren finden Sie unter Installieren Service Operations-Arbeitsbereich Für ITOM Anwendung.

Attribute in Express-Liste Link-Ansicht

Die Tabelle listet die in der Linkansicht verfügbaren Knotenattribute mit ihrem Symbol und ihrer Beschreibung auf.

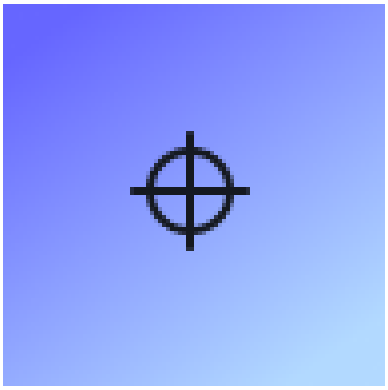
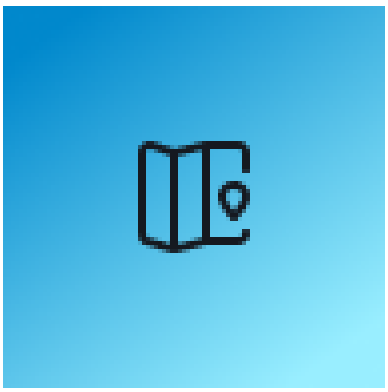
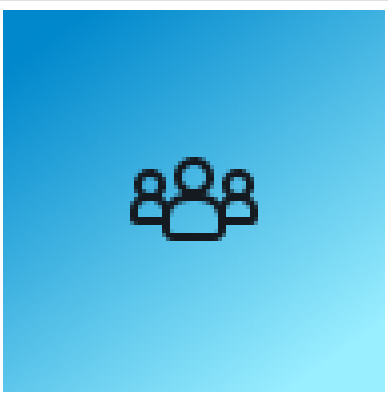
Hinweis: „Attribut“ ist ein generischer Begriff, der Felder und Tags darstellt, die in den Warnungen oder Konfigurationselementen (CI) gefunden wurden.

Attribute in der Linkansicht

Attributname	Symbol	Beschreibung
Betroffener Service		Service in Configuration Management Database (CMDB) Betroffen von einer Warnung für ein CI.
Ressource		Knotenressource, die für das Ereignis relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

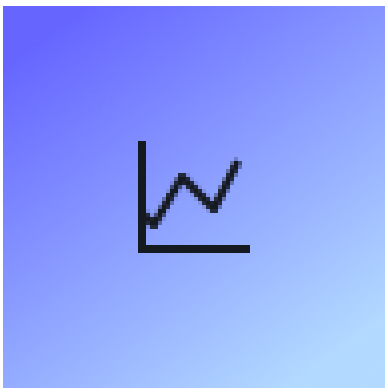
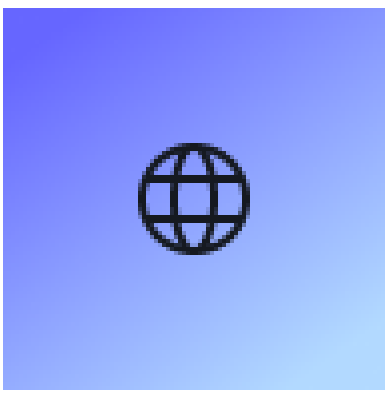
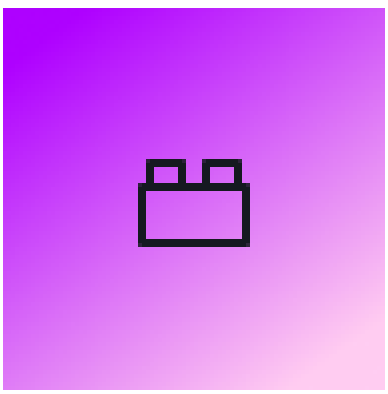
Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Quelle		Ereignisüberwachungssoftware, die das Ereignis generiert hat, z. B. SolarWinds Oder SCOM. Maximale Länge: 100 Zeichen
Region		Vordefiniertes Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Standort		Vordefiniertes Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Zuweisungsgruppe		Warnungszuweisungsgruppe.

Automatische Übersetzung

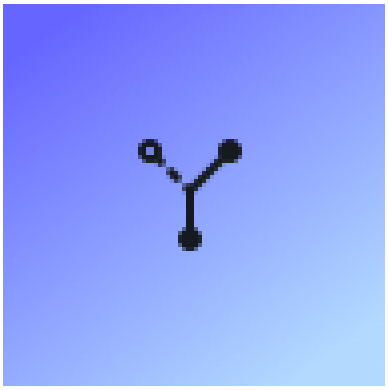
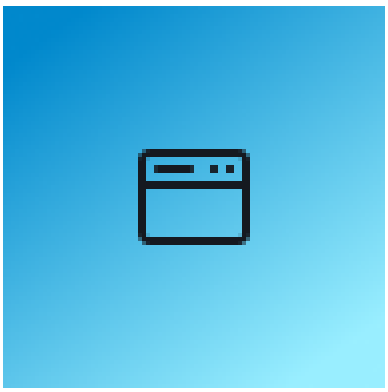
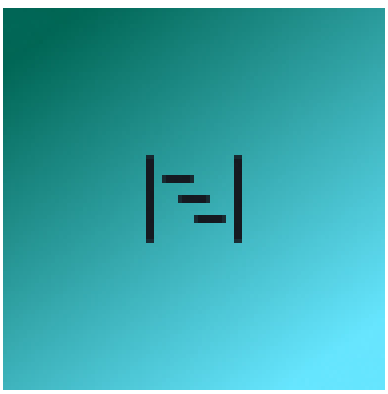
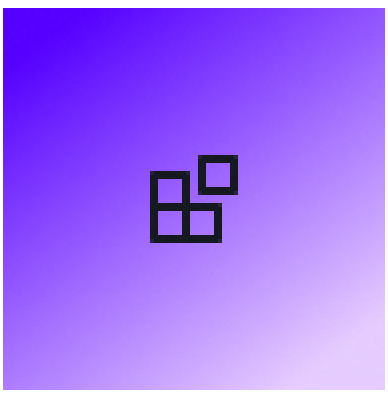
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Umgebung		Vordefiniertes Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Metrik		Eindeutiger Name, der beschreibt, welche Metrikdaten erfasst werden.
IP-Adresse		Vordefiniertes Attribut, das aus der Connector-Nutzlast extrahiert wurde.
CI		JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: {"name":"SAP ORA01","type":"Oracle"} ({"Name": "SAP ORA01", "Typ": "Oracle"}). Der CI-Bezeichner, der das Event generiert hat, wird im Feld Zusätzliche Informationen angezeigt. Maximale Länge: 1.000 Zeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

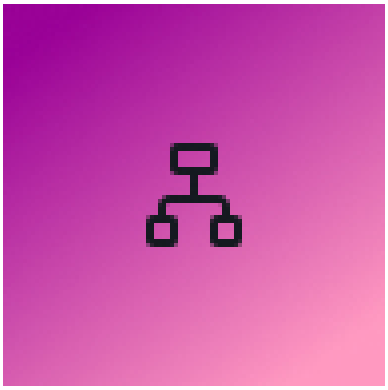
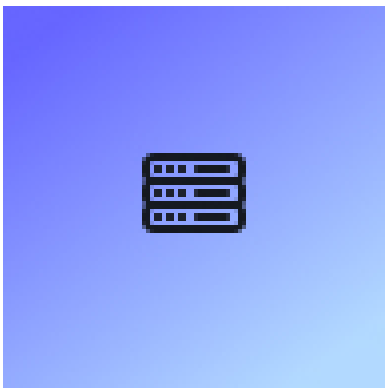
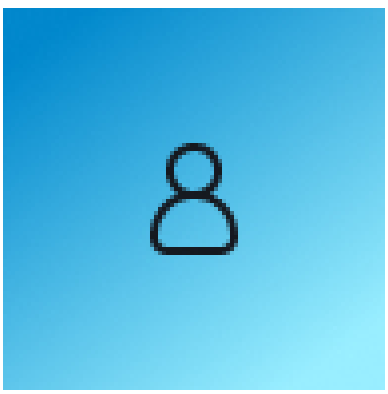
Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Knoten		Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, die dem Ereignis zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Anwendung		Vordefiniertes Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Prozess		Ein Prozess oder ein Cluster von Prozessen, die auf dem Host ausgeführt werden und von der horizontalen Discovery identifiziert werden.
Komponente		Ein logischer Teil einer Serviceinstanz, in der die Warnung erkannt wurde, wobei für jede untergeordnete Warnung eine Komponente angezeigt wird.

Automatische Übersetzung

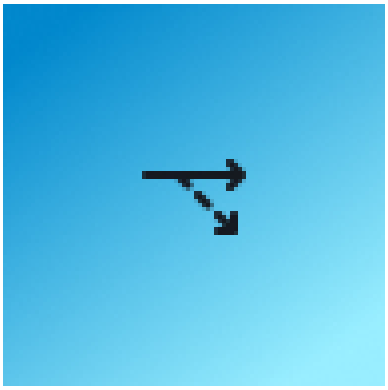
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Service		Attribut, das aus der Protokolldatei extrahiert wurde. Die Auswirkung dieser Warnung auf den Service ist möglicherweise nicht klar oder definiert.
Host		Attribut, das aus der Protokolldatei extrahiert wurde. Möglicherweise wurde sie in der CMBD nicht identifiziert.
Anwender		Attribut, das aus der Protokolldatei extrahiert wurde.
Account		Attribut, das aus der Protokolldatei extrahiert wurde.

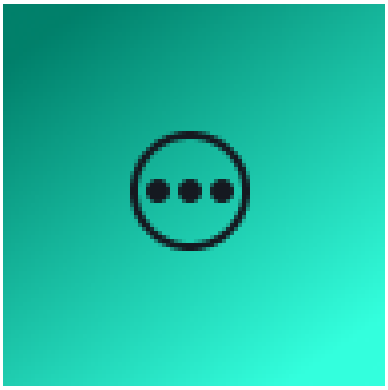
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Pfad		Pfad oder Route, der aus der Protokolldatei extrahiert wurde.
Anforderungs-ID		Die aus der Protokolldatei extrahierte Anforderungs-ID.
URL		Webadresse oder URL, die aus der Protokolldatei extrahiert wurde.
Erkennung		Eine identifizierte Anomalie für eine Metrik, gemessen von Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

Attributname	Symbol	Beschreibung
Sonstige **Hinweis:** Dieses Attribut ist anwenderdefiniert. Alle anderen Attribute sind im System vordefiniert.		Anwenderdefiniertes Attribut. **Hinweis:** Alle anderen Attribute sind im System vordefiniert.

Linien, die Attribute verknüpfen

Verknüpfung	Visuelle Darstellung	Beschreibung
Durchgezogene Linie		Durchgehende Linie, die Attribute in der Verknüpfungsansicht verknüpft, die angibt, dass die Attribute eine oder mehrere Warnungen teilen.
Gepunktete Linie		Gepunktete Linien, die Attribute in der Verknüpfungsansicht verknüpfen, die angeben, dass die Attribute durch Gruppierungskriterien korreliert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsfeldzuordnung auf der Antwortseite

Die Felder, die auf der Antwortseite konfiguriert werden sollen, wenn eine Aktion ausgewählt wird, die durch eine Warnungsautomatisierung ausgelöst werden soll.

Wählen Sie Felder für Automatisierungsaktionen aus

Feld	Beschreibung
Incident-Feldname	Name des Felds, das im Incident angezeigt wird.
Feld zuordnen	Option, die angibt, wie das Incident-Feld zugeordnet werden soll: • **Identisch mit** : Das ausgewählte Incident-Feld hat denselben Wert wie das angegebene Warnungsfeld. • **Bis** : Das ausgewählte Incident-Feld wird auf einen angegebenen Wert festgelegt.
Warnungsfeldwert	Wert, der im Warnungsfeld festgelegt wird: • Wenn Sie auswählen **Identisch mit** In der Spalte Zuordnungsfeld wird der Warnungsfeldwert, der im Feld Incident angezeigt werden soll, auch in der Spalte Incident-Feldname angezeigt. • Wenn Sie auswählen **Bis** Geben Sie in der Spalte Zuordnungsfeld den Warnungsfeldwert ein, der im angegebenen Incident-Feld angezeigt werden soll.

Informationen zur Rückkehr zum Verfahren finden Sie unter Erstellen Sie die Antwortautomatisierung.

Parameter für ausgehenden Webhook

Die Parameter, die beim Senden von Daten an andere Systeme mithilfe eines ausgehenden Webhooks konfiguriert werden sollen.

Parameter für ausgehenden Webhook

Parameter	Definition
Ziel-URL-Feld	Der Webhook-Endpunkt (URL), an den die Warnung gesendet werden soll.
Registerkarte „JSON-Nutzlastdaten“	Die Warnungsdaten im JSON-Format, die an die angegebene URL gesendet werden. Geben Sie die Details ein, über die Sie benachrichtigt werden möchten, wenn die Automatisierung ausgelöst wird. Sie können Warnungsfelder einfügen, indem Sie auswählen **Feldwerte Einfügen** Oder fügen Sie anwenderdefinierte Felder hinzu, indem Sie {custom_field.JSON_path} eingeben. Um zusätzliche Warnungsfelder hinzuzufügen, wählen Sie aus **Warnungsfelder einfügen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für ausgehenden Webhook (Fortsetzung)

Parameter	Definition
Nutzlast-Header	Fügen Sie vordefinierte oder anwenderdefinierte Metadaten-Header in hinzu **Schlüssel** Und **Wert** Felder. Ein Schlüssel ist der Name eines Headerfelds, und ein Wert sind die entsprechenden Daten, die diesem Headerfeld zugewiesen sind.
Nutzlast testen	Wählen Sie diese Option aus, um sicherzustellen, dass der Webhook ordnungsgemäß funktioniert und das Empfangssystem die Daten wie erwartet verarbeiten kann.

Informationen zur Rückkehr zum Verfahren finden Sie unter Erstellen Sie die Antwortautomatisierung.

Detailseite für Anwendungsservice

Bietet umfassende Informationen zu einem Anwendungsservice, einschließlich Name, Geschäftsrelevanz, Besitzstand, Prozess- und Betriebsstatus, datenverkehrsbasierte Discovery-Details, Discovery-Status und relevante Kommentare. Dies ermöglicht eine gründliche Analyse des aktuellen Status und der Nutzung des Anwendungsservice, bietet Klarheit in Bezug auf Besitz und Relevanz und hilft bei der effektiven Priorisierung von Ressourcen und Aktionen.

Felder der Detailseite für Anwendungsservice

Feld	Beschreibung
Name	Name des Anwendungsservice.
Business-Relevanz	Wichtigkeitsebene des Service für den Geschäftsbetrieb.
Eigentum von	Person oder Team, die für die Verwaltung und Überwachung des Service verantwortlich ist.
Prozessstatus	Aktuelle Phase oder Status der operativen Prozesse des Service.
Betriebsstatus	Aktuelle Phase oder Bedingung der Betriebsprozesse des Service, die anzeigt, ob er reibungslos funktioniert oder Probleme auftreten.
Verkehrsbasierte Discovery	Option zum Identifizieren von Serviceinstanzen basierend auf Netzwerkverkehrsmustern.
Discovery-Status	Fähigkeit des Systems, den Service innerhalb seines Netzwerks zu finden und zu erkennen.
Kommentare	Zusätzliche Hinweise oder relevante Informationen zum Service, die beim Verständnis seiner Verwaltung oder Nutzung hilfreich sein können.

Informationen zur Rückkehr zum Verfahren finden Sie unter Zeigen Sie Anwendungsservicedetails in an Service Operations-Arbeitsbereich.

Erstellen Sie Listenfelder

Erstellen Sie anwenderdefinierte Listen mit Feldern, die auf Ihre Anforderungen zugeschnitten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das von Ihnen ausgefüllte Formular hängt davon ab, ob Sie Ihre Liste auf einem vorhandenen (**Von vorhandenem starten**) Oder eine neue Liste erstellen (**Erstellen Sie Ihre eigenen**).

Mit vorhandenem Formular beginnen

Feld	Beschreibung
Liste	Vorhandene Liste, die Sie ändern möchten.
Listenname	Name für Ihre Liste. Der Standardname in diesem Feld ist der Name der vorhandenen Liste in **Liste** Feld mit – Kopieren Angehängt.
Spalten auswählen	Datensatzfelder, die in die Listenansicht aufgenommen werden sollen. Die Spalten aus der ausgewählten Liste werden angezeigt. Sie können Spalten hinzufügen oder entfernen, um die Liste zu ändern.
Filter hinzufügen	Bedingung zum Filtern der Liste. Standardmäßig werden die auf die ausgewählte Liste angewendeten Bedingungen angezeigt. Sie können diese Bedingung ändern.

Erstellen Sie Ihr eigenes Formular

Feld	Beschreibung
Listenname	Name für Ihre Liste.
Quelle auswählen	Quelltabelle für die Datensätze.
Spalten auswählen	Die Spalten, die in der Liste angezeigt werden sollen. Dieses Feld wird mit Spalten aus einer Arbeitsbereichslistenansicht gefüllt, falls vorhanden. Wenn keine Arbeitsbereichsliste vorhanden ist, werden die Spalten mit der Listenansicht Standard der ausgewählten Tabelle ausgefüllt.
Filter hinzufügen	Bedingung zum Filtern der Liste.

Informationen zur Rückkehr zum Verfahren finden Sie unter Erstellen Sie eine Liste in Service Operations-Arbeitsbereich Für ITOM

Formularfelder „Konfiguration der Metrikansicht“

Definieren Sie, wie Metriken in angezeigt werden Service Operations-Arbeitsbereich.

Formular „Konfiguration der Metrikansicht“

Feld	Beschreibung
Titel	Name der Metrik
Aktiv	Option zum Aktivieren der Metrik.
Reihenfolge	Numerischer Wert, der die Reihenfolge der Metriken auf der Seite angibt.
Configuration Item-Typ	Typ des Konfigurationselements. Verfügbare Optionen sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfiguration der Metrikansicht“ (Fortsetzung)

Feld	Beschreibung
	• cmdb_ci_app_server_tomcat • cmdb_ci_metric_extension • cmdb_ci_app_win_server
Quellmetriktypen	Metriktypen, die von der Metrik überwacht werden sollen. Klicken Sie auf das Schlosssymbol ( ), um die Liste der Quellmetriktypen zu entsperren und die zu überwachenden Metriktypen auszuwählen.
Diagrammtyp	Typ des Diagramms, in dem die Metrik angezeigt wird Service Operations-Arbeitsbereich, Auch **Position** Oder **Gestapelter Balken** .

Informationen zur Rückkehr zum Verfahren finden Sie unter Warnungsmetriken konfigurieren.

Integrations- und Konfigurationsintegritätsereignisfelder

Füllen Sie die Ereignisfelder aus, um Details wie Ereigniszeit, Beschreibung, Warnungsnummer, Status, Schweregrad zu erfassen. Metrikname, Knoten, Nachrichtenschlüssel und Fehlermeldung, um eine präzise Nachverfolgung zu ermöglichen effektives Incident-Management und verbesserte Fehleranalyse.

Ereignisfelder

Feld	Beschreibung
Zeit des Ereignisses	Gibt an, wann das Ereignis aufgetreten ist.
Beschreibung	Stellt Details zum Ereignis oder Incident bereit.
Warnung	Gibt die Warnungsnummer an, die basierend auf dem Ereignis ausgelöst wird.
Status	Beschreibt den aktuellen Status des Ereignisses (z. B. Offen, Geschlossen).
Schweregrad	Gibt den Schweregrad des Ereignisses an (z. B. Kritisch, Warnung).
Metrikname	Gibt die spezifische Metrik an, die dem Ereignis zugeordnet ist.
Knoten	Gibt den Knoten oder das Gerät im Zusammenhang mit dem Ereignis an.
Nachrichtenschlüssel	Eindeutiger Bezeichner für die Ereignisnachricht.
Fehlermeldung	Stellt zusätzliche Informationen zu Fehlern bereit, die dem Ereignis zugeordnet sind.

Informationen zur Rückkehr zum Verfahren finden Sie unter Überprüfen Sie die Integrations- und Konfigurationsintegrität.

Connector-Felder abrufen

Füllen Sie die Felder für erweiterte Einstellungen des Pull-Connectors aus, um den Ereignisabruf und die Synchronisierung basierend auf bestimmten Anforderungen wie Verbindungseinstellungen, Ereignishäufigkeit und Zeitzoneneinstellungen zu optimieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für erweiterte Einstellungen

Feld	Beschreibung
Verbundener MID-Server	Legen Sie fest, ob das System die optimale auswählen soll MID-Server Oder wählen Sie ein bestimmtes aus MID-Server Selbst. Führen Sie nur aus, wenn Sie Änderungen an vornehmen müssen MID-Server Andernfalls lassen Sie es leer, und lassen Sie das System das Optimum auswählen MID-Server.
Zeitplan für Eventsammlung (Sekunden)	Geben Sie die Häufigkeit in Sekunden ein, die angibt, wie oft das System nach neuen Ereignissen aus der externen Ereignisquelle suchen soll. Der Wert darf nicht niedriger sein als die minimale Zeitplaneigenschaft, die standardmäßig 120 Sekunden beträgt.
Protokoll	Definiert das Kommunikationsprotokoll, das zum Abrufen von Ereignissen von externen Geräten verwendet wird.
Schweregrad_by_State_type	Bestimmt den Schweregrad, der Ereignissen basierend auf ihrem Statustyp zugewiesen ist.
time_zone	Gibt die Zeitzone an, die für die Aufzeichnung und Anzeige von Ereigniszeitstempeln verwendet wird.
offset_min	Legt den Zeitversatz für den Ereignisabruf fest, um eine genaue Synchronisierung sicherzustellen.
Port	Überprüfen Sie die Standardwerte für Ihren Connector-Typ, z. B. Portdetails oder Zeitformate, und ändern Sie sie nach Bedarf. Standardwerte aus Ihrem Connector sind ausgefüllt. Gibt die Portnummer an, die für die Kommunikation mit externen Geräten verwendet wird.
max_fetch_interval_min	Begrenzt das maximale Intervall zwischen Ereignisabrufvorgängen.
initial_sync_in_days	Legt die Dauer für den anfänglichen Synchronisierungsprozess beim Abrufen von Verlaufsdaten fest.

Informationen zur Rückkehr zum Verfahren finden Sie unter Konfigurieren Sie einen Ereignis-Pull-Connector.

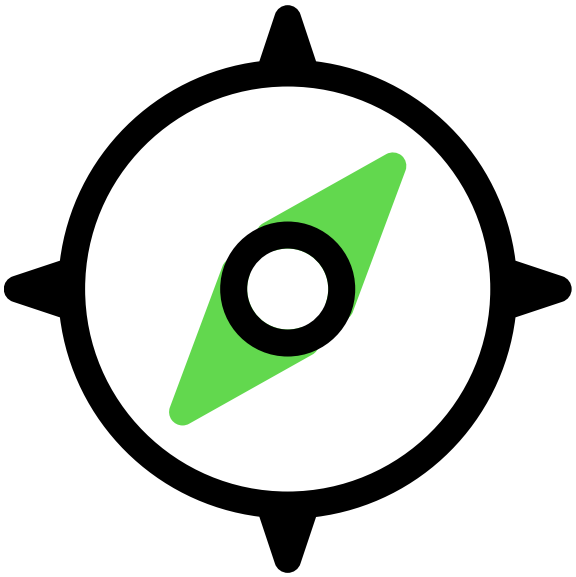
Synthetische Überwachung

Die ServiceNow®Synthetische Überwachung Mit der Anwendung können Unternehmen die Leistung und Verfügbarkeit kritischer Services proaktiv verwalten und verbessern. Durch die Simulation von Anwendertransaktionen auf API-Endpunkten identifiziert diese Lösung Leistungsengpässe, trägt zur Gewährleistung der Betriebszeit bei und optimiert die Anwender-Experience.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

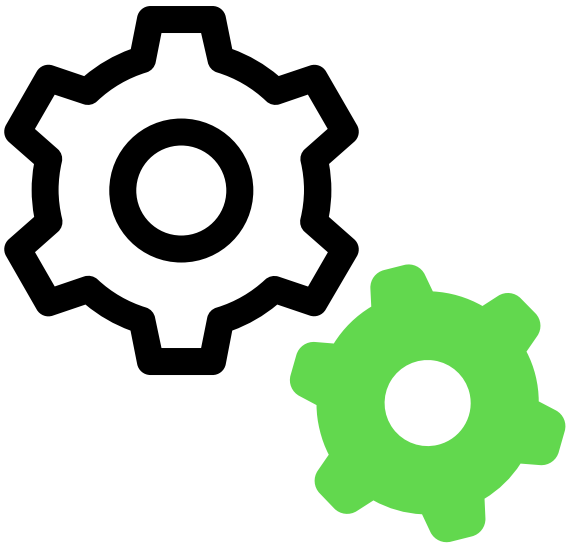
Erste Schritte

Untersuchen



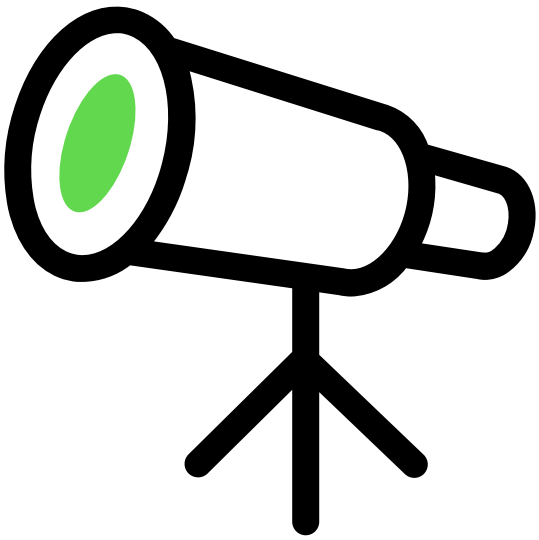
Erfahren Sie mehr über
Synthetische Überwachung

Konfigurieren



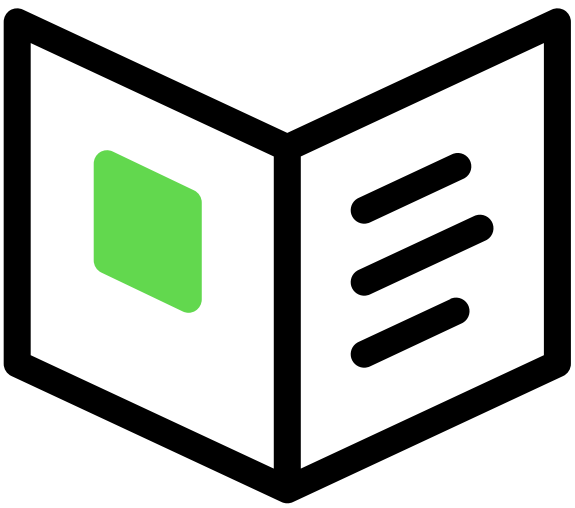
Fügen Sie Anwender hinzu, und erstellen
und verwalten Sie einen Synthetic-Monitor

Identifizieren



Verwenden Synthetische Überwachung
Um Leistungsprobleme zu identifizieren

Referenz



Suchen Sie Referenzinformationen
zu Synthetische Überwachung

Automatische Übersetzung

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow-Universität

Jetzt erstellen

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://www.servicenow.com

ServiceNow Store

ServiceNow Store

Support

- https://support.servicenow.com/now
- Known Error-Portal

Synthetische Überwachung erkunden

Erfahren Sie, wie Synthetische Überwachung Bietet proaktive, automatisierte Tests von Serviceendpunkten. Durch die Simulation von Anwenderinteraktionen kann die IT Fehler, Leistungsprobleme und Ausfälle identifizieren, bevor sie sich auf echte Anwender auswirken.

Synthetische Überwachung – Übersicht

Synthetic-Überwachungen rufen HTTP-Endpunkte in kontinuierlich auf Configuration Management Database (CMDB) Zum Testen der Verfügbarkeit, der Antwortzeiten oder des Vorhandenseins einer definierten Zeichenfolge im Antworttext. Wenn ein Test die konfigurierten Kriterien nicht erfüllt, kann er Sie vor Ihren Kunden vor Endpunktproblemen warnen.

Sie können beispielsweise einen Monitor erstellen, der den testet `ABRUFEN` HTTP-Endpunkt eines Service. Sie können diesen Monitor so konfigurieren, dass er nach einem Statuscode von 200 und einer Antwortzeit von weniger als 500 ms sucht. Wenn ein anderer Code als ist `200` Wird zurückgegeben oder die Anforderung dauert länger als 500 ms, der Test schlägt fehl. Eine Warnung kann dann generiert und gesendet werden Ereignismanagement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Synthetische Überwachung Tests können von ausgeführt werden Agent Client Collector(ACC) in Ihrem Netzwerk auf einem bereitgestellt MID-Server, Oder auf der ServiceNow Plattform.

Hinweis: Die HTTP-Endpunkte müssen in der Tabelle „HTTP-Endpunkte“ [cmdb_ci_endpoint_http] vorhanden sein. Endpunkte, die von getestet wurden ServiceNow Plattform muss öffentlich zugänglich sein.

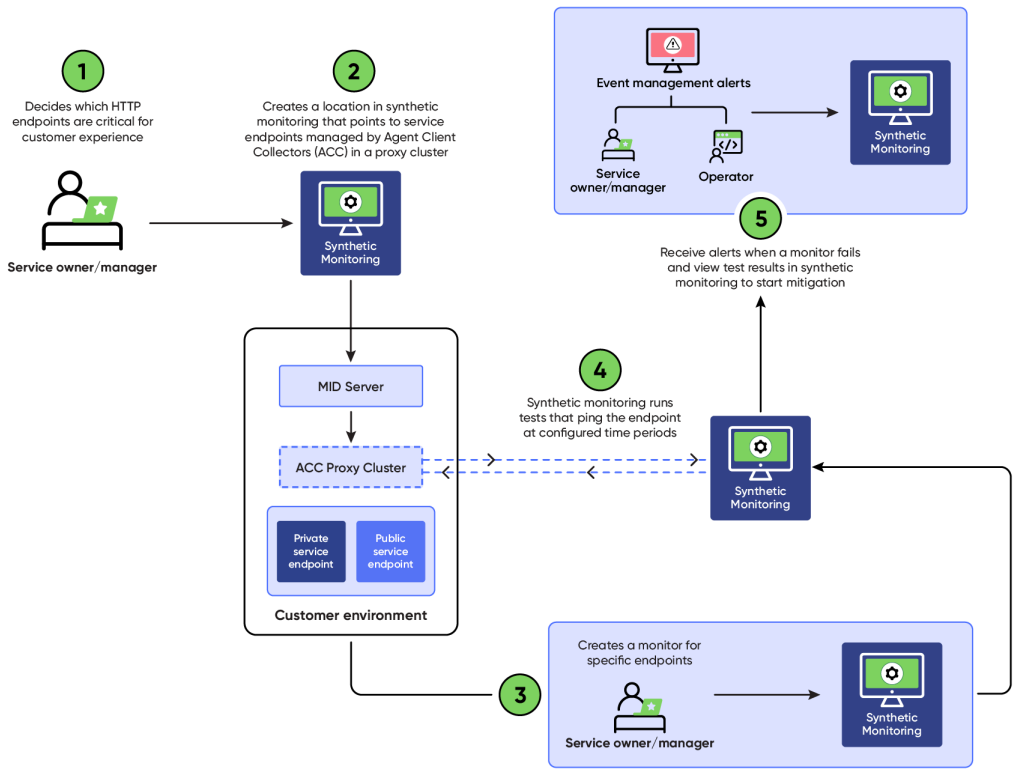
Synthetische Überwachung Anwender

Synthetische Überwachung Anwender

Anwender	Beschreibung
Synthetische Überwachung Administrator (Administratorrolle)	Weist Rollen zu, erstellt und bearbeitet Überwachungen und zeigt Überwachungstests und ihre Ergebnisse an.
Serviceverantwortlicher (Editorrolle)	Erstellt und bearbeitet Überwachungen und kann Überwachungstests und ihre Ergebnisse auch anzeigen.
Network Operations Center (NOC)-Operator (Viewer-Rolle)	Überwacht Tests und ihre Ergebnisse.

Synthetische Überwachung Vom Kunden gehosteter Workflow

Synthetic-Überwachungs-Workflow



Administratoren, Serviceverantwortliche und NOC-Operatoren verwenden Synthetische Überwachung Auf folgende Weise:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Als Serviceverantwortlicher bestimmen Sie basierend auf der Geschäftsrelevanz, welche Endpunkte überwacht werden sollen.
2. Als Administrator oder Serviceverantwortlicher konfigurieren Sie Standorte, von denen aus die Tests ausgeführt werden sollen.

   Hinweis: Die ServiceNow Der gehostete Standort ist standardmäßig verfügbar und muss nicht konfiguriert werden. Von diesem Standort getestete Endpunkte müssen jedoch öffentlich verfügbar sein.

3. Als Administrator oder Serviceverantwortlicher konfigurieren Sie den Monitor und überprüfen dann die Ergebnisse der vom Monitor gesendeten Tests. Wenn die Ergebnisse nicht erfolgreich sind, beheben Sie Probleme mit der Konfiguration. Sie können auch eine Warnung erstellen, die ausgelöst wird, wenn ein Test fehlschlägt.
4. Synthetische Überwachung Führt Tests basierend auf der Konfiguration des Monitors aus und meldet die Ergebnisse jedes Tests.
5. Als Serviceverantwortlicher oder -Betreiber überwachen Sie die Testergebnisse und reagieren auch auf generierte Warnungen. Sie können zugehörige Konfigurationselemente (Configuration Items, CIs) anzeigen, um mit der Selektierung des Problems zu beginnen, wenn ein Test fehlschlägt.

Synthetische Überwachung – Vorteile

Synthetische Überwachung – Vorteile

Vorteil	Funktion	Anwender
Zeigen Sie Informationen zur aggregierten Überwachung an. Zeigen Sie an Synthetische Überwachung Homepage, auf der Sie: • Sehen Sie sich eine Aggregatansicht aller Monitore an • Zeigen Sie den Status aller Monitore an. • Detailinformationen zu einem Monitor anzeigen	Zeigen Sie Aggregatinformationen zu den Monitoren an.	Operatoren, Serviceverantwortliche
Visualisieren Sie synthetische Testergebnisse. Zeigen Sie die Detailseite für einen Monitor an, auf dem Sie Folgendes sehen können: • Der Status und die Konfiguration des Monitors. • Diagramme, die den Testerfolg und die Antwortzeit anzeigen. • Ein Verlaufsprotokoll von synthetischen Testläufen, einschließlich Details und dem Antworttext.	Zeigen Sie einen Monitor und seine Tests an.	Operatoren, Serviceverantwortliche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Synthetische Überwachung – Vorteile (Fortsetzung)

Vorteil	Funktion	Anwender
Erhalten Sie Echtzeitbenachrichtigungen für Ausfälle, bevor sie sich auf Anwender auswirken.	Konfigurieren Sie optional Warnungen, wenn Tests nicht erfolgreich sind.	Operatoren, Serviceverantwortliche
Geben Sie Einblicke mit Stakeholdern frei.	Zeigen Sie Informationen zur aggregierten Überwachung an.	Operatoren, Serviceverantwortliche
Aktualisieren Sie Monitore entsprechend Ihren Geschäftsanforderungen.	Bearbeiten Sie vorhandene Monitore, einschließlich Deaktivierung .	Servicebesitzer

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Synthetische Überwachung finden Sie unter:

- Synthetische Überwachung konfigurieren
- Identifizieren von Systemproblemen mit Synthetische Überwachung
- Synthetische Überwachung – Referenz

Synthetische Überwachung konfigurieren

Planen und konfigurieren Sie Ihre Implementierung von Synthetische Überwachung.

Konfiguration – Übersicht

Synthetische Überwachung installieren

Sie können installieren Synthetische Überwachung Anwendung (`Com.snc.uib.SOW_synthetics`) Mit der Administratorrolle.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfung des folgenden Elements: Synthetische Überwachung Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.
- Bestätigen Sie, dass die Konfigurationselemente (Configuration Items, CI), die Sie überwachen möchten, in vorhanden sind CMDB Tabelle „HTTP-Endpunkte“ [cmdb_ci_endpoint_http].
- Bestätigen Sie, dass konfigurierte Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [Discovery_credentials] vorhanden sind, wenn Ihr Endpunkt eine Authentifizierung erfordert.

> **Hinweis:** Synthetische Überwachung Unterstützt nur API-Schlüssel-Anmeldeinformationen und Anmeldeinformationen für Standardauthentifizierung.

Erforderliche Rolle: sn_SOW_Synthetics.synthetics_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Synthetische Überwachung installiert:

- Plugins
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Mit Synthetische Überwachung installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach Synthetische Überwachung Anwendung (com.snc.uib.SOW_Synthetics) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installationsdetails überprüfen“ werden alle Abhängigkeiten aufgeführt, die zusammen mit Ihrer Anwendung installiert werden.
4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Nächste Maßnahme

Erstellen Synthetische Überwachung Standorte

Erstellen Synthetische Überwachung Standorte

Erstellen Sie einen Synthetische Überwachung Standort zum Ausführen einer Synthetic-Überwachung. Wenn Sie Überwachungen von ausführen möchten ServiceNow Glide-Instanz können Sie dieses Verfahren überspringen.

Vorbereitungen

Sie benötigen mindestens einen der folgenden Elemente:

- A MID-Server
- Mindestens eine Agent Client Collector(ACC)-Agent, der die Integrität und Leistung der zu überwachenden HTTP-Endpunkte mit überwacht Synthetische Überwachung. Wenn Sie Tests nur über ausführen möchten ServiceNow AI Platform, Sie müssen keinen Standort einrichten.

Hinweis:

- Wenn Ihr Synthetic Monitor einen privaten HTTP-Endpunkt testet, darf Ihr Standort nur ACC-Agents enthalten, die sich innerhalb derselben Netzwerkgrenzen wie der HTTP-Endpunkt befinden.
- Wenn Ihr Monitor einen HTTP-Endpunkt aus verschiedenen Rechenzentren, Cloud-Providern oder geografischen Regionen testet, muss für jeden ein anderer Standort verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_SOW_Synthetics.synthetics_admin

Warum und wann dieser Vorgang ausgeführt wird

Synthetic-Monitore können gehostet werden von:

- A MID-Server
- Ein Cluster von Agent Client Collector Service Desk-Mitarbeiter
- A ServiceNow Glide-Instanz, solange alle überwachten Endpunkte öffentlich verfügbar sind

Sie können beliebig viele Standorte erstellen, müssen jedoch mindestens einen Standort haben, um einen Synthetic-Monitor zu erstellen.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**an.
2. Navigieren zu **Setup der Synthetics-Überwachung** > **Verwalten Sie Standorte**an.
3. Wählen Sie Aus **Erstellen Sie einen neuen Standort** .
4. Erweitern Sie die Karte Standortdetails, und geben Sie einen eindeutigen Namen und eine optionale Beschreibung für diesen Standort ein.
   Die Beschreibung muss eindeutig angeben, wo die Server oder Service Desk-Mitarbeiter an diesem Standort ausgeführt werden. Beispiel: `US-1-East-Cluster` .
5. In **Standorttyp** Wählen Sie entweder aus **MID-Server** Oder **Agent Client Collector** , Abhängig davon, wo der Monitor gehostet werden soll .
6. Erweitern Sie **Wählen Sie Aus** Karte und wählen Sie eine oder mehrere aus MID Servers Oder ACC-Service Desk-Mitarbeiter.
7. Wählen Sie **Speichern**.

> **Hinweis:** Sie können Standorte aus dem Menü „Synthetic Locations“ löschen, zu dem Sie navigieren können, indem Sie auswählen **Alle** > **Synthetics-Überwachung** > **Synthetic-Standorte**an. Sie müssen jedoch zuerst alle an diesem Standort ausgeführten Monitore entfernen, indem Sie entweder die Monitore bearbeiten, um einen anderen Standort zu verwenden, oder die Monitore löschen. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic-Monitor.

Nächste Maßnahme

Erstellen und bearbeiten Sie einen Synthetic-Monitor

Erstellen und bearbeiten Sie einen Synthetic-Monitor

Erstellen oder bearbeiten Sie einen Synthetic Monitor, um die Verfügbarkeit und Leistung Ihrer HTTP-Endpunkte zu testen, bevor Ihre Kunden Probleme erkennen.

Vorbereitungen

- Ein Konfigurationselement (Configuration Item, CI) für den Endpunkt, den Sie testen möchten.
- Wenn Sie private Endpunkte testen oder die Überwachungen aus Ihrer Umgebung ausführen möchten, müssen mindestens ein Standort erstellt werden, um den Monitor zu hosten. Informationen zum Erstellen eines Standorts finden Sie unter Erstellen Synthetische Überwachung Standorte.

Erforderliche Rolle: sn_SOW_Synthetics.Synthetics_Editor oder sn_SOW_Synthetics.Synthetics_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* Und wählen Sie aus Synthetische Überwachung Symbol ( ).
2. Erstellen Sie auf der Seite „Übersicht“ entweder einen Synthetic-Monitor, oder bearbeiten Sie einen vorhandenen.
   - Um einen Synthetic-Monitor zu erstellen, wählen Sie aus **Neu** .
   - Um einen vorhandenen zu bearbeiten, wählen Sie den Monitor aus, den Sie bearbeiten möchten, und wählen Sie dann aus **Details** Registerkarte.
3. Füllen Sie im Formular die Felder aus.

   a. Geben Sie im Abschnitt „Überwachungsdetails“ einen eindeutigen Namen für den Monitor und eine Beschreibung ein.

   b. Füllen Sie die Felder im Abschnitt „HTTP-Einstellungen“ aus.

Abschnitt „HTTP-Einstellungen“

Feld	Beschreibung
HTTP-Methode	HTTP-Methode, die Sie für den Endpunkt überwachen möchten.
HTTP-Endpunkt-CI	CI für den Endpunkt, den der Monitor testen soll. Wenn der Endpunkt nicht vorhanden ist, wählen Sie aus **Verwalten Sie HTTP-Endpunkte in CMDB** Um ein neues CI zu erstellen.
Zugehöriges Service-CI	Anwendungsservice-CI im Zusammenhang mit dem HTTP-Endpunkt. Der eingegebene Wert wird verwendet, um die CI-Beziehung zwischen dem HTTP-Endpunkt und dem Anwendungsservice zu erstellen oder zu aktualisieren.
Support-Gruppe	Gruppe, die benachrichtigt und Warnungen zugewiesen wird, wenn diese Überwachung fehlschlägt.
Abfrageparameter	Zeichenfolge von Abfrageparametern, die in die Anforderungs-URL aufgenommen werden sollen. **Hinweis:** Die Zeichenfolge darf das führende Fragezeichen nicht enthalten. Verwenden Sie zum Beispiel `id=XYZ&Customer=myco` Anstelle von `?ID=XYZ&Customer=myco` .
Anmeldeinformationen	Anmeldeinformationen erforderlich, wenn der Endpunkt eine Authentifizierung erfordert. Unterstützte Anmeldeinformationen sind Standardauthentifizierungs- und Zugriffstoken.
Header	Schlüssel-Wert-Paare für die HTTP-Anforderungsheader. Sie können mehrere Paare hinzufügen.
Textkörper	Text, der verwendet wird, wenn die API einen Nachrichtentext erwartet, z. B. ein JSON-Fragment.

   c. Wählen Sie im Abschnitt Standorte einen oder mehrere Standorte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um den Test dieses Monitors über auszuführen ServiceNow Instanz, wählen Sie aus **Aktuelle Instanz** .

  Hinweis: Wenn Tests über die Plattform ausgeführt werden, können aus Leistungsgründen jede Minute nur sechs Tests ausgeführt werden.

  Der Endpunkt für die Überwachung muss öffentlich verfügbar sein.

- Wählen Sie einen der zuvor erstellten Standorte aus.
- Wählen Sie Aus **Erstellen Sie einen neuen Standort** Um einen neuen Standort zu erstellen.

Weitere Informationen zum Erstellen eines Standorts finden Sie unter Erstellen Synthetische Überwachung Standorte.

d. Definieren Sie im Abschnitt „Assertion“ einen erfolgreichen Test, indem Sie mindestens ein Kriterium, einen Operator und einen Wert auswählen.

Hinweis: Mehrere Kriterien sind mit verbunden UND Ausdruck, daher muss der Test alle Kriterien erfüllen, um erfolgreich zu sein.

Kriterientyp	Beschreibung des Erfolgs
Statuscode	Endpunkt gibt den angegebenen Statuscode zurück.
Antwortzeit (in ms)	Endpunkt sendet eine Antwort in einem schnelleren Zeitraum als der angegebene Wert.
Antworttext	Endpunkt sendet einen Zeichenfolgenwert im Antworttext, der dem ausgewählten Operator und dem angegebenen Wert entspricht.

e. Geben Sie im Abschnitt Häufigkeit die Anzahl der Minuten zwischen den einzelnen Testläufen ein.

f. Wahlweise: Um eine Warnung über senden zu lassen Ereignismanagement Wenn ein Test fehlschlägt:

- Aktivieren Sie im Abschnitt „Warnungseinstellungen“ den Umschalter.
- Wählen Sie einen Warnungsschweregrad für einen Testfehler aus.

4. Wählen Sie **Speichern**.

Ergebnis

Auf der Übersichtsseite für den Synthetic-Monitor werden die Ergebnisse der Tests angezeigt, die der Monitor ausführt. Weitere Informationen finden Sie unter Identifizieren von Systemproblemen mit Synthetische Überwachung.

Synthetic-Monitore verwalten

Bearbeiten oder löschen Sie Synthetic-Monitore, nachdem Sie sie erstellt haben.

Vorbereitungen

Erforderliche Rolle: sn_SOW_Synthetics.Synthetics_Editor

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* Und wählen Sie aus Synthetische Überwachung Symbol ( ).
2. Befolgen Sie diese Anweisungen, um einen Monitor zu bearbeiten.

Option	Beschreibung
Bearbeiten Sie mehrere Überwachungskonfigurationen	Von Synthetische Überwachung Zielseite, wählen Sie einen oder mehrere Monitore aus, und wählen Sie aus **Bearbeiten** . Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic-Monitor. **Hinweis:** Aktuelle Werte werden in den Feldern nicht angezeigt. Wenn Sie kein Feld bearbeiten, bleiben die ursprünglichen Werte erhalten. Wenn Sie andere Eigenschaften als Anmeldeinformationen, Standort oder Warnungseinstellungen bearbeiten möchten, müssen Sie jeweils einen einzelnen Monitor über bearbeiten **Details** Registerkarte.
Bearbeiten Sie eine einzelne Monitorkonfiguration	Von Synthetische Überwachung Zielseite, wählen Sie einen Monitor aus, um ihn zu öffnen, und wählen Sie dann aus **Details** Registerkarte zum Bearbeiten. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic-Monitor.
Löschen Sie Monitore	Wählen Sie auf der Zielseite für Synthetic Monitoring eine oder mehrere zu löschende Monitore aus, und wählen Sie sie aus **Löschen** .

Identifizieren von Systemproblemen mit Synthetische Überwachung

Tests, die von Synthetic Monitors ausgeführt werden, ermöglichen es Serviceverantwortlichen und -Betreibern, die Leistung des Serviceendpunkts im Maßstab anzuzeigen.

Übersicht über die Verwendung Synthetische Überwachung

Als Serviceverantwortlicher können Sie verwenden Synthetische Überwachung Um die Endpunkte Ihres Service zu überwachen und sicherzustellen, dass sie verfügbar sind und wie erwartet funktionieren. Sie können benachrichtigt werden, wenn synthetische Tests fehlschlagen, sodass Sie Probleme schnell mindern können. Sie können Trends in HTTP-API-Erfolgsraten und Antwortzeiten anzeigen.

Als Operator können Sie verwenden Synthetische Überwachung Als Teil der Selektierung von Problemen. Wenn Sie erfahren, dass bei einem Service Probleme gemeldet werden, können Sie Testergebnisse für die Endpunkte dieses Service anzeigen. Wenn Tests fehlschlagen oder die Antwortzeiten langsam sind, könnte dies zu untersuchen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Aggregatinformationen zu den Monitoren an

Die Synthetische Überwachung Zielseite zeigt eine Übersicht über alle erstellten Monitore, einschließlich inaktiver Monitore.

Von hier aus können Sie den Status für alle Ihre Monitore anzeigen. Wenn Sie oben eine Karte auswählen, wird die Liste der Monitore gefiltert. Sie können beispielsweise nur die Monitore anzeigen, die fehlgeschlagen sind oder sich in einem unbekannten Status befinden.

Standardmäßig wird die Liste der Monitore nach dem Zeitstempel in sortiert **Aktualisiert** Spalte. Sie können einen anderen Spaltenheader auswählen, um nach dieser Kategorie zu sortieren.

Zeigen Sie einen Monitor und seine Tests an

Um die Details eines Monitors und die Ergebnisse seiner Tests anzuzeigen, wählen Sie einen Monitor aus der aus Synthetische Überwachung Zielseite. Die Seite „Überwachungsdetails“ enthält wichtige Informationen, die erforderlich sind, um die Leistung der Überwachung zu verstehen.

Verwenden Sie die Informationen im Header, um die grundlegende Integrität des Monitors zu verstehen, einschließlich seines Status und wann er zuletzt einen Test ausgeführt hat.

Verwenden Sie die Konfigurationskarte, um die grundlegenden Konfigurationsparameter des Monitors zu verstehen. Wenn sich ein Monitor in befindet `Unbekannt` status können Sie den Endpunkt-Link verwenden, um sicherzustellen, dass der richtige Endpunkt für den Monitor ausgewählt ist. Ein `Unbekannt` der status tritt häufig aufgrund eines Problems mit dem zugehörigen auf Agent Client Collector(ACC) Proxy.

Zeigen Sie einzelne Tests an

Auf der Karte Metriken werden zwei Diagramme angezeigt, die Ihnen helfen, die Integrität der einzelnen Tests zu verstehen, die der Monitor ausgeführt hat. Die **Fehlgeschlagene Tests** Das Diagramm zeigt jeden Test mit einem Wert von an `0` Wann es erfolgreich war, und ein Wert von `1` Wenn dies fehlgeschlagen ist. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um weitere Details anzuzeigen.

Die **Antwortzeit** Das Diagramm zeigt die Zeit in Millisekunden, die benötigt wurde, um eine Antwort vom Endpunkt zu erhalten. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um Details anzuzeigen.

Hinweis: Testergebnisse werden 21 Tage lang aufbewahrt.

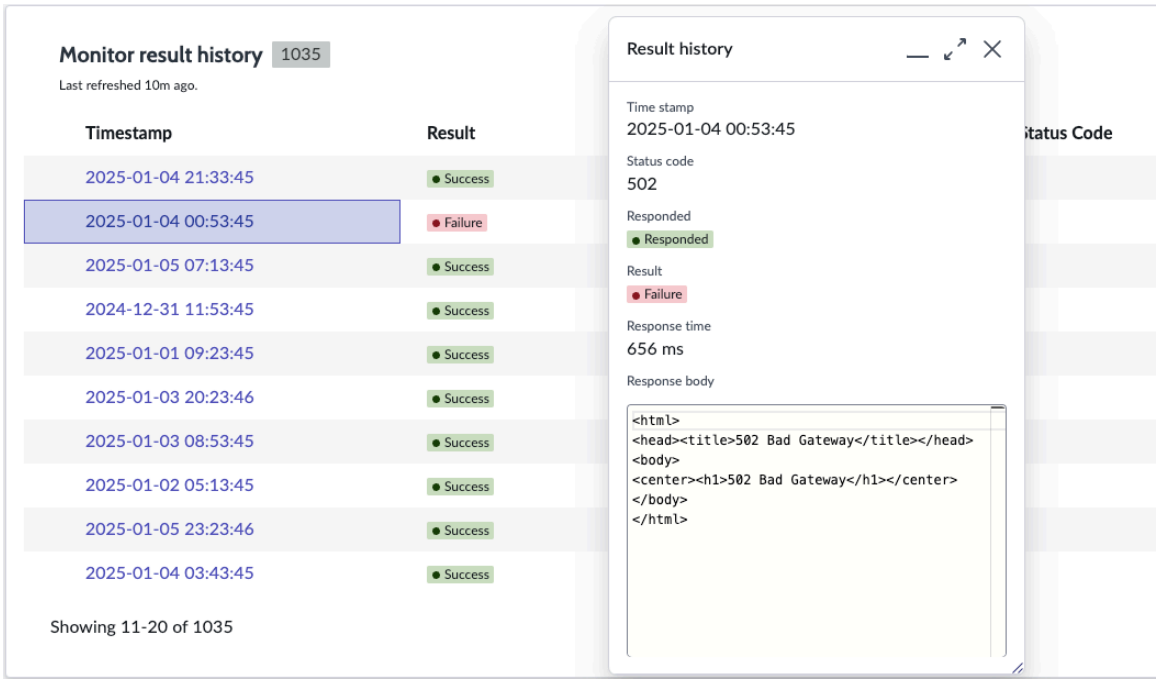
Die **Überwachen Sie den Ergebnisverlauf** Tabelle listet jeden Test auf. Standardmäßig wird die Tabelle anhand des Zeitstempels von der neuesten nach der ältesten sortiert. Sie können nach einer beliebigen Spalte sortieren, um Probleme zu finden. Sie können beispielsweise nach sortieren **Ergebnis** Um alle Fehler zusammen anzuzeigen, oder Sie können nach sortieren **Antwortzeit** Zum Anzeigen der Tests mit der höchsten Latenz.

Wenn ein Monitor so konfiguriert wurde, dass eine Warnung generiert wird, wenn er fehlschlägt, wird ein Link zur Warnung in angezeigt **Warnung** Spalte. Klicken Sie auf einen Warnungslink, um ihn anzuzeigen Details .

Wenn Sie einen Fehler oder eine hohe Latenz sehen, wählen Sie einen Test aus, um Details anzuzeigen, einschließlich des Antworttexts, die helfen können, Probleme zu erklären.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antworttext im Modal „Details“



Zeigen Sie Informationen zur aggregierten Überwachung an

Zeigen Sie Informationen zu allen Ihren Synthetic-Monitoren an.

Vorbereitungen

Erforderliche Rolle: sn_SOW_Synthetics.Synthetics_Viewer, sn_SOW_Synthetics.Synthetics_Editor, sn_SOW_Synthetics.Synthetics_admin

Prozedur

1. Navigieren zu **Alle** > *`Service Operations-Arbeitsbereich`* Und wählen Sie aus Synthetische Überwachung Symbol ( ).
2. Um die Liste der Monitore zu filtern, wählen Sie oben auf der Seite eine Karte aus.
   Um beispielsweise nur Monitore anzuzeigen, bei denen Tests fehlgeschlagen sind, wählen Sie aus **Fehlgeschlagen** Karte.
3. Um Details zu jedem vom Monitor ausgeführten Test anzuzeigen, wählen Sie einen Monitornamen aus.
   Die Detailseite des Monitors wird geöffnet. Weitere Informationen zu dieser Seite finden Sie unter Zeigen Sie die Testergebnisse eines Monitors an.
4. Um die Liste der Monitore zu exportieren, wählen Sie aus **Exportieren** .
   Sie können in die folgenden Dateiformate exportieren:
   - XLSX
   - CSV
   - JSON
   - PDF

Zeigen Sie die Testergebnisse eines Monitors an

Zeigen Sie die Ergebnisse von Tests an, die von einem Monitor ausgeführt werden, zusammen mit Konfigurationsdetails und zugehörigen Konfigurationselementen (Configuration Items, CIs).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_SOW_Synthetics.Synthetics_Viewer, sn_SOW_Synthetics.Synthetics_Editor, sn_SOW_Synthetics.Synthetics_admin

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* Und wählen Sie aus Synthetische Überwachung Symbol ( ).
2. Wählen Sie einen Monitor aus der Liste aller Monitore aus.
3. Zeigen Sie die Gesamtintegrität des Monitors im Header an, der seinen Status sowie den Zeitpunkt der letzten Ausführung und Aktualisierung anzeigt.
4. Zeigen Sie eine Übersicht über die Konfiguration des Monitors in an **Konfiguration** Karte.
   - Um die vollständige Konfiguration anzuzeigen, verwenden Sie **Details** Registerkarte. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic-Monitor.
   - Um die Integrität des zugehörigen CI anzuzeigen, wählen Sie den Link aus.
5. Zeigen Sie Integritätsmetriken für den Monitor über an **Metriken** Karte.
   Die **Fehlgeschlagene Tests** Das Diagramm zeigt jeden Test mit einem Wert von an `0` Wenn erfolgreich und ein Wert von `1` Wenn dies fehlgeschlagen ist. Die **Antwortzeit** Das Diagramm zeigt die Zeit in Millisekunden, die benötigt wurde, um eine Antwort vom Endpunkt zu erhalten. Bewegen Sie den Mauszeiger über einen Punkt in den Diagrammen, um Details anzuzeigen.
   - Verwenden Sie das Dropdown-Menü, um den Zeitraum zu ändern.
   - Verwenden Sie das Kontextmenü, um die Zeichen zu aktualisieren.
6. Zeigen Sie den Status der einzelnen Tests in an **Überwachen Sie den Ergebnisverlauf** Karte.
   Um die Details für einen Test anzuzeigen, wählen Sie dessen Zeitstempel aus. Weitere Informationen zu den Testdetails finden Sie unter Zeigen Sie Testdetails an.

Hinweis: Das Filtern der Liste wirkt sich auf die in den Metrikdiagrammen angezeigten Daten aus.

Zeigen Sie Testdetails an

Zeigen Sie die Ergebnisse eines einzelnen synthetischen Tests an, der von einem Monitor ausgeführt wird.

Vorbereitungen

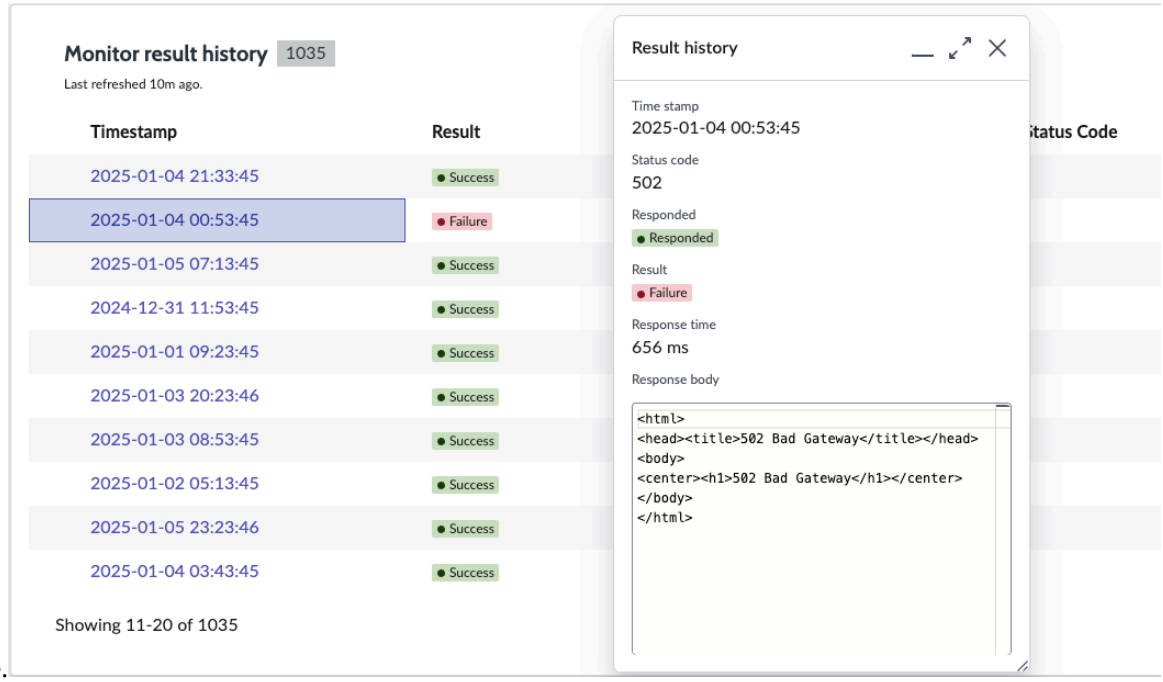
Erforderliche Rolle: sn_SOW_Synthetics.Synthetics_Viewer, sn_SOW_Synthetics.Synthetics_Editor, sn_SOW_Synthetics.Synthetics_admin

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* Und wählen Sie aus Synthetische Überwachung Symbol ( ).
2. Wählen Sie einen Monitor aus der Liste aller Monitore aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie einen Test aus der Liste der Tests aus.
   Das Modal zeigt Informationen zum Test an, einschließlich eines Antworttexts. In diesem Beispiel wird gezeigt, dass die Anforderung an ein ungültiges Gateway gesendet wurde.



Synthetische Überwachung – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Synthetische Überwachung Anwendung, z. B. installierte Komponenten und Seitendetails.

Mit Synthetische Überwachung installierte Komponenten

Bei der Aktivierung des Synthetische Überwachung-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Installierte Rollen

Rolle	Beschreibung	Enthält Rollen
Synthetic-Monitor-Viewer [sn_SOW_Synthetics.Synthetics_Viewer]	Zeigt Testkonfigurationen und ihre Ergebnisse an.	• cmdb_read • sn_sow.sow_user • agent_client_collector_user • sn_SOW_Synthetics.credential_Re
Synthetic-Monitor-Editor [sn_SOW_Synthetics.Synthetics_Editor]	Erstellt und bearbeitet Tests. Zeigt Testkonfigurationen und ihre Ergebnisse an.	• credential_admin • sn_cmdb_Editor • sn_SOW_Synthetics.Synthetics_V

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Beschreibung	Enthält Rollen
Synthetic-Monitor-Administrator [sn_Synthetics.Synthetics_admin]	Weist Rollen zu. Erstellt und bearbeitet Tests. Zeigt Testkonfigurationen und ihre Ergebnisse an.	• agent_client_collector_admin • sn_SOW_Synthetics.Synthetics_E • sn_sow_itsm_admin.sow_admin_us
Synthetic Monitor-Anmeldeinformationsleser [sn_SOW_Synthetics.credential_Reader]	Wird intern verwendet, um aus der Tabelle „Anmeldeinformationen“ zu lesen.	Keine [Discovery_credentials]
Synthetic Monitor-Ereignisautor [sn_SOW_Synthetics.Synthetics_Event_Writer]	Wird intern zur Kommunikation mit verwendet MID-Server.	Keine

Installierte Tabellen

Tabelle	Beschreibung
Überprüfen [sn_Synthetics_Check]	Konfigurationsinformationen für synthetische Prüfungen.
Ausführungsstandort überprüfen [sn_Synthetics_Check_Execution_location]	Konfiguration des Ausführungsstandorts für synthetische Prüfungen.
Einzel-API [sn_Synthetics_Check_Single_api]	Zusätzliche Konfigurationsinformationen und Ergebnisse der letzten Ausführung für einzelne synthetische API-Prüfungen.
Einzel-API-Header [sn_Synthetics_Check_Single_api_Header]	Schlüssel-Wert-Paare von Anforderungsheadern für einzelne synthetische API-Prüfungen.
Einzel-API zu Richtlinie [sn_Synthetics_Check_Single_api_Policy]	Synthetic-Testdaten der einzelnen API und die entsprechenden Agent Client Collector(ACC) Richtlinien.
Einzel-API-Ergebnis [sn_Synthetics_Check_Single_api_result]	Ergebnisse aus jeder Ausführung der Synthetic-Prüfung.
Private Synthetics-Standorte [sn_Synthetics_private_location]	Definitionen der ACC-Agent-Proxy-Cluster, die für verfügbar sind Synthetische Überwachung. Erweitert die Tabelle „Proxy-Agent-Cluster“ [sn_Agent_Cluster].

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und Synthetische Überwachung

Domänentrennung wird für Synthetische Überwachung unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domänentrennung und Synthetische ÜberwachungÜbersicht

Domänentrennung ist in allen Aspekten der Anwendung Synthetische Überwachung vorhanden. Benutzer, die zu einer bestimmten Domäne gehören, sehen nur die Daten, die in ihrer eigenen Domäne vorhanden sind.

So funktioniert Domain Separation in Synthetische Überwachung

Wenn Daten in durch Domänen getrennt sind Synthetische Überwachung, Anwender können die Überwachungsdaten nur in ihrer eigenen Domäne konfigurieren und anzeigen. Standardmäßig werden alle Benutzer und Datensätze auf die übergeordnete Domäne festgelegt, es sei denn, der Administrator weist sie einer bestimmten Domäne zu.

Sie definieren die domänengetrennte Umgebung, wenn Sie Ihre Dateneingaben konfigurieren. Alle relevanten Datensätze und Datenverarbeitungen in Synthetische Überwachung Der Programm-Flow befindet sich in derselben Domäne wie die Dateneingabe. Der Domänenname einer Dateneingabe wird in der Spalte Domäne angezeigt, die in den Tabellen in Ihrer Instanz angezeigt wird.

Die Verwendung der Domänentrennung in Ihrer Instanz ist für Synthetische Überwachung transparent. Die Anwendung verwaltet alle Aspekte der Daten, z. B. die Überwachungskonfigurationen und -Ergebnisse. Wenn eine Eigenschaft geändert wird, wirkt sich der neue Wert nur auf neue Quellen in der spezifischen Domäne aus.

Beim Einrichten Agent Client Collector(ACC) für nicht gehostete Synthetics-Prüfungen erfordert jede Domäne, die nicht gehostete Synthetics unterstützt, einen eigenen ACC-Cluster und MID-Server. Der ACC-Cluster und MID-Server Muss in einer Blattdomäne erstellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Zielseite von Synthetische Überwachung

Lesen Sie die folgenden Informationen, um zu verstehen, was auf angezeigt wird Synthetische Überwachung Zielseite, auf der Sie aggregierte Informationen zu Ihren Synthetic-Monitoren anzeigen können.

Informationen zusammenfassen

Die Karten zeigen aggregierte Informationen für alle Monitore an, unabhängig davon, ob sie aktiv sind oder nicht. Wählen Sie eine Karte aus, um die Überwachungsliste zu filtern.

Aggregatkarten

Kartentitel	Beschreibung
Gesamtanzahl Überwachungen	Gesamtzahl der erstellten Monitore.
Bestanden	Gesamtanzahl der Monitore, die den Wert zurückgegeben haben, der als Assertion des Monitors festgelegt wurde, z. B. einen Statuscode von 200 .
Fehlgeschlagen	Gesamtanzahl der Monitore, die einen anderen Wert zurückgegeben haben als den, der als Assertion konfiguriert wurde.
Ausstehend	Gesamtanzahl der Monitore, die sich im Status „Ausstehend“ befinden. Monitore sind auf festgelegt **Ausstehend** Vor den ersten Testläufen.
Angehalten	Gesamtanzahl der Monitore, die sich im Status „Angehalten“ befinden. Angehaltene Monitore sind diejenigen, die auf festgelegt wurden **Überwachung deaktiviert** Auf der Konfigurationsseite.
Unbekannt	Gesamtanzahl der Monitore, die aufgrund eines Problems mit dem zugehörigen nicht ausgeführt werden Agent Client Collector(ACC) Proxy.

Überwachungsliste

Standardmäßig werden in dieser Liste alle Monitore angezeigt, die erstellt wurden. Sie können oben auf der Seite eine Karte auswählen, um zu einer Liste von Monitoren mit diesem Status zu filtern. Wählen Sie einen Monitor aus, um die zugehörige Detailseite anzuzeigen.

Detailseite eines Synthetic-Monitors

Lesen Sie die folgenden Informationen, um zu verstehen, wie Sie die Detailseite eines synthetischen Monitors verwenden, um die Ergebnisse seiner Tests anzuzeigen.

Header

Der Header bietet eine Übersicht über den Monitor.

Element	Beschreibung
Überwachungsname	Name, der dem Monitor bei der Erstellung gegeben wurde.
Aktiviert	Angabe, ob der Monitor aktiv ist.
Status	Status des letzten Testlaufs. Werte können einer der folgenden sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	• Ausstehend: Der Monitor wartet basierend auf der konfigurierten Häufigkeit auf die Ausführung des ersten Tests. • Erfolg: Der Test wurde ausgeführt und hat die von Ihnen festgelegten Assertionskriterien bestanden. • Unbekannt: Der Test konnte nicht ausgeführt werden, wahrscheinlich aufgrund eines Problems mit dem zugehörigen Agent Client Collector(ACC) Proxy. • Fehler: Der Test wurde ausgeführt, aber die Assertionskriterien wurden nicht erfüllt. Wählen Sie einen Zeitstempel-Link aus, um den Antworttext anzuzeigen, um weitere Informationen zum Test zu erhalten.
Letzter Test ausgeführt	Zeitstempel, der angibt, wann der letzte Test ausgeführt wurde.
Zuletzt aktualisiert	Zeitstempel, der angibt, wann der Monitor zuletzt bearbeitet und gespeichert wurde.

Registerkarte „Übersicht“

Die **Übersicht** Die Registerkarte bietet eine zusammengefasste Ansicht aller Tests, die der Monitor ausgeführt hat. Auf dieser Registerkarte wird Folgendes angezeigt:

- Konfigurationskarte: Aktuelle Standardkonfiguration des Monitors.
- Metrikkarte: Diagramme, die die Leistung jedes Tests für den in der Zeitauswahl ausgewählten Zeitraum bereitstellen.
- Ergebnisverlauf überwachen: Alle vom Monitor ausgeführten Tests und seine Ergebnisse.

Registerkarte „Details“

Sie können verwenden **Details** Registerkarte, um einen Monitor zu erstellen oder einen vorhandenen zu bearbeiten. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic-Monitor.

CSDM-Richtlinien auf ITOM-Integrität anwenden

ITOM-Integrität Hilft Ihnen, die Integrität von Services in Ihrer Organisation nachzuverfolgen und zu erhalten. ITOM-Integrität CSDM Referenz dient als grundlegender Blueprint für die Aufrechterhaltung optimaler IT-Vorgänge durch die Standardisierung von Datenmodellen und Prozessen. Das Hauptziel besteht darin, Ihnen zu helfen, die beiden Hauptfunktionen zu verstehen, die innerhalb von zusammenarbeiten CSDM Framework.

ITOM-Integrität Besteht aus zwei Hauptfunktionen, die verwenden CSDM Framework.

Ereignismanagement

Ereignismanagement Sammelt Warnungen aus Infrastrukturereignissen, die von Überwachungstools von Drittanbietern erfasst wurden. Ereignismanagement Verwendet IT-bezogene Informationen, die von erfasst wurden Discovery Zum Zuordnen von Warnungen zu CIs. Basierend auf den erfassten Informationen stellt Ereignismanagement Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen.

Metrik-Anomalieerkennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analysiert proaktiv Ihre IT-Infrastruktur, um Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von erweitertem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur ermittelt die Anwendung automatisch dynamische Schwellenwerte und identifiziert Anomalien, die auf potenzielle Serviceausfälle hindeuten.

Informationen zum Einrichten von CSDM finden Sie unter Implementierung des CSDM-Frameworks in Phasen .

Weitere Informationen zu finden CSDM Framework, siehe CSDM-Modell erkunden .

ITOM-IntegritätÜberlegungen zu CSDM Framework

ITOM-Integrität Richtet an aus CSDM Framework zur Gewährleistung einer standardisierten Datenverwaltung und zur Optimierung des IT-Betriebs.

Wichtige Überlegungen zur Implementierung ITOM-Integrität Für CSDM Framework umfasst Folgendes.

Identifizierung erforderlicher Konfigurationselemente (Configuration Items, CIs) für eine optimale Nutzung Ereignismanagement Vorteile

Ereignismanagement Verwendet Konfigurationselemente (Configuration Items, CIs), die vom Betriebsteam überwacht werden, um Warnungen mit dem entsprechenden CI zu korrelieren und ihre Auswirkungen auf den überwachten Service zu bewerten.

Definieren technischer Services in Ereignismanagement

Dynamische CI-Gruppenservices, früher als technische Services bekannt, nutzen die CMDB CI-Gruppenfähigkeit zum Abfragen von CMDB, Ermöglicht die effiziente Gruppierung von Konfigurationselementen (Configuration Items, CIs) für verschiedene operative Zwecke.

Erkennen allgemeiner Anwendungsfälle für den dynamischen CI-Gruppenservice

In Ereignismanagement(EM) fungiert der dynamische CI-Gruppenservice als logischer Gruppierungsmechanismus für Konfigurationselemente (Configuration Items, CIs), der Technologie- oder Serviceverantwortlichen Einblicke in den Integritätsstatus der gruppierten Entitäten bietet.

ITOM-Integrität und CSDM-Tabellen

ITOM-Integrität Nutzt und verwaltet CSDM Tabellen, während verschiedene ServiceNow Produkte verbessern den Betrieb und tragen zu einem Mehrwert bei.

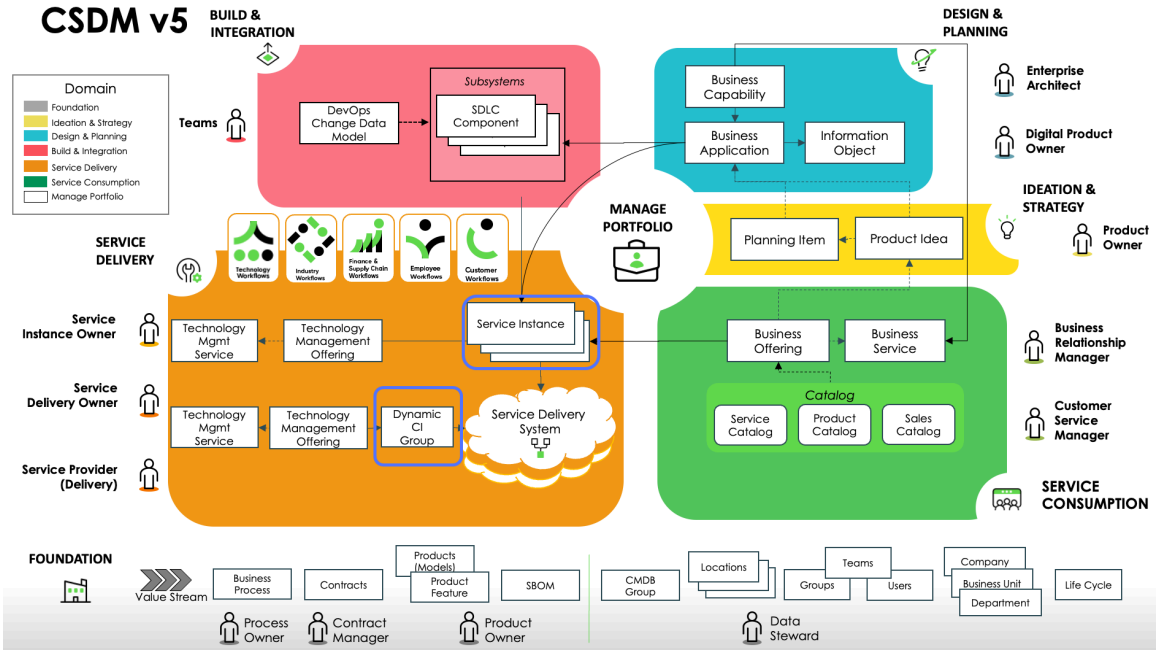
CSDM-Tabellen in der CMDB, die von ITOM-Integrität verwaltet werden

ITOM-Integrität Verwaltet die folgenden Tabellen:

- Tabelle „zugeordneter Anwendungsservice“ [cmdb_ci_Service_detected] (mit CSDM v5 hat sich die Bezeichnung für die Tabelle von „Anwendungsservice“ in „Serviceinstanz“ geändert .)
- Konfigurationselementtabelle [ci_*]
- Dynamische CI-Gruppentabelle [cmdb_ci_query_based_Service]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ITOM verwaltete CSDM-Tabellen



Mit installierte Plugins oder Anwendungen ITOM-Integrität

Tabellen, die die mit installierten Plugins oder Anwendungen auflisten ITOM-Integrität Anwendungen. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Ereignismanagement

Mit installierte Plugins oder Anwendungen Ereignismanagement(com.glideapp.itom.snac)

Plugin- oder Anwendungsname	Beschreibung
Inhalt der Warnungsverwaltung (com.em-Alert-mgmt-content)	Enthält alle erforderlichen Basissystem-Subflows, die für die Warnungskorrektur verwendet werden können.
ITOM Lizenzierung (com.snc.itom.license)	Zentrale Komponenten für ITOM Lizenzierungsmodell, das berechnet und anzeigt, wie viele Abonnements für ITOM Anwendungen, die Ihre Organisation kauft und verbraucht.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.
Serviceanalytik (com.snc.sa.analytics)	Stellt Warnungs-Analytics basierend auf maschinellem Lernen (ML) und Topologielernen bereit.
Ereignismanagement Und Service-Mapping Kern (com.snc.service-watch)	Besteht aus den gemeinsamen Komponenten von Ereignismanagement und Service-Mapping.
Tag-basierte Warnungs-Clustering-Engine (sn_em_tbac)	Stellt eine Zero-Code-Methode bereit, die die Warnungsgruppierung vereinfacht und Warnungskorrelation ohne Notwendigkeit durchführt CMDB, Modelltraining oder Feinabstimmung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Ereignismanagement(com.glideapp.itom.snac) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Regel-Management für Warnmeldungen (sn_em_arm)	Ermöglicht Anwendern von Ereignismanagement, automatisch auf Warnungen zu reagieren. Eine Warnungsverwaltungsregel bestimmt die erforderliche Warnungsantwort.

Health Log Analytics

Mit installierte Plugins oder Anwendungen Health Log Analytics(sn_occ)

Plugin- oder Anwendungsname	Beschreibung
Integrationsgemeinschaften für CMDB(sn_cmdb_int_util)	Enthält eine Sammlung von Dienstprogrammfunktionen, die eine allgemeine Methode für die Verarbeitung des Schlüssels bereitstellen CMDB Attribute und sind für alle verfügbar CMDB Zertifizierte Integrationen.
ITOM Cloud-Services Core (sn_itom_Cloud_svc)	Generiert relevante Themen für Mandanten, sodass sie Daten aus ihrer Kundeninfrastruktur an übertragen können ServiceNow Automatisch. Diese Themen sind hauptsächlich für die Verwendung mit dem Hermes Messaging-Service vorgesehen.
Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont)	Ein konfigurierbarer Arbeitsbereich mit einer einheitlichen Experience für mehrere IT Operations Management-Workflows. Sie können den Lebenszyklus von Warnungen in IT Operations Management-Workflows durch eine einfache, intuitive und übersichtliche Anwenderoberfläche, automatisierte Empfehlungen und eine zielgerichtete Experience verwalten.
Health Log Analytics Kern (com.glideapp.itom.occultus)	Wichtige Komponenten für Health Log Analytics Bereichsbezogene Anwendung.
Microsoft Teams Spoke für ServiceNow IntegrationHub (com.sn.ms_Teams.ah)	Stellt Aktionen bereit, die Prozessanalysten beim Entwerfen von Flows verwenden können, um das Senden von Nachrichten über zu automatisieren ServiceNow Incident- und Problemdatensätze zu einem Microsoft Teams Kanal.
Slack Webhooks-Spoke für ServiceNow IntegrationHub (com.sn.slack.ah)	Verwenden Sie Slack-Webhooks, um Nachrichten zu senden und Details für ServiceNow-Incidents, Probleme und Änderungen bei Slack-Kanälen aufzuzeichnen.
Normalisierungsdatenservices Client (com.Glide.Data_Services_Canonicalization.Client)	Hilft bei der Aufrechterhaltung der Konsistenz, indem überprüft wird, ob Datensätze für ein bestimmtes Unternehmen mit der Liste der Standardfirmennamen übereinstimmen. Wenn das Plugin ein Unternehmensnamenfeld mit einer Variante dieses Namens findet, ersetzt es den Standardnamen an seiner Stelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Reliability Management

Mit installierte Plugins oder Anwendungen Service Reliability Management(sn_SOW_srm)

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Service Reliability Management(SRM) Allgemein (sn_SOW_srm_common)	Stellt allgemeine Dienstprogramme und Konfigurationseinstellungen bereit, die von verwendet werden Service Reliability Management Zum Beispiel Kernfunktionen im Zusammenhang mit der Verwaltung von Teams und Services und der Metrikberechnung für Services.
Service Reliability Management (Globale Abhängigkeiten) (com.snc.srm)	Unterstützt globale Skripts und Dienstprogramme für Service Reliability Management Für Service Operations-Arbeitsbereich.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont)	Ein konfigurierbarer Arbeitsbereich mit einer einheitlichen Experience für mehrere IT Operations Management-Workflows. Sie können den Lebenszyklus von Warnungen in IT Operations Management-Workflows durch eine einfache, intuitive und übersichtliche Anwenderoberfläche, automatisierte Empfehlungen und eine zielgerichtete Experience verwalten.
Bereitschaftsplanung (Com.snc.on_call_Rotation)	Bietet die Möglichkeit, Rufbereitschaftszeitpläne und Eskalationsbäume zu erstellen. Wenn ein Incident erstellt wird, können Sie die Eskalation dynamisch an eine Rufbereitschaftsressource weiterleiten.
SOW – Warnungsautomatisierung (sn_SOW_Alert_rules)	Stellt Operatoren in bereit Service Operations-Arbeitsbereich Mit der Möglichkeit, Warnungsautomatisierung für ihr Team zu erstellen und zu verwalten. Diese Automatisierung kann zum Anreichern, Verarbeiten und Gruppieren von Warnungen verwendet werden.
Servicelevel-Zielmanagement Für Service Operations-Arbeitsbereich(sn_SOW_Slo)	Enthält Funktionen zum Überwachen und Verwalten der Serviceintegrität mithilfe von Servicelevel-Indikatoren (SLIs), Servicelevel-Zielen (SLOs) und Fehlerbudgets.

Service Operations-Arbeitsbereich für ITOM

Mit installierte Plugins oder Anwendungen Service Operations-Arbeitsbereich ITOM Apps (sn_SOW_itom_CONT)

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Kern (sn_SOW)	Kernfähigkeiten und Arbeitsbereichskonfigurationen für Service Operations-Arbeitsbereich.
Ereignismanagement Kern (sn_em_ai)	Ermöglicht das Nachverfolgen und Überwachen von Warnungen im ServiceNow Mitarbeiterbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Service Operations-Arbeitsbereich ITOM Apps (sn_SOW_itom_CONT) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Integrations-Launchpad (sn_itom_integ_App)	Bietet eine neue und verbesserte Experience zum Anzeigen, Konfigurieren und Verwalten aller verfügbaren ITOM-Integrität-Integrationen.
Service Operations-Arbeitsbereich Warnungsverwaltung (sn_SOW_em)	Eine detaillierte Warnungsdatensatzseite mit zusätzlichen Daten wie den Registerkarten „Schneller Überblick“, „Playbook“ und „Metriken“.
Service Operations-Arbeitsbereich Express-Liste (sn_itom_aiops_list)	Eine zentrale und konsolidierte Plattform, mit der Betreiber Warnungen an einem Ort selektieren, analysieren und beheben können. Express-Liste Bietet eine Live-Ansicht von Warnungen, dynamische Filterung, einen Vorschaubereich mit zusätzlichem Kontext und wichtigen Details zu jeder Warnung sowie automatisierte technische Analysen mit Now Assist.
Service Operations-Arbeitsbereich Log Analytics (sn_SOW_hla)	Ein Protokoll-Viewer in Service Operations-Arbeitsbereich. Die Anwendung enthält auch die anwenderdefinierte Elasticsearch Datenquelle für Performance Analytics(PA) Dashboards.
AIOps-Dashboards (sn_aiops_Dashboard)	Bietet umfassende Visualisierungen kritischer Betriebsdaten und umsetzbare Einblicke, die proaktive Antworten auf potenzielle Probleme erleichtern. Die Anwendung zielt auf mehrere Ziele ab ITOM Personas mit unterschiedlichen Anforderungen, mit denen Sie Leistungskennzahlen (KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontexte für die IT-Umgebung insgesamt gewinnen können.
Ereignismanagement Connectors (sn_em_Connector)	Eine Sammlung vordefinierter Schnittstellen (Connectors) für die Erfassung von Ereignissen aus Überwachungstools von Drittanbietern oder Agent Client Collector in einer ServiceNow-Instanz.
Service Operations-Arbeitsbereich UI-Komponenten (sn_itom_uib_comp)	Ein verbundenes Repository zur Aufbewahrung gemeinsamer interner UI-Komponenten.

Metrikdaten

Mit aktivierte Plugins Metrikdaten(Com.snc.sa.metric)

Plugin-Name	Beschreibung
Operational Intelligence – Überwachung der Erweiterungsintegrität (com.snc.sa.metric.Health)	Enthält einige Funktionen, die Selbstüberwachungsfunktionen für ermöglichen Metrikdaten-Komponenten in MID-Server.
Highcharts-Reporting (com.Glide.Highcharts)	Stellt einige UI-Funktionen für bereit Metrikdaten.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit aktivierte Plugins Metrikdaten(Com.snc.sa.metric) (Fortsetzung)

Plugin-Name	Beschreibung
	identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
ITOM UI-Komponenten (com.snc.itom.ui)	Gemeinsam genutzte UI-Komponenten für ITOM Produkte, die einige UI-Funktionalität für bereitstellen Metrikdaten.
MID-Server Verteilter Cluster (com.snc.Agent.Distributed.Cluster)	Aktiviert die Verwaltung der MID-Cache-Komponente von Metrikdaten Von ServiceNow Instanz.
V3-Komponenten auflisten (com.Glide.ui.list_v3_components)	Stellt einige UI-Funktionen für bereit Metrikdaten Und Komponenten, die für Liste v3 erforderlich sind, einschließlich REST-Endpunkte, Anweisungen und Vorlagen.
MetricBase (Com.snc.clotho)	Die Datenbank, in der Rohmetrikdaten wie CPU-Auslastung und Datenträgerfrei gespeichert werden und in der das Modell für die Anomalieerkennung vorhanden ist.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.

Agent Client Collector

Mit installierte Plugins oder Anwendungen Agent Client Collector Framework(sn_Agent)

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Globale Dienstprogramme (com.snc.sa.accutils)	Eine Reihe von global bereichsbezogenen Dienstprogrammen, die bereichsübergreifende Transaktionen zwischen erleichtern Agent Client Collector Framework Und ein ServiceNow Instanz.
Konfigurationsverwaltung Für Bereichsbezogene Apps (CMDB) (Com.snc.cmdb.scope)	Bietet bereichsbezogene Anwendungen Zugriff auf Identifizierungs-Engine-APIs.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.

Mit installierte Plugins oder Anwendungen Agent Client Collector-Überwachung(sn_itmon)

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
Metrikdaten (sn_metrics_ng)	Eine Begleitanwendung für die Familie Metrikdaten Plugin, das zusätzliche Funktionen und Erweiterungen bietet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Agent Client Collector-Überwachung(sn_itmon) (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Metric Explorer (sn_itom_metric_exp)	Ermöglicht es Betreibern, das Metrikverhalten zu untersuchen und verschiedene Metriken über Hosts, Anwendungen und Services hinweg zu vergleichen und zu korrelieren, damit sie Probleme beheben und die Ursache finden können.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
Metrikdaten (Com.snc.sa.metric)	Bietet die Möglichkeit, Anwendungsmetrikdaten zu erfassen, zu erkunden und zu analysieren und Anomalien zu identifizieren und anzuzeigen. Metrikdaten Generiert Anomaliewarnungen, die zu IT-Warnungen heraufgestuft werden können und im angezeigt werden Service Operations-Arbeitsbereich Und Dashboard „Serviceintegrität“.

Mit installierte Plugins oder Anwendungen Agent Client Collector Visibility – Inhalt(sn_ACC_Visibility)

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Visibility – Inhalt Inhalt (sn_ACC_VIS_content)	Stellt Agent-basierte Infrastruktur-Discovery und -Sammlungen bereit Software Asset Management(SAM) zu unterstützende Metriken Discovery Und Digitale Endanwender-Experience(DEX) Anwendungen.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

Mit installierte Anwendungen Agent Client Collector Log Analytics(sn_accl)

Anwendungsname	Beschreibung
Agent Client Collector-Überwachung (sn_itmon)	Bietet die Möglichkeit, Ihre Konfigurationselemente (Configuration Items, CIs) zu überwachen. Diese Anwendung enthält vordefinierte Überwachungsprüfungen und -Richtlinien, die auf den Service Desk-Mitarbeiter angewendet werden.
Health Log Analytics (sn_occ)	Hilft Ihnen, Probleme schneller zu lösen, indem Sie maschinell generierte Protokolldaten in Echtzeit erfassen, analysieren und korrelieren, um IT-Probleme vorherzusagen, bevor sie sich auf Sie auswirken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit installierte Plugins oder Anwendungen Agent Client Collector Security Incident Response(sn_secops_ACC)

Plugin- oder Anwendungsname	Beschreibung
Security Incident Response (sn_si)	Ermöglicht Ihnen die Verwaltung und Automatisierung des Lebenszyklus Ihrer Security Incidents von der anfänglichen Priorisierung bis zur Eindämmung und Lösung. Verwenden Sie die automatisierten Workflows, um schnell und konsistent zu reagieren und Trends und Engpässe anhand der Daten zu verstehen, die von Analytics-gesteuerten Dashboards und umfassenden Reporting-Systemen bereitgestellt werden.
Sicherheitssupport Orchestration(sn_sec_cmn_orch)	Abhängigkeit für Vulnerability Response Und Security Incident Response Anwendungen.
Threat Intelligence Support allgemein (sn_ti)	Ermöglicht es Ihnen, Indikatoren für Kompromittierung (IoCs) zu finden und Security Incidents mit Threat Intelligence-Daten zu ergänzen. Threat Intelligence Ermöglicht es Ihnen, auf die STEX-Daten (Structured Threat Information Expression) Ihres Unternehmens zuzugreifen und einen Referenzpunkt bereitzustellen.
Agent Client Collector Spoke (sn_ACC_Spoke)	Stellt ein Framework zum Schreiben anwenderdefinierter Workflows oder Automatisierungen bereit, die für Agents oder CIs ausgeführt werden sollen.
Sicherheitssupport Core (com.snc.security_support.core)	Stellt ein robustes Kerndatenmodell und ein UI-Framework speziell für Integrationen von Sicherheitsvorgängen bereit. Dieses umfassende Modell dient als Rückgrat für die nahtlose Integration verschiedener Sicherheitstools und -Systeme, wodurch ein reibungsloser Datenfluss und effiziente Vorgänge gefördert werden.
Security Support Common (sn_sec_cmn)	Aktiviert die Kernfunktionalität, die von verwendet wird Security Operations Anwendungen.
Sicherheitsintegrations-Framework (sn_sec_int)	Verwaltet die allgemeine Funktionalität für Security Operations Integrationen, einschließlich beider Security Incident Response Und Vulnerability Response. Mit dem Security Integration Framework können Sie vorhandene Funktionen und Funktionen verwenden, ohne sie erneut implementieren zu müssen.
Agent Client Collector Framework (sn_Agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
Vulnerability Response Abhängigkeiten (com.snc.si_dep)	Aktiviert alle abhängigen Plugins, die zur Unterstützung von erforderlich sind Vulnerability Response Anwendung.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit aktivierte Plugins ITOM-Optimierung
- Mit Now Assist für ITOM installierte Anwendungen

Agent Client Collector

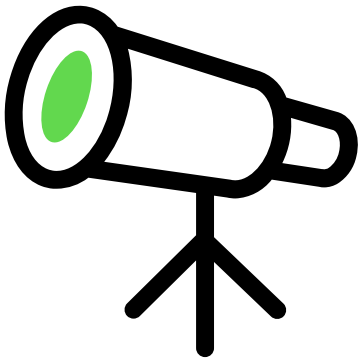
Agent Client Collector ist ein Agent, der auf Infrastrukturkomponenten installiert wird. Agent Client Collector basiert auf einem Sensu-Framework, mit dem Sie Überwachungsprüfungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aus der Community übernehmen und erweitern können. Der Agent führt Befehle auf den Computern aus, auf denen er installiert ist, und sendet über den MID-Server Ausgabedaten an die ServiceNow®-Instanz, wobei Events und Metriken in der entsprechenden Datenbank gespeichert werden.

Sehen Sie sich dieses Video an, um einen Überblick über die Funktionsweise von Agent Client Collector zu erhalten.

https://player.vimeo.com/video/1096666842?h=77a5520958&badge=0&autopause=0&player_id=0&app_id=58479

Agent Client Collector Framework	Agent Client Collector-Überwachung	Agent Client Collector Visibility – Inhalt
		
Analysieren Sie CI-Daten, die an die Instanz gesendet werden, und stellen Sie Daten für andere bereit Agent Client Collector Anwendungen.	Überwachen Sie Ihre Serviceverfügbarkeit, und stellen Sie sicher, dass Ihre Infrastruktur und ihre Anwendungen ordnungsgemäß ausgeführt werden.	Erfassen Sie Hostdaten auf Servern mit Agent Client Collector Visibility – Inhalt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Log Analytics	Security Incident Response	Live-CI-Ansicht
Protokolldaten streamen von Linux Und Windows Hosts zu ServiceNow Instanz.	Automatisieren Sie die Datensammlung und Antwortaktionen zur Ergänzung von Security Incidents mit Agent Client Collector.	Zeigen Sie Live-Daten für Incident-bezogene CIs an, um Incidents zu lösen.

Agent Client Collector Framework

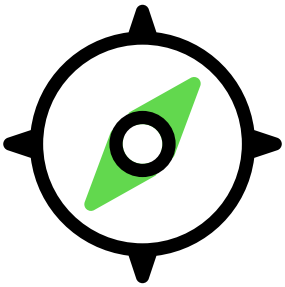
Die Agent Client Collector Framework Die Anwendung (ACC-F) verwaltet die Agent-Installation in Ihren Infrastrukturkomponenten und ermöglicht das Senden von Ausgabedaten an ServiceNow® Instanz über MID-Server. Zusätzlich zu MID-Server, Sie müssen die Konfigurationsverwaltungsdatenbank für bereichsbezogene Apps installieren (CMDB).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

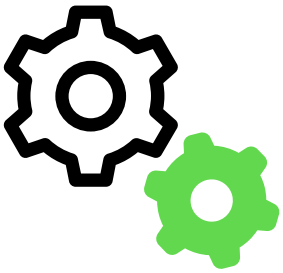
Erste Schritte

Untersuchen



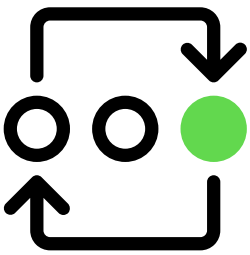
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen kennen, die der bietet Agent Client Collector Framework Anwendungsangebote.

Konfigurieren



Konfigurieren Sie die zu aktivierenden Funktionen und Komponenten Agent Client Collector Framework.

Arbeiten Sie mit Prüfungen und Richtlinien



Machen Sie sich mit der Arbeit mit Prüfungen vertraut, um Daten aus den Komponenten des Service Desk-Mitarbeiters zu sammeln.

Datensammlung

Aktivieren Sie das Sammeln von Daten aus Agent Client Collector Hosts.

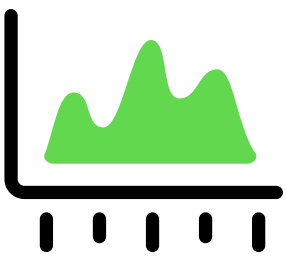
Agent Client Collector Protokolle

Verfolgen Sie Ereignisse in Ihrem System mit Agent Client Collector Protokolle

Agent Client Collector Integritäts-Dashboard

Überwachen Sie den Status der Service Desk-Mitarbeiter in Ihrem System.

Agent Client Collector Funktionsmatrix



Zeigen Sie die Verfügbarkeit an Agent Client Collector Funktionen.

Referenz

Rufen Sie zusätzliche Details zu Feldbeschreibungen, Konfigurationseigenschaften und Protokollebenen ab.

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum für Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Framework erkunden

Die Agent Client Collector Framework(ACC-F) ist eine leistungsstarke Lösung zur Überwachung der Leistung und Integrität von Infrastrukturkomponenten mithilfe von auf Servern und Geräten installierten Agents. Es erfasst und sendet kritische Systemdaten zur Analyse an ServiceNow, um die proaktive Verwaltung und Fehlerbehebung von Konfigurationselementen (Configuration Items, CIs) zu ermöglichen.

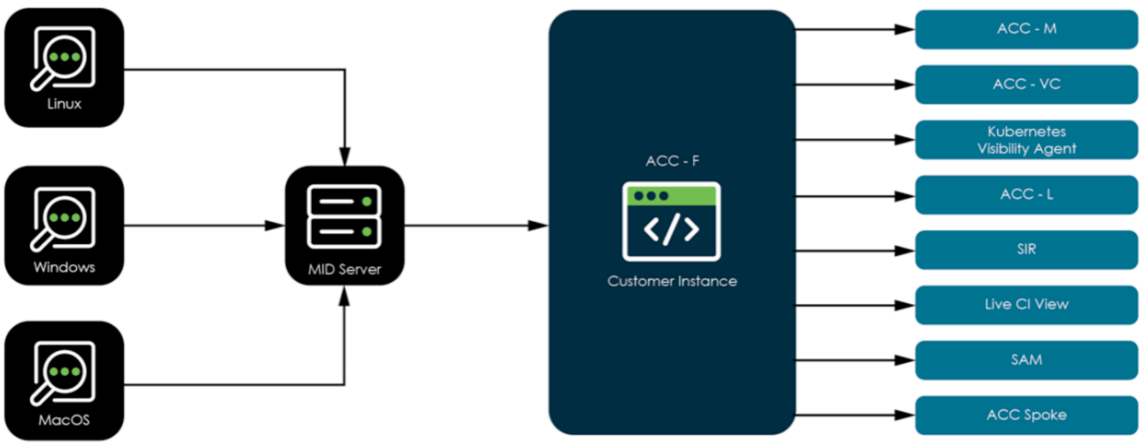
Agent Client Collector Framework – Übersicht

Die Agent Client Collector Framework Ermöglicht Unternehmen die Überwachung und Verwaltung der Integrität ihrer Infrastruktur über Agents, die auf wichtigen Systemen installiert sind. Diese Service Desk-Mitarbeiter führen vordefinierte Befehle auf den Computern aus, auf denen sie installiert sind, und senden die resultierenden Daten an die zurück ServiceNow® Instanz über ein dediziertes MID-Server. Das -Framework ermöglicht die nahtlose Verwaltung von beiden Agent Client Collector Und MID-Server, Speichert Ereignisdaten und Leistungsmetriken in der entsprechenden Datenbank. Durch Einblicke in die CI-Leistung hilft ACC-F Organisationen, Probleme schnell zu identifizieren und zu lösen, wodurch die betriebliche Effizienz und die Systemzuverlässigkeit verbessert werden.

Agent Client Collector Framework – Workflow

Die folgende Abbildung beschreibt das Layout und den Daten-Flow in Agent Client Collector Framework Anwendung.

Erfassen und Verteilen von Daten mit ACC-F



1. Agent-Installation: Der Agent wird auf Infrastrukturkomponenten wie Servern, Geräten und Netzwerkgeräten installiert. Diese Service Desk-Mitarbeiter sind für die Ausführung von Systembefehlen und die Erfassung von Leistungsdaten vom Hostcomputer verantwortlich. ACC-F wird auf dem des Kunden bereitgestellt ServiceNow® Instanz.
2. Datensammlung: Der Service Desk-Mitarbeiter führt vordefinierte Skripts oder Abfragen (Prüfungen) für die Infrastrukturkomponenten aus, um verschiedene Systemmetriken und -Ereignisse zu erfassen. Dies umfasst Leistungsdaten wie CPU-Auslastung, Arbeitsspeichernutzung, Festplattenspeicher und Netzwerkaktivität. Der Service Desk-Mitarbeiter erfasst auch Fehlerprotokolle und Systemwarnungen.
3. MID-Server Kommunikation: Der Service Desk-Mitarbeiter sendet die gesammelten Daten an die ServiceNow Instanz über ein dediziertes MID-Server. Die MID-Server Fungiert als sichere Kommunikationsbrücke zwischen der Infrastruktur und der ServiceNow-Plattform, um sicherzustellen, dass Daten zuverlässig und sicher übertragen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Datenspeicher: Nach Erhalt der Daten wird ServiceNow Die Instanz speichert die Ereignisse und Leistungsmetriken in der relevanten Datenbank. Diese Daten werden dann den jeweiligen Konfigurationselementen (Configuration Items, CIs) in zugeordnet ServiceNow CMDB Configuration Management Database (CMDB), Ermöglicht eine effiziente Nachverfolgung und Berichterstellung.
5. Datenanalyse und -Berichterstellung: Die erfassten Daten werden innerhalb von analysiert ServiceNow Instanz, in der sie für Überwachungs-, Fehlerbehebungs- und Berichtszwecke verwendet wird. Diese Analyse hilft, potenzielle Probleme oder Verbesserungsbereiche zu identifizieren und Warnungen oder Aktionen auszulösen, um Probleme proaktiv zu lösen.
6. Feedback-Schleife: Basierend auf der Analyse kann das System Korrekturaktionen auslösen, z. B. das Ausführen von Korrekturskripts, das Neukonfigurieren von Einstellungen oder das Benachrichtigen verantwortlicher Teams für weitere Untersuchungen. Das Feedback wird zurück in das System geschleift, was eine kontinuierliche Überwachung und Optimierung ermöglicht.

Agent Client Collector Framework – Vorteile

Agent Client Collector Framework Stellt Daten für andere bereit Agent Client Collector Komponenten.

Vorteil	Funktion	Anwender
Überwachen Sie die Integrität, Leistung und Verfügbarkeit Ihres Systems durch die automatisierte Erfassung von Ereignissen und Metriken, wobei automatisierte Konfigurationen genutzt werden.	Agent Client Collector-Überwachung	NOC-Anwender, Ereignismanagement Administrator
Verfolgen Sie den Serverbestand, Softwareinstallationen und die Nutzung kontinuierlich mit nicht-Administratorzugriff und minimaler Netzwerkkommunikation.	Agent Client Collector Visibility – Inhalt	CMDB/Discovery-Administrator
Erfassen Sie detaillierte Bestandsdaten von Geräten, die nicht mit Ihrem Netzwerk verbunden sind oder in isolierten Umgebungen ausgeführt werden (Air-Gaps).	Agent Client Collector Framework – Air Gapped Configuration Item Management-Lösung	CMDB/Discovery-Administrator
Minimieren Sie die Selektierungszeit von Incidents, indem Sie direkt auf Live-Gerätedetails und -Interaktionen zugreifen, um sie zu beheben.	Live-CI-Daten mit Agent Client Collector anzeigen	ITSM-Anwender
Löst Remote-Aktionen für verwaltete Geräte aus, ohne zusätzliche Anmeldeinformationen oder Netzwerkkommunikation.	Agent Client Collector Security Incident Response	Automatisierungsexperte
Streamen Sie Protokolldaten in Ihre Instanz, um Probleme vorherzusagen und zu lösen, bevor sie auftreten, um die Auswirkungen auf die Anwender zu minimieren.	Agent Client Collector Log Analytics	Agent Client Collector-Administrator

Agent Client Collector Framework – Anwendungsfall

Die Agent Client Collector Framework Der Anwendungsfall zeigt, wie eine Finanzorganisation verwenden kann Agent Client Collector Framework Zur Unterstützung der IT-Asset-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfallübersicht

Eine führende Finanzorganisation benötigte eine robuste IT-Discovery-Lösung, um Compliance aufrechtzuerhalten, kritische Systeme zu sichern und ein wachsendes Remote-Personal zu verwalten. Während die Organisation anfänglich auf agentenlose Discovery-Methoden angewiesen war – wo MID Servers Fragen Sie Systeme ab, und füllen Sie die CMDB aus – sie stand vor erheblichen Herausforderungen. Diese Einschränkungen beeinträchtigten ihre Fähigkeit, sichere Umgebungen und Remote-Endpunkte effektiv zu überwachen, was zu potenziellen Sicherheits- und Compliance-Risiken führte.

Herausforderungen

- Eingeschränkter Serverzugriff: Die Sicherheitsrichtlinien der Finanzorganisation sind eingeschränkt MID Servers Von der Initiierung von Verbindungen zu Core-Banking-Servern und vertraulichen Finanzdatenbanken. Dadurch ist die agentenlose Discovery für diese Assets mit hoher Sicherheit unzureichend.
- Remote-Sichtbarkeit der Belegschaft: Die wachsende Remote-Belegschaft des Unternehmens bedeutete, dass viele Mitarbeiter-Laptops und Mobilgeräte außerhalb des Unternehmensnetzwerks betrieben wurden. Die agentenlose Discovery konnte keine Daten von diesen Endpunkten erfassen, wodurch bei der Asset-Nachverfolgung und Compliance-Überwachung blinde Flecken entstehen.
- Regulatorische Compliance: Finanzinstitute müssen strengen Vorschriften (z. B. PCI, DSS und SOX) unterliegen, die detaillierte und auditierbare Asset-Daten erfordern. Die agentenlose Discovery hatte Probleme, diese Anforderungen zu erfüllen, insbesondere für die eingehende Überwachung und Richtliniendurchsetzung.

Lösungen

Um diese Herausforderungen zu bewältigen, implementierte die Finanzorganisation einen Agent-basierten Discovery-Ansatz.

- Agent-Bereitstellung auf kritischen Servern: Service Desk-Mitarbeiter wurden auf Core-Banking-Servern und sensiblen Finanzdatenbanken installiert. Dies ermöglichte eine kontinuierliche, sichere Überwachung ohne Verstoß gegen Zugriffsbeschränkungen.
- Remote-Endpunktverwaltung: Service Desk-Mitarbeiter, die auf Remote-Mitarbeiter-Laptops bereitgestellt werden, bieten Echtzeit-Datensammlung und -Überwachung, unabhängig vom Standort. Dadurch wurde sichergestellt, dass alle Geräte, auch solche außerhalb des Unternehmensnetzwerks, in die Asset-Discovery einbezogen wurden.
- Erweiterte Datensammlung: Die Service Desk-Mitarbeiter haben detaillierte Systeminformationen und erzwungene Sicherheitsrichtlinien direkt für jedes Asset erfasst, um die Compliance mit regulatorischen Standards sicherzustellen und die Auditbereitschaft zu verbessern.

Ergebnisse

- Umfassende Asset-Transparenz: Die Organisation erzielte vollständige Transparenz in ihrer gesamten IT-Umgebung, einschließlich sicherer Rechenzentren und Remote-Endpunkte. Dies reduzierte blinde Flecken und verbesserte die Entscheidungsfindung für IT-Betriebs- und Sicherheitsteams.
- Verbesserte Compliance- und Audit-Bereitschaft: Die Agent-basierte Discovery lieferte granulare, auditierbare Daten, die strenge regulatorische Anforderungen erfüllten. Dies

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

hat die Compliance-Berichterstellung optimiert und das Risiko regulatorischer Strafen reduziert.

- Verbesserte Sicherheitslage: Durch die Durchsetzung von Richtlinien auf Endpunktebene hat die Organisation ihre Cybersicherheitsmaßnahmen gestärkt und vertrauliche Finanzdaten vor potenziellen Bedrohungen geschützt.

Dieser Ansatz ermöglichte es dem Finanzinstitut, die Kontrolle über seine IT-Umgebung zu behalten, seine Remote-Mitarbeiter effektiv zu unterstützen und die Compliance mit Branchenvorschriften sicherzustellen – entscheidende Faktoren für den Schutz sensibler Finanzvorgänge und die Aufrechterhaltung des Kundenvertrauens.

Agent Client Collector-Architektur

Agent Client Collector ist ein ServiceNow-Agent, der zur Überwachung der Infrastruktur und der installierten Anwendungen Ihres Unternehmens auf Windows-, Linux- und macOS-Geräten installiert ist.

Agent Client Collector Architektur: Übersicht

Agent Client Collector basiert auf einem Sensu-Framework und wird mit Überwachungsfunktionen für Server, Datenbanken, Anwendungsserver und Middleware installiert. Außerdem wird die Überwachung durch zusätzliche Prüfungen der Sensu-Community oder Nagios-kompatibler Plugins erweitert, sodass Sie die Überwachung an Ihre Anforderungen anpassen können.

Überwachung mit Prüfungen und Richtlinien

Der Service Desk-Mitarbeiter führt Prüfungen auf dem Host durch, um relevante Daten zu sammeln und sie in Ereignisse oder Metriken umzuwandeln. Diese Prüfungen sind in definiert ServiceNow Und sind Überwachungsrichtlinien zugeordnet. Eine Richtlinie ist eine Kombination aus den überwachten Konfigurationselementen (Configuration Items, CIs) und den Prüfungen, die für diese CIs ausgeführt werden. Die Prüfungen sind Richtlinien zugeordnet, um verschiedene Aspekte des Systems zu überwachen.

Sie können Prüfungsinstanzen anpassen, z. B. die Häufigkeit anpassen oder Parameter wie Anmeldeinformationen für Datenbanken angeben, ohne die ursprüngliche Prüfungsdefinition zu beeinträchtigen. Die Anpassung einer Prüfinstanz wirkt sich nur auf die Prüfinstanz aus, die der Richtlinie zugeordnet ist, und ändert die globale Prüfungsdefinition nicht. Diese Anpassung gewährleistet Flexibilität bei der Überwachung verschiedener CIs in verschiedenen Szenarien.

Datensammlung und -Übertragung

Nach der Installation sammelt der Service Desk-Mitarbeiter Informationen zu seinem Host und seinen Prozessen. Der Service Desk-Mitarbeiter sendet die gesammelten Daten an den ServiceNow Instanz über MID-Server. Die MID-Server Dient als Brücke zwischen dem Service Desk-Mitarbeiter und dem ServiceNow Instanz, die sicherstellt, dass die Daten umgewandelt und sicher zur Verarbeitung gesendet werden.

In der Instanz werden CIs für den Host und Anwendungen erstellt, die aus den laufenden Prozessen klassifiziert sind (z. B. Microsoft SQL Server). Sobald diese CIs erstellt wurden, werden die aktiven Überwachungsrichtlinien, die den CIs zugeordnet sind, in die des Service Desk-Mitarbeiters heruntergeladen MID-Server, Der dann die Richtlinien zur Ausführung an den Service Desk-Mitarbeiter weitergibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenspeicherung und -Verwendung

Die Ergebnisse der Prüfungen werden in gespeichert ServiceNow Instanz:

- CI-Daten: CMDB Für Konfigurationselemente.
- Ereignisdaten: Ereignistabelle (z. B. Warnungen, die durch Schwellenwertverletzungen ausgelöst werden).

Diese Daten können für Überwachung, Warnungen und Berichterstellung genutzt werden. Die Integration gewährleistet Echtzeittransparenz in die Integrität Ihrer Infrastruktur und Anwendungen und ermöglicht gleichzeitig die proaktive Problemerkennung und -Behebung.

1. Definieren Sie eine Überwachungsrichtlinie in ServiceNow Instanz.
2. Die MID-Server Ruft die Prüfinstanzen aus der Instanz ab und übergibt sie an den Service Desk-Mitarbeiter.
3. Der Service Desk-Mitarbeiter führt die Prüfungen aus, sammelt Daten und sendet die Ergebnisse an zurück MID-Server.
4. Die MID-Server Sendet die gesammelten Daten an die ServiceNow Instanz, in der sie gespeichert ist CMDB Oder Ereignistabellen.

Die Befehle und deren Konfigurationen, die für den Agent ausgeführt werden, werden als **Prüfungen** bezeichnet. Im Umfang des Agent sind standardmäßig **Prüfungsdefinitionen** enthalten, die einen bestimmten Befehl und die standardmäßige Häufigkeit festlegen, mit der er ausgeführt wird. Prüfungen werden für die Instanz definiert und über den MID-Server an den Agent übergeben.

Eine **Richtlinie** ist eine Kombination der durch Agent Client Collector überwachten CIs und der Prüfungen, die für diese CIs ausgeführt werden. Sie verknüpfen Prüfungsdefinitionen mit Richtlinien. Diese Prüfungsdefinitionen werden dann als **Prüfungsinstanzen** bezeichnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Prüfungsinstanzen entsprechend Ihren Anforderungen anpassen. Passen Sie beispielsweise das Ausführungsintervall oder die für die Richtlinie spezifischen Parameter an, z. B. die Anmeldeinformationen für den Zugriff auf eine MySQL-Datenbank. Die Anpassung einer Prüfungsinstanz wird nur für die mit der Richtlinie verknüpfte Prüfungsinstanz wirksam, wirkt sich also nicht auf die ursprüngliche Prüfungsdefinition oder bereits erstellte Prüfungsinstanzen in anderen Richtlinien aus.

Agent Client Collector-Plugins

Ein Agent Client Collector Plugin ist ein Skript oder eine Gruppe von Skripts, die erweitern Agent Client Collector Fähigkeiten von . Plugins verbessern die Überwachung, indem sie Metriken erfassen, spezielle Prüfungen durchführen und Ereignisse basierend auf Bedingungen auslösen, z. B. die Warteschlangengröße einer Anwendung überwachen, wenn sie 60 % oder 80 % erreicht. Plugins stellen eine skalierbare, anpassbare Überwachung sicher, um sich an sich entwickelnde Infrastruktur- oder Anwendungsanforderungen anzupassen.

Plugin-Check-Abhängigkeit

Plugins sind eng mit Prüfungen in integriert Agent Client Collector Framework. Zwischen dem Plugin und der Prüfung wird eine Abhängigkeit erstellt, um sicherzustellen, dass das Plugin neben der zugehörigen Prüfung ausgeführt wird.

- Plugin-Abhängigkeit: Ein Plugin kann einer oder mehreren Prüfungen zugeordnet werden und umgekehrt, wobei Prüfungen von mehreren Plugins abhängen können.
- Ausführung: Plugins und Prüfungen werden auf demselben Service Desk-Mitarbeiter ausgeführt und arbeiten zusammen, um Daten zu sammeln, spezielle Aufgaben auszuführen oder erforderliche Ereignisse auszulösen

Erstellen und Verwalten von Plugins

Sie können erstellen Agent Client Collector Plugins nach Bedarf, um die Überwachung an Ihre spezifische Umgebung anzupassen. Diese Plugins sind normalerweise als tar.gz-Dateien formatiert, die die Skripts enthalten, die die Funktionalität des Plugins definieren.

- Plugin-Erstellung: Anwenderdefinierte Plugins werden entwickelt und in tar.gz-Dateien verpackt.
- Integration mit Prüfungen: Nach der Erstellung wird das Plugin mit Prüfungen integriert, indem die entsprechenden Abhängigkeiten festgelegt werden, um sicherzustellen, dass Plugin und Prüfung zusammen ausgeführt werden.
- Anpassung: Plugins können angepasst werden, um die spezifischen Anforderungen Ihrer Überwachungsanforderungen zu erfüllen, egal ob es sich um das Hinzufügen detaillierterer Metriken, das Überprüfen von Systemschwellenwerten oder das Generieren anwenderdefinierter Ereignisse handelt.

Vorinstallierte Plugins

Agent Client Collector Framework Enthält eine Reihe vorinstallierter Plugins, die grundlegende Funktionen für allgemeine Überwachungsaufgaben bereitstellen, z. B. das Sammeln von Standardmetriken oder die Überwachung wichtiger Systemparameter. Für detailliertere Informationen zu den Plugins, die im Lieferumfang enthalten sind Agent Client Collector Als Teil von ITOM-Integrität, Siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Überprüfen Sie die Datensammlung in Agent Client Collector

Sammeln Sie Daten, indem Sie wichtige Informationen aus dem Hostsystem eines Service Desk-Mitarbeiters sammeln, bevor Sie Prüfungen oder Richtlinien ausführen. Dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess stellt sicher, dass die Agent Client Collector Verfügt über genaue und aktuelle Daten zu Infrastruktur, Prozessen und Anwendungen, die auf dem Host ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Gesammelte Daten werden als Konfigurationselementdaten (Configuration Item, CI) gespeichert, die als Grundlage für Überwachung, Warnungen und dienen Metrikdaten In ServiceNow® Instanz.

Bevor Prüfungen und Richtlinien ausgeführt werden können, Agent Client Collector Sammelt Daten zu:

- Hostsystemdetails (z. B. Hardware und Betriebssystemversion des Systems)
- Installierte Anwendungen und Services
- Ausführen von Prozessen
- Ressourcennutzungsmetriken (z. B. CPU-, Arbeitsspeicher- und Datenträgerauslastung)

Erfasste Daten werden in gespeichert ServiceNow Instanz in entweder CMDB(Configuration Management Database) oder Ereignistabelle.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Suchen Sie auf der Seite „Agent Client Collectors“ nach **Hostdatensammlung** Spalte für einen Service Desk-Mitarbeiter.
   Ein grünes gesammeltes Symbol Collected Gibt eine erfolgreiche Datensammlung für den spezifischen Service Desk-Mitarbeiter an.

Prüfungen und Richtlinien

Eine Prüfung ist eine Kombination aus einem Befehl und der zugehörigen Konfiguration. Die Prüfung wird auf ausgeführt Agent Client Collector Geräte von , um Daten von diesen Geräten zu erfassen.

Überprüfungen

Prüfungen werden mit dem Basissystem bereitgestellt. Mit diesen Befehlen werden Skripts ausgeführt, die Überwachungsdaten für Ihre Betriebssysteme und Anwendungen bereitstellen. Der Standardname einer Prüfung gibt den Gegenstand der Überwachung/Messung, die Entität und die Überwachungsdaten an. Zum Beispiel ein Scheck mit dem Namen `os.linux.check-system-cpu`Überprüft die CPU-Daten auf einem Linux System. Der in der Prüfung identifizierte Befehl wird auf dem überwachten Gerät ausgeführt und liefert eine Ausgabe und einen Status. Jeder einzelne Scheck wird als bezeichnet **Prüfungsdefinition** . Nach der Zuordnung zu Richtlinien werden Prüfungsdefinitionen als bezeichnet **Überprüfen Sie Instanzen** .

Sie können Prüfungsinstanzen entsprechend Ihren Anforderungen anpassen. Passen Sie beispielsweise das Ausführungsintervall oder die für die Richtlinie spezifischen Parameter an, z. B. die Anmeldeinformationen für den Zugriff auf eine MySQL-Datenbank. Die Anpassung einer Prüfungsinstanz wird nur für die mit der Richtlinie verknüpfte Prüfungsinstanz wirksam, wirkt sich also nicht auf die ursprüngliche Prüfungsdefinition oder bereits erstellte Prüfungsinstanzen in anderen Richtlinien aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Prüfungstypen gehören zum Lieferumfang des Ereignismanagement-Basissystems:

- **Event**: Das Ergebnis der Prüfung wird in ein Ereignismanagement-Event umgewandelt.
- **Metrik**: Die Werte aus dem Prüfungsergebnis werden in Metriken umgewandelt.

Für Details zu Agent Client Collector Framework Standardprüfungen, siehe Standardprüfungen des Agent Client Collector-Framework.

Für Details zu Agent Client Collector-Überwachung Standardprüfungen und -Richtlinien, siehe Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.

Für Details zu Agent Client Collector Visibility – Inhalt Standardprüfungen und -Richtlinien, siehe Agent Client Collector Visibility – Inhalt – Standardprüfungen und Richtlinien.

Wenn auf den Geräten des Agent keine Prüfungen ausgeführt werden, befindet sich der Agent möglicherweise im CPU-Schutzmodus. Der CPU-Schutzmodus wird aktiviert, wenn der CPU-Verbrauch eines Geräts zu hoch ist. Um eine Liste aller deaktivierten Prüfungen im Zusammenhang mit dem Service Desk-Mitarbeiter anzuzeigen, navigieren Sie auf der Seite „Agent Client Collectors“ zum Agent-Datensatz (**Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**), wählen Sie einen Service Desk-Mitarbeiter und dann aus **Deaktivierte Prüfungen** Registerkarte unten auf der Seite.

In acc.yml Konfigurationsdatei können Sie die Schwellenwerte für den CPU-Schutzmodus ändern, die bestimmen, wann eine Prüfung deaktiviert ist. Um eine Prüfung erneut zu aktivieren, wählen Sie die Prüfung aus, und wählen Sie aus **Deaktivieren Sie die Prüfung erneut** In **Aktionen für ausgewählte Zeilen...** Dropdown-Liste. Details zu den Schwellenwerten für den CPU-Schutzmodus finden Sie unter Agent Client Collector-CPU-Schutzschwellenwerte. Einzelheiten zum manuellen Deaktivieren der Datensammlung finden Sie unter Agent Client Collector-Datensammlung anhalten.

Konfigurieren Sie die Eigenschaft cpu_Protection_Behavior, um zu bestimmen, ob alle Prüfungen in den CPU-Schutzmodus wechseln, oder nur die Prüfung, die den konfigurierten cpu_percentage_limit-Wert mit der höchsten CPU-Auslastung innerhalb des Überwachungsintervalls überschreitet. Details finden Sie unter Agent Client Collector-CPU-Schutzschwellenwerte.

Ein Scheck ist als markiert **Veraltet** Wenn es keiner Richtlinie mehr zugeordnet ist. Um einen veralteten Scheck zu entfernen, aktivieren Sie ihn, indem Sie das Kontrollkästchen neben dem Scheck aktivieren und auswählen **Deaktivieren Sie Prüfungen erneut** Von **Aktionen für ausgewählte Zeilen...** Zelle.

Im Basissystem gibt der Beendigungsstatus des Events wie folgt seinen Schweregrad an:

- 0 = OK
- 1 = WARNUNG
- 2 = KRITISCH

Sie können zusätzliche Schweregrade hinzufügen (z. B. SCHWERWIEGEND und GERINGFÜGIG), indem Sie ein benutzerdefiniertes Skript ausführen. Die folgenden Beendigungsstatus geben diese Schweregrade an:

- 13 = SCHWERWIEGEND
- 14 = GERINGFÜGIG

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungen für die Ausführung von Prüfungsbefehlen

Wenn der servicenow-Basissystemanwender nicht über die Berechtigungen zum Ausführen bestimmter Prüfungsbefehle verfügt, gehen Sie für die relevanten Betriebssysteme wie folgt vor:

- Unter Linux: Erteilen Sie Benutzer servicenow die Berechtigung, den Befehl mit sudo-Berechtigungen auszuführen. Stellen Sie sicher, dass die folgenden Sudo-Konfigurationsanforderungen erfüllt sind:
  - tty-Anforderungen und Passwortanforderungen deaktiviert
  - Alle Umgebungsvariablen beibehalten
  - Zur Ausführung von Befehlen Unterstützung eines dynamischen PATH

  Beispielkonfiguration in /Etc/sudoers Datei:

```
Cmnd_Alias ACC_F = /usr/sbin/dmidecode -s
 baseboard-serial-number, /usr/sbin/dmidecode -s
 chassis-serial-number, /usr/sbin/dmidecode -s system-serial-number, /usr/sbin/dmidecode
 -s system-uuid, /usr/sbin/ss -tanp
servicenow ALL=(root)
 SETENV: /var/cache/servicenow/agent-client-collector/osquery/bin/osqueryi *, ACC_F
Defaults:servicenow !requiretty
Defaults exempt_group += servicenow
```

  Hinweis: Befehlspfade können variieren. Weitere Informationen finden Sie im Handbuch für Sudoers.

  - Die Zeichenfolge SETENV: ermöglicht dem Benutzer servicenow die Beibehaltung von Umgebungsvariablen.
  - Durch die Zeichenfolge !requiretty wird tty deaktiviert.
  - Durch Hinzufügen des Benutzers servicenow zu exempt_group werden die Passwortanforderungen umgangen und dynamische PATH-Variablen zur Ausführung von sudo-Befehlen aktiviert.

  Stellen Sie sicher, dass Sie in der Prüfungsdefinition im Abschnitt zu den Prüfbefehlparametern den Prüfungsparameter *must_sudo* mit dem Wert **true** konfigurieren.

- In einem macOS System: Stellen Sie sicher, dass der Anwender, der den Agent-Service ausführt, zu einer Anwendergruppe mit Berechtigungen zum Abfragen aller tcp-Verbindungen auf dem Host gehört.
- In einem Windows System: Wird verwendet Windows Anwenderverwaltung: Fügen Sie den servicenow-Anwender den Gruppen mit den entsprechenden Berechtigungen hinzu, damit der Anwender die erforderlichen Befehle ausführen kann.

Richtlinien

A **Richtlinie** Ist eine Kombination der CIs, die von überwacht werden Agent Client Collector Und die Prüfungsdefinitionen, die für diese CIs ausgeführt werden.

Damit eine einzelne Richtlinie mehrere Anmeldeinformationen unterstützt, weisen Sie der Richtlinie einen Anmeldeinformationsalias zu. Beispiel: Wenn Sie MySQL-Server für beide haben Linux Und Windows Mit unterschiedlichen Anmeldeinformationen müssen Sie für jeden Anmeldeinformationstyp separate Richtlinien erstellen. Wenn Sie jedoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einen Anmeldeinformationsalias verwenden, können Sie dem Alias eine einzelne Richtlinie zuweisen. Der Agent ordnet dann die relevanten Anmeldeinformationen der überwachten Anwendung zu. Weitere Informationen zu Anmeldeinformationsaliassen finden Sie unter Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen .

Warnungen, die von Richtlinien mit einer Prüfung vom Ereignistyp generiert werden, werden automatisch geschlossen, wenn die CI-Überwachung aufgrund einer der folgenden Gründe beendet wird:

- Deaktivierung der Richtlinie
- Deaktivierung der Prüfung, die die Warnung verursacht hat
- Löschung der Prüfung aus der Richtlinie
- Löschung der Richtlinie
- Änderung des Richtlinienfilters, der die überwachten CIs bestimmt

Parameter in sichern Agent Client Collector

Parameter in sichern Agent Client Collector(ACC) bezieht sich auf die sichere Übergabe vertraulicher Daten wie Anwendernamen, Passwörter und API-Schlüssel während der Ausführung der Prüfung, ohne die sensiblen Daten in der Befehlszeile offenzulegen. Parameter werden über die Standardeingabe (STDIN) an das Skript übergeben, wodurch sie in Protokollen oder anderen Prozessen ausgeblendet werden, die Befehlszeilenargumente erfassen könnten.

Je nach verwendeter Codierungssprache kann die Implementierung sicherer Parameter variieren. Beispiel: Unter Linux wird in Bash der Befehl `read` (`read <variable_name>`) verwendet, wobei `<variable_name>` durch den in STDIN eingegebenen Wert ersetzt wird.

Sicherer Parameterdatenfluss

1. Sichere Parameter erstellen: Definieren Sie sichere Parameter in der Instanz, und verweisen Sie auf Anmeldeinformationen, die geschützt werden müssen (z. B. Anwendernamen und Passwörter). Details finden Sie unter Sichere Parameter für Prüfungen erstellen.
2. Sichere Parameter konfigurieren: Legen Sie einen fest **Reihenfolge** Wert zur Bestimmung der Reihenfolge, in der Anmeldeinformationen an die Standardeingabe übergeben werden.
3. Anmeldeinformationen übergeben: Übertragen Sie Anmeldeinformationen aus dem MID-Server An den Service Desk-Mitarbeiter basierend auf dem Scheck, dem er zugewiesen ist. Wenn die Prüfung ausgeführt wird, übergibt der Agent die gesicherten Parameter mit STDIN an das Skript in der Reihenfolge, die durch den in der Instanz konfigurierten Wert für die **Reihenfolge** angegeben ist.
4. Prüfung ausführen: Nach der Ausführung senden die Service Desk-Mitarbeiter die sicheren Parameter über STDIN in der angegebenen Reihenfolge an das Skript.
5. Skript ausführen: Das Skript ruft die sicheren Parameter aus STDIN ab und verwendet sie zur Ausführung mit den gesicherten Anmeldeinformationen.

Vorteile von sicheren Parametern

- Verbesserte Sicherheit: Die Weitergabe vertraulicher Daten wie Anwendernamen und Passwörter direkt in der Befehlszeile stellt eine Sicherheitsbedrohung dar, da sie nicht autorisiertem Zugriff oder böswilligen Anwendern ausgesetzt sein könnten. Sichere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter stellen sicher, dass solche Daten sicher verarbeitet und in der Ansicht ausgeblendet werden.

- Datenfreigabe verhindern: Bei Verwendung sicherer Parameter werden die Anmeldeinformationen nicht im nur-Text-Format in der Befehlszeile geschrieben, wodurch das Risiko vermieden wird, dass sie in Protokollen oder Prozesslisten erfasst werden.
- Datenflusssteuerung: Sichere Parameter ermöglichen die kontrollierte und anpassbare Übergabe von Anmeldeinformationen an das Skript, um die korrekte Verarbeitung und den richtigen Zeitpunkt vertraulicher Informationen sicherzustellen.

Agent Client Collector Konfigurationsdatendateien

Konfigurationsdatendateien speichern dynamische Instanzdaten, z. B. VM-Details, die während der Ausführung von Prüfungsdefinitionen verwendet werden. Dadurch wird sichergestellt, dass Prüfungen mit aktuellen und genauen Informationen über die überwachte Instanz ausgeführt werden.

Struktur der Konfigurationsdatendateien

- Anhangsbasiert: Eine Konfigurationsdatendatei enthält einen einzelnen Anhang mit Instanzdaten, z. B. Azure VM-Details.
- Synchronisierung: Wenn ein Anhang hinzugefügt oder gelöscht wird, wird die Datendatei für alle synchronisiert MID Servers Mit konfiguriert Agent Client Collector. Wenn eine Datei oder ihr Anhang gelöscht wird, wird sie auch aus entfernt MID-Server.
- Zugriffspunkt: Auf die Konfigurationsdatendateien kann im zugegriffen werden MID-Server Um Statisch/Cache/config-files .
- Größe: Konfigurationsdatendateien dürfen nicht größer als 10 MB sein.

Prüfungsdefinitionen, die von Konfigurationsdatendateien verwendet werden

- Prüfungsdefinition: Einzelne Prüfungseinträge werden als Prüfungsdefinitionen bezeichnet. Beispiel: *`os.linux.check-system-cpu`*Überprüft die CPU in Linux Systeme.
- Zugriff auf Prüfungsdefinitionen: Über kann auf Prüfungsdefinitionen zugegriffen werden **Alle** > **Agent Client Collector** > **Konfiguration** > **Prüfungsdefinitionen**an.

Dateizuordnung

- Download-Prozess: Wenn eine Prüfung ausgeführt wird, lädt der Service Desk-Mitarbeiter die Konfigurationsdatendatei herunter, die dieser Prüfung zugeordnet ist.
- Domänenspezifische Synchronisierung: Dateien werden nur mit Service Desk-Mitarbeitern innerhalb derselben Domäne synchronisiert, um eine sichere und lokalisierte Datenverarbeitung sicherzustellen.

Arbeiten mit Konfigurationsdatendateien

Konfigurationsdatendateien dienen als Repository für dynamische Instanzdaten, die von Prüfungsdefinitionen verwendet werden, wenn sie ausgeführt werden. Diese Dateien stellen sicher, dass Prüfungen mit genauen Echtzeitinformationen zu den überwachten Systemen oder Instanzen ausgeführt werden. Konfigurationsdatendateien funktionieren wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Instanzspezifische Daten speichern: Konfigurationsdatendateien speichern dynamische Instanzdaten, z. B. VM-Details, Serverkonfigurationen und andere systemspezifische Informationen. Diese Daten werden während der Ausführung von Prüfungsdefinitionen verwendet, um sicherzustellen, dass die neuesten Informationen verfügbar sind.
- Prüfungsdefinitionen erstellen: Eine Prüfungsdefinition wird mit einer zugehörigen Konfigurationsdatendatei erstellt. Beispielsweise kann eine Prüfungsdefinition, die die CPU-Daten des Systems überwacht, Konfigurationsdaten enthalten, die die Systemumgebung detaillieren und sicherstellen, dass Prüfungen genaue und relevante Instanzdaten verwenden.
- Synchronisieren Sie mit MID Servers: Wenn eine Konfigurationsdatendatei hinzugefügt oder aktualisiert wird, wird sie alle synchronisiert MID Servers Kommunikation mit Agent Client Collector. Wenn die Datei oder der Anhang gelöscht wird, wird sie auch aus dem entfernt MID Servers, Stellt Konsistenz und aktuelle Datenverfügbarkeit sicher.
- Mit aktualisierten Daten ausführen: Während der Ausführung wird die ausgeführt Agent Client Collector Service Desk-Mitarbeiter lädt die relevante Konfigurationsdatendatei aus dem herunter MID-Server. Der Service Desk-Mitarbeiter verwendet diese Daten, um die Prüfung auszuführen und den Zugriff auf die aktuellsten und genauesten Instanzinformationen sicherzustellen.
- Daten speichern und abrufen: Konfigurationsdatendateien werden im gespeichert MID-Server In Statisch/Cache/config-files Verzeichnis. Dieser Speicherort erleichtert den einfachen Zugriff und die Verwaltung und stellt sicher, dass die erforderlichen Daten für Prüfungen bei Bedarf immer verfügbar sind.

Agent Client Collector Protokolle

Agent Client Collector (ACC) Protokolle spielen eine entscheidende Rolle bei der Überwachung der Aktivität und Leistung des Service Desk-Mitarbeiters. Protokolle bieten wertvolles Feedback, das hilft, potenzielle Probleme zu identifizieren, insbesondere wenn die Leistung des Service Desk-Mitarbeiters suboptimal ist. Durch die Bereitstellung von Einblicken in Problembereiche sind diese Protokolle wichtig für die Fehlerbehebung und Lösung von Problemen und verbessern letztlich die Gesamteffektivität des Service Desk-Mitarbeiters.

Agent Client Collector (ACC) Protokolle bieten wichtige Vorteile für die Überwachung und Aufrechterhaltung der Leistung von Service Desk-Mitarbeitern.

- Konfigurierbare Schweregradstufen: Agent Client Collector Mit Protokollen können Sie die Schweregradstufen für die Überwachung konfigurieren, einschließlich `Error`, `Debug`, Und `Info`. Diese Flexibilität hilft, sich auf bestimmte Bereiche zu konzentrieren, z. B. die Nachverfolgung von Fehlern oder die Diagnose von Problemen.
- Verwaltung der Protokollaufbewahrung: Sie können Richtlinien zur Protokollaufbewahrung einrichten, um festzulegen, wie oft Protokolle gelöscht werden sollen, um Systemressourcen zu erhalten. Dadurch wird sichergestellt, dass die Protokolle verwaltbar bleiben und sich nicht negativ auf die Systemleistung auswirken.
- Identifizierung von Leistungsproblemen: Protokolle bieten wertvolle Einblicke, um Bereiche zu identifizieren, in denen Service Desk-Mitarbeiter möglicherweise Probleme haben, und tragen so zur Verbesserung der Leistung von Service Desk-Mitarbeitern bei.

Für Details zum Suchen und Verwalten Agent Client Collector Protokolle, siehe Agent Client Collector-Protokolle anzeigen.

Agent Client Collector-API

Verwenden Sie Agent Client Collector(ACC) API zum Erstellen eines Flows, der einen ausführt `Osquery` Befehl für Service Desk-Mitarbeiter und verarbeitet die Ergebnisse. Durch die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutzung der ACC-API können Sie die Abfrage von Mitarbeiterdaten automatisieren und die Verarbeitung von Ergebnissen optimieren, wodurch die Überwachung und Verwaltung der Systemleistung erleichtert wird.

Das System unterstützt osquery 5,7.0, was Kompatibilität mit einer Reihe von Abfragen für eine effiziente Datensammlung bietet.

Die ACC-API ermöglicht eine nahtlose Integration und Automatisierung für die Ausführung von Abfragen und die Verwaltung von Service Desk-Mitarbeitern. So funktioniert es:

1. Osquery-Befehle ausführen: Sie können die ACC-API verwenden, um osquery-Befehle an Service Desk-Mitarbeiter zu senden. Diese Befehle erfassen eine Vielzahl von System- und Leistungsdaten von den Zielcomputern.
2. Ergebnisse verarbeiten: Nachdem der osquery-Befehl für die Agents ausgeführt wurde, verarbeitet die ACC-API die Ergebnisse und gibt die erforderlichen Daten zurück. Diese Daten können für Überwachungs-, Problembehandlungs- oder Berichterstellungszwecke verwendet werden.
3. Unterstützung für osquery 5,7.0: Die ACC-API ist mit osquery 5,7 kompatibel. Dadurch wird sichergestellt, dass die neuesten Funktionen und Verbesserungen unterstützt werden, sodass Sie erweiterte Abfragefunktionen für eine verbesserte Datensammlung nutzen können.
4. API-Funktionen aktivieren: Um die ACC-API zu verwenden, aktivieren Sie die Agent- und Richtlinien-APIs. Auf diese Weise können Sie verschiedene Aspekte Ihrer Service Desk-Mitarbeiter konfigurieren und verwalten, einschließlich ihrer Kommunikation, Datensammlung und Abfrageausführung.

Weitere Informationen zu Agent-APIs finden Sie unter Aktivieren Sie Agent APIs .

Details zum Aktivieren von Richtlinien-APIs finden Sie unter Aktivieren Sie Richtlinien-APIs .

Agent Client Collector Scan-Suite für Integritätsinstanz

Die Agent Client Collector Die Scan-Suite für Integritätsinstanzen (ACC) besteht aus Prüfungen, die Anomalien und andere Probleme erkennen, die in Ihrer Instanz auftreten können. Diese Prüfungen sollen die Gesamtintegrität und Leistung des ACC sicherstellen und potenzielle Probleme proaktiv identifizieren, bevor sie sich auf den Systembetrieb auswirken.

Die Scan-Suite der ACC-Integritätsinstanz besteht aus den folgenden Prüfungen.

Prüfungen der ACC-Integritätsinstanz-Scan-Suite

Name überprüfen	Beschreibung
ACC-doppelter Agent für Host-CI	Identifiziert Konfigurationselemente (Configuration Items, CIs), die mehreren aktiven Agents zugeordnet sind, und weist auf potenzielle Probleme bei der CI-Identifizierung hin. Erfordert den Import von Global.ACCInstanceScanUtil Für Instanzen, die mit verknüpft sind Xanadu Release oder früher.
ACC-Fehler-Framework	Überprüft, ob der ACCErrorManager erstellt wurde, wodurch Fehler der relevanten bereichsbezogenen ACC-App zugeordnet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfungen der ACC-Integritätsinstanz-Scan-Suite (Fortsetzung)

Name überprüfen	Beschreibung
	Erkennt, ob eine Automatisierungsquellenanwendung, eine Automatisierungsfehlerkategorie und ein Automatisierungsfehlercode für vorhanden sind Agent Client Collector Framework Anwendung.
ACC – geänderte Skripteinbindungen finden	Erkennt geänderte Elemente Agent Client Collector Framework Skripteinbindungen, die nach dem Upgrade möglicherweise geändert wurden. Erfordert den Import von Global.ACCInstanceScanUtil Für Instanzen, die mit verknüpft sind Xanadu Release oder früher.
ACC hat Upgrades übersprungen	Meldet Upgrades, die seit dem letzten Upgrade übersprungen wurden. Erfordert den Import von Global.ACCInstanceScanUtil Für Instanzen, die mit verknüpft sind Xanadu Release oder früher.
ACC – Plugin-Ordnerhierarchie verifizieren	Validiert die korrekte Erstellung von ACC-Plugin-Ordnern und kennzeichnet doppelte Ordner, die zu Synchronisierungsproblemen führen können.
Anzahl aktiver ACC-Richtlinien	Zählt die Anzahl der aktiven veröffentlichten Richtlinien. Wenn die Anzahl über 300 liegt, empfiehlt die Richtlinienkonsolidierung, um die Leistung zu verbessern.
ACC-Agent zu MID-Verbindung	Überprüft die Verbindung von 1000 Agents pro 1 GB Java Virtual Machine (JVM), um sicherzustellen, dass MID-Server Ist nicht überlastet. Konfigurieren Sie bei Überlastung zusätzliche JVMs, oder verteilen Sie Agents an andere MID Servers.
ACC verifiziert, ob die CI-Anzahlen von sn_Agent übereinstimmen	Stellt sicher, dass die Datensätze in den Tabellen „sn_Agent_ci_extended_info“ und „sn_Agent_cmdb_ci_Agent“ übereinstimmen, wodurch die Datenkonsistenz für Service Desk-Mitarbeiter bestätigt wird.

Für Details zum Importieren von Global.ACCInstanceScanUtil Skripteinbindung, siehe Skripteinbindung ACCInstanceScanUtil [KB1630132] artikel in Now Support Knowledge Base.

Weitere Informationen zu Instanzscans finden Sie unter Instance Scan .

Für Details zur Ausführung von Agent Client Collector Scan-Suite für Integritätsinstanz, siehe Führen Sie einen Suite-Scan aus .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domain Separation und Agent Client Collector

Domänentrennung wird für unterstützt Agent Client Collector(ACC). Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

So funktioniert Domain Separation in Agent Client Collector

Domänentrennung in ACC ermöglicht die Isolierung von Daten, die von erfasst werden Agent Client Collector An eine bestimmte Domäne. Daher können nur Anwender innerhalb dieser Domäne auf diese Daten zugreifen und sie anzeigen. Ebenso sind Service Desk-Mitarbeiter und ihre zugehörigen Konfigurationen an bestimmte Domänen gebunden, um sicherzustellen, dass Vorgänge innerhalb einer Domäne sich nicht auf andere auswirken oder in andere eindringen. Dadurch wird eine besser organisierte und sicherere Umgebung für die Verwaltung mehrerer Gruppen, Geschäftsbereiche oder Regionen geschaffen.

- Datensicherheit und Datenschutz: Durch die Einschränkung des Datenzugriffs basierend auf Domänen wird das Risiko von nicht autorisiertem Zugriff und domänenübergreifendem Datenverlust reduziert, wodurch sichergestellt wird, dass vertrauliche Informationen innerhalb der festgelegten Domäne bleiben.
- Zugriffssteuerung: Durch die Isolierung von Domänen können Organisationen strenge Zugriffskontrollen durchsetzen, sodass nur bestimmte Anwender oder Teams die für ihre Domäne relevanten Daten anzeigen oder mit ihnen interagieren können.

Anwendungsfälle für Domänentrennung in Agent Client Collector

- Zusammenarbeit mehrerer Abteilungen mit Datenisolierung: IT- und Finanzabteilungen können ihre jeweiligen Systeme unabhängig überwachen, ohne dass sich Daten überschneiden. Wenn beispielsweise ein Problem mit einem Server im Zahlungsverarbeitungssystem auftritt, kann die Finanzabteilung bestimmte Prüfungen in ihrer Domäne ohne Interferenzen ausführen.
- Regulatorische Compliance: Domänentrennung hilft bei der Einhaltung von Vorschriften wie DSGVO oder SOX, indem sichergestellt wird, dass nur autorisierte Mitarbeiter auf vertrauliche Daten zugreifen können. Beispielsweise kann die Compliance-Abteilung regulatorische Prüfungen überwachen, während der Zugriff auf IT-Infrastrukturdaten eingeschränkt wird.
- Incident-Management und -Fehlerbehebung: ES kann Netzwerkprobleme beheben, während das Finanzministerium Transaktionssysteme überwacht. Die Domänentrennung ermöglicht es beiden Abteilungen, unabhängig zu arbeiten, wodurch eine schnellere Lösung sichergestellt und das Datenrisiko verhindert wird.

Zugehörige Informationen

Domänentrennung für Service Provider

Anwendungsfall: Optimierung der Datenisolierung und -Überwachung mit Domänentrennung

Durch die Optimierung der Datenisolierung und -Überwachung mit Domänentrennung wird sichergestellt, dass Finanzinstitute vertrauliche Informationen schützen, die betriebliche Effizienz verbessern und Compliance gewährleisten, indem Abteilungsdaten sicher getrennt werden.

Anwendungsfallübersicht

In einem großen Finanzinstitut müssen Abteilungen wie IT, Finanzen, Compliance und HR ihre Systeme unabhängig verwalten und vertrauliche Daten schützen. Die Agent Client

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Collector(ACC) sammelt Daten von verschiedenen Service Desk-Mitarbeitern auf Servern und Geräten, und die Domänentrennung stellt sicher, dass die Daten jeder Abteilung sicher isoliert sind. Dies ermöglicht es Abteilungen, ihre eigene Überwachung, Fehlerbehebung und Berichterstellung zu verwalten, wodurch das Risiko domänenübergreifender Interferenzen oder nicht autorisierter Zugriffe erheblich reduziert wird.

Herausforderungen ohne Domänentrennung

- Datenschutz- und Sicherheitsrisiken: Vertrauliche Daten können nicht autorisierten Anwendern zugänglich gemacht werden. Beispielsweise könnten IT-Mitarbeiter versehentlich auf Finanz- oder Gehaltsabrechnungsdaten zugreifen, was gegen Datenschutzrichtlinien verstößt.
- Betriebliche Ineffizienz: Abteilungen müssten Konfigurationen freigeben, was die Verwaltung und Behebung von Problemen erschwert, was zu Verwirrung und Ineffizienzen führt.
- Compliance-Probleme: Die Erfüllung regulatorischer Anforderungen für die Datenisolierung wäre schwierig, da das Risiko von Compliance-Verstößen besteht.
- Erhöhtes Risiko der Datenbeschädigung: Gemeinsam genutzte Umgebungen können zu versehentlicher Datenbeschädigung führen, da sich Änderungen in einer Abteilung auf andere auswirken können.

Lösung

- Datenisolierung: Jede Abteilung verfügt über eine dedizierte Domäne, die sicherstellt, dass Daten, die von Service Desk-Mitarbeitern erfasst werden, nur innerhalb dieser Domäne zugänglich sind.
- Unabhängige Konfiguration und Überwachung: Abteilungen legen ihre eigenen Prüfungen, Richtlinien und Aufgaben fest, ohne andere zu beeinträchtigen.
- Zugriffssteuerung: Die rollenbasierte Zugriffssteuerung (RBAC) schränkt den Anwenderzugriff auf Daten innerhalb ihrer Domäne ein. Beispielsweise kann SIE nur auf Infrastrukturdaten zugreifen, während die Finanzabteilung nur auf Finanztransaktionsdaten zugreifen kann.
- Verbesserte Sicherheit: Domänentrennung stellt sicher, dass Anwender in einer Abteilung nicht auf Daten aus anderen Abteilungen zugreifen können, wodurch das Risiko eines nicht autorisierten Zugriffs reduziert wird.

Ergebnis

- Verbesserte Datensicherheit: Vertrauliche Daten werden geschützt, wodurch das Risiko nicht autorisierter Zugriffe reduziert wird.
- Betriebseffizienz: Abteilungen arbeiten unabhängig und verwalten Konfigurationen und Überwachung ohne Konflikte.
- Regulatorische Compliance: Einfachere Einhaltung von Datenschutzbestimmungen (DSGVO, SOX) durch sichere Datentrennung.
- Reduzierte Datenbeschädigung: Isolierte Umgebungen verhindern unbeabsichtigte abteilungsübergreifende Auswirkungen und verbessern die Systemstabilität.

Anwendungsfall: Regulatorische Compliance in einer Finanzdienstleistungslösung

Ein Finanzinstitut muss sicherstellen, dass seine Daten nur für die Abteilungen zugänglich sind, die über eine Autorisierung für die angegebenen Daten verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Herausforderung

Das Finanzinstitut muss Vorschriften einhalten, die eine strikte Datentrennung zwischen Abteilungen (z. B. HR, IT oder Finanzen) erfordern.

Lösung

1. Erstellen Sie separate Domänen für jede Abteilung (IT, Finanzen, HR, Compliance usw.) in Agent Client Collector(ACC)-Konfiguration.
2. Wenden Sie Zugriffssteuerungen an, damit vertrauliche Daten (z. B. Mitarbeiterdatensätze und Finanztransaktionen) nur für autorisierte Abteilungen zugänglich sind.
3. Verwenden Sie ACC-Integritätsinstanzscans, um sicherzustellen, dass die Datentrennung beibehalten wird, insbesondere bei der Aktualisierung oder Fehlerbehebung von Systemen.
4. Überprüfen Sie die Einstellungen für die Domänentrennung regelmäßig, um die Compliance mit Datenschutzbestimmungen wie DSGVO, SOX oder PCI-DSS sicherzustellen.

Ergebnis

Die Einhaltung rechtlicher und regulatorischer Anforderungen wird sichergestellt, und vertrauliche Daten werden vor nicht autorisiertem Zugriff geschützt.

Agent Client Collector Framework konfigurieren

Planen und konfigurieren Sie Ihre Agent Client Collector Framework-Implementierung.

Agent Client Collector Framework Die Konfiguration folgt normalerweise den folgenden Schritten:

1. Konfigurieren Sie einen Agent-Registrierungsschlüssel.
2. Websocket-Server auf MID-Server installieren.
3. Websocket-Endpunkt konfigurieren.
4. Häufigkeit der Aktualisierung der Liste der MID-Server für Agents konfigurieren.
5. Erstellen und bearbeiten Agent Client Collector Plugins.
6. Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden.
7. Installieren Sie Agent Client Collector .

   Das zu befolgende Installationsverfahren hängt vom Betriebssystem ab, auf dem Sie die Installation durchführen (Linux, Windows, Oder macOS).

   Hinweis: Agent Client Collector unterstützt nicht mehrere Service Desk-Mitarbeiter, die auf einem einzelnen Hostgerät installiert sind. Für jeden Host darf nur ein ACC-Agent konfiguriert sein, der mit einem einzelnen ServiceNow kommuniziert. Instanz.

8. Agent Client Collector Monitoring auf dem MID-Server aktivieren.
9. Optimieren Sie die Verteilung von Service Desk-Mitarbeitern an MID Servers.
10. Agent Client Collector-Konfigurationsdateien für Agents anzeigen.
11. Erstellen Sie einen Agent Client Collector Konfigurationsdatendatei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Manuell aktualisieren Agent Client Collector Zertifikate.
13. Aktivieren Sie die sichere OpenSSL-Signatur für Plugins.
14. Durchführen Zscaler Korrektur.

Wird Konfiguriert Agent Client Collector Mit MID-Server

Konfigurieren Sie Agent Client Collector Mit MID-Server Zum Aktivieren der Kommunikation zwischen Netzwerkservern und ServiceNow Instanz.

Konfigurieren Sie einen Agent Client Collector Mit MID-Server Mit einem einzeiligen Befehl

Verwenden Sie einen einzeiligen Befehl, um einen einzurichten Agent Client Collector Mit MID-Server. Sie können auch den einzeiligen Befehl verwenden, um Agents mit einer Konfiguration ohne MID ZU migrieren, die mit verwendet werden soll MID-Server.

Vorbereitungen

Erforderliche Rolle:

- In einem Linux Oder macOS Umgebung: Stamm
- In einem Windows Umgebung: Agent_Client_Collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Ausführung des einzeiligen Befehls enthält Kennzeichnungen, die die Optionen angeben, die dem hinzugefügt werden sollen acc.yml Konfigurationsdatei. Diese Optionen bestimmen die Konfiguration von Agent Client Collector Mit MID-Server. Wenn Sie keine Option im Befehl angeben, ist die vorhandene Option im acc.yml Datei wird verwendet. Wenn keine Option vorhanden ist, gibt eine Fehlermeldung an, dass der Parameter erforderlich ist, um die Verbindung zu einem Endpunkt zu ermöglichen.

Durch die Ausführung eines Befehls wird validiert, ob eine Verbindung mit dem angegebenen Parameter hergestellt werden kann (z. B. dem angegebenen api-Schlüsselwert). Der Befehl überprüft jedoch nicht, ob der Wert des Parameters gültig ist.

Prozedur

1. Führen Sie den folgenden Befehl in einem Terminalfenster aus: `acc-Gateway-MID-<flags>` .
   Die verfügbaren Kennzeichnungen werden in der folgenden Tabelle angezeigt:

MID-Server-Konfigurationskennzeichnungen

Kennzeichnung	Typ	Beschreibung
-Y, <--acc-yml>	Zeichenfolge	Standort von acc.yml Wird konfiguriert. Kann auch verwendet werden, um Parameter zu ändern und zu validieren, wenn sich die Datei an einem anderen Speicherort als dem Standard befindet. Optional. Wenn kein Wert eingegeben wird, der Standardspeicherort des acc.yml Datei wird verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kennzeichnung	Typ	Beschreibung
-A, <--api-key>	Zeichenfolge	Der API-Schlüssel, der von verwendet werden soll MID-Server.
-B, <--Back-End-url>	Zeichenfolge	Mindestens eine Back-End-Verbindungs-URLs, die einen websocket-Endpunkt für einen angeben MID-Server. Mehrere Werte werden durch Kommas zwischen Einträgen ohne Leerzeichen angegeben, die die Werte trennen. Beispiel: `<url1>,<url2>` .
-H, Hilfe	N/V	Erklärt, was der angegebene Befehl bewirkt.

2. Starten Sie den Service Desk-Mitarbeiter neu, damit die Konfigurationseinstellungen in eingegeben werden `acc.yml` Datei.

Websocket-Server auf MID-Server installieren

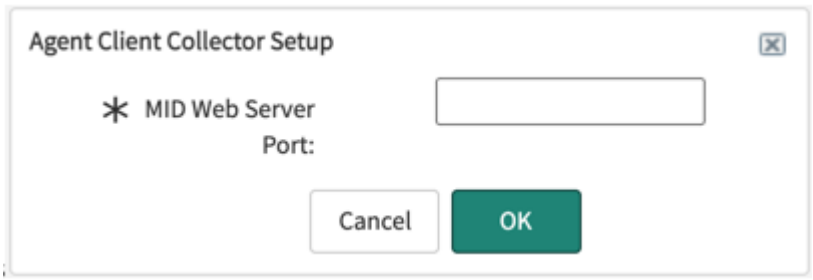
Konfigurieren Sie den websocket-Server auf MID Servers Dient zum Aktivieren von Verbindungen von Service Desk-Mitarbeitern zur MID-Server. Sie können pro nur einen websocket-Server konfigurieren MID-Server.

Vorbereitungen

- Stellen Sie sicher, dass Sie Curl (oder ähnliche Software) auf Ihrem herunterladen und installieren MID-Server Windows-Computer.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**an.
2. Wählen Sie den Namen des relevanten MID-Server aus.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Setup ACC Listener** (ACC-Listener einrichten). Das Dialogfeld **Agent Client Collector Setup (Setup von Agent Client Collector)** wird angezeigt.



4. Geben Sie den MID-Webserver-Port ein (**8800**) Im angezeigten Feld.

Hinweis: Sie können den Standardport ändern, **8800** , Nach Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die sichere TLS-Konfiguration aufzurufen, führen Sie folgenden Befehl aus: `wss://<mid_ip>:<websocket_port>/ws/events`.
- Dient zum Aufrufen der TLS 1,3-Unterstützung für MID-Webserver, Legen Sie den folgenden Parameter in fest `Wrapper-override.conf` Datei in MID-Server: `-Djdk.tls.server.protocols="TLSv1.3"`
- In einem Linux Umgebung, Portnummern unter 1024 können nur mit Superuser-Berechtigungen verwendet werden.

5. Klicken Sie auf **OK**.
   Eine Bestätigungsmeldung mit der URL für die Agent-Konfigurationsdatei wird angezeigt.

   Der Webserver und die websocket-Erweiterung sind für konfiguriert MID-Server. Um die Konfiguration zu überprüfen, navigieren Sie zu den folgenden Menüoptionen:

   - **Agent Client Collector** > **MID-Webserver**an. Wenn Sie die Felder im resultierenden Formular bearbeiten, müssen Sie die MID-Webservererweiterung neu starten, damit Ihre Änderungen gespeichert werden.
   - **Agent Client Collector** > **Websocket-Endpunkt**

6. Überprüfen Sie die Gültigkeit des Websocket mit curl:

   a. Geben Sie in ein cmd- oder Terminal-Fenster folgenden Befehl ein: *`curl -Lk -H "Authorization: Key <API_KEY>" https://<mid_server_address>:<port>/api/mid/mon`*.

   b. Stellen Sie sicher, dass Sie eine gültige JSON-Antwort (und keine Fehlermeldung) erhalten, z. B.:

JSON-Skript bei erfolgreicher Installation


```
{
  "uptime" : "53d 23h 50m 3s",
  "memory" : "used 127MB, total 503MB",
  "connectedAgentsNum" : 1,
  "interactiveResultQueueSize" : "0",
  "nonInteractiveResultQueueSize" : "0",
  "policiesNum" : 3,
  "allChecksNum" : 3,
  "eventsRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)",
  "metricRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)",
  "connectedAgents" : [ {
    "client" : {
      "name" : "10-196-39-193-new",
      "address" : "[redacted]",
      "agent_id" : "d56aa0470b49bfd6",
      "version" : "2.1.9",
      "timestamp" : 1602838990267,
      "isWindows" : false,
      "silent_mode" : false,
      "checkTimeout" : 120
    },
    "metricsRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)"
  } ]
```


Websocket-Endpunkt konfigurieren

Konfigurieren Sie ein websocket, damit der Endpunkt Webzugriff über bereitstellen kann MID-Server Zu Agent Client Collector(ACC).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie für zusätzliche Sicherheit sicher MID Servers Für bereitgestellt Agent Client Collector Werden nicht für andere Komponenten bereitgestellt.

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**an.
2. Wählen Sie einen MID-Server.
3. Wählen Sie aus **ACC-WebSocket-Endpunkte** Registerkarte unten auf der Seite.
4. Wählen Sie **Neu**.
5. Konfigurieren Sie die Felder auf der Seite.

ACC-WebSocket-Endpunktseite

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den websocket-Endpunkt ein.
MID-Server	Der Name des ausgewählten MID-Server.
Kurzbeschreibung	Geben Sie optional eine Kurzbeschreibung für den websocket-Endpunkt ein.
Zugängliche IP-Adresse	Wenden Sie eine externe/öffentliche IP an, wenn an MID-Server Hat eine interne IP, auf die von einem Service Desk-Mitarbeiter nicht zugegriffen werden kann. Wird für Cloud-Lösungen mit einem Service Desk-Mitarbeiter verwendet, der nur Zugriff auf hat MID-ServerÖffentliche IP von . Wenn MID-Server Und alle Service Desk-Mitarbeiter befinden sich in derselben Virtual Private Cloud (VPC). Dieses Feld kann leer gelassen werden.

6. In **Zugehörige Links** Abschnitt auswählen **Starten** Zum Aktivieren des websocket-Endpunkts.

Häufigkeit der Aktualisierung der Liste der MID-Server für Agents konfigurieren

Standardmäßig wird die Liste der mit Agents verbundenen MID Server einmal täglich aktualisiert. In einer dynamischen Umgebung, in der häufig MID Server hinzugefügt werden, empfiehlt es sich, häufigere Aktualisierungen zu planen oder den Aktualisierungsauftrag bei Bedarf auszuführen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur
1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.
2. Suchen Sie den Auftrag **Update MID Server list for All Agents** (MID Server-Liste für alle Agents aktualisieren).
3. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. So bearbeiten Sie die Häufigkeit, mit der der Auftrag ausgeführt wird:

   a. Wählen Sie im Feld **Execute** (Ausführen) die Option **Periodically** (Regelmäßig) aus.
   Das Feld **Repeat Interval** (Wiederholungsintervall) wird angezeigt.

Feld „Repeat interval" (Wiederholungsintervall)

   b. Konfigurieren Sie die Häufigkeit, mit der der Auftrag ausgeführt werden soll.
   Die Zellen neben der Zelle **Hours** (Stunden) stellen Minuten bzw. Sekunden dar.

   c. Klicken Sie auf **Aktualisieren**, um die Auftragshäufigkeit zu aktualisieren.

Agent Client Collector Monitoring auf dem MID-Server aktivieren

Aktivieren Sie Agent Client Collector Monitoring auf dem MID-Server, indem Sie in einem einzigen Vorgang das Agent Client Collector-Framework (ACC-F) und die Metrikdaten-Erweiterungen konfigurieren. Durch Aktivieren der Agent Client Collector-Überwachung wird auch die Überwachung von Agents ermöglicht, die mit dem MID-Server verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**an.
2. Wählen Sie auf der MID-Server-Seite einen MID-Server, um die Details des MID-Server s anzuzeigen.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Setup ACC Monitoring** (ACC-Monitoring einrichten) und geben Sie die entsprechende Portnummer in das Feld **Port des MID Web Server** des Dialogfelds ein.

Ergebnis
Der MID-Server ist so konfiguriert, dass er sowohl Agent Client Collector als auch Metrikdaten unterstützt.

Hinweis: Sie werden nur beim ersten Setup der ACC-Überwachung zur Eingabe einer Portnummer aufgefordert.

Automatische MID-Server-Auswahl

Automatische Auswahl von MID Servers Stellt sicher, dass jeder Service Desk-Mitarbeiter die effizienteste verfügbare verwendet MID-Server.

Agent Client Collector automatisch MID-Server Der Auswahlfunktionssatz ist standardmäßig deaktiviert. Es gibt mehrere Faktoren, die berücksichtigt werden müssen, bevor bestimmt wird, ob automatisch MID-Server Die Auswahl ist für Ihre Anwendungsfälle richtig.

Überlegungen zu Anwendungsfällen

Automatisch MID-Server Die Auswahl bietet mehrere Vorteile. MID-Server-Fähigkeiten Kann die Liste von einschränken MID Servers Ein Service Desk-Mitarbeiter kann potenziell eine Verbindung zu herstellen. Automatisch MID-Server Die Auswahl hält die Back-End-URL-Konfigurationsliste auf dem Agent-Host ohne zusätzliche Workflows auf dem neuesten Stand.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn automatisch MID-Server Die Auswahl ist aktiviert, führt der Service Desk-Mitarbeiter einen Konnektivitätstest für die Liste der verfügbaren durch MID Servers Und bestimmt die beste Verbindung basierend auf der Latenz und der Anzahl der derzeit verbundenen Service Desk-Mitarbeiter.

Es gibt jedoch mehrere zusätzliche Überlegungen, die automatisch werden können MID-Server Auswahl für Ihren Anwendungsfall falsch.

ACC automatisch MID-Server Die Auswahl ist kein echter Lastenausgleichsmodul und sollte als Failover-Mechanismus betrachtet werden. Die Auswahl einer Back-End-URL ist komplexer, da sie aus mehreren Eingabequellen abgeleitet wird. Wenn stattdessen ein Anwendungslastausgleichsmodul verwendet wird, muss nur eine Back-End-URL angegeben werden. Weitere Informationen finden Sie unter Lastenausgleichsmodul von Agent Client Collector aktivieren.

Standardmäßig erhält jeder Service Desk-Mitarbeiter die Liste aller Mitarbeiter MID Servers Auf ACC-Verbindungen hören. Da diese Liste enthält MID Servers In eingeschränkten Bereichen können Service Desk-Mitarbeiter versuchen, eine Verbindung zu ihnen herzustellen, wodurch Sicherheitswarnungen generiert werden können.

Ihre DNS-Konfiguration sollte berücksichtigt werden, bevor Sie automatisch verwenden MID-Server Auswahl, da die Lösung zu unerwarteten Ergebnissen führen kann. Die DNS-Auflösung wird regelmäßig durchgeführt. Endanwender-Compute-Systeme, die zwischen internen Unternehmens-, WLAN-, VPN- oder externen Netzwerken wechseln, können möglicherweise nicht erneut eine Verbindung herstellen, wenn sich der Netzwerkkontext geändert hat.

Automatischer Auswahlprozess

Wenn die automatische Auswahl aktiviert ist, sendet die ServiceNow-Instanz periodisch MID-Server-Aktualisierungen an bestehende Agents. Der Agent wählt einen MID-Server basierend auf Informationen aus, die er von der ServiceNow-Instanz erhält.

Während der automatischen Ausführung MID-Server Bei Auswahl wählt der Service Desk-Mitarbeiter eine primäre MID- und eine sekundäre MID-Liste aus und schreibt sie in die Konfigurationsdatei des Service Desk-Mitarbeiters. Der Service Desk-Mitarbeiter verwendet diese Liste als Failover-Schutz, wenn der primäre MID/sekundäre MID in der Liste die Verbindung verliert.

Wenn ein Service Desk-Mitarbeiter erkennt, dass sich seine IP-Adresse geändert hat, stellt er automatisch eine Verbindung mit dem effizientesten her MID-Server Verfügbar in der Liste des Service Desk-Mitarbeiters von MID Servers.

Um die Kommunikation zwischen MID-Server und Agent zu sichern, verwenden Sie den einheitlichen Schlüsselspeicher des MID-Server s. Für Details zur Verwendung von MID-Server Einheitlicher Schlüsselspeicher, siehe MID-Server Einheitlicher Schlüsselspeicher an.

Zugehörige Informationen

Automatische Auswahl der MID-Server aktivieren

Automatische Auswahl der MID-Server aktivieren

Aktivieren von „automatisch“ MID-Server Mit der Auswahl kann der Service Desk-Mitarbeiter einen Konnektivitätstest für die Liste der verfügbaren durchführen MID Servers Und bestimmen Sie die beste Verbindung basierend auf der Latenz und der Anzahl der derzeit verbundenen Service Desk-Mitarbeiter. Automatisch MID-Server Die Auswahl ist standardmäßig deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

- Zum Aktivieren des regelmäßigen Sendens MID-Server Updates von ServiceNow Instanz für vorhandene Service Desk-Mitarbeiter festlegen *sn_agent.enable_auto_mid_selection*Systemeigenschaft zu **Wahr** .
- Zum Aktivieren der automatischen Funktion MID-Server Auswahl für einzelne Service Desk-Mitarbeiter:
  1. Legen Sie fest *enable-auto-mid-selection*Eigenschaft in der des Service Desk-Mitarbeiters acc.yml Datei in **Wahr** .
  2. Aktivieren und führen Sie die geplanten Aufgaben „MID-Liste für alle Service Desk-Mitarbeiter aktualisieren“ und „MID-Liste für alle neuen Service Desk-Mitarbeiter aktualisieren“ aus.

Nächste Maßnahme
Zum Deaktivieren der automatischen Funktion MID-Server Bei erneuter Auswahl legen Sie jede der Eigenschaften wieder auf fest **Falsch** .

Konfigurieren Sie Agent Client Collector Fähigkeiten für MID Servers

Konfigurieren Sie MID Servers Mit Agent Client Collector Fähigkeiten zum Aktivieren von MID Servers Für die Arbeit mit Service Desk-Mitarbeitern. Service Desk-Mitarbeiter mit identischen Elementen MID-Server Fähigkeiten sind für automatische Funktionen berechtigt MID-Server Auswahl.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Eine Fähigkeit definiert MID-Server Funktionen. Beliebig MID-Server Die mit einer Fähigkeit zugewiesen ist, die hat **Ist ACC Capability=true** Ist aktiviert, um mit einem Service Desk-Mitarbeiter zu arbeiten. Für Details zu MID-Server Fähigkeiten, siehe MID-Server-Fähigkeiten .

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Fähigkeiten**an.
2. Wählen Sie eine Fähigkeit aus, um zu aktivieren MID-Server Für die Zusammenarbeit mit dem Service Desk-Mitarbeiter.
   a. Wählen Sie die Spalte ACC-Fähigkeit neben dem Eintrag AgentClientCollector aus.
   b. Legen Sie den Wert auf fest **Wahr** .
3. Aktivieren Sie andere Fähigkeiten für Agent Client Collector MID Servers Indem Sie die Spalte ist ACC-Fähigkeit neben dem Eintrag AgentClientCollector auswählen und den Wert auf festlegen **Wahr** .

Ergebnis
MID Servers Mit den gleichen Fähigkeiten können während der automatischen Verwendung verwendet werden MID-Server Auswahl.

Konfigurieren Sie die automatische MID-Server Auswahl basierend auf Agent Client Collector Fähigkeiten

Konfigurieren Sie MID Servers Die nicht für die automatische Verwendung berechtigt sind MID-Server Auswahl mit dem Service Desk-Mitarbeiter. Beispielsweise möchten Sie einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

blockieren MID-Server Von der Verbindung mit Ihrem Service Desk-Mitarbeiter aufgrund von Firewall-Einschränkungen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Service Desk-Mitarbeiter mit verschiedenen Ebenen von Agent Client Collector(ACC)-Fähigkeit kann für automatisch nicht berücksichtigt werden MID-Server Auswahl. Wenn Sie einen blockieren möchten MID-Server Von automatisch MID-Server Auswahl können Sie zuweisen MID-Server Verschiedene ACC-Fähigkeiten von allen MID Servers, Aber nicht das primäre MID-Server, In Ihrer Umgebung.

Prozedur

1. Konfigurieren Sie Agent Client Collector Fähigkeiten für MID Servers, Wie in beschrieben Konfigurieren Sie Agent Client Collector Fähigkeiten für MID Servers.
2. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**an.
3. Wählen Sie aus MID-Server Dass Sie nicht für die automatische Verwendung berechtigt sein möchten MID-Server Auswahl.
4. Wählen Sie das Symbol „zusätzliche Aktionen“ aus Und wählen Sie aus **Ansicht** > **Standardansicht**an.
5. Wählen Sie aus **Fähigkeiten** Registerkarte.
6. Stellen Sie sicher, dass MID-Server Ist nicht den Fähigkeiten zugewiesen, die haben **Ist ACC Capability=true** Auf der **Fähigkeiten** Registerkarte.

Example: Wird Konfiguriert MID Servers Um nicht für die automatische Verwendung berechtigt zu sein MID-Server Auswahl

1. Weisen Sie zu **AgentClientCollector** Fähigkeit zu MID-Server A und MID-Server C, aber nicht an MID-Server B.
2. Auf der Seite „MID-Server-Fähigkeiten“:
   a. Weisen Sie eine Fähigkeit zu zu zu MID-Server A und MID-Server C.
   b. Weisen Sie eine andere Fähigkeit zu zu zu zu MID-Server B.
3. Installieren Agent Client Collector Framework Und geben Sie an MID-Server A als MID-Server Während der Installation.

   Nach der Installation hat der Service Desk-Mitarbeiter **Status=Aktiv** Und ist MID-Server Ist MID-Server A.
4. Führen Sie aus MID-Server Wählen Sie die geplante Aufgabe aus, um zu bestimmen, welche MID Servers Sind für automatische Anwendungen berechtigt MID-Server Auswahl.

   MID-Server B ist für die automatische Auswahl nicht berechtigt, da es nicht über dieselbe ACC-Fähigkeit verfügt wie MID-Server A. MID-Server C ist berechtigt, da es dieselbe ACC-Fähigkeit wie hat MID-Server A.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration ohne MID Agent Client Collector

Konfigurieren Sie MID-less Agent Client Collector Zum Aktivieren des Sendens von Informationen über die Cloud. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Konfigurieren Sie MID-less Agent Client Collector Mit einem einzeiligen Befehl

Verwenden Sie einen einzeiligen Befehl, um einen MID-less-Befehl einzurichten Agent Client Collector. Sie können auch den einzeiligen Befehl verwenden, um mit konfigurierte Agents zu migrieren MID-Server Um eine Konfiguration ohne MID ZU haben.

Vorbereitungen

Erforderliche Rolle:

- In einem Linux Oder macOS Umgebung: Stamm
- In einem Windows Umgebung: Agent_Client_Collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Ausführung des einzeiligen Befehls enthält Kennzeichnungen, die die Optionen angeben, die dem hinzugefügt werden sollen acc.yml Konfigurationsdatei. Diese Optionen bestimmen die Konfiguration von MID-less Agent Client Collector. Wenn Sie keine Option im Befehl angeben, ist die vorhandene Option im acc.yml Datei wird verwendet. Wenn keine Option vorhanden ist, gibt eine Fehlermeldung an, dass der Parameter erforderlich ist, um die Verbindung zu einem Endpunkt zu ermöglichen.

Durch die Ausführung eines Befehls wird validiert, ob eine Verbindung mit dem angegebenen Parameter hergestellt werden kann (z. B. dem angegebenen Registrierungsschlüsselwert). Der Befehl überprüft jedoch nicht, ob der Wert des Parameters gültig ist.

Prozedur

1. Führen Sie den folgenden Befehl in einem Terminalfenster aus: `acc-Gateway-ics-<flags>` .
   Die verfügbaren Kennzeichnungen werden in der folgenden Tabelle angezeigt:

Konfigurationskennzeichnungen ohne MID

Kennzeichnung	Typ	Beschreibung
-Y, <--acc-yml>	Zeichenfolge	Standort von acc.yml Wird konfiguriert. Kann auch verwendet werden, um Parameter zu ändern und zu validieren, wenn sich die Datei an einem anderen Speicherort als dem Standard befindet. Kann auch verwendet werden, um einen anderen Dateispeicherort zu ändern, um zu überprüfen, ob die angegebenen Parameter gültig sind. Optional. Wenn kein Wert eingegeben wird, der Standardspeicherort des acc.yml Datei wird verwendet.
-B, <--Back-End-url>	Zeichenfolge	Die gRPC-URL für ITOM Gateway für Cloud-Services (ICS).
-i, <--instance-url>	Zeichenfolge	Die Instanz-URL.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kennzeichnung	Typ	Beschreibung
-R, <registration-key>	Zeichenfolge	Der Registrierungsschlüssel für ITOM Gateway für Cloud-Services (ICS).
-H, Hilfe	N/V	Erklärt, was der angegebene Befehl bewirkt.

2. Starten Sie den Service Desk-Mitarbeiter neu, damit die Konfigurationseinstellungen in eingegeben werden acc.yml Datei.

Wird ohne MID installiert Agent Client Collector

Wird ohne MID installiert Agent Client Collector Ermöglicht Ihnen das Senden von Daten vom Service Desk-Mitarbeiter über die Cloud an die Instanz. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vor Verwendung von MID-less Agent Client Collector, Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Ihr ServiceNow Instanz wurde von einem F5-Lastenausgleichsmodul zu Application Delivery Controller, Version 2 (ADCv2) migriert und verfügt über mTLS-Unterstützung.
   a. Navigieren Sie zu <instance_url>/adcv2/Server
      - Wenn ein Servername angezeigt wird, befindet sich die Instanz in ADCv2.
      - Wenn die Seite nicht gefunden oder umgeleitet wird, befindet sich die Instanz nicht in ADCv2. Um von F5 zu ADCv2 zu migrieren, wenden Sie sich an den Kundensupport.
   b. Navigieren Sie zu <instance_url>/adcv2/Supports_tls

      Wenn die URL einen Wert von zurückgibt **Wahr** , MTLS wird unterstützt.
2. Installieren Sie ITOM Bereichsbezogenes App-Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).

   Stellen Sie sicher, dass Sie über einen verfügen ITOM-Operator Professional Abonnement, um die Installation von zu aktivieren ITOM Bereichsbezogenes App-Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).

   Wenn Sie verwenden Agent Client Collector Visibility – Inhalt, Installieren Sie Agent Client Collector Visibility – Inhalt Plugin (sn_ACC_VIS_content).
3. Konfigurieren Sie einen Agent-Registrierungsschlüssel in der Instanz. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.

Installieren Sie ohne MID Agent Client Collector Mit einem einzeiligen Befehl in einem Windows Umgebung

Installieren Sie ohne MID Agent Client Collector Auf einem Windows Computer, um das Senden von Daten vom Service Desk-Mitarbeiter an die Instanz über die Cloud zu ermöglichen. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vorbereitungen

- Installieren Sie ITOM Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).
- Onboarding für Ihre zu verwendende Instanz ITOM Cloud-Services. Weitere Informationen erhalten Sie vom Kundensupport.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Senden von Daten über die Cloud in einer Bereitstellung ohne MID finden Sie unter DEX-Architektur .

Prozedur

1. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab.
   - AMER (Amerika): itomcnc-prod-gateway.amer.sncapps.service-now.com:443
   - EMEA (Europa): itomcnc-prod-gateway.emea.sncapps.service-now.com:443
   - APAC (Asien-Pazifik): itomcnc-prod-gateway.apac.sncapps.service-now.com:443
2. Auf der Windows Server, auf dem der Agent installiert ist, geben Sie den folgenden Befehl ein:

```
msiexec /i <msi_file_path> /quiet /qn /norestart CONNECT_WITHOUT_MID="true"
 ACC_CNC="<gateway_endpoint>" REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>"
```

Die folgende Tabelle zeigt die Parameterwerte im Befehl.

Befehlszeilenparameter für Installation

Parameter	Beschreibung
CONNECT_WITHOUT_MID	Geben Sie An **Wahr** Zum Aktivieren von MID-less Agent Client Collector Installation. Wenn Sie keinen Wert angeben, der reguläre MID-Server websocket-Installation wird aufgerufen.
ACC_CNC	Geben Sie einen öffentlichen Gateway-Endpunkt für an Agent Client Collector.
REGISTRIERUNGSSCHLÜSSEL	Aktiver und gültiger Registrierungsschlüssel, mit dem der Service Desk-Mitarbeiter kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der der Service Desk-Mitarbeiter registriert ist.
ACC_ALLOW_LIST	Optionale Zeichenfolge. Um die Allow-Liste zu deaktivieren, legen Sie fest *`ACC_ALLOW_LIST=0`*. Die Allow-Liste ist standardmäßig aktiviert. **Hinweis:** Das Deaktivieren der Allow-Liste gefährdet die Sicherheit Ihres Systems und ist als temporäre Maßnahme während der Aktualisierung der Allow-Liste gedacht. Aktivieren Sie nach Abschluss des Updates die Einstellung Allow List by (Liste zulassen nach) **ACC_ALLOW_LIST=1** .
ACC_VALIDATE_SIG	Optionale Zeichenfolge. Um die Verifizierung der Zertifizierungsvalidierung des Installationsprogramms zu deaktivieren, legen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
	Sie fest *ACC_VALIDATE_SIG=0*Die Sie hinzufügen können, um die Verifizierung der Zertifizierungsvalidierung des Installationsprogramms zu deaktivieren. Die Validierung ist standardmäßig aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Zugehörige Informationen

Agent Client Collector Parameter für Installationsbefehl ohne MID

Installieren Sie ohne MID Agent Client Collector Manuell in einem Linux Umgebung

Installieren Sie ohne MID Agent Client Collector Manuell auf einem Linux Computer, um das Senden von Daten vom Service Desk-Mitarbeiter an die Instanz über die Cloud zu ermöglichen. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vorbereitungen

- Installieren Sie ITOM Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).
- Onboarding für Ihre zu verwendende Instanz ITOM Cloud-Services. Weitere Informationen erhalten Sie vom Kundensupport.
- Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Senden von Daten über die Cloud in einer Bereitstellung ohne MID finden Sie unter DEX-Architektur .

Prozedur

1. Laden Sie das entsprechende Installationspaket herunter.
   a. Navigieren zu > **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads**an.
   b. Laden Sie die entsprechende RPM- oder deb-Installationsdatei herunter.
   c. Laden Sie die relevanten Signaturdateien herunter Dient zum Validieren der Installationsdateien.
2. **Wahlweise:** Überprüfen Sie die Paketsignatur.
   a. Extrahieren Sie die Installationsdatei (falls komprimiert), indem Sie den folgenden Befehl ausführen:
   `unzip agent_client-collector-<version_number>-x86_64-rpm-rpm.zip`
   b. Validieren Sie die Signatur der Installationsdatei, indem Sie die angegebenen Befehle ausführen.
      - In einem RPM-basierten System:

```
openssl dgst -sha256 -verify {<ServiceNow DGST pem key>} -signature {<signature
file>} agent-client-collector-<version number>-x86_64.rpm
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wo <ServiceNow DGST Pem Key> Ist .PEM Datei aus extrahiert .Zip Datei, und <signature file> Ist .Bin Datei aus extrahiert .Zip Datei.

Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-x86_64.rpm
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
$ unzip agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
Archive: agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
inflating: ServiceNow_Digicert_DGST.pem
extracting: agent-client-collector-3.0.0-x86_64.bin
$ openssl dgst -sha256 -verify ServiceNow_Digicert_DGST.pem -signature
 agent-client-collector-3.0.0-x86_64.bin agent-client-collector-3.0.0-x86_64.rpm
Verified OK
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile angezeigt werden.

- Auf einem Debian-basierten System:

  (Optional) gpg –-Import ServiceNow_DigiCert_public.gpg

  Sudo gpg –-verify Agent-Client-Collector-<version number>-<distro>_amd64.deb

  Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-debian-9_amd64.deb
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
$ unzip agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
Archive: agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
extracting: ServiceNow_Digicert_Public.gpg
$ gpg --import ServiceNow_Digicert_Public.gpg
gpg: /home/admin/.gnupg/trustdb.gpg: trustdb created
gpg: key 985DD52C6A0ABB45: public key "ServiceNow, Inc. (Signing)
 <seceng@servicenow.com>"
imported
gpg: Total number processed: 1
gpg: imported: 1
$ dpkg-sig --verify agent-client-collector-3.0.0-debian-9_amd64.deb
Processing agent-client-collector-3.0.0-debian-9_amd64.deb...
GOODSIG _gpgbuilder 9B928FB49771DF6C047430DD985DD52C6A0ABB45 1665054068
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile angezeigt werden.

3. Installieren Sie Agent Client Collector Paket, das den Paketmanager verwendet, der zugeordnet ist Linux Verteilung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BS	Befehl
RHEL-basiert	Yum/dnf localinstall
SLES	Zypper-Installation
Debian-basiert	APT-Get-Installation

Alternativ können Sie, wenn diese Befehle nicht richtig konfiguriert sind, die Core-Befehle verwenden, die für die Ausführung mit den Paketmanager-Befehlen konfiguriert sind.

- RPM-basiertes System: `# Rpm -VI Agent-Client-Collector-<version number>-x86_64.rpm`
- Debian-basiertes System: `# Dpkg -i Agent-Client-Collector-<version number>-<distro>_amd64.deb`

Vergewissern Sie sich, dass die Paketbefehle mit Ihrem Systemadministrator korrekt konfiguriert sind.

Hinweis: Für einige Dateisysteme sind möglicherweise Einschränkungen aktiviert, z. B. /Var/ Kann mit bereitgestellt werden *noexec*Kennzeichnung. Da der Agent ausführen muss Agent Client Collector Plugins, die normalerweise in gespeichert werden /Var/Cache Verzeichnis müssen Sie die Anwendung in bestimmten Ordnern bereitstellen, indem Sie die Installationspfade mit anpassen `--relocate`Option als .U/min Parameter.

Beispiel: `RPM -i --relocate /var/Cache=/opt/Cache Agent-Client-Collector-<version_number>-x86_64.rpm`

Die folgenden Pfade können verschoben werden:

Pfad	Notizen
/Etc	Beim Aktualisieren müssen Sie auch aktualisieren `allow-list`Parameter in acc.yml Datei mit dem neuen Pfad.
/usr/share	N/V
/var/cache	Wird aktualisiert /Var Das Verzeichnis behält alle bei /Var Unterverzeichnisse, geschachtelt unter dem neuen Verzeichnis.
/var/log	
/var/run	
/var	

Überprüfen Sie die Pfade in /Usr/lib/systemd/System/acc.service Um sicherzustellen, dass sie wie erwartet angezeigt werden.

4. Führen Sie den entsprechenden Paket-Upgrade-Befehl basierend auf der cpu aus, mit der Ihr Computer ausgeführt wird:
   - Intel-cpu:

     ```
     sudo installer -pkg agent-client-collector-<version number>-macos_x64.pkg -target /
     ```

   - Apple Silikon-cpu:

     ```
     sudo installer -pkg agent-client-collector-<version number>-macos_arm64.pkg -target /
     ```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Befehl sichert auch die Agent-ID und die Konfigurationsdateien vor dem Upgrade und stellt sie wieder her.

5. In acc.yml Konfigurationsdatei:

   a. Legen Sie die folgenden Parameter fest:

Parameter	Wert
Back-End-url	„<gateway URL>“
Connect-ohne-MID	wahr
Instanz-url	„<instance URL>“
Registrierungsschlüssel	„<regsitration-key>“
Unsicher-überspringen-tls-verifizieren	falsch

   b. Kommentieren Sie aus *api-key*Parameter.

6. Speichern Sie die Konfigurationsdatei.
7. Konfigurieren Sie Sudoers.

   Die Konfiguration wird normalerweise von automatisiert Linux Sysadmin. Um die manuelle Konfiguration durchzuführen, wenn Sie die Richtigkeit vor der vollständigen Konfiguration sicherstellen möchten, führen Sie die folgenden Schritte aus.

```
# visudo -f /etc/sudoers.d/01_servicenow
User_Alias ACC_USERS = servicenow
Cmnd_Alias ACC_CMD = /usr/sbin/dmidecode -s
 baseboard-serial-number,/usr/sbin/dmidecode -s
 chassis-serial-number,/usr/sbin/dmidecode -s system-serial-number,/usr/sbin/dmidecode
 -s system-uuid,/usr/sbin/ss -tanp
ACC_USERS ALL = (root) NOPASSWD:ACC_CMD
Defaults:ACC_USERS !requiretty
```

8. Konfigurieren Sie den Agent so, dass er als Dienst ausgeführt wird.

   a. Schützen Sie den Ressourcenverbrauch, indem Sie die angegebenen Werte zu hinzufügen /Usr/lib/systemd/System/acc.service Datei.

   - CPUShares=128
   - CPUQuota = 10 %
   - Arbeitsspeicherlimit = 192M
   - BlockIOWeight = 10
   - LimitNICE=15

   Zum Beispiel:

```
# vi /usr/lib/systemd/system/acc.service
[Unit]
Description=Agent-Now acc
After=network-online.target
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
[Service]
Environment=AGENT_ROOT=/usr/share
Environment=AGENT_CACHE_ROOT=/var/cache
Environment=AGENT_CONFIG_ROOT=/etc
Environment=AGENT_LOG_ROOT=/var/log
Environment=AGENT_RUN_ROOT=/var/run
Environment=RUBYOPT=-Eutf-8
User=servicenow
Group=servicenow
ExecStart=/usr/share/servicenow/agent-client-collector/bin/acc-service start acc
KillMode=process
Restart=on-failure
RestartSec=1min
CPUShares=128
CPUQuota=10%
MemoryLimit=192M
BlockIOWeight=10
LimitNICE=+15
[Install]
WantedBy=network-online.target
```

b. Führen Sie den Befehl „Daemon neu laden“ aus, wenn Sie die Servicedatei nach dem Aktivieren des ACC-Service geändert haben.

```
# Systemctl Daemon-reload
```

c. Aktivieren und starten Sie den Service, indem Sie die folgenden Befehle ausführen.

```
# Systemctl aktivieren nach
```

```
# Systemctl Start gemäß
```

Installieren Sie ohne MID Agent Client Collector Mit einem einzeiligen Befehl in einem Linux Umgebung

Installieren Sie ohne MID Agent Client Collector Auf einem Linux Computer, um das Senden von Daten vom Service Desk-Mitarbeiter an die Instanz über die Cloud zu ermöglichen. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vorbereitungen

- Installieren Sie ITOM Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).
- Onboarding für Ihre zu verwendende Instanz ITOM Cloud-Services. Weitere Informationen erhalten Sie vom Kundensupport.
- Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Senden von Daten über die Cloud in einer Bereitstellung ohne MID finden Sie unter DEX-Architektur .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Registrierungsschlüssel**an.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Registrierungsschlüsselwert, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf problemlos abrufen können.
2. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab.
   - AMER (Amerika): itomcnc-prod-gateway.amer.sncapps.service-now.com:443
   - EMEA (Europa): itomcnc-prod-gateway.emea.sncapps.service-now.com:443
   - APAC (Asien-Pazifik): itomcnc-prod-gateway.apac.sncapps.service-now.com:443
3. Auf der Linux Server, auf dem der Agent installiert ist, geben Sie den folgenden Befehl ein:

```
CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>" INSTANCE_URL="https://<instance_url>" bash
 -c "$(curl -L https://<instance_url>/api/sn_agent/agents/install_agent)"
```

Weitere Informationen zu den Parameterwerten im Befehl finden Sie unter Agent Client Collector Parameter für Installationsbefehl ohne MID.

Installieren Sie ohne MID Agent Client Collector Manuell in einem macOS Umgebung

Installieren Sie ohne MID Agent Client Collector Manuell auf einem macOS Computer, um das Senden von Daten vom Service Desk-Mitarbeiter an die Instanz über die Cloud zu ermöglichen. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vorbereitungen

- Installieren Sie ITOM Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).
- Onboarding für Ihre zu verwendende Instanz ITOM Cloud-Services. Weitere Informationen erhalten Sie vom Kundensupport.
- Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Senden von Daten über die Cloud in einer Bereitstellung ohne MID finden Sie unter DEX-Architektur .

Prozedur

1. Laden Sie die Installationsdateien auf Ihren lokalen Computer herunter.

```
curl -L <download link from the Agent Downloads page on the instance>
```

2. Validieren Sie die Signatur der Installationsdatei.

```
pkgutil --check-signature agent-client-collector-<version number>-macos-catalina_x64.pkg
```

Hinweis: Stellen Sie sicher, dass die .pkg-Zertifikatkette über das Installationszertifikat der ServiceNow-Entwickler-ID verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Installieren Sie das Agent Client Collector-Paket.

```
sudo installer -pkg agent-client-collector-<version number>-macos-catalina_x64.pkg
 -target /
```

4. Kopieren Sie die Installationsdateien.

   a. Beispiel-Konfigurationsdatei:
   sudo cp -p /Library/Application\ Support/servicenow/agent-client-collector/acc.yml.example /Library/Application\ Support/servicenow/agent-client-collector/acc.yml

   b. Beispiel für eine Allow-Listen-Datei:
   sudo cp -p /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json.default /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json

5. **Wahlweise:** Um neue Prüfdefinitionen für die Allow-Liste zu erstellen, deaktivieren Sie zuerst die Allow-Liste, indem Sie den *`allow-list`*-Parameter in der Datei acc.yml auskommentieren.

   (Optional) sudo -H -u _servicenow vi /Library/Application\ Support/servicenow/agent-client-collector/acc.yml

   Hinweis: Diese Aktion beeinträchtigt die Sicherheit Ihres Systems und wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Sobald das Update abgeschlossen ist, aktivieren Sie die Allow-Liste wieder, indem Sie den Kommentar des Allow-Listen-Parameters in der Konfigurationsdatei entfernen.

   Weitere Informationen zum Hinzufügen benutzerdefinierter Prüfungen zu einer Allow-Liste finden Sie unter Agent Client Collector-Zulassungsliste generieren.

6. In acc.yml Konfigurationsdatei:

   a. Legen Sie die folgenden Parameter fest:

Parameter	Wert
Back-End-url	„<gateway URL>“
Connect-ohne-MID	wahr
Instanz-url	„<instance URL>“
Registrierungsschlüssel	„<regsitration-key>“
Unsicher-überspringen-tls-verifizieren	falsch

   b. Kommentieren Sie aus *`api-key`*Parameter.

7. Speichern Sie die Konfigurationsdatei.
8. Um sicherzustellen, dass die Konfigurationsdatei auf einen gültigen Endpunkt verweist, führen Sie die folgenden Befehle aus, um neu zu starten Agent Client Collector:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
sudo launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist
sudo launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist
```

Hinweis: Standardmäßig führt das Beenden des Installationsprogramms dazu, dass das Programm sofort neu gestartet wird. Damit das Programm nach dem Beenden im angehaltenen Zustand bleibt, legen Sie die Keep Alive-Eigenschaft in der Datei /Library/LaunchDaemons/com.sn.acc.plist auf **false** fest.

Installieren Sie ohne MID Agent Client Collector Mit einem einzeiligen Befehl in einem macOS Umgebung

Installieren Sie ohne MID Agent Client Collector Auf einem macOS Computer, um das Senden von Daten vom Service Desk-Mitarbeiter an die Instanz über die Cloud zu ermöglichen. Das Senden von Informationen über die Cloud ermöglicht den MID-Server Zur Verwendung für persistentere Ressourcen.

Vorbereitungen

- Installieren Sie ITOM Plugin „Cloud Services Core“ (sn_itom_Cloud_svc).
- Onboarding für Ihre zu verwendende Instanz ITOM Cloud-Services. Weitere Informationen erhalten Sie vom Kundensupport.
- Konfigurieren Sie einen Agent-Registrierungsschlüssel.
- Erforderliche Rolle: Stamm

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Registrierungsschlüssel**an.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Registrierungsschlüsselwert, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf einfach abrufen können.
2. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab:
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`
3. Auf dem Server, auf dem Sie installieren Agent Client Collector Geben Sie den folgenden Befehl ein:

```
CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>" INSTANCE_URL="https://<instance_url>" bash
 -c "$(curl -L https://<instance_url>/api/sn_agent/agents/install_agent)"
```

In der folgenden Tabelle werden die Parameterwerte im Befehl beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlszeilenparameterwerte

Parameter	Wert
CONNECT_WITHOUT_MID	Geben Sie An **Wahr** Zum Aktivieren der Installation ohne MID. Wenn Sie keinen Wert angeben, der reguläre MID-Server websocket-Installation wird aufgerufen.
ACC_CNC	Öffentlicher Gateway-Endpunkt für Agent Client Collector Die Sie angeben können.
REGISTRIERUNGSSCHLÜSSEL	Aktiver und gültiger Agent-Registrierungsschlüssel, mit dem der Service Desk-Mitarbeiter kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der sich der Service Desk-Mitarbeiter registriert.
ACC_ALLOW_LIST	Optional *ACC_ALLOW_LIST=0*Zeichenfolge, die Sie hinzufügen können, um die Allow-Liste zu deaktivieren. Standard: Die Allow-Liste ist aktiviert. **Hinweis:** Wenn Sie die Allow-Liste deaktivieren, gefährden Sie die Sicherheit Ihres Systems. Diese Aktion ist als temporäre Maßnahme gedacht, während Sie die Allow-Liste aktualisieren. Nachdem Sie das Update abgeschlossen haben, entfernen Sie es *ACC_ALLOW_LIST=0*Über die Befehlszeile.
ACC_VALIDATE_SIG	Optional *ACC_VALIDATE_SIG=0*Zeichenfolge, die Sie hinzufügen können, um die Verifizierung der Zertifizierungsvalidierung des Installationsprogramms zu deaktivieren. Standard: Validierung ist aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Konfigurieren Sie einen Agent-Registrierungsschlüssel

Konfigurieren Sie einen Agent-Registrierungsschlüssel, damit Sie MITTELLOS bereitstellen können Agent Client Collector. Bereitstellung ohne MID Agent Client Collector Ermöglicht Ihnen die Verwendung von MID-Server Für persistentere Ressourcen.

Vorbereitungen

Installieren Sie die Plugins, die für die Bereitstellung ohne MID erforderlich sind Agent Client Collector.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die geplante Aufgabe „Agent-Registrierungsschlüssel bereinigen“ wird täglich ausgeführt und löscht abgelaufene Registrierungsschlüssel. Die Dauer, für die ein Registrierungsschlüssel gültig ist, wird von gesteuert *sn_agent.registration_key_validity.days*Eigenschaft, basierend auf der Erstellung des Schlüssels. Die Zeit, die der Kunde vor dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bevorstehenden Ablauf des Schlüssels benachrichtigt wird, wird von gesteuert *sn_agent.registration_key_notification.days*Eigenschaft.

Wenn das Ablaufdatum eines Schlüssels näher rückt, erstellen Sie einen neuen Registrierungsschlüssel, und geben Sie ihn in alle vorhandenen Automatisierungsaufträge ein, um einen Ausfall der Registrierung zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Registrierungsschlüssel**an.
2. Wählen Sie **Neu**.
3. In **Name** Geben Sie einen beschreibenden Namen für den Registrierungsschlüssel ein.
4. **Wahlweise:** Um Benachrichtigungen zu erhalten, wenn ein Registrierungsschlüssel bald abläuft, wählen Sie im eine Gruppe mit einer gültigen E-Mail-Adresse aus **Besitzgruppe** Feld.
   Wenn Schlüssel über die geplante Aufgabe „Agent-Registrierungsschlüssel bereinigen“ gelöscht werden, erhält die angegebene Gruppe eine E-Mail-Benachrichtigung.
5. Wählen Sie **Absenden**.

Ergebnis

Der neue Agent-Registrierungsschlüssel kann zur Installation verwendet werden.

Zugehörige Informationen

Wird ohne MID installiert Agent Client Collector

Agent Client Collector Framework Konfigurationseigenschaften

Erstellen und bearbeiten Agent Client Collector Plugins

Je nach Bedarf können Sie die Standard-Plugins bearbeiten oder neue Plugins hinzufügen. Durch das Erstellen und Bearbeiten von Plugins werden die Überwachungsfunktionen von Agent Client Collector angepasst.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **ACC-Plugins**an.
2. Klicken Sie auf **Neu**.
   Die Seite **Agent Client Collector Plugin - New record** (Agent Client Collector-Plugin - Neuer Datensatz) wird angezeigt.
3. Geben Sie Werte in die Felder auf der Seite ein, wie in der folgenden Tabelle beschrieben.

Plugin-Felder für Agent Client Collector

Feld	Beschreibung
Name	Name des Plugin. Dieses Feld wird automatisch mit dem Namen der an das Plugin angehängten tar.gz-Datei gefüllt und wird nur angezeigt, wenn ein vorhandener Datensatz ausgewählt wird.
Beschreibung	Beschreibung des Plugin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Betriebssystem	Wählen Sie das Betriebssystem aus, das vom Plugin überwacht werden soll.
Plattform	Wählen Sie die Plattform aus, die vom Plugin überwacht werden soll.
Aktiv	Hierüber aktivieren Sie das Plugin und laden es auf den MID Server herunter.
Erweitert	Duch Aktivierung dieses Kontrollkästchens ermöglichen Sie die Auswahl der vom Plugin zu überwachenden Version des Betriebssystems.
BS-Version	Wählen Sie die Betriebssystemversion aus, die mit dem Plugin überwacht werden soll. Dieses Feld ist nur verfügbar, wenn das Kontrollkästchen **Advanced** (Erweitert) aktiviert ist.

4. Folgen Sie den Anweisungen auf der UI-Seite, um eine tar.gz-Datei an den Plugin-Datensatz anzuhängen.

Benutzerdefiniertes Plugin mit Zertifikat schützen

Wenn Sie eine anpassen oder erstellen Agent Client Collector Plugin können Sie das Plugin entweder mit einem Drittparteizertifikat oder einem internen sicheren Zertifikat im Skript des Plugins sichern. Offizielle Plugins werden von einer externen Zertifizierungsstelle signiert.

Standardmäßig ist die Verwendung eines selbstsignierten Zertifikats aktiviert. Um diese Funktion zu deaktivieren, legen Sie die Eigenschaft *`verify-plugin-signature`* auf **False** fest. Wenn Sie ein selbst signiertes Zertifikat deaktivieren, verwenden Ihre konfigurierten Plugins kein Zertifikat.

Weitere Informationen zum Konfigurieren eines selbstsignierten Zertifikats mit OpenSSL finden Sie unter Aktivieren Sie die sichere OpenSSL-Signatur für Plugins. Weitere Informationen zum Konfigurieren eines Drittparteizertifikats finden Sie in der Dokumentation des Drittanbieters.

Wenn die aktuellen Zertifikate des Service Desk-Mitarbeiters ein Plugin nicht validieren können, Agent Client Collector Fordert die aktualisierten Zertifikate von der synchronisierten an MID-Server. Sie können den Service Desk-Mitarbeiter manuell aktualisieren, um diese Zertifikate vor der geplanten Synchronisierung zu erhalten. Details finden Sie unter Manuell aktualisieren Agent Client Collector Zertifikate.

Sie können die Zertifikate manuell in einem Verzeichnis auf speichern MID-Server Die mit den installierten Agents verbunden ist. Jeder Service Desk-Mitarbeiter, der in Ihrer Umgebung installiert ist, kann dann auf die Zertifikate zugreifen MID-Server.

Weitere Informationen zum Konfigurieren der Eigenschaften der Zertifikatsynchronisierung finden Sie unter Synchronisierungseigenschaften für die Validierung Agent Client Collector Plugins.

Installation von Agent Client Collector

Sie können installieren Agent Client Collector Auf einem beliebigen unterstützten Hostcomputer. Die Agent Client Collector Stellt eine Verbindung zu her MID-Server Mithilfe des HTTP/S-Protokolls bleibt die Verbindung nach dem Herstellen aktiv. Eins MID-Server Kann mehrere Service Desk-Mitarbeiter gleichzeitig bearbeiten, während ein einzelner Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Desk-Mitarbeiter mit einem arbeitet MID-Server Und wechselt zu einem anderen MID-Server Wenn erforderlich, um Failover-Schutz bereitzustellen.

Wenn sich die IP-Adresse eines Agent ändert, wird basierend auf der MID-Server-Liste des Agent ein MID-Server ausgewählt, zu dem eine Verbindung hergestellt wird.

Die maximale Anzahl von Agents, die mit einem einzigen MID-Server verbunden sein können, kann in der Eigenschaft `sn_agent.mid.max_allowed_agents` MID-Server konfiguriert werden. Der Standardwert ist 4.000.

Für ACC-VC eine standardmäßige 1 GB MID-Server Kann 700 Service Desk-Mitarbeiter gleichzeitig unterstützen. Eine 8-GB-Konfiguration für einen MID-Server Kann 8.000 Service Desk-Mitarbeiter gleichzeitig unterstützen. Sie können auch skalieren. Beispiel: 5 MID Servers Mit einer Heap-Größe von 8 GB können Agents bis zu 40 000 verarbeiten.

Der Standardanwenderaccount ist ein lokaler Anwender namens **servicenow** . Dieser Anwender verfügt über Berechtigungen auf Basisebene.

In der folgenden Tabelle werden die Berechtigungen beschrieben, die für die Arbeit mit verschiedenen Funktionen erforderlich sind, die dem Service Desk-Mitarbeiter zugeordnet sind, pro Betriebssystem. Ein Sternchen (*) gibt an, dass keine speziellen Berechtigungen erforderlich sind.

Agent bei Endpunktbereitstellung

Funktion	Windows	Linux	macOS
Basisbestand	*	*	*
Seriennummer(n)	*	Sudo dmidecode	*
Ausführen von Prozessen	Programme debuggen	*	*
Zuordnung von TCP-Verbindungen zu laufenden Prozessen	*	Sudo ss	*
Speichergeräte	LOKALES SYSTEM	*	*
Angemeldete Benutzer	LOKALES SYSTEM	*	*
Selbstupgrade des Pakets	LOKALES SYSTEM	Sudo-RPM/dpkg	Nicht unterstützt

Wenn Sie den Agent vollständig auf einem einzelnen Hostserver neu installieren, wird ein zweiter Agent-Datensatz in der Instanz registriert. Löschen Sie den ursprünglichen Service Desk-Mitarbeiter auf der **Agent Client Collectors** Seite (**Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**) an.

Service Desk-Mitarbeiter, deren **Status = Ausgefallen** Oder **Verbindung Getrennt** Die nicht gelöscht wurden, werden nach 30 Tagen automatisch gelöscht. Sie können diese Einstellung auf der Autolush-Formularseite ändern (siehe Autolush-Formular).

Verwenden Sie das Manual Transport Layer Security Protocol (mTLS) für die sichere Authentifizierung zwischen MID-Webserver Und den Service Desk-Mitarbeiter (der Client).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details finden Sie unter Verbinden Sie den Service Desk-Mitarbeiter mit dem MID-Server MTLS wird verwendet.

Für Details zur Verwendung Agent Client Collector In einer Air-Gap-Umgebung finden Sie unter Agent Client Collector Framework – Lösung für die Verwaltung von Konfigurationselementen [KB1585753] artikel in Now Support Knowledge Base.

Agent Client Collector unterstützt Domänentrennung. Die Domäne des Agent und der von ihm erstellten CIs ist abhängig von der MID-Server-Domäne, mit der der Agent verbunden ist. Die Domäne des Anwenders muss die niedrigste Domänenebene (bekannt als Blattdomäne) sein, um die Erstellung einer WebSocket-Endpunkterweiterung für zu ermöglichen MID-Server.

Zugehörige Informationen

Agent Client Collector-Installation unter einem Linux-Betriebssystem

Installieren Sie Agent Client Collector Auf einem Windows Computer manuell

Agent Client Collector-Installation unter einem macOS-Betriebssystem

Agent Client Collector – Systemanforderungen

Systemanforderungen sind die grundlegenden Spezifikationen und Konfigurationen, die für die Installation und Ausführung erforderlich sind Agent Client Collector(ACC) effektiv.

Vor der Installation von Agent Client Collector müssen Sie folgende Schritte ausführen:

- Bei der Arbeit mit MID-Server:
  - Stellen Sie sicher, dass bei Ihrer Instanz mindestens ein MID Servers ordnungsgemäß registriert und validiert wurde, sodass dieser für eine Agent-Verbindungsanforderung verfügbar ist. Weitere Informationen finden Sie unter MID-Server werden konfiguriert . In einer Staging-Umgebung benötigen Sie nur eine MID-Server. Konfigurieren Sie in einer Produktionsumgebung jedoch mindestens zwei MID Servers Zur Unterstützung der Zero-Touch-Konfiguration und stellen Sie sicher, dass ein MID-Server Ist immer verfügbar, wenn einer fehlschlägt.
  - Stellen Sie sicher, dass eine validierte Verbindung vom angegebenen Server vorhanden ist, auf dem Sie den Service Desk-Mitarbeiter installieren MID-Server.
  - Stellen Sie sicher, dass MID-Server Port, auf dem Agent Client Collector Listener-Ausführungen sind zugänglich.
- Befolgen Sie bei der Arbeit mit einer Bereitstellung ohne MID die Anweisungen, die in beschrieben sind Konfiguration ohne MID Agent Client Collector.
- Stellen Sie sicher, dass in Ihrer Instanz die folgenden Plugins installiert sind:

Anwendung	Plugin
ACC-F	○ MID-Server ○ CMDB Für bereichsbezogene Anwendungen ○ Agent Client Collector Globale Dienstprogramme ○ MID-Webserver ○ Service-Fehlermanagement

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Plugin
ACC-VC	○ Agent Client Collector Visibility – Inhalt ○ Agent Client Collector Framework ○ Plugin Discovery [com.snc.discovery]
ACC-M	○ Agent Client Collector Framework ○ Agent Client Collector Monitoring ○ Ereignismanagement and Service-Mapping Core ○ Metrikdaten – Plugin [com.snc.sa.metric]
ACC-L	○ Agent Client Collector Framework ○ Agent Client Collector Log Analytics ○ Health Log Analytics
DEX	○ Agent Client Collector Framework ○ ITOM Cloud-Services Core [sn_itom_Cloud_svc]

Sie können überprüfen, ob diese Plugins auf dem installiert sind **Systemdefinitionen** > **Plugins** Seite.

Alle Plugins, die zum Lieferumfang des Basissystems gehören, sind mit dem ServiceNow-Zertifikat signiert. Optional können Sie anwenderdefinierte Plugins verwenden und sie mit Ihrem eigenen Zertifikat signieren, wie in beschrieben Aktivieren Sie die sichere OpenSSL-Signatur für Plugins.

- Stellen Sie sicher, dass Ihr System über die Mindestanforderungen für die Installation von Service Desk-Mitarbeitern verfügt.

Mindestanforderungen für die Installation

Agent Client Collector-Komponente	Anforderungen
Agent Client Collector Framework	○ 1 GB RAM ○ 300 MB freier Speicherplatz ○ 1 CPU-Kern
Agent Client Collector-Überwachung	○ 1 GB RAM ○ 1 GB freier Speicherplatz ○ 1 CPU-Kern
Agent Client Collector Visibility – Inhalt	○ 1 GB RAM ○ 1 GB freier Speicherplatz ○ 1 CPU-Kern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Sie installieren Agent Client Collector Unter einer der unterstützten Betriebssystemverteilungen:

Unterstützte Betriebssystemverteilungen

Betriebssystem	Verteilung
Linux	○ Red Hat Enterprise Linux – RHEL und Oracle Linux – OL 7, 8, 9 ○ CentOS 7, CentOS Stream 8 und 9 ○ SLES 12, 15 ○ Debian 9, 10, 11 ○ Ubuntu 18.04, 20.4, 22.04, 24,04 LTS ○ Amazon Linux 2 AMIS ○ Felsig Linux8 und 9
Windows (ACC-M und ACC-L werden nur auf Servern unterstützt, nicht auf Endpunkten)	○ Windows Server 2012, 2012r2, 2016, 2019, 2022 ○ Windows 10 Enterprise Edition ○ Windows 11 Professional und Enterprise ○ Windows 11 Oberfläche auf ARM64
macOS(Sowohl auf x86_64 als auch auf arm64 (Apple Silicon)-Architekturen. ACC-M und ACC-L werden nur auf Servern unterstützt, nicht auf Endpunkten)	○ Catalina ○ Big Sur ○ Monterey ○ Ventura ○ Sequoia

Wichtig: Alle unterstützten Betriebssysteme funktionieren nur mit dem CPU-Architekturtyp x86-64. ACC-F v3.1.1 fügt auch native Unterstützung für ARM64 auf Apple Silicon-Architekturen hinzu. Aktuelle Informationen finden Sie unter Agent Client-Sammlung auf nicht-x86-64-Computern und eingebetteten Tafeln [KB1172387] artikel in Now Support Knowledge Base.

Bei Verwendung von ACC-L: Agent Client Collector wird mit dem standardmäßigen `servicenow`-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector `servicenow`-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu /var/log/ unter Linux und des Pfads zu C:\Windows\System32 unter Windows. Informationen zum Konfigurieren von Berechtigungen für den `servicenow`-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Bei der Bestimmung der Anzahl der Computer und Server, die zur Unterstützung Ihrer Service Desk-Mitarbeiter erforderlich sind (z. B. die Anzahl der Computer, die Proxy-Agents erfordern), müssen Sie die Leistungs-KPIs der Service Desk-Mitarbeiter berücksichtigen. Details zu Service Desk-Mitarbeiter-Leistungs-KPIs finden Sie unter Agent Client Collector Leistung und Platzbedarf für URL-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden

Stellen Sie Agent Client Collector auf einem virtuellen Computer während einer Massenbereitstellung mithilfe des Basis-Image bereit. Bei der Massenbereitstellung findet eine automatische Installation statt, bei der der Installationsstatus nicht transparent ist.

Vorbereitungen

Verwenden Sie Microsoft SCCM, um die Bereitstellung und Sicherheit Ihrer Geräte zu verwalten, wie im KB-Artikel Create a Windows service account with Log on as a Service (Windows-Servicekonto mit Anmeldung als Service erstellen) beschrieben.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agenten-Downloads**an.
2. Laden Sie die Installationsdatei des entsprechenden Betriebssystems herunter.
3. Installieren Sie den Agent gemäß den entsprechenden BS-Anweisungen.
4. Führen Sie den folgenden Befehl aus, um den Agent-Service zu stoppen:
   - In einem Windows Umgebung: Führen Sie den Befehl aus `sc – AgentClientCollector stoppen`
   - In einem Linux Umgebung: Führen Sie den Befehl aus `Sudo systemctl Stoppkonz`
5. Stellen Sie sicher, dass `acc.yml` Datei enthält keinen verschlüsselten API-Schlüssel.
   Beispiel: `api-Schlüssel: „<nur-Text-API-Schlüssel hier einfügen>“`
6. Löschen Sie den Inhalt des Cache-Verzeichnisses des Service Desk-Mitarbeiters, wobei die Verzeichnisstruktur intakt bleibt:
   - In einem Windows Umgebung: C:\ProgramData\ServiceNow\Agent-Client-Collector\Cache
   - In einem Linux Umgebung: /Var/Cache/servicenow/Agent-Client-Collector
7. Bei der Installation auf einem Windows Stellen Sie sicher, dass die Installation erfolgreich war, indem Sie einen der folgenden Schritte ausführen:
   - Aktivieren Sie die Protokollierung in der automatischen Installation, und stellen Sie sicher, dass die Protokolldatei mit der Zeichenfolge Windows Installer installed the product endet.
   - Stellen Sie sicher, dass der Service **AgentClientCollector** den Status Running (Wird ausgeführt) aufweist.
8. Bei der Installation auf einem Linux Computer, greifen Sie auf den Computer zu, auf dem der Agent installiert ist, und ändern Sie den /Usr/share/servicenow/Agent-Client-Collector/serial_number.txt Datei auf eine der folgenden Arten:
   - Ändern Sie deren Inhalt mit der Seriennummer des Hosts, indem Sie den folgenden Befehl ausführen: `sudo -n dmidecode -s system-serial-number`
   - Weisen Sie dem Benutzer servicenow sudo-Berechtigungen zu, um die Ausführung des folgenden `osqueryi`-Befehls zu ermöglichen: `sudo -E env "PATH=$PATH" osqueryi --logger_min_status=3 --line "select hardware_serial from system_info"`

   Hinweis: Sie müssen den Hostnamen der virtuellen Maschine nach der Bereitstellung in einen eindeutigen Wert ändern, um Schäden am CI des Hosts zu vermeiden.

9. Starten Sie den Agent-Service als Schritt nach der Bereitstellung neu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In einem Windows Umgebung: Führen Sie den Befehl aus `sc startet AgentClientCollector`
- In einem Linux Umgebung: Führen Sie den Befehl aus `Sudo systemctl Start` gemäß

Lastenausgleichsmodul von Agent Client Collector aktivieren

Aktivieren Sie einen Lastenausgleichsmodul, um sicherzustellen, dass Sie funktionsfähig sind MID Servers. Ein Lastenausgleichsmodul verteilt Ressourcen auf mehrere MID Servers Um sicherzustellen, dass keine Einzelperson MID-Server Ist überlastet.

Vorbereitungen

1. Installieren Sie Agent Client Collector Framework.
2. Konfigurieren Sie Agent Client Collector Webserver.
3. Stellen Sie sicher, dass Sie Zugriff auf die Lastenausgleichsmodul-Konfiguration der internen Anwendung haben.
4. Überprüfen Sie, ob die Datei `<mid_server_install_path>/static/hello.txt` Wurde während erstellt MID-Server Setup.

   `hello.txt` Ist eine leere Datei, die manuell erstellt wird, um eine HTTP-Antwort 200 abzurufen.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Lastenausgleichsmodule sind standardmäßig nicht konfiguriert. Gehen Sie wie folgt vor, um einen Lastenausgleichsmodul in Ihrer Umgebung zu konfigurieren.

Prozedur

1. Konfigurieren Sie den Lastenausgleichsmodul so, dass er in verwendet werden kann *`backend-url`*Parameter in `acc.yml` Konfigurationsdatei.
2. Führen Sie die folgenden Setup-Aktionen für den Lastenausgleichsmodul aus:

   a. Erhöhen Sie die Leerlauf-Zeitüberschreitung auf 300 Sekunden.

   b. Konfigurieren Sie die Lastenausgleichsmodul-Zielgruppe mit *`https`*Und Port 443.
   Konfigurieren Sie alle MID Servers Hinter dem Lastenausgleichsmodul als Ziele.

   c. Konfigurieren Sie die Integritätsprüfung des Lastenausgleichsmoduls, um zu überwachen `<mid_server_install_path>/static/hello.txt` Datei erstellt während MID-Server Setup.
   Die Integritätsprüfung stellt sicher, dass keine Kommunikationsunterbrechungen zwischen dem Lastenausgleichsmodul und dem auftreten MID-Server.

3. Fügen Sie hinzu `<mid_server_install_path>/static/hello.txt` Datei für jeden statischen Ordner MID-Server.
   Sie können die Datei an einem anderen Speicherort ablegen, für den keine Anmeldeinformationen erforderlich sind, um das Setup zu vereinfachen.
4. Aktualisieren Sie die ACC.yml-Konfigurationsdatei mit dem entsprechenden FQDN (*`backend-url`*Wert) und Portnummer, und deaktivieren Sie automatisch MID-Server Auswahl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
backend-url:
 - wss://<fqdn>:<port>/ws/events
enable-auto-mid-selection: false
```

5. Starten Sie neu Agent Client Collector.

Ergebnis

Die Agent Client Collector Der Datenfluss wird wie in beschrieben fortgesetzt Agent Client Collector-Architektur.

Hinweis:

Bei der Arbeit mit SSL werden alle Zertifikate oder Zertifikatketten konfiguriert, die von verwendet werden MID Servers Muss von Stammzertifikatstellen signiert werden, deren Zertifikate in einer einzelnen gebündelt sind .PEM Datei. Um die signierten Zertifikate an den Agent zu übertragen, geben Sie die PEM-Datei in der Eigenschaft `trusted-ca-file` der YML-Konfigurationsdatei des Agent an. Informationen zur Verbesserung der Sicherheit mit der SSL-/TLS-Konfiguration finden Sie unter Dokumentationsmaterial für ITOM Agent Client Collector artikel in Now Support Knowledge Base.

Führen Sie ein Upgrade für einen Agent in einer Instanz durch

Führen Sie ein selektives Selbstupgrade anstelle eines Massenupgrades durch, um die Effizienz bei der Arbeit mit Service Desk-Mitarbeitern zu erhöhen, die schwer zugänglich sind, z. B. Service Desk-Mitarbeitern, die in der Cloud bereitgestellt werden. Sie können ein selektives Upgrade für bis zu 20 Service Desk-Mitarbeiter gleichzeitig durchführen.

Vorbereitungen

Hinweis: Ein selektives Upgrade ist für die Service Desk-Mitarbeiter-Version 2.7.0 und höher verfügbar.

Unterstützte Betriebssysteme: Windows Und Linux.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Bei der Arbeit in Linux Umgebung: Stellen Sie sicher, dass Sie über sudo-Berechtigungen verfügen und die folgenden Konfigurationen festgelegt sind:

Linux-Betriebssysteme

BS	BS-Version	Befehle	Agent-Version
CentOS,Red Hat	7, 8	• /Usr/bin/systemctl Start gemäß • /Usr/bin/systemctl STOP ACC • <systemctl location>- Daemon-reload (Standardstandort ist /Usr/bin) • /Usr/bin/rpm -UV <Cache dir location>/ Upgrade/agent-client-collector-upgrade.rpm Standardspeicherort des Cache-Verzeichnisses: /Var/Cache/ servicenow/Agent-Client-Collector • Entpacken Sie -o : Entpackt die Signaturdatei, um die Installation zu validieren. • openssl-dgst -sha256 -Verify : Überprüft die Verwendung einer Signatur aus einer servicenow-Installationsdatei.	2,7
Debian, Ubuntu		• /Usr/bin/systemctl Start gemäß • /Usr/bin/systemctl STOP ACC • <systemctl location>- Daemon-reload (Standardstandort ist /Usr/bin) • /Usr/bin/dpkg --	2,7

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-Installationen müssen auf diese URL zugreifen: https://install.service-now.com/.

Erforderliche Rolle:

- Windows: Lokaler SYSTEMACCOUNT (Agent Client Collector Service wird ausgeführt als *Local System*)
- Linux: Sudo rpm/dpkg
- macOS: Sudo-Paket

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector Unterstützt selektives Selbstupgrade in den folgenden Betriebssystemen:

- Windows: Aufgrund von Windows UAC-Einschränkungen, muss der Service Desk-Mitarbeiter als lokaler SYSTEMACCOUNT ausführen, um das Upgrade über durchzuführen *msiexec*.
- Linux: RPM und DEB

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie den Service Desk-Mitarbeiter aus, für den Sie ein Upgrade durchführen möchten.
3. In **Zugehörige Links** Abschnitt auswählen **Service Desk-Mitarbeiter upgraden** .
4. Wählen Sie im Bestätigungsdialogfeld aus **Upgrade** .
   Die **Agent-Upgrade-Verläufe** Seite wird angezeigt, auf der Sie den Upgrade-Fortschritt in überwachen können **Status** Spalte, die entweder angezeigt wird **Erfolg** Oder **Fehlgeschlagen** .
5. Zeigen Sie das Protokoll für das Service Desk-Mitarbeiter-Upgrade in an **Nachricht** Spalte.
   Für ein fehlgeschlagenes Upgrade auf einem Linux Computer, navigieren Sie zu <Cacheverzeichnisspeicherort>/Upgrade/agent-client-collector-upgrade.rpm Datei und stellen Sie sicher, dass die Konfigurationen für das entsprechende Betriebssystem gemäß festgelegt sind Linux Tabelle „Betriebssysteme“, oben.

   Für ein fehlgeschlagenes Upgrade auf einem Windows Computer, überprüfen Sie die relevante Protokolldatei unter <user folder>\AppData\local\Temp\ACC_Logs :
   - ACC-Protokolle: ACC_Upgrade.log
   - MSI-Protokolle: MSI_ACC_Upgrade.log

Führen Sie ein Upgrade für mehrere Agents in einer Instanz durch

Wenn Sie ein selektives Upgrade eines Service Desk-Mitarbeiters in einer Instanz durchführen, können Sie mehrere Instanzen auswählen, die gleichzeitig aktualisiert werden sollen.

Vorbereitungen

Unterstützte Betriebssysteme: Windows Und Linux.

ACC-Installationen müssen auf diese URL zugreifen: https://install.service-now.com/.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können bis zu 20 Service Desk-Mitarbeiter gleichzeitig für ein Upgrade auswählen. Um eine große Anzahl von Service Desk-Mitarbeitern zu aktualisieren, integrieren Sie Agent Client Collector In Ihre Softwarebereitstellungstools.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Aktivieren Sie das Kontrollkästchen neben den Agents, die Sie upgraden möchten.
   Sie können bis zu 20 Service Desk-Mitarbeiter auswählen.
3. In **Aktionen für ausgewählte Zeilen...** Feld auswählen **Service Desk-Mitarbeiter upgraden** .
4. Wählen Sie im Bestätigungsdialogfeld aus **Upgrade** .

Zugehörige Informationen

Führen Sie ein Upgrade für einen Agent in einer Instanz durch

Führen Sie ein hohes Volumen durch Agent Client Collector Upgrade

Führen Sie ein Upgrade für ein hohes Volumen von durch Agent Client Collector Service Desk-Mitarbeiter, wenn Sie alle Ihre Service Desk-Mitarbeiter gleichzeitig upgraden möchten.

Vorbereitungen

Konfigurieren Sie Agent Client Collector Webserver. Details finden Sie unter Websocket-Server auf MID-Server installieren.

Stellen Sie sicher, dass MID-Server, MID-Webserver, Und MID-Server websocket-Server wird ausgeführt.

Erforderliche Rollen: Agent_Client_Collector_admin

- In einem Windows Umgebung: Lokaler SYSTEMACCOUNT
- In einem Linux Umgebung: Sudo rpm/dpkg
- In einem macOS Umgebung: Sudo-Paket

Warum und wann dieser Vorgang ausgeführt wird

Ein Upgrade mit hohem Volumen wird nicht unterstützt Agent Client Collector Bis MID-Server Kommunikation über mTLS.

Beim Durchführen eines Upgrades mit hohem Volumen werden alle Service Desk-Mitarbeiter aktualisiert, die nicht die aktuellste Version verwenden. Für Agents, die bereits die aktualisierte Version verwenden, wird kein Upgrade durchgeführt.

Prozedur

1. Stellen Sie sicher, dass die Versionsnummer, auf die Sie ein Upgrade durchführen möchten, verfügbar ist.
   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
   b. Suchen Sie nach `sn_agent.agent_version`Eigenschaft.
      Die in angezeigte Nummer **Wert** Spalte ist die Versionsnummer, auf die ein Upgrade durchgeführt werden kann.
2. Aktivieren Sie die Eigenschaft in der Tabelle „Systemeigenschaften“ (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**), um das Upgrade zu aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie nach *sn_agent.auto_upgrade_enabled*Eigenschaft.

b. Legen Sie den Eigenschaftswert mit **wahr** fest.
Das Upgrade beginnt innerhalb einer Minute nach Aktivierung der Eigenschaft.

Ergebnis

Bei der geplanten Aufgabe werden jeweils 50 Service Desk-Mitarbeiter aktualisiert MID-Server Pro Stunde.

- Erfolgreich aktualisierte Agents werden auf angezeigt *Agent Client Collectors*Seite (**Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**) Und zeigt die Zielversion in an **Version** Spalte.
- Die *Agent Upgrade Histories*Die Registerkarte eines auf der Seite „Agent Client Collectors“ ausgewählten Service Desk-Mitarbeiters enthält die folgenden Informationen.
  - Die **Status** Spalte gibt den Fortschritt des Upgrades an (*Success*Oder *Failed*).
  - Die **Nachricht** Spalte zeigt das Protokoll an, das für den bestimmten Service Desk-Mitarbeiter relevant ist.
- Service Desk-Mitarbeiter, die kein Upgrade erfolgreich durchgeführt haben, zeigen die vorherige Versionsnummer an. Informationen zum Upgrade dieser Service Desk-Mitarbeiter finden Sie unter Wiederholen Sie das Upgrade mit hohem Volumen für fehlgeschlagene Service Desk-Mitarbeiter.

Um die Anzahl der Service Desk-Mitarbeiter zu ändern, die gleichzeitig aktualisiert werden, aktualisieren Sie den Wert von *sn_agent.auto_upgrade.max_upgrades_per_handler_per_hour*Eigenschaft (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an. Die maximale Anzahl von Service Desk-Mitarbeitern, die gleichzeitig für alle aktualisiert werden können MID Servers Ist 1.000.

Um die Häufigkeit des Upgrades zu ändern, aktualisieren Sie den Wert des Wiederholungsintervalls in **Service Desk-Mitarbeiter Inkrementell Upgraden** Geplante Aufgabe (**Alle** > **Systemdefinition** > **Geplante Aufgaben**) an.

Wiederholen Sie das Upgrade mit hohem Volumen für fehlgeschlagene Service Desk-Mitarbeiter

Wenn das Upgrade mit hohem Volumen für bestimmte Service Desk-Mitarbeiter fehlschlägt, müssen Sie den Verlauf der problematischen Service Desk-Mitarbeiter löschen, um das Upgrade erneut zu aktivieren. Wenn sich die Ziel-Upgrade-Version ändert, müssen Sie den Verlauf der Service Desk-Mitarbeiter nicht löschen, da die Service Desk-Mitarbeiter mit dem nächsten geplanten Upgrade mit hohem Volumen upgraden.

Vorbereitungen

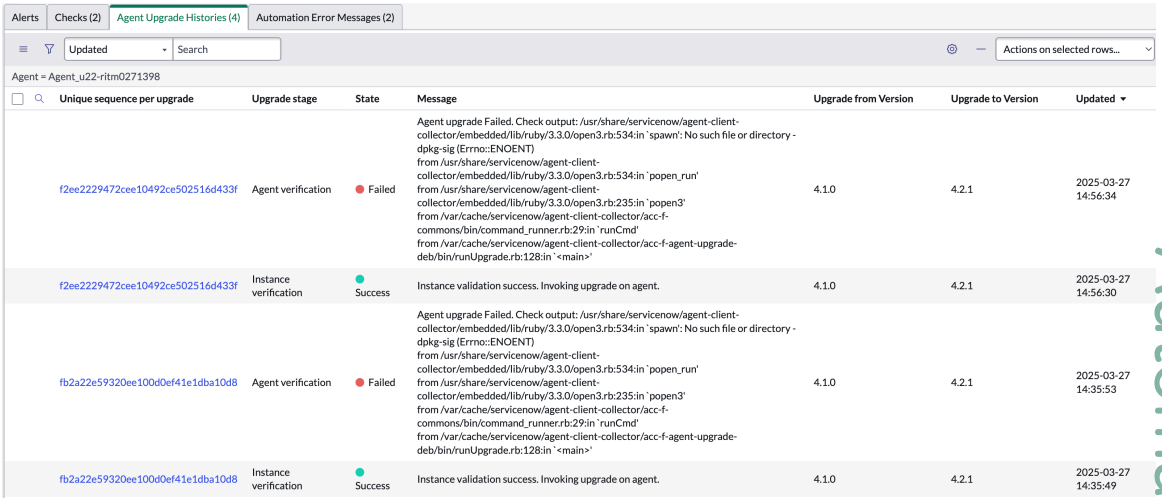
Erforderliche Rollen: Agent_Client_Collector_admin

- In einem Windows Umgebung: Lokaler SYSTEMACCOUNT
- In einem Linux Umgebung: Sudo rpm/dpkg
- In einem macOS Umgebung: Sudo-Paket

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Seite Agent Client Collectors **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie einen Eintrag aus, für den die *`Version`*Nummer ist nicht die höchste verfügbare Version.
3. Suchen Sie nach *`Agent Upgrade Histories`*Registerkarte.



4. Unter dem Kontrollkästchen Symbol, bewegen Sie den Mauszeiger neben einen fehlgeschlagenen Upgrade-Eintrag, und aktivieren Sie das Kontrollkästchen, das angezeigt wird.
5. Wählen Sie den Pfeil neben dem aus **Aktionen für ausgewählte Zeilen...** Dropdownliste und wählen Sie aus **Löschen** .

Ergebnis

Die angegebenen Service Desk-Mitarbeiter werden mit dem nächsten geplanten Upgrade für hohe Volumina aktualisiert.

Agents manuell neu starten

Führen Sie einen manuellen Neustart eines Service Desk-Mitarbeiters durch, wenn die Agent-Konfigurationsdatei aktualisiert wurde oder wenn der Agent instabil ist. Ein manueller Neustart ist nur für Agents möglich, die entweder in einer Windows-Umgebung installiert sind oder als Linux-basierte Agents `systemd` verwenden.

Vorbereitungen

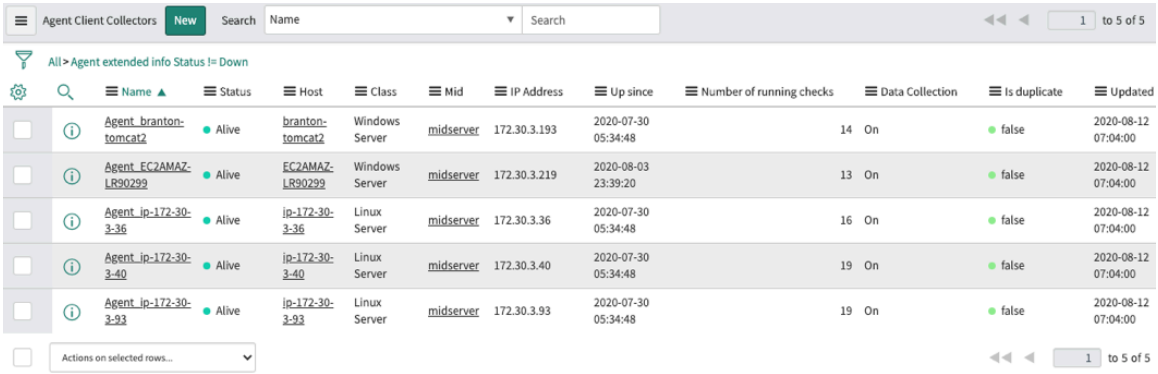
Erforderliche Rolle: agent_client_collector_admin

Prozedur

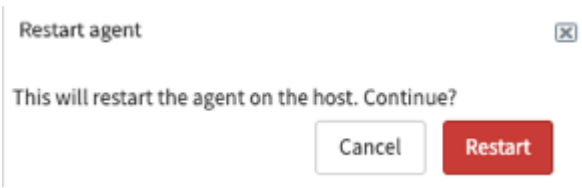
1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
   Die Seite **Agent Client Collectors** wird mit der Liste der Agents angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Aktivieren Sie das Kontrollkästchen des Agent, den Sie neu starten möchten.
   Sie können mehrere Agents auswählen.
3. Wählen Sie in der Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) unter der Liste der Agents die Option **Restart Agent** (Agent neu starten) aus.
   Ein Bestätigungsdialogfeld wird angezeigt.



4. Wählen Sie Aus **Starten Sie Neu** .
   Alternativ können Sie den Service Desk-Mitarbeiter aus dem Agent-Datensatz neu starten, indem Sie den Namen des Service Desk-Mitarbeiters und in auswählen **Zugehörige Links** Abschnitt auswählen **Starten Sie den Agent neu** .

Agent Client Collector-Installation unter einem Linux-Betriebssystem

Installieren Agent Client Collector Auf einem System, das ein Linux-Betriebssystem verwendet, entweder mithilfe eines einzeiligen Befehlsskripts oder gemäß dem Installationsverfahren, um in Ihren eigenen Paketverteilungsmechanismus einzubetten. Das Installationsverfahren sorgt für Konsistenz bei der Verwendung von Paketverteilungslösungen.

Installieren Agent Client Collector Auf einem Linux System

Installieren Agent Client Collector Mit einem Paketverteilungstool. Vor der Installation können Sie manuell installieren Agent Client Collector Auf einigen Computern, um sicherzustellen, dass Ihre Service Desk-Mitarbeiter die richtigen Richtlinien und Prüfungen enthalten, bevor Sie eine große Anzahl von Service Desk-Mitarbeitern installieren.

Vorbereitungen

- Stellen Sie sicher, dass Agent Client Collector Listener ist auf konfiguriert MID Servers, Und der Service ist auf Ihren Zielhosts verfügbar.
- Stellen Sie sicher, dass das Betriebssystem und die Version Ihres Servers unterstützt werden. Eine Liste der unterstützten Betriebssysteme und Versionen finden Sie unter Installation von Agent Client Collector.
- Überprüfen Sie, ob Einschränkungen oder Anforderungen während der Bereitstellung beachtet werden müssen, z. B. die Angabe eines anderen Accounts als des standardmäßigen servicenow-Accounts. Weitere Informationen zum Einbetten des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Desk-Mitarbeiters in Ihr eigenes automatisiertes System finden Sie unter ITOM Agent Client Collector – Dokumentationsmaterial [KB1122613] .

- Stellen Sie sicher, dass MID-Server Und ist MID-Webserver Und ACC-WebSocket-Endpunkterweiterungen werden ausgeführt.
- Rufen Sie ab MID-Server ACC-Listener-Informationen, die im Agent angegeben werden sollen *backend-url*Parameter.
  1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**an.
  2. Wählen Sie einen MID-Server.
  3. Wählen Sie aus **ACC-WebSocket-Endpunkte** Registerkarte.
  4. Wählen Sie einen websocket-Endpunkt aus.
  5. Kopieren Sie den Wert in **Endpunkt-URL** Feld.
- Rufen Sie ab MID-Server API-Schlüssel, der im Agent angegeben ist *api-key*Parameter.
  1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Webserver API-Schlüssel**an.
  2. Wählen Sie den API-Schlüssel aus, den Sie verwenden möchten.
  3. In **Zugehörige Links** Abschnitt auswählen **Zeigen Sie den API-Schlüssel an** .
  4. Kopieren Sie den API-Schlüsselwert, und schließen Sie das Popup-Fenster.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Während Linux Installation (und Upgrade), ist die ausführbare Agent-Datei mit aktiviert Linux Fähigkeiten (CAP_SETFCAP, CAP_SETPCAP) standardmäßig. Speichern Sie Apps wie Agent Client Collector Log Analytics(ACC–L) Kann dies verwenden, um Fähigkeiten zum Lesen des gesamten Dateisystems (CAP_DAC_READ_SEARCH) zu gewähren. Das System durchläuft verschiedene Sicherheitsmaßnahmen, z. B. die doppelte Verifizierung der Inhaltsquelle, die Nutzung des Plugin-Verifizierungsprozesses usw., um sicherzustellen, dass die Gewährung von Fähigkeiten kein Sicherheitsrisiko darstellt. Dieses Verfahren setzt voraus, dass Sie mit den Befehlen für vertraut sind Linux Fähigkeiten.

Um diese erweiterten Fähigkeiten zu deaktivieren, führen Sie die folgenden Befehle basierend auf aus Linux Betriebssystem/Verpackungssystem:

Befehle zum Deaktivieren der erweiterten Linux-Fähigkeit

Betriebssystem/Verpackungssystem	Befehle
U/MIN	ACC_SKIP_CAPS=true yum/dnf localinstall ACC_SKIP_CAPS=wahr rpm -VI Agent-Client-Collector-<version number>-x86_64.rpm
Debian	ACC_SKIP_CAPS=wahr apt-get-Installation ACC_SKIP_CAPS=wahr dpkg -i Agent-Client-Collector-<version number>-<distro>_amd64.deb

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehle zum Deaktivieren der erweiterten Linux-Fähigkeit (Fortsetzung)

Betriebssystem/Verpackungssystem	Befehle
SLES	`ACC_SKIP_CAPS=True Zypper-Installation`

Prozedur

1. Laden Sie die entsprechenden Installationspakete herunter.
   - Für manuelle Installation:
     a. Navigieren zu > **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads**an.
     b. Laden Sie die entsprechende RPM- oder deb-Installationsdatei herunter.
     c. Laden Sie die relevanten Signaturdateien herunter Dient zum Validieren der Installationsdateien.
   - Führen Sie für die Befehlszeileninstallation die folgenden Befehle aus, um die Signatur- und Installationsdateien auf Ihren lokalen Computer herunterzuladen:

```
curl -LO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-<version_number>-x86_64.rpm
curl -LO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-<version_number>-x86_64-rpm-rpm.zip
```

   Hinweis: Jeder Curl-Befehl muss in einer einzelnen Zeile angezeigt werden.

2. **Wahlweise:** Überprüfen Sie die Paketsignatur.
   a. Extrahieren Sie die Installationsdatei (falls komprimiert), indem Sie den folgenden Befehl ausführen:
   `unzip agent_client-collector-<version_number>-x86_64-rpm-rpm.zip`
   b. Validieren Sie die Signatur der Installationsdatei, indem Sie die angegebenen Befehle ausführen.
      - In einem RPM-basierten System:

```
openssl dgst -sha256 -verify {<ServiceNow DGST pem key>} -signature {<signature file>} agent-client-collector-<version number>-x86_64.rpm
```

      Wo `<ServiceNow DGST Pem Key>` Ist .PEM Datei aus extrahiert .Zip Datei, und `<signature file>` Ist .Bin Datei aus extrahiert .Zip Datei.

      Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-x86_64.rpm
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
$ unzip agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
Archive: agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
inflating: ServiceNow_Digicert_DGST.pem
extracting: agent-client-collector-3.0.0-x86_64.bin
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
$ openssl dgst -sha256 -verify ServiceNow_Digicert_DGST.pem -signature
 agent-client-collector-3.0.0-x86_64.bin agent-client-collector-3.0.0-x86_64.rpm
Verified OK
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile angezeigt werden.

- Auf einem Debian-basierten System:

  (Optional) `gpg –-Import ServiceNow_DigiCert_public.gpg`

  `Sudo gpg –-verify Agent-Client-Collector-<version number>-<distro>_amd64.deb`

  Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-cli
ent-collector-3.0.0-debian-9_amd64.deb
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-cli
ent-collector-3.0.0-debian-9_amd64-deb-deb.zip
$ unzip agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
Archive: agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
extracting: ServiceNow_Digicert_Public.gpg
$ gpg --import ServiceNow_Digicert_Public.gpg
gpg: /home/admin/.gnupg/trustdb.gpg: trustdb created
gpg: key 985DD52C6A0ABB45: public key "ServiceNow, Inc. (Signing)
 <seceng@servicenow.com>"
imported
gpg: Total number processed: 1
gpg: imported: 1
$ dpkg-sig --verify agent-client-collector-3.0.0-debian-9_amd64.deb
Processing agent-client-collector-3.0.0-debian-9_amd64.deb...
GOODSIG _gpgbuilder 9B928FB49771DF6C047430DD985DD52C6A0ABB45 1665054068
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile angezeigt werden.

3. Installieren Sie Agent Client Collector Paket, das den Paketmanager verwendet, der zugeordnet ist Linux Verteilung.

BS	Befehl
RHEL-basiert	Yum/dnf localinstall
SLES	Zypper-Installation
Debian-basiert	APT-Get-Installation

Alternativ können Sie, wenn diese Befehle nicht richtig konfiguriert sind, die Core-Befehle verwenden, die für die Ausführung mit den Paketmanager-Befehlen konfiguriert sind.

- RPM-basiertes System: `# Rpm -VI Agent-Client-Collector-<version number>-x86_64.rpm`
- Debian-basiertes System: `# Dpkg -i Agent-Client-Collector-<version number>-<distro>_amd64.deb`

Vergewissern Sie sich, dass die Paketbefehle mit Ihrem Systemadministrator korrekt konfiguriert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Für einige Dateisysteme sind möglicherweise Einschränkungen aktiviert, z. B. /Var/ Kann mit bereitgestellt werden *noexec*Kennzeichnung. Da der Agent ausführen muss Agent Client Collector Plugins, die normalerweise in gespeichert werden /Var/Cache Verzeichnis müssen Sie die Anwendung in bestimmten Ordnern bereitstellen, indem Sie die Installationspfade mit anpassen `--relocate`Option als .U/min Parameter.

Beispiel: `RPM -i --relocate /var/Cache=/opt/Cache Agent-Client-Collector-<version_number>-x86_64.rpm`

Die folgenden Pfade können verschoben werden:

Pfad	Notizen
/Etc	Beim Aktualisieren müssen Sie auch aktualisieren *allow-list*Parameter in acc.yml Datei mit dem neuen Pfad.
/usr/share	N/V
/var/cache	Wird aktualisiert /Var Das Verzeichnis behält alle bei /Var Unterverzeichnisse, geschachtelt unter dem neuen Verzeichnis.
/var/log	
/var/run	
/var	

Überprüfen Sie die Pfade in /Usr/lib/systemd/System/acc.service Um sicherzustellen, dass sie wie erwartet angezeigt werden.

4. Konfigurieren Sie bei der Installation eines .deb-Pakets die des Service Desk-Mitarbeiters acc.yml Konfigurationsdatei.

   a. Kopieren Sie die Beispielkonfigurationsdatei, indem Sie den folgenden Befehl ausführen.

   ```
   # cp -p /etc/servicenow/Agent-Client-Collector/ACC.yml.example /etc/servicenow/Agent-Client-Collector/ACC.yml
   ```

   b. Benennen Sie die Allow-Listendatei um.

   ```
   # cp -p /etc/servicenow/Agent-Client-Collector/check-allow-list.json.default /etc/servicenow/Agent-Client-Collector/Check-allow-list.JSON
   ```

   Hinweis: Dieser Schritt ist für RPM-Pakete, die mit enthalten sind, nicht relevant acc.yml Und Check-allow-list.JSON Dateien, die im Basissystem enthalten sind.

5. Aktualisieren Sie die Konfigurationsdatei, und fügen Sie hinzu *check-allow-list.json*Bis /Etc/ servicenow/Agent-Client-Collector Und kopieren Back-End-url Und api-Schlüssel Aus der Instanz. Zum Beispiel:

```
---
# Agent Client Collector configuration
backend-url:
 - "wss://YOUR_MID_ENDPOINT_HERE:YOUR_MID_PORT_HERE/ws/events"
api-key: "YOUR_API_KEY_HERE"
log-level: "info"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
insecure-skip-tls-verify: false
allow-list: /etc/servicenow/agent-client-collector/check-allow-list.json
verify-plugin-signature: true
max-running-checks: 10
disable-sockets: true
disable-api: true
statsd-disable: true
enable-auto-mid-selection: false
agent_cpu_threshold:
 cpu_percentage_limit: 25
 repeated_high_cpu_num: 3
 monitor_interval_sec: 60
 agent_cpu_threshold_disabled: false
```

Die *allow-list*Funktion, die angibt, welche Befehle vom Agent ausgeführt werden dürfen, ist aktiviert.

6. Konfigurieren Sie Sudoers.

Die Konfiguration wird normalerweise von automatisiert Linux Sysadmin. Um die manuelle Konfiguration durchzuführen, wenn Sie die Richtigkeit vor der vollständigen Konfiguration sicherstellen möchten, führen Sie die folgenden Schritte aus.

```
# visudo -f /etc/sudoers.d/01_servicenow
User_Alias ACC_USERS = servicenow
Cmnd_Alias ACC_CMD = /usr/sbin/dmidecode -s
 baseboard-serial-number,/usr/sbin/dmidecode -s
 chassis-serial-number,/usr/sbin/dmidecode -s system-serial-number,/usr/sbin/dmidecode
 -s system-uuid,/usr/sbin/ss -tanp
Cmnd_Alias ACC_CMD_SETENV = /usr/bin/netstat -ltnup,/usr/bin/ls
 -l /proc/*,/usr/bin/cat /proc/*
ACC_USERS ALL = (root) NOPASSWD:ACC_CMD
ACC_USERS ALL = (root) NOPASSWD:SETENV:ACC_CMD_SETENV
Defaults:ACC_USERS !requiretty
```

7. Konfigurieren Sie den Agent so, dass er als Dienst ausgeführt wird.

a. Schützen Sie den Ressourcenverbrauch, indem Sie die angegebenen Werte zu hinzufügen /Usr/lib/systemd/System/acc.service Datei.

- CPUShares=128
- CPUQuota = 10 %
- Arbeitsspeicherlimit = 192M
- BlockIOWeight = 10
- LimitNICE=15

Zum Beispiel:

```
# vi /usr/lib/systemd/system/acc.service
[Unit]
Description=Agent-Now acc
After=network-online.target
[Service]
Environment=AGENT_ROOT=/usr/share
Environment=AGENT_CACHE_ROOT=/var/cache
Environment=AGENT_CONFIG_ROOT=/etc
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Environment=AGENT_LOG_ROOT=/var/log
Environment=AGENT_RUN_ROOT=/var/run
Environment=RUBYOPT=-Eutf-8
User=servicenow
Group=servicenow
ExecStart=/usr/share/servicenow/agent-client-collector/bin/acc-service start acc
KillMode=process
Restart=on-failure
RestartSec=1min
CPUShares=128
CPUQuota=10%
MemoryLimit=192M
BlockIOWeight=10
LimitNICE=+15
[Install]
WantedBy=network-online.target
```

b. Führen Sie den Befehl „Daemon neu laden“ aus, wenn Sie die Servicedatei nach dem Aktivieren des ACC-Service geändert haben.

`# Systemctl Daemon-reload`

c. Aktivieren und starten Sie den Service, indem Sie die folgenden Befehle ausführen.

`# Systemctl aktivieren nach`

`# Systemctl Start gemäß`

Validieren Linux Installation

Nach der Installation von Agent Client Collector Auf einem Linux System: Validieren Sie die Installation, indem Sie sicherstellen, dass sie ordnungsgemäß abgeschlossen wurde.

Vorbereitungen

Installieren Sie Agent Client Collector Auf einem Linux System (siehe Installieren Agent Client Collector Auf einem Linux System).

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Führen Sie aus `# Systemctl-Status gemäß` Befehl.
Die *`active (running)`* Der Indikator wird angezeigt, wenn der Service ordnungsgemäß ausgeführt wird.

```
# systemctl status acc
● acc.service - Agent-Now ACC
Loaded: loaded (/usr/lib/systemd/system/acc.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-25 14:10:24 UTC; 6 months 23 days ago
Main PID: 2693 (acc)
Tasks: 10 (limit: 512)
Memory: 143.4M (limit: 192.0M)
CPU: 12h 57min 50.442s
CGroup: /system.slice/acc.service
└─2693 /usr/share/servicenow/agent-client-collector/bin/acc start --config-file
/etc/servicenow/agent-client-collect...
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Zeigen Sie verschlüsselte an *api-key* Und *agent-key-id* Wird verwendet, indem ausgeführt wird Grep -E „^api-key|Agent-key-ID“ /etc/servicenow/Agent-Client-Collector/ACC.yml Befehl.

```
# grep -E '^api-key|agent-key-id' /etc/servicenow/agent-client-collector/acc.yml
api-key: "encrypted:adskfjldfjlasd+ajflksadjmoreunreadablestringasdfdfkdjksdjaasdfas"
agent-key-id: b4ac2ab4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4a
```

Hinweis: Die *grep* Befehl muss in einer einzelnen Zeile angezeigt werden.

3. Zeigen Sie die Verbindung des Service Desk-Mitarbeiters mit seiner Back-End-URL an, indem Sie ausführen Grep „erfolgreich verbunden“ /var/log/servicenow/Agent-Client-Collector/acc.log Befehl.

```
# grep 'successfully connected' /var/log/servicenow/agent-client-collector/acc.log
2022-11-17T19:03:17.94 [INFO] [agent] successfully connected to the url:
wss://MY_BACKEND_FQDN:MY_BACKEND_PORT/ws/events
```

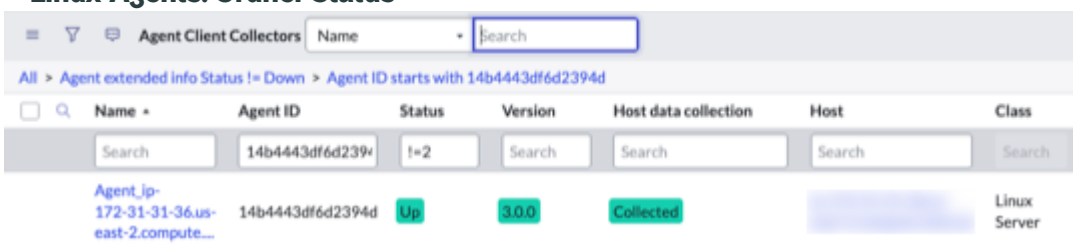
Hinweis: Die *grep* Befehl muss in einer einzelnen Zeile angezeigt werden.

4. Überprüfen Sie die eindeutige Agent-ID, indem Sie ausführen # Echo $(hexdump -e '/1 "%02x" /var/Cache/servicenow/Agent-Client-Collector/Agent_now_ID) Befehl.

```
# echo $(hexdump -e '/1
 "%02x"' /var/cache/servicenow/agent-client-collector/agent_now_id)
14b4443df6d2394d
```

Die angegebene Service Desk-Mitarbeiter-ID wird auf der Seite „Service Desk-Mitarbeiter“ in einer Instanz (**Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**) Mit **Status = Aktiv** Und **Hostdatensammlung = erfasst** (Beide werden grün angezeigt).

Linux-Agents: Grüner Status



Upgrade Agent Client Collector Auf einem Linux System

Aktualisieren Sie Ihr vorhandenes Agent Client Collector Version auf einem System, auf dem ein Linux-Betriebssystem ausgeführt wird, wenn das einzeilige Befehlsskript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten.

Vorbereitungen

- Das Upgrade-Verfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. **Wahlweise:** Sichern Sie vertrauliche Dateien, indem Sie den folgenden Befehl ausführen.

```
tar -Pcvzf /root/acc_backup.tar.gz /etc/servicenow/agent-client-collector \
/var/cache/servicenow/agent-client-collector/agent_now_id \
/usr/lib/systemd/system/acc.service
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Laden Sie das .rpm/.deb-Agent-Paket und die Signaturdateien herunter, wie in beschrieben Installieren Agent Client Collector Auf einem Linux System.
3. Upgrade des Pakets.
   - In einem RPM-basierten System:

     RPM: UV Agent-Client-Collector-<version number>-x86_64.rpm

   - In einem DEB-basierten System:

     Dpkg -i Agent-Client-Collector-<version number>-<distro>_amd64.deb
4. Stellen Sie die Systemd-Servicedatei (wenn Sie die Datei angepasst haben) entweder mit einem Automatisierungstool oder durch erneutes Laden der Systemd-Konfiguration wieder her.

```
tar -C / -Pxvzf /root/acc_backup.tar.gz usr/lib/systemd/system/acc.service
```

```
systemctl daemon-reload
```

5. Ändern Sie *owner:group*Stellen Sie die richtige Einstellung durch Ausführen des folgenden Befehls ein.

```
chown -R
 servicenow:servicenow /{etc,var/cache,var/log,usr/share}/servicenow/agent-client-collector
```

6. Starten Sie den Service neu, und stellen Sie sicher, dass er mit seiner Back-End-url verbunden ist.

```
systemctl restart acc
tail -f /var/log/servicenow/agent-client-collector/acc.log
```

Deinstallieren Agent Client Collector Von einem Linux System manuell

Deinstallieren Sie Agent Client Collector Manuell von einem Linux-Computer aus, wenn das Befehlsskript nicht verfügbar ist, da der spezifische Agent nicht mit der Instanz verbunden ist.

Vorbereitungen

- Das Deinstallationsverfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird ein deinstallierter Agent nach 30 Tagen aus dem System entfernt. Um diese Zeit zu ändern, aktualisieren Sie *sn_agent_ci_extended_info*Tabelle, zugänglich über die Seite „automatisch leeren“ (Eingabetaste *sys_auto_flush.LIST*In das Suchfilterfeld der Instanz).

Prozedur

1. Halten Sie den Service an.
   sudo systemctl stop acc
2. Verwenden Sie das entsprechende Paketverwaltungstool, um den Service zu entfernen.
   - Entfernen Sie Agent-Client-Collector
   - APT-GET – Entfernen Sie Agent-Client-Collector
   - Zypper entfernt Agent-Client-Collector

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alternativ können Sie basierend auf dem verwendeten Betriebssystem einen der folgenden Befehle ausführen.

- RPM: E Agent-Client-Collector
- Dpkg -r Agent-Client-Collector

3. Wenn Sie entweder ausgeführt haben U/min Oder Dpkg Befehl, entfernen Sie alle verbleibenden Dateien aus Ihrem System.

```
# userdel -r servicenow
# groupdel servicenow
# rm -R /{etc,var/cache,var/log,usr/share}/servicenow/agent-client-collector
```

Warnung: Verwenden Sie nicht den Befehl rm -RF, da dies zu Datenverlust führen kann.

Einzeilige Agent Client Collector-Installation unter Linux

Verwenden Sie ein effizientes einzeiliges Befehlsskript, um Agent Client Collector auf einem Computer mit Linux-Betriebssystem zu installieren. Wenn ein Skript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten, müssen Sie Agent Client Collector möglicherweise manuell installieren.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Stellen Sie sicher, dass das Entpacken-Programm auf Ihrem installiert ist Linux Computer.
- Bestimmen Sie die Ressourcengrenzwerte für den Service Desk-Mitarbeiter, der in konfiguriert werden soll /Usr/lib/systemd/System/acc.service Datei nach der Installation.
- Stellen Sie sicher, dass Sie über verfügen openssl Und DIG (Für RHEL/CentOS/SUSE-Installation) Pakete verfügbar, die vom Installationsskript verwendet werden sollen.
- Stellen Sie sicher, dass Sie über verfügen gpg Paket zur Validierung verfügbar (für Ubuntu/Debian-Installation).
- Wenn Sie eine einzeilige Installation für mehr als einen Agent durchführen, laden Sie das Agent-Paket auf Ihren lokalen Computer herunter. Platzieren Sie das Paket mit einem Ansible-Skript auf Ihrem *FTP*-Server. Weitere Informationen zur Massenbereitstellung von Agents finden Sie unter Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden.
- Damit der Agent die Betriebssystem-Seriennummern und TCP-Verbindungen mit zugehörigen laufenden Prozessen abrufen kann, ist auf Linux-Systemen sudo-Zugriff für „dmidecode“ und „ss“ erforderlich.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Rufen Sie die Websocket-URL-Parameter des MID-Server s ab.
   a. Navigieren zu **Agent Client Collector** > **Websocket-Endpunkt** Und wählen Sie den entsprechenden websocket-Endpunkt aus.
   b. Kopieren Sie den Wert des Felds **Endpunkt-URL**, der im Installationsbefehl verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Kopieren und bearbeiten Sie die folgende Befehlszeile, und ersetzen Sie die Befehlsparameter durch Ihre eigenen Informationen.
   `ACC_API_KEY=<api_key> ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events bash -c "$(curl -L https://<instance URL>/api/sn_agent/agents/install_agent)"`

   Befehlsparameter

Parameter	Wert
ACC_API_KEY	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird Wenn kein ACC_API_KEY-Wert angegeben ist, werden Sie während der Ausführung des Skripts aufgefordert, den API-Schlüsselwert einzugeben.
ACC_MID	URL des MID-Server-Websocket Wenn Sie mehrere angeben MID Servers, Geben Sie eine durch Kommas getrennte Zeichenfolge ein MID-Server.

3. **Wahlweise:** Wenn Sie neue Prüfdefinitionen erstellen müssen, die in die Allow-Liste aufgenommen werden sollen, die angibt, welche Prüfungen für den Agent aktiviert sind, deaktivieren Sie die Allow-Liste, indem Sie *`ACC_ALLOW_LIST=0`* zur einzeiligen Befehlszeichenfolge hinzufügen.

   Hinweis: Diese Aktion beeinträchtigt die Sicherheit Ihres Systems und wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Nach der Aktualisierung aktivieren Sie die Allow-Liste erneut, indem Sie *`ACC_ALLOW_LIST=0`* aus der einzeiligen Befehlszeichenfolge entfernen.

4. **Wahlweise:** Wenn der Zertifikatvalidierungsprozess zu zeitaufwendig ist oder Sie den Agent für Entwicklungszwecke verwenden, können Sie die Zertifikatvalidierung umgehen, indem Sie der einzeiligen Befehlszeichenfolge *`ACC_VALIDATE_SIG=0`* hinzufügen.
5. Führen Sie den einzeiligen Befehl aus (der in Schritt angegeben ist) 2, Oben) auf dem Server, auf dem Agent Client Collector Ist installiert.
6. **Wahlweise:** Konfigurieren Sie Ressourcengrenzwerte für den Service Desk-Mitarbeiter in /Usr/lib/systemd/System/acc.service Datei entsprechend Ihren Geschäftsanforderungen.

   (Optional) Die Standardwerte in der Datei sind:

   - *`CPUShares`*: 128
   - *`CPUQuota`*: 10 %
   - *`MemoryLimit`*: 192M
   - *`BlockIOWeight`*: 10
   - *`LimitNICE`*: +15

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector unter Linux mit einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem Linux-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn das Skript nicht mit der Instanz verbunden ist, müssen Sie Agent Client Collector möglicherweise manuell deinstallieren.

Vorbereitungen

- Das Deinstallationsverfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

Deinstallieren Agent Client Collector Durch Ausführen des folgenden Befehls in einem Befehlsfenster, in dem <instance url> Ist die URL von ServiceNow Instanz.
`Bash -c „$(curl -L https://<instance url>/api/sn_Agent/Agents/install_Agent)“ -s „--remove“` .

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei acc.yml und das zugehörige Verzeichnis von Ihrem Computer entfernt.

Agent Client Collector Installation auf einem Windows Computer

Bei der Installation von Agent Client Collector Auf einem Windows Auf dem Computer entweder eine Installationsdatei herunterladen und einen Assistenten verwenden, um den Service Desk-Mitarbeiter manuell zu installieren, oder die automatische Installation verwenden, um die Installation und Konfiguration des Service Desk-Mitarbeiters zu automatisieren. Mit der manuellen Installation können Sie den Service Desk-Mitarbeiter auf einem einzelnen System testen, während Sie die automatische Installation den Service Desk-Mitarbeiter skalieren können.

Installieren Sie Agent Client Collector Auf einem Windows Computer manuell

Installieren Sie Agent Client Collector Auf einem Windows Computer manuell, wenn Sie den Service Desk-Mitarbeiter auf einem einzelnen System testen möchten.

Vorbereitungen

1. Stellen Sie sicher, dass Sie konfiguriert haben Agent Client Collector Webserver. Details finden Sie unter Websocket-Server auf MID-Server installieren.
2. Überprüfen Sie Betriebssystem und Version Ihres Servers.
3. Wenn Sie Microsoft Internet Explorer verwenden, gehen Sie wie folgt vor, um die Agent Client Collector-Installationsdatei vorzubereiten:
   a. Navigieren zu **Servermanager** > **Lokaler Server**an.
   b. Deaktivieren Sie **Verstärkte Sicherheitskonfiguration für IE**.
   c. Laden Sie die Installationsdatei herunter.
   d. Ändern Sie die Erweiterung der Installationsdatei von .man in .msi.

Informationen zur Fehlerbehebung finden Sie unter KB2200094 artikel in der HI Knowledge Base.

Erforderliche Rolle: agent_client_collector_admin

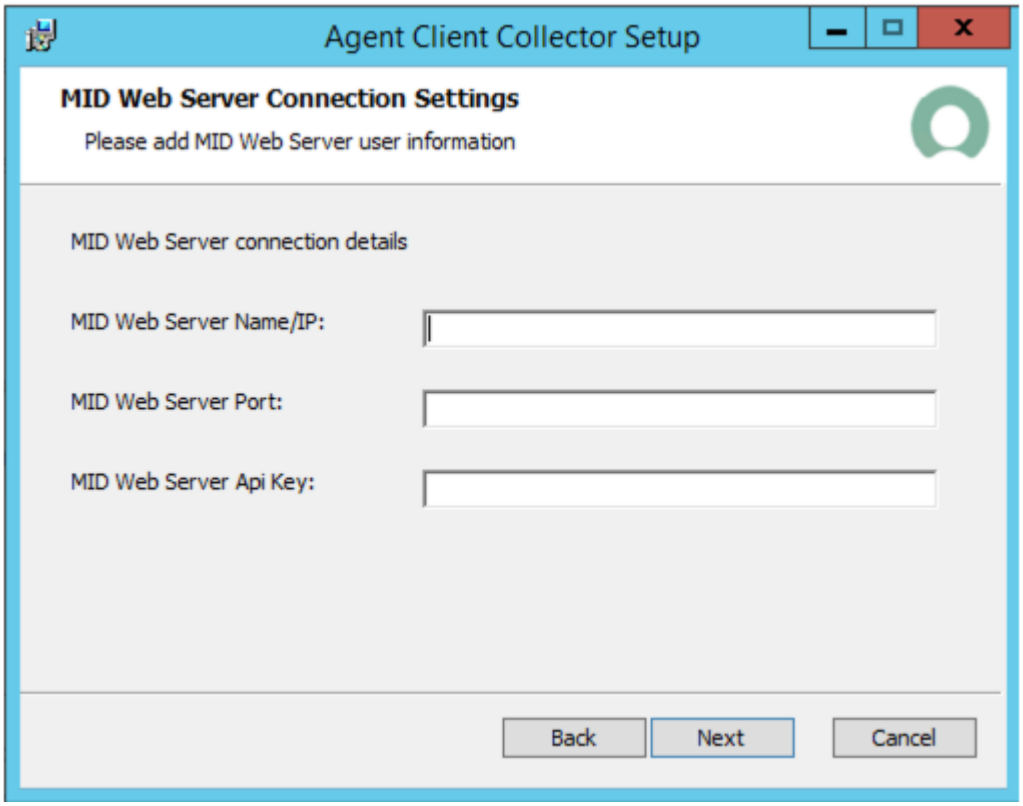
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Agent Client Collector** > **Agenten-Downloads**an.
2. So führen Sie die Installation mit dem Assistenten durch:

   a. Laden Sie die .msi-Datei herunter, auf die über den Link in der Benutzeroberfläche zugegriffen werden kann.
   Der Installationsassistent wird geöffnet.

   b. Wählen Sie Aus **Als Nächstes** Bis Sie erreichen **MID-Webserver-Verbindungseinstellungen** Seite.



   c. Geben Sie in die Felder des Dialogfelds die relevanten Parameter ein:

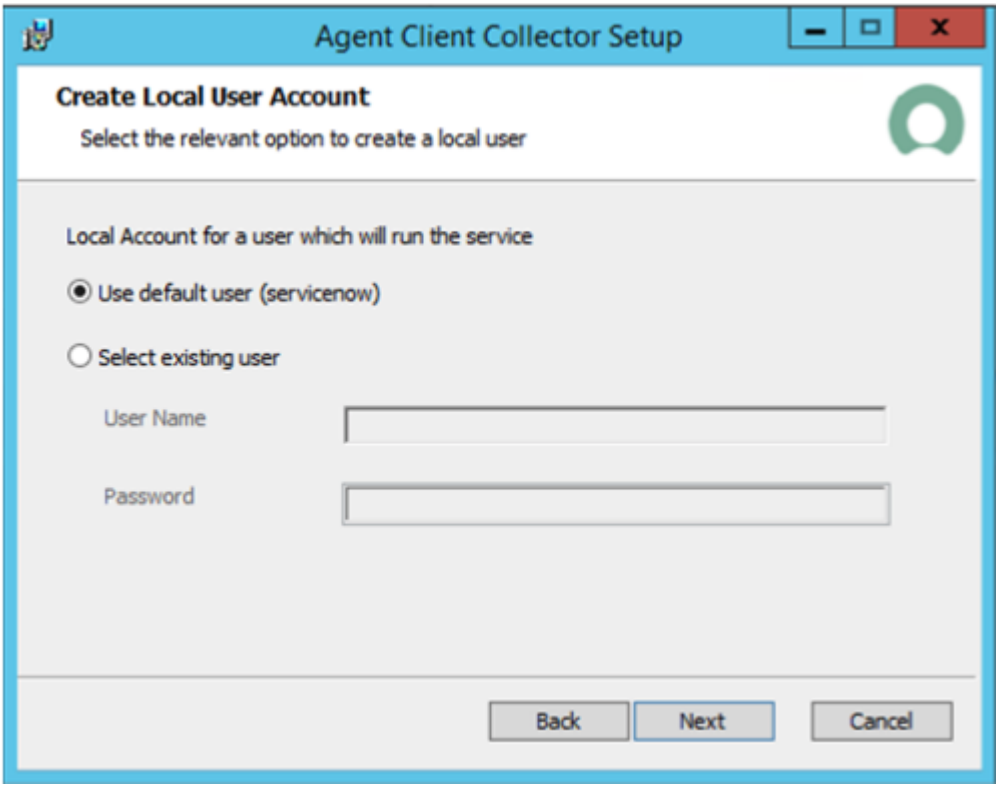
Felder für MID-Webserver-Verbindungseinstellungen

Feldname	Beschreibung
MID Web Server Name/IP (Name/IP des MID-Webservers)	IP-Adresse des MID-Webservers
MID Web Server Port (Port des MID-Webservers)	Portnummer des MID-Webservers. Verwenden Sie eine Zahl zwischen 1024 und 49151.
MID Web Server API Key (API-Schlüssel des MID-Webservers)	API-Schlüssel für den Zugriff auf den MID-Webserver

   d. Wählen Sie **Weiter**.
   Die Seite **Create Local User Account** (Lokales Benutzerkonto erstellen) wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wählen Sie im Dialogfeld die relevante Option aus.

Dialogfeld „Create Local User Account" (Lokales Benutzerkonto erstellen)

Optionen	Beschreibung
Use default user (servicenow) (Standardbenutzer (servicenow) verwenden)	Standardbenutzer, mit dem Agent Client Collector auf einem Windows-Computer ausgeführt werden soll Wenn Sie diese Option auswählen, wird ein lokaler Anwender mit dem Namen erstellt **servicenow** Als Teil der Installation. Das servicenow-Anwenderpasswort wird zufällig generiert und nicht im System gespeichert. Auf dem Hostcomputer wird ein Sicherheitsereignis erstellt, das bei Wiederholung das Öffnen eines Supportfalls erfordert. Weitere Informationen finden Sie unter KB1649116 artikel in der HI Knowledge Base.
Select existing user (Vorhandenen Benutzer auswählen)	Wenn Sie diese Option auswählen, konfigurieren Sie die folgenden Unterfelder:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen	Beschreibung
	▪ **User Name** (Benutzername): Benutzername zum Anmelden bei der Windows-Umgebung ▪ **Password**: (Passwort) Kennwort des ausgewählten Benutzers Der Anwender kann einer der folgenden sein: ▪ Lokaler Anwender (vom Besitzer der virtuellen Maschine erstellt; bietet zusätzliche Resilienz). ▪ Domänenanwender (erstellt von IT-Mitarbeitern). ▪ Group Managed Service Account (GMSA): Geben Sie den Namen des gruppenverwalteten Service-Accounts in ein **Anwendername** Und lassen Sie das Feld **Passwort** Feld leer. ▪ Lokaler Service-Account: Geben Sie Ein *LOCALSERVICE*In **Anwendername** Und lassen Sie das Feld **Passwort** Feld leer. ▪ Lokaler Systemaccount: Geben Sie Ein *SYSTEM*In **Anwendername** Und lassen Sie das Feld **Passwort** Feld leer. Aufgrund von Windows UAC-Einschränkungen. Die Ausführung des Service Desk-Mitarbeiters als lokaler SYSTEMACCOUNT ist erforderlich, um ein Upgrade über durchzuführen *msiexec*.

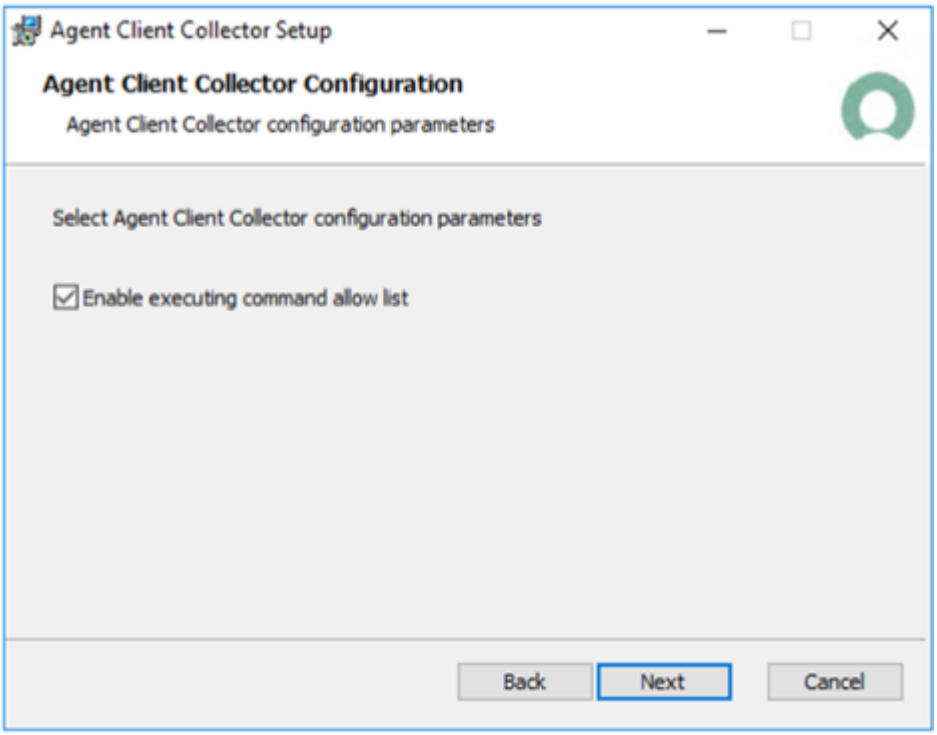
Hinweis: Mithilfe eines lokalen Systemkontos wird die lokale Gruppe erstellt *ServiceNow Users*, Und fügt der Gruppe den erstellten Anwender hinzu. Die Gruppe „ServiceNow-Anwender“ hat Zugriff auf Agent Client Collector Verzeichnisse und hat die folgenden Berechtigungen:

- **Performance Monitor**: Gehört zum Lieferumfang des Basissystems; ermöglicht die Anzeige aller Leistungszähler im System
- **Melden Sie sich als Service an** : Ermöglicht das Starten von Netzwerkservices und Services, die kontinuierlich ausgeführt werden, auch wenn niemand bei der Konsole angemeldet ist.
- **Debuggen von Programmen** : Aktiviert das Debugging von Prozessen und das Lesen von Prozessdetails für Anwender außerhalb von ServiceNow Anwendergruppe.

f. Wählen Sie Aus **Erstellen Sie Einen Anwender** .
Im System wird ein Windows-Benutzer mit den angegebenen Anmeldeinformationen erstellt, und die Seite „Agent Client Collector Configuration“ (Agent Client Collector – Konfiguration) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Um die **Allow-Liste** mit den aktivierten Prüfungen zur Ausführung nach der Einrichtung zu aktivieren, aktivieren Sie auf der daraufhin angezeigten Seite das Kontrollkästchen **Enable executing command allow list** (Ausführungsbefehl für Allow-Liste aktivieren).



h. Wählen Sie Aus **Als Nächstes** Um die Installationsseite zu öffnen.

Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**, um den Assistenten zu beenden und zu schließen.

Nach einer erfolgreichen Installation startet der Service automatisch und generiert Folgendes:

- Benutzer: Standard = servicenow (Zur Verwaltung des Service kann auch ein vorhandener Benutzer konfiguriert werden.) Der Benutzer servicenow gehört zur lokalen Benutzergruppe der **ServiceNow-Benutzer**.
- Service: AgentClientCollector
- Dateispeicherort:
  - Standard für Installation = C:\Programme\ServiceNow\agent-client-collector
  - Standard für Servicedateien = C:\ProgramData\ServiceNow\Agent-Client-Collector , Der enthält Cache , Konfiguration , Und Protokoll Ordner.

3. Wenn Sie die automatische Installation ausführen möchten, um Installationsberichte zu deaktivieren, führen Sie die Befehlszeile im Abschnitt **Silent installation** (Automatische Installation) des Verfahrens wie folgt aus:

```
msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value>
ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events ACC_ALLOW_LIST=False
```

Um die Allow-Liste der angegebenen Prüfungen beim Ausführen der automatische Installation zuzulassen, setzen Sie den Parameter *`ACC_ALLOW_LIST`* auf **True**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Zum Konfigurieren mehrerer MID Servers Führen Sie bei der Silent-Installation die Befehlszeile aus, die im angezeigt wird **Automatische Installation** Abschnitt des Verfahrens mit kommagetrennten Werten wie folgt:
`msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value> ACC_MID="wss://<mid1_ip>:<websocket1_port>/ws/events,wss://<mid2_ip>:<websocket2_port>/ws/events"`

   Fügen Sie die folgenden Parameterwerte in den Befehl ein:

   Befehlsparameter

Parameter	Wert
ACC_API_KEY	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird
ACC_MID	URL des MID-Server-Websocket
DENY_LOCAL_LOGON	Wenn auf festgelegt *True*, Verhindert, dass sich andere Anwender als der standardmäßige servicenow-Anwender beim Service anmelden. Standardwert: False
PASSWORD_NEVER_EXPIRES	Wenn auf festgelegt *True*, Das Passwort für den standardmäßigen servicenow-Anwender läuft nie ab. Standardwert: False
START_SERVICE	Wenn auf festgelegt *True*, Agent Client Collector Service wird nach der Installation automatisch gestartet. Standardwert: True
LOCALUSERNAME	Account, auf dem ausgeführt wird Agent Client Collector Als Windows Service. Mögliche Werte: ○ SYSTEM ○ LOCALSERVICE ○ DOMÄNE\GMSA$ ○ Zeichenfolge (lokaler Anwendername) Standard = `servicenow` Wenn Sie die Konten SYSTEM, LOCALSERVICE oder DOMÄNE\GMSA $ verwenden, müssen Sie kein Passwort konfigurieren.
LOCALPASSWORD	Passwort für den im Parameter LOCALUSERNAME angegebenen Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die konfigurierten MID-Server-Werte werden automatisch der Datei acc.yml hinzugefügt. Der Agent stellt eine Verbindung zum ersten verfügbaren MID-Server in der Liste her.

Um einen sekundären MID Server zu konfigurieren, geben Sie im Abschnitt backend-url der Datei acc.yml die folgende Syntax gemäß .yml-Standard ein: - "wss://<MID IP>:<Web socket port>/ws/events" (mit Anführungszeichen).

Manuelles Upgrade von Agent Client Collector auf einem Windows-System

Führen Sie ein manuelles Upgrade Ihrer vorhandenen Agent Client Collector-Version auf einem Windows-Betriebssystem durch.

Vorbereitungen

Sichern Sie Agent Client Collector Konfigurationsdateien, z. B. acc.yml , Check-allow-list.JSON , Agent_now_ID Und Agent_now_Keystore . Die Agent_now_ID Befindet sich im Cache-Verzeichnis: C:\ProgramData\ServiceNow\Agent-Client-Collector\Cache

Das Sichern von Konfigurationsdateien ist eine Sicherheitsmaßnahme zum Schutz der Dateien während des Upgrades. Konfigurationsdateien müssen nur wiederhergestellt werden, wenn Upgradeprobleme auftreten, die eine Neuinstallation erfordern.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Drücken Sie die Windows-Taste auf Ihrer Tastatur, und geben Sie **Dienste** ein, um die Services-Seite zu öffnen.
2. Suchen Sie den Agent Client Collector-Dienst.
3. Klicken Sie mit der rechten Maustaste auf den Agent Client Collector-Dienst und wählen Sie **Anhalten** aus.
4. Wählen Sie in der Windows-Systemsteuerung die Option **Programm deinstallieren** aus.
5. Wählen Sie das Agent Client Collector-Programm und anschließend **Deinstallieren** aus.
6. Navigieren zu **Agent Client Collector** > **Agenten-Downloads** Und Laden Sie das MSI-Installationsprogramm in herunter **Windows-Downloads** Abschnitt.
7. Installieren Sie den neuen Agent, wie in Installieren Sie Agent Client Collector Auf einem Windows Computer manuell beschrieben.
   Sie können entweder das manuelle oder das einzeilige Verfahren verwenden. Beim Wiederherstellen von Sicherungsdateien ersetzt das System die Werte der Konfigurationsdatei.
8. Halten Sie den Dienst nach Abschluss der Installation an.
9. Stellen Sie die agent_now_id- und agent_now_keystore-Konfigurationsdateien wieder her.
10. Starten Sie den Agent Client Collector-Dienst neu.

Agent Client Collector manuell von einem Windows-Computer deinstallieren

Anstatt mit dem einzeiligen Befehl können Sie Agent Client Collector auf einem Windows-Computer auch manuell deinstallieren. Nutzen Sie das manuelle Verfahren, wenn das Befehlsskript nicht verfügbar ist, weil der entsprechende Agent nicht mit der Instanz verbunden ist.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Deinstallieren Sie Agent Client Collector In Windows Systemsteuerung.

Installieren Sie Agent Client Collector Auf einem Windows Computer mit automatischer Installation

Installieren Sie Agent Client Collector Auf einem Windows Computer mit automatischer Installation, wenn Sie den Agent skalieren möchten.

Warum und wann dieser Vorgang ausgeführt wird

Bei der automatischen Installation wird automatisch ein lokaler Anwender mit dem Namen erstellt **servicenow** (Es sei denn, ein anderer vorhandener Anwender wird mit aufgerufen *LOCALUSERNAME*Parameter, wie in der Tabelle der Befehlsparameter im folgenden Verfahren beschrieben). Das servicenow-Anwenderpasswort wird zufällig generiert und nicht im System gespeichert. Auf dem Hostcomputer wird ein Sicherheitsereignis erstellt, das bei Wiederholung das Öffnen eines Supportfalls erfordert. Weitere Informationen finden Sie unter KB1649116 artikel in Now Support Knowledge Base.

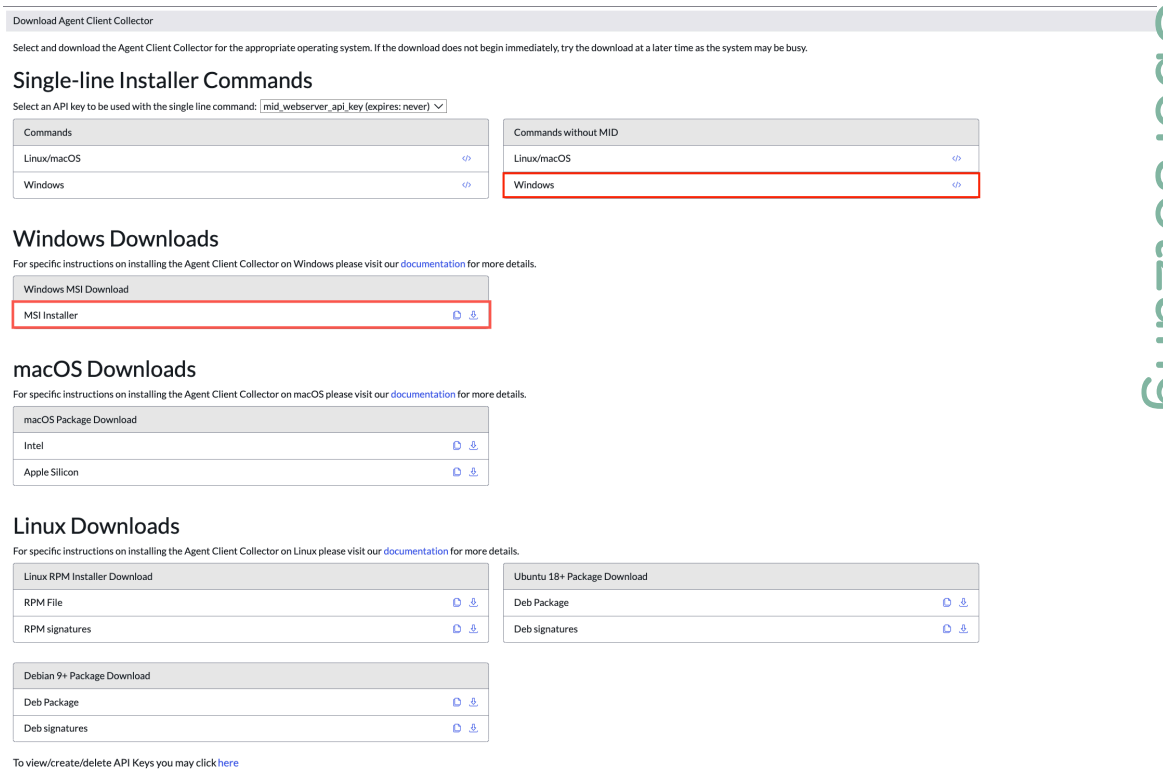
Vorbereitungen

ACC-Installationen müssen auf diese URL zugreifen: https://install.service-now.com/.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads**an.
2. Von Windows Download-Abschnitt herunterladen: Laden Sie das MSI-Installationsprogramm herunter, indem Sie das Download-Symbol ( ).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn Sie die automatische Installation ausführen möchten, um Installationsberichte zu deaktivieren, führen Sie die Befehlszeile im Abschnitt **Silent installation** (Automatische Installation) des Verfahrens wie folgt aus:
   `msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value> ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events ACC_ALLOW_LIST=False`

   Um die Allow-Liste der angegebenen Prüfungen bei der Ausführung der stillen Installation zu aktivieren, legen Sie fest *ACC_ALLOW_LIST*Parameter bis **Wahr** .

4. Um mit der automatische Installation mehrere MID Servers zu konfigurieren, führen Sie die Befehlszeile im Abschnitt **Silent installation** (Automatische Installation) des Verfahrens wie folgt mit kommagetrennten Werten aus:
   `msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value> ACC_MID="wss://<mid1_ip>:<websocket1_port>/ws/events,wss://<mid2_ip>:<websocket2_port>/ws/events"`

   Fügen Sie die folgenden Parameterwerte in den Befehl ein:

Befehlsparameter

Parameter	Typ	Wert
ACC_API_KEY	Zeichenfolge	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird
ACC_MID	Zeichenfolge	URL des MID-Server-Websocket
ACC_ALLOW_LIST	Boolean	Gibt an, ob die Allow-Liste aktiviert (wahr) oder deaktiviert (falsch) ist. Standard = Wahr
START_SERVICE	Boolean	Gibt an, ob der Service Desk-Mitarbeiter bei der Installation automatisch startet (wahr) oder manuell gestartet werden muss (falsch). Standard = Wahr
LOCALUSERNAME	Zeichenfolge	Account, auf dem ausgeführt wird Agent Client Collector Als Windows Service. Mögliche Werte: ○ SYSTEM ○ LOCALSERVICE ○ DOMÄNE\GMSA$ ○ Zeichenfolge (lokaler Anwendername) Standard = servicenow Bei Verwendung der Konten „SYSTEM“,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Typ	Wert
		„LOCALSERVICE“ oder „DOMÄNE\GMSA$“: ○ Sie müssen kein Passwort konfigurieren. ○ Sie müssen den entsprechenden MSI-Befehl ausführen, wie in beschrieben Account-Befehle für LocalService, LocalSystem und GMSA während Windows Installation.
LOCALUSERPASSWORD	Zeichenfolge	Passwort, das für den Zugriff auf den Service Desk-Mitarbeiter verwendet wird. Standard = <zufällig generiertes Passwort>
ISDOMAIN	Boolean	Weist dem einen Domänenanwenderaccount zu Windows Service. Mögliche Werte: ○ 0: DOMÄNE wird ignoriert ○ 1: DOMÄNE wird verwendet
DOMAIN	Zeichenfolge	Gibt die Anwenderdomäne an. Gilt nur für Domänenanwenderaccounts (nicht GMSA)
PASSWORD_NEVER_EXPIRES	Boolean	Gibt an, ob das Anwenderpasswort abläuft (falsch) oder nie abläuft (wahr). Standard = falsch

Die konfigurierten MID-Server-Werte werden automatisch der Datei acc.yml hinzugefügt. Der Agent stellt eine Verbindung zum ersten verfügbaren MID-Server in der Liste her.

Um einen sekundären MID Server zu konfigurieren, geben Sie im Abschnitt backend-url der Datei acc.yml die folgende Syntax gemäß .yml-Standard ein: - "wss://<MID IP>:<Web socket port>/ws/events" (mit Anführungszeichen).

Für <MID IP> Wert, können Sie entweder den MID-FQDN oder CNAME zuweisen. Um hohe Verfügbarkeit zu aktivieren, verwenden Sie entweder den Algorithmus für die automatische MID-Auswahl, oder verwalten Sie eine virtuelle IP mit einem Lastenausgleichsmodul. Weitere Informationen finden Sie unter ITOM Agent Client Collector – Dokumentationsmaterial [KB1122613] artikel in HI Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector unter einem Windows-System mit einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem Windows-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn das Skript nicht mit der Instanz verbunden ist, müssen Sie Agent Client Collector möglicherweise manuell deinstallieren.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

Deinstallieren Sie Agent Client Collector, indem Sie den folgenden Befehl in einem Befehlsfenster ausführen. `msiexec /quiet /x <path_to_acc_msi_file>` .

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei acc.yml und das zugehörige Verzeichnis von Ihrem Computer entfernt.

Agent Client Collector-Installation unter einem macOS-Betriebssystem

Installieren Sie Agent Client Collector auf einem System, auf dem macOS verwendet wird. Sie können entweder ein einzeiliges Befehlsskript verwenden oder eine manuelle Installation durchführen, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Dient zum Aktivieren des privilegierten Zugriffs auf Informationen in macOS System, fügen Sie hinzu *_servcienow*Anwenderaccount zur Administratorgruppe (oder gleichwertig).

Die Einbindung von Agent Client Collector in ein benutzerdefiniertes Basis-Image zur Massenbereitstellung wird unter macOS nicht unterstützt.

Einzeilige Agent Client Collector-Installation unter macOS durchführen

Verwenden Sie ein effizientes einzeiliges Befehlsskript, um Agent Client Collector auf einem Computer mit macOS-Betriebssystem zu installieren. Nehmen Sie eine manuelle Installation vor, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Stellen Sie sicher, dass Sie die *pkgutil*-Pakete zur Verfügung haben, die vom Installationsskript verwendet werden.
- Stellen Sie sicher, dass die Ziel-Agents über Folgendes verfügen:
  - ServiceNow-Installationsserver [install.service-now.com]
  - ServiceNow instance
  - MID-Server, mit dem der Agent eine Verbindung herstellt

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Rufen Sie die Websocket-URL-Parameter des MID-Server ab.
   a. Navigieren zu **Agent Client Collector** > **Websocket-Endpunkt**an.
   b. Wählen Sie den relevanten Websocket-Endpunkt aus.
   c. Kopieren Sie den Wert des Felds **Endpunkt-URL**, der im Installationsbefehl verwendet werden soll.
2. Rufen Sie den API-Schlüssel ab.
   a. Navigieren zu **Agent Client Collector** > **Bereitstellung** > **MID-Webserver API-Schlüssel**an.
   b. Kopieren Sie den **API-Schlüssel**-Wert, der im Installationsbefehl verwendet werden soll.
3. Führen Sie den folgenden Befehl auf dem Server aus, auf dem Agent Client Collector installiert wird.

```
ACC_API_KEY=<api_key> ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events bash
 -c "$(curl -L https://<instance URL>/api/sn_agent/agents/install_agent)"
```

Geben Sie die folgenden Werte in die Befehlszeile ein:

Befehlszeilenparameter

Parameter	Wert
ACC_API_KEY	Ersetzen Sie die *<api_key>*-Zeichenfolge durch den API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird. Wenn kein Wert angegeben ist, werden Sie während der Ausführung des Skripts aufgefordert, den API-Schlüsselwert einzugeben.
ACC_MID	Ersetzen Sie die *<mid_ip>*-Zeichenfolge durch die URL des MID-Server-Websockets. Wenn Sie mehrere MID Servers angeben, geben Sie die MID-Server als kommagetrennte Zeichenfolge ein.
ACC_ALLOW_LIST	(Optional) Fügen Sie die Zeichenfolge *ACC_ALLOW_LIST=0* hinzu, um die Allow-Liste zu deaktivieren. Die Allow-Liste ist standardmäßig aktiviert. **Hinweis:** Wenn die Allow-Liste deaktiviert ist, beeinträchtigt dies die Sicherheit Ihres Systems und es wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Nach der Aktualisierung aktivieren Sie die Allow-Liste erneut, indem Sie *ACC_ALLOW_LIST=0* aus der einzeiligen Befehlszeichenfolge entfernen.
ACC_VALIDATE_SIG	(Optional) Fügen Sie die Zeichenfolge *ACC_VALIDATE_SIG=0* hinzu, um die Überprüfung der Validierung des Installationszertifikats zu deaktivieren. Die Validierung ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
	Standard: Validierung ist aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Agent Client Collector manuell unter macOS installieren

Installieren Sie Agent Client Collector manuell auf einem Computer, auf dem macOS verwendet wird, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Navigieren zu **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads** Und laden Sie die signierte herunter .Paket Relevant für Ihr Betriebssystem.
- Speichern Sie das .pkg-Installationspaket auf einem Ihrer installierten Agents.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Laden Sie die Installationsdateien auf Ihren lokalen Computer herunter.

```
curl -L <download link from the Agent Downloads page on the instance>
```

2. Validieren Sie die Signatur der Installationsdatei.

```
pkgutil --check-signature agent-client-collector-<version number>-macos-catalina_x64.pkg
```

Hinweis: Stellen Sie sicher, dass die .pkg-Zertifikatkette über das Installationszertifikat der ServiceNow-Entwickler-ID verfügt.

3. Installieren Sie das Agent Client Collector-Paket.

```
sudo installer -pkg agent-client-collector-<version number>-macos-catalina_x64.pkg
 -target /
```

4. Kopieren Sie die Installationsdateien.

   a. Beispiel-Konfigurationsdatei:
   sudo cp -p /Library/Application\ Support/servicenow/agent-client-collector/
   acc.yml.example /Library/Application\ Support/servicenow/agent-client-collector/acc.yml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Beispiel für eine Allow-Listen-Datei:
sudo cp -p /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json.default /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json

5. **Wahlweise:** Um neue Prüfdefinitionen für die Allow-Liste zu erstellen, deaktivieren Sie zuerst die Allow-Liste, indem Sie den *allow-list*-Parameter in der Datei acc.yml auskommentieren.

   (Optional) sudo -H -u _servicenow vi /Library/Application\ Support/servicenow/agent-client-collector/acc.yml

   Hinweis: Diese Aktion beeinträchtigt die Sicherheit Ihres Systems und wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Sobald das Update abgeschlossen ist, aktivieren Sie die Allow-Liste wieder, indem Sie den Kommentar des Allow-Listen-Parameters in der Konfigurationsdatei entfernen.

   Weitere Informationen zum Hinzufügen benutzerdefinierter Prüfungen zu einer Allow-Liste finden Sie unter Agent Client Collector-Zulassungsliste generieren.

6. Speichern Sie die Konfigurationsdatei.
7. Verbinden Sie in der Konfigurationsdatei den Agent mit dem MID-Server.

   a. Legen Sie die MID-Server-Verbindung fest.

   ```
   "wss://<MID Server IP>:<Web Socket Port>/ws/events"
   ```

   Der Websocket-Port wurde auf dem MID-Server konfiguriert, als er als Agent Client Collector-Listener festgelegt wurde.

   b. Suchen Sie den *api-key*-Parameter und geben Sie den API-Schlüsselwert in doppelten Anführungszeichen wie folgt an:
   api-key:"111111111"
   Der angegebene API-Schlüssel wird bei der ersten Ausführung des Agent verschlüsselt.

8. Um sicherzustellen, dass die Konfigurationsdatei auf einen gültigen Endpunkt verweist, führen Sie die folgenden Befehle aus, um neu zu starten Agent Client Collector:

   ```
   sudo launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist
   sudo launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist
   ```

   Hinweis: Standardmäßig führt das Beenden des Installationsprogramms dazu, dass das Programm sofort neu gestartet wird. Damit das Programm nach dem Beenden im angehaltenen Zustand bleibt, legen Sie die Keep Alive-Eigenschaft in der Datei /Library/LaunchDaemons/com.sn.acc.plist auf **false** fest.

Upgrade Agent Client Collector Manuell auf einem macOS System

Führen Sie ein manuelles Upgrade Ihres vorhandenen durch Agent Client Collector Version auf einem System, auf dem ein ausgeführt wird macOS. Ein manuelles Upgrade ist nützlich, wenn das einzeilige Befehlsskript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Das Upgrade-Verfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. **Wahlweise:** Sichern Sie manuell Agent-ID Und acc.yml Konfigurationsdateien durch Ausführen der folgenden Befehle.

```
mkdir -p /tmp/acc-upgrade-backup

cp -rp /Library/Application\
 Support/servicenow/agent-client-collector/acc.yml /tmp/acc-upgrade-backup

cp -rp /Library/Application\
 Support/servicenow/agent-client-collector/check-allow-list.json /tmp/acc-upgrade-backup

cp -rp /Library/Application\
 Support/servicenow/agent-client-collector/agent_now_id /tmp/acc-upgrade-backup
```

   Das manuelle Sichern der Konfigurationsdateien bietet eine zusätzliche Sicherheitsebene, indem sichergestellt wird, dass Ihre Dateien vor Beginn des Upgradeprozesses gesichert werden.

2. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads**an.
3. In **MacOS-Downloads** Laden Sie das entsprechende Agent-Paket und die Signatur herunter .Paket Dateien.
4. Führen Sie ein Paket-Upgrade basierend auf der cpu Ihres durch macOS Wird mit ausgeführt.
   - Intel cpu:

     ```
     sudo installer -pkg agent-client-collector-<version number>-macos_x64.pkg
     ```

   - Apple Silikon-cpu:

     ```
     sudo installer -pkg agent-client-collector-<version number>-macos_arm64.pkg
     ```

   Dieser Befehl sichert auch die Agent-ID und die Konfigurationsdateien vor dem Upgrade und stellt sie wieder her.

5. Überprüfen Sie, ob das Upgrade erfolgreich war.

   a. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.

   b. Überprüfen Sie die folgenden Werte für Ihren Service Desk-Mitarbeiter:

   - **Hostdatensammlung** = Erfasst
   - **Version** = <relevante Versionsnummer>

Agent Client Collector unter macOS mit einem einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem macOS-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn der Agent mit der Instanz verbunden ist, deinstallieren Sie Agent Client Collector manuell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Das Deinstallationsverfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

Führen Sie den folgenden Befehl aus.

```
bash -c "$(curl -L https://<Instance URL>/api/sn_agent/agents/install_agent)" -s "--remove"
```

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei acc.yml und das zugehörige Verzeichnis von Ihrem Computer entfernt. Der Benutzer und die Gruppe **_servicenow**, die als Teil des Installationsprozesses erstellt wurden, werden ebenfalls entfernt.

Agent Client Collector auf einem macOS-Computer manuell deinstallieren

Deinstallieren Sie Agent Client Collector unter macOS manuell, anstatt das Verfahren mit einzeiligem Befehl zu verwenden, wenn der betreffende Agent nicht mit der Instanz verbunden ist.

Vorbereitungen

- Das Upgrade-Verfahren ist für beide gleich MID-Server Und Bereitstellungen ohne MID.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Deaktivieren und beenden Sie den Dienst in einem Befehlsfenster:
   `sudo launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist`
2. Löschen Sie die folgenden Dateien/Verzeichnisse:

```
sudo rm /Library/LaunchDaemons/com.sn.acc.plist
sudo rm -rf /opt/servicenow/agent-client-collector
sudo rm -rf /var/run/servicenow/agent-client-collector
sudo rm -rf /Library/Application\ Support/servicenow/agent-client-collector
```

3. Entfernen Sie den **_servicenow**-Benutzer und die Gruppe.

```
sudo /usr/bin/dscl . -delete /Users/_servicenow
sudo /usr/bin/dscl . -delete /Groups/_servicenow
```

4. Entfernen Sie **Paket** Aus der Liste der installierten Pakete.

```
sudo pkgutil --forget com.servicenow.agent-client-collector
```

Optimieren Sie die Verteilung von Service Desk-Mitarbeitern an MID Servers

Optimieren Sie die Verteilung von Agents, indem Sie die Weitergabe von einem MID-Server zum anderen zulassen. Agents werden immer mit dem MID-Server mit der schnellsten Antwortzeit verbunden.

Vorbereitungen

Stellen Sie sicher, dass die folgenden Einstellungen konfiguriert sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Systemeigenschaft *sn_agent.enable_auto_mid_selection* ist auf „True“ festgelegt. Bei Verwendung der Datei acc.yml heißt die Eigenschaft *enable_auto_mid_selection*.
- Auf der MID-Server-Seite (**Agent Client Collector** > **MID-Server**):
  - Status: In Betrieb
  - Validiert: Ja

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Nur validiert MID Servers Kann Verbindungen von Service Desk-Mitarbeitern akzeptieren.

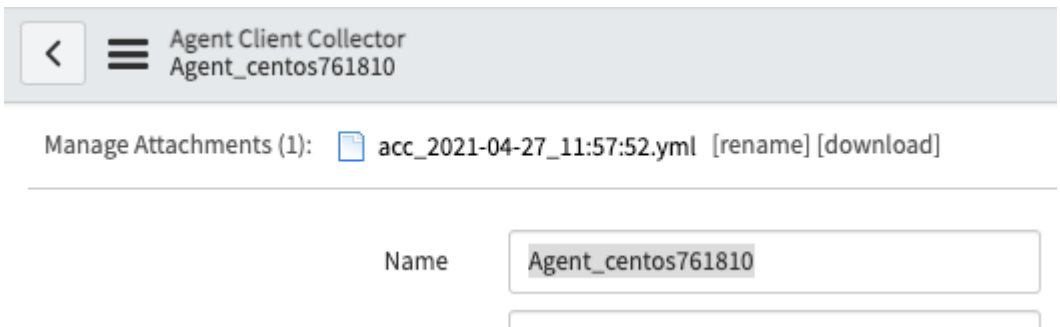
Prozedur
1. Navigieren zu **Agent Client Collector** > **Bereitstellung** > **MID-Server**an.
2. Aktivieren Sie auf der Seite **MID Server [Ansicht „Agent Client Collector“]** das Kontrollkästchen neben dem MID-Server, über den Sie Agents neu verteilen möchten.
3. Wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option **Try redistributing connected agents** (Neuverteilung verbundener Agents versuchen) aus.
   Beachten Sie die Anzahl der Service Desk-Mitarbeiter, die Ihrem zugewiesen sind MID Servers.
4. Aktualisieren Sie die Seite, um die Ergebnisse des Neuverteilungsversuchs anzuzeigen.
   Die Werte in der Spalte **Anzahl der Agents** für alle betroffenen MID-Server ändern sich, wenn Agents neu verteilt wurden.

Agent Client Collector-Konfigurationsdateien für Agents anzeigen

Zeigen Sie die acc.yml Agent Client Collector-Konfigurationsdatei an, ohne auf den Hostserver zugreifen zu müssen, indem Sie die Datei von einem Agent abrufen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie auf der Seite „Agent Client Collector“ einen Agent aus.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Grab agent config (acc.yml)** (Agent-Konfiguration abrufen (acc.yml)).
   Auf der Seite wird eine Meldung angezeigt, die angibt, dass die Datei angehängt wird.
4. Warten Sie einige Sekunden, und aktualisieren Sie die Seite.
   Die acc.yml-Konfigurationsdatei wird als Anhang auf dem Agent angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurationsdateioptionen

Erstellen Sie einen Agent Client Collector Konfigurationsdatendatei

Erstellen Sie einen Agent Client Collector Konfigurationsdatendatei und ordnen Sie sie Prüfungsdefinitionen zu, damit Sie die Informationen zu Ihrer Instanz anzeigen können. Sie können den Konfigurationsdatendateien, die von Prüfungsdefinitionen während Prüfungsausführungen verwendet werden, auch einen Anhang hinzufügen oder löschen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Eine Prüfungsdefinition ist ein einzelner Scheckeintrag im System. Details finden Sie unter Agent Client Collector Konfigurationsdatendateien.

Anhänge der Konfigurationsdatendatei enthalten Instanzdaten, z. B. Konfigurationselementinformationen (Configuration Item, CI), die bei der Ausführung einer Prüfung verwendet werden.

Domänentrennung wird in unterstützt Agent Client Collector Konfigurationsdatendateien.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Konfigurationsdateien**an.
2. Wählen Sie **Neu**.
3. Fügen Sie einen Anhang hinzu, oder entfernen Sie ihn.

Aktion	Beschreibung
Fügen Sie eine Datei hinzu	Synchronisieren Sie den Datensatz und das relevante MID Servers. **a.** Wählen Sie das Büroklammer-Symbol aus . Das Dialogfeld Anhänge wird geöffnet. **b.** Wählen Sie Aus **Wählen Sie die Datei aus** Und wählen Sie eine Datei zum Anhängen aus. **c.** Schließen Sie das Dialogfeld Anhänge.
Löschen Sie eine Datei	Löschen Sie optional einen Anhang, der dem Datensatz nicht zugeordnet werden soll. **a.** Wählen Sie Aus **Verwalten Sie Anhänge** . Das Dialogfeld Anhänge wird geöffnet. **b.** Aktivieren Sie das Kontrollkästchen neben dem Anhang, den Sie entfernen möchten. **c.** Wählen Sie **Entfernen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Anhangname muss für jede Domäne eindeutig sein und darf nur aus alphanumerischen Zeichen bestehen.

Wenn der Anhang ungültige Zeichen enthält oder ein Duplikat eines anderen Anhangs ist, treten die folgenden Situationen auf:

- Die Konfigurationsdatei wird automatisch auf festgelegt **Aktiv = Falsch** .
- In der Spalte Fehler wird eine Meldung angezeigt, die ein Problem mit dem Anhang anzeigt.

Jeder Datensatz kann nur einen Anhang enthalten.

4. **Wahlweise:** In **Beschreibung** Geben Sie eine Beschreibung für die Konfigurationsdatendatei ein.
5. Wählen Sie **Absenden**.

Ergebnis

- Die Konfigurationsdatendatei wird auf der Seite „Agent Client Collector-Konfigurationsdatei“ aufgeführt.
- Die **Name** Wert wird automatisch auf den Namen des Anhangs festgelegt.

Prüfungen verwenden die Konfigurationsdatendatei mit Instanzdaten während der Ausführung der Prüfung.

Manuell aktualisieren Agent Client Collector Zertifikate

Rufen Sie selbst signierte Zertifikate aus dem ab ServiceNow Installieren Sie den Server, anstatt auf den geplanten zu warten MID-Server Synchronisierung.

Vorbereitungen

- Stellen Sie sicher, dass das selbstsignierte Zertifikat in einem platziert ist .Zip Datei in MID-Server An folgendem Standort: Agent\static\cert
- Stellen Sie sicher, dass die Zertifizierungsstelle Teil des Truststores des Agent-Hosts ist, da die Zertifikatkette vor der Signatur des Kunden-Plugins validiert wird.
- Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die MID-Server Sucht einmal täglich oder nach dem Neustart auf Updates.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**an.
2. Wählen Sie einen MID-Server.
3. Wählen Sie im Abschnitt zugehörige Links die Option aus **Löst die ACC-Zertifikatsynchronisierung aus** .
4. Starten Sie neu MID-Server.

Ergebnis

Wenn ein Service Desk-Mitarbeiter eine Zertifikatprüfung nicht durchführt, synchronisiert der Service Desk-Mitarbeiter die im verfügbaren Zertifikate MID-Server. Die Synchronisierung wird für Zertifikate auf der durchgeführt ServiceNow Installieren Sie den Server und die selbstsignierten Zertifikate, die in platziert werden .Zip Datei in MID-Server S

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent\static\cert Ordner. Zertifikate werden von heruntergeladen Agent Client Collector Wenn der Service Desk-Mitarbeiter die zugeordneten Plugin-Assets einer Prüfungsdefinition nicht validieren kann.

Aktivieren Sie die sichere OpenSSL-Signatur für Plugins

Erstellen Sie ein selbstsigniertes Zertifikat für ein Agent Client Collector-Plugin. Das folgende Verfahren zeigt ein Beispiel für die Erstellung eines x509-Zertifikats mit OpenSSL. Informationen zu anderen Zertifikatstypen können Sie der OpenSSL-Dokumentation entnehmen.

Vorbereitungen

- Vergewissern Sie sich zum Prüfen der Signatur des Plugin, dass die Eigenschaft *`verify-plugin-signature`* in der Datei acc.yml des Agent auf **True** festgelegt ist.
- Stellen Sie Sicher **OpenSSL** Ist auf Ihrem System installiert.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Aktivieren eines sicheren OpenSSL-Signaturmechanismus für Plugins funktioniert mit einem Agent Client Collector Installiert auf einem Linux System.

Prozedur

1. Erstellen Sie eine Plugin-Datei mit der Erweiterung tar.gz.
   Weitere Informationen finden Sie unter Erstellen und bearbeiten Agent Client Collector Plugins.
2. Generieren Sie Ihr eigenes sicheres Selbstzertifikat für die Plugin-Datei.

   a. Erstellen Sie ein x509-Zertifikat.

   ```
   openssl req -nodes -x509 -sha256 -newkey rsa:2048 -keyout "sign.key" -out "sign.crt"
    -days 365 -subj

    "/C=<CountryName>/ST=<StateOrProvinceName>/L=<Locality>/O=<Organization>/O
   U=<OrganizationalUnit>/CN=sign"
   ```

   b. Signieren Sie die Plugin-Datei.

   ```
   openssl dgst -sha256 -sign "sign.key" -out sign.txt.sha256 <plugin-name>.tar.gz
   ```

   Alternativ können Sie Plugins mit einer Zertifizierungsstelle signieren. Weisen Sie dabei das PEM-Format des Zertifikats zu, und platzieren Sie es im Verzeichnis cert des Agent.

   c. Vergewissern Sie sich, dass die Signatur richtig konfiguriert ist.

   ```
   openssl dgst -sha256 -verify  <(openssl x509 -in "sign.crt" -pubkey -noout) -signature
    sign.txt.sha256 <plugin-name>.tar.gz
   ```

   Wenn die Datei gültig ist, lautet die Ausgabe Verified OK.

   d. Codieren Sie das Zertifikat der Signatur mit base64-Codierung.

   ```
   base64 sign.txt.sha256 > sign.txt.sha256_encode64.sig
   ```

   Eine sign.txt.sha256_encode64.sig-Datei wird erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Befehle aus, um ein neues Verzeichnis zu erstellen und einzufügen tar.gz Und Sign.txt.sha256_encode64.sig Dateien.
   a. Mkdir Signed-Plugin
   b. mv <plugin-name>.tar.gz Signed-Plugin
   c. mv Sign.txt.sha256_encode64.sig signed-Plugin
   d. cd signiert – Plugin
4. Erstellen Sie eine weitere tar.gz Datei, indem Sie dieselben Befehle ausführen, die Sie für den ersten ausgeführt haben tar.gz Datei.
   a. Teer -C . -Zcvf ../<plugin-name>.tar.gz *
   b. cd..

   Hinweis: Speichern Sie die neue Datei unter ../<plugin-name>.tar.gz Um Benennungskollisionen mit dem Original zu vermeiden <plugin-name>.tar.gz Datei, die im aktuellen Verzeichnis vorhanden ist.
5. Laden Sie die neue tar.gz-Plugin-Datei in die Instanz hoch.
6. Legen Sie die Plugin-Datei als fest *`active=true`*.
7. Platzieren Sie Signieren.crt Datei in der des Service Desk-Mitarbeiters zertifikat Verzeichnis, das sich in befindet Konfiguration Ordner.
8. In acc.yml Datei, festlegen Plugin-Signatur verifizieren Bis **Wahr** .

Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzu

Fügen Sie dem Truststore Ihres Betriebssystems (OS) ein selbstsigniertes Zertifikat hinzu. Durch Hinzufügen eines Zertifikats zum Truststore können Sie überprüfen, ob das Zertifikat authentisch ist und Ihre Verbindungen sicher sind.

Warum und wann dieser Vorgang ausgeführt wird

Das Verfahren zum Hinzufügen eines Zertifikats zu einem Truststore hängt vom Betriebssystem des Hosts ab.

Durch das Hinzufügen eines selbstsignierten Zertifikats zum Truststore wird das Betriebssystem angewiesen, dem Zertifikat beim Herstellen sicherer Verbindungen zu vertrauen. Auf diese Weise können die Anwendungen sicher mit Services kommunizieren, die das selbstsignierte Zertifikat verwenden. Wenn Sie ein Zertifikat hinzufügen, das nicht vertrauenswürdig ist, können Sie die Sicherheit Ihres Systems gefährden.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Auf einem Windows BETRIEBSSYSTEM:
   a. Drücken Sie Windows Schaltfläche + R Auf Ihrer Tastatur.
      Die **Ausführen** Feld wird geöffnet.
   b. Geben Sie die Zeichenfolge ein Certmgr.msc Und drücken Sie **Geben Sie Ein** .
      Der Zertifikatmanager wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Erweitern Sie das Verzeichnis vertrauenswürdige Stammzertifizierungsstellen.

d. Auswählen und halten (oder mit der rechten Maustaste klicken) **Zertifikate** .

e. Auswahlvorgang **Alle Aufgaben** > **Importieren**an.
Der Zertifikatimport-Assistent wird geöffnet.

f. Führen Sie die Schritte im Assistenten für Zertifikatimport aus.
Details finden Sie unter Importieren Sie ein selbstsigniertes Zertifikat.

Alternativ können Sie eine hinzufügen Windows Zertifizieren Sie mit PowerShell, indem Sie als Administrator den folgenden Befehl ausführen:

```
Import-Certificate -FilePath <path to your certificate file> -CertStoreLocation
 Cert:\LocalMachine\Root
```

2. Auf einem macOS:

a. Importieren Sie das Zertifikat in einen Schlüsselbund, indem Sie den folgenden Befehl in einem Terminalfenster ausführen:

```
bash

code:
sudo security add-trusted-cert -d -r trustRoot -k "/Library/Keychains/System.keychain"
 <path to your certificate file>
```

b. Geben Sie das Administratorpasswort ein, wenn Sie dazu aufgefordert werden.

c. Öffnen Sie die Anwendung Keychain Access, um sicherzustellen, dass das Zertifikat hinzugefügt wurde.
Ein erfolgreich hinzugefügtes Zertifikat wird als bezeichnet: **Dieses Zertifikat ist als vertrauenswürdige for...plugin-Verifizierung markiert.**

3. Auf einem Linux BETRIEBSSYSTEM:

a. Bereiten Sie die selbstsignierte Zertifikatdatei als PEM-Datei (Privacy Enhanced Mail) vor.

b. Kopieren Sie das Zertifikat in das Verzeichnis der Zertifizierungsstelle (Certificate Authority, CA), das das Verzeichnis ist, in dem die Zertifikate gespeichert werden.

- Führen Sie auf einem Debian/Ubuntu-basierten System den folgenden Befehl aus:

```
sudo cp <path to certificate file> /etc/pki/ca-trust/source/anchors/do
```

- Auf einem Red Hat/Fedora-basiertes System: Führen Sie den folgenden Befehl aus:

```
sudo cp <path to certificate file> /etc/pki/ca-trust/source/anchors
```

c. Aktualisieren Sie die CA-Zertifikate:

- Führen Sie auf einem Debian/Ubuntu-basierten System den folgenden Befehl aus:

```
update-ca-certificates
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Befehl liest das Zertifikatpaket im /Usr/local/share/CA-Certificates Verzeichnis, aktualisiert das Zertifikatpaket und speichert es in /Ext/ssl/certs/CA-certificate.crt .

- Auf einem Red Hat/Fedora-basiertes System: Führen Sie den folgenden Befehl aus:

```
sudo update-ca-trust extract
```

Ergebnis
Ihr selbstsigniertes Zertifikat befindet sich auf dem Betriebssystem, mit dem Sie arbeiten.

Importieren Sie ein selbstsigniertes Zertifikat

Importieren Sie ein selbstsigniertes Zertifikat in ein Windows System mithilfe des Zertifikatimport-Assistenten. Der Zertifikatimport-Assistent ist erforderlich, um den selbst signierten Zertifikatimport-Prozess für einen abzuschließen Windows Betriebssystem (OS).

Vorbereitungen
Stellen Sie sicher, dass Sie das Verfahren zum Importieren eines selbst signierten Zertifikats in ein befolgt haben Windows System, wie in beschrieben Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzu.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Wählen Sie auf der ersten Seite des Assistenten aus **Als Nächstes** .
   Der Truststore befindet sich normalerweise im Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen des Zertifikatmanagers.
2. Navigieren Sie zu dem Speicherort, an dem sich die selbstsignierte Zertifikatdatei befindet.
   Die Datei befindet sich normalerweise im Service Desk-Mitarbeiter Konfiguration/Zertifikat Verzeichnis.
3. Wählen Sie die Zertifikatdatei aus, halten Sie sie gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie sie aus **Installieren Sie das Zertifikat** .
4. Wählen Sie **Weiter**.
5. Wählen Sie die Option aus, um das Zertifikat im Truststore Trusted Root Certification Authority (Vertrauenswürdige Stammzertifizierungsstellen) zu platzieren.
6. Wählen Sie Aus **Als Nächstes** Und **Beenden** Um den Assistenten abzuschließen.

Ergebnis
Das Zertifikat wird in den Truststore importiert.

Nächste Maßnahme
Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie aus **Bestätigen** Zum Bestätigen des Imports.

Widerrufen Agent Client Collector Zertifikate

Beenden Sie die Kommunikation zwischen dem Service Desk-Mitarbeiter und ITOM Cloud-Services durch Entfernen von Agent Client Collector Zertifikat. Beispielsweise könnte es zu einer Sicherheitsverletzung kommen, aufgrund derer Sie die Kommunikation stoppen möchten, indem Sie das Zertifikat des Service Desk-Mitarbeiters widerrufen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie den Service Desk-Mitarbeiter aus, für den Sie das Zertifikat widerrufen möchten.
3. Wählen Sie aus **Service Desk-Mitarbeiter-Zertifikat Widerrufen** Schaltfläche.
4. Wählen Sie den Grund für den Zertifikatwiderruf aus.
   Eine Liste und eine Erklärung der verfügbaren Widerrufsgründe finden Sie unter Agent Client Collector Gründe für Zertifikatwiderruf.
5. Wählen Sie **OK**.
   Das Zertifikat des Service Desk-Mitarbeiters wird widerrufen, und die ITOM Die Zertifikatwiderrufliste (Certificate Revocation List, CRL) der Cloud-Services-Ebene wurde aktualisiert.

Ergebnis

Kommunikation zwischen Service Desk-Mitarbeiter und ITOM Cloud-Services werden angehalten.

Zugehörige Informationen

Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzu

Agent-Zertifikatrotation

Die Agent Client Collector Das Zertifikat ist zwei Jahre gültig und muss vor Ablauf rotiert werden, um Probleme mit der Agent-Konnektivität zu vermeiden. Wenn der Ablauf bevorsteht, initiiert der Service Desk-Mitarbeiter eine Zertifikatrotationsanforderung.

Wenn Agent Client Collector Der Zertifikatablauf von rückt näher. Systemeigenschaften überprüfen, ob ein gültiges Zertifikat vorhanden ist, wenn das vorhandene Zertifikat abläuft.

- *certificate-rotation-days-out*: Gibt An Die Anzahl der Tage vor Ablauf des Zertifikats, die ein Service Desk-Mitarbeiter versucht, sein Zertifikat zu rotieren. In konfiguriert acc.yml Konfigurationsdatei. Standard = 28.
- *sn_agent.certificate_rotation_days_out*: Gibt die Anzahl der Tage vor Ablauf des Zertifikats an, die das System eine Zertifikatrotationsanforderung für einen bestimmten Service Desk-Mitarbeiter akzeptiert. Konfiguriert auf der Seite „Systemeigenschaften“ (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an. Standard = 28.

Zugehörige Informationen

Agent Client Collector-Konfigurationsdateien für Agents anzeigen

Konfigurationsdateioptionen

Durchführen Zscaler Korrektur

Wenn die auf dem Windows- oder macOS-Agent installierte Zscaler-Anwendung nicht ordnungsgemäß ausgeführt wird, können Sie die App anhalten und neu starten. Dieser Prozess wird als *remediation* (Fehlerkorrektur) bezeichnet. Durch Ausführung der Fehlerkorrektur wird automatisch ein Incident auf dem Agent erstellt. Die Zscaler-Status können Sie auch im Zscaler-Dashboard als Diagramm anzeigen.

Standardmäßig wird die Überwachungsprüfung gemäß **Zscaler-Überwachungsrichtlinie** alle 30 Minuten ausgeführt, um den Status der Zscaler-App zu überprüfen, die auf dem Agent ausgeführt wird. Die Zscaler-Überwachungsrichtlinie beinhaltet die folgenden Prüfungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *zscaler-monitoring-check*: Überprüft den Status der auf dem Agent ausgeführten Zscaler-App.
- *zscaler-remediation-check*: Wird nur aufgerufen, wenn die Zscaler-App nicht effizient ausgeführt wird. Diese Prüfung fährt die App herunter, startet sie neu und erstellt automatisch einen Incident.

  Für eine Zscaler-App, bei der die Fehlerkorrektur nicht ordnungsgemäß verläuft, wird alle 24 Stunden nur ein Incident erstellt. Wenn die Fehlerkorrekturprüfung beispielsweise mehrmals auf einem Agent ausgeführt wird, werden neue Fehlerkorrektureinträge erstellt, die bis nach Ablauf von 24 Stunden demselben Incident zugeordnet werden. Anschließend wird ein zweiter Incident erstellt. Wenn die App Zscaler erfolgreich neu gestartet wird, wird der Incident geschlossen.

  Ausgabe der Zscaler-Fehlerkorrektur:

  - Pro Fehlerkorrektur erzeugte Datenmenge: 2 KB
  - Maximale Anzahl von Fehlerkorrekturen, die an einem Tag ausgeführt werden können: 48 (eine alle 30 Minuten)
  - Maximale Datenmenge, die von einem einzelnen Agent pro Tag erzeugt wird: 96 KB
  - Maximale Datenmenge, die von 20.000 Service Desk-Mitarbeitern pro Tag erzeugt wird: 1.92 GB

Überprüfen ZscalerÜberwachung

Überprüfen Sie den Überwachungsstatus von Zscaler App, um sicherzustellen, dass sie ordnungsgemäß ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Überwachungs-App inaktiv ist, lautet der Zscaler-Tunnelstatus entweder *51(SERVICE-DOWN-ERROR)* oder *56(SYSTEM_SOCKETS_EXHAUSTED_ERROR)*. In diesem Fall wird eine Fehlerkorrekturprüfung ausgeführt, bei der die Zscaler-App heruntergefahren und neu gestartet wird.

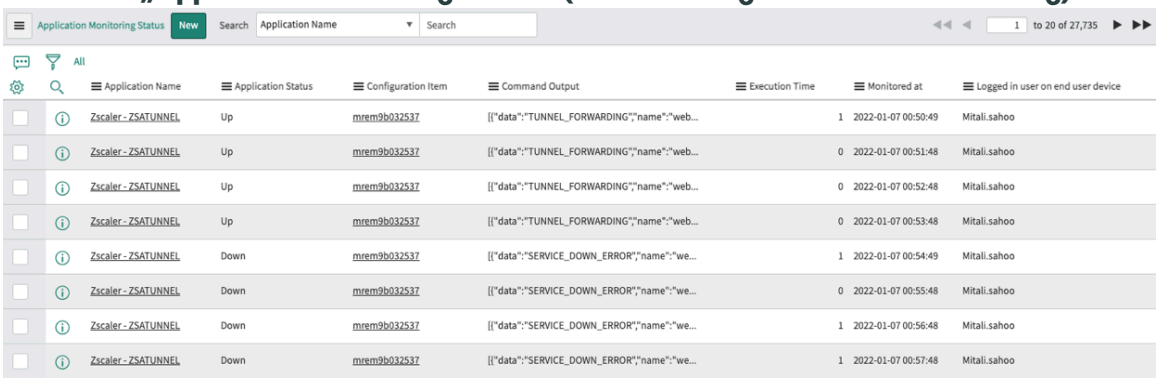
Standardmäßig findet die Zscaler-Überwachungsprüfung (*zscaler-monitoring-check*) automatisch alle 30 Minuten statt. Wenn bei der App Zscaler Probleme auftreten, sollten Sie die Prüfung häufiger oder sofort ausführen. Details finden Sie unter Zscaler-Überwachungsprüfung anpassen.

Prozedur

1. Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Überwachungsstatus**an.
   Die Seite **Application Monitoring Status** (Überwachungsstatus der Anwendung) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Application Monitoring Status“ (Überwachungsstatus der Anwendung)



- Wenn die App Zscaler ordnungsgemäß ausgeführt wird, wird in der Spalte **Anwendungsstatus** der Wert **In Betrieb** angezeigt.
- Wenn die App Zscaler nicht ordnungsgemäß ausgeführt wird, zeigt die Spalte **Anwendungsstatus** den Wert **Ausgeschaltet** an.

2. Wenn in der Spalte **Anwendungsstatus** der Wert **Ausgeschaltet** angezeigt wird, wird die Fehlerkorrekturprüfung (*`zscaler-remediation-check`*) ausgeführt.
   - Weitere Informationen zum Anpassen des Zeitraums, nach dem der Zscaler-Status vom System überprüft wird, finden Sie unter Wartezeit der Zscaler-Fehlerkorrektur anpassen.
   - Weitere Informationen zur Überwachung von Zscaler-Fehlerkorrekturprüfungen finden Sie unter Zscaler-Fehlerkorrektur überprüfen.

Wartezeit der Zscaler-Fehlerkorrektur anpassen

Konfigurieren Sie den Zeitraum (in Sekunden), nach dem der Zscaler-Status von der Zscaler-Fehlerkorrekturprüfung geprüft wird. Dieser Zeitraum gibt an, wie oft der Zscaler-Status vom System überprüft wird, nachdem die Fehlerkorrekturprüfung ausgeführt wurde.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Agent Client Collector** > **Service Desk-Mitarbeiter** > **Konfiguration** > **Prüfungsdefinition**an.
2. Wählen Sie *`zscaler-remediation-check`*.
3. Ändern Sie im Feld **Befehl** den Wert in: `zscaler_app_remediator.rb --wait_time=<time_in_sec>`.
   Dabei entspricht `<time_in_sec>` der Anzahl der Sekunden, die vom System vor Prüfung des Zscaler-Status gewartet wird.
   Standardmäßig beträgt die Wartezeit des Systems 30 Sekunden.
4. Wählen Sie **Speichern**.
   - Wenn die Zscaler-App innerhalb der konfigurierten `wait_time` (Wartezeit) ausgeführt wird, lautet das Fehlerkorrekturergebnis **Erfolg**.
   - Wenn die Zscaler-App nicht innerhalb der konfigurierten `wait_time` (Wartezeit) ausgeführt wird, lautet das Fehlerkorrekturergebnis **Fehlgeschlagen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zscaler-Überwachungsprüfung anpassen

Passen Sie die Häufigkeit an, mit der die Zscaler-Überwachungsprüfung ausgeführt wird. Standardmäßig wird die Zscaler-Überwachungsprüfung alle 30 Minuten ausgeführt. Wenn die App Zscaler nicht effizient funktioniert, können Sie die Prüfung so einstellen, dass sie häufiger ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Anpassen der Zscaler-Überwachungsprüfung finden Sie unter Durchführen Zscaler Korrektur.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien**an.
2. Wählen Sie den Eintrag **Zscaler Monitoring Policy** (Zscaler-Überwachungsrichtlinie) aus.
3. Wählen Sie die Registerkarte **Zeitplanung** aus.
4. Ändern Sie im Feld **Intervall (Sek.)** den Wert in die Sekundenanzahl der Wartezeit, die zwischen den Ausführungen der Überwachungsprüfung eingelegt werden soll.
   Der Standardwert lautet 1800.

   Um die Überwachungsprüfung sofort auszuführen, geben Sie den Wert **1** ein.

Ergebnis

Zscaler-Überwachungsprüfungen werden gemäß der im Feld **Intervall (Sek.)** angegebenen Häufigkeit ausgeführt.

Zscaler-Fehlerkorrektur überprüfen

Vergewissern Sie sich, dass die Zscaler-App durch die Zscaler-Fehlerkorrektur heruntergefahren und neu gestartet wird, nachdem die Überwachungsprüfung fehlgeschlagen ist.

Vorbereitungen

Überprüfen Sie, ob ZscalerÜberwachungsprüfung gibt einen zurück **Anwendungsstatus** Wert von **Ausgefallen** , Gibt an, dass Zscaler App funktioniert nicht ordnungsgemäß.

Erforderliche Rolle: agent_client_collector_admin

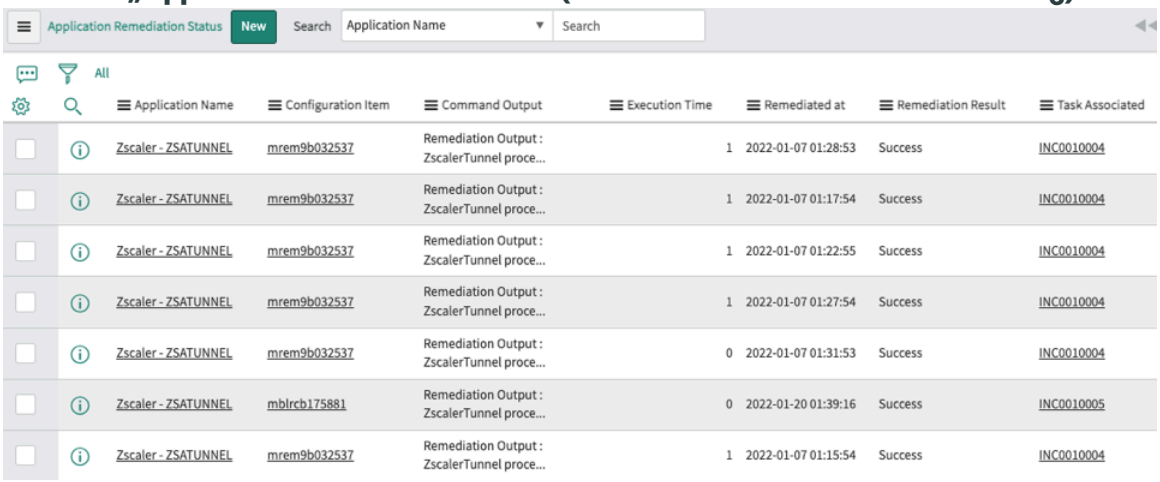
Prozedur

Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Ergebnis der Fehlerkorrektur**an.

Die Seite **Application Remediation Status** (Fehlerkorrekturstatus der Anwendung) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Application remediation status“ (Fehlerkorrekturstatus der Anwendung)



Application Name	Configuration Item	Command Output	Execution Time	Remediated at	Remediation Result	Task Associated
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:28:53	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:17:54	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:22:55	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:27:54	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	0	2022-01-07 01:31:53	Success	INC0010004
Zscaler - ZSATUNNEL	mblrcb175881	Remediation Output : ZscalerTunnel proce...	0	2022-01-20 01:39:16	Success	INC0010005
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:15:54	Success	INC0010004

Wenn die Fehlerkorrektur Zscaler erfolgreich herunterfährt und neu startet, enthält die Spalte **Remediation Result** (Ergebnis der Fehlerkorrektur) den Wert **Erfolg**. Die **Aufgabe Zugeordnet** Die Spalte zeigt einen Link zu dem bei der Korrektur erstellten Incident an. Wenn die Fehlerkorrektur erfolgreich ist, wird der Incident automatisch geschlossen.

Zscaler-Dashboard verwenden

Verwenden Sie das Zscaler-Dashboard, um die Status der Zscaler-Überwachung und -Fehlerkorrektur im Diagrammformat anzuzeigen.

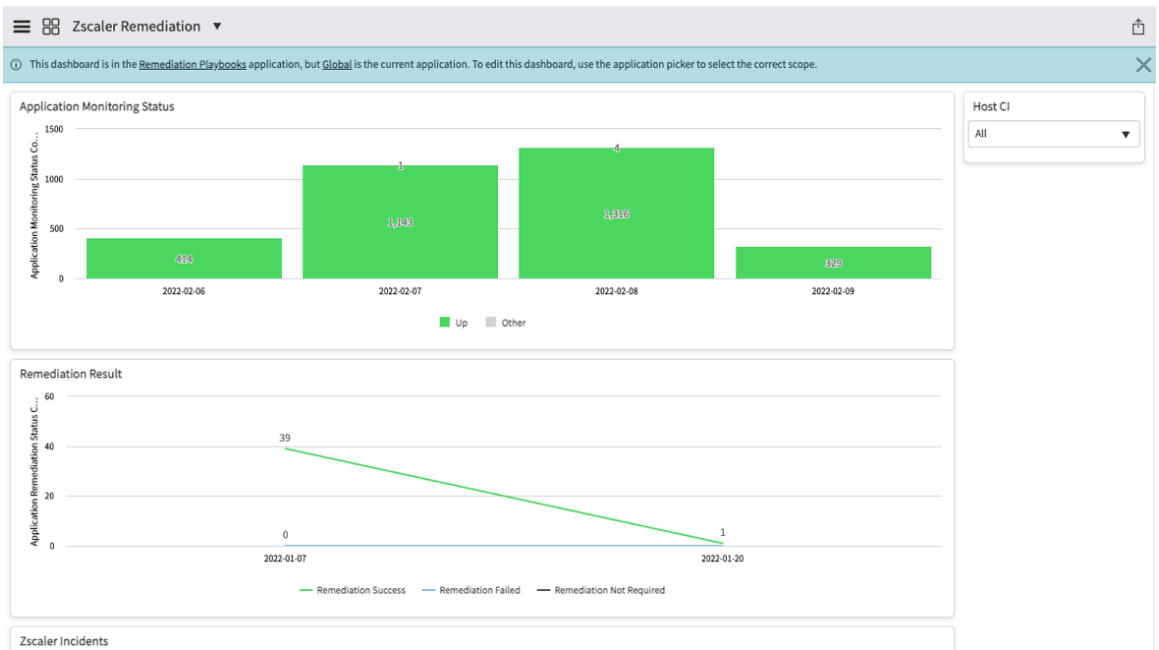
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Dashboard**an.
   Das Dasbhoard „Zscaler Remediation“ (Zscaler-Fehlerkorrektur) wird angezeigt.

Zscaler-Dashboard



Das Dashboard zeigt Diagramme an, die in die folgenden Abschnitte unterteilt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte im Dashboard „Zscaler Remediation“ (Zscaler-Fehlerkorrektur)

Abschnitt	Beschreibung
Application Monitoring Status (Überwachungsstatus der Anwendung)	Zeigt ein Balkendiagramm der Anzahl der Zscaler-Apps nach Datum und deren Status (In Betrieb, Ausgeschaltet, Unbekannt, Sonstige) an.
Remediation Result (Ergebnis der Fehlerkorrektur)	Zeigt ein Liniendiagramm der Anzahl der Zscaler-Fehlerkorrekturen und deren Status (Erfolg, Fehlgeschlagen, Nicht erforderlich) an.
Zscaler Incidents (Zscaler-Incidents)	Zeigt ein Liniendiagramm der Anzahl der erstellten Zscaler-Incidents und deren Status (Geöffnet, Geschlossen) an.

2. **Wahlweise:** Wählen Sie im Fenster **Host-CI** oben rechts auf der Seite das CI aus, dessen Daten Sie anzeigen möchten.
   Der Standardwert ist Alle. Damit wird angegeben, dass das Dashboard Daten von allen CIs auf dem Host anzeigt.

Erfassen Sie Daten von Ihren Systemgeräten

Führen Sie einen Prüfungsbefehl auf Ihrem Server oder Ihrer Datenbank aus, um Daten von diesen Geräten zu erfassen. Abhängig von der aufgerufenen Prüfung können erfasste Daten Überwachungsdaten, Sichtbarkeitsdaten, Protokolldaten oder Anwendermetriken sein.

Richtlinien

A Die Richtlinie besteht aus den Configuration Items (CIs), die von überwacht werden Agent Client Collector, Und die Prüfungen, die für diese CIs ausgeführt werden. Richtlinien definieren, welche Prüfungen ausgeführt werden sollen, wann und für welche CIs sie ausgeführt werden sollen.

Überprüfungen

Eine Richtlinie führt eine Reihe von Prüfungen aus. Jede Prüfung ist mit den folgenden Attributen definiert :

- Befehl Zur Ausführung
- Überprüfungstyp
- Zeitüberschreitung bei Befehl
- Zu verwendende Plugins (tar.gz Dateien, die sicher und automatisch in den Service Desk-Mitarbeiter heruntergeladen werden)

Bestimmt, wann Prüfungen ausgeführt werden

Richtlinienprüfungen werden basierend auf einem der ausgeführt Folgende Planungsmodelle :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Intervallbasierte Planung: Die Mindestanzahl von Sekunden zwischen jeder Prüfungsausführung. Zum Beispiel:
  - Ein Intervallwert ist mindestens einmal pro Stunde (mindestens einmal alle 3.600 Sekunden).
  - Der Service Desk-Mitarbeiter war während des geplanten Intervalls ausgefallen, als die Prüfung ausgeführt werden sollte.

  Wenn der Service Desk-Mitarbeiter wieder hochgefahren ist, führt er die Prüfung innerhalb einer Stunde aus.

  Wenn ein Prüfungsintervall weniger als eine Stunde beträgt, wird die Prüfung basierend auf der angegebenen Zeit seit der Prüfung ausgeführt S Letzte Ausführung. Beispiel: Für eine Prüfung, die alle acht Stunden ausgeführt werden soll:
  - Die Prüfung wird um 00:00 (Mitternacht) ausgeführt.
  - Die Prüfung wird erneut um 08:00 (8 UHR) ausgeführt.

  Wenn der Service Desk-Mitarbeiter jedoch um 8:00 Uhr ausgefallen ist und um 09:03 Uhr wieder einsatzbereit ist, wird die Prüfung innerhalb einer Stunde ausgeführt, also zwischen 09:03 und 10:03 Uhr. Wenn die Prüfung um 09:57 ausgeführt wird, erfolgt die nächste Ausführung um 17:57 (5:57 Uhr). In diesen Fällen wählt die Prüfung zufällig die Laufzeit aus, um sicherzustellen, dass sie alle acht Stunden ausgeführt wird.

  Ein Scheck Abgeschlossen Wird ausgeführt, wenn die Ergebnisse an gesendet werden MID-Server(In einer MID-Bereitstellung) oder ITOM Cloud-Services (ICS)-Pod (in einer Bereitstellung ohne MID).
- Cron-basierte Planung : Wird zu festen Zeiten oder Intervallen ausgeführt (z. B. jeden Tag um 18:00 Uhr oder alle zwei Stunden).

Bestimmung, wo Prüfungen ausgeführt werden

Richtlinien überwachen die Konfigurationselemente (CIs), die den Agent-Hosts zugeordnet sind. Um die spezifischen CI-Typen zu bestimmen, die überwacht werden sollen, können Sie Filter erstellen. Weitere Informationen zum Konfigurieren von Richtlinienfiltern finden Sie unter Servicefilter für eine Richtlinie erstellen.

Richtlinienzuordnungen werden aktualisiert

Wenn Aktivieren einer Richtlinie, Agent Client Collector Framework Ordnet überwachte CIs einer Richtlinie zu. Diese Richtlinienzuordnung wird alle sieben Tage nach der ersten Zuordnung wiederholt. Alle 15 Minuten (standardmäßig) Agent Client CollectorÜberwacht CMDB Für alle Änderungen, die den Filterbedingungen entsprechen, und aktualisiert die Zuordnung entsprechend. Dient zum Ändern der Häufigkeit, mit der die Zuordnung zwischen geändert werden soll CMDB Und CI aktualisiert wird, ändern Sie die Eigenschaft sn_Agent_Sync_Filters_interval_min auf der Seite „Systemeigenschaften“ (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an.

Neue Agent Client Collector-Richtlinie erstellen

Richtlinien bestehen aus den von Agent Client Collector überwachten CIs und den Prüfungen, die für diese CIs ausgeführt werden. Beim Erstellen einer Richtlinie konfigurieren Sie einen Filter, der die CIs bestimmt, für die die Prüfungen ausgeführt werden sollen. Zum Beispiel eine Richtlinie zum Ausführen von Prüfungen auf allen Apache-Webservern. Sie können neue Richtlinien erstellen oder die Standardrichtlinien bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Prüfungsdefinition einer Richtlinie zuordnen, wird eine Kopie der Definition als Prüfungsinstanz erstellt. Diese Werte werden auf der Registerkarte **Prüfungsinstanzen** unten im Formular **Richtlinie** angezeigt. Alle Änderungen, die Sie an einer Prüfungsinstanz vornehmen, wirken sich nur auf die Instanz in der Richtlinie aus. Die ursprüngliche Prüfungsdefinition bleibt unverändert. Wenn Sie die ursprüngliche Prüfungsdefinition ändern, gelten die Änderungen nicht für bereits erstellte Prüfungsinstanzen. Es wird empfohlen, eine Kopie einer Prüfungsdefinition zu erstellen, wenn Sie deren Standardparameter ändern, nachdem Sie eine oder mehrere Prüfungsdefinitionen in einer Richtlinie initiiert haben.

Einige Richtlinienprüfungen erfordern Anmeldeinformationen, andere nicht. Beispiel:

- Für Agent Client Collector sind keine Anmeldeinformationen für Prüfungen erforderlich, wenn diese auf demselben Server ausgeführt werden. Beim Zugriff auf Software, die Root-Zugriff oder Administratorzugriff erfordert (wie MySQL), sind hingegen Anmeldeinformationen erforderlich.
- Wenn Agent Client Collector als Proxy verwendet wird:
  - Anmeldeinformationen müssen aufgerufen werden, damit der Agent über SNMP oder andere Protokolle eine Verbindung zum Remote-Gerät herstellen kann.
  - Erhöhen Sie in der Datei acc.yml den im blauen Feld der Registerkarte **Proxy Settings** (Proxy-Einstellungen) angegebenen Wert *cpu_percentage_limit* des Agent.
- Wenn Agent Client Collector den HTTP-Endpunkt verwendet:
  - Wenn für die URL keine Anmeldung erforderlich ist (wie bei einer öffentlichen Website), werden keine Anmeldeinformationen benötigt.
  - Wenn für die URL eine Anmeldung erforderlich ist (wie bei einem API-Endpunkt), werden Anmeldeinformationen benötigt.

Auf der Registerkarte **Credentials** (Anmeldeinformationen) weisen Sie der Richtlinie wie folgt einen Anmeldeinformationsalias zu.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Klicken Sie auf **Neu**.
   Die Seite **Policy** (Richtlinie) wird angezeigt.
3. Geben Sie in die Felder auf der Seite die in der folgenden Tabelle beschriebenen Werte ein:

Formular „Policy Definition“ (Richtliniendefinition)

Feld	Beschreibung
Name	Beschreibender Name für die Richtlinie
Beschreibung	Beschreibung der Richtlinie
Veröffentlichungsstatus	Hartcodiert als **Draft** (Entwurf), was bedeutet, dass die Richtlinie noch nicht veröffentlicht wurde. Dieses Feld können Sie nicht bearbeiten.
Hierarchie	Hartcodiert als **Keine**. Wenn der Richtlinie eine untergeordnete Richtlinie hinzugefügt wird, ändert

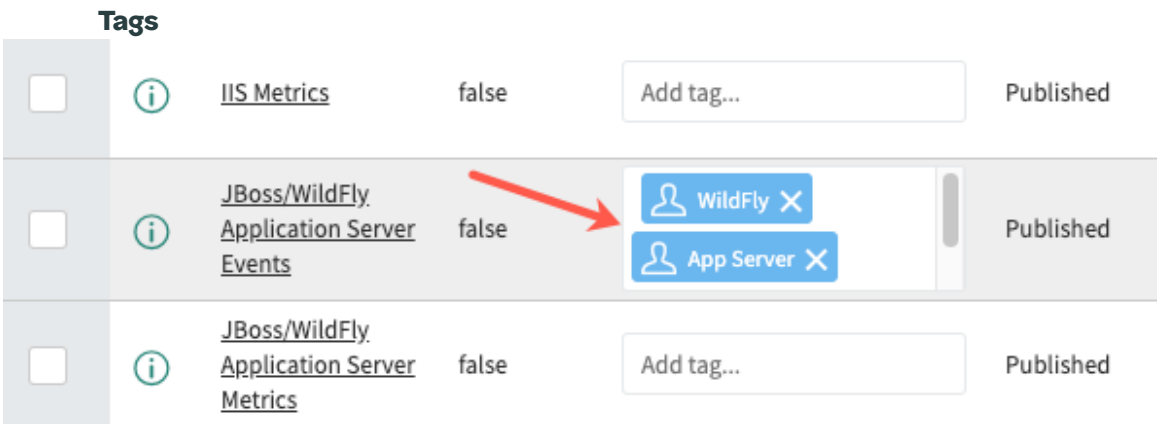
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sich der Wert in **Übergeordnet**. Untergeordnete Richtlinien haben den Wert **Untergeordnetes Element**.

4. Wählen Sie auf der Registerkarte **Monitored CIs** (Überwachte CIs) eine der folgenden Optionen aus:
   - **Manuelle Berechnung** : Wählen Sie diese Option aus, um die Richtlinie aus der geplanten Richtlinienberechnung auszuschließen, wobei alle Änderungen an den betroffenen CIs der Richtlinie ignoriert werden.

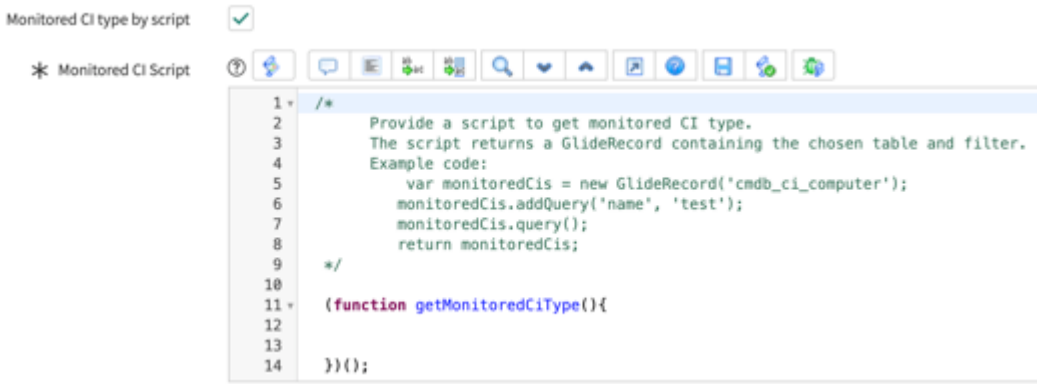
     Wählen Sie diese Option aus, wenn die Richtlinie ein einzelnes CI überwacht. Andernfalls dauert die geplante Aufgabe „Überwachungsrichtlinien aktualisieren und veröffentlichen“ ungewöhnlich lange, bis sie abgeschlossen ist.
   - **Monitored CI type by filter** (Überwachter CI-Typ durch Filter): Konfigurieren Sie die folgenden Unterfelder:
     - **Monitored CI type** (Überwachter CI-Typ): Wählen Sie den CI-Typ aus, der mithilfe der Richtlinienprüfungen überwacht werden soll.
     - **Filter**: Konfigurieren Sie einen Filter, sodass mit den Richtlinienprüfungen nur CI-Typen überwacht werden, die die angegebenen Kriterien erfüllen. In den verfügbaren Kriterien sind die **Tags** eines CI enthalten.



   - **Monitored CI type by script** (Überwachter CI-Typ durch Skript): Ermöglicht die Angabe der überwachten CIs mithilfe eines Skripts. Mit einem Skript können Sie einen CI-Filter nicht nur für eine einzelne Tabelle, sondern für miteinander verknüpfte Tabellen erstellen. Bei der Suche nach einem CI können Sie beispielsweise einen Filter sowohl in einer Linux-Servertabelle als auch in einer Oracle-Tabelle festlegen. Am Ende des Skripts wird ein Objekt zurückgegeben, das die Tabelle und den Filter enthält.

     Beispiel für ein Skript, das im Feld **Monitored CI Script** (Überwachtes CI-Skript) angezeigt wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- **Monitored CI type by CMDB Group** (Überwachter CI-Typ nach CMDB-Gruppe): Ermöglicht die Angabe der überwachten CIs mithilfe eines Skripts. Wenn Sie diese Option auswählen, wird das Feld **Monitored CMDB group** (Überwachte CMDB-Gruppe) eingeblendet, in dem Sie eine CMDB-Gruppe auswählen, die der Richtlinie zugeordnet werden soll.
  - Details zu CMDB-Gruppen finden Sie unter CMDB-Gruppen .
  - Details zum Erstellen einer CMDB-Abfrage mit dem CMDB-Abfragegenerator finden Sie unter Erstellen Sie eine CMDB-Abfrage mit dem CMDB-Abfragegenerator .

5. Wählen Sie Schecks in aus **Verfügbar** Zelle im **Prüfungen** Und verschieben Sie sie in die **Ausgewählt** Zelle, in der sie in die Richtlinie aufgenommen werden sollen.
   Prüfungen können mehrmals ausgewählt werden, wenn Sie mehrere Prozesse überwachen. Sie können auch im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) eine Gruppe von Prüfungen auswählen, die Prüfungen der ausgewählten Gruppe in der Zelle **Available** (Verfügbar) anzeigt.
6. **Wahlweise:** Konfigurieren Sie einen Proxy-Server auf dem **Proxy-Einstellungen** Registerkarte.

   (Optional) Konfigurieren Sie einen Proxy-Server nur dann, wenn Sie den Agent als Proxy zum Melden von Daten auf Remote-Computern verwenden. Details finden Sie unter Agent auf einem Proxy-Server konfigurieren.
7. Wählen Sie auf der Registerkarte **Zeitplanung** eine der folgenden Optionen aus:
   - **Interval-based scheduling** (Intervallbasierte Zeitplanung): Konfigurieren Sie das Zeitintervall (in Sekunden), um die Häufigkeit anzugeben, mit der die Prüfungen der Richtlinie ausgeführt werden.
   - **Cron-based scheduling** (Cron-basierte Zeitplanung): Ermöglicht die Konfiguration der Richtlinie so, dass sie nur während eines bestimmten Zeitraums oder bestimmter Zeitrahmen aktiv ist.
     a. Wählen Sie das Entsperren-Symbol ( ), um die Auswahl von Cron-Ausdrücken zu aktivieren.
     b. Wählen Sie das Suchsymbol ( ), um einen Cron-Ausdruck auszuwählen. Wählen Sie **Neu**, um einen neuen Cron-Ausdruck zu erstellen, oder wählen Sie einen der im Basissystem enthaltenen Cron-Ausdrücke aus:
        - Stündlich jede Nacht von 17:00 bis 7:00 Uhr
        - Minütlich jeden Tag von 8:00 bis 16:59 Uhr
        - Minütlich von Mo bis Fr von 8:00 bis 16:59 Uhr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie einen neuen Cron-Ausdruck erstellen, müssen Sie ihn im gültigen Cron-Format eingeben.

Der angegebene Cron-Ausdruck übernimmt die Zeitzone des Computers, auf dem der Agent gehostet wird.

Hinweis: Wenn für die Prüfungsdefinition ein Wert für **Intervall** oder **Cron** angegeben wurde, überschreibt dieser Wert den in diesen Feldern konfigurierten Wert.

8. In **So senden Sie die Prüfergebnisse** Feld die Häufigkeit auswählen, mit der Prüfungsergebnisse gesendet werden sollen.
   - Wenn sich der Ereignisschweregrad ändert (Standard für Ereignisprüfungen)
   - Prüfergebnisse immer senden (Standard für nicht-Ereignis-Prüfungen)
   - Prüfergebnisse nicht senden
   - Wenn sich die Prüfergebnisse ändern
   - (Erweitert) basierend auf den Austrittscodes der Prüfung: Ergebnisse nur senden, wenn der Austrittscode 240 (OK), 241 (Warnung) oder 242 (Kritisch) lautet. Wenn die Befehlsausgabe jedoch leer ist, werden auch wenn einer dieser Codes Teil des Ausgangscodes ist, keine Prüfergebnisse gesendet.
9. Wählen Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) eine der folgenden Optionen aus:
   - **Credential name** (Anmeldeinformationsname): Wählen Sie Anmeldeinformationen aus, die der Richtlinie zugewiesen werden sollen. Die Parameter für Anmeldeinformationen werden auf Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) der zugehörigen Prüfungsdefinition angezeigt.
   - **Credential alias** (Anmeldeinformationsalias): Klicken Sie auf das Suchsymbol , um einen Alias für die Anmeldeinformationen auszuwählen, mit dem bei den Prüfungen der Richtlinie eine Verbindung mit dem überwachten CI hergestellt wird. Die auf der Seite **Connection & Credential Aliases** (Aliasse für Verbindungen und Anmeldeinformationen) erstellten Optionen sind verfügbar. Weitere Informationen zu Anmeldeinformationsaliassen finden Sie unter Anmeldeinformationsaliasse für Discovery .
10. Klicken Sie auf **Speichern**.
    Die folgenden Schaltflächen werden angezeigt:
    - **Veröffentlichen** : Veröffentlicht den Richtlinienentwurf und verschiebt ihn **Veröffentlichungsstatus** Bis **In Warteschlange** . Eine Richtlinie in der Warteschlange wird vom Richtlinienveröffentlichungsauftrag verarbeitet. Der Auftrag berechnet, welche Service Desk-Mitarbeiter die Richtlinie ausführen, und sendet die Richtlinie dann an die entsprechende MID Servers. Der Auftrag verschiebt dann die Richtlinie **Veröffentlichungsstatus** Bis **Veröffentlicht** . Eine veröffentlichte Richtlinie ist für den Agent aktiv.
    - **Delete** (Löschen): Löscht die Richtlinie

Zugehörige Informationen

Richtlinienhierarchie erstellen

Richtlinienhierarchie erstellen

Richtlinien werden an Gruppen von zugehörigen CIs angehängt. Mit einer Untergruppe zugehöriger CIs können Sie mithilfe einer Richtlinienhierarchie eine neue Richtlinie an die Untergruppe anhängen, ohne die neue Richtlinie von Grund auf neu zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Mit einer Richtlinienhierarchie können Sie eine Richtlinie als Vorlage zum Erstellen einer neuen Richtlinie verwenden, die dann an eine Untergruppe der CIs der ursprünglichen Richtlinie angehängt wird. Die ursprüngliche Richtlinie ist die **übergeordnete** Richtlinie, und die neue Richtlinie ist die **untergeordnete** Richtlinie.

Hinweis: Sie können keine untergeordnete Richtlinie erstellen, wenn ein Proxy-Agent für die übergeordnete Richtlinie vorhanden ist.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Wählen Sie auf der Seite **Policies** (Richtlinien) eine veröffentlichte Richtlinie mit dem Hierarchiewert **None** (Keine) oder **Parent** (Übergeordnet) aus.
3. Klicken Sie auf die Schaltfläche **Create Child** (Untergeordnet erstellen) oben auf der Seite oder unterhalb der Registerkarte **Monitored CIs** (Überwachte CIs).
   Eine neue (untergeordnete) Richtlinie mit denselben Parametern wie die ursprüngliche Richtlinie wird geöffnet. Der Name der Richtlinie lautet *<Policy name><date and time created>*.

   Hinweis: Die untergeordnete Richtlinie erbt die Parameter der übergeordneten Richtlinie nur bei der Erstellung. Es findet keine kontinuierliche Vererbung von der übergeordneten zur untergeordneten Richtlinie statt.

   Die folgenden Felder werden mit den angegebenen Werten hartcodiert angezeigt:

   Felder für untergeordnete Richtlinie

Feld	Wert
Veröffentlichungsstatus	Entwurf
Hierarchie	Untergeordnetes Element
Übergeordnet	<Name der übergeordneten Richtlinie>

   Der Wert im Feld **Order** (Reihenfolge) gibt die Priorität an, mit der der Agent an die Richtlinie angehängt wird. Je niedriger die Zahl, desto höher die Priorität, wobei jede erstellte untergeordnete Richtlinie jeweils einen höheren Wert als die vorhergehende Richtlinie annimmt. Diesen Wert können Sie bei Bedarf ändern.
4. Ändern Sie die Parameter der Richtlinie nach Bedarf.
   Die folgenden Schaltflächen werden auf der Seite der untergeordneten Richtlinie angezeigt:

Schaltfläche	Beschreibung
Compare to Parent (Mit übergeordneter vergleichen)	Klicken Sie auf diese Schaltfläche, um die Unterschiede zwischen der untergeordneten und der übergeordneten Richtlinie anzuzeigen.
Return to Parent (Zurück zu übergeordneter)	Klicken Sie auf diese Schaltfläche, um die Seite der untergeordneten Richtlinie zu verlassen (ohne zu speichern) und zur übergeordneten Richtlinie zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Schaltflächen werden auf der Seite der übergeordneten Richtlinie angezeigt:

Schaltfläche	Beschreibung
Deaktivieren	Wird für eine aktive Richtlinie angezeigt. Ermöglicht die Auswahl aus folgenden Optionen: ○ Übergeordnete Richtlinie und alle untergeordneten Richtlinien deaktivieren ○ Nur die übergeordnete Richtlinie deaktivieren
Aktivieren	Wird für eine inaktive Richtlinie angezeigt. Ermöglicht die Auswahl aus folgenden Optionen: ○ Übergeordnete Richtlinie und alle untergeordneten Richtlinien aktivieren ○ Nur die übergeordnete Richtlinie aktivieren
Löschen	Ermöglicht die Auswahl aus folgenden Optionen: ○ Übergeordnete Richtlinie und alle untergeordneten Richtlinien löschen ○ Nur die übergeordnete Richtlinie löschen

5. Wählen Sie **Speichern**.
   Untergeordnete Richtlinien werden auf der Registerkarte **Child Policies** (Untergeordnete Richtlinien) der übergeordneten Richtlinie angezeigt.

Veröffentlichte Richtlinien bearbeiten

Eine Richtlinie mit dem Status **Published** (Veröffentlicht) wurde über den MID-Server an den Agent übermittelt. Um eine veröffentlichte Richtlinie zu bearbeiten, müssen Sie die Bearbeitung aktivieren.

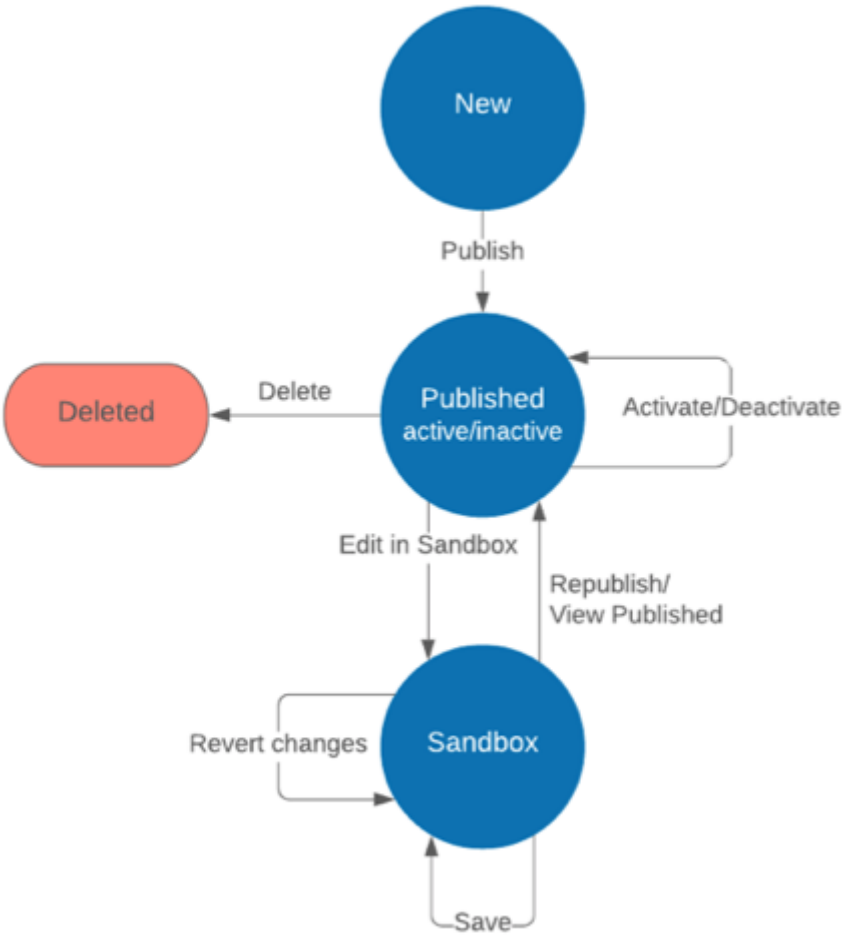
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Um die Bearbeitung der Richtlinie zu aktivieren, wählen Sie eine veröffentlichte Richtlinie und dann die Option **Edit in Sandbox** (In Sandbox bearbeiten) aus. Sie bearbeiten die Richtlinie in der Sandbox und speichern, veröffentlichen oder löschen die Richtlinie nach Bedarf. Das folgende Diagramm veranschaulicht den Bearbeitungsablauf einer veröffentlichten Richtlinie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



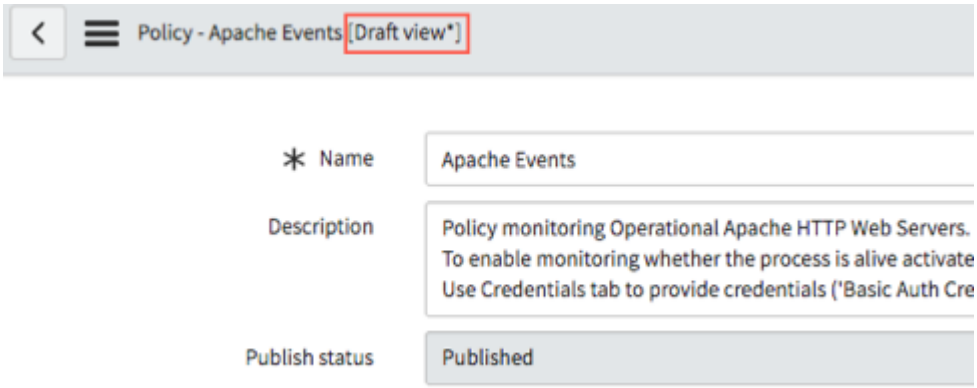
Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Klicken Sie auf eine Richtlinie mit **Publish status** = **Published** (Veröffentlichungsstatus = Veröffentlicht).
3. Aktivieren oder deaktivieren Sie die Richtlinie nach Bedarf, indem Sie auf die Schaltfläche **Activate** (Aktivieren) oder **Deactivate** (Deaktivieren) klicken.
4. Klicken Sie auf die Schaltfläche **Edit in Sandbox** (In Sandbox bearbeiten).
   Daraufhin wird die Richtlinie in der **Draft view** (Entwurfsansicht) angezeigt, und Sie können ihre Felder bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie diese Option auswählen, können auch die Prüfungsinstanzen der Richtlinie bearbeitet werden.
- Auch in der **Draft view** (Entwurfsansicht) bleibt der **Publish status** (Veröffentlichungsstatus) der Richtlinie **Published** (Veröffentlicht).



Bei der Bearbeitung einer Richtlinie können Sie die folgenden Optionen auswählen:

Schaltflächen zum Bearbeiten von Richtlinien

Schaltfläche	Beschreibung
Alle Änderungen rückgängig machen	Setzt alle Bearbeitungen, die Sie an den Richtlinienfeldern in der Sandbox vorgenommen haben, auf die zuletzt veröffentlichten Werte zurück. Die Richtlinie wird in den **Publish status** (Veröffentlichungsstatus) **Published** (Veröffentlicht) zurückgesetzt und bleibt zur Bearbeitung in der **Draft view** (Entwurfsansicht). Diese Schaltfläche wird nur angezeigt, wenn Sie in den Richtlinienfeldern in der Sandbox Werte geändert haben.
Veröffentlichte anzeigen	Kehrt zur zuletzt veröffentlichten Richtlinie zurück. Die Richtlinie wird in den Status **Published** (Veröffentlicht) zurückgesetzt.
Speichern	Hiermit werden Ihre Bearbeitungen an den Richtlinienfeldern in der Sandbox gespeichert. Die Richtlinie bleibt in der **Draft view** (Entwurfsansicht), der **Publish status** (Veröffentlichungsstatus) lautet **Published*** (Veröffentlicht*). Das Sternchen zeigt an, dass die aktuell veröffentlichte Version nicht die aktuelle ist, da es unveröffentlichte Bearbeitungen gibt.
Erneut veröffentlichen	Veröffentlicht Ihre Bearbeitungen an den Richtlinienfeldern in der Sandbox. Die Richtlinie wird mit Ihren Aktualisierungen gespeichert und wird als veröffentlichte Richtlinie geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltfläche	Beschreibung
	○ Die veröffentlichten Richtlinien **Veröffentlichungsstatus** Ist auf festgelegt **In Warteschlange** Wenn sich die Richtlinie ändert, führt dies zu: ▪ Ein Change, in dem Service Desk-Mitarbeiter die Richtlinie ausführen (d. h. eine Änderung des überwachten CI-Filters). ▪ Eine Änderung in den Prüfinstanzen der Richtlinie. Der Veröffentlichungsauftrag der Richtlinie berechnet Richtlinien in der Warteschlange neu und sendet sie an die entsprechende MID Servers. ○ Die veröffentlichten Richtlinien **Veröffentlichungsstatus** Ist auf festgelegt **Bereit zur Veröffentlichung** Wenn Änderungen an der Richtlinie keine Neuberechnung für Service Desk-Mitarbeiter erfordern (d. h. eine Änderung des Richtlinienintervalls). Der Veröffentlichungsauftrag der Richtlinie sendet Richtlinien, die bereit zur Veröffentlichung sind, an die entsprechende MID Servers, Ohne diese Richtlinien neu zu berechnen. Nachdem der Richtlinienveröffentlichungsauftrag eine Richtlinie verarbeitet hat, die Richtlinie **Veröffentlichungsstatus** Verschiebt sich zu **Veröffentlicht** . Diese Schaltfläche wird nur nach der Bearbeitung von Richtlinienfeldern einer Richtlinie angezeigt, deren **Publish status** somit gleich **Published*** (Veröffentlichungsstatus = Veröffentlicht*) ist.
Löschen	Löscht die Richtlinie Über diese Schaltfläche, die nur verfügbar ist, wenn die veröffentlichte Richtlinie angezeigt wird, wird sowohl die veröffentlichte Richtlinien als auch die die Richtlinie in der Sandbox gelöscht.

5. Wählen Sie Schecks in aus **Verfügbar** Zelle der Registerkarte Prüfungen, und verschieben Sie sie in **Ausgewählt** Zelle, in der sie in die Richtlinie aufgenommen werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfungen können mehrmals ausgewählt werden, wenn Sie mehrere Prozesse überwachen. Sie können auch im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) eine Gruppe von Prüfungen auswählen, die Prüfungen der ausgewählten Gruppe in der Zelle **Available** (Verfügbar) anzeigt.

6. Zeigen Sie in der Tabelle **Check Instances** (Prüfungsinstanzen) die für die Richtlinie konfigurierten Prüfungsinstanzen an, oder wählen Sie eine Prüfungsinstanz zur Bearbeitung aus.
7. Zeigen Sie auf der Registerkarte **Agents** die Agents an, von denen die Richtlinie ausgeführt wird.

   Die Liste der Agents wird basierend auf den überwachten CIs berechnet.

   Diese Registerkarte ist nur für veröffentlichte Richtlinien verfügbar.

Servicefilter für eine Richtlinie erstellen

Konfigurieren Sie einen Servicefilter, sodass mit der Richtlinie nur die Services überwacht werden, die dem Filter entsprechen.

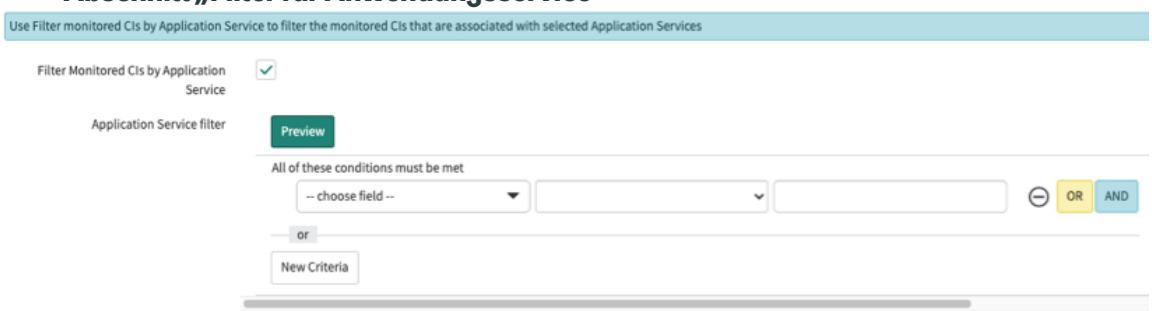
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
   Die Seite **Richtlinien** wird angezeigt.
2. Wählen Sie eine Richtlinie aus.
   Die Detailseite der Richtlinie wird angezeigt.
3. Wählen Sie die Schaltfläche **In Sandbox bearbeiten** aus, um die Bearbeitung des Formulars zu aktivieren.
4. Aktivieren Sie auf der Registerkarte „Überwachte CIs“ das Kontrollkästchen **Filter Monitored CIs by service** (Überwachte CIs nach Service filtern).
   Der Abschnitt **Filter für Anwendungsservice** wird angezeigt.

Abschnitt „Filter für Anwendungsservice“



5. Konfigurieren Sie Bedingungen in den Feldern und wählen Sie unten auf der Seite **Speichern** aus.
   Die Richtlinie wird mit dem angegebenen Servicefilter konfiguriert. Nur CIs, die dem Servicefilter entsprechen, werden in die Protokolle der Richtlinie aufgenommen.

Agent Client Collector-Richtlinien exportieren und importieren

Sie können eine oder mehrere Agent Client Collector-Richtlinien aus einer ServiceNow-Instanz in eine andere verschieben, indem Sie die Richtlinien exportieren und dann in der Zielinstanz importieren. Nur veröffentlichte Richtlinien können exportiert werden.

Vorbereitungen

Vergewissern Sie sich, dass Sie die Richtlinien, die Sie exportieren möchten, in der Quellinstanz veröffentlicht haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie in einer domänengetrennten Umgebung arbeiten, werden importierte Richtlinien von der Quellinstanzdomäne zur identischen Domäne in der Zielinstanz verschoben. Daher müssen Sie sicherstellen, dass Sie in der Zielinstanz dieselben Domänen definiert haben wie in der Quellinstanz, indem Sie entweder die Quellinstanz klonen oder Domänen aus der Quellinstanz exportieren und in die Zielinstanz importieren.

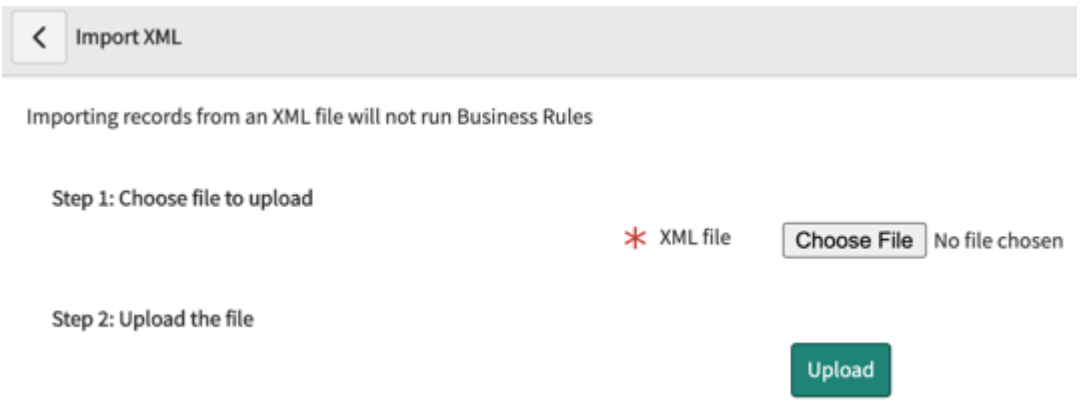
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Aktivieren Sie die Kontrollkästchen der veröffentlichten Richtlinien, die Sie exportieren möchten.
3. Wählen Sie in der Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) unter der Liste der Richtlinien die Option **Export policies** (Richtlinien exportieren) aus.
   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Ja**.
   Die ausgewählten Richtlinien werden als Update Set-Datei im XML-Format exportiert und in Ihrem Browser heruntergeladen. Das generierte Update Set weist die folgende Namenskonvention auf: AccPolicyExport <Aktuelles Datum und aktuelle Uhrzeit>. Beispiel: AccPolicyExport 2020-08-11 15:35:05.
5. Importieren Sie die Richtlinie in die Zielinstanz.

   a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**an.
   Die Seite **Retrieved Update Sets** (Abgerufene Update Sets) wird angezeigt.

   b. Klicken Sie mit der rechten Maustaste auf einen der Tabellenheader, und wählen Sie **Import XML** (XML importieren) aus.
   Die Seite **Import XML** (XML importieren) wird angezeigt.



   c. Klicken Sie auf die Schaltfläche **Choose File** (Datei wählen), und wählen Sie das zuvor heruntergeladene Update Set für den Import aus.

   d. Klicken Sie auf **Hochladen**.

   Hinweis: Wenn sich der exportierte Inhalt in einem Bereich befindet, wird das importierte Update Set auf der Seite **Retrieved Update Sets** (Abgerufene Update Sets) in Form von mehreren Datensätzen angezeigt. Der Datensatz mit dem Bereich **Global** ist das übergeordnete Element, die anderen Datensätze werden mit dem Global-Datensatz als übergeordnetes Update Set angezeigt. Der Importvorgang lässt sich nur mit dem Global-Datensatz des Update Set initiieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Wählen Sie das Update Set **Global** aus.

f. Klicken Sie auf der Seite **Retrieved Update Sets** (Abgerufene Update Sets) auf **Preview Update Set Batch** (Vorschau auf Update Set-Batch), um zu überprüfen, ob Konflikte mit vorhandenen Richtlinien in der Zielinstanz bestehen.
Lösen Sie Konflikte gegebenenfalls.

g. Wenn keine Konflikte bestehen, klicken Sie auf **Commit Update Set Batch** (Commit für Update Set-Batch ausführen), um das Update Set zu validieren und zu bestätigen.

h. Navigieren zu **Agent Client Collector** > **Richtlinien** Und überprüfen Sie, ob die importierten Richtlinien in der Richtlinienliste angezeigt werden.
Die importierten Richtlinien werden mit den entsprechenden MID Servers n in der Zielinstanz synchronisiert und können sofort verwendet werden.

Hinweis: Beim Importprozess werden alle vorhandenen Richtlinien in der Zielinstanz überschrieben, und die importierten Richtlinien werden auf **Published** (Veröffentlicht) gesetzt. Entwurfskopien von Richtlinien, die in der Zielinstanz erstellt wurden, werden jedoch nicht geändert. Löschen Sie daher nach Abschluss des Importvorgangs Entwurfsdatensätze der importierten Richtlinien, da diese Datensätze nicht mit den veröffentlichten Richtlinien in der Zielinstanz synchronisiert werden.

Prüfungen erstellen und bearbeiten

Sie können eine Prüfung abhängig vom Typ der Entität (z. B. einem Server oder einer Anwendung) auswählen, die Sie überwachen möchten. Nach Bedarf können Sie die Standardprüfungen anzeigen und bearbeiten oder neue Prüfungen erstellen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**an.
2. Klicken Sie auf **Neu**.
Die Seite **Check Definition** (Prüfungsdefinition) wird angezeigt.

   Hinweis: Die Verwendung von Ruby-Skripts in einer Windows-Umgebung verursacht einen hohen CPU-Verbrauch.

3. Geben Sie Werte in die Felder auf der Seite ein, wie in beschrieben Agent Client Collector Definitionsseite überprüfen.
4. Geben Sie auf der Registerkarte **Parameter** nach Bedarf Parameterdefinitionen ein.
Parameter werden für verwendet **Befehl** Feld, wenn die einfache Vorlage verwendet wird, wie in beschrieben Agent Client Collector Definitionsseite überprüfen.

   Die Informationen, die Sie für Parameter hinzufügen können, werden in beschrieben Registerkarte „Prüfdefinitionsformularparameter“.

Prüfungsdefinitionen oder Prüfungsinstanz testen

Wenn Sie mit einer Prüfungsdefinition oder Prüfungsinstanz arbeiten, können Sie die Prüfung mit dem zugewiesenen Agent testen, um sicherzustellen, dass die Prüfung ordnungsgemäß konfiguriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**an.
2. Wählen Sie in der Liste eine Prüfungsdefinition aus.

   Hinweis: Bei Prüfungstest in Prüfungsinstanz:

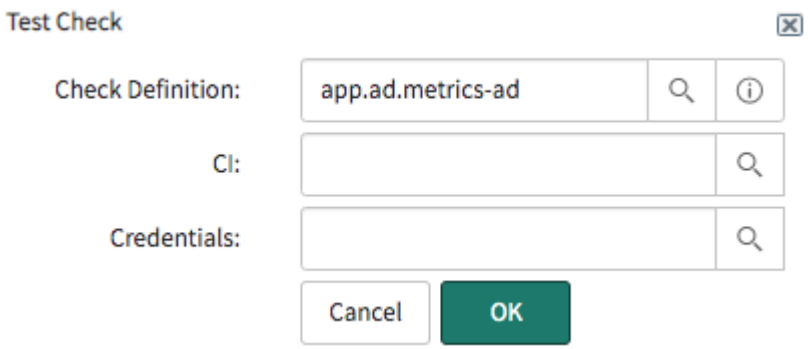
   a. Navigieren zu **Agent Client Collector** > **Richtlinien**an.

   b. Wählen Sie eine Richtlinie aus.

   c. Wählen Sie in der Richtlinie eine Prüfungsinstanz aus.

   Fahren Sie mit den folgenden Schritten in diesem Verfahren fort.

3. Klicken Sie im Abschnitt **Related Links** (Zugehörige Links) auf **Test Check** (Testüberprüfung).
   Das Dialogfeld **Test Check** (Testüberprüfung) wird angezeigt.



4. Konfigurieren Sie die Felder im Dialogfeld.

Felder des Dialogfelds „Testprüfung“

Feld	Beschreibung
Prüfungsdefinition	Zeigt den Namen der ausgewählten Prüfungsdefinition an
CI	Wählen Sie das CI aus, für das die Prüfung ausgeführt werden soll. Zur Auswahl verfügbar sind diejenigen CIs, die die beiden folgenden Kriterien erfüllen: ○ Gehören zu der im Feld **Check group** (Überprüfungsgruppe) angegebenen Gruppe ○ Gehört zu einem Service Desk-Mitarbeiter mit **Aktiv** Status. Wenn das Feld **Check group** (Überprüfungsgruppe) leer ist, wird der Standardwert **cmdb_ci_computer** eingetragen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Berechtigungen	Wählen Sie die Anmeldeinformationen des Benutzers aus, mit dem der Agent eine Verbindung herstellen soll. Dieses Feld wird nur angezeigt, wenn Sie auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) in der Prüfungsdefinition sichere Prüfungsparameter konfiguriert haben.
Proxy-Agent	Wählen Sie den Proxy-Agent aus, der der Prüfung zugeordnet werden soll. Dieses Feld wird nur angezeigt, wenn Sie mit einer Prüfungsinstanz arbeiten und eine der Optionen auf der Registerkarte **Proxy Settings** (Proxy-Einstellungen) in der Richtlinie der Instanz ausgewählt wurde.

Sichere Parameter für Prüfungen erstellen

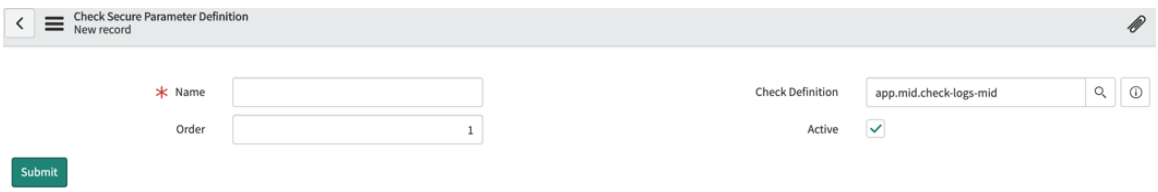
Beim Erstellen einer Prüfungsdefinition oder einer Prüfungsinstanz können Sie die Parameter konfigurieren, die gesichert werden sollen, wenn der Agent die Prüfung ausführt. Während der Prüfungsausführung werden die gesicherten Parameter verschleiert, wodurch ihre Informationen gesichert werden. Nur Anmeldeinformationen werden verschleiert.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**an.
2. Wählen Sie in der angezeigten Liste eine Prüfungsdefinition aus.
   Die Seite **Check Definition** (Prüfungsdefinition) wird angezeigt.
3. Scrollen Sie zum Ende der Seite, und wechseln Sie zur Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen).
4. Klicken Sie auf **Neu**.
   Die Seite **Check Secure Parameter Definition New Record** (Sichere Parameterdefinitionen überprüfen: Neuer Datensatz) wird angezeigt.



5. Konfigurieren Sie die Felder auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Name	Name des Parameters, formatiert als Referenzpräfix. So ist beispielsweise `cred_` ein Referenzpräfix für die Tabelle mit den Anmeldeinformationen.
Prüfungsdefinition	Name der mit dem Parameter verbundenen Prüfungsdefinition
Reihenfolge	Zahl, die die Reihenfolge angibt, in der der Parameter an den Prüfungsbefehl/das Prüfungsskript gesendet wird. Wenn Sie beispielsweise die folgenden Parameter konfigurieren: ○ Name=**cred_user_name**, Reihenfolge=**1** ○ Name=**cred_password**, Reihenfolge=**2** Dann wird der Parameter *username* an erster und der Parameter *password* an zweiter Stelle an die Standardeingabe gesendet. Der Befehl *READ* wird zuerst für den Parameter *username* und dann für den Parameter *password* ausgeführt. In Ihrem *Bash*-Skript können Sie dann *$username* und *$password* verwenden.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den sicheren Parameter zu aktivieren.

6. Klicken Sie auf **Absenden**.
   Der konfigurierte Parameter wird in der Tabelle auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) angezeigt.

   Wiederholen Sie diesen Vorgang, um mehrere sichere Parameter einzugeben.
7. Geben Sie die sicheren Parameter in das Feld **Command prefix** (Befehlspräfix) der Prüfungsdefinition ein.

Prüfungstyp erstellen

Erstellen Sie einen Prüfungstyp, um den Befehl `osquery` für den Agent auszuführen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_integration oder agent_client_collector_admin

Prozedur

1. Geben Sie in einer Ereignismanagement-Instanz in der Navigationsleiste `sn_agent_check_type.list` ein.
   Die Seite **Check Types** (Prüfungstypen) wird angezeigt.
2. Klicken Sie auf **Neu**.
   Die Seite `Check Type - New Record` (Prüfungstyp – Neuer Datensatz) wird angezeigt.
3. Geben Sie im Feld **Name** den Namen `osquery` ein.
4. Geben Sie in das Feld **Instance Script** (Instanzskript) das folgende Skript ein:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
for (var index = 0; index < checkResults.length; index++) {
var check = checkResults[index].check;
gs.info('result ' +
index + ': requestId: ' +
check.requestId + ' agent_name: ' +
checkResults[index].agent_id +
' ci_id: ' + check.ci_id +
' status: ' + check.status +
' output: ' + check.output);

}
```

Sie können dieses Skript nach Bedarf ändern. Mit diesem Ausgangsskript können Sie jedoch überprüfen, ob die Einrichtung erfolgreich war.

5. Klicken Sie auf **Absenden**.

Prüfungsdefinitionen erstellen

Erstellen Sie eine Prüfungsdefinition, um den Befehl `osquery` für den Agent auszuführen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_integration oder agent_client_collector_admin

Prozedur

1. In einem Ereignismanagement Instanz, navigieren Sie zu **Agent Client Collector** > **Prüfungsdefinitionen**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Feld **Name** den Namen `util.osquery` ein.
4. Geben Sie im Feld **Check type** (Prüfungstyp) den Namen `osquery` ein.
5. Geben Sie im Feld **Command** (Befehl) das folgende Skript ein:

```
osqueryi  --logger_min_status 1 --json "{{.labels.params_query}} "
```

6. In **Plugins** Geben Sie ein `Osquery` Plugin.
7. Geben Sie im Abschnitt **Parameter** die folgenden Werte für eine Prüfungsparameterdefinition ein.

Spalte	Wert
Name	query
Standardwert	* aus logged_in_users auswählen
Obligatorisch	Wahr

8. Klicken Sie auf **Test check** (Testüberprüfung), und wählen Sie einen der verfügbaren Agents aus. Das angezeigte Testergebnis gibt an, ob die Überprüfung erfolgreich war oder fehlgeschlagen ist.

Prüfungen aus Agent Client Collector-Community aktivieren

Sie können Prüfungen aus der GitHub-Community abrufen und zur Verwendung in Agent Client Collector (ACC) anpassen oder eigene Skripts erstellen. Erstellen Sie ein Plugin mit der benutzerdefinierten Sensu-Prüfung, und installieren Sie es für eine ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Kopieren Sie eine Prüfung aus der GitHub-Community auf Ihren lokalen Computer.
2. Erstellen Sie eine tar.gz-Datei, die an Ihr Plugin angehängt werden soll:
   a. Erstellen Sie einen Ordner auf Ihrem lokalen Computer.
   b. Erstellen Sie einen Unterordner mit der Bezeichnung bin.
   c. Legen Sie die Prüfungen im Ordner bin ab, die Sie ausführen möchten (Skripts und ausführbare Dateien).
   d. Erteilen Sie in einer Linux-Umgebung den Prüfungen Ausführungsberechtigungen, indem Sie für jede Prüfung *chmod + x filename* ausführen.
   e. Navigieren Sie zum übergeordneten Ordner (über dem bin-Ordner).
   f. Führen Sie in einer Linux-Umgebung den Befehl *tar -C <parent_folder_name> --zcvf <my_plugin_name>.tar.gz ** aus.
   Verwenden Sie in einer Windows-Umgebung ein Archivierungsdienstprogramm, das das Format tar.gz unterstützt.
   g. Achten Sie in einer Windows-Umgebung darauf, dass in den Ordner bin die folgenden Skripts eingefügt werden:
      - Batch-Skript, das für die Ausführung des Prüfbefehls und zur Initiierung der Ausführung konfiguriert ist. Beispiel:*powershell <%~dp0>\test.ps1*.

        Die Variable *<%~dp0>* verweist auf das Laufwerk (*d*) und den Pfad (*p*) der Batch-Datei.
      - Das relevante Skript (z. B. test.ps1), das im Batch-Skript ausgeführt werden soll
3. Erstellen Sie ein neues ACC-Plugin (siehe Erstellen und bearbeiten Agent Client Collector Plugins).
4. Testen Sie das neue Plugin.
   a. Erstellen Sie eine neue Prüfungsdefinition für die angepasste Sensu-Prüfung.
   Details finden Sie unter Prüfungen erstellen und bearbeiten.
   b. Navigieren Sie auf der Seite **Check Definition** (Prüfungsdefinition) zum Abschnitt **Related Links** (Zugehörige Links), und klicken Sie auf **Generate allow list content** (Inhalte für Allow-Liste generieren).
   c. Kopieren Sie die Einträge, die Sie in die Allow-Liste aufnehmen möchten, und fügen Sie sie der Datei check-allow-list.json des Agent entweder manuell oder mit einem Automatisierungs-Tool hinzu.
   Der Speicherort dieser Datei ist im Parameter allow-list der Datei acc.yml des Agent angegeben.
   d. Erstellen Sie eine neue Richtlinie, und fügen Sie die neu erstellte Prüfungsdefinition hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zum Erstellen einer Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

e. Wählen Sie die Prüfungsdefinition aus, und klicken Sie im Abschnitt **Related Links** (Zugehörige Links) auf **Test check** (Testüberprüfung).

5. Aktivieren Sie Anmeldeinformationen beim Testen einer Prüfung:

a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.

b. Klicken Sie auf **Neu**.

c. Wählen Sie den Typ der Anmeldeinformationen aus, die Sie erstellen möchten.
Weitere Informationen zum Erstellen von Anmeldeinformationen finden Sie unter Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen .

d. Geben Sie Werte in die Felder auf der Seite ein, um dem ausgewählten Anmeldeinformationstyp Anmeldeinformationen zuzuweisen.

e. Klicken Sie auf **Absenden**.

6. Erstellen Sie für Ihre Prüfung sichere Parameter (siehe Sichere Parameter für Prüfungen erstellen).

Wird Aktiviert Agent Client Collector Datensammlung

Sie können Aktionen ausführen, die die Datensammlung von den Hosts verbessern, auf denen Agent Client Collector Wird ausgeführt.

Aufruf-API zum Senden einer osquery-Anforderung erstellen

Erstellen Sie ein Hintergrundskript, um eine `osquery`-Anforderung zu senden. Die `Osquery` „Anforderung“ aktiviert die Datensammlung aus dem Betriebssystem Ihres Hosts.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie das folgende Hintergrundskript:
   - `"MTLV9DE22016"` ist der Name des Servers, auf dem ein Agent ausgeführt wird.
   - `"c8bf9072539333003e76ddeeff7b12c5"` ist die sys_id der zuvor erstellten Prüfungsdefinition.

```
cis = new GlideRecord("cmdb_ci_server");
   cis.addQuery("name", "MTLV9DE22016");
   cis.query();
   check = {
      "checkDefId": "c8bf9072539333003e76ddeeff7b12c5",
      "params": {
         "query": "select pid,cmdLine from processes limit 4"
      }
   };
   var agentNow = new sn_agent.AgentNowHandler();
   gs.info('request_id: ' + agentNow.runCheckForCis(cis,check,'1',60000));
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Führen Sie das Skript zur Ausgabe der Anforderungs-ID aus:
request_id: `eefbff7ab75733003e766068de11a981`

3. Überprüfen Sie die Systemprotokolle auf Nachrichten vom Instanzskript.

```
result 0 requestId: 06c6c887b79733003e766068de11a912 agent_name: MTLV9DE22016 ci_id:
00726c36539333003e76ddeeff7b12db status: 0 output: [
{"cmdline":"","pid":"0"},
{"cmdline":"","pid":"1"},
{"cmdline":"","pid":"45"},
{"cmdline":"","pid":"46"}
]
```

Zeigen Sie die Hostdatensammlung für einen Service Desk-Mitarbeiter an

Führen Sie die Datensammlung auf dem Host eines Service Desk-Mitarbeiters aus, um die Komponenten zu erkennen, die auf dem Host ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Die geplante Aufgabe „Hostdaten für Service Desk-Mitarbeiter aktualisieren“ erfasst Hostdaten und wird stündlich für Folgendes ausgeführt:

- Hosts, die in den letzten 12 Stunden nicht erkannt wurden.
- Host, für den Discovery Fehlgeschlagen.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
In **Hostdatensammlung** Spalte, zeigen Sie den Status der Datensammlung auf dem Host des Service Desk-Mitarbeiters an. Die möglichen Status sind:

Status der Hostdatensammlung

Status	Beschreibung
<empty>	Gibt an, dass der Service Desk-Mitarbeiter in der letzten Minute hinzugefügt wurde und die geplante Aufgabe Überwachungsrichtlinien aktualisieren und veröffentlichen noch nicht ausgeführt wurde, um die Datensammlung zu initiieren. Der Auftrag wird jede Minute ausgeführt.
Erfasst (grün)	Die Hostdatensammlung ist abgeschlossen.
Sammeln (gelb)	Hostdatensammlung wird ausgeführt.
Sammlung fehlgeschlagen (rot)	Hostdatensammlung fehlgeschlagen.

2. **Wahlweise:** Suchen Sie nach **Zuletzt erfasste Hostdaten** Spalte, die angezeigt werden soll, wann die Datensammlung zuletzt auf dem Host durchgeführt wurde.

Agent Client Collector-Zulassungsliste generieren

Geben Sie die Prüfungen an, die in die Liste der Prüfungen aufgenommen werden sollen, die für den Service Desk-Mitarbeiter ausgeführt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Die standardmäßige Allow-Liste enthält alle validierten Prüfungen und ist in den Richtlinien des Basissystems enthalten. Wenn die Allow-Liste nicht richtig gelesen werden kann, werden keine Prüfungen für den Agent ausgeführt.

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**an.
   Die Seite **Check Definitions** (Prüfungsdefinitionen) wird angezeigt.
2. Klicken Sie im Abschnitt **Related Links** (Zugehörige Links) unten auf der Seite auf **Generate allow list** (Allow-Liste generieren).

   Hinweis: Alternativ können Sie eine Prüfungsdefinition oder den Datensatz einer Prüfungsinstanz auswählen und auf **Generate allow list** (Allow-Liste generieren) klicken, um eine vollständige Allow-Liste zu generieren.

   Die Seite **Agent Client Collector Command Allow-list Generator** (Agent Client Collector: Befehls-Allow-Listen-Generator) wird mit einer Liste der Prüfungen aus dem Feld **Befehl** der Prüfungsinstanzdatensätze angezeigt.

   Die Werte werden mit den folgenden Attributen angezeigt:

Befehlsattribute

Attribut	Beschreibung
exec	Befehl, der ausgeführt wird
args	Mögliche Argumentzeichenfolgen
skip_arguments	Boolescher Wert. Legt fest, ob geprüft werden soll, ob das Argument der Allow-Liste hinzugefügt wurde ○ **true**: Überspringt die Argumentvalidierung und prüft nur auf ungültige Zeichen, insbesondere |; \<>&'$() ○ **false**: Führt eine Argumentvalidierung durch, um sicherzustellen, dass das Argument in der Allow-Liste enthalten ist. Wenn es nicht enthalten ist, kann der Befehl nicht ausgeführt werden.

3. Kopieren Sie die Einträge, die Sie in die Allow-Liste aufnehmen möchten, und fügen Sie sie der Datei check-allow-list.json des Agent entweder manuell oder mit einem Automatisierungs-Tool hinzu.
   Der Speicherort dieser Datei wird im Parameter `allow-list` der Datei acc.yml des Agent angegeben.

Hostdatensammlung bei Bedarf ausführen

Sie können die Hostdatensammlung bei Bedarf durchführen, wenn Sie die Datensammlung durchführen müssen, bevor die Ausführung des Auftrags geplant ist.

Vorbereitungen
Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen von CIs verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
   Die Seite **Agent Client Collectors** wird angezeigt.
2. Wählen Sie einen Agent mit **Status = Alive** aus.
3. Klicken Sie im Agent-Formular auf die Schaltfläche **Hostdaten erfassen**.

Agent Client Collector-Datensammlung anhalten

Wenn der CPU-Verbrauch auf Ihrem Server zu hoch wird, können Sie die Agent Client Collector-Datensammlung manuell deaktivieren, um alle vom Agent durchgeführten Prüfungen mit Ausnahme der Keep-Alive-Nachrichten des Agent anzuhalten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
   Die Seite **Agent Client Collectors** wird mit einer Liste der konfigurierten Agents angezeigt.
2. Aktivieren Sie die Kontrollkästchen neben den relevanten Agents.
3. Wählen Sie in der Dropdown-Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) die Option **Pause data collection** (Datensammlung anhalten) aus, um die Datensammlung auf den Agents anzuhalten (**Data Collection = Off (manual)** (Datensammlung = Aus (manuell))).

   Wählen Sie **Resume data collection** (Datensammlung fortsetzen) aus, um die Datensammlung auf den Agents fortzusetzen.

   Alternativ können Sie den Status eines Agent festlegen, indem Sie den Agent auswählen und im Abschnitt **Related Links** (Zugehörige Links) auf den Link **Pause data collection** (Datensammlung anhalten) klicken, um die Datensammlung für den Agent anzuhalten. Um die Datensammlung für den Agent wieder aufzunehmen, klicken Sie auf den Link **Resume data collection** (Datensammlung fortsetzen).

Validieren Sie Assets auf dem MID-Server

Validieren Sie Assets auf Ihrem MID-Server Um sicherzustellen, dass sie mit den Assets auf Ihrem übereinstimmen ServiceNow Instanz. Durch die Validierung von Assets wird sichergestellt, dass die Instanz genaue Daten zu allen Ihrer bereitstellt MID-Server Assets.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**an.
2. Wählen Sie ein aus MID-Server Eintrag in MID Servers Seite.
3. Wählen Sie aus **Validieren Sie Assets** Link.
   Die **Warteschlangen** Die Seite wird angezeigt und zeigt die ECC-Warteschlange an.
4. Aktualisieren Sie die Warteschlange, um den neuen Eingabedatensatz anzuzeigen.
5. Wählen Sie den Datensatz aus, um seine Ergebnisse anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Validierungsstatus ist in sichtbar **Nutzlast** Abschnitt des Formulars.

Wenn Assets nicht validiert sind, starten Sie neu MID-Server. Assets werden automatisch synchronisiert, wenn MID-Server Startet neu.

Validiert Assets für Service Desk-Mitarbeiter

Validieren Sie Assets für Ihre Service Desk-Mitarbeiter, um sicherzustellen, dass sie mit den Assets auf Ihrem übereinstimmen ServiceNow Instanz. Durch die Validierung von Assets wird sichergestellt, dass die Instanz genaue Daten zu allen Assets Ihrer Service Desk-Mitarbeiter bereitstellt.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Nur Assets, die ausgeführt werden können, werden validiert. Beispiel: Wenn Sie einen Service Desk-Mitarbeiter auf einem ausführen macOS, Nur macOS Assets in Ihrer Instanz werden validiert.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie einen Service Desk-Mitarbeiter im aus **Agent Client Collectors** Seite.
3. Wählen Sie aus **Validieren Sie Assets** Link.
   Die **Warteschlangen** Die Seite wird angezeigt und zeigt die ECC-Warteschlange an.
4. Aktualisieren Sie die Warteschlange, um den neuen Eingabedatensatz anzuzeigen.
5. Wählen Sie den Datensatz aus, um seine Ergebnisse anzuzeigen.

   Der Validierungsstatus ist in sichtbar **Nutzlast** Abschnitt des Formulars.

   Wenn Assets nicht validiert sind, navigieren Sie zurück zu **Agent Client Collectors** Seite und wählen Sie aus **Löschen Sie Assets** Link.

   Die Assets werden beim nächsten Ausführen eines Befehls, der das Asset erfordert, automatisch erneut synchronisiert.

Verwenden Agent Client Collector Protokolle

Verwenden Agent Client Collector Protokolle zur Nachverfolgung von Ereignissen in Ihrem System. Protokollebenen geben den Schweregrad jedes Ereignisses an.

Agent Client Collector-Protokollebenen konfigurieren

Sie konfigurieren die Protokollebenen, die die Agent Client Collector-Protokolle einhalten sollen. Alle Events, die die angegebene Protokollebene erreichen oder sie überschreiten, werden in den Agent Client Collector-Protokollen verzeichnet.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Geben Sie die gewünschte Protokollebene in der Konfigurationsdatei acc.yml an.
   Alternativ können Sie die Protokollebene wie folgt als Argument in der Kennzeichnung der Befehlszeile `--loglevel` angeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
acc start --log level debug
```

2. Starten Sie den Agent mit dem Servicemanager neu:
   - **Linux**:

     ```
     sudo service acc restart
     ```

   - **Windows**:

     ```
     sc.exe stop AgentClientCollector
     sc.exe start AgentClientCollector
     ```

   - **macOS**:

     ```
     sudo launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist
     ```

Hinweis: Sie müssen den Service neu starten, nachdem Sie die Protokollebene geändert haben.

Agent Client Collector-Protokolle anzeigen

Sie können die Aktivitätsprotokolle für Agent Client Collector anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector Protokolle sind zugänglich von:

- **Linux**: /var/log/servicenow/agent-client-collector/acc.log
- **Windows**: Durch die Konfigurationskennzeichnung log-file angegebener Speicherort. Der Standardspeicherort lautet: C:/ProgramData/ServiceNow/agent-client-collector/log/acc.log.

  Wenn das Verzeichnis C:/ProgramData ausgeblendet ist (z. B. bei älteren Windows-Versionen), ändern Sie den Explorer-Filter, um ausgeblendete Elemente anzuzeigen.
- **MacOS** : Der Standardstandort ist: /Library/Application\ Support/servicenow/Agent-Client-Collector

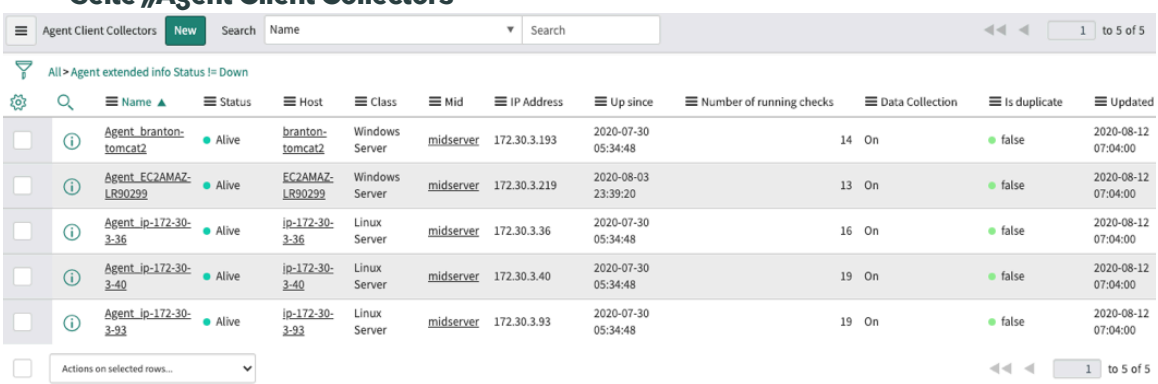
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
   Die Seite **Agent Client Collectors** wird angezeigt.

Seite „Agent Client Collectors“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die angezeigten Spalten sind diejenigen, die ausgewählt werden, wenn Sie auf das Einstellungssymbol klicken.

Die Spalte **Host** gibt den Hostnamen des Agent an.

Die Spalte **Class** (Klasse) gibt den CI-Typ des Agent an.

2. Wählen Sie einen HR-Mitarbeiter aus.
   Die Seite **Agent Client Collector** wird angezeigt.
3. Klicken Sie im Abschnitt **Related Links (Zugehörige Links)** auf **Grab Agent Log (Agent-Protokoll abrufen)**.
   Die Seite **Queues** (Warteschlangen) wird für den ausgewählten Agent geöffnet.
4. Aktualisieren Sie die Seite, und klicken Sie auf den entsprechenden Eintrag mit dem Wert **Queue = input** (Warteschlange = Eingabe).
   Die **Nutzlast** Abschnitt auf der **Warteschlange** Das Formular zeigt das Protokoll für an Agent Client Collector.

Protokollüberwachung in einer Linux-Umgebung aktivieren

Um Überwachungsprotokolle in einer Linux-Umgebung zu aktivieren, wählen Sie die relevante Richtlinie aus, und weisen Sie ihr spezifische Prüfungsparameter zu. Wenn die Protokollüberwachung aktiviert ist und eine angegebene Zeichenfolge im überwachten Protokoll erkannt wird, wird ein Event erstellt.

Vorbereitungen

Stellen Sie sicher, dass der Benutzer servicenow Zugriff auf die überwachte Protokolldatei hat oder dass der angegebene Benutzer den `sudo`-Befehl ausführen kann.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Wählen Sie die Richtlinie zur **Linux-Protokollüberwachung** aus.
3. Wählen Sie **util.check-logs** auf der Registerkarte **Check Instances (Prüfungsinstanzen)** aus, um die Überwachung von Protokolldateien zu aktivieren, die nicht dem *`root`*-Benutzer gehören.
   Stellen Sie sicher, dass der Agent Client Collector *`servicenow`*-Benutzer über Leseberechtigungen für die überwachte Protokolldatei verfügt.
4. Geben Sie die Protokolldatei an, die bei der Prüfung durchsucht werden soll:
   a. Wählen Sie auf der Registerkarte **Check Parameter Definitions** (Definition von Prüfungsparametern) am unteren Seitenrand in der Spalte **Name** den Eintrag **file** (Datei) aus.
   b. Geben Sie im Feld **Default value** (Standardwert) den Pfad zu der Protokolldatei ein, die Sie durchsuchen möchten.
5. Geben Sie die Zeichenfolge an, die Sie im Protokoll suchen möchten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie auf der Registerkarte **Check Parameter Definitions** (Definition von Prüfungsparametern) am unteren Seitenrand in der Spalte **Name** den Eintrag **pattern** (Muster) aus.

b. Geben Sie im Feld **Default value** (Standardwert) die Suchmuster-Zeichenfolgen ein, nach denen Sie in der Protokolldatei suchen möchten, z. B. `404` und `Error`. Die Standardwerte lauten `SEVERE` (Schwerwiegend) und `Exception`(Ausnahme).

   Stellen Sie sicher, dass Sie mehrere Muster durch eine Pipe (|) trennen und als Parameter in Anführungszeichen weitergeben. Zum Beispiel: `"SEVERE|404"`.

6. Klicken Sie auf **Update** (Aktualisieren), um Ihre Prüfungsinstanz zu speichern und zur Seite **Policy - Linux Log Monitoring** (Richtlinie - Linux-Protokollüberwachung) zurückkehren.
7. Wählen Sie die Prüfung **util.check-logs-sudo** aus, um Protokolle zu überwachen, die dem Root-Benutzer gehören.
8. Wiederholen Sie die Schritte 4 und 5, um Protokolle zu überwachen, die dem Root-Benutzer gehören.
9. Ändern Sie für die Prüfung **util.check-logs-sudo** wie folgt die Datei `etc/sudoers` auf dem Host oder virtuellen Linux-Computer:
   Wenn der Agent am Standardspeicherort des Hosts (`/usr/share/servicenow/agent-client-collector`) oder auf einem virtuellen Linux-Computer installiert ist, fügen Sie der Datei `/etc/sudoers` die folgende Zeichenfolge hinzu:

```
servicenow ALL=
 SETENV: /
var/cache/servicenow/agent-client-collector/monitoring-plugin-linux/bin/check-log.rb *
Defaults:servicenow !requiretty
Defaults exempt_group += servicenow
```

10. Klicken Sie auf der Seite **Policy** (Richtlinie) auf **Save** (Speichern) und dann auf **Publish** (Veröffentlichen), um die Richtlinie zum Überwachen der Protokolldatei zu aktivieren.

Protokollüberwachung in einer Windows-Umgebung aktivieren

Um Überwachungsprotokolle in einer Windows-Umgebung zu aktivieren, wählen Sie die relevante Richtlinie aus, und weisen Sie ihr spezifische Prüfungsparameter zu. Wenn die Protokollüberwachung aktiviert ist und eine angegebene Zeichenfolge im überwachten Protokoll erkannt wird, wird ein Event erstellt.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Wählen Sie die Richtlinie zur **Windows-Protokollüberwachung** aus.
3. Wählen Sie **os.windows.check-log** auf der Registerkarte **Check Instances** (Prüfungsinstanzen) aus, um die Überwachung von Windows-Protokolldateien zu aktivieren.
4. Geben Sie auf der Registerkarte **Check Parameters** (Prüfungsparameter) die in der folgenden Tabelle beschriebenen Protokollparameter an, die durch die Prüfung überwacht werden sollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter überprüfen

Name	Wert
warning	Häufigkeit des Auftretens der angegebenen Musterzeichenfolgen im Protokoll, durch die ein *warning*-Event generiert wird. Standard = 1. Beispiel: Wenn der Wert für *pattern* gleich **Exception** (Ausnahme) ist und das Protokoll ein Ausnahme-Event enthält, wird ein *warning*-Event generiert.
critical	Häufigkeit des Auftretens der angegebenen Musterzeichenfolgen im Protokoll, durch die ein *critical*-Event generiert wird. Standard = 2. Beispiel: Wenn der Wert für *pattern* gleich **Exception** (Ausnahme) ist und das Protokoll zwei Ausnahme-Events enthält, wird ein *critical* -Event generiert.
file	Speicherort der Protokolldatei
pattern	Zeichenfolgen, nach denen im Protokoll gesucht wird. Standardwerte: **Severe** (Schwerwiegend) und **Exception** (Ausnahme). Andere mögliche Werte: **404** und **Error** (Fehler) Stellen Sie sicher, dass Sie mehrere Muster durch eine Pipe (|) trennen und als Parameter in Anführungszeichen weitergeben. Zum Beispiel: `"SEVERE|404"`.

Legen Sie die Agent-Protokollebene fest

Konfigurieren Sie die Agent-Protokollebene direkt von ServiceNow® Instanz, ohne Zugriff auf erforderlich zu sein acc.yml Konfigurationsdatei.

Warum und wann dieser Vorgang ausgeführt wird

Durch die Konfiguration der Agent-Protokollebene in der Instanz wird die Protokollebene vorübergehend geändert und die Protokollebene in nicht aktualisiert acc.yml Konfigurationsdatei. Beim Neustart des Service Desk-Mitarbeiters wird die Protokollebene auf den in festgelegten Status zurückgesetzt acc.yml Konfigurationsdatei.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. Wählen Sie in den zugehörigen Links die Option aus **Legen Sie Die Protokollebene Fest** .
4. Wählen Sie im Dialogfeld „Protokollebene festlegen“ die Protokollebene aus, die für den Service Desk-Mitarbeiter aufgerufen werden soll, und wählen Sie aus **OK** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Setzen Sie die Protokollebene auf die ursprünglich konfigurierte Ebene zurück, indem Sie eine der folgenden Aktionen ausführen:
   - Wählen Sie in den zugehörigen Links die Option aus **Protokollebene Zurücksetzen** .
   - Starten Sie den Service Desk-Mitarbeiter neu.

Löschen Agent Client Collector Assets

Löschen Sie den Asset- und Konfigurationsdatei-Cache-Ordner, und steuern Sie Plugin-Downloads. Durch das Löschen des Cache-Ordners werden unerwünschte Plugins entfernt, die mit dem Service Desk-Mitarbeiter synchronisiert wurden.

Vorbereitungen

Stellen Sie sicher, dass Folgendes auf Ihrem System installiert ist:

- Agent Client Collector Framework (ACC-F), ab Version 3.5.5
- MID-Server
- CMDB
- Agent Client Collector Agent, ab Version 3.5.5
- Globale ACC-Dienstprogramme

Stellen Sie sicher, dass **Disable_Assets** Systemeigenschaft in acc.yml Konfigurationsdatei ist auf festgelegt **Falsch** .

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. In **Zugehörige Links** Abschnitt auswählen **Löschen Sie Assets** .
4. Wählen Sie im Bestätigungsdialogfeld aus **Löschen Sie Service Desk-Mitarbeiter-Assets** .
5. **Wahlweise:** Wählen Sie Aus **Erfassen Sie Hostdaten** Um Ihre Plugins aus der Instanz erneut herunterzuladen.
   Plugins werden automatisch heruntergeladen, wenn sie von ihren jeweiligen Prüfungen/Richtlinien verwendet werden.

Integritäts-Dashboard von Agent Client Collector

Im Agent Health-Dashboard können Sie den Status der Agents in Ihrem System überwachen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agent Health-Dashboard**an.
   Die Seite **Agent Health Dashboard** (Agent-Integritäts-Dasbhoard) wird angezeigt. Sie enthält Informationen zu den konfigurierten Agents in den Dashboard-Widgets.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Widget **Agents by Data Collection Status** (Agents nach Datenerfassungsstatus) gibt **Aus (manuell)** an, dass Agents manuell deaktiviert wurden (für Wartungsarbeiten oder zur Problembehandlung), und **Aus (automatisch)** bedeutet, dass Agents automatisch deaktiviert wurden (nachdem sie den Schwellenwert für die CPU-Auslastung überschritten hatten).

2. Klicken Sie auf das Pfeilsymbol zum Aktualisieren in der rechten oberen Ecke eines Widgets, um dessen Daten nach Bedarf zu aktualisieren.

   Sie können alle Widgets im Dashboard aktualisieren, indem Sie auf dieses Symbol im Formularheader klicken und dann **Aktualisieren** auswählen.

Agent-Funktionsmatrix anzeigen

Die Agent-Funktionsmatrix von Agent Client Collector zeigt die Verfügbarkeit von Agent Client Collector-Funktionen an. Die Matrix zeigt Daten in einem Diagramm und einer Tabelle an.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Agent-Funktionsmatrix zeigt die Granularität der Agent Client Collector-Funktionen an, die vollständig, teilweise und nicht unterstützt werden. Für ein teilweise unterstützte Funktion können Instanz- und Framework-Anforderungen erfüllt sein, sie wird jedoch unter mindestens einer Agent-Version ausgeführt, die die Funktionsanforderungen nicht erfüllt.

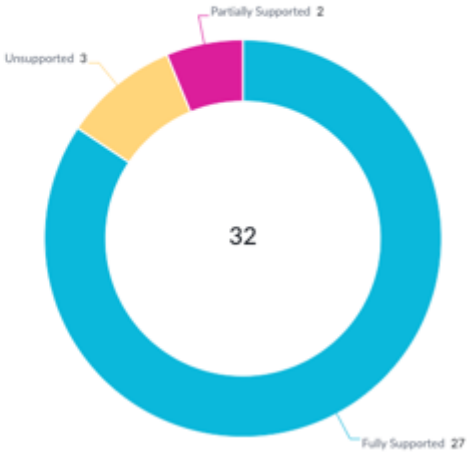
Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agenten-Funktionsmatrix**an.
   Die **Agent-Funktionsmatrix** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent-Funktionsmatrix

Agent Feature Matrix



Die Matrix zeigt den Support-Status von an Agent Client Collector Funktionen, die vollständig unterstützt, teilweise unterstützt und nicht unterstützt werden (nicht unterstützt).

2. Wählen Sie im Diagramm eine der Kategorien aus.
   Eine Liste aller Funktionen in der Kategorie wird auf der Seite **Agent Feature Support Status** (Status der Unterstützung von Agent-Funktionen) angezeigt.

Seite „Agent Feature Support Status“ (Status der Unterstützung von Agent-Funktionen)

sn_agent_feature_support_status 27

Last refreshed just now.

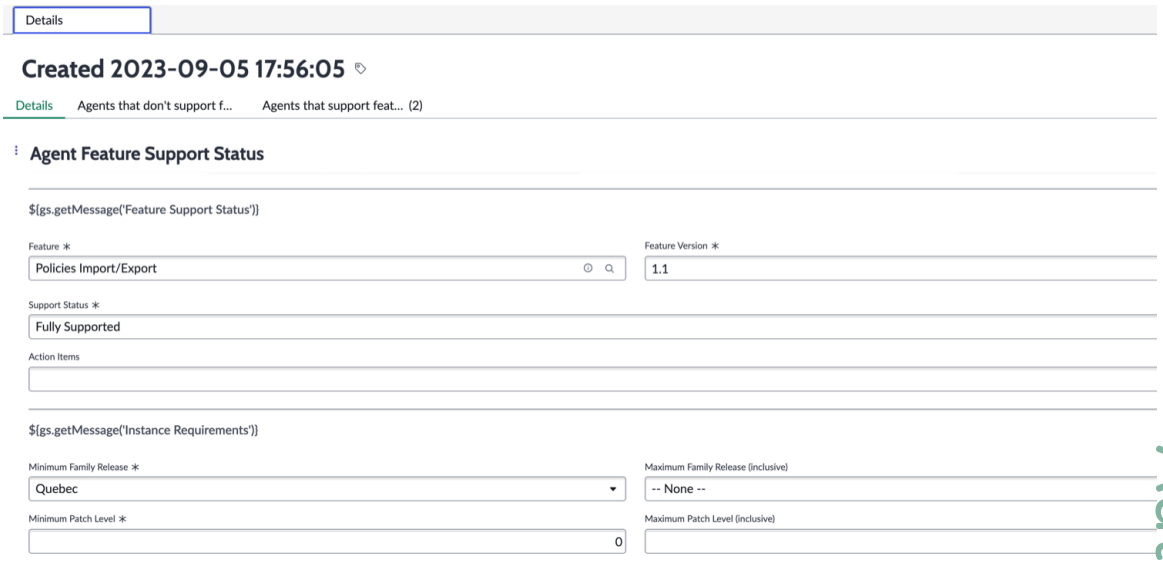
Feature	Feature Version	Support Status
OSQuery	5.7.0	Fully Supported
API Key	1.0	Fully Supported
Auto syncing certifications to agent	1.0	Fully Supported
Trigger MID selection when IP changes	1.0	Fully Supported
Policies Import/Export	1.1	Fully Supported
Allow List support per plugin	1.0	Fully Supported
Allow List	1.0	Fully Supported

3. Wählen Sie eine der Funktionen aus.
   Die Seite **Agent Feature Support Status** (Status der Unterstützung von Agent-Funktionen) wird für die spezifische Funktion angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite mit Details zum Status des Support-Service Desk-Mitarbeiters für Funktionen



Auf der Seite wird Folgendes angezeigt:

- Abschnitte, die den Supportstatus der Funktion und die verschiedenen Instanzanforderungen der Funktion angeben. Das Feld **Action Items** (Aktionselemente) zeigt die Aktionen an, die Sie ausführen müssen, um eine Funktion, die entweder teilweise oder nicht unterstützt wird, vollständig zu unterstützen.
- Instanzanforderungen und Agent-Framework-Versionsanforderungen, die von der Agent-Funktion erfüllt wurden.

Agent-Fehler anzeigen

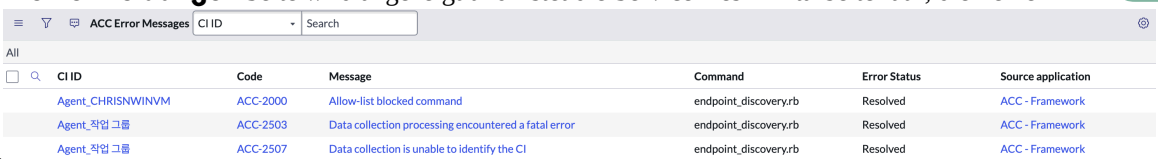
Agent Client Collector(ACC) Fehler sind in Protokollen im Zusammenhang mit dem Service Desk-Mitarbeiter und dem sichtbar ServiceNow Instanz. Diese Funktion bietet eine verbesserte Sichtbarkeit von Agent-Fehlern und ermöglicht eine schnellere Fehlerlösung.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agenten-Probleme**an.
   Die **ACC-Fehlermeldungen** Seite wird angezeigt und listet die Service Desk-Mitarbeiter auf, die Fehler enthalten.



   In den folgenden Spalten werden die angegebenen Informationen zu den Fehlern angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „ACC-Fehlermeldungen“

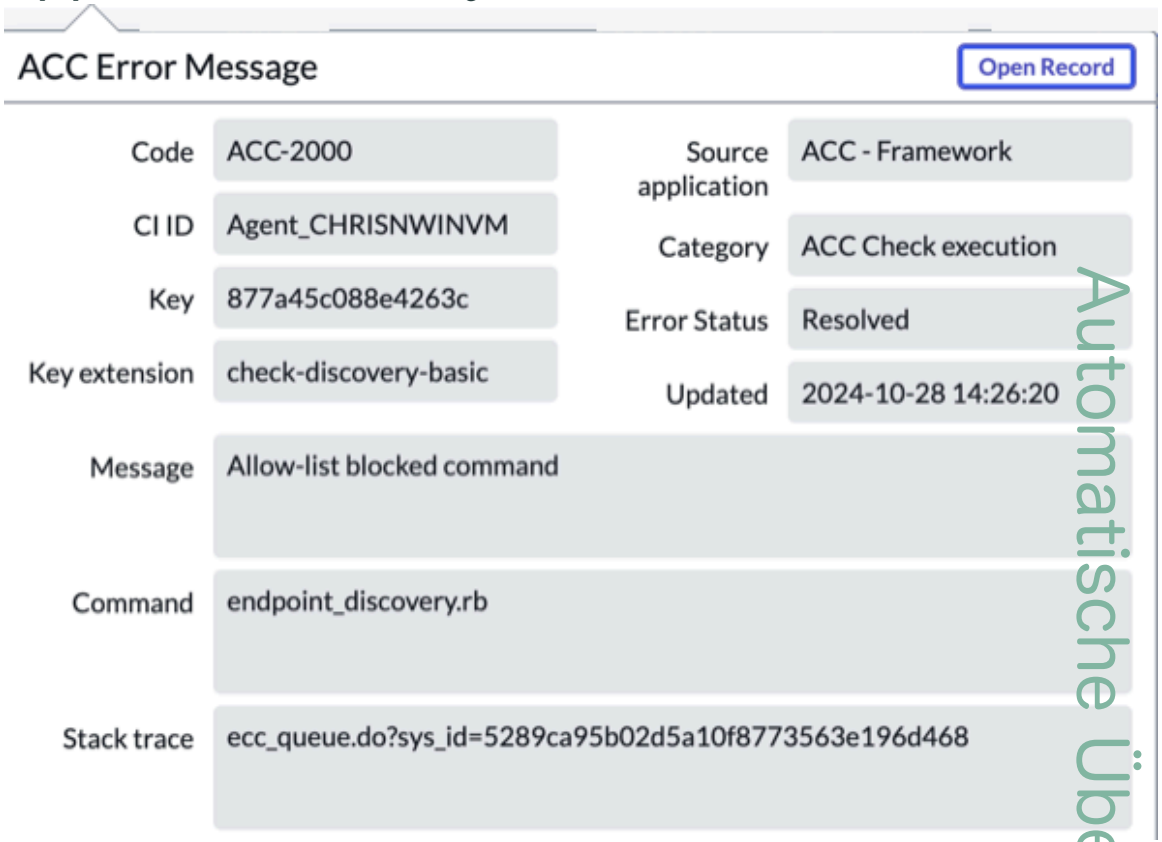
Spalte	Beschreibung
CI-ID	Der Name des Service Desk-Mitarbeiters, der den Fehler enthält, oder eines Konfigurationselements (Configuration Item, CI) mit einem Problem.
Code	Fehlercode, der dem Problem zugewiesen ist.
Nachricht	Eine Meldung, die den Fehler beschreibt.
Quellanwendung	Die Anwendung, die den Fehler auslöst.
Fehlerstatus	Gibt den Status des Fehlers an: **Aktiv** Oder **Gelöst** .
Kategorie	Die Fehlerkategorie, unter der der Fehler klassifiziert ist.
Schlüssel	Interner Wert, der zur Identifizierung des Fehlers verwendet wird. Gibt für Datensammlungsfehler an **Agent_ID** Wert.
Schlüsselerweiterung	Interner Wert, der zur Identifizierung des Fehlers verwendet wird. Gibt für Prüfungsausführungsfehler den Prüfungsnamen an.
Befehl	Der Befehl, der beim Auftreten des Fehlers ausgeführt wird (falls zutreffend).
Stack Trace	Ein Verweis auf **ecc_Queue** Datensatz, der verarbeitet wurde und den Fehler ausgelöst hat (falls zutreffend).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Nicht alle Spalten sind standardmäßig auf der Seite sichtbar.
- Wählen Sie das Infosymbol (ⓘ) Neben einem Fehler, um ein Popup-Fenster mit vollständigen Informationen zum Fehler anzuzeigen.

Popup-Fenster „ACC-Fehlermeldung“



Das Infosymbol ist sichtbar, wenn Sie den Mauszeiger unter das Suchsymbol ( ) Neben dem Fehlereintrag.

2. **Wahlweise:** So zeigen Sie Fehler für einen bestimmten Service Desk-Mitarbeiter an:

   a. Auswahlvorgang **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
   Die **Agent Client Collectors** Tabelle wird angezeigt.

   b. Wählen Sie einen HR-Mitarbeiter aus.

   c. Wählen Sie aus **Automatisierungsfehlermeldungen** Registerkarte unten auf der Seite, um Fehler im Zusammenhang mit dem Service Desk-Mitarbeiter anzuzeigen.

Ergebnis

Wenn ein Fehler dazu führt, dass die Registrierung eines Service Desk-Mitarbeiters fehlschlägt, wird dies der Fall **Status** Spaltenanzeigen **Registrierungsfehler** Auf der Seite „Agent Client Collectors“ (**Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**) an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Framework-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Agent Client Collector Framework-Listen und -Formularen.

Agent Client Collector -Benutzerrollen

Administratoren können Benutzerrollen zuweisen, um Zugriff auf Agent Client Collector zu gewähren. Die folgenden Standardrollen für das Agent Client Collector-Framework (ACC-F) sind in dem ServiceNow-System enthalten, auf dem Agent Client Collector installiert ist.

Agent Client Collector – Benutzerrollen

Rolle	Beschreibung
agent_client_collector_admin	Alle Berechtigungen für Agent Client Collector, einschließlich: • Zugriff auf REST-API • Richtlinien, Prüfungen, Agents und Websockets hinzufügen, bearbeiten und löschen • MID-Server-Verwaltung
agent_client_collector_integration	Zugriff auf REST-API
agent_client_collector_user	• Prüfungen und Richtlinien anzeigen • Zugriff auf einige REST APIs
evt_mgmt_admin	Startet den ACC-Listener

Standardprüfungen des Agent Client Collector-Framework

Das Agent Client Collector-Framework stellt mit dem Basissystem Standardprüfungen bereit.

Prüfungen

In der folgenden Tabelle sind die Standardprüfungen aufgeführt, die im Lieferumfang des Basissystem des Agent Client Collector-Framework vorhanden sind.

Typ	Name	Beschreibung	Befehl
Neu starten	restart	Startet den Agent neu. Die Prüfung ist standardmäßig aktiviert.	Agent neu starten
Discovery	check-discovery-basic	Führt eine Basiserkennung des Hosts des Agent durch, um Folgendes zu erkennen: • Host-CI, einschließlich IP-Adresse,	endpoint_discovery.rb

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Name	Beschreibung	Befehl
		Seriennummer und Hostname. • Laufende Prozesse (cmdb_running_process) des Hosts • TCP-Ports (cmdb_tcp) Die Überprüfung wird standardmäßig alle 12 Stunden (43.200 Sekunden) durchgeführt und läuft nach 600 Sekunden Inaktivität ab. Plugins: osquery, acc-f-commons, acc-f-modules	

Hinweis: Die Prüfungen `check-read-log` und `config-file-reader` sind nur für den internen Gebrauch bestimmt.

Agent Client Collector Leistung und Platzbedarf für URL-Überwachung

In den folgenden Tabellen werden die Performance-KPIs des Service Desk-Mitarbeiters und deren Stellfläche auf dem Host während der Ausführung der URL-Überwachung der Datensammlung auf verschiedenen Betriebssystemen angezeigt.

URL-Überwachungsprüfungen für einen Linux System

Linux Cent OS 8, 2 CPUs, 4 GB RAM					
Prüfungen pro Minute	100	250	500	1000	1500
Metriken (erwartet/ tatsächlich)	700/700	1750/1750	3500/3500	7000/7000	10500/10500
Netzwerknutzung – Tx (MID > Agent)	35 KB/s	78 KB/s	146 KB/s	286 KB/s	430 KB/s
Netzwerknutzung – Rx (MID < Agent)	15 KB/s	27 KB/s	51 KB/s	107 KB/s	116 KB/s
Netzwerknutzung – Tx (Service Desk-Mitarbeiter > MID)	8 KB/s	23 KB/s	37 KB/s	89 KB/s	113 KB/s
Netzwerknutzung – Rx (Service	28 KB/s	72 KB/s	142 KB/s	285 KB/s	426 KB/s

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

URL-Überwachungsprüfungen für einen Linux System (Fortsetzung)

Linux Cent OS 8, 2 CPUs, 4 GB RAM					
Desk-Mitarbeiter < MID)					
Arbeitsspeicherverbrauch	22 MB	25 MB	26 MB	34 MB	39 MB
CPU aller Prüfungen	~3 %	~7 %	~11 %	~21 %	~24 %
Verarbeiten Sie die CPU-Auslastung	1% - 1.5%	1.5% - 2.5%	5% - 6%	6% - 7%	12% - 13%
CPU-Auslastung des Hosts	~10 %	~19 %	~23 %	~45 %	~53 %

Agent Client Collector Gründe für Zertifikatwiderruf

In der folgenden Tabelle werden die möglichen Gründe für das Widerrufen von aufgelistet und beschrieben Agent Client Collector Zertifikat zum Anhalten der Kommunikation zwischen dem Service Desk-Mitarbeiter und ITOM Cloud-Services.

Gründe für Zertifikatwiderruf

Grund	Beschreibung
Nicht angegeben	Widerrufen Sie ein Zertifikat, ohne einen bestimmten Widerrufscode anzugeben. **Hinweis:** Dieser Ursachencode stellt keinen Audit-Pfad bereit, der angibt, warum ein Zertifikat widerrufen wurde.
Schlüsselkompromittierung	Sie vermuten, dass der private Schlüssel, der einem Zertifikat zugeordnet ist, gefährdet ist. Wenn beispielsweise ein Laptop gestohlen wird, der zu einem Anwender in Ihrer Organisation gehört, können alle auf dem Laptop gespeicherten privaten Schlüssel gefährdet werden.
CA-Gefährdung	Sie vermuten, dass der private Schlüssel einer Zertifizierungsstelle gefährdet wurde und sich in den Händen einer nicht autorisierten Person befindet. Wenn der private Schlüssel einer CA widerrufen wird, berücksichtigt die CA-Hierarchie auch alle Zertifikate unter dieser widerrufenen CA.
Zugehörigkeit geändert	Eine Person arbeitet nicht mehr in der Organisation, oder der Computeraccount, für den das Zertifikat ausgestellt wurde, wird nicht mehr verwendet. Kann auch verwendet werden, wenn eine Person die Rollen innerhalb einer Organisation ändert und nicht mehr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gründe für Zertifikatwiderruf (Fortsetzung)

Grund	Beschreibung
	das Zertifikat verwenden muss, das ihrer vorherigen Rolle zugeordnet ist. Beispielsweise könnte ein Mitarbeiter aus der Einkaufsabteilung wechseln und kein Zertifikat mehr benötigen, um Einkaufsanforderungen zu autorisieren.
Veraltet	Gibt an, dass ein neues Zertifikat anstelle eines zuvor ausgestellten Zertifikats ausgestellt werden muss. Wenn Sie beispielsweise eine Zertifikatvorlage aktualisieren und Zertifikate neu ausstellen, können Sie das vorherige Zertifikat mit diesem Ursachencode widerrufen.
Einstellung des Betriebs	Ein Server oder eine Workstation wird außer Betrieb genommen, und alle an den Server ausgestellten Zertifikate sind nicht mehr erforderlich. Sie können diesen Widerrufsgrund bei der Außerbetriebnahme einer CA verwenden.
Zertifikat halten	Ein temporärer Widerruf, der angibt, dass eine ZERTIFIZIERUNGSSTELLE ein Zertifikat zu diesem bestimmten Zeitpunkt nicht validiert. **Hinweis:** Die Verwendung dieses Ursachencodes macht es schwierig, festzustellen, ob ein Zertifikat zu einem bestimmten Zeitpunkt gültig war.
Aus CRL entfernen	Aktiviert das zukünftige Aufheben des Widerrufs des Zertifikats, indem das Zertifikat aus der Zertifikatwiderrufliste (Certificate Revocation List, CRL) entfernt wird.
Recht zurückgezogen	Der Zertifikatinhaber verfügt nicht mehr über die erforderlichen Berechtigungen, um das Zertifikat weiterhin zu verwenden.
AA-Gefährdung	Gibt die vermutete oder tatsächliche Gefährdung der im Zertifikat validierten Authentifizierungsstelle (Authentication Authority, AA) an.

Agent Client Collector Definitionsseite überprüfen

Die Felder, die beim Erstellen einer Prüfungsdefinition auf der Seite „Prüfungsdefinition“ konfiguriert werden sollen.

Formular „Check Definition“ (Prüfungsdefinition)

Feld	Beschreibung
Name	Beschreibender Name der Prüfung
Check Type (Prüfungstyp)	Wählen Sie den Typ der Prüfung aus. Die verfügbaren Überwachungsoptionen lauten wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition) (Fortsetzung)

Feld	Beschreibung
	• Events • Metriken
Aktiv	Aktivieren Sie diese Option, um die Prüfung zu aktivieren.
Is Proxy Valid (Ist Proxy-fähig)	Aktivieren Sie dies, um anzugeben, dass die Richtlinie der Prüfung so eingerichtet ist, dass diese als Proxy fungiert. Wenn diese Option in der Prüfinstanz angezeigt wird, ist sie schreibgeschützt.
Command Auto Generation (Befehl automatisch erstellen)	Wählen Sie diese Option aus, um den Befehl automatisch mit dem Wert **Command Prefix** (Befehlspräfix) und den Werten der Registerkarte **Parameter** zu generieren.
Command Prefix (Befehlspräfix)	Der Befehl, der für die automatische Generierung verwendet wird, wenn **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist. Das Präfix besteht aus einem beliebigen Teil des Befehls, der statisch ist (sich nicht ändert), z. B. der Skriptname.
Befehl	• Geben Sie den Befehl ein, den Agent Client Collector ausführt. **Hinweis:** Wenn das Kontrollkästchen **Command Auto Generation** (Befehl automatisch erstellen) aktiviert ist, wird dieses Feld mit dem Präfix und den Flags der aktiven Parameter ausgefüllt, die auf der Registerkarte **Parameter** angegeben sind. • Das Feld enthält Parameter aus einem oder mehreren der folgenden Elemente: ◦ Simple template (Einfache Vorlage): {{.labels.params_field_name}}: Übernimmt Werte aus Einträgen auf der Registerkarte **Parameter**. Beispielsweise bedeutet die Zeichenfolge {{.labels.params_warning}}, dass der Wert des Parameters *warning* verwendet wird (sofern er auf der Registerkarte **Parameter** konfiguriert wurde). ◦ Monitored CI (Überwachtes CI): {{.labels.params_ci_field_name}}: Übernimmt Werte automatisch aus dem überwachten CI, wobei field_name durch den exakten Namen des obligatorischen Felds in der CI-Tabelle ersetzt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition) (Fortsetzung)

Feld	Beschreibung
Konfigurationsdatendateien	Wählen Sie die Konfigurationsdatendateien aus, die heruntergeladen werden sollen, wenn die Prüfung ausgeführt wird.
Beschreibung	Beschreibung der Prüfung
Ausführungsmodus	Der Ausführungsmodus der Prüfung. Verfügbare Optionen sind: • *shell*: Zur Verwendung für Prüfungen, die nicht unterstützt werden *execv*. • *execv*: Bietet erhöhte Sicherheit während der Ausführung der Prüfung. Die Standardausführungsmodi sind: • Vorhandene Prüfungsdefinitionen: *shell* • Neue Prüfungsdefinitionen: *execv* • Wenn kein Wert in das Feld eingegeben wird: *shell* Wenn dieses Feld beim Upgrade auf Version 2,9 schreibgeschützt ist, stellen Sie sicher, dass Sie den schreibgeschützten Status deaktivieren, wie in beschrieben (KB1122498) artikel im Now Support Knowledge Base.
Intervall	Zeit in Sekunden, die zwischen Prüfungsausführungen gewartet wird. Ein Wert von 60 bedeutet beispielsweise, dass die Prüfung alle 60 Sekunden ausgeführt wird. Der angegebene Wert muss eine ganze Zahl sein.
Zeitüberschreitung	Die Zeit in Sekunden, nach der die Prüfungsausführung angehalten wird, wenn keine Ausgabe zurückgegeben wird. Ein Wert von 60 bedeutet beispielsweise, dass die Ausführung angehalten wird, wenn die Prüfungsausführung 60 Sekunden lang keinen Wert zurückgibt.
Schwellenwert für Event-Statusänderung	Anzahl der aufeinanderfolgenden Male, die der Antwortstatus einer Prüfung auftreten muss, bevor ein neues Event gesendet wird. Wenn dieser Wert beispielsweise auf 5 festgelegt ist, wird eine Prüfung durchgeführt, deren Antwortstatus sich von ändert **OK** Bis **Fehler** Generiert ein neues Ereignis mit einem **Fehler** Status erst nach dem fünften aufeinanderfolgenden Auftreten der Statusänderung. Nach dem Neustart eines Service Desk-Mitarbeiters wird immer ein erstes Ereignis gesendet. Standardwert: 5 (außer AWS Ereignisrichtlinien)
Schwellenwert für Reparatur des Ereignisstatus	Anzahl der aufeinanderfolgenden Male, die sich der Antwortstatus einer Prüfung verbessern muss, bevor ein neues Event gesendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition) (Fortsetzung)

Feld	Beschreibung
	Wenn dieser Wert beispielsweise auf 3 festgelegt ist, generiert eine Prüfung, deren Antwortstatus sich von **Fehler** in **OK** ändert, ein neues Event mit dem Status **OK** erst nach dem dritten Auftreten des Statuswechsels in Folge. Standardwert: 1 (außer AWS Ereignisrichtlinien)
Regulärer Ausdruck für Anmeldeinformationsfehler	Zeichenfolge in der Ausgabe der Prüfung, die angibt, dass die Prüfung aufgrund eines Fehlers in den Anmeldeinformationen fehlgeschlagen ist. Der Agent sucht dann weiter nach Anmeldeinformationen, die Teil des Anmeldeinformationsalias sind, bis die richtigen gefunden werden. Dieses Feld ist relevant (und obligatorisch), wenn die Richtlinie der Prüfung einen Anmeldeinformationsalias verwendet. Geben Sie die Zeichenfolge beim Erstellen einer neuen Prüfung manuell ein.
Plugins	Wählen Sie die Plugins aus, die mit der Prüfung verknüpft sein sollen. Anschließend werden die Plugins heruntergeladen, bevor die Prüfung ausgeführt wird.

Registerkarte „Prüfdefinitionsformularparameter“

Definitionen der Registerkarte Parameter für **Befehl** Feld im Prüfungsdefinitionsformular.

Registerkarte „Parameter“

Feld	Beschreibung
Name	Beschreibender Name für den Parameter
Default value / value (Standardwert/Wert)	Standardwert/Wert des Parameters
Aktiv	Boolescher Wert. Wenn der Parameter auf **true** gesetzt ist, wird er im Feld **Command** (Befehl) übernommen, sofern das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist.
Obligatorisch	Boolescher Wert. Bei Festlegung auf **true** muss ein Parameterwert angegeben werden, damit der Befehl ausgeführt werden kann.
Flagge	Zeichenfolge. Dieses Präfix wird im Feld **Command** (Befehl) vor dem Parameterwert eingefügt, wenn das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist.
Wert erforderlich	Boolescher Wert. Wenn der Parameter auf **true** gesetzt und das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist, wird der Wert dieses Parameters dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Parameter“ (Fortsetzung)

Feld	Beschreibung
	Feld **Command** (Befehl) hinter dem Wert im Feld **Flag** (Kennzeichnung) hinzugefügt.

Felder des Dialogfelds „Testprüfung“

Die Dialogfeldfelder beim Testen einer Prüfungsdefinition.

Felder des Dialogfelds „Testprüfung“

Feld	Beschreibung
Prüfungsdefinition	Zeigt den Namen der ausgewählten Prüfungsdefinition an
CI	Wählen Sie das CI aus, für das die Prüfung ausgeführt werden soll. Zur Auswahl verfügbar sind diejenigen CIs, die die beiden folgenden Kriterien erfüllen: • Gehören zu der im Feld **Check group** (Überprüfungsgruppe) angegebenen Gruppe • Gehört zu einem Service Desk-Mitarbeiter mit **Aktiv** Status. Wenn das Feld **Check group** (Überprüfungsgruppe) leer ist, wird der Standardwert **cmdb_ci_computer** eingetragen.
Berechtigungen	Wählen Sie die Anmeldeinformationen des Benutzers aus, mit dem der Agent eine Verbindung herstellen soll. Dieses Feld wird nur angezeigt, wenn Sie auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) in der Prüfungsdefinition sichere Prüfungsparameter konfiguriert haben.
Proxy Agent	Wählen Sie den Proxy-Agent aus, der der Prüfung zugeordnet werden soll. Dieses Feld wird nur angezeigt, wenn Sie mit einer Prüfungsinstanz arbeiten und eine der Optionen auf der Registerkarte **Proxy Settings** (Proxy-Einstellungen) in der Richtlinie der Instanz ausgewählt wurde.

Agent Client Collector Datensammlungseigenschaften

Beschreibung der Eigenschaften, die das Verhalten von bestimmen Agent Client Collector Datensammlung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensammlungseigenschaften

Eigenschaft	Beschreibung
sn_agent.host-data_collection_refresh_duration_seconds	Die Zeit (in Sekunden) zwischen Agent-Datensammlungen auf dem Host. Gilt nur, wenn dem Service Desk-Mitarbeiter kein Host-CI zugewiesen ist. Standard: 43200 (12 Stunden)
sn_agent.disco_minimum_threshold_for_rediscovery_in_minutes	Die Mindestanzahl von Minuten seit der letzten Endpunkt-Discovery für eine bestimmte IP vor Discovery Kann erneut ausgelöst werden. Diese Eigenschaft verhindert, dass Endpunkt-Discovery zu häufig ausgeführt wird, z. B. in Fällen, in denen ein Netzwerk zeitweise eine Pause hat oder ein Laptop wiederholt neu gestartet wird. Standardwert: 60
sn_agent.disco_disable_ci_clobber_of_agentless_disco	Verwenden Sie *true*, Gibt an, dass Daten, die von ServiceWatch- oder ServiceNow Discovery-Quellen erfasst werden, Vorrang haben Agent Client Collector Wenn der Schwellenwert in *sn_agent.disco_ci_clobber_of_agentless_disco_thre* wurde nicht überschritten. Standardwert: wahr
sn_agent.disco_ci_clobber_of_agentless_disco_threshold_days	Maximale Anzahl von Tagen, seit ein vorhandenes CI mit Agent-loser Discovery erkannt wurde, wobei das vorhandene CI verknüpft ist, anstatt vom Agent erneut erkannt zu werden. Tritt in Kraft, wenn *endpoint_disco_disable_ci_clobber_of_agentless_di* **Wahr** Und es sind mehr als 14 Tage (standardmäßig) vergangen, seit eine nicht-ACC-Discovery-Quelle (z. B. ServiceWatch oder ServiceNow) das CI erkannt hat. Nachdem dieser Schwellenwert überschritten wurde, kann Agent Discovery ein vorhandenes CI ausführen und überschreiben, unabhängig davon, ob das CI zuvor von einer nicht-ACC-Discovery-Quelle erkannt wurde. Dieser Prozess stellt die zuletzt erkannten Daten in der CMDB dar. Standard: 14
sn_agent.ci_prefers_ip_version	Gibt an, ob IPv4 oder IPv6 die bevorzugte Version ist, wenn ein IP-Adresswert im Feld IP-Adresse des CI-Datensatzes gespeichert wird. Standard: 4
sn_agent.ci_serial_number.pref_order	Geben Sie die Reihenfolge der Felder an, um einen Seriennummernwert zu finden, der in den Host-CIs gespeichert werden soll *serial_number*Feld während der Agent-Datensammlung. Werte müssen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensammlungseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	durch Kommas getrennt, ohne Leerzeichen und in Kleinbuchstaben angegeben werden. Standard: bios,System,UUID,Baseboard,Chassis
sn_agent.mac_ci_name_pref_order	Geben Sie die Reihenfolge der Werte an, nach der der CI-Datensatz festgelegt wird *Name*Feld wird während der macOS-Datensammlung ausgefüllt. Werte müssen durch Kommas getrennt, ohne Leerzeichen und in Kleinbuchstaben angegeben werden. Standard: Name,Hostname,Computer_Name,local_hostname
sn_agent.host_data_collection.disable_when_containerized	Wenn auf festgelegt *true*, Gibt an, dass die Datensammlung für containerisierte Agents deaktiviert ist. Standardwert: wahr

Agent Client Collector Eigenschaften der Richtliniensammlung

Beschreibung der Eigenschaften, die das Verhalten von bestimmen Agent Client Collector Richtliniensammlung.

Eigenschaften der Richtliniensammlung

Eigenschaft	Beschreibung
sn_agent.full_policy_calculation_cycle_days	Die Anzahl der Tage, bis eine Richtlinie einen vollständigen Berechnungszyklus erreicht. Wenn der letzte vollständige Berechnungszyklus der Richtlinie mehr als 7 Tage zurückliegt, wird die Richtlinie abgefragt, um ihren Berechnungszyklus vollständig zu berechnen. Standard: 7
sn_agent.max_number_of_monitored_cis_per_policy	Die maximale Anzahl überwachter CIs, die pro Richtlinie verarbeitet werden können. Standard: 400000
sn_agent.max_num_of_monitored_ci_to_process_with_agent	Die maximale Anzahl überwachter CIs, die mit Agents verknüpft sind und pro Richtlinie verarbeitet werden können. Standardwert: 1000
sn_agent.policy_force_recalc_interval_limit	Die Intervallgrenze in Minuten, die verwendet wird, um zu bestimmen, ob eine erzwungene Neuberechnung für Richtlinien erforderlich ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Richtliniensammlung (Fortsetzung)

Eigenschaft	Beschreibung
	Durch die erzwungene Neuberechnung werden sowohl die überwachten CIs einer Richtlinie als auch der entsprechende Agent neu verteilt. Standard: 10
sn_agent.policy_force_recalc_required	Wenn auf festgelegt *true*, Überprüft, ob eine erzwungene Neuberechnung für Richtlinien erforderlich ist. Durch die erzwungene Neuberechnung werden die überwachten CIs einer Richtlinie und der entsprechende Agent neu verteilt. Standardwert: wahr
sn_agent.populate_proxy_agent_monitored_ci	Wenn auf festgelegt *true*, füllt die überwachten CIs für bestimmte Richtlinien neu aus, um die Verteilung der CIs unter Proxy-Agents anzuzeigen. Standardwert: false

Agent Client Collector Framework Konfigurationseigenschaften

Beschreibung der Eigenschaften, die das Verhalten von bestimmen Agent Client Collector Framework Konfiguration.

Framework-Konfigurationseigenschaften

Eigenschaft	Beschreibung
sn_agent.agent_static_import_char_read_limit	Das Limit für Zeichen für ein bestimmtes Nutzlastelement. Bezieht sich nur auf das zu verarbeitende Konfigurationselement und nicht auf die Gesamtgröße des Anhangs. Standard: 1000000
sn_agent.agent_upgrade_wait_time	Maximale Anzahl von Minuten, für die ein Service Desk-Mitarbeiter vor dem Betreten erfolgreich ein Upgrade durchführen kann *Warning*Status. Standard: 30
sn_agent.agent_version	Die aktuelle ACC-F-Release-Version, die auf der Instanz installiert ist. Typ: Zeichenfolge
sn_agent.appl_classification_behavior	Die Merkmale und Verhaltensweisen für Anwendungen während der Agent-Discovery. Wenn auf festgelegt *simple*, Erstellt ein Shell-CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Framework-Konfigurationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	Standard: Einfach
sn_agent.auto_upgrade.enabled	Bei „wahr“ aktualisiert die Instanz automatisch vorhandene Agent Client Collector Installationen in der Version, die in der Eigenschaft „sn_Agent.Agent_Version“ festgelegt ist, wenn die Agent-Version niedriger als die Version der Eigenschaft ist. Typ: Boolesch Standardwert: false
sn_agent.auto_upgrade.max_upgrades_per_hour	Die maximale Anzahl von Agent Client Collector Upgrades möglich pro MID-Server Jede Stunde. Typ: Ganzzahl Standard: 50 **Hinweis:** Das Ändern dieses Werts kann sich negativ auf die Systemleistung auswirken.
sn_agent.auto_upgrade.max_upgrades_per_hour	Die maximale Anzahl von Agent Client Collector Upgrades für alle Service Desk-Mitarbeiter möglich MID Servers. Typ: Ganzzahl Standardwert: 1000 **Hinweis:** Das Ändern dieses Werts kann sich negativ auf die Systemleistung auswirken.
sn_agent.config_publish.max_payload_size	Die Größe in Byte, die die config_published_Payload im Warteschlangenthema „MonitoringProbe ECC“ erreichen kann, bevor ein Fehler protokolliert und die Nutzlast übersprungen wird. Standard: 15000000
sn_agent.ecc_queue.max_payload_size	Die maximal zulässige Nutzlastgröße für einen ECC-Warteschlangendatensatz, der vom Service Desk-Mitarbeiter verarbeitet werden soll. Standard: 5000000
sn_agent.enable_auto_mid_selection	Wenn auf festgelegt **Wahr** , Die Instanz sendet eine Liste von MID Servers An die Service Desk-Mitarbeiter. Dient zum Aktivieren der automatischen Auswahl von MID-Server Legen Sie in der Liste fest *auto-mid-selection*Eigenschaft auf „wahr“ in der ACC.yml-Datei des Service Desk-Mitarbeiters. Automatische Auswahl von MID Servers Stellt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Framework-Konfigurationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	sicher, dass jeder Service Desk-Mitarbeiter die effizienteste verfügbare verwendet MID-Server. Standardwert: false **Hinweis:** Diese Eigenschaft bestimmt nur, ob eine Liste von MID-Servern an den Agent gesendet wird. • Ob diese Eigenschaft zuvor auf festgelegt wurde **Wahr** Und wird dann auf festgelegt **Falsch** , Die automatische MID-Auswahl wird für den zuvor gesendeten durchgeführt MID-Server Listen Sie auf, wenn *auto-mid-selection*Eigenschaft ist auf festgelegt **Wahr** In der ACC.yml-Datei. • Wenn diese Eigenschaft auf festgelegt ist **Wahr** Und *auto-mid-selection*Eigenschaft in der ACC.yml-Datei ist auf festgelegt **Falsch** , Kein automatisches Element MID-Server Auswahl wird durchgeführt.
sn_agent.installer_max_endpoints	Maximale Anzahl von MID-Webserver Endpunkt-URLs, die während der einzeiligen Installation des Agent ausgewählt werden sollen. Standard: 3
sn_agent.keep_alive.alive_duration	Die Zeit in Sekunden, innerhalb der der Zeitstempel „Last_updated“ des Service Desk-Mitarbeiters aktualisiert werden muss. Nach diesem Zeitraum wird der Status des Service Desk-Mitarbeiters von verschoben *Up*Bis *Warning*. Wenn der angegebene Zeitraum erneut vergeht, wird der Status von verschoben *Warning*Bis *Down*. Standard: 120
sn_agent.keep_alive.disconnected_duration	Die Zeit in Sekunden, innerhalb der der Zeitstempel Last_Keepalive aktualisiert werden muss. Nach diesem Zeitraum ändert sich der Status des Service Desk-Mitarbeiters von *Up*Bis *Disconnected*. Standard: 600
sn_agent.logging.verbosity	Die Mindestanzahl von Nachrichten, die für protokolliert werden Agent Client Collector Framework. Nachrichten mit dem angegebenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Framework-Konfigurationseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	Status und schwerwiegenderen Elementen werden protokolliert. Optionen: • Fehler • warnen • Info • debuggen Standard: Info
sn_agent.max_sys_ids_in_query	Die maximale Anzahl von SYS-IDs, die während GlideRecord-Abfragen zurückgegeben werden sollen. Standard: 400000
sn_agent.maximum_mids_to_select	Die maximale Anzahl von MID Servers Die für das Service Desk-Mitarbeiter-Setup ausgewählt werden kann. Standard: 20
sn_agent.min_upgrade_history_per_agent	Die Mindestanzahl der pro Service Desk-Mitarbeiter gespeicherten Upgrades. Standardwert: 2
sn_agent.registration_key_validity.days	Die Anzahl der Tage nach der Erstellung eines Registrierungsschlüssels, in denen der Schlüssel gültig ist, bevor er gelöscht wird. Standard: 90
sn_agent.registration_key_notification.days	Die Anzahl der Tage vor dem Löschen des Registrierungsschlüssels, in denen eine E-Mail-Benachrichtigung an die Besitzgruppe des Schlüssels gesendet wird, die über die ausstehende Löschung informiert. Standard: 14
sn_agent.sync_filters_interval_min	Die Anzahl der Minuten, nach denen CMDB-Änderungen erkannt und dann mit synchronisiert werden MID-Server. Standard: 10
sn_agent.time_ago_in_seconds_to_query_ecc_queue	Bei der Verarbeitung von „ecc_Queues“ werden nur diejenigen abgefragt, die innerhalb der angegebenen Zeit (in Sekunden) erstellt wurden. Standard: 43200 (12 Stunden)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Datensammlungstabellen

Agent Client Collector Führt die Datensammlung basierend auf den bereichsbezogenen Apps durch, die Sie installiert haben. Agent Client Collector Framework Führt die Basisdatensammlung, und durch Agent Client Collector Visibility – Inhalt Führt eine erweiterte Datensammlung durch.

Die geplante Aufgabe „Hostdaten für Service Desk-Mitarbeiter aktualisieren“ erfasst stündlich Hostdaten auf Hosts, für die in den letzten 12 Stunden keine Datensammlung ausgeführt wurde. Der Auftrag erfasst die in den folgenden Tabellen beschriebenen Daten.

Agent Client Collector Framework-Datensammlung

Daten	CMDB-Feld
hostname	ci.name
Physischer Arbeitsspeicher	ci.RAM
Hardwarelieferant	ci.Hersteller
Hardwaremodell	ci.model_ID
CPU-Name	ci.cpu_type
BS-Domäne	ci.os_Domain
BS-Name	ci.os
BS-Version	ci.os_Version
IPv4-Adresse	ci.ip_address
Standard-Gateway	ci.default_gateway
Seriennummer	ci.serial_number
DNS-Name	ci.name
FQDN	ci.fqdn
TCP-Verbindungen	cmdb_tcp
Laufende Prozesse	cmdb_running_process
Seriennummern **Hinweis:** Beim Sammeln von Daten von Linux-Hosts `Dmidecode` Muss mit konfiguriert werden `Sudo` Berechtigungen zum Sammeln aller Seriennummern.	cmdb_serial_number

Agent Client Collector Visibility – Inhalt-Datensammlung

Daten	CMDB-Feld
CPU-Hersteller	ci.cpu_manufacturer
CPU-Geschwindigkeit	ci.cpu_Speed
BS-Arch	ci.os_address_width
CPU-Anzahl	ci.cpu_count
Anzahl der CPU-Kerne	ci.cpu_Core_count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Visibility – Inhalt-Datensammlung (Fortsetzung)

Daten	CMDB-Feld
CPU-Kern-Thread	ci.cpu_Core_Thread
Ist virtuell	ci.virtuell
Startdatum (Betriebszeit)	ci.Start_date
Objekt-ID	ci.object_ID
TCP-Verbindungen	cmdb_tcp
Laufende Prozesse	cmdb_running_process

Account-Befehle für LocalService, LocalSystem und GMSA während Windows Installation

Bei der Installation eines Service Desk-Mitarbeiters auf einem Windows Host mit einem LocalService-, LocalSystem- oder GMSA-Account. Sie müssen MSI-Befehle ausführen, um die Accounts zu aktivieren.

Account-Typbefehle

Kontotyp	Befehl
LocalSystem	msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="SYSTEM"
LocalService	msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="LOCALSERVICE"
GMSA	msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="DOMAIN\gMSA$"

Sicherstellen, dass die API mit einem Mitarbeiter verknüpft ist

Rufen Sie die API `AgentNowHandler.hasAgent` auf, um zu bestimmen, ob das CI einem Mitarbeiter zugeordnet ist. Die API ruft eine sys_id des CI ab und gibt ein true/false-Ergebnis zurück.

In der Methode `hasAgent()` wird eine sys_id des CI als Zeichenfolgenparameter verwendet. Sie gibt **true** zurück, wenn das CI eine der folgenden Bedingungen erfüllt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das CI ist sn_agent_cmdb_ci_agent, und dieser Agent ist aktiv.
- Das CI ist ein Host (der cmdb_ci_hardware erweitert), und es ist einem Mitarbeiter zugeordnet.
- Das CI ist eine Anwendung (die cmdb_ci_appl erweitert), und es besitzt eine Beziehung vom Typ „Wird-ausgeführt“ zu einem mit einem Mitarbeiter verknüpften Host.

Beispiel:

```
var agentNow = new sn_agent.AgentNowHandler();
gs.info('Agent assocation with CI? ' +
agentNow.hasAgent('158279505372b30034b8ddeeff7b1270'); // sys_id of agent
```

Konfigurationsdateioptionen

Optionen, die in verfügbar sind acc.yml Konfigurationsdatei.

Grundlegende Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei

Option	Typ	Standard	Beschreibung	Beispiel
name	Zeichenfolge	Agent_<Wert von *hostname*Befehl>	Der in der SN-Instanz registrierte Agent-Name kann vom Anwender angegeben werden. Das Ergebnis des Befehls „hostname“ wird als Standard verwendet.	Name: <Name des Service Desk-Mitarbeiters>
Back-End-url	Liste	wss://127.0,0.1:8800/ WS/Events	Liste der MID-Webserver-Endpunkt-URLs, mit denen kommuniziert werden soll. Wenn die Kommunikation nicht mit der ersten URL konfiguriert werden kann, wechselt das System zu den folgenden URLs, bis eine Verbindung hergestellt wird. Funktioniert, wenn Enable-Auto-Mid-selection=wahr	Back-End-url: <MID-Server-ip>:<websocket port>
api-Schlüssel	Zeichenfolge	<None>	API-Schlüssel, der von verwendet wird MID-Server Dient zur Authentifizierung eingehender Agent-Verbindungen. Wert	api-Schlüssel: <MID-Webserver-api-Schlüssel>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grundlegende Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			wird beim ersten Start des Service Desk-Mitarbeiters verschlüsselt.	
Anwender	Zeichenfolge	Administrator	Anwendername, der für die Standardauthentifizierung verwendet wird. Wenn dieser Parameter leer ist, startet der Service Desk-Mitarbeiter nicht.	`Anwender: „Agent-01“`
Passwort	Zeichenfolge	Administrator	Passwort, das für die Standardauthentifizierung verwendet wird. Wert wird beim ersten Start des Service Desk-Mitarbeiters verschlüsselt. Wenn dieser Parameter leer ist, startet der Service Desk-Mitarbeiter nicht.	`Passwort: <secure-password>`
log-level	Zeichenfolge	Info	Menge der Protokollierung, die in der Datei acc.log angezeigt werden soll. Werte: • Panic (Kritisch) • Schwerwiegend • Fehler • Warnen • Info • Debuggen	`Protokollebene: Debuggen`
allow-list	Zeichenfolge	/Etc/servicenow/Agent-Client-	Pfad zur JSON-Datei, die die Liste der Prüfungsbefehle	`Allow-list: /Etc/Agent/Check-allow-list.JSON`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grundlegende Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
		Collector/Check-allow-list.JSON	enthält, die der Agent ausführen kann. Kommentieren Sie diesen Parameter, um die Allow-Liste zu deaktivieren. Wenn dieser Parameter leer ist, wird die Allow-Liste deaktiviert.	
appl_classification_Behavior	Liste	Einfach	Gibt an, ob die Shell-CI-Erstellung für den Agent aktiviert werden soll. Mögliche Werte: • Einfach: Gibt an, dass die Shell-CI-Erstellung aktiviert ist. • Aus: Gibt an, dass für die Anwendung keine Shell-CIs erstellt werden. • Vollständig: Gibt an, dass abgeschlossen ist Discovery Der Anwendungs-CIs wird anhand von Mustern ausgeführt.	appl_classification_Behavior: Aus

Erweiterte Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei

Option	Typ	Standard	Beschreibung	Beispiel
Plugin-Signatur verifizieren	Boolean	True	Überprüft die Plugin-Signatur vor der Ausführung. Deaktivieren Sie	Verify-Plugin-Signature: Wahr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			diese Option, wenn Sie selbstsignierte Plugins oder Entwicklungs-Plugins verwenden.	
Unsicher-überspringen-tls-verifizieren	Boolean	Falsch	Bestimmt, ob das Zertifikat beim Herstellen einer Verbindung mit überprüft wird MID-Server.	`insecure-skip-tls-verify: false`
Aktivieren-Auto-MID-Auswahl	Boolean	True	Steuert die Funktion „Automatische MID-Auswahl“, um eine Verbindung mit dem optimal herzustellen MID-WebserverVon der Instanz bereitgestellt.	`Enable-Auto-MID-Auswahl: Wahr`
Check-command-bevorzugen-installiert	Boolean	Falsch	Gibt die Einstellung der ausführbaren Dateien an, die in ACC-Plugins bereitgestellt werden, oder der ausführbaren Dateien, die in der PFADVARIABLE des Hostsystems verfügbar sind. • Falsch = ACC-Plugins • Wahr = ausführbare Dateien in der PFADVARIABLE des Hostsystems	`Check-command-preferred-installed: Falsch`
powershell_installiert	Boolean	Falsch	Deaktiviert die Ausführung des powershell-Befehls für Agents.	`powershell-installiert: Wahr`
Allow-list-global-only	Boolean	Falsch	Auf festlegen **Wahr** Dient zur Verbesserung der Sicherheit, indem nur auf die Allow-	`Allow-list-global-only: Falsch`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			Liste gesetzt wird, die in definiert ist `allow-list`Parameter, den Sie während der Konfiguration angeben, wobei Allow-Listen ignoriert werden, die mit ACC-Plugins gebündelt sind.	
Assets deaktivieren	Boolean	falsch	Gibt an, ob eine Prüfung, die mit einer Asset-Abhängigkeit (Plugin) ausgeführt wird, ACC-Plugins aus dem abruft ServiceNow® Instanz oder verwendet eine Kopie der Plugins in ihrem Cache-Ordner. Wenn auf festgelegt **Falsch** , Zusätzliche Assets können während der Ausführung der Prüfung heruntergeladen werden. Auf festlegen **Wahr** Um die Sicherheit zu verbessern und sicherzustellen, dass während der Ausführung der Prüfung keine neuen Plugins heruntergeladen werden.	„Disable-Assets“: „Falsch“
Agent-Upgrade-url-path	Zeichenfolge	https://install.service-	Gibt einen alternativen	Agent-Upgrade-url-path:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
		now.com/glide/distribution/builds/package/app-signed/	Webserver-URL-Endpunkt zum Herunterladen von ACC-Installationspaketen beim Ausführen eines selektiven Upgrades an.	https://<ip address>:<port>/ACC_installers
Zertifikat-Rotation-days-out	Ganzzahl	28	Gibt die Anzahl der Tage vor Ablauf des Zertifikats an, die ein Service Desk-Mitarbeiter versucht, sein Zertifikat zu rotieren.	Certificate-Rotation-days-out=28
Aktivieren Sie-patterns-on-Agent	Boolean	falsch	Ermöglicht das Sammeln von Details zu den Anwendungen, die auf ausgeführt werden Agent Client Collector. Dieser Parameter ist nur bei Verwendung von erforderlich Agent Client Collector Für Musterausführung.	Enable-patterns-on-Agent: Wahr
Keepalive-Filter-nics	Boolean	wahr	Gibt an, ob Netzwerkschnittsteller Controller (NICs) nach dem Agent gefiltert werden (**Wahr**) Oder MID-Server(**Falsch**) Während der Keepalive-Aktion.	Keepalive-Filter-nics: Wahr
Keepalive-number_nics_per_ip_type	Ganzzahl	1	Gibt die maximale Anzahl von Netzwerkschnittsteller Controllern (NICs) pro IP-Typ (IP4, IP6) an, die mit einer Keepalive-Aktion gesendet werden.	Keepalive-number_nics_per_ip_type: 4

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die ACC.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			Die angegebene Nummer wird für jeden IP-Typ gesendet. Wenn der Wert beispielsweise 1 ist, werden maximal 2 NICs gesendet (jeweils 0-1 für IP4 und IP6). Wenn der Wert 4 ist, werden maximal 8 NICs gesendet (jeweils 0-4 für IP4 und IP6).	

PAC-Dateiparameter (Proxy Auto-Configuration)

Option	Typ	Standard	Beschreibung	Beispiel
pac-Datei	Zeichenfolge (Erforderlich)	„“ (leer)	Gibt den Speicherort der PAC-Datei an, die für die Proxy-Konfiguration verwendet werden soll. Kann entweder sein: • Ein lokaler Dateipfad (z. B.: Datei:///etc/Proxy/Proxy.pac) • Eine Remote-URL (z. B.: https://proxy.company.com/proxy.pac)	pac-Datei: „https://proxy.company.com/proxy.pac"
pac-Cache-ttl	Dauer (Optional)	30 m (30 Minuten)	Bestimmt, wie lange Proxy-Regeln aus der PAC-Datei im Arbeitsspeicher zwischengespeichert werden. Wenn Sie dies auf 0	pac-Cache-ttl: „1h“ # Cache für 1 Stunde

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PAC-Dateiparameter (Proxy Auto-Configuration) (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			festlegen, wird das Caching deaktiviert.	
pac-refresh-interval	Dauer (Optional)	30 m (30 Minuten)	Gibt an, wie oft der Service Desk-Mitarbeiter nach Updates für die PAC-Datei suchen soll. Nützlich, wenn die PAC-Datei Remote gehostet wird und regelmäßig aktualisiert werden kann.	pac-refresh-interval: „15 m“ # Prüfen Sie alle 15 Minuten auf Updates
pac-Dial-timeout	Dauer (Optional)	30s (30 Sekunden)	Gibt die Wartezeit an, die beim Herstellen einer Verbindung über einen Proxy-Server vor einer Zeitüberschreitung gewartet werden soll.	pac-Dial-timeout: Zeitüberschreitung für 10 Sekunden bei „10s“
pac-Reset-on-Connect-error	Boolean (Optional)	wahr	Bei „wahr“ löscht der Service Desk-Mitarbeiter den PAC-Cache und versucht, die PAC-Datei zu aktualisieren, wenn ein Proxy-Verbindungs-Proxy fehlschlägt. Dies hilft bei der Wiederherstellung von Proxy-Konfigurationsänderungen oder temporären Proxy-Problemen.	pac-Reset-on-Connect-error: Wahr

Synchronisierungseigenschaften für die Validierung Agent Client Collector Plugins

Verwenden Sie die folgenden Eigenschaften, wenn Sie öffentliche Zertifikate aus dem synchronisieren MID-Server Zu Agent Client Collector.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsynchronisierung: MID-Eigenschaften

Eigenschaft	Beschreibung
Mid.ACC.cert_Monitor_disable	Möglichkeit, die Synchronisierung der öffentlichen Zertifikate durch den Monitor zu deaktivieren. Standardwert: False
Mid.ACC.cert_Monitor_interval	Intervall (in Sekunden), in dem der Monitor öffentliche Zertifikate aus einer konfigurierten Endpunkt-URL synchronisiert. Standardwert: 86.400
Mid.ACC.cert_Monitor_target_url	Endpunkt-URL-Präfix (minus Dateiname), ab dem der Monitor öffentliche Zertifikate synchronisiert. Standardwert: ServiceNow Installieren Sie den Server
Mid.ACC.cert_Monitor_target_filename	Zieldateiname der Endpunkt-URL, ab der der Monitor öffentliche Zertifikate synchronisiert. Standardwert: SNCertificates.zip

Zertifikatsynchronisierung: Agent-Eigenschaften

Eigenschaft	Beschreibung
Ruft-Zertifikate-aus-MID ab	Status, der angibt, ob die öffentlichen Zertifikate aus abgerufen werden MID-Server Für Plugin-Asset-Validierung. Standardwert: True

Agent Client Collector Status

In der folgenden Tabelle werden aufgelistet und beschrieben Agent Client Collector Status.

Agent Client Collector-Status

Status	Beschreibung
In Betrieb	Service Desk-Mitarbeiter ist verbunden und funktioniert ordnungsgemäß.
Warnung	Agent wurde seit mehr als 2 Minuten nicht aktualisiert (basierend auf dem Wert der Eigenschaft „sn_Agent.Keep_alive.alive_duration“).
Ausgeschaltet	Agent ist heruntergefahren.
Wird neu gestartet...	Neustart des Service Desk-Mitarbeiters wird ausgeführt.
Wird aktualisiert…	Agent-Upgrade wird ausgeführt.
Verbindung getrennt	Service Desk-Mitarbeiter MID-Server Ist ausgefallen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Status (Fortsetzung)

Status	Beschreibung
Unbekannt	Service Desk-Mitarbeiter MID-Server Hat seit mehr als 10 Minuten keine Keepalive-Kommunikation gesendet (basierend auf dem Wert der Systemeigenschaft sn_Agent.Keep_alive.disconnected_duration).

Agent Client Collector-Protokollebenen

Die folgende Tabelle zeigt die verfügbaren Protokollebenen, die den Schweregrad von Agent Client Collector-Events angeben.

Protokollebene	Beschreibung
Panic (Kritisch)	Kritische Fehler, die dazu führen, dass der Service unerwartet beendet wird
Fatal (Schwerwiegend)	Schwerwiegende Fehler, die dazu führen, dass der Service heruntergefahren wird (Status 0)
Fehler	Nicht schwerwiegende Servicefehlermeldungen
Warnung	Warnmeldungen, die auf potenzielle Probleme hinweisen
Info	Informationsmeldungen, die Serviceaktionen darstellen
Debuggen	Detaillierte Meldungen zum Servicebetrieb, die bei der Problembehandlung helfen

Parameter für Agent Client Collector-Protokollrotation

Wenn Agent Client Collector-Protokolle zu groß werden, können sie Systemressourcen beanspruchen. Um die Systemeffizienz sicherzustellen, konfigurieren Sie Parameter in acc.yml Datei, mit der Abmeldungen aus dem Systemspeicher rotiert werden sollen (Windows-Standardspeicherort = C:\ProgramData\ServiceNow\Agent-Client-Collector\config\acc.yml . Linux-Standardspeicherort = /etc/servicenow/agent-client-collector/acc.yml).

Parameter für Protokollrotation

Parameter	Definition
log-file-and-stdout	Protokolle werden in die stdout-Datei geschrieben. Standardwert: **false**
Protokoll-Aufbewahrungsdauer	Maximales Alter in Tagen der Protokolldatei, bevor sie aus dem Systemspeicher rotiert wird. Standard: **3**
Protokollaufbewahrungsdateien	Maximale Anzahl von Protokolldateien, die gespeichert werden können, bevor sie aus dem System rotiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für Protokollrotation (Fortsetzung)

Parameter	Definition
	Standard: **3**
Log-max-size	Maximale Größe in MB der Protokolldatei, bevor sie aus dem Systemspeicher rotiert wird. Standard: **10**.
log-level	Protokollebene, die von den Protokollen gemessen werden soll. Available options are: **Panic, Fatal, Error, Warn, Info, Debug** (Kritisch, Schwerwiegend, Fehler, Warnung, Info, Debug). Standard: **Info** Die angegebene Protokollebene stellt die niedrigste Ebene der im Protokoll angezeigten Events dar. Beispiel: Einem Benutzer, der **Error** angibt, werden alle Events der Stufe „Error“ (Fehler) sowie schwerwiegende und kritische Events angezeigt.

Agent Client Collector-CPU-Schutzschwellenwerte

Wenn ein Service Desk-Mitarbeiter die konfigurierten Schwellenwerte erfüllt, die in den des Service Desk-Mitarbeiters angegeben sind acc.yml Datei, wechselt sie in den CPU-Schutzmodus, entweder für eine einzelne Prüfung oder für alle Prüfungen. Agents im CPU-Schutzmodus werden in den Agent-Protokollen mit der Syntax angezeigt Service Desk-Mitarbeiter .

Parameter	Beschreibung
agent_cpu_threshold_disabled	Um zu verhindern, dass sich der Service Desk-Mitarbeiter selbst abschaltet, wenn die CPU einen bestimmten Schwellenwert erreicht, legen Sie den Wert auf fest **Wahr** . Standard = False
cpu_percentage_limit	Prozentsatz der CPU-Nutzung durch den Agent, der den Agent in den CPU-Schutzmodus versetzt Standard = 5%
cpu_protection_behavior	Zuweisen **Einzelperson** Damit das System nur die einzelne Prüfung deaktiviert, die bestanden hat *cpu_percentage_limit*Wert. Wenn mehrere Prüfungen den Schwellenwert überschritten haben, wird die Prüfung mit der höchsten CPU deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
	Zuweisen **Alle** Um alle Prüfungen zu deaktivieren und die Datensammlung anzuhalten. Mögliche Werte: Alle, einzeln Standard: Alle
repeated_high_cpu_num	Anzahl der aufeinanderfolgenden Male, die der CPU-Verbrauch *cpu_percentage_limit* überschreiten muss, damit der Agent in den CPU-Schutzmodus wechselt Standard = 3
monitor_interval_sec	Gibt die Häufigkeit in Sekunden an, mit der die Agent-Überwachung ausgeführt wird, um zu überprüfen, ob *cpu_percentage_limit* überschritten wird Standard = 60

Agent Client Collector-Überwachung

Agent Client Collector-Überwachung Ermöglicht es Ihnen, Ihre Serviceverfügbarkeit zu überwachen, den Zustand und die Leistung Ihrer Umgebung zu überprüfen und sicherzustellen, dass Ihre Infrastruktur und ihre Anwendungen ordnungsgemäß ausgeführt werden.

Erste Schritte

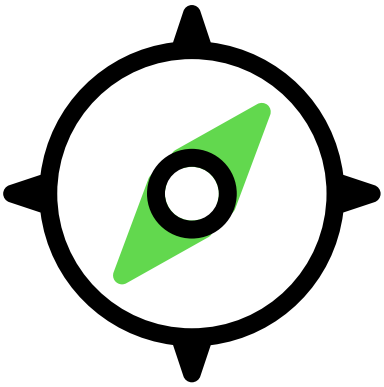
Hinweis:

Wenn auf den Geräten des Agent keine Prüfungen ausgeführt werden, befindet sich der Agent möglicherweise im CPU-Schutzmodus. Der CPU-Schutzmodus wird automatisch aktiviert, wenn der CPU-Verbrauch eines Geräts aus einem von zwei Gründen zu hoch ist: Entweder führt der Anwender zu viele Prüfungen aus, oder der Computer ist unzureichend ausgestattet. Wenn dies geschieht, ändert sich der Status „Datensammlung“ des Service Desk-Mitarbeiters in „aus“. ACC-F generiert ein Ereignis und zeichnet es in einem Protokoll auf. Informationen zum manuellen Fortsetzen der Datenerfassung durch den ACC-Service Desk-Mitarbeiter finden Sie unter Agent Client Collector-Datensammlung anhalten.

Der Anwender muss die Aktivität des ACC überwachen, um das Problem durch manuelles Eingreifen zu lösen, und dann die ACC-Erfassung erneut aktivieren. Informationen zum Einrichten der ACC-Überwachung finden Sie unter Agent Client Collector Monitoring auf dem MID-Server aktivieren.

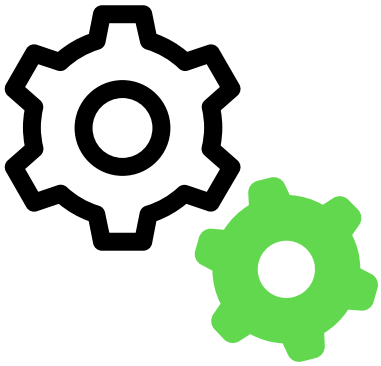
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



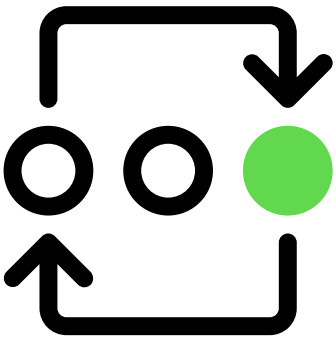
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen kennen, die der bietet Agent Client Collector-Überwachung Anwendungsangebote.

Konfigurieren



Konfigurieren Sie die zu aktivierenden Funktionen und Komponenten Agent Client Collector-Überwachung.

Metrikdaten

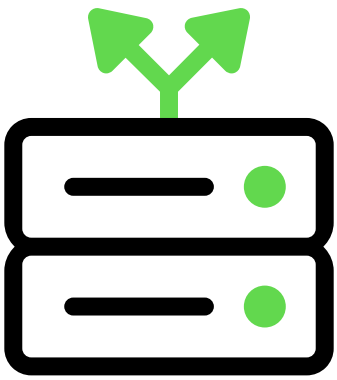


Verwenden Metrikdaten Um Metrikdaten zu erkunden und Anomalien zu identifizieren.

Arbeiten Sie mit Monitoring Technology Dashboard

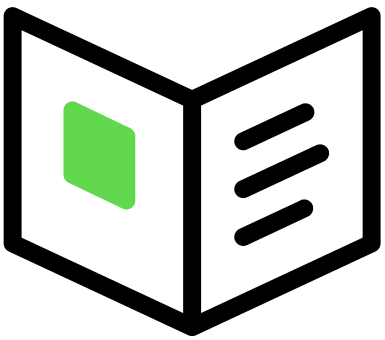
Überwachen Sie Serverressourcen nach Plattform.

Proxy-Agents verwenden



Überwachen Sie die Integrität und Leistung Ihrer Konfigurationselemente (Configuration Items, CIs), wenn der Agent außerhalb Ihres Hostservers bereitgestellt wird.

Referenz



Rufen Sie zusätzliche Details zu Prüfungen und Richtlinien sowie zur Metriksammlung ab.

Automatische Übersetzung

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum für Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Überwachung erkunden

Agent Client Collector-Überwachung Basiert auf einem Sensu-Framework, mit dem Sie Überwachungsprüfungen aus der Community übernehmen und erweitern können. Agent Client Collector-Überwachung Sammelt Daten zur Infrastruktur und zu installierten Anwendungen Ihres Unternehmens.

Agent Client Collector-Überwachung – Übersicht

Prüfungen und Richtlinien werden auf dem Client des Agent ausgeführt, um die relevanten Daten abzurufen, die gegebenenfalls in Events oder Metriken umgewandelt werden. Events und Metriken werden vom Agent über einen Metrikdaten MID-Server zur ServiceNow-Instanz gesendet und in der entsprechenden Datenbank gespeichert. Ein einzelner MID-Server kann mehrere Agents unterstützen (z. B. ACC-M und ACC-L). Wie Sie den MID-Server für Metrikdaten konfigurieren, erfahren Sie unter MID Server und verteilter MID Server-Cluster für Metric Intelligence.

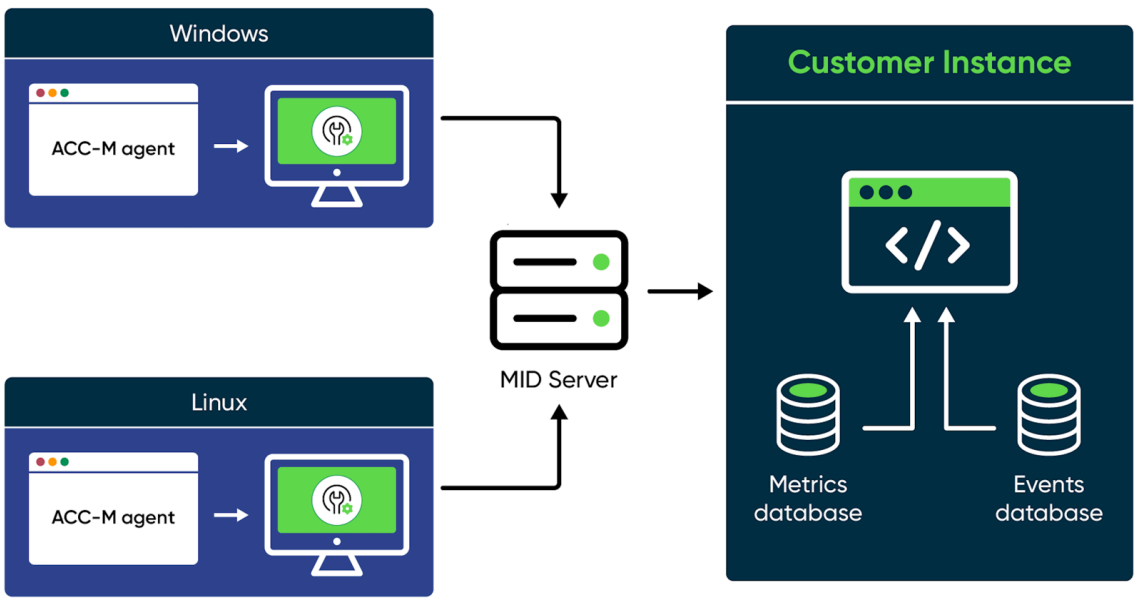
Agent Client Collector-Überwachung Im Lieferumfang enthalten Ereignismanagement-Plugin und erfordert auch die Installation von Request Metricbase (Clotho DB), wie in beschrieben Konfiguration von Metricbase (Clotho DB) anfordern (KB0816088) .

Für Details zu den mit installierten Plugins Agent Client Collector-Überwachung, Siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Agent Client Collector-Überwachung – Workflow

Die folgende Abbildung beschreibt das Layout und den Daten-Flow in Agent Client Collector-Überwachung Anwendung.

Überwachung der Serviceintegrität und -Verfügbarkeit mit ACC-M



Agent Client Collector-Überwachung – Vorteile

Vorteil	Funktion	Anwender
Überwachen Sie Protokolle, die Ereignisse nachverfolgen, die in auftreten Windows Umgebung	Windows Ereignisprotokollüberwachung	Agent Client Collector-Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

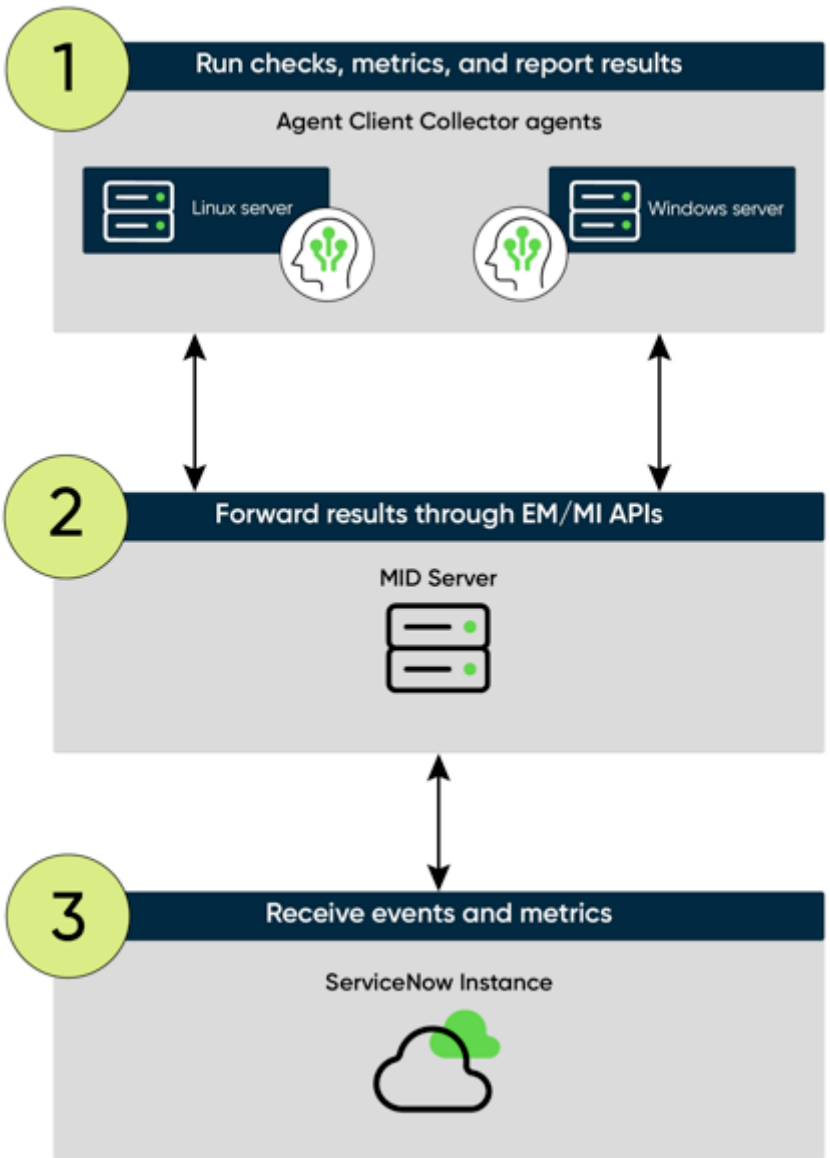
Vorteil	Funktion	Anwender
Überwachen Sie Betriebssysteme und Anwendungen	Betriebssystem- und Anwendungsüberwachung mit Agent Client Collector	Agent Client Collector-Administrator
Erfassen Sie Metriken für Hostdaten	Metrikdaten	Agent Client Collector-Administrator

Agentbasierter Datenfluss

Agent Client Collector sammelt Informationen zum Zustand des CI, für den der Agent installiert ist, und zu den Anwendungen, die auf den Hosts ausgeführt werden. Der Agent führt mehrere Prüfungen durch und übermittelt die Ergebnisse der Prüfungen an den MID-Server, wo sie in Events oder Metriken umgewandelt werden.

Events werden in der Events-Datenbank der Instanz und Metriken in der Metrikdatenbank gespeichert.

Die folgende Abbildung zeigt den Datenfluss von Agent Client Collector zur Instanz.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die nummerierten Einträge im Flow stellen Folgendes dar:

1. Die angegebenen Prüfungen werden für den Agent ausgeführt. Daten, einschließlich Metriken, werden an den MID-Server übermittelt.
2. Der MID-Server analysiert die Daten und klassifiziert die Ergebnisse als Events oder Metriken. Der MID-Server verwendet die REST API, um die Ergebnisse an die Instanz zu senden.
3. Die Instanz empfängt die Daten und speichert sie in der entsprechenden Datenbank.

Agent Client Collector-Überwachung – Anwendungsfall

Die Agent Client Collector-Überwachung Der Anwendungsfall zeigt, wie Organisationen eine einheitliche Überwachung in hybriden IT-Umgebungen erreichen können.

Anwendungsfallübersicht

Viele Unternehmen arbeiten heute in einer hybriden IT-Umgebung, in der einige Ressourcen lokal gehostet werden, während sich andere in der Cloud befinden. Diese Komplexität führt häufig zu einer fragmentierten Überwachung, was es schwierig macht, einen einheitlichen Überblick über die Integrität VON IT-Services zu erhalten. Agent Client Collector-Überwachung (ACC-M) schließt diese Lücke, indem ein umfassendes und konvergiertes Bild der Services der Organisation bereitgestellt wird, unabhängig davon, wo sie gehostet werden. ACC-M ist eine leichte Überwachungslösung, die sich nahtlos in die vorhandenen integrieren lässt ServiceNow Plattform.

Herausforderung

Ein IT-Betriebsteam hatte aufgrund der unterschiedlichen Infrastruktur Schwierigkeiten, die Serviceintegrität kohärent zu überwachen. Lokale Ressourcen wie Datenbanken und ERP-Systeme wurden mit traditionellen Methoden überwacht, während Cloud-Services über separate Überwachungstools verfügten. Diese Fragmentierung führte zu:

- Mangelnde Echtzeittransparenz in der allgemeinen Serviceintegrität.
- Verzögerte Problemerkennung und Fehlerbehebung.
- Mehrere Überwachungs-Dashboards, die die Komplexität für das IT-Team erhöhen.
- Schwierigkeiten bei der Korrelation von lokalen und Cloud-Warnungen, was zu Ineffizienzen führt.

Lösung

ACC-M ermöglicht einheitliche Echtzeittransparenz in einer hybriden IT-Umgebung. Es verbessert die betriebliche Effizienz, reduziert Ausfallzeiten und schafft eine resilientere IT-Infrastruktur, die sowohl lokale als auch cloudbasierte Services unterstützt.

ACC-M optimiert die Überwachung von lokalen und Cloud-Ressourcen in einer einzigen, einheitlichen Anzeige, indem die folgenden Lösungen angeboten werden:

Von ACC-M implementierte Lösungen

Lösung	Beschreibung	Ergebnis
Einheitliche Überwachung über Umgebungen hinweg	ACC-M erfasst Integritätsmetriken, Leistungsdaten und	Verbesserte Antwort:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ACC-M implementierte Lösungen (Fortsetzung)

Lösung	Beschreibung	Ergebnis
	Warnungsstatus sowohl von lokalen als auch von Cloud-Infrastrukturkomponenten. ACC-M verwendet schlanke Agents, die auf Servern, VMs und Cloud-Ressourcen installiert sind, um relevante Daten zu sammeln und Folgendes bereitzustellen: • CPU- und Arbeitsspeicherauslastung für lokale Server. • Netzwerkleistungsmetriken. • Verfügbarkeits- und Leistungsmetriken für Cloud-Services, z. B. Datenbanken und Speicher.	Mit einer einheitlichen Ansicht aller Ressourcen kann das IT-Betriebsteam schnell erkennen, wo Probleme auftreten, und sie basierend auf den gesamten Serviceauswirkungen priorisieren, wodurch die durchschnittliche Zeit bis zur Lösung (MTTR) reduziert wird.
Konvergierte Integritätsansicht	ACC-M bietet dem IT-Team des Unternehmens ein konvergiertes Integritäts-Dashboard innerhalb von ServiceNow Plattform, die Folgendes bereitstellt: • Eine einheitliche Ansicht sowohl der lokalen als auch der Cloud-Ressourcen. • Echtzeit-Updates zur Serviceintegrität, um sicherzustellen, dass Hybridservices gemeinsam und nicht isoliert überwacht werden. • Integrierte Einblicke in Serviceabhängigkeiten und Korrelation von Incidents, die sowohl lokale als auch Cloud-Systeme betreffen.	Proaktive Überwachung und Wartung: Die Echtzeit-Integritätsmetriken von ACC-M ermöglichen eine proaktive Überwachung von Services und vermeiden Ausfälle, indem Probleme identifiziert und gelöst werden, bevor sie eskalieren.
Hybrid-Warnungen und Automatisierung	Mit ACC-M können Sie automatisierte Warnungen sowohl für lokale als auch Cloud-Umgebungen einrichten und ihre Prozesse zur Reaktion auf Incidents optimieren. Wenn bei	Betriebliche Effizienz: Durch die Konvergenz von On-Premise- und Cloud-Überwachung in einer einzigen Plattform sind mehrere Überwachungstools

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ACC-M implementierte Lösungen (Fortsetzung)

Lösung	Beschreibung	Ergebnis
	einem Service in der Hybridumgebung ein Problem auftritt, führt ACC-M Folgendes aus: • Generiert automatisch Warnungen mit angereichertem Kontext, um zu identifizieren, ob das Problem auf die lokale Infrastruktur oder Cloud-Services zurückzuführen ist. • Löst automatisierte Workflows für die Korrektur basierend auf dem Warnungstyp aus, wodurch manuelle Eingriffe reduziert werden.	nicht mehr erforderlich. Dies reduziert die Komplexität und gibt IT-Ressourcen frei, um sich auf strategischere Aufgaben zu konzentrieren.
Visualisierung Der Serviceintegrität	Mit ServiceNow Mit der Servicezuordnung können Sie visualisieren, wie Services in der gesamten hybriden Infrastruktur erbringen. ACC-M speist dies mit kontinuierlichen Echtzeitdaten, wodurch das IT-Team Folgendes tun kann: • Verfolgen Sie Abhängigkeiten zwischen lokalen und Cloud-Services nach. • Identifizieren Sie potenzielle Fehlerpunkte, bevor sie sich auf das Geschäft auswirken. • Sehen Sie auf einen Blick, welche Services funktionsfähig, verschlechtert oder gefährdet sind, wo immer sie gehostet werden.	Verbesserte Geschäftskontinuität: Mit einem vollständigen Überblick über die Integrität der Hybridinfrastruktur kann DIE IT sicherstellen, dass kritische Business-Services betriebsbereit sind und ausgeführt werden, was die allgemeine Geschäftskontinuität verbessert.

Windows Ereignisprotokollüberwachung

Windows Die Ereignisprotokollüberwachung verfolgt, analysiert und verwaltet Ereignisprotokolle, die von verschiedenen generiert wurden Windows BS-Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Windows Die Richtlinie für Betriebssystemereignisse enthält die Prüfung os.windows.check-event-log, die misst Windows Ereignisprotokoll für Schwellenwerte, die in den Parametern der Prüfung angegeben sind. Weitere Informationen zu den konfigurierbaren Prüfparametern finden Sie unter Windows Filterparameter für Ereignisprotokoll.

Betriebssystem- und Anwendungsüberwachung mit Agent Client Collector

Die Überwachung von IT Operations Management (ITOM) für Agent Client Collector ist in der ServiceNow®-Instanz installiert. Dadurch werden das spezifische Betriebssystem und die Anwendungen überwacht, die auf dem Host-Computer installiert sind.

Agent Client Collector überwacht die folgenden Anwendungen.

ACC-Anwendungen

Betriebssystem/Anwendung	Konfigurationsbeschreibung
Windows	Keine spezielle Konfiguration erforderlich.
Linux	Keine spezielle Konfiguration erforderlich.
Apache HTTP Server	Weitere Informationen finden Sie unter Apache HTTP-Serverüberwachung mit Agent Client Collector konfigurieren.
Apache Tomcat	Weitere Informationen finden Sie unter Apache Tomcat-Überwachung mit Agent Client Collector konfigurieren.
IBM WebSphere	Keine spezielle Konfiguration erforderlich. Der Zugriff erfolgt über JMX. Standardverwaltungsport: **9100**.
IIS	Keine spezielle Konfiguration erforderlich.
JBoss/WildFly	Keine spezielle Konfiguration erforderlich. Standardport: **9990**. Informationen zur Fehlerbehebung finden Sie unter Leistungsüberwachung im Red Hat-Kundenportal.
Microsoft SQL Server	Keine spezielle Konfiguration erforderlich. Stellen Sie sicher, dass der Instanzname im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen.
My SQL	Keine spezielle Konfiguration erforderlich. Standardport: **3306**.
Oracle-Datenbank	Keine spezielle Konfiguration erforderlich. Stellen Sie sicher, dass der SID- und Oracle-Basispfad im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen. Standardport: **1521**.
Oracle WebLogic	Keine spezielle Konfiguration erforderlich. Der Zugriff erfolgt über einen JMX-Port. Standardport: **7001**. Stellen Sie sicher, dass der WebLogic-Basisparameter (wls_home) im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-Anwendungen (Fortsetzung)

Betriebssystem/Anwendung	Konfigurationsbeschreibung
	Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den **WebLogic**-Installationsverzeichnissen verfügt.

Wenn Sie die Anwendungen **Microsoft SQL Server**, **Oracle Database** und **Oracle WebLogic** verwenden, müssen Sie Discovery ausführen, um CI-Felder in der Instanz zu konfigurieren. Stellen Sie sicher, dass das Plugin Discovery (com.snc.discovery) installiert ist, um die Ausführung von Discovery zu ermöglichen.

Wenn die Anwendung auf einem anderen Port als dem Standardport ausgeführt wird, stellen Sie sicher, dass Sie die Portnummer in den Parametern der Prüfungsinstanz aktualisieren.

Apache HTTP-Serverüberwachung mit Agent Client Collector konfigurieren

Um Agent Client Collector für die Apache HTTP-Serverüberwachung zu konfigurieren, nehmen Sie in der Apache HTTP-Serveranwendung die folgenden Konfigurationen vor.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren Sie auf dem Host des Apache HTTP-Servers zu einem der folgenden Speicherorte:
   - In einer Linux-Umgebung:
     - /etc/httpd
     - /etc/httpd/conf
     - /etc/apache2
     - /etc/apache2/conf
   - In einer Windows-Umgebung: conf-Verzeichnis im Apache-Installationsverzeichnis
2. Suchen Sie entweder die Datei httpd.conf oder die Datei apache2.conf.
3. Stellen Sie sicher, dass die folgende Zeile keinen Kommentar enthält:
   LoadModule status_module modules/mod_status.so
4. Konfigurieren Sie den Port der Prüfungsinstanz so, dass er mit dem Port identisch ist, an dem Apache lauscht. (Der Standardport ist für beide **80**.)
5. Um eine sichere Verbindung zu gewährleisten, konfigurieren Sie SSL wie folgt:
   a. Stellen Sie sicher, dass die folgende Zeile keinen Kommentar enthält:
   LoadModule ssl_module modules/mod_ssl.so
   b. Aktivieren Sie den Parameter *ssl_secure_connection* in der Prüfungsinstanz.
   c. Konfigurieren Sie den Port der Prüfungsinstanz für sichere Verbindungen so, dass er mit dem Port identisch ist, an dem Apache lauscht. (Der Standardport ist **443**.)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Apache-Modul

Apache SLL/TLS, starke Verschlüsselung: Vorgehensweise

Apache Tomcat-Überwachung mit Agent Client Collector konfigurieren

Um Agent Client Collector für die Apache-Tomcat-Überwachung zu konfigurieren, nehmen Sie in der Apache Tomcat-Anwendung die folgenden Konfigurationen vor.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Öffnen Sie einen JMX-Verwaltungsport, wenn Sie den Server starten:

   a. In einer Linux-Umgebung:

      i. Erstellen Sie im Verzeichnis bin im Tomcat-Stammverzeichnis die Datei setenv.sh.

      ii. Stellen Sie sicher, dass die Datei Folgendes enthält:

```
export CATALINA_OPTS=$CATALINA_OPTS"
-Dcom.sun.management.jmxremote=true
-Dcom.sun.management.jmxremote.port={PORT NUMBER}
-Dcom.sun.management.jmxremote.rmi.port={PORT NUMBER}
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djava.rmi.server.hostname=127.0.0.1"
```

      iii. Führen Sie `chmod 755 setenv.sh` aus, um der Datei setenv.sh Ausführungsberechtigungen zuzuweisen.

   b. In einer Windows-Umgebung:

      i. Erstellen Sie im Verzeichnis bin im Tomcat-Stammverzeichnis die Datei setenv.bat.

      ii. Stellen Sie sicher, dass die Datei Folgendes enthält:

```
@echo=off
if defined CATALINA_OPTS (
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote=true
) else (
set CATALINA_OPTS=-
Dcom.sun.management.jmxremote=true
)
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.port={PORT NUMBER}
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.rmi.port={PORT NUMBER}
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.ssl=false
set CATALINA_OPTS=%CATALINA_OPTS% -
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Djava.rmi.server.hostname=127.0.0.1
```

{PORT NUMBER} entspricht der Nummer des Ports, den Sie für die JMX RMI-Überwachung öffnen. Der von der Prüfungsdefinition erstellte Standardwert lautet **9000**.

2. Starten Sie Tomcat neu.
   a. In einer Linux-Umgebung: Führen Sie zunächst das Skript shutdown.sh und dann das Skript startup.sh aus.
   b. In einer Windows-Umgebung: Führen Sie zunächst das Skript shutdown.bat und dann das Skript startup.bat aus.

Überwachen Sie HTTP-Punkte

Verwenden Sie **HTTP-Einstiegspunkte überwachen** Und **Überwachung von HTTP-Einstiegspunktmetriken** Richtlinien, die mit enthalten sind ITOM Zu überwachende bereichsbezogene App für Überwachung http Und https Einstiegspunkte und Einstiegspunkte-Metriken. Sie können diese Richtlinien nach Bedarf anpassen oder eine neue Richtlinie für die Überwachung von Serviceeinstiegspunkten konfigurieren.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Einstiegspunkt ist der Zugangspunkt für einen Service. In einer Agent Client Collector-Richtlinie geben Sie den zu überwachenden Service an. Die Einstiegspunkte des Service werden dann mithilfe der Richtlinie überwacht.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Wählen Sie eine der Richtlinien **Monitoring HTTP Entry Points** bzw. **Monitoring HTTP Entry Points Metrics** aus.
   Die entsprechende Seite **Policy - Monitoring HTTP Entry Points** wird geöffnet.
3. Auf der Registerkarte **Monitored CIs** (Überwachte CIs):
   a. Stellen Sie im Feld **Table** (Tabelle) sicher, dass die Datenbankansichts-Tabelle **sn_itmon_http_entrypoint** ausgewählt ist, damit Agent Client Collector HTTP- und HTTPS-Einstiegspunkte zur Überwachung abruft.
   b. Konfigurieren Sie im Abschnitt **Filter** einen Filter für die Services und Einstiegspunkte, die aus der Datenbankansichts-Tabelle **sn_itmon_http_entrypoint** übernommen werden sollen.
4. Klicken Sie auf die Registerkarte **Proxy Settings** (Proxy-Einstellungen), und wählen Sie den Proxy-Typ aus, den Sie für die Einstiegspunktüberwachung aktivieren möchten.
   - **Single proxy agent** (Einzelner Proxy-Agent): Wählen Sie diese Option aus, um die Überwachung eines einzelnen Agent zu aktivieren, den Sie im Feld **Proxy agent** auswählen, das nach Auswahl dieser Option eingeblendet wird.
   - **Multi-proxy agents by filter** (Mehrere Proxy-Agents durch Filter): Wählen Sie diese Option aus, um die Überwachung mehrerer Agents zu aktivieren. Konfigurieren Sie einen Filter im Abschnitt **Proxy Filter**, der nach Auswahl dieser Option eingeblendet wird, um nur die Agents zu überwachen, die mit den Filterbedingungen übereinstimmen.
   - **Script based proxy** (Skriptbasierter Proxy): Wählen Sie diese Option aus, um die Überwachung eines Agent basierend auf einem Skript zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen einen Proxy zum Ausführen einer HTTP-Richtlinie konfigurieren.

5. Klicken Sie auf die Registerkarte **Checks** (Prüfungen), und wählen Sie im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) die Option **HTTP** aus, um alle HTTP-Prüfungen in der Zelle **Available** (Verfügbar) anzuzeigen.
6. Wählen Sie die relevanten Prüfungen aus, und klicken Sie auf die Schaltfläche mit dem Rechtspfeil, um sie in die Zelle **Selected** (Ausgewählt) zu verschieben.
7. Aktivieren Sie das Kontrollkästchen **Active** (Aktiv) oben auf der Seite, um die Richtlinie zu aktivieren.
8. Klicken Sie auf **Aktualisieren**.
   Die Richtlinie überwacht die in den Konfigurationen der Richtlinie angegebenen Einstiegspunkte.

Agent Client Collector-Überwachung konfigurieren

Planen und konfigurieren Sie Ihre Agent Client Collector-Überwachung-Implementierung.

Zum Konfigurieren Agent Client Collector-Überwachung, Führen Sie die folgenden Schritte aus:

1. Konfigurieren Sie ein MID-Server Für die Arbeit mit Agent Client Collector-Überwachung.
2. Zu überwachende Metriken auswählen und konfigurieren.
3. Konfigurieren Sie die Aktionsebene für die Anomalieerkennung.
4. Regel für Konfigurationseinstellungen erstellen.
5. Erfassung und Auswertung von Metriken aktivieren.

Führen Sie je nach den Prüfungen und Metriken, die Sie überwachen möchten, die folgenden Aktionen aus, um die Aktivierung der vollständigen Prüfung und die Metriksammlung zu aktivieren:

1. Anzeige von HAProxy-Metriken aktivieren.
2. Aktivieren Sie die Ausführung von Lackprüfungen.
3. Wählen Sie aus Azure Richtlinien, die für die Metriksammlung aktiviert werden sollen.
4. Erstellen Azure Richtlinien für die Metriksammlung.

Konfigurieren Sie ein MID-Server Für die Arbeit mit Agent Client Collector-Überwachung

Verbinden Sie Service Desk-Mitarbeiter mit einem MID-Server Zum Aktivieren Agent Client Collector-Überwachung Funktionalität.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

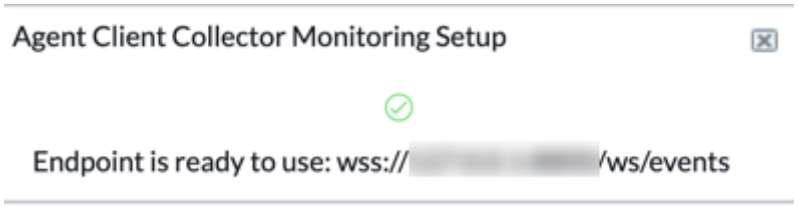
Für Details zur Konfiguration Agent Client Collector Informationen zur Protokollüberwachung finden Sie unter Agent Client Collector Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**an.
2. Wählen Sie aus MID-Server Dass Sie eine Verbindung zum Service Desk-Mitarbeiter herstellen möchten.
3. In **Zugehörige Links** Abschnitt auswählen **Richten Sie die ACC-Überwachung ein** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis
Ein Bestätigungsfenster wird angezeigt, das angibt, dass MID-Server Ist mit dem Service Desk-Mitarbeiter verbunden.



Zugehörige Informationen

Konfigurieren Sie mehrere MID Servers Für die Arbeit mit Agent Client Collector-Überwachung

Konfigurieren Sie mehrere MID Servers Für die Arbeit mit Agent Client Collector-Überwachung

Verbinden Sie Service Desk-Mitarbeiter mit mehreren MID Servers Zum Aktivieren Agent Client Collector-Überwachung Funktionalität. Mehrere MID Servers Kann sich gegenseitig durch Lastenausgleich und Domänentrennung unterstützen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Beim Konfigurieren mehrerer MID Servers, Verwenden Sie denselben Port für alle MID Servers. Wenn Sie verschiedene Ports verwenden, müssen Sie jeden hinzufügen MID-Server Einzeln, wie in beschrieben Konfigurieren Sie ein MID-Server Für die Arbeit mit Agent Client Collector-Überwachung.

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**an.
2. Aktivieren Sie die Kontrollkästchen, die dem entsprechen MID Servers Sie möchten eine Verbindung zu Ihrem Service Desk-Mitarbeiter herstellen.
3. In **Aktionen für ausgewählte Zeilen...** Fenster auswählen **Richten Sie die ACC-Überwachung ein** .
   Die Option enthält die Anzahl von MID Servers Aus der Anzahl der verfügbaren ausgewählt MID Servers. Beispiel: **ACC-Überwachung einrichten (7 von 8)** Gibt an, dass 7 MID Servers Wurden von 8 verfügbaren ausgewählt MID Servers.

Ergebnis
Ein Bestätigungsfenster wird angezeigt, das angibt, dass ausgewählt wurde MID Servers Sind mit dem Service Desk-Mitarbeiter verbunden.

Zu überwachende Metriken auswählen und konfigurieren

Metric Intelligence verwendet Datenquellen, die Hunderte von Metriken für alle CIs überwachen können. Wählen Sie für jeden Datenquelltyp aus, welche Details für welche CIs wichtig sind, und aktivieren oder deaktivieren Sie dann den entsprechenden Überwachungstyp, um die Menge der verarbeiteten Daten zu steuern.

Vorbereitungen
Unter Erste Schritte mit Metrikdaten finden Sie allgemeine Schritte zum Setup von Metrikdaten.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die SCOM-Datenquelle (standardmäßig verfügbar) erfasst etwa 400 Metriktypen von erkannten Geräten, z. B. „% verfügbarer Arbeitsspeicher“ und „% des freien Speicherplatzes“. Die Verarbeitung von Daten aus allen Metriktypen kann das System überlasten und die Leistung beeinträchtigen. Es kann erforderlich sein, ausgewählte Metriktypen für bestimmte CIs zu deaktivieren, um diese Last zu reduzieren.

Die Gesamtanzahl der Metriken, die verarbeitet werden können, hängt von der Anzahl der MID Server und deren Hardwarekonfiguration ab. Weitere Informationen zu Hardwareanforderungen und Skalierbarkeit von Metriken finden Sie unter MID Server und verteilter MID Server-Cluster für Metric Intelligence.

Hinweis: Die Einstellung `Active` („true“ oder „false“) für eine Metrik in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] hat Vorrang vor der Einstellung für die entsprechende Metrik in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map]. Wenn ein Metriktyp in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] deaktiviert ist, werden alle Datensätze, die sich auf die entsprechenden Metriken beziehen, aus der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] entfernt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Metriktypen**an.
   In der Liste **Überwachungssystemmetriken** werden die Metriktypen angezeigt, die pro Datenquelle und CI-Typ erfasst werden.
2. Prüfen Sie die Liste **Typen der Überwachungssystemmetrik**, und legen Sie den Wert in der Spalte **Aktiv** je nach Bedarf auf **false** oder **true** fest.

Spalte	Beschreibung
Quelle	Datenquelle, die den Metriktyp überwacht.
Typ der Quellmetrik	Metriken wie „% freier Speicherplatz“, die für den CI-Typ überwacht werden
Aktionsebene der Anomalie-Erkennung	Die Ebene der Verarbeitung und Analyse der Erkennung von Anomalien, die auf CIs und Metriken angewendet wird. Verfügbare Optionen: ○ **Nur Metriken**: Die Metriken aus der Datenquelle werden nur erfasst, ohne sie weiter zu verarbeiten. ○ **Grenzen**: Beinhaltet die Verarbeitungsebene „Nur Metriken“. Zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt. ○ **Anomaliepunktzahlen**: Beinhaltet die Verarbeitungsebene „Grenzen“. Zusätzlich werden Anomaliepunktzahlen berechnet und angezeigt. ○ **Anomaliewarnungen**: Beinhaltet die Verarbeitungsebene „Anomaliepunktzahlen“. Zusätzlich werden gegebenenfalls Anomaliewarnungen erzeugt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	○ **IT-Warnungen**: Beinhaltet die Verarbeitungsebene „Anomaliewarnungen“. Zusätzlich werden gegebenenfalls IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.
Typ des überwachten Objekts	CI-Typ, der überwacht wird.
Aktiv	Bestimmt, ob die Metrikdaten von Warnungszusammenfassungs- und RCA-Metriken von Ereignismanagement verarbeitet werden.
Einheit	Einheitentyp, der dem Quellmetriktyp zugeordnet ist und in den Berichten von Metric Intelligence angezeigt wird.

Konfigurieren Sie die Aktionsebene für die Anomalieerkennung

Mit einer Regel für Konfigurationseinstellungen können Sie die Ebene der Anomalie-Erkennungs-Verarbeitung und -analyse präzisieren, die für bestimmte CIs und Metriken angewendet wird. Legen Sie eine Verarbeitungsebene fest, die die Bedeutung der Metriken in den verschiedenen Phasen der Implementierung widerspiegelt, um bei Bedarf die Datenlast zu reduzieren.

Die Anomalie-Erkennung umfasst mehrere Verarbeitungsebenen. Auf der untersten Ebene werden Metrikdaten aus Datenquellen gesammelt. Auf der höchsten Ebene werden statistische Modelle erzeugt, Anomaliepunktzahlen berechnet sowie Anomalie- und IT-Alarme erstellt. Sie können den vollständigen Anomalie-Erkennungs-Prozess oder eine reduzierte Verarbeitungsebene für bestimmte Datenreihen anwenden.

Verwenden Sie die Konfigurationseinstellung von `anomaly_detection_action_level` in einer Regel für Konfigurationseinstellungen, um die Verarbeitungsebene für bestimmte CIs und Metriken festzulegen. Beispielsweise können Sie zunächst nur einen kleinen Prozentsatz von CIs und Metriken festlegen, um Anomaliewarnungen zu generieren, und diesen Prozentsatz später erhöhen.

Aktionsebenen

Die Konfigurationseinstellung für `anomaly_detection_action_level` bietet Aktionsebenen, die bei „Nur Metriken“ für die grundlegende Anomalieverarbeitung beginnen und bei „IT-Warnungen“ für die vollständige Verarbeitung und Analyse enden.

Aktionsebenen von der niedrigsten bis zur höchsten:

Nur Metriken

Es werden nur Metriken aus der Datenquelle ohne weitere Verarbeitung erfasst.

Grenzen

Die Verarbeitungsebene „Nur Metriken“ und zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt.

Anomaliepunktzahlen

Die Verarbeitungsebene „Grenzen“ und zusätzlich werden die Anomaliepunktzahlen berechnet und angezeigt.

Anomaliewarnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Verarbeitungsebene „Anomaliepunktzahlen“ und zusätzlich werden ggf. Anomaliewarnungen erzeugt.

IT-Warnungen

Die Verarbeitungsebene „Anomaliewarnungen“ und zusätzlich werden ggf. IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.

Zugehörige Informationen

Regel für Konfigurationseinstellungen erstellen

Regel für Konfigurationseinstellungen erstellen

Konfigurationseinstellungen wirken sich darauf aus, wie Metrikdaten verarbeitet werden. Konfigurationseinstellungsregeln überschreiben das standardmäßige Metrikverarbeitungsverhalten, um die Systemaktionen zu bestimmen, wenn eine Anomalie erkannt wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Reihe von Konfigurationseinstellungen bestimmen das Verhalten von Metrikdaten MID Servers. Im Basissystem werden diese Konfigurationseinstellungen mit Standardwerten, Datentypen und gültigen Wertebereichen konfiguriert. Sie können diese Konfigurationseinstellungen nicht direkt ändern oder neue hinzufügen. Sie können jedoch eine Metrikkonfigurationsregel mit neuen Konfigurationseinstellungen erstellen, die die Standardwerte auf den MID Servern überschreiben.

Wenden Sie diese Regeln dann manuell auf alle an Metrikdaten MID Servers In einem einzelnen Synchronisierungsvorgang oder verlassen Sie sich auf einen stündlichen Systemauftrag, um die Synchronisierung durchzuführen.

Um wirksam zu werden, Metrikdaten MID Servers Muss mit den Aktualisierungen der Konfigurationseinstellungsregeln synchronisiert werden.

Es ist zulässig, über mehrere Regeln für eine Einstellung zu verfügen, die sich auf dieselben CIs auswirken. In diesem Fall gilt Folgendes:

- Regeln, in denen ein Filter definiert ist, haben Vorrang vor einer globalen Regel, in der kein Filter definiert wurde.
- Wenn mehrere Regeln, die sich auf denselben CI-Satz auswirken, dieselbe Priorität haben, wird nur die zuletzt zu definierende Regel angewendet.
- Wenn mehrere Regeln mit unterschiedlichen Prioritäten denselben CI-Satz betreffen, werden Regeln mit der höchsten Priorität angewendet.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**an.
2. Klicken Sie im Bereich „Metrikkonfigurationsregeln“ auf **Neu**, und füllen Sie das Formular aus.

Formular „Metrikkonfigurationsregeln“

Feld	Beschreibung
Name	Regelname
Reihenfolge	Regelpriorität in allen anderen Regeln. Höhere Zahlen stehen für höhere Prioritäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Filtern nach	Kontrollkästchen zum Anzeigen des Felds **Regel**, in dem Sie Bedingungen angeben können, die CIs erfüllen müssen, damit die Regel angewendet wird. Beispiel: Wählen Sie in der Liste **Feld auswählen** den Eintrag **Add Related Fields (Zugehörige Felder hinzufügen)** aus, und fügen Sie dann den Filter **[Klasse][ist][Linux-Server]** hinzu. Wenn diese Option deaktiviert ist, gilt die Regel global für alle CIs in der Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map].

3. Klicken Sie mit der rechten Maustaste auf den Formulartitel, und wählen Sie **Speichern** aus.
4. Klicken Sie im Formularabschnitt „Überschriebene Konfigurationen der Metrik“ auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Formular „Überschriebene Konfigurationen der Metrik“

Feld	Beschreibung
Name	Konfigurationseinstellung, für die der Wert überschrieben werden soll. Klicken Sie auf das Symbol , um die Liste aller Konfigurationseinstellungen anzuzeigen. Klicken Sie auf das Symbol , um das Dialogfeld **Metrikeinstellungen** mit Details wie dem Bereich möglicher Werte anzuzeigen. Weitere Informationen zu Konfigurationseinstellungen finden Sie in den folgenden Tabellen („Konfigurationseinstellungen“ und „Interne Konfigurationseinstellungen“).
Regel	Regel, für die die erstellte Konfigurationseinstellung gilt
Wert	Neuer Wert, der den Standardwert für die angegebene Konfigurationseinstellung überschreibt.

Sie können die folgenden Konfigurationseinstellungen im Feld **Name** ändern.

Hinweis: Der in der Metrikkonfigurationsregel angegebene Filter gilt nicht für Einstellungen mit einem globalen Bereich.

Konfigurationseinstellungen

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
anomaly_detection_enabled Anomalie-Erkennung aktivieren/deaktivieren.	N/V	wahr	Boolean	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Hinweis: Wenn anomaly_detection_action_level festgelegt ist, wird anomaly_detection_enabled ignoriert.				
anomaly_detection_action_level Aktionsebene der Anomalieanalyse und -verarbeitung. Weitere Informationen finden Sie unter Konfigurieren Sie die Aktionsebene für die Anomalieerkennung.	Auswahlmöglichkeiten: ○ Nur Metriken ○ Grenzwerte ○ Anomaliepunktzahlen ○ Anomaliewarnungen ○ IT-Warnungen	○ Neue Datensätze: Grenzen ○ Aktualisierte Datensätze: Anomaliewarnungen	Auswahl	CI/Metrik
buffer_anomaly_eviction_size Maximale Anzahl von Anomalien auf individueller Metrikebene, die im internen Puffer gespeichert werden können, bevor sie für jedes CI/Metrik-Paar an die Instanz gesendet werden	60–1440	60	ganze Zahl	Global
buffer_ci_score_eviction_size Maximale Anzahl von Anomalien auf CI-Ebene, die im internen Puffer gespeichert werden können, bevor sie an die Instanz gesendet werden (aktuell nicht verwendet)	60–1440	60	ganze Zahl	Global
buffer_metric_eviction_size Maximale Anzahl von Metriken, die im internen Puffer gespeichert werden können, bevor sie für jedes CI/Metrik-Paar an die Instanz gesendet werden	60–1440	60	ganze Zahl	Global
connection_login_timeout_secs Maximale Zeit in Sekunden für die Anmeldung bei der	30–60	30	ganze Zahl	Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
lokalen Datenbank auf dem MID Server				
corrupt_data_count_threshold Mindestanzahl von Schulungspunkten (Durchschnitt: 15 Minuten), die für statistische Analysen erforderlich ist	10–100	30	ganze Zahl	Global
deprioritize_early_batching_of_anomalous_ci Senden Sie anomale CI-Informationen sofort oder in regelmäßigen Abständen.	N/V	falsch	Boolean	Global
mad_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, damit ein Modell auf Basis der mittleren absoluten Abweichung vom Median (Median Absolute Deviation, MAD) in Erwägung gezogen werden kann.	10–120	10	ganze Zahl	CI/Metrik
max_pool_connections_size Maximale Anzahl von Verbindungen für lokalen Datenbankpool	10–50	25	ganze Zahl	Global
observation_time_min Erwartetes minimales Beobachtungsintervall für Metrik	1–1440	1	ganze Zahl	CI/Metrik
robust_central_percentage Prozentsatz der Restdaten zur Berechnung der Reststandardabweichung für die Ausreißererkennung. Wenn auf 100 festgelegt, wird die Standardabweichung der regulären Stichprobe verwendet.	50–100	90	doppelt	Global
sparse_gap_fraction_threshold	0–100	50	doppelt	Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Wenn mehr als dieser Prozentsatz der Daten fehlt und keine andere Klasse identifiziert wurde, klassifizieren Sie sie als SPARSE. Versuchen Sie nicht, ein WEEKLY-Modell anzupassen.				
weekly_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, um nur eine WÖCHENTLICHE saisonabhängige Zerlegung zu berücksichtigen	14–90	15	ganze Zahl	CI/Metrik
daily_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, um nur eine TÄGLICHE saisonabhängige Zerlegung zu berücksichtigen	2–90	3	ganze Zahl	CI/Metrik
build_snpm_model Erstellung eines SNPM-Datenmodells aktivieren/deaktivieren	N/V	wahr	Boolean	CI/Metrik
snpm_minimum_data_count Mindestanzahl der Datenpunkte, die für die Erstellung eines stationären, nicht-parametrischen Modells erforderlich sind	0 – 1e9	5.000	ganze Zahl	CI/Metrik

Die folgenden Konfigurationseinstellungen sind für die interne Verwendung bestimmt.

Interne Konfigurationseinstellungen

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
anomaly_memory_time_min Anomaliepunktzahl-Rechnerparameter: Speicherzeit für anormale Situation	1–600	45	doppelt	CI/Metrik
excess_z_score	0–3	0,8	doppelt	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Anomaliepunktzahl-Rechnerparameter: Minimale Anomalie für Ausreißer akkumuliert				
linear_accumulator_threshold Schwellenwert der Entscheidungsstruktur: ACCUMULATOR-Analyse	0,5–5	1	doppelt	Global
low_freq_power_threshold Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	0–100	50	doppelt	Global
low_variability_threshold Schwellenwert der Entscheidungsstruktur: TRENDY-Analyse	0,0000000001–0,001	0,0001	doppelt	Global
mid_freq_power_threshold Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	0–100	33	doppelt	Global
multinomial_count_threshold Schwellenwert der Entscheidungsstruktur: MULTINOMIAL-Analyse	1–1000	40	ganze Zahl	Global
non_zero_diff_threshold Schwellenwert der Entscheidungsstruktur: NEAR_CONSTANT-Analyse	0–100	5	doppelt	Global
normal_memory_time_min Anomaliepunktzahl-Rechnerparameter: Speicherzeit für normale Situation	1–600	1	doppelt	CI/Metrik
normal_probability_ewma_timescale_min	1–600	15	doppelt	CI/Metrik

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Anomaliepunktzahl-Rechnerparameter: Normale Bewertungszeitskala				
normal_probability_weight Anomaliepunktzahl-Rechnerparameter: Anpassungsfaktor normale Bewertung	0–1	1	doppelt	CI/Metrik
sigmoid_offset Anomaliepunktzahl-Rechnerparameter: Konvertierung der Anomalie zu Punktzahl	0–5	2,1	doppelt	CI/Metrik
sigmoid_weight Anomaliepunktzahl-Rechnerparameter: Konvertierung der Anomalie zu Punktzahl	0–5	1,2	doppelt	CI/Metrik
tiny_variability_threshold Schwellenwert der Entscheidungsstruktur: NEAR_CONSTANT-Analyse	0–0,001	0,0000000001	doppelt	Global
weekly_peak_hi_limit Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	7–14	10	doppelt	Global
weekly_peak_lo_limit Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	0,5–7	0,7	doppelt	Global
weekly_vs_daily_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von WEEKLY größer als von DAILY sein muss, um das bevorzugte statistische Modell zu sein	100–1000	200	doppelt	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
daily_vs_noisy_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von DAILY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	20–1000	200	doppelt	CI/Metrik
weekly_vs_noisy_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von WEEKLY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	100–1000	200	doppelt	CI/Metrik
trendy_vs_noisy_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von TRENDY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	10–1000	50	doppelt	CI/Metrik
seasonal_loess_width_in_hours Wird auf die saisonale Komponente eines WEEKLY- oder DAILY-Modells angewendet, bevor eine Prognose für das zukünftige Verhalten erstellt wird. Wenn auf 0 festgelegt, wird jeder Datenpunkt im Saisonmodell unabhängig vom Rest der Datenpunkte.	6–24	12	doppelt	CI/Metrik
robustness Beeinflusst, wie Ausreißer zu saisonabhängigen und Trendberechnungen beitragen	N/V	wahr	Boolean	CI/Metrik
snpm_min_value_threshold Mindestwert der Daten, die zum Erstellen eines SNPM-Modells erforderlich sind	-1e9 – 1e9	0	doppelt	CI/Metrik
snpm_max_observation_interval_in_sec	60–600000	120	ganze Zahl	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Maximales erwartetes Beobachtungsintervall, das zum Erstellen eines SNPM-Modells erforderlich ist				
min_std_jump_fraction Mindestverhältnis des lokal berechneten Beobachtungsrauschpegels zur typischen Sprunggröße, das die Neuberechnung einer größeren Abweichung des Beobachtungsrauschens rechtfertigt	0,0–1,0	0,2	doppelt	CI/Metrik
dynamic_threshold_error_smoothing Ob der exponentiell gewichtete gleitende Durchschnitt verwendet werden soll, um die Reste in der dynamischen Schwellenwertanalyse zu glätten	N/V	wahr	Boolean	CI/Metrik
ewma_alpha Der Alpha-Wert des exponentiell gewichteten gleitenden Durchschnitts in der dynamischen Schwellenwertanalyse	1e-15–1,0	0,02739726027	doppelt	CI/Metrik
dynamic_threshold_beginning_smoothing_length Anzahl der geglätteten Datenpunkte, die auf den Mittelwert der doppelten Glättungslänge festgelegt werden soll	0–10.000	250	ganze Zahl	CI/Metrik
dynamic_threshold_error_buffer_minutes Anzahl der Datenpunkte um jeden Ausreißer, die gruppiert werden sollen	1–1000	30	ganze Zahl	CI/Metrik
dynamic_threshold_search_start Startwert, bei dem nach dem optimalen Steuerungsfaktor gesucht wird	0,5–20,0	3,0	doppelt	CI/Metrik

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
dynamic_threshold_search_interval Intervall zwischen Suchwerten des optimalen Kontrollfaktors	0,1–5,0	0,5	doppelt	CI/Metrik
dynamic_threshold_search_count Anzahl der Werte, die für die Suche nach dem optimalen Steuerungsfaktor erforderlich sind	1–50	19	ganze Zahl	CI/Metrik
dynamic_threshold_error_sequence_limit Maximale Anzahl von Fehlergruppen für einen bestimmten Steuerungsfaktorwert bei der Suche	1–20	5	ganze Zahl	CI/Metrik
dynamic_threshold_minimum_data_count Mindestanzahl der erforderlichen Rohdatenpunkte vor dem Versuch der dynamischen Schwellenwertbestimmung	1–10.000	5.000	ganze Zahl	CI/Metrik
linear_seasonal_log_likelihood_threshold Schwellenwert, der bei der Entscheidung verwendet wird, ob ein angepasstes Modell mit linearer Saisonalität einem Modell mit einer periodischen Komponente vorgezogen wird	10–5.000	1.000	ganze Zahl	CI/Metrik

Zugehörige Informationen

Konfigurieren Sie mehrere MID Servers Für die Arbeit mit Agent Client Collector-Überwachung

Regeln für Konfigurationseinstellungen synchronisieren

Die Konfigurationseinstellungsregeln für Metric Intelligence enthalten benutzerdefinierte Werte, die Standardwerte überschreiben, die derzeit auf MID Servern für Metric Intelligence vorhanden sind. Um wirksam zu werden, müssen die Metric Intelligence-MID Server mit dem Update Set der Konfigurationseinstellungsregeln synchronisiert werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Synchronisierung manuell initiieren, um die Aktualisierungen sofort auf alle Metric Intelligence-MID Server anzuwenden. Oder Sie verlassen sich auf einen Systemauftrag, der nach einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

stündlich wiederkehrenden Zeitplan ausgeführt wird und nach Updates für die Metrikkonfigurationsregeln sucht. Wenn festgestellt wird, dass Aktualisierungen vorhanden sind, sendet der Systemauftrag diese Aktualisierungen an die Metric Intelligence-MID Server.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagementregeln** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**an.
2. Klicken Sie im Bereich „Metrikkonfigurationsregeln“ auf **Mit MID synchronisieren**.

Nächste Maßnahme

Stellen Sie sicher, dass alle Metric Intelligence-MID Server mit dem aktualisierten Satz der Konfigurationseinstellungsregeln synchronisiert wurden:

1. Navigieren zu **Ausgabe und Artefakte** > **ECC-Warteschlange**an.
2. Suchen Sie im Bereich **Warteschlangen** in der Spalte **Themen** nach `MetricConfigProbe`.
3. Überprüfen Sie die Spalte **Agent** und stellen Sie sicher, dass alle MID Server aktualisiert wurden.

Erfassung und Auswertung von Metriken aktivieren

Zum Aktivieren von ServiceNow Instanz zum Sammeln und Auswerten von Metriken müssen Sie eine verteilte erstellen MID-Server Cluster, zuordnen MID Servers Mit dem Cluster und aktivieren Metrikdaten Für Ihren MID-Server.

Vorbereitungen

Stellen Sie sicher, dass in Ihrer Instanz die folgenden Plugins installiert sind:

- Ereignismanagement (com.glideapp.itom.snac)
- Metrikdaten – Com.snc.sa.metric-Plugin
- MetricBase

So überprüfen Sie, dass das Plugin MetricBase ordnungsgemäß installiert wurde:

1. Geben Sie im Instanznavigationsbereich `stats.do` ein.
2. Suchen Sie nach dem Abschnitt mit den **MetricBase-Statistiken**, und stellen Sie sicher, dass Folgendes angezeigt wird:
   - Status: ONLINE
   - Name: clotho

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Erstellen Sie eine verteilte MID-Server Cluster in Ihrer Instanz:

   a. Navigieren zu **MID-Server** > **Cluster**an.
   Die MID-Server Die Seite „Cluster“ wird geöffnet und zeigt die Liste der konfigurierten an MID-Server Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Klicken Sie auf **Neu**.
Die Seite **MID Server-Cluster – Neuer Datensatz** wird geöffnet.

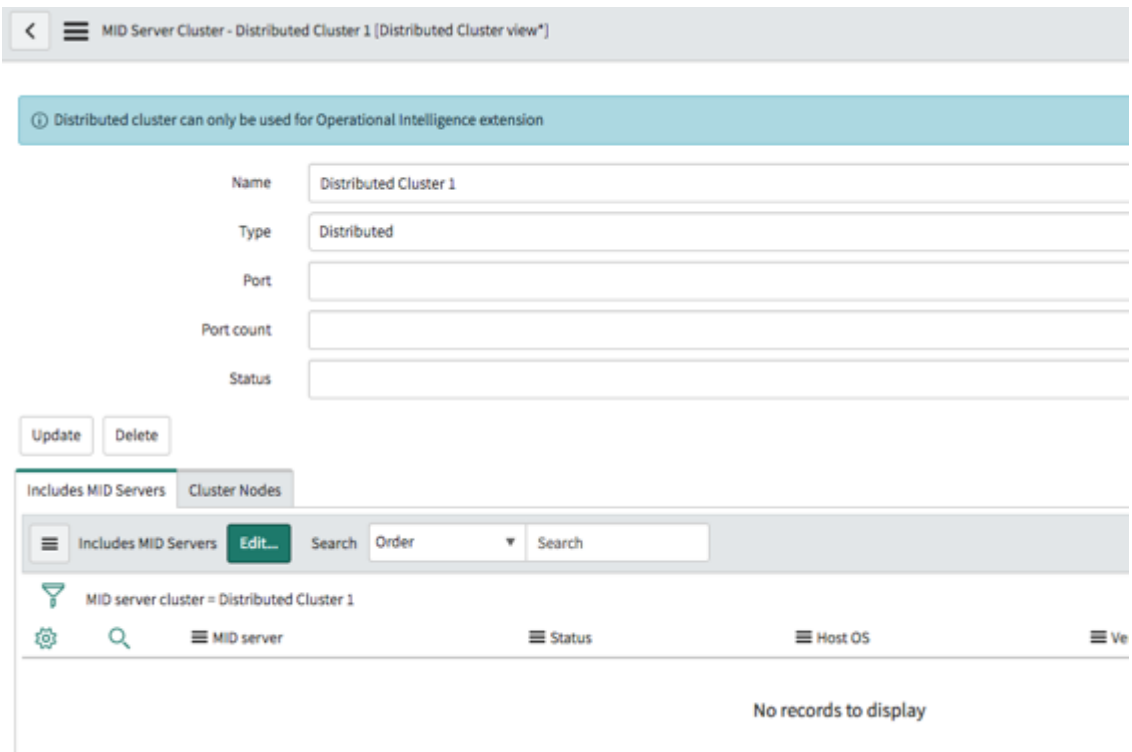
c. Weisen Sie im Feld **Name** einen beschreibenden Namen für das Cluster zu.

d. Wählen Sie im Feld **Typ** die Option **Verteilt** aus.

e. Klicken Sie auf **Absenden**.
Verteilt MID-Server Wird in angezeigt MID-Server Seite „Cluster“.

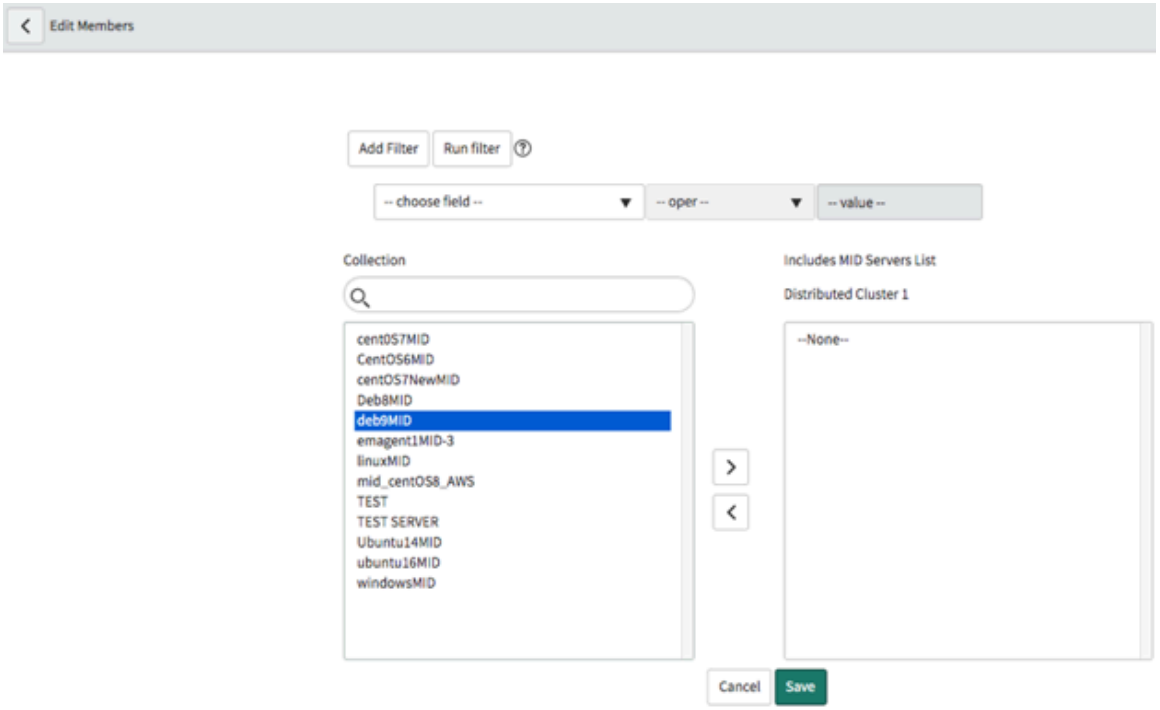
2. Zuweisen MID Servers An verteilt MID-Server Cluster:

a. Auf der MID-Server Seite „Cluster“ wählen Sie verteilt aus MID-Server Cluster.
Die folgende Seite wird angezeigt:



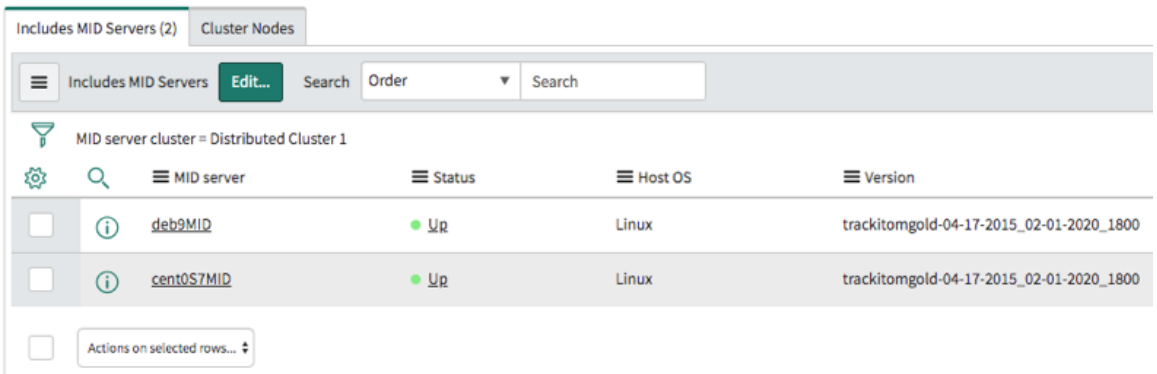
b. Klicken Sie auf der Registerkarte **Enthält MID Server** auf **Bearbeiten**.
Die Seite **Mitglieder bearbeiten** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Wählen Sie das entsprechende aus MID Servers Klicken Sie in der linken Zelle auf die Pfeilschaltfläche nach rechts Um sie in die rechte Zelle zu verschieben.
In einer Staging-Umgebung ist es akzeptabel, mit nur einem MID-Server im Cluster zu arbeiten.

d. Klicken Sie auf **Speichern**.
Die **Enthält MID-Server** Auf der Registerkarte wird angezeigt MID Servers Die Teil des Clusters sind.

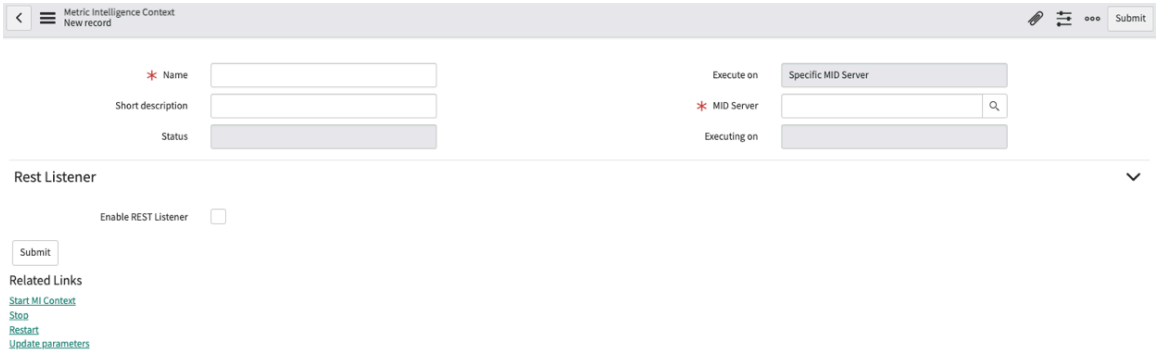


3. Aktivieren Metrikdaten Für Ihren MID-Server:

a. Navigieren zu **MID-Server** > **Erweiterungen** > **Metrikdaten**an.
Die Seite **Metric Intelligence Metrics Contexts** (Metric Intelligence-Metrikkontexte) wird angezeigt.

b. Klicken Sie auf **Neu**.
Die Seite **Metric Intelligence Contexts - New record** (Metric Intelligence-Kontexte – Neuer Datensatz) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Metrikdaten-Metrikerweiterung ein.

d. In **MID-Server** Wählen Sie das Feld aus MID-Server Dem Sie zuordnen möchten Metrikdaten Metrikerweiterung.

e. Wählen Sie aus **ACC dedizierter MID** Kontrollkästchen zum Zuweisen des angegebenen MID-Server Nur als MID-Server Im verteilten Cluster.
Durch Auswahl dieser Option sparen Sie Systemressourcen und -speicher.

f. In **Zugehörige Links** Klicken Sie unten auf der Seite auf **Start**an.
Eine Meldung mit dem Status der Erweiterung wird angezeigt.

g. Klicken Sie auf **Absenden**.

h. Klicken Sie auf **Start**.

Zugehörige Informationen

Erfassung und Auswertung von Metriken beschränken

Erfassung und Auswertung von Metriken beschränken

Sie können die Metriken beschränken, die der MID-Server an die Instanz sendet, indem Sie entweder ein bestimmtes CI oder einen kompletten CI-Typ deaktivieren.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

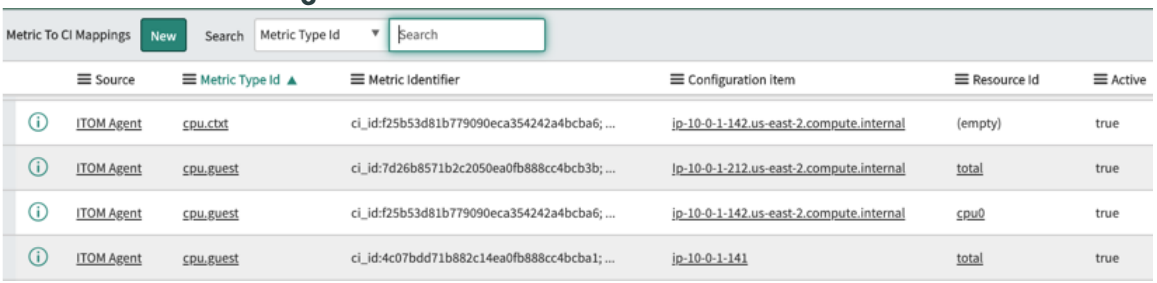
1. So beschränken Sie die Sammlung und Auswertung von Metriken für bestimmte CIs:

a. Navigieren zu **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**an.
Die Seite **Metrik-Zuordnung an CIs** wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrik-Zuordnung an CIs



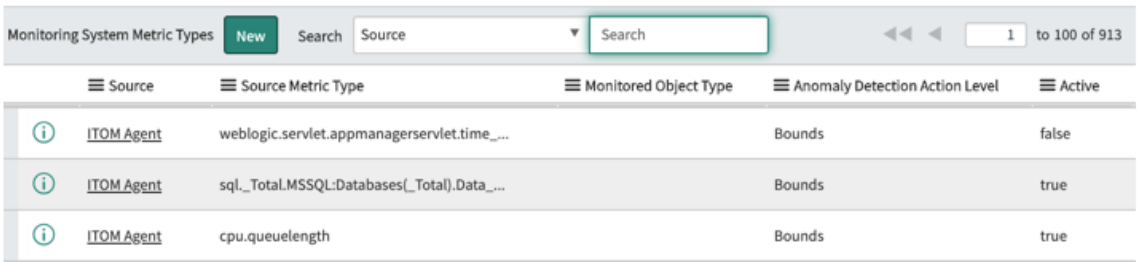
Hinweis: Die Zuordnung der Metrik zum CI wird sowohl anhand der Metrik-ID als auch durch das Konfigurationselement identifiziert.

b. Um zu verhindern, dass Metriken für eine bestimmte Metrik und ein bestimmtes CI gesendet werden, legen Sie den Wert der Spalte **Aktiv** auf **false** fest.

2. So beschränken Sie die Sammlung und Auswertung von Metriken für einen kompletten CI-Typ:

a. Navigieren zu **Ereignismanagement** > **Anomalie-Erkennung** > **Metriktypen**an.
Die Seite **Typen der Überwachungssystemmetrik** wird angezeigt.

Typen der Überwachungssystemmetrik



b. Um zu verhindern, dass Metriken für einen Metriktyp gesendet werden, legen Sie den Wert der Spalte **Aktiv** auf **false** fest.

Blockereigniserstellung für nicht vorhandene Entitäten

Rufen Sie auf `skip_events_for_nonexistent`Parameter zum Blockieren der Ereigniserstellung, wenn ein bestimmter Prozess, Service oder Protokoll nicht vorhanden ist. Rufen Sie diesen Parameter auf, wenn Sie nicht über diese nicht vorhandenen Entitäten benachrichtigt werden möchten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Prozess, Service oder Protokoll ist nicht vorhanden, wenn die folgenden Prüfungen keine gültigen Werte für die angegebenen Parameter enthalten:

Parameter überprüfen

Überprüfen	Parameter
os.linux.check-process	`file_pid`, `daemon_name`
util.check-windows-service	`service`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter überprüfen (Fortsetzung)

Überprüfen	Parameter
os.Windows-Check-log	`file`
util.checks-logs	`file`
util.checks-logs-sudo	`file`

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Prüfungsdefinitionen**an.
2. Suchen Sie die Prüfungsdefinition, für die Sie Ereignisse blockieren möchten.
3. Auf der **Überprüfen Sie Die Parameterdefinitionen** Wählen Sie die Registerkarte aus `skip_events_for_nonexistent`.
4. Wählen Sie aus **Aktiv** Kontrollkästchen, um den Parameter zu aktivieren und die Erstellung von Warnungen zu verhindern, wenn der Prozess, der Service oder das Protokoll für die angegebene Prüfung nicht gefunden werden.
   Wenn Sie eine Benachrichtigung über den fehlenden Prozess oder Service erhalten möchten, verlassen Sie die `skip_events_for_nonexistent`Parameter mit dem Standardwert **Falsch** .

Anzeige von HAProxy-Metriken aktivieren

Konfigurieren Sie die Statistikseite für HAProxy-Metriken, um die Überwachung Ihrer Systemgeräte durch Anzeige von HAProxy-Metriken zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

HAProxy bietet Lastenausgleichs- und Reverse-Proxy-Funktionen für HTTP- und TCP-Anforderungen. Durch HAProxy-Prüfungen werden Back-End-Server entfernt, die mehrere Integritätsprüfungen hintereinander nicht bestehen. Außerdem wird eingehender Datenverkehr im Rahmen des Lastenausgleichs an Back-End-Server übertragen.

Prozedur

1. Greifen Sie auf die HAProxy-Konfigurationsdatei zu, die unter /etc/haproxy/haproxy.cfg gespeichert ist.
2. Fügen Sie den folgenden Code am Ende der Datei hinzu:

```
listen frontend *:8080      #Haproxy
Monitoring run on port 8080
mode http
option forwardfor
option httpclose
stats enable
stats show-legends
stats refresh 5s
stats uri /stats       #URL for HAProxy monitoring
stats realm Haproxy\Statistics.   #Title for pop up window
stats auth admin:admin     #User and Password for login to the monitoring dashboard
stats admin if TRUE
default_backend backend       #This is optional for monitoring backend
```

3. Führen Sie den folgenden Befehl aus, um HAProxy neu zu starten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
sudo service haproxy restart
```

4. Zeigen Sie die HAProxy-Metriken auf dem System an, indem Sie die Statistikseite für HAProxy-Metriken aufrufen, auf die Sie über die folgende URL zugreifen können:
   http://<HAProxyServer>:8080/stats

Zugehörige Informationen

HAProxy – Standardprüfungen und Richtlinien

Aktivieren Apache Kafka Integritätsüberwachung

Legen Sie Konfigurationen in fest Apache HTTP-Serveranwendung zum Aktivieren von Agent Client Collector Durchzuführen Apache Kafka HTTP-Serverüberwachung.

Vorbereitungen

- Aktivieren Sie Java Management Extensions (JMX) für die Kafka-Metriksammlung, indem Sie den folgenden Befehl ausführen:

```
Environment="JMX_PORT=9999"
```

- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Aktivieren Sie die Erfassung Apache Kafka Leistungsmetriken mit Java Management Extensions (JMX) durch Ausführen des folgenden Befehls:

```
JMX_PORT=9999  bin/kafka-server-start.sh  config/server.properties
```

2. Konfigurieren Sie den Administratorserver-Port, indem Sie die Portnummer der Eigenschaft admin.serverPort in der Datei zookeeper.properties ändern.
   Der Standardport ist 8080.

Aktivieren Sie die Ausführung von Lackprüfungen

Verwenden Sie Anwendungsfingerabdrücke, um das Varnish-CI (Configuration Item) zu erkennen und so die Ausführung von Varnish-Prüfungen zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

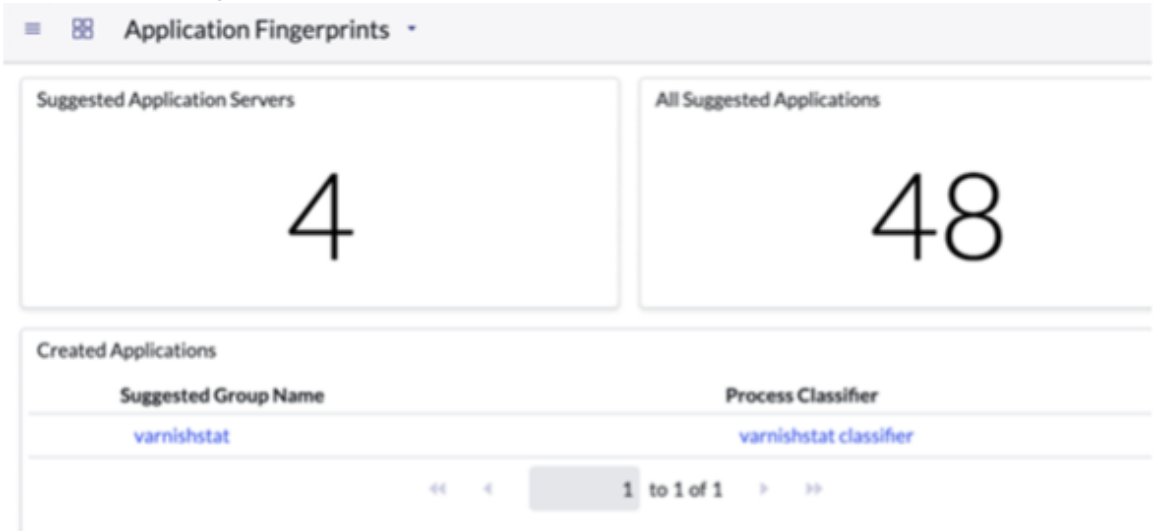
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**an.
2. Wählen Sie die Kachel **Fingerabdrücke der Anwendung** aus.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Wählen Sie die Kachel **Alle vorgeschlagenen Anwendungen** aus.
4. Wählen Sie auf der Seite „Anwendungsvorschläge“ in der Spalte **Vorgeschlagener Gruppenname** den Eintrag **varnishstat** aus.
   Die varnishstat-Details werden auf der Seite „Anwendungsvorschläge“ angezeigt.
5. Wählen Sie „Anwendung erkennen“ aus.
   Von Discovery wird nach einem Anwendungs-CI für den varnishstat-Eintrag gesucht. Das CI wird im Dashboard „Fingerabdrücke der Anwendung“ im Abschnitt **Erstellte Anwendungen** angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Erstellte Anwendungen“ des Dashboards „Fingerabdrücke der Anwendung“



6. Führen Sie auf dem Hostcomputer „grundlegende Discovery“ aus.

Ergebnis

Das varnishstat-CI wird erkannt, und in der Tabelle u_cmdb_ci_varnishstat wird ein Datensatz erstellt.

Die Varnish-Richtlinien und -Prüfungen können ausgeführt werden.

Wählen Sie aus Azure Richtlinien, die für die Metriksammlung aktiviert werden sollen

Aktivieren Sie Azure Richtlinien, die mit enthalten sind Agent Client Collector Basissystem so Azure Virtuelle Computer können Metriken erfassen. Diese Metriken helfen Ihnen, die Konfigurationselemente (Configuration Items, CIs) in zu überwachen CMDB.

Vorbereitungen

- Bereiten Sie eine Instanz mit einem aktiven vor MID-Server Und Metrikbasis.
- Installieren Agent Client Collector Framework Und Agent Client Collector-Überwachung.
- Ausführen Discovery Auf der Azure Cloud-Account zum Ausfüllen von CMDB Mit zu überwachenden CIs.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Bereiten Sie den Proxy-Agent vor, der von der Richtlinie verwendet werden soll, und konfigurieren Sie ihn. Weitere Informationen zum Konfigurieren eines Proxy-Agents finden Sie unter Proxy-Agents in werden verwendet Agent Client Collector.
2. Weisen Sie die Anmeldeinformationen zu Azure Richtlinie.
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
   b. Wählen Sie die entsprechende Richtlinie aus.
   Details zu den Richtlinien, die mit dem Basissystem verfügbar sind, finden Sie unter Azure Cloud-Metriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie aus **Anmeldeinformationen** Registerkarte.

d. In **Anmeldeinformationsname** Wählen Sie die Anmeldeinformationen aus, die für die Richtlinie aufgerufen werden sollen.
Um die verfügbaren Anmeldeinformationen anzuzeigen, wechseln Sie zur Seite Anmeldeinformationen, indem Sie zu navigieren **Alle** > **Discovery** > **Anmeldeinformationen**an.

Stellen Sie sicher, dass Sie auswählen **Typ=Azure** Anmeldeinformationen. Wenn Sie Anmeldeinformationen erstellen müssen, wählen Sie aus **Neu** Und wählen Sie aus **Azure-Service-Prinzipal** Anmeldeinformationen.

e. In **Anmeldeinformationsalias** Feld, weisen Sie den Anmeldeinformationen einen Alias zu.

3. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien** Und wählen Sie die relevante Richtlinie aus, die aktiviert werden soll.
4. Wählen Sie das Symbol für den Anwendungsbereich aus Und überprüfen Sie, ob Sie sich in befinden Agent Client Collector-Überwachung Bereich zum Bearbeiten der Richtlinie.
5. Aktivieren Sie die Richtlinie im Bearbeitungsmodus, indem Sie auswählen **Bearbeiten Sie in Sandbox** .
6. Aktivieren Sie den Proxy-Agent, der zum Ausführen der Prüfung verwendet werden soll.
   a. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
   b. Wählen Sie Aus **Einzelner Proxy-Agent** Und wählen Sie den Proxy-Agent aus, der zum Ausführen der Prüfung von verwendet werden soll **Proxy-Agent** Feld.
7. Wählen Sie **Speichern**.
8. Veröffentlichen Sie die Richtlinie erneut, indem Sie auswählen **Erneut Veröffentlichen** .

Erstellen Azure Richtlinien für die Metriksammlung

Erstellen Sie eigene Richtlinien zum Aktivieren Azure Zum Sammeln der Metriken für die Ressourcen, die Richtlinien haben, die nicht im Basissystem enthalten sind. Die Azure Die Prüfung des Metriksammlers bringt die Metriken über den an den Service Desk-Mitarbeiter Azure Metriken-Batch-API.

Vorbereitungen

- Stellen Sie sicher, dass die Konfigurationselemente (Configuration Items, CIs), für die Sie die Metriken erfassen möchten, in enthalten sind CMDB. CIs werden normalerweise während ausgefüllt Discovery.
- Stellen Sie sicher, dass *`sn_agent.multi_ci_dev_mode`*Eigenschaft ist auf festgelegt **Wahr** Auf der **Systemeigenschaften** Seite (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Wählen Sie **Neu**.
3. Wählen Sie das Symbol für den Anwendungsbereich aus Und überprüfen Sie, ob Sie sich in befinden Agent Client Collector-Überwachung Umfang.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In **Name** Feld einen Namen für die Richtlinie eingeben.
5. Konfigurieren Sie einen Filter, der bestimmt, welche CIs von der Richtlinie überwacht werden sollen, indem Sie auswählen **Überwachte CIs** Registerkarte und **Überwachter CI-Typ nach Filter** Kontrollkästchen, wie in der folgenden Tabelle beschrieben.

Filter für überwachte CIs

Option	Aktion
Überwachter CI-Typ	Wählen Sie den zu überwachenden CI-Typ aus. Der CI-Typ muss mit der Ressource übereinstimmen, die Sie in der JSON-Skriptdatei eingegeben haben, die die zu überwachenden Metriken enthält.
<Filter fields>	Konfigurieren Sie die Bedingungen, die erfüllt sein müssen, damit die Ressourcen im angegebenen überwachten CI-Typ überwacht werden. Stellen Sie sicher, dass Sie die folgenden Bedingungen festlegen: ○ **Objekt-ID** = <Name der in der JSON-Skriptdatei eingegebenen Ressource, die die zu überwachenden Metriken enthält> ○ **Status** = Verfügbar Der Status „verfügbar“ gibt an, dass Ressourcen zur Überwachung verfügbar sein müssen.
Vorschau	Wählen Sie diese Option aus, um die Anzahl der Ressourcen anzuzeigen, die der angegebenen Bedingung entsprechen. Die Anzahl der übereinstimmenden Ergebnisse wird neben angezeigt **Vorschau** Schaltfläche. Wählen Sie das Ergebnis aus, um alle CI-Datensätze anzuzeigen, die der Bedingung entsprechen.

6. Fügen Sie hinzu Azure Metriksammler überprüft die Richtlinie.
   a. Auf der **Prüfungen** Registerkarte suchen Sie nach **Azure Metrics Collector** Checken Sie in ein **Verfügbar** Zelle.
   b. Wählen Sie die Pfeilschaltfläche nach rechts, um den Scheck in zu verschieben **Ausgewählt** Zelle.
7. Konfigurieren Sie einen Proxy-Server für den Zugriff auf Azure Metriken.
   a. Auf der **Proxy-Einstellungen** Wählen Sie die Registerkarte aus **Einzelner Proxy-Agent** .
   b. In **Proxy-Agent** Feld den Proxy-Agent auswählen, um die Richtlinie auszuführen und abzurufen Azure Metriken.
8. Konfigurieren Sie die Anmeldeinformationen für die Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie aus **Anmeldeinformationen** Registerkarte.

b. In **Anmeldeinformationsname** Wählen Sie das Feld aus **azure_metrics_Collector** .

9. Wählen Sie **Speichern**.

10. Fügen Sie der Prüfungsinstanz sichere Parameter hinzu.

a. In der Richtlinie **Instanzen Überprüfen** Wählen Sie den Abschnitt aus **Azure Metrics Collector** Überprüfen Sie die Instanz.

b. Auf der **Überprüfen Sie Die Sicheren Parameter** Wählen Sie die Registerkarte aus **Neu** .

c. Fügen Sie die Parameter für die sichere Prüfung hinzu, die in der folgenden Tabelle beschrieben werden.

Parameter für sichere Prüfung

Name	Reihenfolgewert
Cred_tenant_ID	1
Cred_Client_ID	2
Cred_Secret_key	3

Stellen Sie sicher, dass **Aktiv** Das Kontrollkästchen ist für jeden Parameter aktiviert.

d. Wählen Sie **Aktualisieren**.

11. Fügen Sie hinzu .JSON Konfigurationsdatei für die Prüfinstanz.
Die Datei sendet die Liste von Azure Ressourcen für den Service Desk-Mitarbeiter.

a. Wählen Sie aus Azure Prüfinstanz des Metriksammlers.

b. Wählen Sie aus **Parameter Überprüfen** Unterregisterkarte.

c. Wählen Sie **Neu**.

d. Füllen Sie im Formular die Felder aus.

Parameterformular überprüfen

Feld	Beschreibung
Name	Beschreibender Name für .JSON Datei, die den Konfigurationsdateien der Instanz hinzugefügt werden soll (**Agent Client Collector** > **Konfigurationsdateien**) an.
Wert	Zeichenfolge, die den Namen von angibt .JSON Datei. Beispiel: acc_Azure_vm_metrics_config.JSON

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kennzeichnung	Wert, den Sie eingeben (**-C**), um anzugeben, dass die Prüfung den Namen der Konfigurationsdatei abruft. Die Konfigurationsdatei enthält einen Namespace und eine Liste von Metriken. Der Wert muss den Namen der Datei angeben, die in die Liste der Konfigurationsdateien hochgeladen wurde (**Agent Client Collector** > **Konfigurationsdateien**), in .JSON Format. Beispiel: acc_Azure_vm_metrics_config.JSON .

Stellen Sie sicher, dass **Aktiv** , **Obligatorisch** , Und **Wert erforderlich** Kontrollkästchen sind aktiviert.

e. Wählen Sie **Absenden**.

12. Erstellen Sie einen .JSON Datei, die die Metriken angibt, die Ihre Richtlinie überwachen soll.

Im folgenden Beispiel wird ein angezeigt .JSON Datei zum Abrufen von Lastenausgleichsmodul-Metriken.

acc_azure_static_ms_lb_config.json

```
{
  "namespace": "Microsoft.Network/loadBalancers",
  "metrics": [
            "AllocatedSnatPorts",
            "ByteCount",
            "DipAvailability",
            "PacketCount",
            "SnatConnectionCount",
            "SYNCount",
            "UsedSnatPorts",
            "VipAvailability"
  ],
  "time_grain": "PT1M"
}
```

Fügen Sie hinzu .JSON Datei in der Liste der Konfigurationsdateien unter **Agent Client Collector** > **Konfigurationsdateien**an.

13. Erstellen Sie eine JSON-Datei, um die Ressourcen anzugeben, die Ihre Richtlinie überwachen soll.

a. Auf der **Proxy-Einstellungen** Wählen Sie die Registerkarte aus **Multi-CI-Modus** .

b. Kopieren Sie ein Skript aus einem der Azure Cloud-Richtlinien, die im Lieferumfang des Basissystems enthalten sind.

- Cloud-Richtlinien, die mit dem Basissystem geliefert werden, werden in beschrieben Erstellen Azure Richtlinien für die Metriksammlung.
- Das Skript befindet sich in **Skript zur Erstellung der Konfigurationsdatei** Feld der Richtlinie **Proxy-Einstellungen** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Fügen Sie das Skript in ein **Skript zur Erstellung der Konfigurationsdatei** Feld Ihrer Richtlinie.

d. Konfigurieren Sie am Ende des Skripts `resource_id`, `region`, Und `sys_id`Parameter mit den Werten des CI, das von der Richtlinie überwacht werden soll.

14. Wählen Sie Aus **Speichern** Und veröffentlichen Sie dann die Richtlinie, indem Sie auswählen **Veröffentlichen** .

Ergebnis

Die konfigurierte Richtlinie ruft die Ressourcen und ihre Metriken aus dem angegebenen ab Azure CI und sendet sie an den Service Desk-Mitarbeiter.

Monitoring Technology Dashboard verstehen

Die Monitoring Technology Dashboard Ermöglicht Ihnen die Überwachung von Serverressourcen für die von Ihnen ausgewählte Plattform. Mit dem Dashboard können Sie die CIs und Server in Ihrem System mit dem höchsten Ressourcenverbrauch und den neuesten aktiven Warnungen identifizieren.

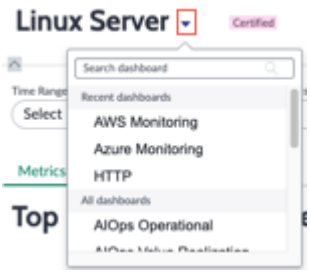
Sie können die Darstellung einzelner Widgets im anpassen Monitoring Technology Dashboard. Sie können beispielsweise die Datenparameter ändern, die für die Metrik „CPU-Auslastung“ (Linux) angezeigt werden, z. B. den Datumsbereich. Sie können die anwenderdefinierten Widgets beim Erstellen eines anwenderdefinierten Dashboards einbeziehen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Die Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden und die 50 neuesten aktiven Warnungen auf den Servern Ihres Betriebssystems an.

Um die Anzeige von zu aktivieren Monitoring Technology Dashboard, Stellen Sie sicher, dass Sie Clotho Version 23.1,0 installiert haben.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie das Betriebssystem aus, dessen Metriken Sie anzeigen möchten.

Wählen Sie den Pfeil neben dem Dashboard-Namen aus, um die Auswahl eines anderen Dashboards zum Anzeigen zu aktivieren:



Monitoring Technology Dashboard für Linux

Mit Linux Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen Linux Infrastruktur. Mit dem Dashboard können Sie die CIs und Server in Ihrem System mit dem höchsten Ressourcenverbrauch sowie die neuesten aktiven Warnungen identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht Des Dashboards

Die Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen auf den Servern Ihres Betriebssystems an.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **Linux-Server** .

Verwenden des Überwachungstechnologie-Dashboards für Linux

Vor der Verwendung von Monitoring Technology Dashboard Für Linux:

- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **Linux-BS-Ereignisse** Und **Linux-BS-Metriken** Richtlinien sind aktiviert.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metrik zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Zeigen Sie auf das relevante Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie die Registerkarte Warnungen aus, um die 50 neuesten aktiven Warnungen für CIs anzuzeigen.

Sie können die Dashboard-Daten nach den folgenden Filtern filtern:

Dashboard-Filter

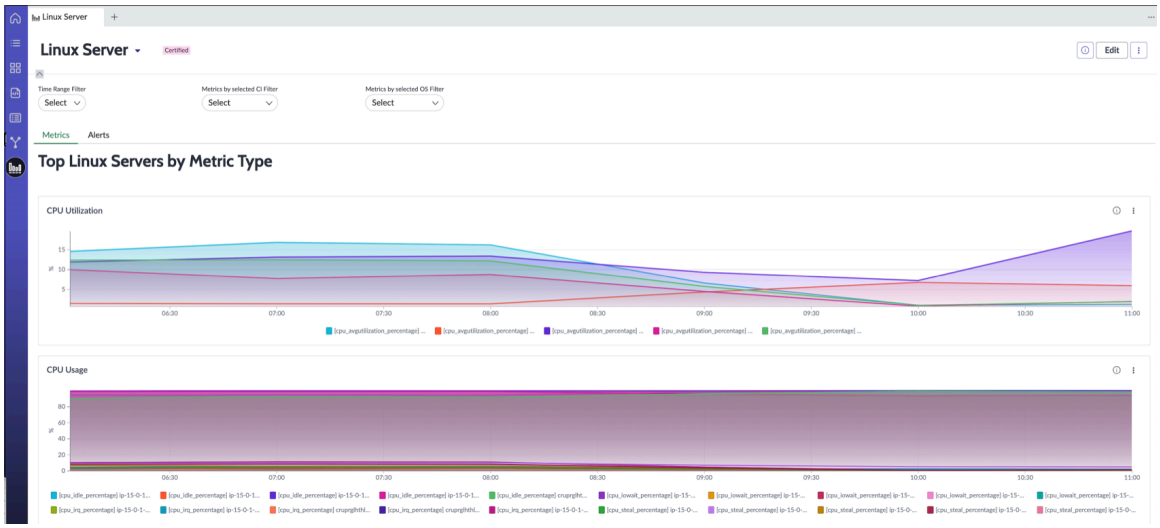
Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitbereich, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem BS-Filter	Das Betriebssystem, für das Metrikdaten im Dashboard angezeigt werden sollen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Server-Dashboard



Auf der Unterregisterkarte „Metriken“ werden die fünf CIs und Server der letzten sechs Stunden mit der besten Leistung gemäß den folgenden Metriken angezeigt.

- CPU-Auslastung
- Betriebszeit des Systems
- CPU-Auslastung
- Lastdurchschnitt
- Arbeitsspeicher
- Speicherverteilung
- Prozesse
- Netzwerknutzung
- Vertauschen
- Festplattenauslastung

Sie können die Darstellung der einzelnen Widgets im anpassen Linux Monitoring Technology Dashboard. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einschließen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Monitoring Technology Dashboard für Windows

Mit Windows Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen Windows Infrastruktur. Mit dem Dashboard können Sie die CIs und Server in Ihrem System mit dem höchsten Ressourcenverbrauch sowie die neuesten aktiven Warnungen identifizieren.

Übersicht Des Dashboards

Die Monitoring Technology Dashboard Für Windows Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen auf den Servern Ihres Betriebssystems an.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **Windows-Server** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Verwenden des Überwachungstechnologie-Dashboards für Windows

Vor der Verwendung von Monitoring Technology Dashboard Für Windows:

- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **Windows-BS-Ereignisse** Und **Windows-BS-Metriken** Richtlinien sind aktiviert:

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metrik zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **Windows-Server** .

Zeigen Sie auf das relevante Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie die Registerkarte Warnungen aus, um die 50 neuesten aktiven Warnungen für CIs anzuzeigen.

Sie können die Dashboard-Daten nach den folgenden Filtern filtern:

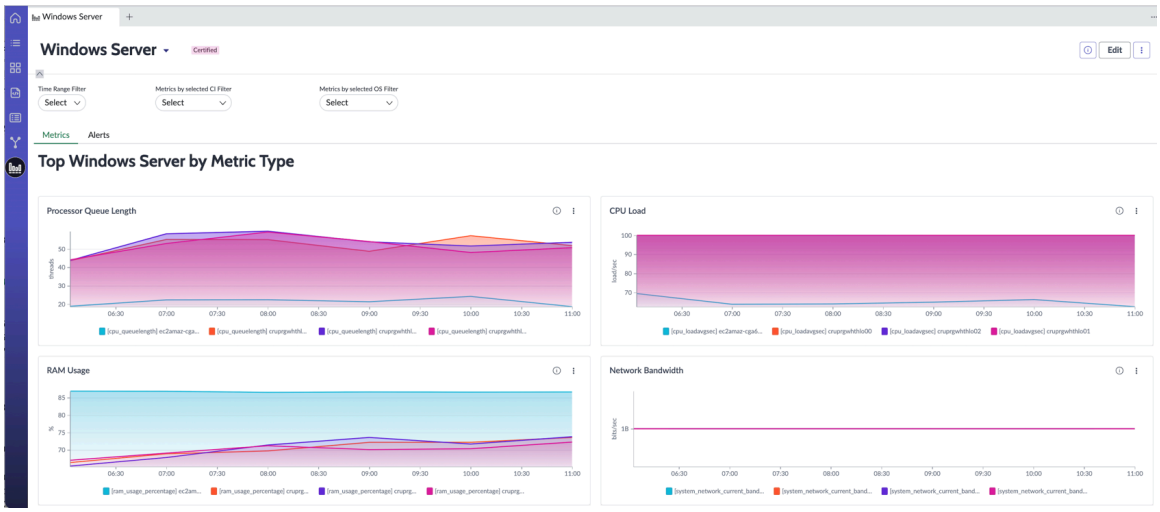
Dashboard-Filter

Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitbereich, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem BS-Filter	Das Betriebssystem, für das Metrikdaten im Dashboard angezeigt werden sollen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Server-Dashboard



Auf der Unterregisterkarte „Metriken“ werden die fünf CIs und Server der letzten sechs Stunden mit der besten Leistung gemäß den folgenden Metriken angezeigt.

- Länge der Prozessorwarteschlange
- CPU-Auslastung
- Betriebszeit des Systems
- CPU-Kern
- RAM-Auslastung
- Netzwerkbandbreite
- Speicherverteilung
- Netzwerk-Flow
- Festplattenauslastung
- Datenträger – Lesen/Schreiben
- Datenträgerverteilung

Sie können die Darstellung der einzelnen Widgets im anpassen Windows Monitoring Technology Dashboard. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einschließen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Monitoring Technology Dashboard Für HTTP

Mit dem HTTP Monitoring Technology Dashboard Sie können die Antwortzeit von überwachen http Und https URLs. Mithilfe des Dashboards können Sie die URLs mit den höchsten Metrikauslesungen in der Infrastruktur Ihres Systems identifizieren und die neuesten aktiven Warnungen für diese URLs anzeigen.

Übersicht Des Dashboards

Das HTTP Monitoring Technology Dashboard Zeigt die fünf URLs mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen für diese URLs an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **HTTP** .

Mit Monitoring Technology Dashboard Für HTTP

Vor der Verwendung von Monitoring Technology Dashboard Für HTTP:

- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **HTTP-Einstiegspunkte-Ereignisse** Und **HTTP-Einstiegspunkte-Metriken** Richtlinien sind aktiviert.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metrik zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Die Azure Monitoring Technology Dashboard Enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

HTTP Monitoring Technology Dashboard Registerkarten

Registerkarte	Beschreibung
Metriken	Zeigt die fünf wichtigsten Leistungsmetriken an, die den URLs in Ihrem System zugeordnet sind.
Alerts	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Verwenden Sie **Zeitbereichsfilter** Zum Filtern des Zeitbereichs, für den Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets auf HTTP anpassen Monitoring Technology Dashboard. Sie können beispielsweise die Datenparameter ändern, die für die Antwortzeitmetrik angezeigt werden, z. B. den Zeitbereich, in dem die Antwortzeit angezeigt wird. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Monitoring Technology Dashboard für Azure

Mit Azure Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen Azure Infrastruktur. Mithilfe des Dashboards können Sie die Konfigurationselemente (Configuration Items, CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen für diese CIs anzeigen.

Übersicht Des Dashboards

Die Azure Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrem an Azure Umgebung. Basierend auf den Dashboard-Metriken möchten Sie möglicherweise die Größe Ihrer CIs und Server ändern, um Ihre Systemleistung und -Effizienz zu verbessern.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **Azure-Überwachung** .

Mit Monitoring Technology Dashboard Für Azure

Vor der Verwendung von Monitoring Technology Dashboard Für Azure:

- Erstellen Sie einen Azure Anmeldeinformationen. Für Details zum Erstellen Azure Anmeldeinformationen, siehe Anmeldeinformationen für Azure-Cloud erstellen.
- Erstellen Sie einen Discovery Planen Sie mithilfe der im vorherigen Schritt erstellten Anmeldeinformationen. Um Details zum Erstellen von zu erhalten Discovery Zeitplan, siehe Erkennung von Azure-Clouds.
- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **Azure-VM-Metriken** , **Azure-Speicher-Account-Metriken** , **Azure-Lastenausgleichsmodul-Metriken** , **Azure-Gateway-Metriken** , Und **Azure-Redis-Cache-Metriken** Richtlinien sind aktiviert
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.

Die Azure Monitoring Technology Dashboard Enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

Azure Monitoring Technology Dashboard Registerkarten

Registerkarte	Beschreibung
Virtuelle Maschinen	Zeigt die Metrikdaten von den virtuellen Computern in an Azure Umgebung.
Speicherkonten	Zeigt die Metrikdaten aus den Speicher-Accounts in an Azure Umgebung.
Load Balancer	Zeigt die Metrikdaten der Lastenausgleichsmodule in an Azure Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Monitoring Technology Dashboard Registerkarten (Fortsetzung)

Registerkarte	Beschreibung
Application Gateway	Zeigt die Metrikdaten aus dem Anwendungs-Gateway in an Azure Umgebung.
Redis	Zeigt die Metrikdaten aus dem Redis-Cache in an Azure Umgebung.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Sie können die Dashboard-Daten nach den folgenden Filtern filtern:

Dashboard-Filter

Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitbereich, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets im anpassen Azure Monitoring Technology Dashboard. Sie können beispielsweise die Zeit ändern, zu der die CPU-Auslastung auf virtuellen Computern angezeigt wird. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Monitoring Technology Dashboard für AWS

Mit AWS Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen AWS Infrastruktur. Mithilfe des Dashboards können Sie die Konfigurationselemente (Configuration Items, CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen auf diesen CIs und Servern anzeigen.

Übersicht Des Dashboards

Die AWS Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrem an AWS Umgebung.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **AWS-Überwachung** .

Mit Monitoring Technology Dashboard Für AWS

Vor der Verwendung von Monitoring Technology Dashboard Für AWS:

- Erstellen Sie einen AWS Anmeldeinformationen. Für Details zum Erstellen AWS Anmeldeinformationen, siehe Wird eingerichtet AWS Service-Accounts.
- Erstellen Sie einen Discovery Planen Sie mithilfe der im vorherigen Schritt erstellten Anmeldeinformationen. Um Details zum Erstellen von zu erhalten Discovery Zeitplan, siehe Zugriff für AWS-Servicekonten einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **AWS-Metriken** , **AWS EC2-Metriken** , Und **AWS DynamoDB-Metriken** Richtlinien sind aktiviert.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metrik zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Die AWS Monitoring Technology Dashboard Enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

AWS Monitoring Technology Dashboard Registerkarten

Registerkarte	Beschreibung
EC2	Zeigt die Metrikdaten von EC2 (virtuelle Computer) in an AWS Umgebung.
EC2-Warnungen	Zeigt die aktiven EC2-Warnungen (virtuelle Maschine) in an AWS Umgebung.
EBS-Inklusionsmodule	Zeigt die Metrikdaten aus dem EBS (Speichervolume) in an AWS Umgebung.
S3	Zeigt die Metrikdaten aus S3 (Cloud Object Storage) in an AWS Umgebung.
RDS	Zeigt die Metrikdaten aus dem RDS (Cloud-Datenbank) in an AWS Umgebung.
ELB	Zeigt die Metrikdaten aus dem ELB (Cloud Load Balancing) in an AWS Umgebung.
DynamoDB	Zeigt die Metrikdaten aus der Dynamo-DB (Cloud-Datenbank) in an AWS Umgebung.
ECS-Cluster	Zeigt die Metrikdaten aus dem ECS-Cluster in an AWS Umgebung.
ECS-Service	Zeigt die Metrikdaten aus dem ECS-Service in an AWS Umgebung.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie aus **Warnungen** Registerkarte, um die 50 neuesten aktiven Warnungen in Ihrer Umgebung anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Verwenden Sie **Zeitbereichsfilter** Zum Filtern des Zeitbereichs, für den Metrikdaten im Dashboard angezeigt werden sollen.

Verwenden Sie **Metriken nach ausgewähltem CI-Filter** Um die CIs auszuwählen, für die Sie Metriken anzeigen möchten.

Sie können die Darstellung der einzelnen Widgets im anpassen AWS Monitoring Technology Dashboard. Sie können beispielsweise die Zeit ändern, zu der die EC2-Metriken angezeigt werden. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Monitoring Technology Dashboard für GCP

Mit GCP Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen GCP Infrastruktur. Mithilfe des Dashboards können Sie die Konfigurationselemente (Configuration Items, CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen auf diesen CIs und Servern anzeigen.

Übersicht Des Dashboards

Die GCP Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrem an GCP Umgebung.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **GCP-Überwachung** .

Mit Monitoring Technology Dashboard Für GCP

Vor der Verwendung von Monitoring Technology Dashboard Für GCP:

- Erstellen Sie einen GCP-Anmeldeinformationen und verwenden Sie sie zum Erstellen von Discovery Zeitplan. Für Details zum Erstellen GCP Anmeldeinformationen, siehe Erkennung von Google Cloud Platform.
- Erstellen Sie einen Discovery Planen Sie mithilfe der im vorherigen Schritt erstellten Anmeldeinformationen. Um Details zum Erstellen von zu erhalten Discovery Zeitplan, siehe Erkennung von Google Cloud Platform.
- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **GCP-GCE-Metriken** Richtlinie ist aktiviert.

  Durch Aktivieren dieser Richtlinie wird die Zuordnung von Metrik zu CI aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Die GCP Monitoring Technology Dashboard Enthält die in der folgenden Tabelle aufgeführten Registerkarten.

Registerkarten des GCP-Überwachungs-Dashboards

Registerkarte	Beschreibung
GCP	Zeigt Diagramme der 14 wichtigsten Betriebssystemressourcen an, z. B. CPU, Arbeitsspeicher, Datenträgervorgänge und Netzwerk.
Alerts	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Verwenden Sie **Zeitbereichsfilter** Zum Filtern des Zeitbereichs, für den Metrikdaten im Dashboard angezeigt werden sollen.

Verwenden Sie **Metriken nach ausgewähltem CI-Filter** Um die CIs auszuwählen, für die Sie Metriken anzeigen möchten.

Sie können die Darstellung der einzelnen Widgets im anpassen GCP Monitoring Technology Dashboard. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einschließen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Monitoring Technology Dashboard für VMware vSphere

Mit VMware vSphere Monitoring Technology Dashboard, Sie können die Integrität und Leistung von überwachen VMware vSphere Infrastruktur. Mithilfe des Dashboards können Sie die Konfigurationselemente (Configuration Items, CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen auf diesen CIs und Servern anzeigen.

Übersicht Des Dashboards

Die VMware vSphere Monitoring Technology Dashboard Zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden an. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrem an VMware vSphere Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zum Anzeigen des Dashboards zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** Und wählen Sie aus **VMware vSphere-Überwachung** .

Mit Monitoring Technology Dashboard Für VMware vSphere

Vor der Verwendung von Monitoring Technology Dashboard Für VMware vSphere:

- Erstellen Sie einen VMware vSphere-Anmeldeinformationen und verwenden Sie sie zum Erstellen von Discovery Zeitplan. Für Details zum Erstellen VMware vSphere Anmeldeinformationen, siehe Erkennung von VMware-Clouds.
- Erstellen Sie einen Discovery Planen Sie mithilfe der im vorherigen Schritt erstellten Anmeldeinformationen. Um Details zum Erstellen von zu erhalten Discovery Zeitplan, siehe Erkennung von VMware.
- Stellen Sie sicher, dass Sie in arbeiten Agent Client CollectorÜberwachungsbereich in Ihrem ServiceNow Instanz.
- Stellen Sie sicher, dass die Rollen Agent_Client_Collector_admin und Dashboard_admin aktiviert sind.
- Aktivieren Metrikdaten Auf der MID-Server.
- Stellen Sie sicher, dass **VSphere-Rechenzentrumsmetriken** , **VSphere-Datenspeichermetriken** , **VSphere ESX Server-Metriken** Und **VSphere VirtualMachine-Metriken** Richtlinien sind aktiviert.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metrik zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.1.0 oder höher aktiviert ist.
- Führen Sie nach dem Upgrade von einer vorherigen Version das im beschriebene Verfahren aus ACC-M-Dashboard-Filter funktionieren beim Upgrade von Tokio/Utah auf Vancouver nicht [KB1438042]. artikel in der NOW Support Knowledge Base.

Die VMware vSphere Monitoring Technology Dashboard Enthält die in der folgenden Tabelle aufgeführten Registerkarten.

VMware vSphere Registerkarten des Überwachungs-Dashboards

Registerkarte	Beschreibung
VirtualMachine	Zeigt Diagramme des oberen Bereichs an VMware vSphere VMs nach Metriktyp.
ESX-Server	Zeigt Diagramme des oberen Bereichs an VMware vSphere ESX-Server nach Metriktyp.
Rechenzentrum	Zeigt Diagramme des oberen Bereichs an VMware vSphere Rechenzentren nach Metriktyp.
Datenspeicher	Zeigt Diagramme des oberen Bereichs an VMware vSphere Datenspeicher nach Metriktyp.
Alerts	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „weitere Optionen“ (⋮) Und wählen Sie aus **Ändern Sie „Gruppieren nach“** . Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder Betriebssystemversion.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Sie können die Dashboard-Daten nach den folgenden Filtern filtern:

Dashboard-Filter

Filter für Zeitbereich	Der Zeitbereich, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets im anpassen VMware vSphere Monitoring Technology Dashboard. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einschließen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Überwachungstechnologie-Dashboard an.

Passen Sie das Überwachungstechnologie-Dashboard an

C Passen Sie die Überwachungstechnologie-Dashboard-Widgets in der Datenvisualisierungsbibliothek an, damit Ihr Dashboard Informationen genau so anzeigt, wie Sie sie sehen möchten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

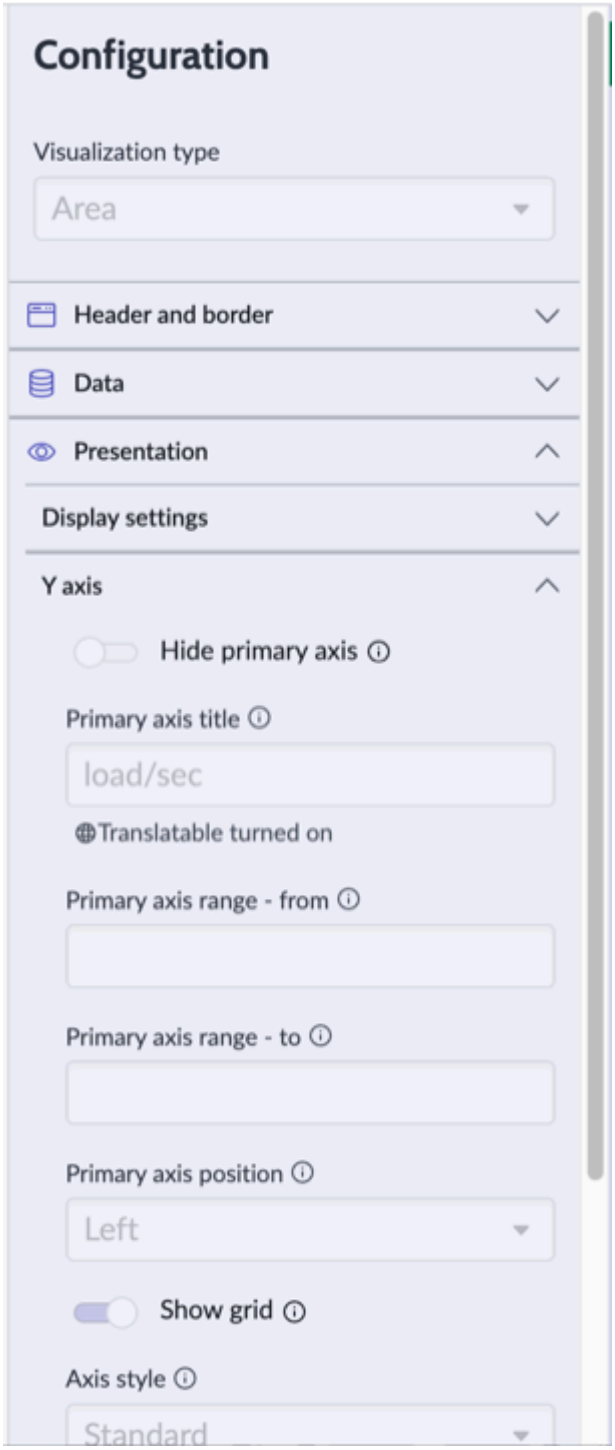
Prozedur

1. Navigieren Sie zum BS-Dashboard, dessen Widgets Sie anpassen möchten.
   - Um auf das Windows Server-Dashboard zuzugreifen, navigieren Sie zu **Alle** > **AIOps** > **Überwachungstechnologie-Dashboard** > **Windows-Server**an.
   - Um auf das Linux Server-Dashboard zuzugreifen, navigieren Sie zu **Alle** > **AIOps** > **Überwachungstechnologie-Dashboard** > **Linux-Server**an.
2. Auswahlvorgang **Analytics-Center** > **Datenvisualisierungen**an.
3. Zeigen Sie alle verfügbaren Widgets an, indem Sie auswählen **Alle** Registerkarte.
4. Wählen Sie das Widget aus, das Sie ändern möchten.
5. Wählen Sie (☰) Symbol, und wählen Sie aus **Duplikat** .
6. In **Neuer Name** Geben Sie im Dialogfeld einen Namen für Ihr dupliziertes Widget ein, und wählen Sie aus **Duplikat** .
7. In den Widgets **Konfiguration** Erweitern Sie auf der rechten Seite die relevanten Optionen, und passen Sie die Informationen an, die das Widget anzeigen soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsregisterkarte



Details zum Arbeiten mit Datenvisualisierungen finden Sie unter Datenvisualisierungen im Analytics Center Datenvisualisierungen im Analytics Center .

8. Wählen Sie Aus **Speichern und schließen** .

Ergebnis

Ihre anwenderdefinierten Widgets werden in der Datenvisualisierungsbibliothek gespeichert und können zum Konfigurieren eines anwenderdefinierten Dashboards verwendet werden (siehe Erstellen Sie ein Dashboard mit dem Inline-Editor).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proxy-Agents in werden verwendet Agent Client Collector

Sie können einen Proxy-Agent verwenden, um die Integrität und Leistung Ihrer Konfigurationselemente (Configuration Items, CIs) zu überwachen, auch wenn sich der Agent in der Cloud oder an einem anderen Ort außerhalb Ihres Hostservers befindet.

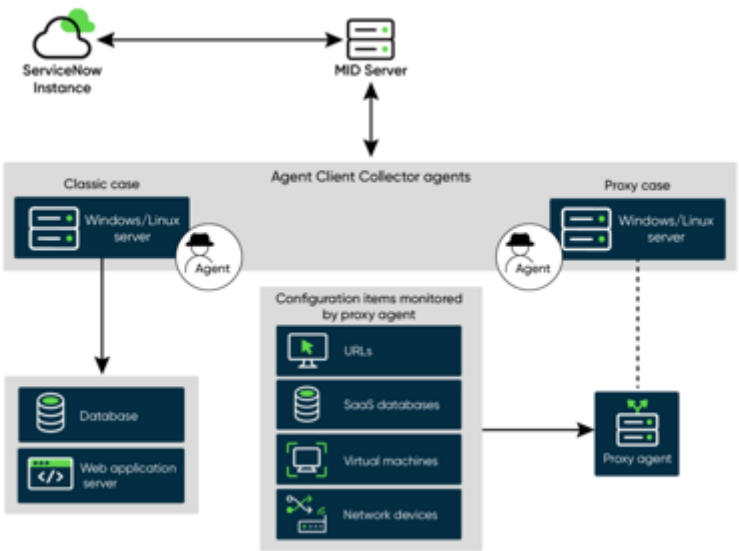
Proxy-Agents werden verwendet, um Folgendes zu überwachen:

- URLs (um sicherzustellen, dass die URLs verfügbar und zugänglich sind)
- Services, die keinen Hostserver haben
- Geschlossene Services, für die Sie keinen Service Desk-Mitarbeiter konfigurieren können
- Externe Datenbanken in der Cloud

Ein Service Desk-Mitarbeiter kann mehrere Entitäten und ihre CIs überwachen.

Das folgende Diagramm zeigt die Verbindung zwischen ServiceNow Instanz, die MID-Server, Und Agent Client Collector Service Desk-Mitarbeiter sowie Proxy-Agents, die CIs überwachen, die außerhalb des Service Desk-Mitarbeiters liegen.

Proxy-Agent-Konfiguration



Sie können den Proxy-Agent so konfigurieren, dass er bei der Überwachung externer Entitäten eine anwenderdefinierte Prüfung durchführt. Informationen zum Erstellen anwenderdefinierter Prüfungen finden Sie unter Prüfungen erstellen und bearbeiten.

Sie können einen Cluster von Proxy-Agents auf mehreren Proxy-Servern erstellen, um die Services zu überwachen, die außerhalb des Hostservers liegen. Informationen zum Erstellen eines Proxy-Agent-Clusters finden Sie unter Erstellen Sie einen Proxy-Agent-Cluster.

Verwenden Sie eine PAC-Datei (Proxy Auto-Configuration), um dynamisch den entsprechenden Proxy-Server zu bestimmen. PAC-Dateien bieten eine flexible und automatisierte Proxy-Konfiguration, sodass der Service Desk-Mitarbeiter verschiedene Proxys für verschiedene Ziele verwenden, direkt mit internen Ressourcen verbinden, komplexe Proxy-Weiterleitungslogik implementieren und Proxy-Failover automatisch verarbeiten kann. Weitere Informationen zu den für die PAC-Dateikonfiguration verwendeten Parametern finden Sie unter Konfigurationsdateioptionen.

Im Folgenden finden Sie eine Beispiel-PAC-Datei:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
function FindProxyForURL (url, host) {

  // Connect directly to internal hosts
  if (isPlainHostName(host) ||
    shExpMatch(host, "*.internal.company.com")) {
    return "DIRECT";
  }

  // use proxy for all other hosts
  return "PROXY proxy.company.com:8080:
}
```

Zugehörige Informationen

Prüfungen und Richtlinien

Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien

Agent auf einem Proxy-Server konfigurieren

Konfigurieren Sie Agent Client Collector auf einem Proxy-Server, wenn Sie Services außerhalb des Hostservers überwachen, z. B. URLs oder externe Datenbanken in der Cloud.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Proxy-Agents sollten dedizierte Agents sein, da die Ausführung anderer Apps auf einem Proxy-Agent wahrscheinlich zu einer Verschlechterung der Leistung führt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter** > **Richtlinien**an.
2. Wählen Sie die Richtlinie aus, die die Prüfungen enthält, die Sie auf einem Proxy-Server ausführen möchten. Sie müssen einen Proxy-Server für Prüfungen und Richtlinien konfigurieren, mit denen externe Services überwacht werden. Einzelheiten über diese Prüfungen und Richtlinien finden Sie unter Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Wählen Sie aus den folgenden Feldern aus.

Feld	Beschreibung
Einzelner Proxy-Agent	Bei Auswahl dieser Option wird das Feld **Proxy Agent** (Proxy-Agent) angezeigt, in dem Sie einen einzelnen Proxy-Agent auswählen.
Mehrere Proxy-Agenten nach Cluster	Wählen Sie diese Option aus, um einer Gruppe von Proxy-Agents die Überwachung der Richtlinien-CIs zu ermöglichen. Wenn Sie dieses Kontrollkästchen aktivieren, wird die **Name des Agent-Clusters** Feld wird angezeigt.
Name des Agenten-Clusters	Wählen Sie einen Agent-Cluster aus, um die Richtlinien-CIs zu überwachen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mehrere Proxy-Agenten via Filter	Wählen Sie dieses Feld aus, um mehrere Proxy-Agents aus der Agent-Liste zu filtern. Wenn Sie diese Option auswählen, werden von allen Proxy-Agents dieselben Services überwacht. Beispielsweise empfiehlt es sich, diese Option für mehrere Proxy-Server an verschiedenen geografischen Standorten zu verwenden. **Hinweis:** ○ Dieses Feld wird nur angezeigt, wenn **Blenden Sie Multi Proxy Agent nach Filter aus, wenn er nicht ausgewählt ist** Eigenschaft (*sys_ui_policy*) lst auf festgelegt **Aktiv=falsch** . ○ Dieses Feld wird nur für vorhandene Richtlinien angezeigt, für die diese Option zuvor ausgewählt wurde. Wenn Sie den Filter in einer vorhandenen Richtlinie entfernen, wird die Option ausgeblendet.
Mehrere Proxy-Agenten via Skript	Wählen Sie dieses Feld aus, um ein Java-Skript für die Auswahl von Proxy-Agents zu konfigurieren. Wenn Sie diese Option auswählen, können Sie Services verschiedenen Proxy-Agents zuweisen. Dies kann als eine Form des Lastenausgleichs dienen.
Prüfungen für alle Proxy-Agenten ausführen (kein Lastenausgleich)	Deaktivieren Sie diese Option, um den Lastenausgleich für die ausgewählten Multi-Proxy-Agents durchzuführen, die die übereinstimmenden CIs in der Richtlinie überwachen **Überwachte CIs** Registerkarte. Wählen Sie diese Option für jeden Service Desk-Mitarbeiter aus, um alle übereinstimmenden CIs in den Richtlinien zu überwachen **Überwachte CIs** Registerkarte. Wenn Sie beispielsweise fünf Agents in einem Cluster oder fünf Agents mit der Filter-/Skriptoption und 10 übereinstimmende CIs in der Richtlinie haben, überwacht jeder Agent zwei CIs, wenn Sie diese Option deaktivieren. Wenn Sie diese Option auswählen, überwacht jeder Service Desk-Mitarbeiter alle 10 übereinstimmenden CIs in der Richtlinie. Für vorhandene oder aktive Richtlinien ist diese Option standardmäßig aktiviert. Für neue und inaktive Richtlinien ist diese Option standardmäßig deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie diese Option nur dann aus, wenn Sie einen externen Endpunkt haben, für den Sie messen möchten, wie schnell auf ihn von verschiedenen Standorten aus zugegriffen wird.

5. Wählen Sie **Aktivieren**.

Erstellen Sie einen Proxy-Agent-Cluster

Erstellen Sie einen Cluster von Agents auf mehreren Proxy-Servern, um Services außerhalb des Hostservers zu überwachen. Durch das Erstellen eines Clusters von Service Desk-Mitarbeitern können Sie diesen Cluster mehreren Richtlinien zuweisen, anstatt die Service Desk-Mitarbeiter jeder Richtlinie einzeln zuweisen zu müssen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Proxy-Agent-Cluster überwacht die CIs, die dem in der Richtlinie angegebenen Filter entsprechen **Überwachte CIs** Registerkarte.

Ein Proxy-Agent-Cluster muss mindestens einen Agent enthalten. Alle Agents des Clusters überwachen die in der zugewiesenen Richtlinie angegebenen CIs. Auf Richtlinienebene ist keine spezielle Konfiguration erforderlich, um die Proxy-Cluster-Überwachung zu aktivieren.

Der CPU-Standardschwellenwert bei der Arbeit mit Proxy-Agent-Clustern beträgt 80 %. Sie können diesen Wert in ändern *proxy_cpu_percentage_limit*Eigenschaft.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Proxy-Agenten-Cluster**an.
2. Wählen Sie **Neu**.
3. In **Name** Feld einen beschreibenden Namen für den Cluster eingeben.
4. Fügen Sie dem Cluster einen Service Desk-Mitarbeiter hinzu.
   a. In **Agents im Cluster** Suchen Sie im Abschnitt **Service Desk-Mitarbeiter** Spalte und wählen Sie aus **Fügen Sie eine neue Zeile ein** .
   b. Wählen Sie das Suchsymbol ( ) Und wählen Sie einen Service Desk-Mitarbeiter aus, der dem Cluster hinzugefügt werden soll.
   c. Wählen Sie das Häkchensymbol ( ), um den Agent dem Cluster hinzuzufügen.
   Wiederholen Sie diesen Schritt für jeden Service Desk-Mitarbeiter, den Sie dem Cluster hinzufügen möchten.
5. Wählen Sie **Absenden**.

Ergebnis
Die **Proxy-Agent-Cluster** Seite wird angezeigt und zeigt den Service Desk-Mitarbeiter an, der dem Cluster hinzugefügt wurde.

Nächste Maßnahme
Wählen Sie diesen Proxy-Cluster aus, um CIs zu überwachen, die in einer Agent-Richtlinie angegeben sind. Details finden Sie unter Agent auf einem Proxy-Server konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie einer Richtlinie einen Proxy-Agent-Cluster zu

Weisen Sie einen Proxy-Agent-Cluster einer Richtlinie zu, wenn Sie Services außerhalb des Hostservers überwachen, z. B. URLs oder externe Datenbanken in der Cloud. Die Agents im Cluster überwachen alle CIs der Richtlinie.

Vorbereitungen
Stellen Sie sicher, dass Sie über eine Richtlinie verfügen, die die Prüfungen zur Überwachung externer Services enthält. Einzelheiten über diese Prüfungen und Richtlinien finden Sie unter Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Auf einem bestimmten Proxy-Agent darf nur eine App ausgeführt werden, da das Ausführen mehrerer Apps wahrscheinlich zu einer Leistungsverschlechterung führt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter** > **Richtlinien**an.
2. Wählen Sie die Richtlinie aus, die die Prüfungen enthält, die Sie auf einem Proxy-Server ausführen möchten.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Wählen Sie Aus **Bearbeiten Sie in Sandbox** Um das Ändern von Feldern im Formular zu aktivieren.
5. Geben Sie an, ob Sie einen einzelnen Proxy-Agent oder einen Proxy-Agent-Cluster zuweisen, um die Richtlinien-CIs zu überwachen.
   - Weisen Sie einen einzelnen Proxy-Agent zu, indem Sie auswählen **Einzelner Proxy-Agent** Und Auswahl eines Service Desk-Mitarbeiters.
   - Aktivieren Sie einen Proxy-Agent-Cluster, indem Sie auswählen **Multi-Proxy-Agents nach Cluster** . Geben Sie den Namen des Clusters im angezeigten Feld an.
6. Legen Sie fest, ob mehrere Proxy-Agents aus der Liste der Agents über einen Filter oder ein Skript ausgewählt werden sollen.
   - Um Service Desk-Mitarbeiter über einen Filter auszuwählen, konfigurieren Sie einen Filter, oder behalten Sie einen vorhandenen Filter bei, oder ändern Sie ihn **Multi-Proxy-Agents nach Filter** Option ist ausgewählt.

     Hinweis:
     - Dieses Feld wird nur angezeigt, wenn **Blenden Sie Multi Proxy Agent nach Filter aus, wenn er nicht ausgewählt ist** Eigenschaft (`sys_ui_policy`) Wurde auf festgelegt **Aktiv=falsch** .
     - Wenn Sie den Filter in einer vorhandenen Richtlinie entfernen, wird die Option ausgeblendet.

   - So wählen Sie Service Desk-Mitarbeiter über ein Skript aus:
     a. Wählen Sie **In Sandbox bearbeiten**.
     b. Löschen Sie alle ausgewählten Proxy-Optionen in **Proxy-Einstellungen** Registerkarte.
     c. Wählen Sie Aus **Multi-Proxy-Agents nach Skript** .
     d. In **Proxy-Skript** Feld, das angezeigt wird, geben Sie ein Skript ein, um Services verschiedenen Proxy-Agents als Form des Lastenausgleichs zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Legen Sie fest, ob ein Lastenausgleich für die ausgewählten Multi-Proxy-Agents durchgeführt werden soll, die die übereinstimmenden CIs in der Richtlinie überwachen **Überwachte CIs** Oder lassen Sie jeden Service Desk-Mitarbeiter die übereinstimmenden CIs überwachen.
   - Um einen Lastenausgleich für die ausgewählten Multi-Proxy-Agents durchzuführen, die die übereinstimmenden CIs überwachen, löschen Sie **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** Option.

     Wenn Sie beispielsweise fünf Agents in einem Cluster oder fünf Agents mit der Filter-/Skriptoption und 10 übereinstimmende CIs in der Richtlinie haben, überwacht jeder Agent zwei CIs.

     Sie können den Lastenausgleich auch zu einem späteren Zeitpunkt aktivieren, wie in beschrieben Aktivieren Sie den Lastenausgleich zwischen Proxy-Agents in einem Cluster.
   - Damit jeder Service Desk-Mitarbeiter alle übereinstimmenden CIs überwacht, wählen Sie aus **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** Option.

     Wenn die Richtlinie 10 übereinstimmende CIs enthält, überwacht jeder Service Desk-Mitarbeiter alle 10. Sie können diese Option beispielsweise für mehrere Proxy-Server an verschiedenen geografischen Standorten verwenden.

     Wenn ein Service Desk-Mitarbeiter nicht ordnungsgemäß funktioniert, werden die überwachten CIs an einen anderen Service Desk-Mitarbeiter weitergeleitet.

   Hinweis: Für vorhandene oder aktive Richtlinien **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** Option ist standardmäßig aktiviert. Für neue und inaktive Richtlinien ist diese Option standardmäßig deaktiviert.

8. Wählen Sie **Aktivieren**.

Zugehörige Informationen

Aktivieren Sie den Lastenausgleich zwischen Proxy-Agents in einem Cluster

Aktivieren Sie den Lastenausgleich zwischen Proxy-Agents in einem Cluster

Aktivieren Sie den Lastenausgleich zwischen Proxy-Agents in einem Cluster, damit überwachte CIs an einen anderen Agent weitergeleitet werden, wenn ein Agent nicht ordnungsgemäß funktioniert. Nach dem Aktivieren des Lastenausgleichs können Sie Folgendes tun v iew die von jedem Proxy-Agent in einer Richtlinie überwachten CIs .

Vorbereitungen

Stellen Sie sicher, dass Sie ein Upgrade auf durchgeführt haben Tokyo Patch 1 oder San Diego Patch 7.

Erforderliche Rolle: Agent_Client_Collector_user

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien**an.
2. Wählen Sie die Richtlinie aus, die die CIs enthält, die die Proxy-Agents überwachen sollen.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Aktivieren Sie den Lastenausgleich für die Proxy-Agents, indem Sie löschen **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Lastenausgleich ist für die Proxy-Agents aktiviert, die die CIs überwachen. Wenn Sie beispielsweise fünf Service Desk-Mitarbeiter und 10 übereinstimmende CIs in der Richtlinie haben, überwacht jeder Service Desk-Mitarbeiter zwei CIs.

5. In **Zugehörige Links** Abschnitt auswählen **Verteilung der CIs des Proxy-Agents anzeigen** .
   In einem Popup-Fenster wird die Verteilung der überwachten CIs auf die Service Desk-Mitarbeiter innerhalb der Richtlinie angezeigt.

Agent Client Collector-Überwachung – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Agent Client Collector-Überwachung Prüfungen und Richtlinien.

Footprint von Agent Client Collector Monitoring

In der folgenden Tabelle wird der Ressourcenverbrauch von Agent Client Collector beschrieben.

Parameter	Linux	Windows
Machine spec (Computerspezifikation)	Cent OS 8, 4 CPU-Kerne, 8 GB Arbeitsspeicher	Windows Server 2019, 2 CPUs, 4 GB Arbeitsspeicher
Network - (Agent > MID)	10,64 KB/s	350-400 Byte/s
Network - (MID > Agent)	48 Byte/s	5-15 Byte/s
Average CPU Utilization (Durchschnittliche CPU-Auslastung)	~1%	~3.89%
Max CPU per check (Max. CPU pro Prüfung)	10 bis 15 %	15 bis 20 %
Memory overhead (avg) (Arbeitsspeicher-Overhead (Durchschnitt))	~ 13,88 MB	~ 31,15 MB

Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien

Agent Client Collector-Überwachung Stellt verschiedene Standardprüfungen und -Richtlinien bereit.

Bereitgestellte Prüfungen

In den folgenden Tabellen sind die Standardprüfungen aufgelistet. Sie können diese Prüfungen nach Bedarf bearbeiten. Weitere Informationen zu einer bestimmten Prüfung finden Sie auf der Seite „Check Definitions“ (Prüfungsdefinitionen) (siehe Prüfungen und Richtlinien).

Linux

Typ	Name	Beschreibung
Event	os.linux.check-process	Zählt die Anzahl der laufenden Prozesse Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Typ	Name	Beschreibung
		finden Sie unter Blockereigniserstellung für nicht vorhandene Entitäten.
Ereignis	os.linux.check-system-cpu	Prüft den Prozentsatz der CPU-Auslastung
Event	os.linux.check-system-cpu-load	Prüft den Prozentsatz der CPU-Datenauslastung im Vergleich zu den konfigurierten Schwellenwerten
Ereignis	os.linux.metrics-system-disk-usage	Prüft die Bereitstellungspunkte und Metriken des Dateisystems
Event	os.linux.check-system-memory-percentage	Prüft den Prozentsatz der Speicherauslastung
Event	os.linux.check-system-memory-swap	Prüft die Auslastung des Arbeitsspeicher-Austauschs
Event	os.linux.check-threads-count	Zählt die Anzahl der im System ausgeführten Threads. Sendet eine Warnung, wenn diese Zahl größer als die Schwellenwerte für Warnung oder Kritisch ist.
Metrik	os.linux.metrics-memory-vmstat	Sammelt vmstat-Speichermetriken
Metrik	os.linux.metrics-process-status	Sammelt Prozessstatusmetriken, die für den Metrikparameter bereitgestellt werden
Metrik	os.linux.metrics-system-cpu	Erfasst CPU-Metriken, einschließlich Kernen.
Metrik	os.linux.metrics-system-cpu-load	Nutzt die Betriebszeit, um CPU-Lastmetriken zu erfassen
Metrik	os.linux.metrics-system-cpu-percentage	Sammelt Metriken für den CPU-Auslastungsprozentsatz, einschließlich des durchschnittlichen CPU-Auslastungsprozentsatzes.
Metrik	os.linux.metrics-system-disk	Sammelt Festplattenmetriken
Metrik	os.linux.metrics-system-disk-capacity	Sammelt Metriken zur Festplattenkapazität
Metrik	os.linux.metrics-system-disk-usage	Erfasst Metriken zur Datenträgernutzung, die den gesamten, verwendeten und verfügbaren Datenträgerspeicher sowie den Prozentsatz des verwendeten Arbeitsspeichers des Datenträgers bereitstellen.
Metrik	os.linux.metrics-system-memory	Sammelt Arbeitsspeichermetriken und stellt Daten in KB bereit.
Metrik	os.linux.metrics-system-memory-percent	Sammelt Metriken zur prozentuellen Speicherauslastung
Metrik	os.linux.metrics-Systembetriebszeit	Erfasst Systembetriebszeit in Sekunden.
Metrik	os.linux.metrics-reboot-count-today	Erfasst die Anzahl der heute durchgeführten Neustarts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Protokollüberwachung

Typ	Name	Beschreibung
Event	util.check-logs	Aktiviert die Überwachung von Protokolldateien, die einem normalen Benutzer gehören. Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Blockereigniserstellung für nicht vorhandene Entitäten.
Ereignis	util.check-logs-sudo	Aktiviert die Überwachung von Protokolldateien, die einem Root-Benutzer gehören. Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Blockereigniserstellung für nicht vorhandene Entitäten.

Linux-Netzwerküberwachung

Typ	Name	Beschreibung
Metrik	os.linux.metrics-Network-Interface	Ruft alle Netzwerkschnittstellen-bezogenen Metriken für Linux-Server ab.
Metrik	os.linux.metrics-netstat.tcp	Ruft Metriken für TCP-Socket-status aus netstat ab. Nützlich auf Web- oder Proxy-Servern mit hohem Datenverkehr mit einer großen Anzahl von kurzlebigen TCP-Verbindungen, die kommen und gehen.

Windows-Protokollüberwachung

Typ	Name	Beschreibung
Event	os.windows.check-log	Aktiviert die Überwachung von Protokolldateien auf einem Windows-Server.

Windows

Typ	Name	Beschreibung
Ereignis	os.windows.check-disk-name	Verwendet den Namen des Speicherlaufwerks als Eingabe und überprüft, ob das Laufwerk vorhanden ist. Gibt einen Wert „KRITISCH\WARNUNG\OK“ basierend auf dem angegebenen Parameter zurück.
Ereignis	os.windows.check-event-log	Misst Windows Ereignisprotokoll für Parameterschwellenwerte und gibt ein KRITISCHES\WARNENDES\OK-Ereignis zurück.
Ereignis	os.windows.check-event-log-count	Misst Windows Ereignisprotokoll für Parameterschwellenwerte und gibt ein KRITISCHES\WARNENDES\OK-Ereignis zurück. Stellt Informationen zur Anzahl der Ereignisse bereit, die innerhalb einer angegebenen Dauer für eine einzelne Protokolldatei und eine einzelne ID aufgetreten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows (Fortsetzung)

Typ	Name	Beschreibung
		Gibt auch die Filter an, die zum Abrufen von Ereignissen für eine bestimmte einwertige Windows-Ereignisebene und den Anbieternamen angewendet werden sollen. Das Abrufen von Ereignissen aus mehreren Protokolldateien wird nicht unterstützt. Die Anzahl der Ereignisse wird angegeben, ohne Details zu jedem Ereignis.
Ereignis	os.windows.check-event-log-details	Sammelt und filtert Windows Ereignisprotokolle basierend auf Duration_Hour , Event_log_level Und Log_file Werte. Ruft und Filter ab Windows Ereignisprotokolle gemäß den angegebenen Parametern. Gibt Details zu den Ereignissen mit dem Status „KRITISCH“, „WARNUNG“ oder „OK“ basierend auf dem angegebenen Schweregrad zurück. Unterstützt am Windows Version 7 und höher.
Ereignis	os.windows.check-env-variables	Überprüft die Umgebungsvariablen mit einem regulären Ausdruck und gibt entweder einen zurück *WARNING*Oder *OK*Wert. Wenn nach der Agent-Installation eine neue Systemvariable erstellt wird, müssen Sie den Agent neu starten. Diese Prüfung kann nur auf die Anwendervariablen zugreifen, die dem aktuellen Anwender zugeordnet sind (während der Agent-Installation verwendet).
Ereignis	os.windows.check-file-hashcode-update	Verwendet den Pfad und den MD5-Hashcode der Datei als Eingabe und überprüft, ob der Dateiinhalt geändert wurde. Gibt einen zurück *CRITICAL*, *WARNING*, Oder *OK*Wert. Für die überwachte Datei sind Leseberechtigungen erforderlich.
Ereignis	os.windows.check-file-update	Verwendet den Pfad und das Intervall der Datei als Eingabe und überprüft, ob der Dateiinhalt geändert wurde. Gibt einen zurück *CRITICAL*, *WARNING*, Oder *OK*Wert. Für die überwachte Datei sind Leseberechtigungen erforderlich.
Ereignis	os.windows.check-modules	Überprüft, ob die Liste der Module vorhanden ist.
Ereignis	os.windows.check-processor-queue-length	Prüft die Länge der Prozessorwarteschlange
Event	os.windows.check-system-cpu-load	Prüft die CPU-Last mit dem Befehl *typeperf*
Event	os.windows.check-system-disk	Prüft die Festplattenauslastung unter bestimmten Parametern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows (Fortsetzung)

Typ	Name	Beschreibung
Event	os.windows.check-system-memory	Erfasst die RAM-Auslastung
Ereignis	os.windows.check-system-patch	Überprüft die Installation des System-Patches. Gibt entweder einen zurück *WARNING*Oder *OK*Wert.
Ereignis	os.windows.check-system-process	Prüft die Aufgabenliste des Benutzers, um laufende Prozesse zu ermitteln
Ereignis	os.windows.check-user-account	Verwendet die Liste der Anwendernamen als Eingabe und überprüft, ob der Anwenderaccount aktiv ist. Gibt einen zurück *CRITICAL*, *WARNING*, Oder *OK*Wert.
Ereignis	os.windows.check-windows-directory	Prüft, ob ein Verzeichnis vorhanden ist
Event	os.windows.check-windows-pagefile	Erfasst die Auslastung der Auslagerungsdatei und vergleicht sie mit den Schwellenwerten für Warnung und Kritisch
Event	os.windows.check-windows-process	Prüft, ob ein Benutzereingabeprozess ausgeführt wird
Event	util.check-windows-service	Prüft, ob unter Windows ein vom Benutzer angegebener Service ausgeführt wird Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Blockereigniserstellung für nicht vorhandene Entitäten.
Metrik	os.windows.metrics-process-status	Ruft die Anzahl der ausgeführten Instanzen, den Prozentsatz der CPU-Auslastung und die Arbeitsspeichernutzung (in Kilobyte) des angegebenen ab Windows Prozess.
Metrik	os.windows.metrics-processor-queue	Erfasst die Länge der Prozessorwarteschlange
Metrik	os.windows.metrics-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde
Metrik	os.windows.metrics-system-disk-usage	Sammelt Metriken zur Festplattenauslastung
Metrik	os.windows.metrics-system-memory-percent	Erfasst die RAM-Auslastung pro Sekunde und stellt den Prozentsatz des freien physischen, freien virtuellen, gesamten physischen Arbeitsspeichers und des gesamten virtuellen Arbeitsspeichers bereit.
Metrik	os.windows.metrics-system-network	Sammelt Netzwerkmetriken
Metrik	os.windows.metrics-system-uptime	Erfasst die Systemverfügbarkeit
Metrik	util.metrics-windows-perf-counters	(Keine Beschreibung)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID Server

Typ	Name	Beschreibung
Event	app.mid.check-active	Prüft anhand des Vorkommens von LogStatusMonitor im MID-Protokoll, ob der MID-Server aktiv ist
Events	app.mid.check-logs-mid	Prüft die MID-Protokolle auf Fehler
Metrik	app.mid.metrics-stats	Sammelt Informationen zum MID-Server aus dem Protokoll und gibt Metriken zurück

HAProxy-Überwachung

Typ	Name	Beschreibung
Ereignis	check-haproxy	Ruft ab HAProxy Details zum Lastenausgleichsmodul, um zu bestimmen, ob er ausgeführt wird.
Metrik	metrics-check-haproxy	Ruft ab HAProxy Lastenausgleichsmodul-Metriken, um zu bestimmen, ob es ausgeführt wird.

HTTP (im Proxy-Modus auszuführen)

Typ	Name	Beschreibung
Event	util.check-http-response	Verwendet eine URL oder eine Kombination aus Host, Pfad, Port und SSL und sucht nach einer Antwort „200“, die einem Muster entspricht, sofern eines angegeben ist. Kann Client-Zertifikate nutzen
Event	util.check-http-follow-redirect	Stellt sicher, dass die URL die maximale Anzahl von Weiterleitungen nicht überschreitet
Metrik	util.metrics-http-curl	Ruft HTTP-Endpunktmetriken mit curl ab

Zusätzliche HTTP-Prüfungen (keine Richtlinie)

Typ	Name	Beschreibung
Ereignis	util.check-http-response-code	Löst ein kritisches Ereignis aus, wenn der URL-Antwortcode nicht mit dem regulären Ausdruck übereinstimmt.

Active Directory-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	metrics.windows.active-directory	Sammelt Active Directory-Metriken auf dem Windows-Host. Verwendung: Winchecks metric-	Wincheckt metric-Windows-Active-dir {{if .Labels.params_scheme}} -S

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
		Windows-Active-dir -s hostname	{{.Labels.params_scheme}} {{end}}

Apache

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.apache.metrics-apache	Ruft Apache HTTP-Servermetriken ab	2.4.x

Apache Kafka

Typ	Event/Metrik	Beschreibung	Mindestversi
Ereignis	kafka.check-zookeeper-status	Löst ein kritisches Ereignis aus, wenn der gehostete ZooKeeper von Apache Kafka ausgefallen ist.	Zookeeper 3.1.2
Ereignis	kafka.check-topic-replicas	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Replikaten hat.	Zookeeper 3.1.2
Ereignis	kafka.check-topic-replication-factor	Löst ein kritisches Ereignis aus, wenn der Replikationsfaktor von mindestens einem Thema über oder unter dem angegebenen Replikationsfaktorparameter liegt.	Zookeeper 3.1.2
Ereignis	kafka.check-topic-leader	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Führungskräften oder einem nicht bevorzugten Replikat als Führungskraft aufweist.	Zookeeper 3.1.2
Ereignis	kafka.check-topic-partitions	Löst ein kritisches Ereignis aus, wenn die Anzahl der Partitionen für ein Thema kleiner als der Parameter „min_partitions“ ist.	Zookeeper 3.1.2
Ereignis	kafka.check-broker-status	Löst ein kritisches Ereignis aus, wenn der Kafka-Broker auf dem Host ausgefallen ist.	Kafka 0.10.1.0
Metrik	kafka.metrics.broker	Sammelt Kafka-Broker-Metriken vom Host.	Kafka 0.10.1.0
Metrik	kafka.metrics.zookeeper	Sammelt ZooKeeper-Metriken vom Host.	Zookeeper 3,5.0-alpha

Azure Kubernetes (K8s) Service-Metriken

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	azure.metrics-k8s-service	Stellt Pod bereit, Knoten und Metriken auf Clusterebene aus allen Azure Kubernetes-Services in Metrikform. Verwendung: metrics-azure-k8s-service.rb	metrics-azure-k8s-service.rb -r {{.labels.params_ci_region}} {{-s {{if.labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Kubernetes (K8s) Service-Metriken (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		Befehlsbeispiel: `metrics-azure-k8s-service.rb -S {{.labels.params_subscription_id}} -r westus2`	

Azure VM-Metriken

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	azure.metrics-vm-cpu	Stellt CPU-bezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T cpu`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-disk	Stellt laufwerksbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T disk`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-memory	Stellt arbeitsspeicherbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T memory`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-network	Stellt netzwerkbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}} -T {{.labels.params_type}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Metriken (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		{{.labels.params_subscription_id}} -T network	
Metrik	azure.metrics-vm-flows	Stellt Flows-bezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: ./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T flows	metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}} -T {{.labels.params_type}}

GCP-GCE-Metriken

Typ	Event/Metrik	Beschreibung
Metrik	gcp.Metriken.GCE	Ruft Metriken aus GCP für ab Google Compute-Engine.
Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetriken für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar.
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server bereitgestellten Ressourcen verfügbar.
Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
Metrik	glassfish.metric-deploy-Apps	Stellt die Metrikausgabe der auf dem GlassFish-Server bereitgestellten Anwendungen bereit.
Metrik	glassfish.metric-Deployment-Lifecycle	Stellt Anwendungen für Lebenszyklusmetriken bereit, die auf dem GlassFish-Server bereitgestellt werden.

Glassfish

Typ	Name	Beschreibung
Metrik	glassfish.metric-jvm-level	Ruft JVM-Metriken auf dem GlassFish-Server ab.
Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetriken für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Glassfish (Fortsetzung)

Typ	Name	Beschreibung
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server bereitgestellten Ressourcen verfügbar.
Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
Metrik	glassfish.metric-deploy-Apps	Stellt die Metrikausgabe der auf dem GlassFish-Server bereitgestellten Anwendungen bereit.
Metrik	glassfish.metric-Deployment-Lifecycle	Stellt Anwendungen für Lebenszyklusmetriken bereit, die auf dem GlassFish-Server bereitgestellt werden.

IBM WebSphere AS

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.websphere.metrics-websphere	Gibt IBM WebSphere-Anwendungsservermetriken zurück. Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den IBM Websphere AS-Installationsverzeichnissen verfügt.	9

IIS

Typ	Event/Metrik	Beschreibung	Mindestversi
Event	app.iis.check-iis-alive	Prüft, ob IIS ausgeführt wird	-
Event	app.iis.check-iis-current-connections	Prüft die Anzahl der aktuellen Verbindungen zum IIS-Server und deren Status, abhängig von der Eingabe. Standardmäßig sind alle Sites mit dem IIS-Server verbunden.	-
Metrik	app.iis.metrics-iis	Gibt IIS-Metriken zurück	-

JBoss/WildFly

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.jboss.metrics-jboss	Ruft JBoss- bzw. WildFly-Servermetriken ab	16, 17

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JBoss/WildFly (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Mindestversi
		Stellen Sie sicher, dass der Anwender, der den Service Desk-Mitarbeiter ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in verfügt JBoss/WildFly Installationsverzeichnisse.	

Kubernetes

Typ	Event/ Metrik	Beschreibung	Befehl
Event	k8s.check-kube-apiserver-available	Überprüft, ob der Kubernetes-API-Server aktiv ist.	check-kube-apiserver-available.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Event	k8s.check-kube-nodes-ready	Überprüft, ob Kubernetes-Knoten betriebsbereit sind.	check-kube-nodes-ready.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Event	k8s.check-kube-pods-pending	Misst den Schwellenwert, bis zu dem sich Pods im Status „Ausstehend“ befinden. Bestimmen Sie den Schwellenwert, indem Sie den Wert des Prüfparameters *pending_timeout* festlegen (Standard = 300 Sekunden).	check-kube-pods-pending.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Event	k8s.check-kube-pods-restarting	Überprüft die Pods, die neu gestartet werden. Bestimmen Sie den Schwellenwert, indem Sie den Wert des Prüfparameters festlegen (Standard = 10).	check-kube-pods-restarting.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}} {{if .labels.params_restart}} -r {{.labels.params_restart}} {{end}}
Event	k8s.check-kube-pods-running	Überprüft die Pods, die sich im Status „Wird ausgeführt“ befinden. Konfigurieren Sie den Schwellenwert im Prüfparameter *not_ready_time* in Sekunden (Standard = 0).	check-kube-pods-running.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}} {{if .labels.params_not_ready_time}} -time {{.labels.params_not_ready_time}} {{end}}
Event	k8s.check-kube-pods-runtime	Überprüft, ob Pods länger als erwartet ausgeführt werden. Konfigurieren Sie den Schwellenwert im Prüfparameter (in Sekunden). Sie können beide Schwellenwerte, WARNUNG und KRITISCH, konfigurieren.	check-kube-pods-runtime.rb {{if .labels.params_critical}} -c {{.labels.params_critical}} {{end}} {{if .labels.params_warning}} -w {{.labels.params_warning}} {{end}} {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Event	k8s.check-kube-service-available	Überprüft, ob Kubernetes-Services ausgeführt werden. Fügen Sie die Liste der zu überwachenden Services dem Feld *check_param* des Service	check-kube-pods-runtime.rb {{if .labels.params_critical}} -c {{.labels.params_critical}} {{end}} {{if .labels.params_warning}} -w

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kubernetes (Fortsetzung)

Typ	Event/ Metrik	Beschreibung	Befehl
		als kommagetrennte Werte (ohne Leerzeichen) hinzu. Wenn Sie ungültige Services eingeben, schlägt die Prüfung fehl.	{{.labels.params_warning}} {{end}} {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Metrik	k8s.metrics-pods	Stellt eine Pod-Anzahl für alle verfügbaren Services bereit.	metrics-pods.rb {{if .labels.params_api_server}} -s {{.labels.params__api_server }} {{end}}

MsSQL

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.msssql.metrics-mssql	Ruft MSSQL-Datenbankmetriken ab	2016
Metrik	app.metrics-mssql-query	Generische MSSQL-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann.	2016

MySQL

Typ	Event/Metrik	Beschreibung	Mindestversi
Event	app.mysql.check-mysql-alive	Prüft, ob die MySQL-Datenbank ausgeführt wird	5.7, 8
Event	app.mysql.check-mysql-threads	Prüft die Anzahl der laufenden Threads in der MySQL-Datenbank. Bestimmt den Status je nach Eingabe: OK, Warnung oder Kritisch.	5.7, 8
Event	util.check-mysql-query	Prüft die Länge des Ergebnissatzes einer MySQL-Abfrage Für diese Prüfung müssen Sie auf dem MySQL-Server die Authentifizierungsmethode native_password verwenden.	5.7, 8
Metrik	app.mysql.metrics-mysql	Gibt MySQL-Datenbankmetriken zurück	5.7, 8
Metrik	app.mysql.metrics-mysql-processes	Gibt Metriken für MySQL-Datenbankprozesse zurück	5.7, 8
Metrik	util.metrics-mysql-query	Erzeugt eine formatierte Metrik für die Länge des Ergebnissatzes einer MySQL-Abfrage	5.7, 8

MongoDB

Typ	Event/Metrik	Beschreibung	Mindestversion
Ereignis	app.mongodb.check-mongodb-alive	Überwacht, ob der MongoDB-Server aktiv ist, und erstellt Warnungen für den	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Mindestversion
		MongoDB-Server-Integritätsstatus.	
Ereignis	app.mongodb.check-mongodb-metrics	Erstellt Warnungen für eine der MongoDB-Metriken basierend auf dem Schwellenwert.	
Metrik	app.mongodb.metrics-mongodb	Gibt Metriken des MongoDB-Servers und aller Datenbanken zurück.	

Oracle

Typ	Event/Metrik	Beschreibung	Mindestversi
Event	app.oracle.check-oracle-alive	Prüft, ob die Oracle-Datenbank ausgeführt wird	12c, 18c
Metrik	app.oracle.metrics-oracle	Gibt Oracle-Datenbankmetriken zurück	12c, 18c
Metrik	util.metrics-oracle-query	Generische Oracle-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann	12c, 18c

Oracle WebLogic AS

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.weblogic.metrics-weblogic	Gibt Metriken für Oracle WebLogic-Anwendungsserver zurück Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den WebLogic-Installationsverzeichnissen verfügt.	12cR2

Tomcat

Typ	Event/Metrik	Beschreibung	Mindestversi
Metrik	app.tomcat.metrics-tomcat	Gibt Metriken für den Apache Tomcat-Server zurück.	8.5.27, 9.x

App

Typ	Name	Beschreibung
Event	util.check-snmp	SNMP-Prüfung, die den Metrikwert mit dem Standardwert vergleicht. Erfordert Eingaben wie Server, Port, SNMP-Community und Grenzwerte
Metrik	util.metrics-snmp	Sammelt Metriken aus einem SNMP-OID-Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

App (Fortsetzung)

Typ	Name	Beschreibung
Metrik	util.metrics-snmp-bulk-sn	Sammelt Metriken aus einer SNMP-Tabellen-OID und gibt das Ergebnis als Tabelle zurück

Serviceerweiterungen (kann jeder Richtlinie zugeordnet werden)

Typ	Event/Metrik	Beschreibung	Befehl
Metrik (Windows)	os.windows.metrics-service-status	Erfasst den Windows-Servicestatus und stellt eine Metrik der Anzahl der ausgeführten Services bereit.	`winchecks metric-windows-service-status -S Wcmsvc --scheme hostname.proc`

Lackieren

Typ	Name	Beschreibung
Metrik	app.varnish.metrics-varnish	Sammelt Varnish-Metriken vom Host.

vSphere

Typ	Name	Beschreibung
Metrik	vsphere.metric-VirtualMachine	Ruft Metriken für die virtuelle vSphere-Maschine ab.
Metrik	vsphere.metric-Datastore	Ruft Metriken für den vSphere-Datenspeicher ab.
Metrik	vsphere.metric-Datacenter	Ruft Metriken für das vSphere-Rechenzentrum ab.
Metrik	vsphere.metric-ESX_Server	Ruft Metriken für den vSphere ESX-Server oder das HostSystem ab

Zscaler

Typ	Name	Beschreibung
Metrik	zscaler-monitoring-check	Überprüft, ob die App Zscaler ordnungsgemäß ausgeführt wird.
Metrik	zscaler-remediation-check	Fährt die App Zscaler herunter, startet sie neu und erstellt einen Incident. Wird nur ausgeführt, wenn bei zscaler-monitoring-check ein Fehler auftritt.

CPU-Erweiterungen

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	os.windows.metrics-system-cpu	Erfasst CPU-Kernmetriken.	`winchecks metric-windows-`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CPU-Erweiterungen (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
			cpu --scheme hostname.proc

Datenträgererweiterungen – Linux-Ereignisse (kann jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.linux.check-disk-ioTimeWeighted	Misst Datenträger ioTimeWeighted Wert, gibt einen zurück **KRITISCH\WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-ioTimeWeighted.rb
os.linux.check-disk-sectorsWritten	Misst die Gesamtzahl der erfolgreich geschriebenen Sektoren, wobei ein zurückgegeben wird **KRITISCH\WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-sectorsWritten.rb
os.linux.check-disk-sectorsRead	Misst die Gesamtzahl der erfolgreich gelesenen Sektoren des Datenträgers, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-sectorsRead.rb
os.linux.check-disk-readTime	Misst die Gesamtzahl der Millisekunden, die von allen Schwellenwerten für Lesevorgänge ausgegeben werden, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-readTime.rb
os.linux.check-disk-writes	Misst die Gesamtzahl der erfolgreich abgeschlossenen Schreibvorgänge, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-writes.rb
os.linux.check-disk-reads	Misst die Gesamtzahl der erfolgreich abgeschlossenen Lesevorgänge, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Nachricht	check-disk-reads.rb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträgererweiterungen – Linux-Ereignisse (kann jeder Richtlinie zugeordnet werden) (Fortsetzung)

Event/Metrik	Beschreibung	Befehl
	gemäß den in den Parametern angegebenen Schwellenwerten.	
os.linux.check-disk-writesMerged	Misst Datenträger schreibenMerged Wert, gibt einen zurück **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-writesMerged.rb
os.linux.check-disk-readsMerged	Misst Datenträger readsMerged Wert, gibt einen zurück **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-readsMerged.rb
os.linux.check-disk-writeTime	Misst die Gesamtzahl der Millisekunden, die alle Schreibvorgänge aufwenden, wobei ein zurückgegeben wird **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-writeTime.rb
os.linux.check-disk-ioInProgress	Misst Datenträger ioInProgress Wert, gibt einen zurück **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-disk-ioInProgress.rb
os.linux.check-disk-iotime	Misst Datenträger-ioTime Wert, gibt einen zurück **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	Check-Disk-ioTime.rb

Datenträgererweiterungen – Windows-Ereignisse (kann jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.windows.check-disk-AvgSecWrite	Misst durchschnittliche Datenträger-Schreibvorgänge pro Sekunde, wobei ein zurückgegeben wird **KRITISCH\WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen.	winchecks check-windows-AvgDisksec-write -w 1 -c 0
os.windows.check-disk-ReadBytes-sec	Misst Datenträger-Lesebytes Wert pro Sekunde, gibt einen	winchecks check-windows-DiskReadBytes-sec -w 1 -c 0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträgererweiterungen – Windows-Ereignisse (kann jeder Richtlinie zugeordnet werden) (Fortsetzung)

Event/Metrik	Beschreibung	Befehl
	zurück **KRITISCH\WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	
os.windows.check-disk-WriteBytes-sec	Misst Datenträger-Schreibbytes Wert pro Sekunde, gibt einen zurück **KRITISCH \WARNUNG\OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	winchecks check-windows-DiskWriteBytes-sec -w 1 -c 0
os.windows.check-disk-AvgSecRead	Misst die durchschnittlichen Datenträger-Lesezugriffe pro Sekunde und gibt einen zurück **KRITISCH\WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	winchecks check-windows-AvgDisksec-read -w 1 -c 0

Datenträgererweiterungen – Windows-Metriken (kann jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.windows.metrics-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite • DiskReadBytesPerSec • DiskWriteBytesPerSec	winchecks metric-windows-disk

Speichererweiterungen (kann jeder Richtlinie zugeordnet werden)

Typ	Event/Metrik	Beschreibung	Befehl
Ereignis (Linux)	os.linux.check-free-physical-memory	Misst den Prozentsatz des freien physischen Arbeitsspeichers des Linux-Systems und gibt einen zurück **KRITISCH \WARNUNG\OK** Ereignisnachricht gemäß den in den Parametern angegebenen Schwellenwerten.	check-free-physical-memory -w 10 -c 5
Ereignis (Linux)	os.linux.check-free-virtual-memory	Misst den Prozentsatz des freien virtuellen	check-free-virtual-memory -w 10 -c 5

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichererweiterungen (kann jeder Richtlinie zugeordnet werden) (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		Arbeitsspeichers des Linux-Systems, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Ereignisnachricht gemäß den in den Parametern angegebenen Schwellenwerten.	
Ereignis (Windows)	os.windows.check-free-physical-memory	Misst den Prozentsatz des freien physischen Arbeitsspeichers des Windows-Systems und gibt einen zurück **KRITISCH \WARNUNG\OK** Ereignisnachricht gemäß den in den Parametern angegebenen Schwellenwerten.	`Winchecks Check-Windows-free-physfical-Memory -W 10 -c 5`
Ereignis (Windows)	os.windows.check-free-virtual-memory	Misst den Prozentsatz des freien virtuellen Arbeitsspeichers des Windows-Systems, wobei ein zurückgegeben wird **KRITISCH \WARNUNG\OK** Ereignisnachricht gemäß den in den Parametern angegebenen Schwellenwerten.	`winchecks check-windows-free-physical-memory -w 10 -c 5`
Metrik (Windows)	os.windows.metrics-system-memory	Sammelt die folgenden Arbeitsspeichermetriken: • FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory • TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemorySize	`winchecks metric-windows-memory --scheme hostname.proc`

Prozesserweiterungen (kann jeder Richtlinie zugeordnet werden)

Typ	Event/Metrik	Beschreibung	Befehl
Ereignis (Linux)	os.linux.check-process-cpu	Misst die CPU-Auslastung des Linux-	`check-process-cpu.rb -p acc -c 95 -w 85`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozesserweiterungen (kann jeder Richtlinie zugeordnet werden) (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		Prozesses und gibt einen zurück **KRITISCH \WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	
Ereignis (Linux)	os.linux.check-process-memory	Misst die Auslastung des Linux-Prozessspeichers und gibt einen zurück **KRITISCH \WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	`check-process-memory.rb -p acc -c 95 -w 85`
Metrik (Linux)	os.linux.metrics-process-usage	Erfasst den Linux-Prozessstatus, einschließlich der vom Prozess verwendeten CPU- und Arbeitsspeicherdaten.	`metrics-process-usage.rb -p acc -s hostname.proc`
Ereignis (Windows)	os.windows.check-process-cpu	Misst die CPU-Auslastung des Windows-Prozesses und gibt einen zurück **KRITISCH \WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	`winchecks check-windows-process-cpu-p acc -c 95 -w 85`
Ereignis (Windows)	os.windows.check-process-memory	Misst die Auslastung des Windows-Prozessspeichers und gibt einen zurück **KRITISCH \WARNUNG \OK** Nachricht gemäß den in den Parametern angegebenen Schwellenwerten.	`winchecks check-windows-process-memory-p acc -c 95 -w 85`
Metrik (Windows)	os.Windows.metrics-Process-usage	Erfasst den Windows-Prozessstatus, einschließlich der vom Prozess verwendeten CPU- und Arbeitsspeicherdaten.	`winchecks metric-windows-process-status -n Svchost -s hostname.proc`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Agent-Richtlinien

In dieser Tabelle sind die unterstützten Richtlinien von Agent Client Collector for Monitoring aufgelistet, denen die Prüfungsdefinitionen zugeordnet sind. Richtlinien bestehen aus den überwachten CIs und den Prüfungen, die für sie ausgeführt werden.

Name	Beschreibung	Prüfungen
Apache Events	Überwacht laufende Apache HTTP-Webserver Um die Überwachung zu aktivieren, wenn der Prozess aktiv ist, aktivieren Sie die entsprechende Prüfung: • Für Linux: os.linux.check-process • Für Windows: os.windows.check-windows-process Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen für die Standardauthentifizierung an.	• os.linux.check-process • os.windows.check-windows-process
Apache Metrics	Überwacht laufende Apache HTTP-Webserver Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen für die Standardauthentifizierung an.	app.apache.metrics-apache
Apache Kafka Ereignisse	Überwacht den Status von Kafka-Broker, Kafka-Themen, Teilnahmen, Replikaten und Zookeeper.	
Apache Kafka Metriken	Überwacht und erfasst Metriken von Kafka Broker und Kafka Zookeeper.	

Azure DB-Metriken	Überwacht Azure Datenbanken in einem Azure Rechenzentrum.
	
	So aktivieren Sie die Prüfungen der Richtlinie:
	• Konfigurieren Sie einen Proxy-Agent.
	• Fügen Sie die folgenden Azure-Serviceprinzipalanmeldeinformationen hinzu:
	  ○ Mandanten-ID
	  ○ Client-ID
	  ○ Geheimer Schlüssel
	• Konfigurieren Sie die Authentifizierungsmethode als **Geheimer Clientschlüssel** .	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	• Fügen Sie der Richtlinie Azure-Anmeldeinformationen hinzu. • Geben Sie an *subscription_id*Wert in jeder Prüfungsinstanz. Der standardmäßig überwachte CI-Typ ist cmdb_ci_Azure_Datacenter, die Bindung erfolgt jedoch in der Cloud-Datenbank (cmdb_ci_Cloud_database). Weitere Informationen zum Konfigurieren einer Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.	
Azure Kubernetes (K8s) Service-Metriken	Überwacht das Azure-CI *cmdb_ci_azure_datacenter*. Wird mit dem Kubernetes-Datencluster *cmdb_ci_kubernetes_cluster* verbunden.	azure.metrics-k8s-service Details finden Sie unter Azure-Systemüberwachung – Standardprüfungen und Richtlinien.
Azure VM-Metriken	Überwacht das Azure-CI *cmdb_ci_azure_datacenter*. Wird mit der VM-Instanz *cmdb_ci_vm_instance* verbunden.	• azure.metrics-vm-cpu • azure.metrics-vm-disk • azure.metrics-vm-memory • azure.metrics-vm-network • azure.metrics-vm-flows Details finden Sie unter Azure-Systemüberwachung – Standardprüfungen und Richtlinien.
Basic Discovery	Führt alle 12 Stunden für alle Agents eine Basiserkennung mit ServiceNow Discovery aus. Diese Prüfung extrahiert Basisinformationen über den Host und seine laufenden Prozesse. Die Hostinformationen werden verwendet, um in der CMDB den entsprechenden Host zu erstellen. Anhand der laufenden Prozesse werden die klassifizierten Anwendungs-CIs erstellt. Sie benötigen erweiterte BS-Berechtigungen, um mit dem netstat-Befehl Ports zu erkennen. Der auszuführende Befehl ist von Ihrem Betriebssystem abhängig:	check-discovery-basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	• Linux: `sudo -n netstat -antp` • Windows: `netstat -anop TCP`	
Docker Container Metrics	Sammelt Leistungsmetriken für Docker-Container Geben Sie die Anmeldeinformationen von Benutzern an, die Mitglieder der Docker-Benutzergruppe sind oder die über sudo-Rechte verfügen. Geben Sie diese Anmeldeinformationen auf der Registerkarte **Credentials** (Anmeldeinformationen) des Richtlinienformulars an.	container.docker.metrics-docker
Docker Engine Metrics	Sammelt allgemeine Metriken für die Docker-Engine Stellt die Anmeldeinformationen eines Benutzers bereit, der entweder Mitglied der Docker-Benutzergruppe ist oder dem auf der Registerkarte **Anmeldeinformationen** sudo-Rechte zugewiesen wurden. Um laufende Prüfungen über diese Richtlinie zu aktivieren, fügen Sie der Docker-Benutzergruppe auf dem Computer, auf dem der Agent ausgeführt wird, den Benutzer servicenow hinzu.	container.docker.metrics-docker-info
F5 SNMP Events	Beispiel für die Verwendung von SNMP-Prüfungen Da der Agent nicht auf SNMP-Geräten ausgeführt wird, geben Sie Folgendes an, um diese Richtlinie durchzuführen: • Einen Proxy-Agent und Anmeldeinformationen. • Den Host des Proxy-Agent. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der SNMP-Community für die Verbindung zum Server an.	util.check-snmp
F5 SNMP Metrics	Beispiel für die Verwendung von SNMP-Metriken Da der Agent nicht auf SNMP-Geräten ausgeführt wird, geben Sie Folgendes an, um diese Richtlinie durchzuführen:	• util.metrics-snmp • util.metrics-snmp-bulk-sn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	• Einen Proxy-Agent und Anmeldeinformationen. • Den Host des Proxy-Agent. Geben Sie auf der Registerkarte **Anmeldeinformationen** die Anmeldeinformationen der SNMP-Community für die Verbindung zum Server an.	
Glassfish-Metriken	Führt Metrikprüfungen auf dem GlassFish-Server aus. GlassFish-Metriken werden in unterstützt ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar über ServiceNow Store .	
HAProxy Ereignisse	Ruft ab HAProxy Details zum Lastenausgleichsmodul, um zu bestimmen, ob er ausgeführt wird. HAProxy Ereignisse werden in unterstützt ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar über ServiceNow Store .	
HAProxy Metriken	Ruft ab HAProxy Lastenausgleichsmodul-Metriken, um zu bestimmen, ob es ausgeführt wird. HAProxy Metriken werden in unterstützt ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar über ServiceNow Store .	
HTTP Entry Points Events	Führt die Prüfung util.check-http-follow-redirect für alle HTTP-Einstiegspunkte aus, die zu den Business Services der Anwendung gehören. Die Services werden mittels Richtlinienfilter ausgewählt. Die Services definieren die Einstiegspunkte. • Zum Aktivieren dieser Prüfung ist eine neue Datenbankansicht verfügbar, die die Tabelle der Anwendungsservices mit der Tabelle der Einstiegspunkte kombiniert. • Sie können die Services filtern, um die Einstiegspunkte zu erhalten. • Warnungen, die Sie erhalten, sind automatisch an die Einstiegspunkte gebunden. Diese Warnungen wirken sich	util.check-http-follow-redirect

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	auf die Auswirkungsberechnung aus, da Einstiegspunkte berücksichtigt werden. • Für diese Richtlinie ist ein Proxy-Agent erforderlich.	
HTTP Entry Points Metrics	Wenn die Warnung beispielsweise an den Einstiegspunkt gebunden ist, identifiziert die Servicezuordnung ein Problem am Einstiegspunkt. • Die Metrik wird an das Einstiegspunkt-CI gebunden. In früheren Releases war die Metrik an den Service gebunden, und der Einstiegspunkt war die Ressource. • Für diese Richtlinie ist ein Proxy-Agent erforderlich.	util.metrics-http-curl
IIS Events	Überwacht laufende IIS-Server	• app.iis.check-iis-alive • app.iis.check-iis-current-connections
IIS Metrics	Überwacht laufende IIS-Server	app.iis.metrics-iis
JBoss/WildFly Application Server Events	Überwachung laufender JBoss/WildFly-Anwendungsserver Um die Überwachung zu aktivieren, wenn der JBoss-Prozess aktiv ist, aktivieren Sie os.linux.check-process. Der Parameter *jboss_home* in der Prüfungsinstanz wird als Speicherort für die JBoss-Installation angegeben.	os.linux.check-process
JBoss/WildFly Application Server Metrics	Überwacht laufende JBoss/WildFly-Anwendungsserver	app.jboss.metrics-jboss
Kubernetes	Überwacht den Zustand der Kubernetes-Infrastruktur, z. B. Cluster, Knoten, Pod-Status, API und Serviceverfügbarkeit. Bei der Ausführung von Kubernetes-Prüfungen: • Der Proxy-Agent muss aktiviert sein. • Geben Sie Kubernetes-Anmeldeinformationen ein, entweder eine Kombination aus Benutzername und Passwort oder ein Bearer-Token (aber nicht beides).	• k8s.check-kube-apiserver-available • k8s.check-kube-nodes-ready • k8s.check-kube-pods-pending • k8s.check-kube-pods-restarting • k8s.check-kube-pods-running • k8s.check-kube-pods-runtime

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	• Um die Richtlinie zu aktivieren und zu veröffentlichen, konfigurieren Sie den Wert *api_server* in den Prüfparameterdefinitionen jeder Prüfung mit einem der folgenden Werte: ○ https://127.0.0.1:<portnumber>/api (wenn API-Server und Agent auf demselben Server ausgeführt werden) ○ https://<api_server_url>/api (wenn API-Server und Agent auf demselben Server oder auf verschiedenen Servern ausgeführt werden) Um localhost als api_server zu verwenden, führen Sie den folgenden Befehl aus: "kubectl proxy -port=8081 &". • Führen Sie Discovery aus , um alle Kubernetes-CIs zu erkennen. Weitere Informationen finden Sie unter Kubernetes-Discovery .	• k8s.check-kube-service-available • k8s.metrics-pods
Linux log monitoring	Überwacht Protokolle auf laufenden Linux-Servern.	• util.check-logs • util.check-logs-sudo
Linux OS Events	Führt Linux-Prüfungen auf ausgeführten Linux-Servern aus.	• os.linux.check-process • os.linux.check-system-cpu • os.linux.check-system-cpu-load • os.linux.check-system-disk-usage • os.linux.check-system-memory-percentage • os.linux.check-system-memory-swap • os.linux.check-threads-count
Linux OS Metrics	Sammelt Linux-Metriken auf laufenden Linux-Servern	• os.linux.metrics-memory-vmstat • os.linux.metrics-process-status • os.linux.metrics-system-cpu • os.linux.metrics-system-cpu-load

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
		• os.linux.metrics-system-disk • os.linux.metrics-system-disk-capacity • os.linux.metrics-system-disk-usage • os.linux.metrics-system-memory • os.linux.metrics-system-memory-percentage • os.linux.metrics.reboot_count_today
MSSQL Events	Überwacht den Betriebsprozess von MSSQL-Servern. Führt os.windows.check-windows-process aus, um zu überwachen, wann der Serverprozess aktiv ist	os.windows.check-windows-process
MSSQL Metrics	Überwacht den Betriebsprozess von MSSQL-Servern. Führt app.mssql.metrics-mssql aus, um Metriken zu erfassen	app.mssql.metrics-mssql
MySQL DB Events	Überwacht laufende MySQL-Instanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.mysql.check-mysql-alive • app.mysql.check-mysql-threads • util.check-mysql-query
MySQL DB Metrics	Überwacht laufende MySQL-Instanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.mysql.metrics-mysql • app.mysql.metrics-mysql-processes • util.metrics-mysql-query
Netzwerk-Ping-Metriken	Überwacht die in erkannte ip-Adresse ServiceNow Instanz. Der überwachte CI-Typ cmdb_ci_Hardware ist an den entsprechenden Server gebunden:	Util.metrics-ping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Diese Richtlinie erfordert einen Proxy-Agent.	
Oracle DB Events	Überwacht laufende Oracle-Datenbankinstanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	app.oracle.check-oracle-alive
Oracle DB Metrics	Überwacht laufende Oracle-Datenbankinstanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.oracle.metrics-oracle • util.metrics-oracle-query
Self-Healing Events	Führt einen Ping-Befehl zu einem anderen Host aus. Diese Prüfung muss im Proxy-Modus ausgeführt werden.	util.check-ping
Tomcat Events	Überwacht laufende Apache Tomcat-Server Um die Überwachung zu aktivieren, wenn der Tomcat-Prozess aktiv ist, aktivieren Sie die entsprechende Prüfung: • Für Linux: os.linux.check-process • Für Windows: util.check-windows-service Wenn der Tomcat-Service unter einem anderen Namen ausgeführt wird, aktualisieren Sie den Wert des Parameters *service* der Prüfungsinstanz auf den korrekten Wert.	• os.linux.check-process • util.check-windows-service
Tomcat Metrics	Überwacht laufende Apache Tomcat-Server Wenn Tomcat-Metriken an einem anderen Port als dem Standardport (9000) ausgeführt werden, aktualisieren Sie den Wert des Parameters *port* der	app.tomcat.metrics-tomcat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Prüfungsinstanz auf den korrekten Portwert.	
Lackieren Sie Metriken	Überwacht und erfasst Metriken aus Varnish. Lackmetriken werden in unterstützt ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar über ServiceNow Store . Sie müssen die Discovery mithilfe von Anwendungsfingerabdrücken durchführen, bevor Sie Lackprüfungen ausführen. Details finden Sie unter Aktivieren Sie die Ausführung von Lackprüfungen.	
VSphere-Metriken	Überwacht und erfasst Metriken von vSphere. VSphere-Metriken werden in unterstützt ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar über ServiceNow Store . Diese Richtlinie erfordert einen Proxy-Agent.	
WebLogic Application Server Events	Überwacht laufende Oracle WebLogic-Anwendungsserver. Diese Richtlinie überwacht, ob der unter Linux ausgeführte WebLogic-Prozess aktiv ist. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	os.linux.check-process
WebLogic Application Server Metrics	Überwacht laufende Oracle WebLogic-Anwendungsserver. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an. Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den WebLogic-Installationsverzeichnissen verfügt.	app.weblogic.metrics-weblogic
WebSphere Application Server Events	Überwacht laufende IBM WebSphere-Server. Diese Richtlinie überwacht, ob der unter Linux ausgeführte WebSphere-Prozess aktiv ist.	os.linux.check-process

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	
WebSphere Application Server Metrics	Überwacht laufende IBM WebSphere-Server. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	app.websphere.metrics-websphere
Windows Protokollüberwachung	Überwacht Protokolle auf laufenden Windows-Servern.	os.windows.check-log Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Blockereigniserstellung für nicht vorhandene Entitäten.
Windows BS-Ereignisse	Führt Windows-Prüfungen auf ausgeführten Windows-Servern aus.	• os.windows.check-processor-queue-length • os.windows.check-system-cpu-load • os.windows.check-system-disk • os.windows.check-system-memory • os.windows.check-system-process • os.windows.check-windows-directory • os.windows.check-windows-directory • os.windows.check-windows-directory • os.windows.check-windows-pagefile • os.windows.check-windows-process
Windows BS-Ereignisse: Erweitert	Wird Ausgeführt Windows Prüft, um Verzeichnisse und Dateien in zu überwachen Windows Server.	• Check-Directory-file-count • Check-Directory-Integrity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
		• Überprüfen Sie das Dateialter • Check-file-response-time • Dateigröße überprüfen • Dateibereich überprüfen • os.windows.check-directory-space
Windows BS-Metriken	Sammelt Windows-Metriken auf laufenden Windows-Servern	• os.windows.metrics-processor-queue-len • os.windows.metrics-system-cpu-load • os.windows.metrics-system-disk-usage • os.windows.metrics-system-memory-percent • os.windows.metrics-system-network • os.windows.metrics-system-uptime
Zscaler-Überwachungsrichtlinie	Führt die Zscaler-Überwachung für alle CIs eines Computers aus.	• zscaler-monitoring-check • zscaler-remediation-check

Active Directory-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Active Directory-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Active Directory-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.DRA_Inbound_Bytes_after_compressed/sec			Zeigt die komprimierte Größe der eingehenden komprimierten Replikationsdaten an (Größe nach der Komprimierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			von DSAs in andere Standorte).
active_dir.DRA_Inbound_Bytes_before_compressed/sec			Zeigt die Originalgröße der eingehenden komprimierten Replikationsdaten an (Größe vor der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Inbound_Bytes_not_compressed/sec			Zeigt die Anzahl der eingehenden replizierten Bytes an, die nicht an der Quelle komprimiert wurden (d. h. von DSAs in den gleichen Standort).
active_dir.DRA_Inbound_Bytes_Total/sec (empfohlene Metrik)			Zeigt die Gesamtzahl der eingehenden replizierten Bytes an. Dieser Zähler ist die Summe der Anzahl unkomprimierter Bytes (nie komprimiert) und der Anzahl komprimierter Bytes (nach der Komprimierung).
active_dir.DRA_Inbound_Full_Sync_Objects_Remaining (empfohlene Metrik)			Zeigt die Anzahl der bis zum Abschluss der vollständigen Synchronisierung verbleibenden Objekte an (falls festgelegt).
active_dir.DRA_Inbound_Object_Updates_Remaining_in_Packet			Zeigt die Anzahl der empfangenen Objektaktualisierungen im aktuellen Verzeichnisreplikations-Aktualisierungspaket, die auf den lokalen Server nicht angewendet wurden.
active_dir.DRA_Inbound_Objects/sec			Zeigt die Rate an, zu der Replikationsaktualisierungen von Replikationspartnern vom lokalen Verzeichnisdienst angewendet werden. Bei diesem Zähler

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			werden Änderungen ausgeschlossen, die empfangen, aber nicht angewendet wurden (z. B. weil die Änderung bereits vorgenommen wurde). Diese Metrik gibt an, wie viele Replikationsaktualisierungsaktivitäten auf dem Server aufgrund von Änderungen auftreten, die auf anderen Servern generiert wurden.
active_dir.DRA_Inbound_Objects_Applied/sec			Zeigt die Anzahl der Objekte an, die von eingehenden Replikationspartnern empfangen wurden, aber keine Aktualisierungen enthalten und daher nicht angewendet werden müssen.
active_dir.DRA_Inbound_Objects_Filtered/sec			Zeigt die Anzahl der durch eingehende Replikation von benachbarten Computern empfangenen Objekte. Ein benachbarter Computer ist ein Domänen-Controller, von dem ausgehend der lokale Domänen-Controller eine lokale Replikation durchführt.
active_dir.DRA_Inbound_Properties_Applied/sec			Zeigt die Anzahl der Eigenschaften an, die aktualisiert werden, weil die eingehende Eigenschaft die Abgleichslogik, nach der der endgültige zu replizierende Wert bestimmt wird, erfolgreich durchlaufen hat.
active_dir.DRA_Inbound_Properties_Filtered/sec			Zeigt die Anzahl der während der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Replikation empfangenen Eigenschaftsänderungen an, die bereits bekannt sind.
active_dir.DRA_Inbound_Properties_Total/sec			Zeigt die Gesamtanzahl der Objekteigenschaften an, die von eingehenden Replikationspartnern empfangen wurden.
active_dir.DRA_Inbound_Values_DNs/sec			Zeigt die Anzahl der von eingehenden Replikationspartnern empfangenen Objekteigenschaftswerte an, bei denen es sich um Distinguished Names (DNs) handelt, die auf andere Objekte verweisen. DN-Werte, z. B. Gruppen- oder Verteilerlistenmitgliedschaften, sind meist aufwendiger anzuwenden als andere Werte.
active_dir.DRA_Inbound_Values_Total/sec			Zeigt die Gesamtanzahl der Objekteigenschaftenwerte an, die von eingehenden Replikationspartnern empfangen wurden. Jedes eingehende Objekt hat mindestens eine Eigenschaft, und jede Eigenschaft hat null oder mehr Werte. Der Wert null bedeutet, dass eine Eigenschaften entfernt wird.
active_dir.DRA_Outbound_Bytes_after_compressed/sec			Zeigt die komprimierte Größe der ausgehenden komprimierten Replikationsdaten an (Größe nach der Komprimierung von DSAs in andere Standorte).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.DRA_Outbound_Bytes_before_compressed/sec			Zeigt die ursprüngliche Größe der ausgehenden komprimierten Replikationsdaten an (Größe vor der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Outbound_Bytes_not_compressed/sec			Zeigt die Anzahl der ausgehend replizierten Bytes an, die nicht komprimiert wurden (z. B. von DSAs in den gleichen Standort).
active_dir.DRA_Outbound_Bytes_Total/sec (empfohlene Metrik)			Zeigt die Gesamtanzahl der ausgehenden replizierten Bytes an. Dieser Zähler ist die Summe der Anzahl unkomprimierter Bytes (nie komprimiert) und der Anzahl komprimierter Bytes (nach der Komprimierung).
active_dir.DRA_Outbound_Objects/sec			Zeigt die Anzahl der Objekte an, bei denen durch die ausgehende Replikation ermittelt wurde, dass sie keine Aktualisierungen aufweisen, über die der ausgehende Partner nicht verfügt.
active_dir.DRA_Outbound_Objects_Filtered/sec			Zeigt die Anzahl der ausgehend replizierten Objekte an.
active_dir.DRA_Outbound_Properties/sec			Zeigt die Anzahl der ausgehend replizierten Eigenschaften an.
active_dir.DRA_Outbound_Values_DNs/sec			Zeigt die Anzahl der Objekteigenschaftenwerte an, die DNs enthalten und an ausgehende Replikationspartner gesendet werden. DN-Werte, z. B.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Gruppen- oder Verteilerlistenmitgliedschaften, sind zeitaufwendiger zu lesen als andere Werte.
active_dir.DRA_Outbound_Values_Total/sec			Zeigt die Anzahl der Objekteigenschaftenwerte an, die an ausgehende Replikationspartner gesendet wurden.
active_dir.DRA_Pending_Replication_Synchronizations			Zeigt die Anzahl der Verzeichnissynchronisierungen an, die sich für diesen Server in der Warteschlange befinden, aber noch nicht verarbeitet wurden.
active_dir.DRA_Sync_Requests_Made			Zeigt die Anzahl der Synchronisierungsanforderungen an benachbarte Computer an.
active_dir.DS_Threads_in_Use (empfohlene Metrik)			Zeigt die aktuelle Anzahl derzeit vom Verzeichnisdienst verwendeter Threads an (dies unterscheidet sich von der Anzahl von Threads im Verzeichnisdienstprozess). Dies ist die Anzahl der Threads, die aktuell von Client-API-Aufrufen verwendet werden, und gibt Aufschluss darüber, ob zusätzliche Prozessoren verwendet werden sollten.
active_dir.LDAP_Bind_Time (empfohlene Metrik)			Zeigt die Dauer (in Millisekunden) der letzten erfolgreichen LDAP-Bindung.
active_dir.LDAP_Client_Sessions (empfohlene Metrik)			Zeigt die Anzahl der derzeit verbundenen LDAP-Client-Sitzungen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.LDAP_Searches/sec (empfohlene Metrik)			Zeigt die Rate der Suchzugriffe von LDAP-Clients an.
active_dir.LDAP_Successful_Binds/sec (empfohlene Metrik)			Zeigt die Anzahl der LDAP-Bindungen pro Sekunde an.

Apache Kafka – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Apache Kafka-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für beide verfügbar Windows Und Linux.

Apache Kafka-Themenereignisse

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.check-zookeeper-status	Löst ein kritisches Ereignis aus, wenn der gehostete ZooKeeper von Apache Kafka ausgefallen ist.	`commonchecks check-kafka-zk-status` [Kennzeichnungen] Mit folgenden Kennzeichnungen: `-p, --port` = ZooKeeper-Port (Standardwert: „2181“). Verwendungsbeispiel: `commonchecks check-kafka-zk-status -p 2181`	Kafka Zookeeper Status OK: Kafka-Zookeeper is Up! (Kafka-ZooKeeper-Status OK: Kafka-ZooKeeper ist aktiv!)
kafka.check-topic-replicas	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Replikaten aufweist.	`commonchecks check-kafka-replicas` [Kennzeichnungen] Mit folgenden Kennzeichnungen: • `-p, --port` = ZooKeeper-Port (Standardwert: „2181“). • `-d, --detailed` = Listet unbekannte Replikate in jeder Partition eines Themas auf.	<topic> has partitions with unknown replicas (<Thema> hat Partitionen mit unbekannten Replikaten.) Unknown replicas are: {"0":["0"],"1":["0"],"2":["0"]} (Unbekannte Replikate sind: {"0":["0"],"1":["0"],"2":["0"]}). <topic> has partitions with unknown replicas (<Thema>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		• -i, --include_list = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • -e, --exclude_list = Kommagetrennte Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig) Verwendungsbeispiel: commonchecks check-kafka-replicas -H localhost -p 2181 -i "test*" -e "accTopic,*offsets" -d	hat Partitionen mit unbekannten Replikaten.) Unknown replicas are: {"0":["0"]} (Unbekannte Replikate sind: {"0": ["0"]}).
kafka.check-topic-replication-factor	Löst ein kritisches Ereignis aus, wenn der Replikationsfaktor mindestens eines Themas über oder unter dem angegebenen Replikationsfaktorparameter liegt.	commonchecks check-kafka-rf [Kennzeichnungen] Mit folgenden Kennzeichnungen: • -p, --port = ZooKeeper-Port (Standardwert: „2181“). • -d, --detailed = Listet unbekannte Replikate in jeder Partition eines Themas auf. • -i, --include_list = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • -e, --exclude_list = Kommagetrennte Liste zum Ausschließen von Themen („*“ als	TestTopic has replication factor 1, which is less than expected: 2. (TestTopic hat Replikationsfaktor 1, was kleiner ist als erwartet: 2). accMetrics has replication factor 1, which is less than expected: 2. (accMetrics hat Replikationsfaktor 1, was kleiner ist als erwartet: 2).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		Platzhalterzeichen zulässig) • -r, --replication factor = Erwarteter Replikationsfaktor für ein Thema (Standardwert: 1) Beispiele: commonchecks check-kafka-partitions -H localhost -p 2181 -r 2 -i "accMetrics,*Topic" -e "testTopic"	
kafka.check-topic-leader	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten führenden Komponenten (Leadern) oder nicht bevorzugten Replikaten als Leader aufweist.	commonchecks check-kafka-leader [Kennzeichnungen] Mit folgenden Kennzeichnungen: • -p, --port = ZooKeeper-Port (Standardwert: „2181“). • -d, --detailed = Eine Liste von Partitionen in jedem Thema mit unbekannten Leadern oder nicht bevorzugten Replikaten. • -i, --include_list = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • -e, --exclude_list = Kommagetrennte Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig) Beispiele:	<topic> contains, partitions with unpreferred replica as leader. (partitions with unpreferred replicas are [0]). (<Thema> enthält Partitionen mit nicht bevorzugten Replikaten als Leader. (Partitionen mit nicht bevorzugten Replikaten sind [0])). <topic> contains, partitions with unpreferred replica as leader. (partitions with unpreferred replicas are [0]). (<Thema> enthält Partitionen mit nicht bevorzugten Replikaten als Leader. (Partitionen mit nicht bevorzugten Replikaten sind [0])).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		commonchecks check-kafka-leader -H localhost -p 2181 -d -e "*offsets"	
kafka.check-topic-partitions	Löst kritische Ereignisse aus, wenn die Anzahl der Partitionen für ein Thema kleiner ist als der Parameter min_partitions.	commonchecks check-kafka-partitions [Kennzeichnungen] Mit folgenden Kennzeichnungen: • -p, --port = ZooKeeper-Port (Standardwert: „2181“). • -P, --min_partitions = Mindestanzahl der Partitionen für ein Thema (Standardwert: 1). • -i, --include_list = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • -e, --exclude_list = Kommagetrennte Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig)	
		Verwendungsbeispiel 1: commonchecks check-kafka-partitions -H localhost -p 2181 -P 3	<topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
			mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet).
		Verwendungsbeispiel 2: commonchecks check-kafka-partitions -H localhost -p 2181 -P 3 -i "accMetrics,*Topic" -e "testTopic"	<topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet).

Hinweis: Werte für die Parameter include_list und exclude_list müssen in doppelte Anführungszeichen gesetzt werden. Beispiel: "test1,*topic".

Apache Kafka-Broker-Ereignisse

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.check-broker-status	Löst ein kritisches Ereignis aus, wenn der Kafka-Broker auf dem Host ausgefallen ist.	`commonchecks check-kafka-broker-status` [Kennzeichnungen] Mit folgenden Kennzeichnungen: `-p, --port` = Port des Kafka-Brokers (Standardwert: „9092“). Verwendungsbeispiel: `commonchecks check-kafka-broker-status -p 9092`	Kafka Broker Status OK: Kafka Broker ubuntu20:9092 is Up! (Kafka-Broker-Status OK: Kafka-Broker ubuntu20:9092 ist aktiv!)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Broker-Metriken

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.metrics.broker	Sammelt Kafka-Broker-Metriken vom Host.	commonchecks metric-kafka-broker [Kennzeichnungen] Mit folgenden Kennzeichnungen: • -J, --javapath = Pfad der ausführbaren Java-Datei (Standardwert: „java“). • -j, --jmxport = JMX-Port (Standardwert: „9999“) Verwendungsbeispiel: commonchecks metric-kafka-broker -J "/usr/bin/java" -j 9999	hostname.Kafka.Broker.ReplicaManag 0.000 hostname.Kafka.Broker.DelayedOpera 627.000 hostname.Kafka.Broker.ControllerSta 0.000 hostname.Kafka.Broker.RequestMetri 0.000

Apache Kafka-ZooKeeper-Metriken

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.metrics.zookeeper	Sammelt ZooKeeper-Metriken vom Host.	commonchecks metric-kafka-zookeeper [Kennzeichnungen] Mit folgender Kennzeichnung: -p, --adminserverport = Port des Verwaltungsservers (Standardwert: „8085“) Verwendungsbeispiel: commonchecks metric-kafka-zookeeper -p 8085	hostname.Kafka.Zookeeper.outstandi 2.000 1648183249 hostname.Kafka.Zookeeper.avg_laten 1.05 1648183249 hostname.Kafka.Zookeeper.num_alive 1.000 1648183249 hostname.Kafka.Zookeeper.open_file_ 124.000 1648183249

Apache Kafka-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Kafka-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Broker-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Broker.RequestMetrics.TotalTimeMs.FetchConsumer.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Consumer-Anforderung.
Kafka.Broker.RequestMetrics.TotalTimeMs.FetchFollower.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Follower-Anforderung.
Kafka.Broker.RequestMetrics.TotalTimeMs.Produce.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Producer-Anforderung.
Kafka.Broker.BrokerTopicMetrics.BytesOutPerSec.OneMinuteRate (empfohlene Metrik)			Zusammengefasste ausgehende Byterate.
Kafka.Broker.BrokerTopicMetrics.BytesInPerSec.OneMinuteRate (empfohlene Metrik)			Zusammengefasste eingehende Byterate.
Kafka.Broker.ReplicaManager.UnderReplicatedPartitions.Value			Anzahl der nicht replizierten Partitionen.
Kafka.Broker.ReplicaManager.IsrExpandsPerSec.OneMinuteRate			Rate, mit der der Pool der synchronen Replikate (In-Sync Replicas, ISRs) kleiner wird.
Kafka.Broker.ReplicaManager.IsrShrinksPerSec.OneMinuteRate			Rate, mit der der Pool der synchronen Replikate (In-Sync Replicas, ISRs) kleiner wird.
Kafka.Broker.KafkaController.ActiveControllerCount.Value (empfohlene Metrik)			Anzahl der aktiven Controller im Cluster.
Kafka.Broker.KafkaController.OfflinePartitionsCount.Value			Anzahl der Offline-Partitionen.
Kafka.Broker.ControllerStats.LeaderElectionRateAndTimeMs.OneMinuteRate (empfohlene Metrik)			Leader-Wahlrate und -Latenz.
Kafka.Broker.ControllerStats.UncleanLeaderElectionsPerSec.OneMinuteRate			Anzahl der nicht bereinigten Auswahlen pro Sekunde.
Kafka.Broker.DelayedOperationPurgatory.PurgatorySize.Fetch.Value			Anzahl der Abrufanforderungen, die in der als „Purgatory“ (Fegefeuer) bezeichneten Datenstruktur von Kafka warten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Broker-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Broker.DelayedOperationPurgatory.PurgatorySize.Produce.Value			Anzahl der Anforderungen, die in der als Producer-„Purgatory“ (Fegefeuer) bezeichneten Datenstruktur von Kafka warten.
Kafka.Broker.RequestMetrics.RequestsPerSec.Produce.OneMinuteRate (empfohlene Metrik)			Anzahl der Producer-Anforderungen pro Sekunde.
Kafka.Broker.RequestMetrics.RequestsPerSec.FetchConsumer.OneMinuteRate (empfohlene Metrik)			Anzahl der Consumer-Anforderungen pro Sekunde.
Kafka.Broker.RequestMetrics.RequestsPerSec.FetchFollower.OneMinuteRate (empfohlene Metrik)			Anzahl der Follower-Anforderungen pro Sekunde.

ZooKeeper-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Zookeeper.outstanding_requests (empfohlene Metrik)			Anzahl der Anforderungen in der Warteschlange.
Kafka.Zookeeper.avg_latency (empfohlene Metrik)			Durchschnittliche Zeit (in ms), die für die Beantwortung einer Client-Anforderung benötigt wird.
Kafka.Zookeeper.num_alive_connections (empfohlene Metrik)			Anzahl der mit ZooKeeper verbundenen Clients.
Kafka.Zookeeper.open_file_descriptor_count			Anzahl der verwendeten Dateideskriptoren.
Kafka.Zookeeper.pending_syncs			Anzahl der ausstehenden Synchronisierungen von Followern.
Kafka.Zookeeper.followers			Anzahl der aktiven Follower.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Systemüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für AWS-Monitoring.

AWS-Metrikenrichtlinie

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
Metrik	aws.metrics-ec2	Gibt Metriken aller EC2-Instanzen in einem AWS-Rechenzentrum zurück	metrics-ec2.rb (Optionen) -F, --filter FILTER Zeichenfolgendars des Filters zum Filtern von EC2-Instanzen nach Tags. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Instanzen, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	./metrics-ec2.rb -F "{name:tag:environment,values:[ENV1,ENV2]} {name:tag:Name,values:[Instance1,Instance2]}" Geben Sie die Filterzeichenfolge mit doppelten Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-ebs	Gibt Metriken aller EBS-Volumes in einem AWS-Rechenzentrum zurück	metrics-ebs.rb (Optionen) -F, --filter FILTER Zeichenfolgendars des Filters zum Filtern von EBS-Volumes nach Tags. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Volumes, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	./metrics-ebs.rb -F "{name:tag:environment,values:[ENV1,ENV2]} {name:tag:Name,values:[Volume1,Volume2]}" Geben Sie die Filterzeichenfolge mit doppelten Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
Metrik	aws.metrics-s3	Gibt Metriken aller S3-Buckets in einem AWS-Rechenzentrum zurück	metrics-s3.rb (Optionen) -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der S3-Buckets, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-s3.rb -b 5` Legen Sie den Parameter *`batch_size`* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-rds	Gibt Metriken aller RDS-Buckets in einem AWS-Rechenzentrum zurück	metrics-rds.rb (Optionen) -F, --filter FILTER Zeichenfolgendarstellung des Filters zum Filtern von RDS-Instanzen nach Tags. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-rds.rb -F "{name:tag:environment,values:[ENV1,ENV2]}{name:tag:engine,values:[MariaDB]}"` Geben Sie die Filterzeichenfolge mit doppelten Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter *`batch_size`* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-classic-elb	Gibt Metriken aller klassischen elastischen Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch Kommas getrennten	`./metrics-elb.rb -t classic -e "classic,itom,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("") für den Parameter *`exclude_lb`* an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-network-elb	Gibt Metriken aller elastischen Netzwerk-Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch Kommas getrennten Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-elb.rb -t network -e "vpc,itom,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("") für den Parameter *exclude_lb* an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest. Ändern Sie das Befehlspräfix nicht.
Metrik	aws.metrics-application-elb	Gibt Metriken aller elastischen Anwendungs-Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch	`./metrics-elb.rb -t application -e "classic,app,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("")

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			Kommas getrennten Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	für den Parameter *exclude_lb* an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest. Ändern Sie das Befehlspräfix nicht.
Metrik	aws.metrics-ec2-count	Gibt die Anzahl der EC2-Instanzen nach instance_type oder Status in einem AWS-Rechenzentrum zurück	metrics-ec2-count.rb (Optionen) -s, --scheme SCHEME Metrikbenennungsschema, Text, der der Metrik vorangestellt werden soll. Standard: aws.ec2 -t, --typ METRIC-Typ Anzahl nach Typ: Status, Instanz. Standard: Instanz	./metrics-ec2-count.rb -t status ./metrics-ec2-count.rb -t status -s metric.aws.ec2

AWS DynamoDB-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl
Metrik	aws.metrics-dynamodb	Überwacht die Integrität von DynamoDB-Tabellen in einem AWS-Rechenzentrum. Wird mit der DynamoDB-	e, --exclude_tb EXCLUDE_TB Schließen Sie Metriken aus Tabellen aus, deren Name eine der durch Kommas getrennten	metrics-dynamodb.rb -r {{.labels.params_ci_region}} {{.labels.params_exclude_tb}} -f {{.labels.params_exclude_tb}} {{end}} {{.labels.params_batch_size}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS DynamoDB-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl
		Tabelle (cmdb_ci_dynamodb_table) verbunden	Zeichenfolgen Inhalt b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Tabellen, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	-b {{.labels.params_filter}} {{end}}

AWS EC2-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl
Metrik	aws.metrics-ecs-cluster	Überwacht ECS-Cluster in einem AWS-Rechenzentrum. Wird mit dem AWS ECS Cluster-CI-Typ (cmdb_ci_cloud_ecs_cluster) verbunden	-F, --filter FILTER Zeichenfolgendarstellu des Filters zum Filtern von ECS-Clustern nach Tags. b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Cluster, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	metrics-ecs-cluster.rb -r {{.labels.params_ci_region}} {{.labels.params_filter}} -f {{.labels.params_filter}} {{end}} {{.labels.params_batch_size}} -b {{.labels.params_filter}} {{end}}
Metrik	aws.metrics-ecs-service	Überwacht ECS-Services in einem AWS-Rechenzentrum. Wird mit dem AWS ECS Service-CI-Typ (cmdb_ci_cloud_ecs_service) verbunden	-F, --filter FILTER Zeichenfolgendarstellu des Filters zum Filtern von ECS-Clustern nach Tags. b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Cluster, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	metrics-ecs-service.rb -r {{.labels.params_ci_region}} {{.labels.params_filter}} -f {{.labels.params_filter}} {{end}} {{.labels.params_batch_size}} -b {{.labels.params_filter}} {{end}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

AWS-Metriken

AWS-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von den angegebenen AWS-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

aws.metrics-ec2-Metriken

Metrikname	Beschreibung
aws.ec2.CPUCreditBalance.Average	Anzahl der verdienten CPU-Guthaben, die eine Instanz seit dem Start gesammelt hat
aws.ec2.CPUUtilization.Average	Durchschnittlicher Prozentsatz der zugewiesenen EC2-Recheneinheiten, die derzeit in der Instanz verwendet werden
aws.ec2.DiskReadOps.Average (Empfohlene Metrik)	Durchschnitt der abgeschlossenen Lesevorgänge aus allen Instanzspeicher-Volumes, die für die Instanz in einem angegebenen Zeitraum verfügbar sind
aws.ec2.DiskWriteOps.Average (Empfohlene Metrik)	Abgeschlossene Schreibvorgänge in allen Instanzspeicher-Volumes, die für die Instanz in einem angegebenen Zeitraum verfügbar sind
aws.ec2.DiskReadBytes.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der gelesenen Bytes aus allen für die Instanz verfügbaren Instanzspeicher-Volumes
aws.ec2.DiskWriteBytes.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der geschriebenen Bytes in allen für die Instanz verfügbaren Instanzspeicher-Volumes
aws.ec2.NetworkIn.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz empfangenen Byte. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkdatenverkehrs für eine einzelne Instanz.
aws.ec2.NetworkOut.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz gesendeten Byte. Diese Metrik identifiziert das Volumen des ausgehenden Netzwerkdatenverkehrs einer einzelnen Instanz.
aws.ec2.NetworkPacketsIn.Average	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz empfangenen Pakete. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkdatenverkehrs als Anzahl der Pakete für eine einzelne Instanz.
aws.ec2.NetworkPacketsOut.Average	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz gesendeten Pakete. Diese Metrik identifiziert das Volumen des

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ec2-Metriken (Fortsetzung)

Metrikname	Beschreibung
	ausgehenden Netzwerkdatenverkehrs als Anzahl der Pakete für eine einzelne Instanz.
aws.ec2.MetadataNoToken.Average	Durchschnittliche Anzahl der erfolgreichen Zugriffe auf den Instanzmetadatenservice mit einer Methode, die kein Token verwendet
aws.ec2.CPUCreditUsage.Average	Durchschnittliche Anzahl der von der Instanz für die CPU-Auslastung ausgegebenen CPU-Guthaben
aws.ec2.CPUSurplusCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für `CPUCreditBalance` null ist
aws.ec2.CPUSurplusCreditsCharged.Average	Durchschnittliche Anzahl der ausgegebenen überschüssigen Guthaben, die nicht durch verdiente CPU-Guthaben abgegolten werden und daher eine zusätzliche Gebühr verursachen
aws.ec2.StatusCheckFailed_Instance.Average	Meldet, ob die Instanz die Instanzstatusprüfung in der letzten Minute bestanden hat
aws.ec2.StatusCheckFailed_System.Average	Meldet, ob die Instanz die Systemstatusprüfung in der letzten Minute bestanden hat
aws.ec2.StatusCheckFailed.Average	Meldet, ob die Instanz die Instanzstatusprüfung und die Systemstatusprüfung in der letzten Minute bestanden hat

aws.metrics-ebs-Metriken

Metrikname	Beschreibung
aws.ebs.VolumeReadBytes.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der während der Lesevorgänge im Zeitraum übertragenen Bytes
aws.ebs.VolumeWriteBytes.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der während der Schreibvorgänge im Zeitraum übertragenen Bytes
aws.ebs.VolumeReadOps.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Lesevorgänge in einem angegebenen Zeitraum
aws.ebs.VolumeWriteOps.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Schreibvorgänge in einem angegebenen Zeitraum
aws.ebs.VolumeTotalReadTime.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Sekunden, die alle Lesevorgänge in einem angegebenen Zeitraum benötigt haben
aws.ebs.VolumeTotalWriteTime.Average	Durchschnittliche Gesamtzahl der Sekunden, die alle Schreibvorgänge in einem angegebenen Zeitraum benötigt haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ebs-Metriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	
aws.ebs.VolumeIdleTime.Average	Durchschnittliche Gesamtzahl der Sekunden in einem angegebenen Zeitraum, in denen keine Lese- oder Schreibvorgänge übermittelt wurden
aws.ebs.VolumeQueueLength.Average	Durchschnittliche Anzahl von Lese- und Schreibvorgangsanforderungen, die in einem angegebenen Zeitraum auf den Abschluss warten
aws.ebs.VolumeThroughputPercentage.Average	Durchschnittlicher Prozentsatz der gelieferten E/A-Vorgänge pro Sekunde (IOPS) der gesamten für ein Amazon EBS-Volume bereitgestellten IOPS
aws.ebs.VolumeConsumedReadWriteOps.Average	Durchschnittliche Gesamtmenge der in einem angegebenen Zeitraum verbrauchten Lese- und Schreibvorgänge (normalisiert auf 256.000 Kapazitätseinheiten)
aws.ebs.BurstBalance.Average	Durchschnittlicher Prozentsatz der im Burst-Bucket verbleibenden E/A-Guthaben (für gp2) oder Durchsatz-Guthaben (für st1 und sc1)

aws.metrics-s3-Metriken

Metrikname	Beschreibung
aws.s3.NumberOfObjects.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der in einem Bucket gespeicherten Objekte für alle Speicherklassen. Alle 12 Stunden erfasst
aws.s3.BucketSizeBytes.Average (Empfohlene Metrik)	Durchschnittliche Datenmenge in Byte, die in einem Bucket in der Speicherklasse STANDARD gespeichert ist. Alle 12 Stunden erfasst

aws.metrics-rds-Metriken

Metrikname	Beschreibung
aws.rds.BinLogDiskUsage.Average	Durchschnittliche Menge des von Protokollen von Binärdateien belegten Speicherplatzes auf dem primären Speicher. Gilt für MySQL-Lesereplikate
aws.rds.BurstBalance.Average	Durchschnittlicher Prozentsatz der verfügbaren Burst-Bucket-E/A-Guthaben für Allzweck-SSDs (gp2)
aws.rds.CPUUtilization.Average (Empfohlene Metrik)	Durchschnittliche CPU-Auslastung in Prozent

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-rds-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.rds.CPUCreditUsage.Average	Durchschnittliche Anzahl der von der Instanz für die CPU-Auslastung ausgegebenen CPU-Guthaben
aws.rds.CPUCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für `CPUCreditBalance` null ist
aws.rds.DatabaseConnections.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der verwendeten Datenbankverbindungen
aws.rds.DiskQueueDepth.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der ausstehenden E/A-Anforderungen (Lese-/Schreibanforderungen), die auf den Zugriff auf das Laufwerk warten
aws.rds.EBSByteBalance%.Average	Durchschnittlicher Prozentsatz der verbleibenden Durchsatzguthaben im Burst-Bucket Ihrer RDS-Datenbank
aws.rds.EBSIOBalance%.Average	Durchschnittlicher Prozentsatz der verbleibenden E/A-Guthaben im Burst-Bucket Ihrer RDS-Datenbank
aws.rds.FailedSQLServerAgentJobsCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der fehlgeschlagenen Microsoft SQL Server Agent-Aufträge in der letzten Minute
aws.rds.FreeableMemory.Average (Empfohlene Metrik)	Durchschnittliche Menge des verfügbaren Arbeitsspeichers
aws.rds.FreeStorageSpace.Average	Durchschnittliche Menge des verfügbaren Speicherplatzes
aws.rds.MaximumUsedTransactionIDs.Average	Durchschnittliche Anzahl der verwendeten maximalen Transaktions-IDs. Gilt für PostgreSQL
aws.rds.NetworkReceiveThroughput.Average (Empfohlene Metrik)	Durchschnittlicher eingehender (empfangener) Netzwerkdatenverkehr in der DB-Instanz, einschließlich des Datenverkehrs der Kundendatenbank und des Amazon RDS-Datenverkehrs, der für Überwachung und Replikation verwendet wird
aws.rds.NetworkTransmitThroughput.Average (Empfohlene Metrik)	Durchschnittlicher ausgehender (gesendeter) Netzwerkdatenverkehr in der DB-Instanz, einschließlich des Datenverkehrs der Kundendatenbank und des Amazon RDS-Datenverkehrs, der für Überwachung und Replikation verwendet wird
aws.rds.OldestReplicationSlotLag.Average	Durchschnittliche Verzögerungsgröße des Replikats mit der größten Verzögerung hinsichtlich der empfangenen Write-Ahead-Protokolldaten (WAL-Daten) Gilt für PostgreSQL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-rds-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.rds.ReadIOPS.Average	Durchschnittliche Anzahl der Laufwerks-E/A-Lesevorgänge pro Sekunde
aws.rds.ReadLatency.Average (Empfohlene Metrik)	Durchschnittliche Zeit, die pro Laufwerks-E/A-Vorgang benötigt wird
aws.rds.ReadThroughput.Average	Durchschnittliche Anzahl der pro Sekunde vom Laufwerk gelesenen Byte
aws.rds.ReplicaLag.Average	Durchschnittliche Zeit, die eine Lese-Replikat-DB-Instanz hinter der Quell-DB-Instanz zurückliegt. Gilt für Lesereplikate von MySQL, MariaDB, Oracle, PostgreSQL und SQL Server
aws.rds.ReplicationSlotDiskUsage.Average	Durchschnittliche Menge des von Replikations-Slot-Dateien verwendeten Speicherplatzes Gilt für PostgreSQL
aws.rds.SwapUsage.Average	Durchschnittliche Menge des in der DB-Instanz verwendeten Swap-Bereichs. Diese Metrik ist für SQL Server nicht verfügbar.
aws.rds.TransactionLogsDiskUsage.Average	Durchschnittlicher von Transaktionsprotokollen verwendeter Speicherplatz Gilt für PostgreSQL
aws.rds.TransactionLogsGeneration.Average	Durchschnittliche Größe der pro Sekunde generierten Transaktionsprotokolle. Gilt für PostgreSQL
aws.rds.WriteIOPS.Average	Durchschnittliche Anzahl der Laufwerks-E/A-Schreibvorgänge pro Sekunde
aws.rds.WriteLatency.Average (Empfohlene Metrik)	Durchschnittliche Zeit, die pro Laufwerks-E/A-Vorgang benötigt wird
aws.rds.WriteThroughput.Average	Durchschnittliche Anzahl der pro Sekunde auf das Laufwerk geschriebenen Byte
aws.rds.CPUSurplusCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für `CPUCreditBalance` null ist
aws.rds.CPUSurplusCreditsCharged.Average	Durchschnittliche Anzahl der ausgegebenen überschüssigen Guthaben, die nicht durch verdiente CPU-Guthaben abgegolten werden und daher eine zusätzliche Gebühr verursachen

aws.metrics-classic-elb-Metriken

Metrikname	Beschreibung
aws.classicElb.EstimatedALBActiveConnectionCount.Average (Empfohlene Metrik)	Durchschnittliche geschätzte Anzahl gleichzeitiger aktiver TCP-Verbindungen von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-classic-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.classicElb.EstimatedALBConsumedLCUs.Average	Durchschnittliche geschätzte Anzahl der von einem Lastenausgleichsmodul für Anwendungen verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (Load Balancer Capacity Units, LCU). Sie zahlen für die Anzahl der pro Stunde verwendeten LCUs.
aws.classicElb.EstimatedALBNewConnectionCount.Average (Empfohlene Metrik)	Durchschnittliche geschätzte Anzahl neuer TCP-Verbindungen die von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen hergestellt werden
aws.classicElb.EstimatedProcessedBytes.Average	Geschätzte Anzahl von Bytes, die von einem Lastenausgleichsmodul für Anwendungen verarbeitet werden
aws.classicElb.DesyncMitigationMode_NonCompliant_Request_Count.Sum	Anzahl der Anforderungen, die nicht RFC 7230 entsprechen
aws.classicElb.HTTPCode_ELB_5XX.Sum (Empfohlene Metrik)	Anzahl der vom Lastenausgleichsmodul generierten HTTP 4XX-Client-Fehlercodes
aws.classicElb.HTTPCode_ELB_4XX.Sum (Empfohlene Metrik)	Anzahl der vom Lastenausgleichsmodul generierten HTTP 5XX-Server-Fehlercodes
aws.classicElb.SurgeQueueLength.Maximum	Maximale Gesamtanzahl der Anforderungen (HTTP-Listener) oder Verbindungen (TCP-Listener), für die die Weiterleitung an eine fehlerfreie Instanz aussteht. Die maximale Größe der Warteschlange beträgt 1.024. Zusätzliche Anforderungen oder Verbindungen werden abgelehnt, wenn die Warteschlange voll ist.
aws.classicElb.SpilloverCount.Sum (Empfohlene Metrik)	Gesamtzahl der Anforderungen, die abgelehnt wurden, da die Warteschlange für Anforderungswellen (Surge Queue) voll ist
aws.classicElb.RequestCount.Sum	Gesamtzahl der während des angegebenen Intervalls abgeschlossenen Anforderungen oder hergestellten Verbindungen
aws.classicElb.Latency.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzeit in Sekunden seit dem Zeitpunkt, zu dem das Lastenausgleichsmodul die Anforderung an eine registrierte Instanz gesendet hat, bis die Instanz mit dem Senden der Antwortheader begonnen hat
aws.classicElb.BackendConnectionErrors.Sum (Empfohlene Metrik)	Gesamtzahl der Verbindungen, die zwischen dem Lastenausgleichsmodul und den registrierten Instanzen nicht erfolgreich hergestellt wurden
aws.classicElb.HealthyHostCount.Average	Durchschnittliche Anzahl der beim Lastenausgleichsmodul registrierten fehlerfreien Instanzen. Eine neu registrierte Instanz gilt als

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-classic-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	fehlerfrei, nachdem sie die erste Integritätsprüfung bestanden hat.
aws.classicElb.UnHealthyHostCount.Average	Durchschnittliche Anzahl der beim Lastenausgleichsmodul registrierten fehlerhaften Instanzen. Eine Instanz gilt als fehlerhaft, nachdem sie den für Integritätsprüfungen konfigurierten Schwellenwert für den Status „fehlerhaft“ überschritten hat.

aws.metrics-network-elb

Metrikname	Beschreibung
aws.networkElb.ActiveFlowCount.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik schließt Verbindungen in den Status SYN_SENT und ESTABLISHED ein.
aws.networkElb.ActiveFlowCount_TCP.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen TCP-Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält nur Verbindungen im Status ESTABLISHED.
aws.networkElb.ActiveFlowCount_TLS.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen TLS-Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält nur Verbindungen im Status ESTABLISHED.
aws.networkElb.ActiveFlowCount_UDP.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen UDP-Flows (oder Verbindungen) von Clients zu Zielen
aws.networkElb.ClientTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der TLS-Handshakes, die während der Aushandlung zwischen einem Client und einem TLS-Listener fehlgeschlagen sind
aws.networkElb.ConsumedLCUs.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_TCP.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für TCP verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_TLS.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für TLS verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_UDP.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für UDP verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.HealthyHostCount.Maximum (Empfohlene Metrik)	Die maximale Anzahl von Zielen, die als fehlerfrei gelten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-network-elb (Fortsetzung)

Metrikname	Beschreibung
aws.networkElb.NewFlowCount.Sum (Empfohlene Metrik)	Gesamtzahl der neuen Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_TCP.Sum (Empfohlene Metrik)	Gesamtzahl der neuen TCP-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_TLS.Sum (Empfohlene Metrik)	Gesamtzahl der neuen TLS-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_UDP.Sum (Empfohlene Metrik)	Gesamtzahl der neuen UDP-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.PeakBytesPerSecond.Maximum (Empfohlene Metrik)	Maximaler durchschnittlicher Durchsatz (Byte pro Sekunde), berechnet während des Stichprobenfensters alle 10 Sekunden. Diese Metrik enthält Datenverkehr zur Integritätsprüfung.
aws.networkElb.PeakPacketsPerSecond.Maximum (Empfohlene Metrik)	Maximale durchschnittliche Paketrate (verarbeitete Pakete pro Sekunde), berechnet während des Stichprobenfensters alle 10 Sekunden. Diese Metrik enthält Datenverkehr zur Integritätsprüfung.
aws.networkElb.ProcessedBytes.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Byte, einschließlich TCP/IP-Header. Diese Anzahl umfasst den Datenverkehr von und zu Zielen, abzüglich des Datenverkehrs der Integritätsprüfung.
aws.networkElb.ProcessedBytes_TCP.Sum	Gesamtanzahl der von TCP-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedBytes_TLS.Sum	Gesamtanzahl der von TLS-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedBytes_UDP.Sum	Gesamtanzahl der von UDP-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedPackets.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Pakete. Diese Anzahl umfasst den Datenverkehr von und zu Zielen, einschließlich des Datenverkehrs der Integritätsprüfung.
aws.networkElb.TargetTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Gesamtzahl der TLS-Handshakes, die während der Aushandlung zwischen einem TLS-Listener und einem Ziel fehlgeschlagen sind
aws.networkElb.TCP_Client_Reset_Count.Sum	Gesamtzahl der Reset(RST)-Pakete, die von einem Client an ein Ziel gesendet wurden. Diese Zurücksetzungen werden vom Client generiert und vom Lastenausgleichsmodul weitergeleitet.
aws.networkElb.TCP_ELB_Reset_Count.Sum	Gesamtzahl der vom Lastenausgleichsmodul generierten Reset(RST)-Pakete

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-network-elb (Fortsetzung)

Metrikname	Beschreibung
aws.networkElb.TCP_Target_Reset_Count.Sum	Gesamtzahl der Reset(RST)-Pakete, die von einem Ziel an einen Client gesendet wurden. Diese Zurücksetzungen werden vom Ziel generiert und vom Lastenausgleichsmodul weitergeleitet.
aws.networkElb.UnHealthyHostCount.Maximum (Empfohlene Metrik)	Die maximale Anzahl von Zielen, die als fehlerhaft gelten

aws.metrics-application-elb-Metriken

Metrikname	Beschreibung
aws.applicationElb.ActiveConnectionCount.Sum (Empfohlene Metrik)	Gesamtzahl gleichzeitiger aktiver TCP-Verbindungen von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen
aws.applicationElb.ClientTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Gesamtzahl der vom Client initiierten TLS-Verbindungen, von denen aufgrund eines TLS-Fehlers keine Sitzung mit dem Lastenausgleichsmodul hergestellt wurden
aws.applicationElb.ConsumedLCUs.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU). Sie zahlen für die Anzahl der pro Stunde verwendeten LCUs. Weitere Informationen finden Sie unter „Preise für Elastic Load Balancing“.
aws.applicationElb.DesyncMitigationMode_NonCompliant_Request_Count.Sum (Empfohlene Metrik)	Gesamtzahl der Anforderungen, die nicht RFC 7230 entsprechen
aws.applicationElb.DroppedInvalidHeaderRequestCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl von Anforderungen, bei denen vom Lastenausgleichsmodul vor der Weiterleitung der Anforderung HTTP-Header mit ungültigen Headerfeldern entfernt wurden. Vom Lastenausgleichsmodul werden diese Header nur entfernt, wenn das Attribut routing.http.drop_invalid_header_fields.enabled auf „true“ festgelegt ist.
aws.applicationElb.ForwardedInvalidHeaderRequestCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl von Anforderungen, die vom Lastenausgleichsmodul weitergeleitet wurden und HTTP-Header mit ungültigen Headerfeldern aufwiesen. Vom Lastenausgleichsmodul werden Anforderungen mit solchen Headern nur weitergeleitet, wenn das Attribut routing.http.drop_invalid_header_fields.enabled auf „false“ festgelegt ist.
aws.applicationElb.GrpcRequestCount.Sum	Gesamtzahl der über IPv4 und IPv6 verarbeiteten gRPC-Anforderungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-application-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.applicationElb.HTTP_Fixed_Response_Count.Sum	Gesamtzahl der erfolgreichen Fixed-Response-Aktionen
aws.applicationElb.HTTP_Redirect_Count.Sum	Gesamtzahl der erfolgreichen Weiterleitungsaktionen
aws.applicationElb.HTTP_Redirect_Url_Limit_Exceeded_Count.Sum (Empfohlene Metrik)	Gesamtzahl der Weiterleitungsaktionen, die nicht abgeschlossen werden konnten, da die URL im Adressheader der Antwort größer als 8 kB ist
aws.applicationElb.HTTPCode_ELB_3XX_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 3XX-Weiterleitungscodes, die vom Lastenausgleichsmodul stammen. Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_4XX_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 4XX-Clientfehlercodes, die vom Lastenausgleichsmodul stammen. Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_5XX_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 5XX-Serverfehlercodes, die vom Lastenausgleichsmodul stammen. Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_500_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 500-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_502_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 502-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_503_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 503-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_504_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 504-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.IPv6ProcessedBytes.Sum	Gesamtzahl der vom Lastenausgleichsmodul über IPv6 verarbeiteten Byte
aws.applicationElb.IPv6RequestCount.Sum	Gesamtzahl der vom Lastenausgleichsmodul empfangenen IPv6-Anforderungen
aws.applicationElb.NewConnectionCount.Sum	Gesamtzahl neuer TCP-Verbindungen, die von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen hergestellt werden
aws.applicationElb.NonStickyRequestCount.Sum	Gesamtanzahl der Anforderungen, bei denen vom Lastenausgleichsmodul ein neues Ziel ausgewählt wurde, da eine vorhandene dauerhafte Sitzung nicht verwendet werden konnte
aws.applicationElb.ProcessedBytes.Sum (Empfohlene Metrik)	Gesamtzahl der vom Lastenausgleichsmodul über IPv4 und IPv6 verarbeiteten Byte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-application-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.applicationElb.RejectedConnectionCount.Sum (Empfohlene Metrik)	Gesamtzahl der Verbindungen, die abgelehnt wurden, da das Lastenausgleichsmodul seine maximale Anzahl von Verbindungen erreicht hatte
aws.applicationElb.RequestCount.Sum	Gesamtzahl der über IPv4 und IPv6 verarbeiteten Anforderungen
aws.applicationElb.RuleEvaluations.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Regeln bei einer pro Stunde gemittelten Anforderungsrate

aws.metrics-ec2-count-Metriken

Metrikname	Beschreibung
aws.ec2.types.<type_name>	Anzahl der EC2-Instanzen für den angegebenen Typ im AWS-Rechenzentrum
aws.ec2.status.running	Anzahl der EC2-Instanzen im Status „Aktiv“ in einem AWS-Rechenzentrum
aws.ec2.status.stopped	Anzahl der EC2-Instanzen im Status „Angehalten“ in einem AWS-Rechenzentrum
aws.ec2.status.total	Anzahl aller EC2-Instanzen in einem AWS-Rechenzentrum

aws.metrics-dynamodb-Metriken

Metrikname	Beschreibung
aws.dynamodb.ConsumedWriteCapacityUnits.Average (Empfohlene Metrik)	Anzahl der über den angegebenen Zeitraum verbrauchten Schreibkapazitätseinheiten, auf deren Basis nachverfolgt wird, wie viel bereitgestellter Durchsatz verwendet wird
aws.dynamodb.ConsumedReadCapacityUnits.Average (Empfohlene Metrik)	Anzahl der über den angegebenen Zeitraum verbrauchten Lesekapazitätseinheiten, auf deren Basis nachverfolgt wird, wie viel bereitgestellter Durchsatz verwendet wird
aws.dynamodb.ProvisionedWriteCapacityUnits.Average (Empfohlene Metrik)	Anzahl der bereitgestellten Schreibkapazitätseinheiten für eine Tabelle
aws.dynamodb.ProvisionedReadCapacityUnits.Average (Empfohlene Metrik)	Anzahl der bereitgestellten Lesekapazitätseinheiten für eine Tabelle
aws.dynamodb.SuccessfulRequestLatency.GetItem.Average (Empfohlene Metrik)	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem GetItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.BatchGetItem.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	des angegebenen Zeitraums. Wird von einem BatchGetItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.PutItem.Average (Empfohlene Metrik)	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem PutItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.BatchPutItem.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem BatchPutItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.Query.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem Query-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.Scan.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem Scan-Vorgang ausgeführt
aws.dynamodb.ReturnedItemCount.Scan.Average	Anzahl der von Scan-Vorgängen während des angegebenen Zeitraums zurückgegebenen Elemente
aws.dynamodb.ReturnedItemCount.Query.Average	Anzahl der von Query-Vorgängen während des angegebenen Zeitraums zurückgegebenen Elemente
aws.dynamodb.UserErrors.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 400-Statuscode generiert wurde. Ein HTTP 400-Code zeigt normalerweise einen clientseitigen Fehler an, z. B. eine ungültige Kombination von Parametern, einen Versuch, eine nicht vorhandene Tabelle zu aktualisieren, oder eine falsche Anforderungssignatur.
aws.dynamodb.SystemErrors.GetItem.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem GetItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.Scan.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem Scan-Vorgang ausgeführt
aws.dynamodb.SystemErrors.Query.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	normalerweise einen internen Servicefehler an. Wird von einem Query-Vorgang ausgeführt
aws.dynamodb.SystemErrors.BatchGetItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem BatchGet-Vorgang ausgeführt
aws.dynamodb.SystemErrors.PutItem.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem PutItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.UpdateItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem UpdateItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.DeleteItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem DeleteItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.BatchWriteItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem BatchWrite-Vorgang ausgeführt
aws.dynamodb.ConditionalCheckFailedRequests.Average (Empfohlene Metrik)	Anzahl der fehlgeschlagenen Versuche, bedingte Schreibvorgänge auszuführen
aws.dynamodb.TimeToLiveDeletedItemCount.Average	Anzahl der über die Gültigkeitsdauer (Time to Live, TTL) gelöschten Elemente während des angegebenen Zeitraums. Diese Metrik hilft Ihnen, die Rate der TTL-Löschungen in Ihrer Tabelle zu überwachen.
aws.dynamodb.TransactionConflict.Average	Aufgrund von Transaktionskonflikten zwischen gleichzeitigen Anforderungen für dieselben Elemente abgelehnte Anforderungen auf Elementebene
aws.dynamodb.ReadThrottleEvents.Average (Empfohlene Metrik)	Anforderungen an DynamoDB, die die bereitgestellten Lesekapazitätseinheiten für eine Tabelle überschreiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.dynamodb.WriteThrottleEvents.Average (Empfohlene Metrik)	Anforderungen an DynamoDB, die die bereitgestellten Schreibkapazitätseinheiten für eine Tabelle überschreiten
aws.dynamodb.ThrottledRequests.GetItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen GetItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.PutItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen PutItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.DeleteItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen DeleteItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.UpdateItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen UpdateItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.BatchGetItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen BatchGetItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.Scan.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen Scan-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.Query.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen Query-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.BatchWriteItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen BatchWriteItem-Vorgang überschreiten
aws.dynamodb.SuccessfulRequestLatency.GetRecords.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem GetRecords-Vorgang ausgeführt
aws.dynamodb.ReturnedBytes.GetRecords.Average	Die Anzahl der von GetRecords-Vorgängen (Amazon DynamoDB-Streams) während des angegebenen Zeitraums zurückgegebenen Byte
aws.dynamodb.ReturnedRecordsCount.GetRecords.Average	Die Anzahl der von GetRecords-Vorgängen (Amazon DynamoDB-Streams) während des angegebenen Zeitraums zurückgegebenen Stream-Datensätze

aws.metrics-ecs-cluster-Metriken

Metrik	Beschreibung
aws.ecs.cluster.CPUReservation.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die durch ausgeführte Aufgaben im Cluster reserviert wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ecs-cluster-Metriken (Fortsetzung)

Metrik	Beschreibung
aws.ecs.cluster.CPUUtilization.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die im Cluster verwendet werden
aws.ecs.cluster.MemoryReservation.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der durch ausgeführte Aufgaben im Cluster reserviert wurde
aws.ecs.cluster.MemoryUtilization.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der im Cluster verwendet wird
aws.ecs.cluster.CpuReserved.Average	CPU-Einheiten, die durch Aufgaben im Cluster reserviert wurden
aws.ecs.cluster.CpuUtilized.Average	CPU-Einheiten, die durch Aufgaben im Cluster verwendet wurden
aws.ecs.cluster.NetworkRxBytes.Average (Empfohlene Metrik)	Anzahl der vom Cluster empfangenen Byte
aws.ecs.cluster.NetworkTxBytes.Average (Empfohlene Metrik)	Anzahl der vom Cluster übertragenen Byte
aws.ecs.cluster.EphemeralStorageReserved.Average	Der flüchtige Speicher ist der flüchtige temporäre Speicher, der an Ihre Instanzen angehängt und nur während der Laufzeit der Instanz vorhanden ist.
aws.ecs.cluster.MemoryUtilized.Average (Empfohlene Metrik)	Arbeitsspeicher, der von Aufgaben im Cluster verwendet wird
aws.ecs.cluster.MemoryReserved.Average (Empfohlene Metrik)	Arbeitsspeicher, der von Aufgaben im Cluster reserviert wurde
aws.ecs.cluster.StorageReadBytes.Average (Empfohlene Metrik)	Anzahl der aus dem Speicher im Cluster gelesenen Byte
aws.ecs.cluster.StorageWriteBytes.Average (Empfohlene Metrik)	Anzahl der in den Speicher im Cluster geschriebenen Byte
aws.ecs.cluster.ContainerInstanceCount.Average (Empfohlene Metrik)	Anzahl der EC2-Instanzen, die den Amazon ECS-Agent ausführen und bei einem Cluster registriert sind
aws.ecs.cluster.ServiceCount.Average (Empfohlene Metrik)	Anzahl der Services im Cluster
aws.ecs.cluster.TaskCount.Average	Anzahl der im Cluster ausgeführten Aufgaben

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ecs-service-Metriken

Metrik	Beschreibung
aws.ecs.service.CPUUtilization.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die im Service verwendet werden
aws.ecs.service.MemoryUtilization.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der im Service verwendet wird
aws.ecs.service.CpuReserved.Average	CPU-Einheiten, die durch Aufgaben im Service reserviert wurden
aws.ecs.service.CpuUtilized.Average	CPU-Einheiten, die durch Aufgaben im Service verwendet wurden
aws.ecs.service.NetworkRxBytes.Average (Empfohlene Metrik)	Anzahl der vom Service empfangenen Byte
aws.ecs.service.NetworkTxBytes.Average (Empfohlene Metrik)	Anzahl der vom Service übertragenen Byte
aws.ecs.service.EphemeralStorageReserved.Average	Der flüchtige Speicher ist der flüchtige temporäre Speicher, der an Ihre Instanzen angehängt und nur während der Laufzeit der Instanz vorhanden ist.
aws.ecs.service.MemoryUtilized.Average	Arbeitsspeicher, der von Aufgaben im Service verwendet wird
aws.ecs.service.MemoryReserved.Average	Arbeitsspeicher, der von Aufgaben im Service reserviert wurde
aws.ecs.service.StorageReadBytes.Average (Empfohlene Metrik)	Anzahl der aus dem Speicher im Service gelesenen Byte
aws.ecs.service.StorageWriteBytes.Average (Empfohlene Metrik)	Anzahl der in den Speicher im Service geschriebenen Byte
aws.ecs.service.RunningTaskCount.Average (Empfohlene Metrik)	Anzahl der Aufgaben, die sich derzeit im Status „WIRD AUSGEFÜHRT“ befinden
aws.ecs.service.DeploymentCount.Average	Anzahl der Bereitstellungen in einem Amazon ECS-Service
aws.ecs.service.DesiredTaskCount.Average (Empfohlene Metrik)	Gewünschte Anzahl von Aufgaben für einen Amazon ECS-Service
aws.ecs.service.TaskSetCount.Average (Empfohlene Metrik)	Anzahl der Aufgabensätze im Service
aws.ecs.service.PendingTaskCount.Average	Anzahl der Aufgaben, die sich derzeit im Status „AUSSTEHEND“ befinden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ecs-service-Metriken (Fortsetzung)

Metrik	Beschreibung
(Empfohlene Metrik)	

Azure-Systemüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für Azure-Systemüberwachung.

Azure Kubernetes (K8s) Service-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	azure.metrics-k8s-service	Stellt Pod bereit, Knoten und Metriken auf Clusterebene aus allen Azure Kubernetes-Services in Metrikform. Verwendung: metrics-azure-k8s-service.rb -S, --subscription ID ARM Subscription ID -r, Region Beispiel: metrics-azure-k8s-service.rb -S {{.labels.params_subscription_id}} -r westus2	metrics-azure-k8s-service.rb -r {{.labels.params_ci_region}} {{-s {{if.labels.params_subscription_id}} -S {{.labels.params_subscription_id}} {{end}}

Azure-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von erfasst werden Azure Prüfungen. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Azure Kubernetes Service-Prüfmetriken

Metrikname	Beschreibung
apiserver_current_inflight_requests (Empfohlene Metrik)	Maximale Anzahl der derzeit auf dem API-Server verwendeten Anforderungen pro Anforderungsart in der letzten Sekunde.
cluster_autoscaler_cluster_safe_to_autoscale	Bestimmt, ob der automatische Skalierer des Clusters Aktionen für den Cluster ausführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Kubernetes Service-Prüfmetriken (Fortsetzung)

Metrikname	Beschreibung
cluster_autoscaler_scale_down_in_cooldown	Bestimmt, ob sich die herunterskalierte Skala in der Abkühlung befindet. Während dieses Zeitrahmens werden keine Knoten entfernt.
cluster_autoscaler_unschedulable_pods_count	Anzahl der Pods, die derzeit im Cluster nicht geplant werden können.
kube_node_status_allocatable_cpu_cores (Empfohlene Metrik)	Gesamtzahl der verfügbaren CPU-Kerne in einem verwalteten Cluster.
kube_node_status_allocatable_memory_bytes (Empfohlene Metrik)	Gesamtmenge des verfügbaren Arbeitsspeichers in einem verwalteten Cluster.
kube_node_status_condition (Empfohlene Metrik)	Status für verschiedene Knotenbedingungen.
kube_pod_status_phase (Empfohlene Metrik)	Anzahl der Pods nach Phase.
kube_pod_status_ready (Empfohlene Metrik)	Anzahl der Pods im Status „bereit“.
node_cpu_usage_millicores (Empfohlene Metrik)	Aggregierte Messung der CPU-Auslastung in Millikernen im Cluster.
node_cpu_usage_percentage (Empfohlene Metrik)	Aggregierte durchschnittliche CPU-Auslastung, gemessen in Prozent im gesamten Cluster.
node_disk_usage_bytes	Anzahl der verwendeten Datenträgerspeicherbytes nach Gerät.
node_disk_usage_percentage (Empfohlene Metrik)	Prozentsatz des vom Gerät verwendeten Datenträgerspeichers.
node_memory_rss_bytes	Anzahl der verwendeten Container-RSS-Arbeitsspeicher-Bytes.
node_memory_rss_percentage (Empfohlene Metrik)	Prozentsatz des verwendeten Container-RSS-Arbeitsspeichers.
node_memory_working_set_bytes	Anzahl der verwendeten Container-Arbeitsspeicher-Bytes.
node_memory_working_set_percentage (Empfohlene Metrik)	Prozentsatz des verwendeten Containerarbeitungs-Satzspeichers.
node_network_in_bytes	Vom Netzwerk empfangene Byte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Kubernetes Service-Prüfmetriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	
node_network_out_bytes (Empfohlene Metrik)	Vom Netzwerk übertragene Byte.

Azure VM-CPU-Metriken

Metrikname	Beschreibung
Percentage CPU (CPU-Prozentsatz) (Empfohlene Metrik)	Der Prozentsatz der zugeteilten Berechnung Einheiten, die derzeit von der/den virtuellen Maschine(n) verwendet werden.
CPU Credits Remaining (CPU-Guthaben verbleibend)	Gesamtanzahl des für Burst verfügbaren Guthabens. Nur verfügbar für Burstable VMs der B-Serie.
CPU Credits Consumed (CPU-Guthaben verbraucht)	Gesamtanzahl des vom virtuellen Computer verbrauchten Guthabens. Nur verfügbar für Burstable VM der B-Serie.

Azure VM-Netzwerk-Metriken

Metrikname	Beschreibung
Netzwerkeingang (Empfohlene Metrik)	Die Anzahl der abrechenbaren Bytes, die auf allen Netzwerkschnittstellen von den virtuellen Computern empfangen wurden (eingehender Datenverkehr) (veraltet).
Netzwerkausgang (Empfohlene Metrik)	Die Anzahl der abrechenbaren Bytes, die von den virtuellen Computern auf allen Netzwerkschnittstellen ausgegeben werden (ausgehender Datenverkehr) (veraltet).
Network In Total (Netzwerkeingang insgesamt) (Empfohlene Metrik)	Die Anzahl der Bytes, die auf allen Netzwerkschnittstellen von den virtuellen Computern empfangen wurden (eingehender Datenverkehr).
Network Out Total (Netzwerkausgang insgesamt) (Empfohlene Metrik)	Die Anzahl der Bytes, die von den virtuellen Computern auf allen Netzwerkschnittstellen ausgegeben werden (ausgehender Datenverkehr).

Azure VM-Laufwerksmetriken

Metrikname	Beschreibung
Disk Read Bytes (Laufwerk-Lesebytes) (Empfohlene Metrik)	Byte, die während des Überwachungszeitraums vom Datenträger gelesen wurden.
Disk Write Bytes (Laufwerk-Schreibbytes)	Byte, die während des Überwachungszeitraums auf den Datenträger geschrieben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Laufwerksmetriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	
Disk Read Operations/Sec (Laufwerk-Lesevorgänge/s) (Empfohlene Metrik)	Datenträger-Lese-IOPS.
Disk Write Operations/Sec (Laufwerk-Schreibvorgänge/s) (Empfohlene Metrik)	Datenträger-Schreib-IOPS.
Data Disk Read Bytes/sec (Datenträger-Lesebytes/s) (Empfohlene Metrik)	Byte pro Sekunde, die während des Überwachungszeitraums von einem einzelnen Datenträger gelesen werden.
Data Disk Write Bytes/sec (Datenträger-Schreibbytes/s) (Empfohlene Metrik)	Byte pro Sekunde, die während des Überwachungszeitraums auf einen einzelnen Datenträger geschrieben werden.
Data Disk Read Operations/Sec (Datenträger-Lesevorgänge/s) (Empfohlene Metrik)	Lesen Sie IOPS von einem einzelnen Datenträger während des Überwachungszeitraums.
Data Disk Write Operations/Sec (Datenträger-Schreibvorgänge/s) (Empfohlene Metrik)	Schreiben Sie IOPS von einem einzelnen Datenträger während des Überwachungszeitraums.
Data Disk Bandwidth Consumed Percentage (Datenträger – Prozentsatz verbrauchter Bandbreite) (Empfohlene Metrik)	Prozentsatz der verbrauchten Bandbreite des Datenträgers pro Minute
Data Disk IOPS Consumed Percentage (Datenträger – Prozentsatz verbrauchter IOPS) (Empfohlene Metrik)	Prozentsatz der verbrauchten E/As des Datenträgers pro Minute
Data Disk Target Bandwidth (Ziel-Bandbreite für Datenträger) (Empfohlene Metrik)	Baseline-Durchsatz in Byte pro Sekunde, den der Datenträger ohne Bursting erreichen kann
Data Disk Target IOPS (Datenträger-Ziel-IOPS) (Empfohlene Metrik)	Baseline-IOPS, die der Datenträger ohne Bursting erreichen kann
Data Disk Max Burst Bandwidth (Maximale Burst-Bandbreite für Datenträger) (Empfohlene Metrik)	Maximaler Durchsatz in Byte pro Sekunde, den der Datenträger mit Bursting erreichen kann

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Laufwerksmetriken (Fortsetzung)

Metrikname	Beschreibung
Data Disk Max Burst IOPS (Max. Burst-IOPS für Datenträger) (Empfohlene Metrik)	Maximale IOPS, die der Datenträger mit Bursting erreichen kann
Data Disk Used Burst BPS Credits Percentage (Prozentsatz des verwendeten Burst-BPS-Guthabens für Datenträger)	Prozentsatz des bisher verwendeten Datenträger-Guthabens für Burst-Bandbreite
Data Disk Used Burst IO Credits Percentage (Prozentsatz des verwendeten Burst-EA-Guthabens für Datenträger)	Prozentsatz des bisher verwendeten Datenträger-Guthabens für Burst-E/A
Premium Data Disk Cache Read Hit (Lese-Treffer für Premium-Datenträger-Cache) (Empfohlene Metrik)	Lese-Treffer für Premium-Datenträger-Cache
Premium Data Disk Cache Read Miss (Lese-Fehler für Premium-Datenträger-Cache) (Empfohlene Metrik)	Lese-Fehler für Premium-Datenträger-Cache
Premium OS Disk Cache Read Hit (Lese-Treffer für Premium-BS-Laufwerks-Cache) (Empfohlene Metrik)	Lese-Treffer für Premium-BS-Laufwerks-Cache
Premium OS Disk Cache Read Miss (Lese-Fehler für Premium-BS-Laufwerks-Cache) (Empfohlene Metrik)	Lese-Fehler für Premium-BS-Laufwerks-Cache

Azure VM-Flow-Metriken

Metrikname	Beschreibung
Eingehender Verkehr (Empfohlene Metrik)	Eingehende Flows sind die Anzahl der aktuellen Flows in eingehender Richtung (Datenverkehr, der in die VM eingeht).
Ausgehender Verkehr (Empfohlene Metrik)	Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)
Inbound Flows Maximum Creation Rate (Maximale Erstellungsrate für eingehende Flows) (Empfohlene Metrik)	Maximale Erstellungsrate eingehender Flows (Datenverkehr, der in die VM eingeht)
Outbound Flows Maximum Creation Rate (Maximale Erstellungsrate für ausgehende Flows) (Empfohlene Metrik)	Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Arbeitsspeichermetriken

Metrikname	Beschreibung
VM Cached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter gecachter Bandbreite) (Empfohlene Metrik)	Prozentsatz der zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
VM Cached IOPS Consumed Percentage (VM – Prozentsatz verbrauchter gecachter IOPS)	Prozentsatz der zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite) (Empfohlene Metrik)	Prozentsatz der nicht zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite)	Prozentsatz der nicht zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
Available Memory Byte (Verfügbarer Arbeitsspeicher (Byte)) (Empfohlene Metrik)	Menge des physischen Arbeitsspeichers in Byte, die sofort für die Zuordnung zu einem Prozess oder für die Systemnutzung in der virtuellen Maschine verfügbar ist.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers

Metrikname	Einheiten	Beschreibung
CPU-Prozentsatz (empfohlene Metrik)	%	Der Prozentsatz der zugeteilten Recheneinheiten, die derzeit von der virtuellen Maschine verwendet werden.
CPU Credits Remaining (CPU-Guthaben verbleibend)		Anzahl der verdienten CPU-Gutschriften, die nicht von der virtuellen Maschine verbraucht wurden.
CPU Credits Consumed (CPU-Guthaben verbraucht)		Gesamtzahl der CPU-Gutschriften, die von der virtuellen Maschine verbraucht wurden.
Netzwerkeingang		Anzahl der Bytes, die auf allen Netzwerkschnittstellen von der Instanz empfangen wurden.
Netzwerkausgang		Anzahl der Bytes, die von der Instanz auf allen Netzwerkschnittstellen gesendet wurden.
Netzwerk insgesamt (empfohlene Metrik)	Byte	Die Anzahl der Bytes, die auf allen Netzwerkschnittstellen von der/den virtuellen Maschine(n) empfangen wurden (eingehender Datenverkehr).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
Netzwerkausgänge insgesamt (empfohlene Metrik)	Byte	Die Anzahl der Bytes, die auf allen Netzwerkschnittstellen von der/den virtuellen Maschine(n) ausgegeben werden (ausgehender Datenverkehr).
Verfügbare Arbeitsspeicherbytes (empfohlene Metrik)	Byte	Menge des physischen Arbeitsspeichers in Byte, der sofort für die Zuteilung zu einem Prozess oder für die Systemverwendung in der virtuellen Maschine verfügbar ist.
VM Cached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter gecachter Bandbreite)		Prozentsatz der zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
VM Cached IOPS Consumed Percentage (VM – Prozentsatz verbrauchter gecachter IOPS)		Prozentsatz der zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite)		Prozentsatz der nicht zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
Prozentsatz des Verbrauchs von nicht zwischengespeicherten IOPS für VM		Prozentsatz der nicht zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
Datenträger-Lesebytes (empfohlene Metrik)	Byte	Byte, die während des Überwachungszeitraums vom Datenträger gelesen wurden.
Datenträger-Schreibbytes (empfohlene Metrik)	Byte	Byte, die während des Überwachungszeitraums auf den Datenträger geschrieben wurden.
Datenträger-Lesevorgänge/Sek. (empfohlene Metrik)	CountPerSecond	Datenträger-Lese-IOPS.
Datenträger-Schreibvorgänge/Sek. (empfohlene Metrik)	CountPerSecond	Datenträger-Schreib-IOPS.
BS-Datenträger – Lesebytes/Sek		Byte/Sek., die während des Überwachungszeitraums vom Datenträger gelesen wurden.
BS-Datenträger-Schreibbytes/Sek		Byte/Sek., die während des Überwachungszeitraums auf den Datenträger geschrieben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
BS-Datenträger-Lesevorgänge/-Sek		Lesen Sie IOPS während des Überwachungszeitraums vom Datenträger.
Schreibvorgänge/Sek. des BS-Datenträgers		Schreiben Sie IOPS während des Überwachungszeitraums vom Datenträger.
Tiefe der BS-Datenträgerwarteschlange		Durchschnittliche Anzahl der Lese- und Schreibanforderungen, die während des Beispielzeitraums für den ausgewählten Datenträger in die Warteschlange gestellt wurden.
Prozentsatz der verbrauchten BS-Datenträgerbandbreite		Prozentsatz der verbrauchten Bandbreite des Datenträgers pro Minute
Prozentsatz der verbrauchten IOPS des BS-Datenträgers		Prozentsatz der verbrauchten E/As des Datenträgers pro Minute
Zielbandbreite des BS-Datenträgers		Baseline-Bytes pro Sekunde Durchsatz der Datenträger kann ohne Bursting erreichen.
Ziel-IOPS des BS-Datenträgers		Baseline-IOPS-Datenträger kann ohne Burst erreichen.
Maximale Burst-Bandbreite des BS-Datenträgers		Maximaler Datendurchsatz in Byte pro Sekunde, den der Datenträger mit Bursting erreichen kann.
Max. Burst-IOPS des Betriebssystemdatenträgers		Maximale IOPS-Daten, die der Datenträger mit Bursting erreichen kann.
Prozentsatz der verwendeten Burst-BPS-Gutschriften des BS-Datenträgers		Prozentsatz der bisher verwendeten Burst-Bandbreitengutschriften für Datenträger.
Prozentsatz der verwendeten Burst-E/A-Gutschriften des BS-Datenträgers		Prozentsatz der bisher verwendeten Burst-E/A-Gutschriften für Datenträger.
Premium OS Disk Cache Read Hit (Lese-Treffer für Premium-BS-Laufwerks-Cache)		Lesetreffer für Premium-BS-Datenträger-Cache.
Premium OS Disk Cache Read Miss (Lese-Fehler für Premium-BS-Laufwerks-Cache)		Fehler beim Lesen des Cache des Premium-BS-Datenträgers.
Eingehende Flows		Anzahl der aktuellen Flows in eingehender Richtung (Datenverkehr, der in die VM geht).
Ausgehende Flows		Anzahl der aktuellen Flows in eingehender Richtung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		(Datenverkehr, der von der VM ausgeht).
Inbound Flows Maximum Creation Rate (Maximale Erstellungsrate für eingehende Flows)		Maximale Erstellungsrate eingehender Flows (Datenverkehr, der in die VM eingeht)
Outbound Flows Maximum Creation Rate (Maximale Erstellungsrate für ausgehende Flows)		Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)

Metrikrichtlinie für Azure-Lastenausgleichsmodul – Metriken für Azure-Metriksammler-Prüfung

Metrikname	Einheiten	Beschreibung
AllocatedSnatPorts (empfohlene Metrik)		Gesamtzahl der SNAT-Ports, die innerhalb des in der Metrikdefinition angegebenen Zeitraums zugewiesen sind *PT*Wert (Zeitraum).
ByteCount (empfohlene Metrik)	Bytes	Gesamtzahl der Bytes, die innerhalb des in der Metrikdefinition angegebenen Zeitraums übertragen wurden *PT*Wert (Zeitraum).
DipAvailability (empfohlene Metrik)	count	Durchschnittlicher Status der Lastenausgleichsmodul-Integritätsprobe pro Zeitdauer.
BlockedCount (empfohlene Metrik)		Gesamtzahl der Pakete, die innerhalb des in der Metrikdefinition angegebenen Zeitraums übertragen wurden *PT*Wert (Zeitraum).
SnatConnectionCount (empfohlene Metrik)	count	Gesamtanzahl der neuen SNAT-Verbindungen, die innerhalb des durch die Metrikdefinition angegebenen Zeitraums erstellt wurden *PT*Wert (Zeitraum).
SYNCount (empfohlene Metrik)		Gesamtzahl der SYN-Pakete, die innerhalb des in der Metrikdefinition angegebenen Zeitraums übertragen wurden *PT*Wert (Zeitraum).
UsedSnatPorts (empfohlene Metrik)		Gesamtzahl der SNAT-Ports, die innerhalb des von der Metrikdefinition angegebenen Zeitraums verwendet werden *PT*Wert (Zeitraum).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikrichtlinie für Azure-Lastenausgleichsmodul – Metriken für Azure-Metriksammler-Prüfung (Fortsetzung)

Metrikname	Einheiten	Beschreibung
VipAvailability (empfohlene Metrik)	count	Durchschnittliche Verfügbarkeit des Lastenausgleichsmodul-Datenpfads pro Zeitdauer.

Azure-Redis-Cache-Richtlinie – Prüfmetriken des Azure-Metriksammlers

Metrikname	Einheiten	Beschreibung
ConnectedClients		Anzahl der Clientverbindungen zum Cache.
TotalBefehlsprognet		Gesamtanzahl der vom Cache-Server verarbeiteten Befehle.
Cachehits (empfohlene Metrik)	count	Anzahl der erfolgreichen Schlüsselsuchen.
Zwischenfälle (empfohlene Metrik)	count	Anzahl der fehlgeschlagenen Schlüsselsuchen.
Cachemissrate		Rate der fehlgeschlagenen Schlüsselsuchen.
Getcommand		Anzahl der GET-Vorgänge aus dem Cache.
Setcommands (empfohlene Metrik)	count	Anzahl der Set-Vorgänge für den Cache.
OperationsPerSecond		Anzahl der sofortigen Vorgänge pro Sekunde, die im Cache ausgeführt werden.
EvictedKeys		Anzahl der Elemente, die aus dem Cache entfernt wurden.
TotalKeys		Anzahl der Schlüssel im Cache.
Ablaufschlüssel		Anzahl der Elemente, die aus dem Cache abgelaufen sind.
Verwendeter Arbeitsspeicher	Bytes	Menge des Cache-Arbeitsspeichers, der für Schlüssel-Wert-Paare im Cache verwendet wird.
Used MemoryRss	Bytes	Menge des während des angegebenen Berichtsintervalls verwendeten Cache-Speichers, einschließlich Fragmentierung und Metadaten
ServerLoad (empfohlene Metrik)	Prozent	Prozentsatz der Zyklen, in denen der Redis-Server mit der Verarbeitung beschäftigt ist und nicht auf Nachrichten im Leerlauf wartet

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Redis-Cache-Richtlinie – Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
CacheWrite (empfohlene Metrik)	BytesPersSecond	Menge der in den Cache geschriebenen Daten.
CacheRead (empfohlene Metrik)	BytesPerSecond	Menge der aus dem Cache gelesenen Daten.
Alle ConnectionsCreatedPerSecond		Anzahl der sofortigen Verbindungen, die pro Sekunde im Cache über Port 6379 oder 6380 (SSL) erstellt wurden.
Alle ConnectionsClosedPerSecond		Anzahl der sofortigen Verbindungen, die pro Sekunde im Cache über Port 6379 oder 6380 (SSL) geschlossen wurden.
AllconnectedClients (empfohlene Metrik)	count	Anzahl der derzeit mit dem System verbundenen Clients.
AlltotalBefehlsprognet		Die kumulative Anzahl aller vom System verarbeiteten Befehle.
ZuteilungsPerSecond		Gesamtzahl der Vorgänge (z. B. Lese- oder Schreibbefehle), die pro Sekunde in allen Instanzen ausgeführt werden.
AllusedMemory (empfohlene Metrik)	Bytes	Gesamtmenge des im System verwendeten Arbeitsspeichers.
AllusedmemoryRss (empfohlene Metrik)	Bytes	Die gesamte residente Satzgröße (Resident Set Size, RSS), die die Menge des physisch im RAM über alle Instanzen hinweg vorhandenen Arbeitsspeichers widerspiegelt, einschließlich Swap.

Azure-Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers

Metrikname	Einheiten	Beschreibung
ApplicationGatewayTotalTime (empfohlene Metrik)	Millisekunden	Zeit, die benötigt wird, um eine Anforderung zu verarbeiten und ihre Antwort zu senden.
AvgRequestCountPerHealthyHost		Durchschnittliche Anforderungsanzahl pro Minute pro fehlerfreiem Back-End-Host in einem Pool.
AzwafBotProtectionMatches		Übereinstimmende Bot-Regeln.
AzwafCustomRuleÜbereinstimmungen		Übereinstimmende Anwenderdefinierte Regeln.
AzwafSecRuleMatches		Übereinstimmende Verwaltete Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
AzwafTotalRequests		Gesamtzahl der von WAF ausgewerteten Anforderungen.
BackendConnectTime		Zeit, die für die Herstellung einer Verbindung mit einem Back-End-Server aufgewendet wurde.
BackendFirstByteResponseTime		Zeitintervall zwischen dem Beginn der Herstellung einer Verbindung zum Back-End-Server und dem Empfang des ersten Bytes des Antwortheaders, annähernd die Verarbeitungszeit des Back-End-Servers.
BackendLastByteResponseTime		Zeitintervall zwischen dem Beginn der Herstellung einer Verbindung zum Back-End-Server und dem Empfang des letzten Bytes des Antworttexts.
BackendResponseStatus		Anzahl der von den Back-End-Mitgliedern generierten HTTP-Antwortcodes. Dies enthält keine Antwortcodes, die vom Anwendungs-Gateway generiert wurden.
BlockedCount		Gesamtzahl der blockierten Vorgänge oder Anforderungen
BytesReceived (empfohlene Metrik)	Bytes	Gesamtzahl der Byte, die das Anwendungs-Gateway von den Clients empfangen hat.
BytesSent (empfohlene Metrik)	Bytes	Gesamtzahl der Byte, die vom Anwendungs-Gateway an die Clients gesendet werden.
Kapazitätseinheiten		Verbrauchte Kapazitätseinheiten.
ClientRtt		Round-Trip-Zeit zwischen Clients und Anwendungs-Gateway. Gibt an, wie lange es dauert, Verbindungen herzustellen und Bestätigungen zurückzugeben.
ComputeUnits		Verbrauchte Einheiten berechnen.
CpuAuslastung		Aktuelle CPU-Auslastung des Anwendungs-Gateways.
CurrentConnections (empfohlene Metrik)	count	Anzahl der aktuellen Verbindungen, die mit dem Anwendungs-Gateway hergestellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metriksammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
GeschätztBilledCapacityUnits		Geschätzte Kapazitätseinheiten, die berechnet werden.
FailedRequests (empfohlene Metrik)	count	Anzahl der fehlgeschlagenen Anforderungen, die das Anwendungs-Gateway bedient hat.
FixedBillableCapacityUnits		Feste Abrechenbare Kapazitätseinheiten.
HealthyHostCount (empfohlene Metrik)	count	Anzahl der fehlerfreien Back-End-Hosts.
NewConnectionsPerSecond		Neue Verbindungen pro Sekunde mit Anwendungs-Gateway hergestellt.
ResponseStatus		HTTP-Antwortstatus, der vom Anwendungs-Gateway zurückgegeben wird.
Durchsatz (empfohlene Metrik)	BytesPerSecond	Anzahl der Byte pro Sekunde, die das Anwendungs-Gateway bedient hat.
Anforderungen insgesamt (empfohlene Metrik)	count	Anzahl der erfolgreichen Anforderungen, die das Application Gateway bedient hat.
UnhealthyHostCount (empfohlene Metrik)	count	Anzahl der fehlerhaften Back-End-Hosts.

Azure-Speicher-Account-Richtlinie: Prüfmetriken des Azure Metrics Collectors

Metrikname	Einheiten	Beschreibung
Transaktionen (empfohlene Metrik)	count	Gesamtzahl der Anforderungen an den Speicher-Account.
Eingang (empfohlene Metrik)	Bytes	Menge der eingehenden Daten. Diese Zahl enthält den Eingang von einem externen Client in Azure Speicher sowie Eingang in Azure.
Ausgang (empfohlene Metrik)	Bytes	Menge der Ausgangsdaten. Diese Zahl enthält den Ausgang von einem externen Client in Azure Speicher sowie Ausgang innerhalb von Azure. Daher spiegelt diese Zahl den abrechenbaren Ausgang nicht wider.
SuccessServerLatency (empfohlene Metrik)	Millisekunden	Durchschnittliche Latenz verwendet von Azure Speicher zur Verarbeitung einer erfolgreichen Anforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Speicher-Account-Richtlinie: Prüfmetriken des Azure Metrics Collectors (Fortsetzung)

Metrikname	Einheiten	Beschreibung
SuccessE2ELatency (empfohlene Metrik)	Millisekunden	Die durchschnittliche End-to-End-Latenz erfolgreicher Anforderungen an einen Speicherservice oder den angegebenen API-Vorgang.
Verfügbarkeit (empfohlene Metrik)	Prozent	Der Prozentsatz der Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang.

Azure Blob Services-Metriken

Metrikname	Beschreibung
Verfügbarkeitsdiagramm	Prozentsatz der Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang. Die Verfügbarkeit wird berechnet, indem der Wert TotalBillableRequests durch die Anzahl der zutreffenden Anforderungen geteilt wird, einschließlich derer, die unerwartete Fehler verursacht haben. Alle unerwarteten Fehler tragen zu verringerter Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang bei.
BlobCapacity (Empfohlene Metrik)	Menge des vom Blob-Service des Speicherkontos verwendeten Speichers in Byte
BlobCount	Anzahl der Blobs im Blob-Service des Speicherkontos
Container Count (Containeranzahl)	Anzahl der Container im Blob-Service des Speicherkontos
Ausgehend (Empfohlene Metrik)	Menge der Ausgangsdaten in Byte. Schließt den ausgehenden Datenverkehr eines externen Clients in den Azure-Speicher sowie den ausgehenden Datenverkehr des Azure-Clients ein. Daher spiegelt diese Zahl nicht den abrechenbaren ausgehenden Datenverkehr wider.
Index Capacity (Indexkapazität) (Empfohlene Metrik)	Vom (hierarchischen) ADLS Gen2-Index genutzter Speicher in Byte
Eingehend (Empfohlene Metrik)	Menge der Eingangsdaten in Byte. Schließt den eingehenden Datenverkehr eines externen Clients in den Azure-Speicher sowie den eingehenden Datenverkehr des Azure-Clients ein.
SuccessE2ELatency (Empfohlene Metrik)	End-to-End-Latenzzeit erfolgreicher Anforderungen an einen Speicherservice oder den angegebenen API-Vorgang in Millisekunden. Schließt die erforderliche Verarbeitungszeit im Azure-Speicher zum Lesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Blob Services-Metriken (Fortsetzung)

Metrikname	Beschreibung
	der Anforderung, zum Senden der Antwort und zum Empfangen einer Bestätigung der Antwort ein.
SuccessServerLatency (Empfohlene Metrik)	Latenz in Millisekunden, die vom Azure-Speicher zur Verarbeitung einer erfolgreichen Anforderung verwendet wird. Dieser Wert enthält nicht die in **SuccessE2ELatency** angegebene Netzwerklatenz.
Transactions	Anzahl der Anforderungen, die an einen Speicherservice oder den angegebenen API-Vorgang gesendet wurden. Enthält erfolgreiche und fehlgeschlagene Anforderungen sowie Anforderungen, die Fehler verursacht haben. Verwenden Sie die Dimension *ResponseType* für die Anzahl der verschiedenen Antworttypen.

Azure Cloud-Metriken

Azure Cloud-Metriken werden aus gesammelt Azure Virtuelle Computer (VMs) und Azure Speicheraccount-Richtlinien. Durch das Sammeln der Cloud-Metriken können Sie die Leistung von überwachen Azure Ressourcen.

Azure Cloud-Metriksammlung – Übersicht

Um mit der Erfassung zu beginnen Azure Cloud-Metriken, müssen Sie die Metriken auswählen, die Sie der hinzufügen möchten CMDB Und legen Sie die relevanten Systemkonfigurationen fest. Sie können beispielsweise die Anzahl der gesendeten und empfangenen Bytes überwachen Azure Ressourcen. Details finden Sie unter Agent Client Collector Visibility – Inhalt – Referenz.

Verwenden Azure Richtlinien

Sie können vorkonfiguriert verwenden Azure Richtlinien für die Metriksammlung, oder Sie können eigene erstellen Azure Richtlinien.

Wenn Sie eine vorkonfigurierte Richtlinie verwenden, führen Sie die folgenden Aufgaben aus:

- Bereiten Sie eine Instanz mit einem aktiven vor MID-Server Und Metrikbasis.
- Installieren Agent Client Collector Framework Und Agent Client Collector-Überwachung.
- Ausführen Discovery Auf der Azure Cloud-Account zum Ausfüllen von CMDB Mit den zu überwachenden Konfigurationselementen (Configuration Items, CIs).
- Konfigurieren Sie einen Proxy-Agent, und weisen Sie der Richtlinie Anmeldeinformationen zu. Proxy-Agents überwachen CIs für Agents, die sich in der Cloud befinden. Mit Anmeldeinformationen kann der Service Desk-Mitarbeiter auf zugreifen Azure Richtlinie.

Die mit dem Basissystem verfügbaren Richtlinien zum Aktivieren und Konfigurieren sind in der folgenden Tabelle beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Basissystem verfügbare Azure-Richtlinien

Richtlinienname	Beschreibung	Link zu unterstützten Metriken
Azure Lastenausgleichsmodul-Metriken	Sammelt die Metriken für Azure Lastenausgleichsmodule.	Unterstützte Metriken für Microsoft Lastenausgleichsmodule
Azure Gateway-Metriken	Sammelt die Metriken für Azure Netzwerk-Gateway.	Unterstützte Metriken für Microsoft Network Gateways
Azure Redis-Cache-Metriken	Sammelt die Metriken für Azure Redis-Cache.	Unterstützte Metriken für Microsoft Redis-Cache
Azure Speicher-Account-Metriken	Sammelt die Metriken für Azure Speicher-Accounts.	Unterstützte Metriken für Microsoft-Speicher-Accounts
Azure VM-Metriken (Virtual Machine)	Sammelt die Metriken für die VMs, die Ihnen bei der Überwachung helfen Azure VMs.	Unterstützte Metriken für virtuelle Microsoft-Computer

Gibt die CIs für die Metriksammlung an

Beim Erstellen von Richtlinien müssen Sie die CIs, für die Sie die Metriken erfassen möchten, in einschließen CMDB. Die CIs werden normalerweise während ausgefüllt Discovery, Der Anwendungen und Geräte in Ihrem Netzwerk findet und aktualisiert CMDB Entsprechend.

Beim Erstellen einer Richtlinie müssen Sie entscheiden, welche CIs die Richtlinie überwachen soll. Um die Überwachung von CIs zu aktivieren, führen Sie die folgenden Aufgaben aus:

1. Konfigurieren Sie Azure Prüfung des Metriksammlers in der Richtlinie.
2. Legen Sie die Anmeldeinformationen für fest Azure Prüfung des Metriksammlers, um das Abrufen von Metriken aus zu ermöglichen Azure Zu Agent Client Collector Service Desk-Mitarbeiter.
3. Generieren Sie eine JSON-Datei, die die Liste der zu überwachenden Ressourcen angibt.
4. Generieren Sie eine JSON-Datei, die die Liste der Metriken angibt, die aus überwachten Ressourcen abgerufen werden sollen.

Weitere Informationen zu den Azure-Richtlinien finden Sie unter Erstellen Azure Richtlinien für die Metriksammlung.

Für Details zu Azure Metriken-Batch-API, siehe Metriken-Batch-API Seite.

Cassandra – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Cassandra-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für verfügbar Linux Nur.

Cassandra Metriken

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
app.cassandra.metrics-cassandra	Gibt Metriken von zurück	metrics-cassandra-graphite.rb	metrics-cassandra-graphite.rb	<host>.cassandra.load 132270.08 1645107221

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra Metriken (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	Cassandra Datenbank.	Optionen: **-h host** Hostname, in dem Cassandra Datenbank wird ausgeführt **-P port** Cassandra JMX-Port	--cfstats -P {{.labels.params_port}} -h {{.labels.params_host}}	

Cassandra-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Cassandra-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Metriken – Cassandra-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.load (empfohlene Metrik)		Byte	Der von Live-Daten auf einem Knoten verwendete Speicherplatz.
cassandra.uptime (empfohlene Metrik)		seconds	
cassandra.heap.used (empfohlene Metrik)		Byte	
cassandra.heap.total (empfohlene Metrik)		Byte	
cassandra.exceptions		count	Anzahl der erfassten internen Ausnahmen. Unter normalen Ausnahmebedingungen sollte dieser Wert null sein.
cassandra.key_cache.size		Byte	Gesamtgröße des belegten Cache in Byte.
cassandra.key_cache.capacity		Byte	Cache-Kapazität in Byte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.key_cache.hits		count	Gesamtzahl der Cache-Treffer.
cassandra.key_cache.requests (empfohlene Metrik)		count	Gesamtzahl der Cache-Anforderungen.
cassandra.key_cache.hit_rate (empfohlene Metrik)		count	Cache-Trefferquote (gesamte Zeitspanne).
cassandra.compactionstats.pending_tasks		count	Anzahl der ausstehenden Komprimierungen.
cassandra.threadpool.ReadStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Lokale Lesevorgänge, die für diesen Thread-Pool in dieser ReadStage ausgeführt werden.
cassandra.threadpool.ReadStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.ReadStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.ReadStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MiscStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verschiedene in dieser Phase ausgeführte Aufgaben.
cassandra.threadpool.MiscStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MiscStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MiscStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.CompactionExecutor.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Komprimierungen werden für diese Threads ausgeführt.
cassandra.threadpool.CompactionExecutor.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.CompactionExecutor.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.CompactionExecutor.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MutationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für alle anderen Schreibvorgänge.
cassandra.threadpool.MutationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MutationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MutationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MemtableReclaimMemory.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Memtable-Recycling.
cassandra.threadpool.MemtableReclaimMemory.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MemtableReclaimMemory.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MemtableReclaimMemory.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.PendingRangeCalculator.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Berechnet den Tokenbereich.
cassandra.threadpool.PendingRangeCalculator.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.PendingRangeCalculator.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.PendingRangeCalculator.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.GossipStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Behandelt Gossip-Anforderungen.
cassandra.threadpool.GossipStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.GossipStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.GossipStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.SecondaryIndexManagement.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt Aktualisierungen von sekundären Indizes durch.
cassandra.threadpool.SecondaryIndexManagement.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.SecondaryIndexManagement.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.SecondaryIndexManagement.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.Hints	Dispatcher.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt eine angedeutete Übergabe (hinted Handoff) durch.
cassandra.threadpool.Hints	Dispatcher.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.Hints	Dispatcher.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.Hints	Dispatcher.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.Request	ResponseStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Koordinatoranforderungen an den Cluster werden in diesem Thread-Pool ausgeführt.
cassandra.threadpool.Request	ResponseStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.Request	ResponseStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.Request	ResponseStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.Read	RepairStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Die Lesereparatur (Read Repair) erfolgt in diesem Thread-Pool.
cassandra.threadpool.Read	RepairStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.Read	RepairStage.completed	count	Anzahl der abgeschlossenen Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.ReadRepairStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.CounterMutationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für Zählerschreibvorgänge.
cassandra.threadpool.CounterMutationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.CounterMutationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.CounterMutationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MigrationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt Schemamigrationen aus.
cassandra.threadpool.MigrationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MigrationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MigrationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MemtablePostFlush.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Bereinigt das Commit-Protokoll, nachdem die Memtable auf den Datenträger geschrieben wurde.
cassandra.threadpool.MemtablePostFlush.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.MemtablePostFlush.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MemtablePostFlush.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für das Schreiben einer Spezifikation (pro Datenträger (0–N) gibt es eine davon).
cassandra.threadpool.PerDiskMemtableFlushWriter_0.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.ValidationExecutor.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt eine Validierungskomprimierung oder -bereinigung durch.
cassandra.threadpool.ValidationExecutor.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.ValidationExecutor.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.ValidationExecutor.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.Sampler.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für die Neufestlegung der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Indexzusammenfassungen von `SStables`.
cassandra.threadpool.Sampler.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.Sampler.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.Sampler.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MemtableFlushWriter.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Schreibt Memtables auf den Datenträger.
cassandra.threadpool.MemtableFlushWriter.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MemtableFlushWriter.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MemtableFlushWriter.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.InternalResponseStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für clusterinterne Rückrufe.
cassandra.threadpool.InternalResponseStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.InternalResponseStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.InternalResponseStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.ViewMutationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für Schreibvorgänge in der materialisierten Ansicht.
cassandra.threadpool.ViewMutationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.ViewMutationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.ViewMutationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.AntiEntropyStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Erstellt einen Hash-Baum für Reparaturen.
cassandra.threadpool.AntiEntropyStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.AntiEntropyStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.AntiEntropyStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.CacheCleanupExecutor.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Für diesen Thread-Pool durchgeführte Cache-Wartung.
cassandra.threadpool.CacheCleanupExecutor.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.CacheCleanupExecutor.completed		count	Anzahl der abgeschlossenen Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.CacheCleanupExecutor.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.message_type.READ.dropped		count	Anzahl der gelöschten Nachrichten. Reguläre Lesevorgänge.
cassandra.message_type.RANGE_SLICE.dropped		count	Anzahl der gelöschten Nachrichten. Gelesener Tokenbereich.
cassandra.message_type._TRACE.dropped		count	Anzahl der gelöschten Nachrichten. Nachverfolgen von Schreibvorgängen.
cassandra.message_type.HINT.dropped		count	Anzahl der gelöschten Nachrichten. Erneute Wiedergabe von Hinweis.
cassandra.message_type.MUTATION.dropped		count	Anzahl der gelöschten Nachrichten. Reguläre Schreibvorgänge.
cassandra.message_type.COUNTER_MUTATION.dropped		count	Anzahl der gelöschten Nachrichten. Zählerschreibvorgänge.
cassandra.message_type.BATCH_STORE.dropped		count	Anzahl der gelöschten Nachrichten. Batchlog-Schreibvorgang.
cassandra.message_type.BATCH_REMOVE.dropped		count	Anzahl der gelöschten Nachrichten. Batchlog-Bereinigung (nach erfolgreicher Anwendung).
cassandra.message_type.REQUEST_RESPONSE.dropped		count	Anzahl der gelöschten Nachrichten. RPC-Rückrufe.
cassandra.message_type.PAGED_RANGE.dropped		count	Anzahl der gelöschten Nachrichten. Lesen als Seite.
cassandra.message_type.READ_REPAIR.dropped		count	Anzahl der gelöschten Nachrichten. Lesereparatur.
cassandra.system_traces.read_count		count	Anzahl der Lesevorgänge für diese Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.system_traces.read_latency			Lokale Leselatenz für diese Tabelle.
cassandra.system_traces.write_count		count	Anzahl der Schreibvorgänge für diese Tabelle.
cassandra.system_traces.write_latency			Lokale Schreiblatenz für diese Tabelle.
cassandra.system_traces.pending_flushes		count	Geschätzte Anzahl der ausstehenden Löschaufgaben für diese Tabelle.
cassandra.system.read_count (empfohlene Metrik)		count	
cassandra.system.read_latency (empfohlene Metrik)		Mikrosekunden	
cassandra.system.write_count (empfohlene Metrik)		count	
cassandra.system.write_latency (empfohlene Metrik)		Mikrosekunden	
cassandra.system.pending_flushes		count	
cassandra.system_distributed.read_count		count	
cassandra.system_distributed.read_latency			
cassandra.system_distributed.write_count		count	
cassandra.system_distributed.write_latency			
cassandra.system_distributed.pending_flushes		count	
cassandra.system_schema.read_count		count	
cassandra.system_schema.read_latency			
cassandra.system_schema.write_count		count	
cassandra.system_schema.write_latency			
cassandra.system_schema.pending_flushes		count	
cassandra.system_auth.read_count		count	
cassandra.system_auth.read_latency			
cassandra.system_auth.write_count		count	
cassandra.system_auth.write_latency			
cassandra.system_auth.pending_flushes		count	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardprüfungen und -Richtlinien für Verzeichnisscanüberwachung

Die Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für die Überwachung des Directory-Scans bereit.

Windows BS-Ereignisse: Erweiterte Richtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Ereignis	Check-Directory-file-count	Überprüft die Anzahl der in einem bestimmten Verzeichnis vorhandenen Dateien und vergleicht sie mit den angegebenen Warnungs- und kritischen Schwellenwerten. Gibt ein KRITISCHES, WARNENDES oder OK-Ereignis basierend auf den Schwellenwerten „Kritisch“ und „Warnung“ zurück.	Check-Directory-file-count.rb (Optionen) -D, --dir absoluter Pfad zum Verzeichnis zum Zählen der Dateien (erforderlich) -W, --Warnungsschwellenwert (erforderlich) -C, --kritischer kritischer Schwellenwert (erforderlich) -H, include_hidden_files als aktiv festgelegt auf **Wahr** Zum	DirectoryFileCount KRITISCH: <Pfad zu dir> hat 165 Dateien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Hinweis: • Zählt die Anzahl der Dateien im Verzeichnis, ohne Dateien in Unterverzeic • Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungs für das überwachte Verzeichnis.	Einbeziehen ausgeblendeter Dateien beim Zählen (Standard ist **Falsch**) **Anwendungsbeis piel:** `Check-Directory-file-count.rb -d /path/to/Directory -W 50 -c 100` berechtigungen	
Ereignis	Check-Directory-Integrity	Vergleicht die Zeit der letzten Änderung des Verzeichnisses mit der aktuellen Zeit, um zu bestimmen, ob innerhalb eines definierten Zeitintervalls Aktualisierungen vorgenommen wurden. Basierend auf diesem Vergleich gibt die Prüfung ein KRITISCHES oder OK-Ereignis zurück.	Common Checks-Directory-Integrity (Optionen) -D, --dirpath DIRPATH: Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -i, --Intervall-Intervall: Zeitintervall in Sekunden, um nach aktuellen Updates zu suchen (erforderlich).	Allgemeine Prüfungen KRITISCH: Verzeichnisintegrität: CHANGES für <path to file> innerhalb der letzten 180 Sekunden ERKANNT (zuletzt geändert: Mi, 04 Dec 2024 12:18:55 EST).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Hinweis: Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	Der Standardwert kann auf 180 Sekunden festgelegt werden. **Anwendungsbeispiel:** `Common Checks Check-Directory-Update -d /path/to/Directory -i 180`	
Ereignis	Überprüfen Sie das Dateialter	Wertet das Alter einer angegebenen Datei aus, indem der Zeitpunkt der letzten Änderung mit dem aktuellen Zeitpunkt verglichen wird. Löst eine Warnung aus, wenn die Datei die definierten Schwellenwerte für „Kritisch“ oder „Warnungsalter“ überschreitet. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	Common Checks – Dateialter überprüfen (Optionen) -F, --filepath FILEPATH: Absoluter Pfad zur zu überprüfenden Datei (erforderlich). -C, --Critical CRITICAL: Schwellenwert für kritisches Alter in Minuten für die Datei (erforderlich). -W, --warning WARNING: Warnungsaltersschwellenwert in Minuten für die Datei (erforderlich). **Anwendungsbeispiel:** `Common Checks Check-file-age -f /path/to/file.txt -c 120 -W 60`	Allgemeine Prüfungen OK: Datei <Pfad zur Datei> Alter: 30 Minuten.
Ereignis	Check-file-response-time	Vergleicht die Zeit, die zum	Common Checks – Dateiantwortzeit prüfen (Optionen)	Allgemeine Prüfungen OK: Antwortzeit des

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Lesen einer angegebenen Datei benötigt wird, und vergleicht sie mit den Schwellenwerten „Kritisch“ und „Warnung“. Basierend auf diesem Vergleich gibt die Prüfung ein KRITISCHES oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	-F, --filepath FILEPATH: Absoluter Pfad zur zu überprüfenden Datei (erforderlich). -C, --Critical CRITICAL: Kritischer Schwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -W, --warning WARNING: Warnungsschwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -T, --TIMEOUT: Maximal zulässige Zeit zum Lesen des Dateiinhalts, angegeben in Sekunden. Der Zeitüberschreitungswert muss größer als der kritische Schwellenwert sein. **Anwendungsbeispiel:** Common Checks Check-file-response-time -f /var/log/servicenow/Agent-Client-Collector/acc.log -c 10 -W 5 -t 20	Dateilesens: 0,0020 Sekunden für Dateiname: /Var/log/servicenow/Agent-Client-Collector/ACC.log.
Ereignis	Dateigröße überprüfen	Misst die Größe einer Datei (die tatsächliche	Common Checks – Dateigröße prüfen (Optionen)	Allgemeine Prüfungen OK: Für Datei <Pfad zur Datei> Größe: 4,72

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Menge der darin enthaltenen Daten) und vergleicht sie mit den angegebenen Schwellenwerten. Gibt basierend auf dem Vergleich der Dateigröße und der Schwellenwerte ein KRITISCHES, WARNENDES oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	-F, --filepath FILEPATH absoluter Pfad zur erforderlichen Datei (erforderlich). -C, --kritisch. Kritischer Schwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 1000 für 1000 KB) (erforderlich) -W, --Warnung. Warnungsschwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 500 für 500 KB) (erforderlich) **Anwendungsbeispiel:** Common Checks Check-file-size -f C:\ProgramData\ServiceNow\Agent-Client-Collector\config\acc.yml	KB liegt innerhalb der Schwellenwerte
Ereignis	Dateibereich überprüfen	Misst die Größe einer Datei auf dem Datenträger anhand der angegebenen Schwellenwerte und gibt basierend auf den Schwellenwerten ein KRITISCHES, WARNENDES	Gemeinsame Prüfungen – Dateibereich prüfen (Optionen) -F, --filepath FILEPATH: Absoluter Pfad zur relevanten Datei (erforderlich). -C, --Critical CRITICAL: Kritischer	Allgemeine Prüfungen OK: Datei <Pfad zur Datei> Speicherplatz: 8,00 KB liegt innerhalb des Schwellenwerts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	Schwellenwert in Kilobyte. Wird als Zahl ohne Einheiten bereitgestellt (z. B. 1000 für 1000 KB) (erforderlich) -W, --warning WARNING: Warnungsschwellenwert in Kilobyte. Wird als Zahl ohne Einheiten bereitgestellt (z. B. 500 für 500 KB) (erforderlich) -B, --blocksize BLOCKSIZE: Blockgröße in Byte (Standard = 4096) (erforderlich) **Anwendungsbeispiel:** Common Checks Check-file-space -f C:\ProgramData\ServiceNow\Agent-Client-Collector\config\acc.yml	
Ereignis	os.windows.check-directory-space	Überprüft den Speicherplatz, der vom Inhalt eines Verzeichnisses belegt wird. Gibt ein KRITISCHES, WARNENDES oder OK-Ereignis basierend auf dem Vergleich mit den angegebenen Schwellenwerten für den Schweregrad kritischer und	Winchecks Check-dir-space (Optionen) -D, --dirpath DIRPATH: Absoluter Pfad zum zu prüfenden Verzeichnis (erforderlich). -C, --Critical CRITICAL: Schwellenwert	Windows-Prüfungen OK: Verzeichnis <Pfad zur Datei> Speicherplatz: 369,25 KB liegt innerhalb der Schwellenwerte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		warnender Ereignisse zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	für kritischen Speicherplatz in Kilobyte (erforderlich). -W, --warning WARNING: Warnungsschwellenwert für Datenträgerspeicher in Kilobyte (erforderlich). -T, --TIMEOUT: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** `Winchecks Check-dir-space -d /path/to/Directory -c 1000 -W 500 -t 120`	

Linux BS-Ereignisse: Erweiterte Richtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Ereignis	Check-Directory-file-count	Überprüft die Anzahl der in einem bestimmten Verzeichnis vorhandenen Dateien und vergleicht sie mit den angegebenen Warnungs- und kritischen Schwellenwerten. Gibt ein KRITISCHES,	Check-Directory-file-count.rb (Optionen) -D, --dir absoluter Pfad zum Verzeichnis zum Zählen der Dateien (erforderlich) -W, --Warnungsschwellenwert (erforderlich)	DirectoryFileCount KRITISCH: <Pfad zu dir> hat 165 Dateien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		WARNENDES oder OK-Ereignis basierend auf den Schwellenwerten „Kritisch“ und „Warnung“ zurück. **Hinweis:** • Zählt die Anzahl der Dateien im Verzeichnis, ohne Dateien in Unterverzeic • Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungs für das überwachte Verzeichnis.	-C, --kritischer kritischer Schwellenwert (erforderlich) -H, include_hidden_files als aktiv festgelegt auf **Wahr** Zum Einbeziehen ausgeblendeter Dateien beim Zählen (Standard ist **Falsch**) **Anwendungsbeispiel:** `Check-Directory-file-count.rb -d /path/to/Directory -W 50 -c 100` berechtigungen	
Ereignis	Check-Directory-Integrity	Vergleicht die Zeit der letzten Änderung des Verzeichnisses mit der aktuellen Zeit, um zu bestimmen, ob innerhalb eines definierten Zeitintervalls Aktualisierungen vorgenommen wurden. Basierend auf diesem Vergleich gibt die Prüfung ein KRITISCHES	Common Checks-Directory-Integrity (Optionen) -D, --dirpath DIRPATH: Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -i, --Intervall-Intervall: Zeitintervall in Sekunden, um	Allgemeine Prüfungen KRITISCH: Verzeichnisintegrität: CHANGES für <path to file> innerhalb der letzten 180 Sekunden ERKANNT (zuletzt geändert: Mi, 04 Dec 2024 12:18:55 EST).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	nach aktuellen Updates zu suchen (erforderlich). Der Standardwert kann auf 180 Sekunden festgelegt werden. **Anwendungsbeispiel:** `Common Checks Check-Directory-Update -d /path/to/Directory -i 180`	
Ereignis	Überprüfen Sie das Dateialter	Wertet das Alter einer angegebenen Datei aus, indem der Zeitpunkt der letzten Änderung mit dem aktuellen Zeitpunkt verglichen wird. Löst eine Warnung aus, wenn die Datei die definierten Schwellenwerte für „Kritisch“ oder „Warnungsalter“ überschreitet. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	Common Checks – Dateialter überprüfen (Optionen) -F, --filepath FILEPATH: Absoluter Pfad zur zu überprüfenden Datei (erforderlich). -C, --Critical CRITICAL: Schwellenwert für kritisches Alter in Minuten für die Datei (erforderlich). -W, --warning WARNING: Warnungsaltersschwellenwert in Minuten für die Datei (erforderlich). **Anwendungsbeispiel:** Common Checks Check-file-age -f /path/	Allgemeine Prüfungen OK: Datei <Pfad zur Datei> Alter: 30 Minuten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			to/file.txt -c 120 -W 60	
Ereignis	Check-file-response-time	Vergleicht die Zeit, die zum Lesen einer angegebenen Datei benötigt wird, und vergleicht sie mit den Schwellenwerten „Kritisch“ und „Warnung“. Basierend auf diesem Vergleich gibt die Prüfung ein KRITISCHES oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	Common Checks – Dateiantwortzeit prüfen (Optionen) -F, --filepath FILEPATH: Absoluter Pfad zur zu überprüfenden Datei (erforderlich). -C, --Critical CRITICAL: Kritischer Schwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -W, --warning WARNING: Warnungsschwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -T, --TIMEOUT: Maximal zulässige Zeit zum Lesen des Dateiinhalts, angegeben in Sekunden. Der Zeitüberschreitungswert muss größer als der kritische Schwellenwert sein. **Anwendungsbeispiel:** Common Checks Check-file-response-time -f /var/log/servicenow/Agent-Client-	Allgemeine Prüfungen OK: Antwortzeit des Dateilesens: 0,0020 Sekunden für Dateiname: /Var/log/servicenow/Agent-Client-Collector/ACC.log.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Collector/acc.log -c 10 -W 5 -t 20	
Ereignis	Dateigröße überprüfen	Misst die Größe einer Datei (die tatsächliche Menge der darin enthaltenen Daten) und vergleicht sie mit den angegebenen Schwellenwerten. Gibt basierend auf dem Vergleich der Dateigröße und der Schwellenwerte ein KRITISCHES, WARNENDES oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	Common Checks – Dateigröße prüfen (Optionen) -F, --filepath FILEPATH absoluter Pfad zur erforderlichen Datei (erforderlich). -C, --kritisch. Kritischer Schwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 1000 für 1000 KB) (erforderlich) -W, --Warnung. Warnungsschwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 500 für 500 KB) (erforderlich) **Anwendungsbeispiel:** Common Checks Check-file-size -f C:\ProgramData\ServiceNow\Agent-Client-Collector\config\acc.yml	Allgemeine Prüfungen OK: Für Datei <Pfad zur Datei> Größe: 4,72 KB liegt innerhalb der Schwellenwerte
Ereignis	Dateibereich überprüfen	Misst die Größe einer Datei auf dem Datenträger anhand der angegebenen Schwellenwerte und gibt	Gemeinsame Prüfungen – Dateibereich prüfen (Optionen) -F, --filepath FILEPATH: Absoluter Pfad zur	Allgemeine Prüfungen OK: Datei <Pfad zur Datei> Speicherplatz: 8,00 KB liegt innerhalb des Schwellenwerts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		basierend auf den Schwellenwerten ein KRITISCHES, WARNENDES oder OK-Ereignis zurück. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	relevanten Datei (erforderlich). -C, --Critical CRITICAL: Kritischer Schwellenwert in Kilobyte. Wird als Zahl ohne Einheiten bereitgestellt (z. B. 1000 für 1000 KB) (erforderlich) -W, --warning WARNING: Warnungsschwellenwert in Kilobyte. Wird als Zahl ohne Einheiten bereitgestellt (z. B. 500 für 500 KB) (erforderlich) -B, --blocksize BLOCKSIZE: Blockgröße in Byte (Standard = 4096) (erforderlich) **Anwendungsbeispiel:** `Common Checks Check-file-space -f C:\ProgramData\ServiceNow\Agent-Client-Collector\config\acc.yml`	
Ereignis	os.linux.check-directory-size	Überprüft den Speicherplatz, der für das Verzeichnis eines Datenträgers zugewiesen ist, und vergleicht ihn mit den angegebenen kritischen Schwellenwerten	Linuxchecks Check-Directory-size (Optionen) -D, --dirpath DIRPATH: Absoluter Pfad zum zu prüfenden	Linux-Prüfungen KRITISCH: Verzeichnis <Pfad zur Datei> Größe: 500,00 KB überschreitet kritischen Schwellenwert 10,00 KB

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		und Warnungsschwellenwerten. **Hinweis:** Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	Verzeichnis (erforderlich). -C, --Critical CRITICAL: Schwellenwert für kritischen Speicherplatz in Kilobyte (erforderlich). -W, --warning WARNING: Warnungsschwellenwert für Datenträgerspeicher in Kilobyte (erforderlich). -T, --TIMEOUT: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** Linuxcheckt `Check-Directory-size -d path/to/Directory -c 100 -W 50 -t 30`	
Ereignis	os.linux.check-directory-space	Überprüft den Speicherplatz, der vom Verzeichnisinhalt belegt ist. Gibt ein KRITISCHES, WARNENDES oder OK-Ereignis basierend auf dem Vergleich mit den Schwellenwerten „Kritisch“ und „Warnung“ zurück.	Linuxchecks – Verzeichnisbereich überprüfen (Optionen) -D, --dirpath DIRPATH: Absoluter Pfad zum zu prüfenden Verzeichnis (erforderlich). -C, --Critical CRITICAL: Schwellenwert	Linux-Prüfungen KRITISCH: Verzeichnis <Pfad zur Datei> Speicherplatz: 374,00 KB überschreitet kritischen Schwellenwert 10,00 KB

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Hinweis: Der Service Desk-Mitarbeiter benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	für kritischen Speicherplatz in Kilobyte (erforderlich). -W, --warning WARNING: Warnungsschwellenwert für Datenträgerspeicher in Kilobyte (erforderlich). -T, --TIMEOUT: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** Linuxcheckt `Check-Directory-space -d /path/to/Directory -c 10 -W 5 -t 30`	

GlassFish – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die GlassFish-Systemüberwachung.

Richtlinie für GlassFish-Metriken

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	glassfish.metric-jvm-level	Ruft die JVM-Metriken des GlassFish-Servers ab. Erfordert Anmeldeinformation für die Standardauthentifiz	-i, --instance Glassfish Monitoring Instance Name (required) -p, --password Glassfish password -P, --port Glassfish API port	glassfish.jvm.garbage-collectors.Scavenge.CollectionCou 200 0 1652959788

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			--ssl Enable secure connnection to Glassfish -u –username Glassfish username Verwendungsbeispiel: metric-glassfish-jvm-level.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance}}	
Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetrik für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar. Erfordert Anmeldeinformation für die Standardauthentifiz	-i, --instance Glassfish Monitoring Instance Name (required) -p, --password Glassfish password -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username Verwendungsbeispiel: metric-glassfish-server-requests.rb -i {{.labels.params_glassfish_server_instance}} {{if .labels.params_port}} -P {{.labels.params_port}} {{end}}	glassfish.http-service.server.request.Count 200 0 1652959788
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server	-i, --instance Glassfish Monitoring Instance Name (required)	glassfish.resources. {{PoolName}}.AverageConnWaitTir 0 1652959936

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		bereitgestellten Ressourcen verfügbar. Erfordert Anmeldeinformation für die Standardauthentifiz	-P, --port Glassfish API port -r --resource_pool Resource Pool Name --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password Verwendungsbeispiel: metric-glassfish-server-resources.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} {{if .labels.params_resource_pool}} -r {{.labels.params_resource_pool}} {{end}} -i {{.labels.params_glassfish_server_instance}}	
Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden. Erfordert Anmeldeinformation für die Standardauthentifiz	-i, --instance Glassfish Monitoring Instance Name (required) -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password	Glassfish.transaction-service.ActiveCount 0 1652959977

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Verwendungsbeispiel: metric-glassfish-transaction-service.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance}}	
Metrik	glassfish.metrics-deployed-apps	Macht Metrikausgaben von Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden. Erfordert Anmeldeinformation für die Standardauthentifiz	-a, --apps Application deployed on Glassfish server (required) -i, --instance Glassfish Monitoring Instance Name (required) -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password Verwendungsbeispiel: metric-glassfish-deployed-applications.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -a {{.labels.params_deployed_apps}} -i {{.labels.params_glassfish_server_instance}}	glassfish.applications.{{Deployed Application}}.ActivatedSessionsTot 0 1652959665
Metrik	glassfish.metrics-deployment-lifecycle	Stellt Lebenszyklusmetrik der GlassFish-	metric-glassfish-deployment-lifecycle.rb (options)	glassfish.deployment.lifecycle.Acti 2 1653022649

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Serveranwendunge bereit. Erfordert Anmeldeinformatior für die Standardauthentifiz	-i, --instance Glassfish Monitoring Instance Name (required) -p --password Glassfish password -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username Verwendungsbeispiel: metric-glassfish-deployment-lifecycle.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance}}	

GlassFish-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von GlassFish-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

glassfish.metrics-deployed-apps – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.applications.{Deployed Application}.TotalServletsLoaded	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher geladenen Servlets.
glassfish.applications.{Deployed Application}.ServletProcessingTime	Deployed Application (Bereitgestellte Anwendung)	ms	Kumulative Servlet-Verarbeitungszeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metrics-deployed-apps – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.applications.{Deployed Application}.ActiveServletsLoaded	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der geladenen Servlets.
glassfish.applications.{Deployed Application}.ExpiredSessionsTotal (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher abgelaufenen Sitzungen.
glassfish.applications.{Deployed Application}.PassivatedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher passivierten Sitzungen.
glassfish.applications.{Deployed Application}.ActivatedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher aktivierten Sitzungen.
glassfish.applications.{Deployed Application}.SessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher erstellten Sitzungen.
glassfish.applications.{Deployed Application}.RejectedSessionsTotal (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher abgelehnten Sitzungen.
glassfish.applications.{Deployed Application}.PersistedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher bestehen bleibenden Sitzungen.
glassfish.applications.{Deployed Application}.ActiveSessions (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der aktiven Sitzungen.
glassfish.applications.{Deployed Application}.RequestCount	Deployed Application (Bereitgestellte Anwendung)	count	Kumulative Anzahl der bisher verarbeiteten Anforderungen
glassfish.applications.{Deployed Application}.MaxTime (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	ms	Längste Antwortzeit für eine Anforderung; kein kumulativer Wert, sondern die längste Antwortzeit unter den Antwortzeiten.
glassfish.applications.{Deployed Application}.ErrorCount (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Kumulativer Wert der Fehleranzahl. Dabei stellt die Fehleranzahl die Anzahl der Fälle dar, in denen der Antwortcode größer oder gleich 400 war.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metrics-deployed-apps – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.applications.{Deployed Application}.ProcessingTime	Deployed Application (Bereitgestellte Anwendung)	ms	Durchschnittliche Anforderungsverarbeitungsdauer.
glassfish.applications.{Deployed Application}.TotalJspCount	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher geladenen JSP-Seiten.
glassfish.applications.{Deployed Application}.JspCount	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der aktiven JSP-Seiten.
glassfish.applications.{Deployed Application}.JspErrorCount (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der durch Aufrufe von JSP-Seiten ausgelösten Fehler.
glassfish.applications.{Deployed Application}.JspReloadedCount	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der neu geladenen JSP-Seiten.

glassfish.metrics-deployment-lifecycle – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.deployment.lifecycle.ActiveApplicationsDeployed (empfohlene Metrik)		count	Gesamtanzahl der bisher bereitgestellten Anwendungen.
glassfish.deployment.lifecycle.TotalApplicationsDeployed (empfohlene Metrik)		count	Anzahl der bereitgestellten Anwendungen.

glassfish.metric-server-requests – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.http-service.server.request.Count	200	count	Anzahl der Antworten mit Statuscode 200.
glassfish.http-service.server.request.Count	2xx	count	Anzahl der Antworten mit einem Statuscode im Bereich 2xx.
glassfish.http-service.server.request.Count	302	count	Anzahl der Antworten mit Statuscode 302.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-requests – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.http-service.server.request.Count304		count	Anzahl der Antworten mit Statuscode 304.
glassfish.http-service.server.request.Count3xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 3xx.
glassfish.http-service.server.request.Count400		count	Anzahl der Antworten mit Statuscode 400.
glassfish.http-service.server.request.Count401		count	Anzahl der Antworten mit Statuscode 401.
glassfish.http-service.server.request.Count403		count	Anzahl der Antworten mit Statuscode 403.
glassfish.http-service.server.request.Count404		count	Anzahl der Antworten mit Statuscode 404.
glassfish.http-service.server.request.Count4xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 4xx.
glassfish.http-service.server.request.Count503		count	Anzahl der Antworten mit Statuscode 503.
glassfish.http-service.server.request.Count5xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 5xx.
glassfish.http-service.server.request.MaxTime		ms	Längste Antwortzeit für eine Anforderung; kein kumulativer Wert, sondern die längste Antwortzeit unter den Antwortzeiten.
glassfish.http-service.server.request.CountBytesReceived (empfohlene Metrik)		count	Anzahl der empfangenen Bytes.
glassfish.http-service.server.request.CountBytesTransmitted (empfohlene Metrik)		count	Anzahl der übertragenen Bytes.
glassfish.http-service.server.request.RequestCount (empfohlene Metrik)		count	Kumulative Anzahl der bisher verarbeiteten Anforderungen.
glassfish.http-service.server.request.CountOpenConnections		count	Anzahl der offenen Verbindungen.
glassfish.http-service.server.request.ProcessingTime (empfohlene Metrik)		ms	Durchschnittliche Anforderungsverarbeitungsdauer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-jvm-level – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.jvm.garbage-collectors.Scavenge.CollectionCount		count	Gesamtanzahl der aufgetretenen Sammlungen.
glassfish.jvm.garbage-collectors.Scavenge.CollectionTime		ms	Ungefähre verstrichene Erfassungszeit in Millisekunden.
glassfish.jvm.garbage-collectors.MarkSweepCompact.CollectionCount		count	Gesamtanzahl der aufgetretenen Sammlungen.
glassfish.jvm.garbage-collectors.MarkSweepCompact.CollectionTime		ms	Ungefähre verstrichene Erfassungszeit in Millisekunden.
glassfish.jvm.memory.CommittedHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die für die Verwendung durch die Java Virtual Machine festgeschrieben ist.
glassfish.jvm.memory.CommittedNonHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die für die Verwendung durch die Java Virtual Machine festgeschrieben ist.
glassfish.jvm.memory.InitHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die von der Java Virtual Machine anfänglich vom Betriebssystem für die Speicherverwaltung angefordert wird.
glassfish.jvm.memory.InitNonHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die von der Java Virtual Machine anfänglich vom Betriebssystem für die Speicherverwaltung angefordert wird.
glassfish.jvm.memory.MaxHeapSize (empfohlene Metrik)		Bytes	Maximale Arbeitsspeichermenge in Byte, die für die Speicherverwaltung verwendet werden kann.
glassfish.jvm.memory.MaxNonHeapSize		Bytes	Maximale Arbeitsspeichermenge in Byte, die für die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-jvm-level – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Speicherverwaltung verwendet werden kann.
glassfish.jvm.memory.ObjectPendingFinalizationCount		count	Ungefähre Anzahl von Objekten, für die die Finalisierung aussteht.
glassfish.jvm.memory.UsedHeapSize		Bytes	Menge des verwendeten Arbeitsspeichers in Byte.
glassfish.jvm.memory.UsedNonHeapSize		Bytes	Menge des verwendeten Arbeitsspeichers in Byte.

glassfish.metric-transaction-service – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.transaction-service.ActiveCount (empfohlene Metrik)		count	Gibt die Anzahl der derzeit aktiven Transaktionen an.
glassfish.transaction-service.CommittedCount (empfohlene Metrik)		count	Stellt die Anzahl der Transaktionen bereit, für die ein Commit ausgeführt wurde.
glassfish.transaction-service.RolledBackCount (empfohlene Metrik)		count	Stellt die Anzahl der Transaktionen bereit, für die ein Rollback ausgeführt wurde.

glassfish.metric-server-resources – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfis.resources.{PoolName}.AverageConnWaitTime	PoolName	ms	Durchschnittliche Dauer der Wartezeit pro erfolgreicher Verbindungsanforderung.
glassfis.resources.{PoolName}.ConnRequestWaitTime	PoolName	ms	Die längsten und kürzesten Wartezeiten von Verbindungsanforderungen. Der aktuelle Wert gibt die Wartezeit der letzten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-resources – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Anforderung an, die vom Pool verarbeitet wurde.
glassfis.resources.{PoolName}.NumConnAcquired	PoolName	count	Anzahl der aus dem Pool abgerufenen logischen Verbindungen.
glassfis.resources.{PoolName}.NumConnCreated	PoolName	count	Die Anzahl der physischen Verbindungen, die seit dem letzten Zurücksetzen erstellt wurden.
glassfis.resources.{PoolName}.NumConnDestroyed	PoolName	count	Anzahl der physischen Verbindungen, die seit dem letzten Zurücksetzen zerstört wurden.
glassfis.resources.{PoolName}.NumConnfailedValidation	PoolName	count	Die Gesamtanzahl der Verbindungen im Verbindungspool, bei denen die Validierung von der Startzeit bis zum Zeitpunkt der letzten Abtastung fehlgeschlagen ist.
glassfis.resources.{PoolName}.NumConnFree	PoolName	count	Die Gesamtanzahl der freien Verbindungen im Pool zum Zeitpunkt der letzten Abtastung.
glassfis.resources.{PoolName}.NumConnnotSuccessfullyMatched	PoolName	count	Anzahl der während des Abgleichs abgelehnten Verbindungen.
glassfis.resources.{PoolName}.NumConnReleased	PoolName	count	Anzahl der für den Pool freigegebenen logischen Verbindungen.
glassfis.resources.{PoolName}.NumConnSuccessfullyMatched	PoolName	count	Anzahl der erfolgreich abgeglichenen Verbindungen.
glassfis.resources.{PoolName}.NumConnTimedOut	PoolName	count	Die Gesamtanzahl der Verbindungen im Pool, bei denen zwischen der Startzeit und dem Zeitpunkt der letzten Abtastung eine Zeitüberschreitung aufgetreten ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-resources – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfis.resources.{PoolName}.NumConnUsed	PoolName	count	Stellt Statistiken zur Verbindungsnutzung bereit. Die Gesamtanzahl der derzeit verwendeten Verbindungen sowie Informationen zur maximalen Anzahl der Verbindungen, die verwendet wurden (die Obergrenzenmarkierung).
glassfis.resources.{PoolName}.NumPotentialConnLeak (empfohlene Metrik)	PoolName	count	Anzahl der potenziellen Verbindungsverluste.
glassfis.resources.{PoolName}.WaitQueueLength (empfohlene Metrik)	PoolName	count	Anzahl der Verbindungsanforderungen in der Warteschlange, die darauf warten, verarbeitet zu werden.

HAProxy – Standardprüfungen und Richtlinien

Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für bereit HAProxyÜberwachung.

HAProxy Ereignisrichtlinie

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Event	check-haproxy	Ruft die Details des ab HAProxy Lastenausgleichsmodul, um zu bestimmen, ob es ausgeführt wird.	commonchecks check-haproxy (options) -h host host -P port Port on which the HAProxy server is running -A all services all services -q Path on which HAProxy Stats URI is configured -use ssl ssl	CheckHAProxy OK: UP: 50% of 4 // services, DOWN: backend/nginx1[L4CON], backend/BACKEND

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy Ereignisrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
			Verwendungsbeispiel: `check-haproxy.rb -h localhost -P 8080 -A true -q stats -use_ssl false`	

HAProxy Metrikrichtlinie

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe

Metrik	metrics-check-haproxy	Ruft ab HAProxy Lastenausgleichsmodul-Metriken, um zu bestimmen, ob es ausgeführt wird.	`commonchecks metrics-check-haproxy (options)`
			`-q host Path on which HAProxy Stats URI is configured`
			`-P port Port on which the HAProxy server is running`
			`-c host host name`
			Verwendungsbeispiel:
			`metrics-check-haproxy.rb -q stats -P 8080 -c localhost`
				`<hostname>.haproxy.frontend.session_current 0 1652265603`
				`<hostname>.haproxy.frontend.session_total 0 1652265603`
				`<hostname>.haproxy.backend.session_current 0 1652265603`
				`<hostname>.haproxy.backend.session_total 1 1652265603`

HAProxy-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von HAProxy-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Front-End-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.frontend.session_current (empfohlene Metrik)		count	Die aktuelle Anzahl der Sitzungen, die zum Ausgeben von Anforderungen verwendet werden.
haproxy.frontend.session_total (empfohlene Metrik)		count	Gesamtanzahl der Sitzungen
haproxy.frontend.bytes_in (empfohlene Metrik)		count	Die Gesamtanzahl der Bytes, die der Server in der letzten Sekunde vom Client empfangen hat.
haproxy.frontend.bytes_out (empfohlene Metrik)		count	Die Gesamtanzahl der vom Server in der letzten Sekunde gesendeten Bytes.
haproxy.frontend.connection_errors (empfohlene Metrik)		count	Die Anzahl der Anforderungen, bei denen beim Versuch, eine Verbindung zu einem Server herzustellen, ein Fehler aufgetreten sind.
haproxy.frontend.warning_retries		count	Die Anzahl der erneuten Versuche, eine Verbindung mit einem Server herzustellen.
haproxy.frontend.warning_redispatched		count	Die Häufigkeit, mit der eine Anforderung an einen anderen Server weitergeleitet wurde.
haproxy.frontend.response_1xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 1xx
haproxy.frontend.response_2xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 2xx
haproxy.frontend.response_3xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 3xx
haproxy.frontend.response_4xx		count	HAProxy Gibt die Anzahl der Antworten nach

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Front-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			HTTP-Statuscode an – 4xx
haproxy.frontend.response_5xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 5xx
haproxy.frontend.response_other		count	HAProxy Gibt die Anzahl der Antworten von nicht-HTTP-Anwendungen an
haproxy.frontend.queue_time		count	Die durchschnittliche Warteschlangenzeit der letzten 1.024 Anforderungen.
haproxy.frontend.connect_time		count	Die durchschnittliche Verbindungszeit der letzten 1.024 Anforderungen.
haproxy.frontend.response_time (empfohlene Metrik)		count	Die Zeit der Antwort an den Client
haproxy.frontend.average_time (empfohlene Metrik)		count	Die durchschnittliche Zeit für die Sitzungen.

Back-End-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.backend.session_current (empfohlene Metrik)		count	Die aktuelle Anzahl der Sitzungen, die zum Ausgeben von Anforderungen verwendet werden.
haproxy.backend.session_total (empfohlene Metrik)		count	Gesamtanzahl der Sitzungen
haproxy.backend.bytes_in (empfohlene Metrik)		count	Die Gesamtanzahl der Bytes, die der Server in der letzten Sekunde vom Client empfangen hat.
haproxy.backend.bytes_out (empfohlene Metrik)		count	Die Gesamtanzahl der vom Server in der letzten Sekunde gesendeten Bytes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Back-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.backend.connection_errors (empfohlene Metrik)		count	Die Anzahl der Anforderungen, bei denen beim Versuch, eine Verbindung zu einem Server herzustellen, ein Fehler aufgetreten sind.
haproxy.backend.warning_retries		count	Die Anzahl der erneuten Versuche, eine Verbindung mit einem Server herzustellen.
haproxy.backend.warning_redispatched		count	Die Häufigkeit, mit der eine Anforderung an einen anderen Server weitergeleitet wurde.
haproxy.backend.response_1xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 1xx
haproxy.backend.response_2xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 2xx
haproxy.backend.response_3xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 3xx
haproxy.backend.response_4xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 4xx
haproxy.backend.response_5xx		count	HAProxy Gibt die Anzahl der Antworten nach HTTP-Statuscode an – 5xx
haproxy.backend.response_other		count	HAProxy Gibt die Anzahl der Antworten von nicht-HTTP-Anwendungen an
haproxy.backend.queue_time		count	Die durchschnittliche Warteschlangenzeit der letzten 1.024 Anforderungen.
haproxy.backend.connect_time		count	Die durchschnittliche Verbindungszeit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Back-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			der letzten 1.024 Anforderungen.
haproxy.backend.response_time (empfohlene Metrik)		count	Die Zeit der Antwort an den Client
haproxy.backend.average_time (empfohlene Metrik)		count	Die durchschnittliche Zeit für die Sitzungen.
haproxy.backend.num_up		count	

HTTP – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die HTTP-Systemüberwachung. Richtlinien enthalten die in den folgenden Tabellen angegebenen Prüfungen.

Richtlinie für HTTP-Einstiegspunktereignisse

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-http-follow-redirect	Überprüft, ob Umleitungslinks in einer festgelegten Anzahl von Anforderungen verfolgt werden können.	Nutzung Check-Head-redirect.rb (Optionen): • -A, --auth-first-only: Standardauthentifizierung nur bei der ersten Anforderung verwenden. • -aws-access-key-id: AWS-Zugriffsschlüssel. Legen Sie entweder die Variable ENV["AWS_ACCESS_KEY_ID"] fest, oder geben Sie diese als Option für den Agent an. • -r -aws-region: AWS-Region (Standardwert: us-east-1).	Check Head Redirect OK (Überprüfung Head Redirect OK)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• --aws-secret-access-key: Geheimer AWS-Zugriffsschlüssel. Legen Sie entweder die Variable ENV["AWS_SECRET_ACCESS_KEY"] fest, oder geben Sie diese als Option für den Agent an. • -R --redirect: Den ersten <N> Umleitungen folgen • -g --get-redirects: Den ersten <N> Umleitungen mit GET-Anforderungen folgen. • -s, --s3-config-bucket: S3-Konfigurations-Bucket zum Abrufen der Konfiguration. • -k, --s3-config-key: S3-Konfigurationsschlüssel zum Abrufen der Konfiguration. • -u, --url: Die URL muss in Monitoring HTTP Entrypoint/ cmdb_ci_endpoint_http_list.do für das CI aktualisiert werden.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Die Parameter Aws-region, aws-secret-key, aws-access-key, s3-config und s3-config-key sind nützlich, wenn Sie keine Verbindungsinformationen in anderen Prüfparametern konfigurieren möchten. Wenn über einen Bucket und einen Schlüssel auf die Umgebung zugegriffen wird, in der die Sensu-Prüfung ausgeführt wird, geben Sie einen AWS-Schlüssel und ein AWS-Token an. Von den Prüfungen wird dann die angegebene JSON-Datei aus S3 abgerufen und die JSON-Konfiguration mit der aktuellen Prüfungskonfiguration zusammengeführt. Verwendungsbeispiel: `command: check-head-redirect.rb -R 10 -u 'https://servicenow.com'`	
Event	util.check-http-response	Überprüft die URL-Antwortzeit und löst ein CRITICAL/WARNING-Ereignis aus, wenn die verstrichene Zeit die angegebenen CRITICAL/WARNING-	Verwendung: check-head-redirect.rb (Optionen) • -R, --redirect: Den ersten <N>	Check Head Redirect OK (Überprüfung Head Redirect OK)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Schwellenwerte überschreitet. Andernfalls wird ein Ereignis vom Typ OK ausgelöst.	Umleitungen folgen. • -w --timeout_warning: Den Schwellenwert für Zeitüberschreitung für „Warnung“ in Millisekunden festlegen. • -c --timeout_critical: Den Schwellenwert für Zeitüberschreitung für „kritisch“ in Millisekunden festlegen. • -u, --url: Die URL muss in Monitoring HTTP Entrypoint/cmdb_ci_endpoint_http_list.do für das CI aktualisiert werden. Verwendungsbeispiel: `command: check-head-redirect.rb -R 10 -u 'https://servicenow.com' -w 3000 -c 5000`	

Richtlinie für HTTP-Einstiegspunkt-Metriken

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	util.metrics-http-curl	Ruft Metriken auf HTTP-Endpunkten mit curl ab. Für diese Prüfung ist ein	Verwendung: • -a, --curl_args "CURL ARGS": Zusätzliche	Prüfung erfolgreich ausgeführt. Ausgabe:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunkt-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Proxy-Agent erforderlich.	an curl zu übergebende Argumente. • s, --scheme SCHEME: Metrikbenennungsschema, Text, der der Metrik angefügt werden soll (Standardwert: hostname). • -u, --url: Die URL muss in Monitoring HTTP Entrypoint/ cmdb_ci_endpoint.http_url für das CI aktualisiert werden. Verwendungsbeispiel: `metrics-curl.rb -u myURL.com -a -Lk`	ws10.curl_timings.time_total 0.219622 1642749209 ws10.curl_timings.time_namelook 0.149494 1642749209 ws10.curl_timings.time_connect 0.151103 1642749209 ws10.curl_timings.time_pretrans 0.168569 1642749209 ws10.curl_timings.time_redirect 0.095899 1642749209 ws10.curl_timings.time_starttran 0.219351 1642749209 ws10.curl_timings.http_code 200 1642749209

HTTP-Einstiegspunktmetriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von HTTP-Einstiegspunktprüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

HTTP-Einstiegspunktmetriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
http_code (empfohlene Metrik)			Statuscode der Anforderung.
time_total (empfohlene Metrik)		milliseconds	Gesamtdauer des Vorgangs.
time_namelookup (empfohlene Metrik)		seconds	Zeit zum Auflösen des Namens in der URL.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Einstiegspunktmetriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
time_connect (empfohlene Metrik)		seconds	Zeit zum Herstellen der Verbindung zum Remote-Host oder Proxy.
time_pretransfer (empfohlene Metrik)		seconds	Zeit zwischen Start und Beginn der Dateiübertragung. Enthält alle Befehle und Aushandlungen vor der Übertragung.
time_starttransfer (empfohlene Metrik)		seconds	Zeit zwischen Start und Übertragung des ersten Bytes. Enthält *time_pretransfer* und die Zeit, die der Server zur Berechnung des Ergebnisses verwendet hat.
time_redirect (empfohlene Metrik)		seconds	Zeit für alle Umleitungsschritte, einschließlich: • Namenssuche • connect • Vorabübertragung • Übertragung Zeigt die vollständige Ausführungszeit für mehrere Umleitungen an.

HTTP-Antwortcodeprüfung

Agent Client Collector bietet die folgende zusätzliche Prüfung für den HTTP-Antwortcode. Diese Prüfung ist keiner Richtlinie zugeordnet.

HTTP-Antwortcodeprüfung

Typ	Name	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-http-response-code	Löst ein kritisches Ereignis aus, wenn der URL-Antwortcode nicht mit dem regulären Ausdruck übereinstimmt.	-u, --url URL needs to be updated in the Monitoring HTTP Entrypoint/cmdb_ci_endpoint	CheckResponseCode OK : URL is in OK state (CheckResponseCode OK: URL ist im Status OK). HTTP Response code

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Antwortcodeprüfung (Fortsetzung)

Typ	Name	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Übergeben Sie die Anmeldeinformation (Benutzername und Passwort) mit sicheren Parametern.	_http_list.do for the CI -r, --response-code Regex string to match the response code. Otherwise, a critical event is raised. Default: 200 -f, --follow_redirects Follows redirect URLs Verwendungsbeispiel: command: check-response-code.rb -u 'https://servicenow.com' -r 2.. -f	is 200, matches regex (HTTP-Antwortcode ist 200, entspricht regulärem Ausdruck)

Internet Information Services (IIS) – Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von IIS-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
iis._Total.Web_Service(_Total).Current_Connections (empfohlene Metrik)		count	Gesamtanzahl der aktuellen Verbindungen mit IIS.
iis._Total.Web_Service(_Total).Total_Get_Requests (empfohlene Metrik)		count	Gesamtanzahl der vom IIS-Server empfangenen HTTP-GET-Anforderungen.
iis._Total.Web_Service(_Total).Total_Post_Requests (empfohlene Metrik)		count	Gesamtanzahl der vom IIS-Server empfangenen HTTP-POST-Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
iis._Total.Web_Service(_Total).Get_Requests/sec (empfohlene Metrik)		Anzahl pro Sekunde	Rate aller vom IIS-Server empfangenen HTTP-GET-Anforderungen.
iis._Total.Web_Service(_Total).Post_Requests/sec (empfohlene Metrik)		Anzahl pro Sekunde	Rate aller vom IIS-Server empfangenen HTTP-POST-Anforderungen.

Linux – Standardprüfungen und Richtlinien

Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für bereit Linux Metrikü berwachung.

Prüfungen von Linux-Überwachungsmetriken

Linux-Metrikrichtlinie

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
os.linux.metrics-process-usage	proc.acc.running	Prozessname	Anzahl der Prozesse, die mit diesem Namen ausgeführt werden (gemäß)	count		
	proc.acc.cpuPercent	Prozessname	Prozentsatz der vom Prozess beanspruchten cpu.	Prozent		
	Proc.ACC.MPercent	Prozessname	Prozentsatz des vom Prozess belegten Arbeitsspeichers.	Prozent		
os.linux.metrics-reboot-count-today	reboot.count.today	Leer	Anzahl der heute durchgeführten Neustarts	count		
os.linux.metrics-system-cpu	cpu.total.user	gesamt	Normale Prozesse, die im Anwendermodus ausgeführt werden; cpu.total.user ist die	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Summe der cpuN.user Metriken.			
	cpu.total.nice	gesamt	Niced-Prozesse, die im Anwendermodus ausgeführt werden; cpu.total.nice ist die Summe der cpuN.nice-Metriken.	count		
	cpu.total.system	gesamt	Zeit, die die CPU für die Ausführung des Kernel aufgewendet hat; cpu.total.System ist die Summe der cpuN.System-Metriken.	Sek		
	cpu.total.idle	gesamt	Gesamtzeit, die die CPU in einem Leerlaufstatus verbracht hat.; cpu.total.idle ist die Summe der cpuN.idle-Metriken.	Sek		
	cpu.total.iowait	gesamt	Gesamtzeit, die die CPU auf den Abschluss von E/A-Vorgängen gewartet hat.; cpu.total.iowait ist die Gesamtzahl der	Sek		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			cpuN.iowait-Metriken.			
	cpu.total.irq	gesamt	Gesamtzeit, die der Prozessor für die Verarbeitung von Interrupts aufwendet.; cpu.total.irq ist die Summe der cpuN.irq-Metriken.	Sek		
	cpu.total.softirq	gesamt	Zeit, die für die Bearbeitung von Soft-Interrupt-Anforderungen aufgewendet wurde; cpu.total.softirq ist die Summe der cpuN.softirq-Metriken.	Sek		
	cpu.total.steal	gesamt	Gesamtzeit, die die virtuelle CPU auf die Wartung einer anderen virtuellen CPU durch den Hypervisor gewartet hat. Gilt nur für virtuelle Computer.	Sek		
	cpu.total.guest	gesamt	Gesamtzeit, die von der CPU für die Ausführung des virtuellen	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Prozessors aufgewendet wurde. Gilt nur für Hypervisoren.			
	cpu.total.guest_nice	gesamt	Gesamtzeit, die die CPU als gutes Gast-BS ausgeführt hat. cpu.total.guset_nice si die Summe der cpuN.Guest_nice-Metriken	Sek		
	cpu.<cpu-core>.user	cpu-core	Zeit, die für die Verarbeitung mit normaler Priorität im Benutzermodus aufgewendet wurde.	Sek		
	cpu.<cpu-core>.nice	cpu-core	Zeit, die im Anwendermodus mit abgeschlossenen Prozessen verbracht wurde.	Sek		
	cpu.<cpu-core>.system	cpu-core	Zeitaufwand für die Ausführung im Kernel-Modus.	Sek		
	cpu.<cpu-core>.idle	cpu-core	Zeit, die in den Ferien verbracht wurde, mit Daumen.	Sek		
	cpu.<cpu-core>.iowait	cpu-core	Wartezeit auf Abschluss der E/A. Dies wird auch als	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Leerlaufzeit betrachtet.			
	cpu.<cpu-core>.irq	cpu-core	Zeit, die für die Verarbeitung von Hardware-Interrupts aufgewendet wurde.	Sek		
	cpu.<cpu-core>.softirq	cpu-core	Zeit, die für die Verarbeitung von Software-Interrupts aufgewendet wurde.	Sek		
	cpu.<cpu-core>.steal	cpu-core	Zeit, die von anderen Betriebssystemen vereinnahmt wurde, die in einer virtuellen Umgebung ausgeführt wurden.	Sek		
	cpu.<cpu-core>.guest	cpu-core	Zeit, die für die Ausführung einer virtuellen CPU oder eines Gast-BS unter der Kontrolle des Kernel aufgewendet wurde.	Sek		
	cpu.<cpu-core>.guest_nice	cpu-core	Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			aufgewendet wurde.			
	cpu.intr	Leer	Seit Startzeit verarbeitete Interrupts.	Sek		
	cpu.ctxt	Leer	Gesamtanzahl der Kontextwechsel über alle CPUs hinweg.	count		
	cpu.btime	Leer	Die Zeit, zu der das System gestartet wurde	Sek		
	cpu.processes	Leer	Anzahl der erstellten Prozesse und Threads, einschließlich jener (aber nicht beschränkt auf jene), die durch Aufrufe der Systemaufrufe fork() und clone() erstellt wurden.	count		
	cpu.procs_running	Leer	Gesamtanzahl der Prozesse, die auf allen CPUs ausgeführt werden.	count		
	cpu.procs_blocked	Leer	Die Anzahl der derzeit blockierten Prozesse, die auf den Abschluss			

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			der E/A warten.			
	cpu.cpu_count	Leer	Anzahl der cpu im System	count		
	cpu.<cpu-core>.cores	cpu-core	Die Anzahl der CPU-Kerne	Anzahl der Kerne		
os.linux.metrics-system-cpu-load	load_avg.one	Leer	Durchschnittliche Systemauslastung über eine Minute.	Thread-Anzahl	Ja	Ja
	Load_avg.five	Leer	Durchschnittliche Systemauslastung über fünf Minuten.	Thread-Anzahl	Ja	Ja
	Load_avg.fünfzehn	Leer	Durchschnittliche Systemauslastung über 15 Minuten.	Thread-Anzahl	Ja	Ja
	load_avg.norm.one	Leer	Durchschnittliche Systemauslastung über eine Minute, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
	load_avg.norm.five	Leer	Durchschnittliche Systemauslastung über fünf Minuten, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
	load_avg.norm.fifteen	Leer	Durchschnittliche Systemauslastung über 15 Minuten, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
os.linux.metrics-system-cpu-percentage	cpu.avgutilization_ Prozentsatz	Leer	Prozentsatz der cpu wurde	Prozent		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			durchschnittlich verwendet			
	cpu.user_Prozent	Leer	Prozentsatz der Zeit, in der die gesamte cpu von normalen Prozessen im Anwendermodus verwendet wurde	Prozent	Ja	Ja
	cpu.nice_-Prozentsatz	Leer	Prozentsatz der Zeit, die alle cpus von abgeglichenen Prozessen im Anwendermodus verwendet werden	Prozent	Ja	Ja
	cpu.System_ Prozentsatz	Leer	Der Prozentsatz der Zeit, die die CPU für die Ausführung des Kernels aufgewendet hat.	Prozent	Ja	Ja
	cpu.idle_percentage	Leer	Prozentsatz der Zeit, die alle cpus inaktiv waren	Prozent	Ja	Ja
	cpu.iowait_-Prozentsatz	Leer	Prozentsatz der Zeit, die alle cpus warten, bis E/A abgeschlossen ist	Prozent	Ja	Ja
	cpu.irq_percentage	Leer	Prozentsatz der Zeit, die alle cpus unterbrechen	Prozent	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.softirq_-Prozentsatz	Leer	Prozentsatz der Zeit, die alle cpus Softwareunterbrechungen bedienen	Prozent	Ja	Ja
	cpu.Steal_Prozentsatz	Leer	Prozentsatz der Zeit, die alle cpus für Betriebssysteme virtueller Hosts gewartet haben	Prozent	Ja	Ja
	cpu.Guest_Prozentsatz	Leer	Prozentsatz der Zeit, die alle cpus gewartet haben, als Gastbetriebssystem	Prozent	Ja	Ja
os.linux.metrics.system-disk	Datenträger.<disk-name>.Lesevorgänge	Datenträgername	Gesamtanzahl der erfolgreich abgeschlossenen Lesevorgänge.	count	Ja	Ja
	disk.<disk-name>.readsMerged	Datenträgername	Gesamtanzahl der zusammengeführten Lesezugriffe	count		
	disk.<disk-name>.sectorsRead	Datenträgername	Gesamtanzahl der erfolgreich gelesenen Sektoren.	count		
	disk.<disk-name>.readTime	Datenträgername	Gesamtanzahl an Millisekunden, die für alle Lesevorgänge aufgewendet wurden.	Millisek		
	Datenträger.<disk-name>.Schreibvorgänge	Datenträgername	Gesamtanzahl der erfolgreich abgeschlossenen Schreibvorgänge.	count	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	disk.<disk-name>.writesMerged	Datenträgernam	Gesamtanzahl der zusammengeführten Schreibvorgänge	count		
	disk.<disk-name>.sectorsWritten	Datenträgernam	Gesamtanzahl der erfolgreich geschriebenen Sektoren.	count		
	disk.<disk-name>.writeTime	Datenträgernam	Gesamtanzahl an Millisekunden, die für alle Schreibvorgänge aufgewendet wurden.	Sonstige Sek		
	disk.<disk-name>.ioInProgress	Datenträgernam	Gesamtzahl der derzeit in Bearbeitung befindlichen E/A-Vorgänge	count		
	Disk.<disk-name>.ioTime		Gesamtzeit, die für E/A-Vorgänge aufgewendet wurde	Millisek	Ja	Ja
	disk.<disk-name>.ioTimeWeighted	Datenträgernam	Gesamtzeit, die für E/A-Vorgänge aufgewendet wurde. Dies kann eine einfache Messung sowohl der E/A-Abschlusszeit als auch des Backlogs bieten, der sich ansammelt.	Millisek		
os.linux.metrics.system-disk-capacity	disk.<file-system-name>.total	Dateisystemnam	Gesamtgröße des Dateisystems.	Byte		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	disk.<file-system-name>.used	Dateisystemname	Gesamtmenge des Speicherplatzes, der vorhandenen Dateien im Dateisystem zugewiesen ist.	Byte		
	disk.<file-system-name>.avail	Dateisystemname	Gesamtmenge des im Dateisystem verfügbaren Speicherplatzes.	Byte		
	disk.<file-system-name>.used_percentage	Dateisystemname	Der Prozentsatz des verfügbaren Speicherplatzes, der derzeit allen Dateien im Dateisystem zugewiesen ist.	Prozent		
	disk.<file-system-name>.itotal	Dateisystemname	Die Gesamtzahl der Inodes im Dateisystem.	count		
	disk.<file-system-name>.iused	Dateisystemname	Die Anzahl der verwendeten Inodes.	count		
	disk.<file-system-name>.iavail	Dateisystemname	Die Anzahl der freien (nicht verwendeten) Inodes.	count		
	disk.<file-system-name>.iused_percentage	Dateisystemname	Der Prozentsatz der verwendeten Inodes.	Prozent		
os.linux.metrics.system-disk-usage	disk_usage.<disk>.total	Datenträgername	Gesamtmenge des verfügbaren Speicherplatzes	Bytes		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			auf diesem Datenträger			
	disk_usage.<disk>.used	Datenträgernam	Gesamtmenge des auf diesem Datenträger verwendeten Speicherplatzes	Bytes		
	disk_usage.<disk>.avail	Datenträgernam	Gesamtmenge des verfügbaren Speicherplatzes auf diesem Datenträger	Bytes		
	Disk_usage.<disk>.used_Prozentsatz	Datenträgernam	Der Prozentsatz des auf diesem Datenträger verwendeten Speicherplatzes	Prozent	Ja	Ja
os.linux.metrics-System-Memoryos.linux.metrics-System-Memory-percent	memory.total	Leer	Insgesamt nutzbarer RAM.	KB		
	memory.free	Leer	Insgesamt freier RAM.	KB		
	memory.available	Leer	Eine Schätzung, wie viel Arbeitsspeicher zum Starten neuer Anwendungen ohne Austausch verfügbar ist.	KB		
	memory.buffers	Leer	Temporärer Speicher, der für Rohdatenträger-Blöcke verwendet wird.	KB		
	memory.cached	Leer	In-Memory Cache	KB		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			für vom Datenträger gelesene Dateien (Seiten-Cache). Enthält nicht „mem_swapcached“.			
	Arbeitsspeicher.swapTotal	Leer	Insgesamt verfügbarer Auslagerungsbereich (Swap Space).	KB	Ja	Ja
	Arbeitsspeicher.tauschfrei	Leer	Derzeit nicht genutzter Auslagerungsbereich.		Ja	Ja
	memory.dirty	Leer	Arbeitsspeicher, der wartet, um auf den Datenträger zurückgeschrieben zu werden.	KB		
	Arbeitsspeicher.swapUsed	Leer	Menge des verwendeten Auslagerungsbereichs.	KB	Ja	Ja
	memory.used	Leer	Menge des verwendeten RAM.	KB		
	Arbeitsspeicher. Used WOBuffersCaches	Leer	Menge des verwendeten Arbeitsspeichers.	KB		
	Arbeitsspeicher. FreeWOBuffersCaches	Leer	Wert von „Memory Available“ aus /proc/ meminfo, falls vorhanden, fällt jedoch auf das Hinzufügen von freiem + gepuffertem + zwischengespeichertem	KB		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Arbeitsspeicher zurück, wenn nicht.			
	Arbeitsspeicher. SwapUsedPercentage	Leer	Prozentsatz des verwendeten Auslagerungsbereichs.	Prozent		
	Memory_percent. Kostenlos	Leer	Prozentsatz des freien RAM	Prozent	Ja	Ja
	Memory_percent. Verfügbar	Leer	Prozentsatz des verfügbaren Arbeitsspeichers	Prozent	Ja	Ja
	Memory_percent. Puffer	Leer	Prozentsatz des Arbeitsspeichers, der für Rohdatenträger-Blöcke verwendet wird	Prozent	Ja	Ja
	Memory_percent. Zwischengespeichert	Leer	Prozentsatz des Arbeitsspeichers, der für den speicherinternen Cache für vom Datenträger gelesene Dateien verwendet wird	Prozent	Ja	Ja
	Memory_percent. Fehlerhaft	Leer	Prozentsatz des Arbeitsspeichers, der auf den Zurückschreiben auf den Datenträger wartet.	Prozent	Ja	Ja
	Memory_percent. Tauschverwendet	Leer	Prozentsatz des verwendeten Auslagerungsbereichs.	Prozent	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	Memory_percent. Used WOBuffersCaches	Leer	Prozentsatz des Arbeitsspeichers wird verwendet	Prozent	Ja	Ja
	Memory_percent. FreeWOBuffersCaches	Leer	Prozentsatz des verfügbaren Arbeitsspeichers	Prozent	Ja	Ja
os.linux.metrics Systembetriebszeit	system.uptime(sec)	Leer	Zeit, während der das System funktioniert und verfügbar ist.	Sek		
os.linux.metrics Memory-vmstat	vmstat.nr_free_pages	Leer	Seiten, die derzeit vom System nicht verwendet werden.	Seiten		
	Vmstat.nr_alloc_Batch	Leer	Seiten, die anderen Domänen zugewiesen sind, da in jeder Domäne jedes NUMA nicht genügend Arbeitsspeicher vorhanden ist	Seiten		
	Vmstat.nr_inactive_anon	Leer	Arbeitsspeicherseiten in jeder Domäne jedes NUMA-Knotens, auf die seit langem nicht zugegriffen wurde	Seiten		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	Vmstat.nr_Active_anon	Leer	Anonyme Seiten des virtuellen Arbeitsspeichers, die kürzlich verwendet wurden	KB		
	Datei „vmstat.nr_inactive_“	Leer	Die Arbeitsspeicherseite, die der Datei entspricht, auf die in jeder Domäne jedes NUMA lange nicht zugegriffen wurde.	KB		
	Datei „vmstat.nr_Active_“	Leer	Die Arbeitsspeicherseite, die der Datei entspricht, auf die kürzlich zugegriffen wurde.	Seiten		
	Vmstat.nr_nicht bedienbar	Leer	Die Anzahl der Seiten befindet sich in der nicht bedienbaren (nicht-)LRU-Liste	count		
	Vmstat.nr_mlock	Leer	Seiten, die einer VM_LOCKED-VMA zugeordnet sind – sind eine Klasse von unbrauchbaren Seiten.	Seiten		
	Vmstat.nr_anon_Seiten	Leer	Dem Arbeitsspeicher	Seiten		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			zugeordnete Seiten, die nicht Teil einer Datei sind.			
	Vmstat.nr_zugeordnet	Leer	Anzahl der zugeordneten Speicherseiten.	count		
	Vmstat.nr_file_Seiten	Leer				
	Vmstat.nr_fehlerhaft	Leer	Seiten, die darauf warten, auf den Datenträger geschrieben zu werden	Seiten		
	Vmstat.nr_ Zurückschreiben	Leer	Seiten, die derzeit auf den Datenträger geschrieben werden	Seiten		
	Vmstat.nr_slab_ zurückforderbar	Leer	Seiten aus der Kernel-SLAB-Arbeitsspeichernutzung, die zurückgefordert werden können	Seiten		
	Vmstat.nr_slab_nicht zurückforderbar	Leer	Seiten aus der Kernel-SLAB-Arbeitsspeichernutzung, die nicht zurückgefordert werden können	Seiten		
	Vmstat.nr_page_table_ pages	Leer	Seiten, die Seitentabellen zugeordnet sind	Seiten		
	Vmstat.nr_Kernel_-Stapel	Leer	Arbeitsspeicherm die Kernel-Stapeln zugeteilt ist.	KBenge,		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.nr_unstable	Leer	Die Anzahl der instabilen Seiten in jeder Domäne jedes NUMA-Knotens	count		
	vmstat.nr_bounce	Leer				
	Vmstat.nr_vmscan_ schreiben	Leer	Die Anzahl der fehlerhaften Seiten, die während eines Scans von LRU(s) zurückgeschrieben wurden	count		
	Vmstat.nr_vmscan_ immediate_reclaim	Leer				
	Vmstat.Nr_writeback_ Temp	Leer				
	Vmstat.nr_isolated_anon	Leer	Die Anzahl der anonymen Speicherseiten, die in jeder Domäne jedes NUMA-Knotens isoliert sind	count		
	Vmstat.nr_isolated_file	Leer	Die Anzahl der Seiten von Dateispeicherseiten, die in jeder Domäne jedes NUMA-Knotens isoliert sind	count		
	vmstat.nr_shmem	Leer	Die Anzahl der Seiten mit	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			freigegebenem Arbeitsspeicher			
	vmstat.nr_dirtied	Leer	Die Anzahl der fehlerhaften Seiten in jeder Domäne jedes NUMA-Knotens	count		
	vmstat.nr_written	Leer				
	vmstat.numa_hit	Leer	Anzahl der Seiten, die diesem Knoten erfolgreich zugeordnet wurden.	count		
	vmstat.numa_miss	Leer	Die Anzahl der Seiten, die auf diesem Knoten aufgrund von wenig Arbeitsspeicher auf dem beabsichtigten Knoten zugewiesen wurden.	count		
	Vmstat.numa_fremd	Leer	Die Anzahl der ursprünglich für diesen Knoten vorgesehenen Seiten, die stattdessen einem anderen Knoten zugewiesen wurden.	count		
	Vmstat.numa_Interleave	Leer	Anzahl der Seiten, die gemäß	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Interleave-Richtlinie erfolgreich diesem Knoten zugeordnet wurden.			
	vmstat.numa_local	Leer	Die Anzahl der Seiten, die diesem Knoten durch einen Prozess auf diesem Knoten erfolgreich zugewiesen wurden	count		
	vmstat.numa_other	Leer	Die Anzahl der Seiten, die diesem Knoten durch einen Prozess auf einem anderen Knoten zugewiesen wurden.	count		
	Vmstat.workingset_refault	Leer				
	Vmstat.workingset_aktivieren	Leer				
	Vmstat.workingset_nodereclaim	Leer				
	Vmstat.nr_anon_transparent_hugepages	Leer				
	vmstat.nr_free_cma	Leer	Freie Seiten für kontinuierliche Arbeitsspeicherzuteilung in jeder Domäne jedes NUMA			
	Vmstat.nr_dirty_-Schwellenwert	Leer				

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	Vmstat.nr_dirty_background_threshold	Leer				
	vmstat.pgpgin	Leer	Die Anzahl der vom Datenträger eingeführten Seiten	count		
	vmstat.pgpgout	Leer	Die Anzahl der auf den Datenträger geschriebenen Seiten	count		
	vmstat.pswpin	Leer	Die Anzahl der Seiten, die aus dem Tausch-Bereich eingebracht werden	count		
	vmstat.pswpout	Leer	Die Anzahl der Seiten, die in den Tausch-Bereich getauscht wurden	count		
	vmstat.pgalloc_dma	Leer				
	Vmstat.pgalloc_dma32	Leer				
	Vmstat.pgalloc_normal	Leer				
	Vmstat.pgalloc_movable	Leer				
	vmstat.pgfree	Leer	Die Anzahl der Seiten, die seit dem letzten Start frei sind	count		
	Vmstat.pgactivat	Leer	Anzahl der Seitenaktivierungen seit dem letzten Start	count		
	vmstat.pgdeactivate	Leer	Anzahl der Seitendeaktivierungen seit dem letzten Start	count		
	vmstat.pgfault	Leer	Geringfügige Fehler seit	Seiten		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			dem letzten Start			
	vmstat.pgmajfault	Leer	Schwerwiegende Fehler seit dem letzten Start	Seiten		
	vmstat.pglazyfreed	Leer				
	vmstat.pgrefill_dma	Leer				
	vmstat.pgrefill_dma32	Leer				
	vmstat.pgrefill_normal	Leer	Anzahl der Neufüllungen der Seite seit dem letzten Start	count		
	Vmstat.pgrefill_movable	Leer				
	Vmstat.pgsteal_ kswapd_dma	Leer				
	Vmstat.pgsteal_ kswapd_dma32	Leer				
	Vmstat.pgsteal_ kswapd_normal	Leer				
	Vmstat.pgsteal_ kswapd_movable	Leer				
	Vmstat.pgsteal_ direct_dma	Leer				
	Vmstat.pgsteal_ direct_dma32	Leer				
	Vmstat.pgsteal_ direct_normal	Leer				
	Vmstat.pgsteal_ direct_movable	Leer				
	Vmstat.pgscan_ kswapd_dma	Leer				
	Vmstat.pgscan_ kswapd_dma32	Leer				
	Vmstat.pgscan_ kswapd_normal	Leer	Anzahl der Seiten, die seit dem Start von kswapd gescannt wurden	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	Vmstat.pgscan_ kswapd_movable	Leer				
	Vmstat.pgscan_ direct_dma	Leer				
	Vmstat.pgscan_ direct_dma32	Leer				
	Vmstat.pgscan_ direct_normal	Leer	Anzahl der seit dem Start zurückgeforderten Seiten	count		
	Vmstat.pgscan_ direct_movable	Leer				
	Vmstat.pgscan_ direct_Throttle	Leer				
	Vmstat.Zone_ reclaim_failed	Leer				
	vmstat.pginodesteal	Leer				
	vmstat.slabs_scanned	Leer				
	Vmstat.kswapd_ inodesteal	Leer				
	Vmstat.kswapd_low_ wmark_hit_schnell	Leer				
	Vmstat.kswapd_High_ wmark_Hit_schnell	Leer				
	vmstat.pageoutrun	Leer	Anzahl der Aufrufe von kswapd-Seiten-Reklamationen	count		
	vmstat.allocstall	Leer	Anzahl der Male, mit denen die Seitenrückforderung direkt aufgerufen wurde (wenig Arbeitsspeicher)	count		
	vmstat.pgrotated	Leer				
	Vmstat.Drop_pagecache	Leer				
	Vmstat.Drop_SLAB	Leer				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	Vmstat.numa_pte_-Updates	Leer				
	Vmstat.numa_huge_pte_Updates	Leer				
	Vmstat.numa_HINT_Faults	Leer				
	Vmstat.numa_Hint_Faults_local	Leer				
	Vmstat.numa_pages_migriert	Leer				
	Vmstat.pgmigrate_Erfolg	Leer				
	vmstat.pgmigrate_fail	Leer				
	vmstat.compact_Migrate_Scanned	Leer				
	vmstat.compact_Free_Scanned	Leer				
	vmstat.compact_isoliert	Leer				
	vmstat.compact_Stoppen	Leer	Die Anzahl, mit der ein Prozess angehalten wird, um die Speicherkomprimierung auszuführen, damit eine große Seite frei verwendet werden kann.	count		
	vmstat.compact_fail	Leer	Die Anzahl der Versuche des Systems, den Arbeitsspeicher zu komprimieren, aber fehlgeschlagen.	count		
	vmstat.compact_Erfolg	Leer	Häufigkeit, mit der vom System	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Arbeitsspeicher komprimiert und eine große Seite zur Verwendung freigegeben wurde.			
	Vmstat.htlb_Buddy_alloc_success	Leer				
	Vmstat.htlb_Buddy_alloc_fail	Leer				
	Vmstat.unevictable_pgs_culled	Leer				
	Vmstat.unevictable_pgs_scanned	Leer				
	Vmstat.unevictable_pgs_rescued	Leer				
	Vmstat.unevictable_pgs_mlocked	Leer				
	Vmstat.unevictable_pgs_munlocked	Leer				
	Vmstat.unevictable_pgs_cleared	Leer				
	Vmstat.unevictable_pgs_stranded	Leer				
	vmstat.thp_fault_alloc	Leer	Die Anzahl der großen Seiten wurde erfolgreich zugewiesen, um einen Seitenfehler zu behandeln.	count		
	Vmstat.thp_fault_Fallback	Leer	Die Anzahl der Seitenfehler kann keine große Seite zuteilen, sondern greift stattdessen auf die	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Verwendung kleiner Seiten zurück.			
	vmstat.thp_collapse_alloc	Leer	Die Anzahl der Reduzierungen eines Bereichs von Seiten auf eine große Seite und der erfolgreichen Zuordnung einer neuen großen Seite zum Speichern der Daten.	count		
	Vmstat.thp_collapse_ alloc_failed	Leer	Die Anzahl der Reduzierungen eines Bereichs von Seiten auf eine große Seite, die Zuordnung ist jedoch fehlgeschlagen.	count		
	vmstat.thp_split	Leer	Die Anzahl der Aufteilung einer großen Seite in Basisseiten	count		
	Vmstat.thp_Zero_ page_alloc	Leer	Die Anzahl der erfolgreichen Zuteilungen der Seite „sehr Null“	count		
	Vmstat.thp_Zero_ page_alloc_failed	Leer	Die Anzahl der Fälle, in denen der Kernel	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			eine riesige Null-Seite nicht zugewiesen hat und auf die Verwendung kleiner Seiten zurückgreift.			
	vmstat.balloon_inflate	Leer				
	Vmstat.Ballon_abblasen	Leer				
	Vmstat.Balloon_ migrieren	Leer				
os.linux.metrics-process-status	proc.<process>.VmSize	Prozessname	Die Gesamtmenge des vom Prozess verwendeten virtuellen Arbeitsspeichers	KB		
	proc.<process>.VmRSS	Prozessname	Der nicht vertauschte physische Arbeitsspeicher, den ein Prozess verwendet hat	KB		
	proc.<process>.VmSwap	Prozessname	Gesamtmenge des verwendeten Auslagerungsbereichs.	KB		

Linux-Netzwerküberwachungsprüfungen

Hinweis: Fügen Sie beim Upgrade von einer früheren Version die Prüfungen in dieser Tabelle manuell der Linux-Metrikrichtlinie hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbe	Erfasste Metriken	Empfohlene Metrik
Metrik	os.linux.metrics-Network-Interface	Ruft alle Netzwerkschnittstellen bezogenen Metriken für Linux-Server ab.	Verwendung: • -X, excludeinterface: Liste der auszuschließenden Schnittstellen (kommagetrennt) • -i, includeinterface: Liste der einzuschließenden Schnittstellen (kommagetrennt) • -I, includeinterfaceregex: Regulärer Ausdruck, der den einzuschließenden Schnittstellen entspricht • -X, excludeinterfaceregex: Regulärer Ausdruck, der den auszuschließenden Schnittstellen entspricht Anwendungsbeispiel: Befehl: Metrics-Network-Interface.rb	• RxBytes (empfohlene Metrik) • RxPackets (empfohlene Metrik) • RxFehler • RxDrops (empfohlene Metrik) • RxFifo • RxFrame • RxCompressed • RxMulticast • RxBytes (empfohlene Metrik) • RxPackets (empfohlene Metrik) • RxFehler • RxDrops (empfohlene Metrik) • RxFifo • RxColls • RxCarrier • RxCompressed	Ja
Metrik	os.linux.metrics-netstat-tcp	Ruft Metriken für TCP-Socket-status aus netstat ab. Nützlich auf Web- oder Proxy-Servern mit hohem Datenverkehr mit einer großen Anzahl von kurzlebigen TCP-	Verwendung: • -P, Port: Der Port, von dem Sie Metriken empfangen möchten. Wertbereich = 1–65535.	• tcp.UNBEKANNT • tcp.EINGERICHTET • tcp.SYN_SENT • tcp.SYN_RECV • tcp.FIN_WAIT1 • tcp.FIN_WAIT2 • tcp.TIME_WAIT • tcp.SCHLIESSEN	nein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbe	Erfasste Metriken	Empfohlene Metrik
		Verbindungen, die kommen und gehen.	• -T, Typ: Der Porttyp, von dem Metriken empfangen werden sollen. Werte = lokal oder Remote. Standard = lokal • -D, disabletcp6: Deaktiviert die tcp6-Prüfung. Geben Sie einen Wert ein, um disabletcp6 = wahr festzulegen. Anwendungsbeispiel: Metriken-netstat-tcp.rb	• tcp.CLOSE_WAIT • tcp.LAST_ACK • tcp.LISTEN • tcp.WIRD GESCHLOSSEN	

Linux-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Linux-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

os.linux.metrics-process-usage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
proc.acc.running			Anzahl der Prozesse, die mit diesem Namen ausgeführt werden (acc).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-process-usage – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
proc.acc.cpuPercent			Prozentsatz der vom Prozess beanspruchten CPU.
proc.acc.memPercent			Prozentsatz des vom Prozess belegten Arbeitsspeichers.

os.linux.metrics-reboot-count-today – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
reboot.count.today			Anzahl der Neustarts heute.

os.linux.metrics-system-cpu – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.total.user			Prozesse mit normaler Priorität, die im Benutzermodus ausgeführt werden; *cpu.total.user* ist die Summe der *cpuN.user*-Metriken.
cpu.total.nice			Niced-Prozesse, die im Anwendermodus ausgeführt werden; *cpu.total.nice*Ist die Summe von *cpuN.nice*Metriken.
cpu.total.system			Zeit, die die CPU für die Ausführung des Kernels aufgewendet hat; *cpu.total.system* ist die Summe der *cpuN.system*-Metriken.
cpu.total.idle			Gesamtzeit, die die CPU im Leerlauf verbracht hat; *cpu.total.idle*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			ist die Summe der *cpuN.idle*-Metriken.
cpu.total.iowait			Gesamtzeit, die die CPU auf den Abschluss von E/A-Vorgängen gewartet hat; *cpu.total.iowait* ist die Summe der *cpuN.iowait*-Metriken.
cpu.total.irq			Gesamtzeit, die der Prozessor für Interrupts aufwendet; *cpu.total.irq* ist die Summe der *cpuN.irq*-Metriken.
cpu.total.softirq			Zeitaufwand für die Verarbeitung von Soft Interrupt-Anforderungen; *cpu.total.softirq* ist die Summe der *cpuN.softirq*-Metriken.
cpu.total.steal			Gesamtzeit, die die virtuelle CPU darauf gewartet hat, dass der Hypervisor eine Verarbeitung für eine andere virtuelle CPU durchführt. Gilt nur für virtuelle Computer.
cpu.total.guest			Gesamtzeit, die von der CPU für die Ausführung des virtuellen Prozessors aufgewendet wurde. Gilt nur für Hypervisoren.
cpu.total.guest_nice			Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität aufgewendet wurde; *cpu.total.guset_nice* ist die Summe der *cpuN.guest_nice*-Metriken

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.<cpu-core>.user			Zeit, die für die Verarbeitung mit normaler Priorität im Benutzermodus aufgewendet wurde.
cpu.<cpu-core>.nice			Zeit, die für die mit nice-Prozesspriorität erfolgende Verarbeitung im Benutzermodus aufgewendet wurde.
cpu.<cpu-core>.system			Zeitaufwand für die Ausführung im Kernel-Modus.
cpu.<cpu-core>.idle			Im Leerlauf verbrachte Zeit.
cpu.<cpu-core>.iowait			Wartezeit auf Abschluss von E/A-Vorgängen. Wird auch als Leerlaufzeit betrachtet.
cpu.<cpu-core>.irq			Zeit, die für die Verarbeitung von Hardware-Interrupts aufgewendet wurde.
cpu.<cpu-core>.softirq			Zeit, die für die Verarbeitung von Software-Interrupts aufgewendet wurde.
cpu.<cpu-core>.steal			Zeit, die von anderen Betriebssystemen vereinnahmt wurde, die in einer virtuellen Umgebung ausgeführt wurden.
cpu.<cpu-core>.guest			Zeit, die für die Ausführung einer virtuellen CPU oder eines Gastbetriebssystems unter der Steuerung des Kernels aufgewendet wurde.
cpu.<cpu-core>.guest_nice			Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität aufgewendet wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.intr			Seit Startzeit verarbeitete Interrupts.
cpu.ctxt			Gesamtanzahl der Kontextwechsel über alle CPUs hinweg.
cpu.btime			Startzeit.
cpu.processes			Anzahl der erstellten Prozesse und Threads, einschließlich jener (aber nicht beschränkt auf jene), die durch Aufrufe der Systemaufrufe fork() und clone() erstellt wurden.
cpu.procs_running			Gesamtanzahl der Prozesse, die auf allen CPUs ausgeführt werden.
cpu.procs_blocked			Anzahl der derzeit blockierten Prozesse, die auf den Abschluss von E/A-Vorgängen warten.
cpu.cpu_count			Die Anzahl der CPUs im System.
cpu.<cpu-core>.cores			Anzahl der CPU-Kerne.

os.linux.metrics-system-cpu-load – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
load_avg.one (empfohlene Metrik)			Durchschnittliche Systemauslastung über eine Minute.
load_avg.five (empfohlene Metrik)			Durchschnittliche Systemauslastung über fünf Minuten.
load_avg.fifteen (empfohlene Metrik)			Durchschnittliche Systemauslastung über 15 Minuten.
load_avg.norm.one			Durchschnittliche Systemauslastung über eine Minute, normalisiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu-load – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			durch die Anzahl der CPUs.
load_avg.norm.five			Durchschnittliche Systemauslastung über fünf Minuten, normalisiert durch die Anzahl der CPUs.
load_avg.norm.fifteen			Durchschnittliche Systemauslastung über 15 Minuten, normalisiert durch die Anzahl der CPUs.

os.linux.metrics-system-cpu-percentage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.avgutilization_percentage			Durchschnittlicher Prozentsatz der verwendeten CPU.
cpu.user_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der die gesamte CPU von Prozessen mit normaler Priorität im Benutzermodus verwendet wurde.
cpu.nice_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs von Prozessen mit nice-Priorität im Benutzermodus verwendet wurden.
cpu.system_percentage (empfohlene Metrik)			Prozentsatz der Zeit, die von der CPU für die Ausführung des Kernels aufgewendet wurde.
cpu.idle_percentage (empfohlene Metrik)			Prozentsatz der Zeit, in der sich alle CPUs im Leerlauf befanden.
cpu.iowait_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von allen CPUs auf den Abschluss

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu-percentage – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			von E/A-Vorgängen gewartet wurde.
cpu.irq_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von allen CPUs Interrupts verarbeitet wurden.
cpu.softirq_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von allen CPUs Software-Interrupts verarbeitet wurden.
cpu.steal_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs virtuelle Hostbetriebssysteme bedient haben.
cpu.guest_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs Gastbetriebssysteme bedient haben.

os.linux.metrics-system-disk – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<disk-name>.reads (empfohlene Metrik)			Gesamtanzahl der erfolgreich abgeschlossenen Lesevorgänge.
disk.<disk-name>.readsMerged			Gesamtanzahl der zusammengeführten Lesevorgänge.
disk.<disk-name>.sectorsRead			Gesamtanzahl der erfolgreich gelesenen Sektoren.
disk.<disk-name>.readTime		milliseconds	Gesamtanzahl an Millisekunden, die für alle Lesevorgänge aufgewendet wurden.
disk.<disk-name>.writes (empfohlene Metrik)			Gesamtanzahl der erfolgreich abgeschlossenen Schreibvorgänge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-disk – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<disk-name>.writesMerged			Gesamtanzahl der zusammengeführten Schreibvorgänge.
disk.<disk-name>.sectorsWritten			Gesamtanzahl der erfolgreich geschriebenen Sektoren.
disk.<disk-name>.writeTime		milliseconds	Gesamtanzahl an Millisekunden, die für alle Schreibvorgänge aufgewendet wurden.
disk.<disk-name>.ioInProgress			Gesamtanzahl der derzeit ausgeführten E/A-Vorgänge.
disk.<disk-name>.ioTime (empfohlene Metrik)			Insgesamt für E/A-Vorgänge aufgewendete Zeit.
disk.<disk-name>.ioTimeWeighted			Insgesamt für E/A-Vorgänge aufgewendete Zeit. Dies kann ein Maß für die E/A-Abschlusszeit und den Rückstand sein, der sich möglicherweise ansammelt.

os.linux.metrics-system-disk-capacity – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<file-system-name>.total			Gesamtgröße des Dateisystems.
disk.<file-system-name>.used			Gesamtmenge des Speicherplatzes, der vorhandenen Dateien im Dateisystem zugewiesen ist.
disk.<file-system-name>.avail			Gesamtmenge des im Dateisystem verfügbaren Speicherplatzes.
disk.<file-system-name>.used_percentage			Prozentsatz des verfügbaren Speicherplatzes, der derzeit allen Dateien im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-disk-capacity – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Dateisystem zugeordnet ist.
disk.<file-system-name>.itotal			Gesamtanzahl von `inodes` im Dateisystem.
disk.<file-system-name>.iused			Anzahl der verwendeten `inodes`.
disk.<file-system-name>.iavail			Anzahl der freien (nicht verwendeten) `inodes`.
disk.<file-system-name>.iused_percentage			Prozentsatz der verwendeten `inodes`.

os.linux.metrics-system-disk-usage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk_usage.<disk>.total			Insgesamt verfügbarer Speicherplatz auf dem Datenträger.
disk_usage.<disk>.used			Gesamtmenge des auf dem Datenträger verwendeten Speicherplatzes.
disk_usage.<disk>.avail			Insgesamt verfügbarer Speicherplatz auf dem Datenträger.
disk_usage.<disk>.used_percentage (empfohlene Metrik)			Prozentsatz des verwendeten Speicherplatzes auf dem Datenträger.

os.linux.metrics-system-memory – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory.total			Insgesamt nutzbarer RAM.
memory.free			Insgesamt freier RAM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-memory – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory.available			Eine Schätzung, wie viel Arbeitsspeicher zum Starten neuer Anwendungen verfügbar ist, ohne dass eine Auslagerung (Swapping) durchgeführt wird.
memory.buffers			Temporärer Speicher, der für Rohdatenträger-Blöcke verwendet wird.
memory.cached			In-Memory Cache für vom Datenträger gelesene Dateien (Seiten-Cache). `mem_swapcached` ist nicht enthalten.
memory.swapTotal (empfohlene Metrik)			Insgesamt verfügbarer Auslagerungsbereich (Swap Space).
memory.swapFree (empfohlene Metrik)			Derzeit nicht genutzter Auslagerungsbereich.
memory.dirty			Arbeitsspeicher, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.
memory.swapUsed (empfohlene Metrik)			Menge des verwendeten Auslagerungsbereichs.
memory.used			Menge des verwendeten RAM.
memory.usedWOBuffersCaches			Menge des verwendeten Arbeitsspeichers.
memory.freeWOBuffersCaches			Wert `MemAvailable` von `/proc/meminfo`, falls vorhanden; falls nicht vorhanden erfolgt Rückgriff auf freien + gepufferten + zwischengespeicherten Speicher.
memory.swapUsedPercentage			Prozentsatz des verwendeten Auslagerungsbereichs.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-memory-percent – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory_percent.free (empfohlene Metrik)			Prozentsatz des freien RAM.
memory_percent.available (empfohlene Metrik)			Prozentsatz des verfügbaren Arbeitsspeichers
memory_percent.buffers (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der für Rohdatenträger-Blöcke verwendet wird.
memory_percent.cached (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der mit In-Memory Cache für vom Datenträger gelesene Dateien verwendet wird.
memory_percent.dirty (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.
memory_percent.swapUsed (empfohlene Metrik)			Prozentsatz des verwendeten Auslagerungsbereichs.
memory_percent.usedWOBuffersCaches (empfohlene Metrik)			Prozentsatz des verwendeten Arbeitsspeichers.
memory_percent.freeWOBuffersCaches (empfohlene Metrik)			Prozentsatz des verfügbaren Arbeitsspeichers.

os.linux.metrics-system-uptime – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
system.uptime(sec)			Zeit, während der das System funktioniert und verfügbar ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.nr_free_pages			Seiten, die derzeit vom System nicht verwendet werden.
vmstat.nr_alloc_batch			Seiten, die anderen Domänen aufgrund von unzureichendem Arbeitsspeicher in jeder Domäne jedes NUMA-Knotens (Non-Uniform Memory Access) zugewiesen sind.
vmstat.nr_inactive_anon			Speicherseiten in jeder Domäne jedes NUMA-Knotens, auf die nicht zugegriffen wurde.
vmstat.nr_active_anon			Seiten des anonymen virtuellen Arbeitsspeichers, die kürzlich verwendet wurden.
vmstat.nr_inactive_file			Speicherseite, die der Datei entspricht, auf die in jeder Domäne jedes NUMA-Knotens nicht zugegriffen wurde.
vmstat.nr_active_file			Speicherseite, die der Datei entspricht, auf die kürzlich zugegriffen wurde.
vmstat.nr_unevictable			Anzahl der Seiten in der (Nicht-)LRU-Liste (Least Recently Used) des Arbeitsspeichers, der nicht freigegeben werden kann (unevictable Memory).
vmstat.nr_mlock			Seiten, die einem virtuellen Speicherbereich (Virtual Memory Area, VMA) mit dem VMA-Flag VM_Locked zugeordnet sind und eine Klasse von Seiten im nicht freigebbaren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Arbeitsspeicher darstellen.
vmstat.nr_anon_pages			Speicherzuordnungsseiten, die nicht Teil einer Datei sind.
vmstat.nr_mapped			Anzahl der zugeordneten Speicherseiten.
vmstat.nr_file_pages			
vmstat.nr_dirtied			Seiten, die darauf warten, auf den Datenträger geschrieben zu werden.
vmstat.nr_writeback			Seiten, die derzeit auf den Datenträger geschrieben werden.
vmstat.nr_slab_reclaimable			Seiten aus der Kernel-Slab-Speichernutzung, die zurückgewonnen werden können.
vmstat.nr_slab_unreclaimable			Seiten aus der Kernel-Slab-Speichernutzung, die nicht zurückgewonnen werden können.
vmstat.nr_page_table_pages			Seiten, die Seitentabellen zugeordnet sind.
vmstat.nr_kernel_stack			Arbeitsspeichermenge, die Kernel-Stapeln zugeteilt ist.
vmstat.nr_unstable			Anzahl der instabilen Seiten in jeder Domäne jedes NUMA-Knotens.
vmstat.nr_bounce			
vmstat.nr_vmscan_write			Anzahl der modifizierten Seiten, die während eines LRU-Scans zurück auf den Datenträger geschrieben wurden.
vmstat.nr_vmscan_immediate_reclaim			
vmstat.nr_writeback_temp			
vmstat.nr_isolated_anon			Anzahl der anonymen Speicherseiten, die in jeder Domäne jedes

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			NUMA-Knotens isoliert sind.
vmstat.nr_isolated_file			Anzahl der Dateispeicherseiten, die in jeder Domäne jedes NUMA-Knotens isoliert sind.
vmstat.nr_shmem			Anzahl der gemeinsam genutzten Speicherseiten.
vmstat.nr_dirtied			Anzahl der modifizierten Seiten in jeder Domäne jedes NUMA Knotens.
vmstat.nr_written			
vmstat.numa_hit			Anzahl der Seiten, die diesem Knoten erfolgreich zugeordnet wurden.
vmstat.numa_miss			Anzahl der Seiten, die diesem Knoten aufgrund von wenig Arbeitsspeicher im vorgesehenen Knoten zugeordnet wurden.
vmstat.numa_foreign			Anzahl der ursprünglich für diesen Knoten bestimmten Seiten, die einem anderen Knoten zugeordnet wurden.
vmstat.numa_interleave			Anzahl der Seiten, die gemäß Interleave-Richtlinie erfolgreich diesem Knoten zugeordnet wurden.
vmstat.numa_local			Anzahl der Seiten, die in diesem Knoten durch einen Prozess in diesem Knoten erfolgreich zugeordnet wurden.
vmstat.numa_other			Anzahl der Seiten, die in diesem Knoten durch einen Prozess in einem anderen Knoten zugeordnet wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.workingset_refault			
vmstat.workingset_activate			
vmstat.workingset_nodereclaim			
vmstat.nr_anon_transparent_hugepages			
vmstat.nr_free_cma			Freie kontinuierliche Speicherzuordnungsseiten in jeder Domäne jedes NUMA-Knotens.
vmstat.nr_dirty_threshold			
vmstat.nr_dirty_background_threshold			
vmstat.pgpgin			Anzahl der vom Datenträger importierten Seiten.
vmstat.pgpgout			Anzahl der auf den Datenträger geschriebenen Seiten.
vmstat.pswpin			Anzahl der aus dem Auslagerungsbereich importierten Seiten.
vmstat.pswpout			Anzahl der in den Auslagerungsbereich ausgelagerten Seiten.
vmstat.pgalloc_dma			
vmstat.pgalloc_dma32			
vmstat.pgalloc_normal			
vmstat.pgalloc_movable			
vmstat.pgfree			Anzahl der seit dem letzten Start verfügbaren Seiten.
vmstat.pgactivate			Anzahl der Seitenaktivierungen seit dem letzten Start.
vmstat.pgdeactivate			Anzahl der Seitendeaktivierungen seit dem letzten Start.
vmstat.pgfault			Geringfügige Fehler seit dem letzten Start.
vmstat.pgmajfault			Schwerwiegende Fehler seit dem letzten Start.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.pglazyfreed			
vmstat.pgrefill_dma			
vmstat.pgrefill_dma32			
vmstat.pgrefill_normal			Anzahl der Seitenauffüllungen seit dem letzten Start.
vmstat.pgrefill_movable			
vmstat.pgsteal_kswapd_dma			
vmstat.pgsteal_kswapd_dma32			
vmstat.pgsteal_kswapd_normal			
vmstat.pgsteal_kswapd_movable			
vmstat.pgsteal_direct_dma			
vmstat.pgsteal_direct_dma32			
vmstat.pgsteal_direct_normal			
vmstat.pgsteal_direct_movable			
vmstat.pgscan_kswapd_dma			
vmstat.pgscan_kswapd_dma32			
vmstat.pgscan_kswapd_normal			Anzahl der von *kswapd* seit dem Start gescannten Seiten.
vmstat.pgscan_kswapd_movable			
vmstat.pgscan_direct_dma			
vmstat.pgscan_direct_dma32			
vmstat.pgscan_direct_normal			Anzahl der seit dem Start zurückgewonnenen Seiten.
vmstat.pgscan_direct_movable			
vmstat.pgscan_direct_throttle			
vmstat.zone_reclaim_failed			
vmstat.pginodesteal			
vmstat.slabs_scanned			
vmstat.kswapd_inodesteal			
vmstat.kswapd_low_wmark_hit_quickly			
vmstat.kswapd_high_wmark_hit_quickly			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.pageoutrun			Anzahl der durch `kswapd` erfolgenden Aufrufe der Seitenrückgewinnung.
vmstat.allocstall			Anzahl der direkten Aufrufe der Seitenrückgewinnung (wenig Arbeitsspeicher).
vmstat.pgrotated			
vmstat.drop_pagecache			
vmstat.drop_slab			
vmstat.numa_pte_updates			
vmstat.numa_huge_pte_updates			
vmstat.numa_hint_faults			
vmstat.numa_hint_faults_local			
vmstat.numa_pages_migrated			
vmstat.pgmigrate_success			
vmstat.pgmigrate_fail			
vmstat.compact_migrate_scanned			
vmstat.compact_free_scanned			
vmstat.compact_isolated			
vmstat.compact_stall			Häufigkeit, mit der ein Prozess bei der Arbeitsspeicherkomprimierung verzögert wird, sodass eine große Seite zur Verfügung steht.
vmstat.compact_fail			Häufigkeit, mit der vom System versucht wurde, den Arbeitsspeicher zu komprimieren, und mit der der betreffende Versuch fehlgeschlagen ist.
vmstat.compact_success			Häufigkeit, mit der vom System Arbeitsspeicher komprimiert und eine große Seite zur Verwendung freigegeben wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.htlb_buddy_alloc_success			
vmstat.htlb_buddy_alloc_fail			
vmstat.unevictable_pgs_culled			
vmstat.unevictable_pgs_scanned			
vmstat.unevictable_pgs_rescued			
vmstat.unevictable_pgs_mlocked			
vmstat.unevictable_pgs_munlocked			
vmstat.unevictable_pgs_cleared			
vmstat.unevictable_pgs_stranded			
vmstat.thp_fault_alloc			Anzahl der großen Seiten, die erfolgreich zur Behandlung eines Seitenfehlers zugeordnet wurden.
vmstat.thp_fault_fallback			Anzahl der Seitenfehler, bei denen die Zuordnung einer großen Seite vor Rückgriff auf die Verwendung kleiner Seiten fehlgeschlagen ist.
vmstat.thp_collapse_alloc			Anzahl der Seiten, die mit der erfolgreichen Zuordnung einer neuen großen Seite zum Speichern der Daten zu einer großen Seite zusammengefasst wurden.
vmstat.thp_collapse_alloc_failed			Anzahl der Seiten, die zu einer großen Seite zusammengefasst wurden, bei denen die Zuordnung jedoch fehlgeschlagen ist.
vmstat.thp_split			Anzahl der Basisseiten, in die eine große Seite aufgeteilt werden soll.
vmstat.thp_zero_page_alloc			Anzahl der erfolgreichen Zuordnungen von großen „Zero Pages“ (Nullseiten).
vmstat.thp_zero_page_alloc_failed			Häufigkeit, mit der vom Kernel eine große

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Nullseite nicht zugeordnet werden konnte und auf die Verwendung kleiner Seiten zurückgegriffen wurde.
vmstat.balloon_inflate			
vmstat.balloon_deflate			
vmstat.balloon_migrate			

os.linux.metrics-process-status – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
proc.<process>.VmSize			Gesamtmenge des vom Prozess verwendeten virtuellen Arbeitsspeichers.
proc.<process>.VmRSS			Der nicht ausgelagerte physische Arbeitsspeicher, der von einem Prozess verwendet wird.
proc.<process>.VmSwap			Gesamtmenge des verwendeten Auslagerungsbereichs.

MongoDB – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die MongoDB-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für Windows und Linux verfügbar.

MongoDB-Ereignisse

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
Event	app.mongodb.check-mongodb-alive	Überwacht, ob der MongoDB-Server aktiv ist, und erstellt Warnungen für den MongoDB-Server-Integritätsstatus.	commonchecks check-mongodb-alive -H db_host -p db_port Wobei:	commonchecks check-mongodb -p {{.labels.params_port}} -H {{.labels.params_host}}	Check mongodb Alive OK: Gibt an, dass der Integritätsstatus des Servers in Ordnung ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
			• db_host = Host, auf dem der Server ausgeführt wird. • db_port = Port für die Verbindung mit dem MongoDB-Server. Verwendungsbeispiel: command: commonchecks check-mongodb-alive -H 10.***.***.*** -p 27017		
Event	app.mongodb.check-mongodb-metrics	Erstellt Warnungen für eine der MongoDB-Metriken basierend auf dem Schwellenwert. Um die Warnungen für eine MongoDB-Servermetrik auszulösen, übergeben Sie den gesamten Metriknamen im Parameter.	commonchecks check-mongodb-metrics -H Hostname -p port -w warning -c critical -d database -m MetricName Wobei: • Hostname = Host, auf dem der Server ausgeführt wird. • port = Port zum Herstellen der Verbindung mit dem MongoDB-Server.	commonchecks check-mongodb-metrics -c {{.labels.params_critical}} -d {{.labels.params_database}} -w {{.labels.params_warning}} -H {{.labels.params_host}} -p {{.labels.params_port}} -m {{.labels.params_metric}}	Check mongodb Metrics OK: Gibt an, dass der Wert von mongodb.connection.current innerhalb des akzeptablen Schwellenwerts liegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
			• warning = Warnungsschwellenwert. • critical = Kritischer Schwellenwert. • database = Datenbankname. • MetricName = Spezifische zu überwachende Metrik. Verwendungsbeispiel: command: commonchecks check-mongodb-alive -H 10.***.***.*** -p 27017		

MongoDB-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
Metrik	app.mongodb.metrics-mongodb	Gibt Metriken des MongoDB-Servers und aller Datenbanken zurück. Beispielmetriken: • mongodb.connections.totalCre: Eingehende Verbindungen • mongodb.locks.Database.acquireCount_IX: Sperrmodus „Intent Exclusive“ • mongodb.locks.Database.acquireCount_X: Sperrmodus „Exklusive“	commonchecks check-mongodb Wobei: • host = Name des Hosts, auf dem der MongoDB-Server ausgeführt wird. • port = Port zum Herstellen der Verbindung mit dem	commonchecks metrics-mongodb -p {{.labels.params_port}} -H {{.labels.params_host}} -d {{.labels.params_database}}	<hostname>.mongodb.connect 20632 1639498004

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
		• mongodb.locks.Database.acquireCount_IS : Sperrmodus „Intent Shared“	MongoDB-Server. • database = Datenbankname.		

MongoDB-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von MongoDB-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

metrics-mongodb – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.asserts.msg (empfohlene Metrik)		count	Anzahl der seit Beginn des MongoDB-Prozesses ausgelösten Nachrichten-Assertionen. Untersuchen Sie die Protokolldatei auf weitere Informationen zu diesen Nachrichten.
mongodb.asserts.regular (empfohlene Metrik)		count	Anzahl der regulären Assertionen, die seit Beginn des MongoDB-Prozesses ausgelöst wurden. Untersuchen Sie die Protokolldatei auf weitere Informationen zu diesen Nachrichten.
mongodb.asserts.rollovers		count	Anzahl, die angibt, wie oft bei den Rollover-Zählern seit dem letzten Start des MongoDB-Prozesses ein Rollover durchgeführt wurde.
mongodb.asserts.tripwire			Anzahl der seit Beginn des MongoDB-Prozesses ausgelösten Tripwire-Assertionen.
mongodb.asserts.user		count	Anzahl der „Benutzer-Asserts“, die seit dem letzten Start des

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			MongoDB-Prozesses aufgetreten sind.
mongodb.asserts.warning (empfohlene Metrik)		count	Anzahl der Warnungen, die seit Beginn des MongoDB-Prozesses ausgelöst wurden.
mongodb.connections.available		count	Anzahl der nicht verwendeten eingehenden Verbindungen, die verfügbar sind.
mongodb.connections.current		count	Anzahl der eingehenden Verbindungen von Clients zum Datenbankserver.
mongodb.connections.totalCreated		count	Anzahl aller eingehenden Verbindungen, die mit dem Server hergestellt wurden.
mongodb.cursor.open.noTimeout		count	Anzahl der offenen Cursor, bei denen die Option `DBQuery.Option.noTimeout` festgelegt ist, damit eine Zeitüberschreitung nach einem Zeitraum der Inaktivität verhindert wird.
mongodb.cursor.open.pinned		count	Anzahl der „angehefteten“ offenen Cursor.
mongodb.cursor.open.total (empfohlene Metrik)		count	Anzahl der Cursor, die MongoDB für Clients verwaltet. Da MongoDB nicht verwendete Cursor aufbraucht, ist dieser Wert normalerweise klein oder null. Wenn jedoch eine Warteschlange, veraltete „Tailable Cursor“ (spezielle bei Abschluss einer Abfrage nicht geschlossene, sondern offen gehaltene Cursor) oder eine große Anzahl von Vorgängen vorhanden sind, kann dieser Wert steigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.cursor.timedOut		count	Gesamtanzahl der Cursor, bei denen seit dem Start des Serverprozesses eine Zeitüberschreitung aufgetreten ist.
mongodb.databaseSizes.avgObjSize	admin	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSizes.avgObjSize	Konfiguration	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSizes.avgObjSize	local	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSizes.collections	admin	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSizes.collections	Konfiguration	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSizes.collections	local	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSizes.dataSize	admin	Bytes	Gesamtgröße der unkomprimierten Daten in der Datenbank. Der Wert `dataSize` wird kleiner, wenn Sie Dokumente entfernen. Für Datenbanken, bei denen die Speicher-Engine `WiredTiger` verwendet wird, kann `dataSize` größer sein als `storageSize`, wenn die Komprimierung aktiviert ist. Der Wert `dataSize` wird kleiner, wenn Dokumente kleiner werden.
mongodb.databaseSizes.dataSize	Konfiguration	Bytes	Gesamtgröße der unkomprimierten Daten in der Datenbank.
mongodb.databaseSizes.dataSize	local	Bytes	Gesamtgröße der unkomprimierten Daten in der Datenbank.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.databaseSizes.indexes	admin	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexes	Konfiguration	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexes	local	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexSize	admin	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.indexSize	Konfiguration	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.indexSize	local	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.objects	admin	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.
mongodb.databaseSizes.objects	Konfiguration	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.
mongodb.databaseSizes.objects	local	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.
mongodb.databaseSizes.storageSize	admin	Bytes	Dieser Wert verringert sich nicht, wenn Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Dokumente entfernen oder verkleinern. Dieser Wert kann für Datenbanken, bei denen die Speicher-Engine `WiredTiger` mit aktivierter Komprimierung verwendet wird, kleiner als `dataSize` sein. `storageSize` enthält keinen den Indizes zugeordneten Speicherplatz. Informationen zur Gesamtindexgröße finden Sie unter `indexSize`.
mongodb.databaseSizes.storageSize	Konfiguration	Bytes	Summe des Speicherplatzes, der allen Sammlungen in der Datenbank zum Speichern von Dokumenten zugeordnet ist, einschließlich des freien Speicherplatzes.
mongodb.databaseSizes.storageSize	Konfiguration	Bytes	Summe des Speicherplatzes, der allen Sammlungen in der Datenbank zum Speichern von Dokumenten zugeordnet ist, einschließlich des freien Speicherplatzes.
mongodb.globalLock.activeClients.readers (empfohlene Metrik)		count	Anzahl der aktiven Clientverbindungen, von denen Lesevorgänge ausgeführt werden.
mongodb.globalLock.activeClients.total		count	Gesamtzahl der internen Clientverbindungen mit der Datenbank, einschließlich der System-Threads sowie der Reader und Writer in der Warteschlange. Diese Metrik ist aufgrund der Einbeziehung von System-Threads höher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			als die Summe von *`activeClients.readers`* und *`activeClients.writers`*.
mongodb.globalLock.activeClients.writers (empfohlene Metrik)		count	Anzahl der aktiven Clientverbindungen, von denen Schreibvorgänge ausgeführt werden.
mongodb.globalLock.currentQueue.readers (empfohlene Metrik)		count	Anzahl der Vorgänge, die sich derzeit in der Warteschlange befinden und auf die Lesesperre warten. Eine durchgängig kleine Lesewarteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis.
mongodb.globalLock.currentQueue.total		count	Gesamtanzahl der Vorgänge in der Warteschlange, die auf die Sperre warten (d. h. die Summe von *`globalLock.currentQueue.readers`* und *`globalLock.currentQueue.writers`*. Eine durchgängig kleine Warteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis. Die *`globalLock.activeClients`*-Reader- und -Writer-Informationen machen Kontext für diese Daten verfügbar.
mongodb.globalLock.currentQueue.writers (empfohlene Metrik)		count	Anzahl der Vorgänge, die sich derzeit in der Warteschlange befinden und auf die Schreibsperre warten. Eine durchgängig kleine Schreibwarteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.globalLock.totalTime		Mikrosekunden	Zeit in Mikrosekunden, seit die Datenbank zuletzt gestartet wurde und die `globalLock` erstellt hat. Dies entspricht in etwa der Gesamtbetriebszeit des Servers.
mongodb.locks.Collection.acquireCount_r		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Collection.acquireCount_w		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Intent Exclusive“ (IX) erfasst wurde.
mongodb.locks.Collection.acquireCount_W		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.locks.Database.acquireCount_r		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Database.acquireCount_w		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Intent Exclusive“ (IX) erfasst wurde.
mongodb.locks.Database.acquireCount_W		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.locks.Global.acquireCount_r		count	Anzahl, die angibt, wie oft die globale Sperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Global.acquireCount_w		count	Anzahl, die angibt, wie oft die globale Sperre

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			im Sperrmodus „Intent Exclusive“ (IX) erfasst wurde.
mongodb.locks.Global.acquireCount_W		count	Anzahl, die angibt, wie oft die globale Sperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.mem.pageFaults		count	Gesamtanzahl der Seitenfehler. Der `extra_info.page_faults`-Zähler kann in Momenten schlechter Leistung drastisch ansteigen und mit Umgebungen mit begrenztem Arbeitsspeicher und größeren Datensätzen korrelieren. Begrenzte und sporadische Seitenfehler weisen nicht unbedingt auf ein Problem hin.
mongodb.mem.resident (empfohlene Metrik)		Mebibyte	Dieser Wert entspricht in etwa der Größe des Arbeitsspeichers (in Mebibyte, MiB), der derzeit vom Datenbankprozess verwendet wird. Während des normalen Gebrauchs steigt dieser Wert tendenziell an. Bei dedizierten Datenbankservern nähert sich die Anzahl häufig der Gesamtmenge des Systemspeichers an.
mongodb.mem.virtual		Mebibyte	Menge des vom mongod-Prozess verwendeten virtuellen Arbeitsspeichers in Mebibyte (MiB).
mongodb.metrics.document.deleted		count	Gesamtanzahl der gelöschten Dokumente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.metrics.document.inserted		count	Gesamtanzahl der eingefügten Dokumente.
mongodb.metrics.document.returned		count	Gesamtanzahl der von Abfragen zurückgegebenen Dokumente.
mongodb.metrics.document.updated		count	Gesamtanzahl der aktualisierten Dokumente.
mongodb.metrics.getLastError.wtime_num (empfohlene Metrik)		count	Gesamtanzahl der `getLastError`-Vorgänge, bei denen der „Write Concern“ (w) so festgelegt ist, dass von mindestens einem Mitglied eines Replikatsatzes die Bestätigung des Schreibvorgangs abgewartet wird (Einstellung: w-Wert größer als 1).
mongodb.metrics.getLastError.wtime_totalMillis (empfohlene Metrik)		Millisekunden	Gesamtzeit in Millisekunden, die vom mongod-Prozess darauf verwendet wurde, `getLastError`-Vorgänge auszuführen, bei denen der „Write Concern“ (w) so festgelegt ist, dass von mindestens einem Mitglied eines Replikatsatzes die Bestätigung des Schreibvorgangs abgewartet wird (Einstellung: w-Wert größer als 1).
mongodb.metrics.getLastError.wtimeouts (empfohlene Metrik)		count	Anzahl, die angibt, wie oft bei „Write Concern“-Vorgängen aufgrund des `wtimeout`-Schwellenwerts für `getLastError` eine Zeitüberschreitung aufgetreten ist. Diese Anzahl wird sowohl für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			standardmäßige als auch für nicht dem Standard entsprechende „Write Concern“-Spezifikationen schrittweise erhöht.
mongodb.metrics.operation.scanAndOrder		count	Gesamtanzahl der Abfragen, von denen sortierte Zahlen zurückgegeben werden und bei denen der Sortiervorgang nicht mit einem Index ausgeführt werden kann.
mongodb.metrics.queryExecutor.scanned		count	Gesamtanzahl der während Abfragen und Abfrageplanauswertungen gescannten Indexelemente. Dieser Zähler ist derselbe wie `totalKeysExamined` in der Ausgabe von explain().
mongodb.metrics.queryExecutor.scannedObjects		count	Gesamtanzahl der Dokumente, die während Abfragen und Abfrageplanauswertungen gescannt wurden. Dieser Zähler ist derselbe wie `totalDocsExamined` in der Ausgabe von explain().
mongodb.metrics.record.moves			Ein Dokument, in dem über Daten im Zusammenhang mit der Datensatzzuordnung in den Speicherdateien auf dem Datenträger berichtet wird.
mongodb.metrics.repl.apply.batches_num		count	Gesamtanzahl der auf alle Datenbanken angewendeten Batches.
mongodb.metrics.repl.apply.batches_totalMillis		count	Gesamtzeit in Millisekunden, die vom mongod-Prozess darauf verwendet wurde, Vorgänge aus der oplog-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Sammlung (Operations Log) anzuwenden.
mongodb.metrics.repl.apply.ops		count	Gesamtanzahl der angewendeten oplog-Vorgänge. Der `metrics.repl.apply.ops`-Wert wird nach jedem Vorgang erhöht.
mongodb.metrics.repl.buffer.count		count	Aktuelle Anzahl der Vorgänge im oplog-Puffer.
mongodb.metrics.repl.buffer.maxSizeBytes		Bytes	Maximale Größe des Puffers. Dieser Wert ist eine konstante Einstellung im mongod-Prozess und kann nicht konfiguriert werden.
mongodb.metrics.repl.buffer.sizeBytes		Bytes	Aktuelle Größe des Inhalts des oplog-Puffers.
mongodb.metrics.repl.network.bytes		count	Gesamtmenge der aus der Replikationssynchronisierungsquelle gelesenen Daten.
mongodb.metrics.repl.network.getmores_num		count	Meldet die Gesamtanzahl der `getmore`-Vorgänge, bei denen es sich um Vorgänge handelt, mit denen ein zusätzlicher Satz von Vorgängen von der Replikationssynchronisierungsquelle angefordert wird.
mongodb.metrics.repl.network.getmores_totalMillis		count	Gesamtzeit, die zum Sammeln von Daten aus `getmore`-Vorgängen erforderlich ist.
mongodb.metrics.repl.network.ops		count	Gesamtanzahl der aus der Replikationsquelle gelesenen Vorgänge.
mongodb.metrics.repl.network.readersCreated		count	Gesamtanzahl der erstellten oplog-Abfrageprozesse. Von MongoDB wird jedes Mal eine neue oplog-Abfrage erstellt, wenn ein Fehler in der Verbindung auftritt,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			einschließlich einer Zeitüberschreitung oder eines Netzwerkvorgangs. Darüber hinaus wird der `metrics.repl.network.readersCr` Wert jedes Mal erhöht, wenn von MongoDB eine neue Quelle für die Replikation ausgewählt wird.
mongodb.metrics.ttl.deletedDocuments		count	Gesamtanzahl der Dokumente, die aus Sammlungen mit einem `ttl`-Index gelöscht wurden.
mongodb.metrics.ttl.passes		count	Gesamtanzahl der Dokumente, die aus Sammlungen mit einem `ttl`-Index gelöscht wurden.
mongodb.network.bytesIn		count	Gesamtanzahl der Bytes, die vom Server über von Clients initiierte Netzwerkverbindungen empfangen wurden.
mongodb.network.bytesOut		count	Gesamtanzahl der Bytes, die vom Server über von Clients initiierte Netzwerkverbindungen gesendet wurden.
mongodb.network.numRequests		count	Gesamtanzahl der eindeutigen Anforderungen, die der Server erhalten hat. Verwenden Sie diesen Wert, um Kontext für die Werte `network.bytesIn` und `network.bytesOut` bereitzustellen und dadurch sicherzustellen, dass die Netzwerkauslastung von MongoDB den Erwartungen und der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Anwendungsnutzung entspricht.
mongodb.opcounters.command		count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz an die Datenbank ausgegebenen Befehle. Von `opcounters.command` werden alle Befehle mit Ausnahme der Schreibbefehle insert (einfügen), update (aktualisieren) und delete (löschen) gezählt.
mongodb.opcounters.delete		count	Gesamtanzahl der Löschvorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcounters.getmore		count	Gesamtanzahl der `getMore`-Vorgänge seit dem letzten Start der mongod-Instanz. Dieser Zähler kann hoch sein, auch wenn die Abfrageanzahl niedrig ist. Von sekundären Knoten werden `getMore`-Vorgänge als Teil des Replikationsprozesses gesendet.
mongodb.opcounters.insert		count	Gesamtanzahl der Einfügevorgänge, die seit dem letzten Start der mongod-Instanz empfangen wurden.
mongodb.opcounters.query		count	Gesamtanzahl der Abfragen, die seit dem letzten Start der mongod-Instanz empfangen wurden.
mongodb.opcounters.update		count	Gesamtanzahl der Aktualisierungsvorgänge, die seit dem letzten Start der mongod-Instanz empfangen wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.opcountersRepl.c	ommand	count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz an die Datenbank ausgegebenen replizierten Befehle.
mongodb.opcountersRepl.d	elete	count	Gesamtanzahl der replizierten Löschvorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcountersRepl.g	etmore	count	Gesamtanzahl der getMore-Vorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcountersRepl.i	nsert (empfohlene Metrik)	count	Gesamtanzahl der replizierten Einfügevorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcountersRepl.q	uery (empfohlene Metrik)	count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz replizierten Abfragen.
mongodb.opcountersRepl.u	pdate	count	Gesamtanzahl der replizierten Aktualisierungsvorgänge seit dem letzten Start der mongod-Instanz.

Ms Exchange – Standardprüfungen und -Richtlinien

Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für die MS Exchange-Überwachung bereit.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	App.msExchange.metrics msExchange	Gibt Microsoft Exchange-Metriken zurück.	winchecks metric-msexchange (options) -s scheme Replaces the host name with this parameter	Metriken vom MS Exchange-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Anwendungsbeispiel: Winchecks metric-msExchange {{if .Labels.params_scheme}} -s {{if .Labels.params_scheme}} {{end}}	

MSSQL – Standardprüfungen und Richtlinien

Die Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für die Überwachung von MSSQL-Metriken bereit.

MSSQL Metrics

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	app.metrics-mssql-query	Generische MSSQL-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann.	winchecks metrics-mssql-query (Optionen) -d, --database DATABASE – Datenbankschema, mit dem eine Verbindung hergestellt werden soll (erforderlich) -q ,--query – Die auszuführende Abfrage; sollte einen Listenmetriknamen und -wert zurückgeben, z. B. SELECT METRIC_NAME, VALUE FROM GV$SYSMETRIC -h, --host HOST – Name des Hosts, mit dem eine Verbindung hergestellt werden soll; Standardwert: localhost	In den Parametern definierte benutzerdefinierte Metriken, die auch Wert und Zeitstempel enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSSQL Metrics (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			-r, --port PORT – Port, mit dem eine Verbindung hergestellt werden soll; Standardwert: 1433 -s, --scheme SCHEME – Metrikbenennungsschema; Text, der . $parent.$child vorangestellt werden soll. **Verwendungsbeispiel** `.winchecks metrics-mssql-query -d master -H localhost -p 1437 -q "select name,size from sys.database_files"`	

MySQL-Standardprüfungen und -Richtlinien

Die Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für die MySQL-Metriküberwachung bereit.

MySQL-Ereignisse

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
Ereignis	app.mysql.check-mysql-alive	Überprüft die Länge eines Ergebnissatzes aus einer MySQL-Abfrage.	Check-mysql-query-result-count.rb (Optionen) -C, --kritische ANZAHL kritischer Schwellenwert für Anzahl der von der Abfrage zurückgegebenen Elemente (erforderlich) -D, --database DATABASE	MysqlQueryCountCheck OK/KRITISCH/ WARNUNG: Meldung zum Verhältnis zwischen Abfragelänge und Schwellenwerten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
			MySQL Database (erforderlich) -H, --Host-MySQL-Host, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“. Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -P, --Port MySQL-Port, mit dem eine Verbindung hergestellt werden soll -Q, --query ABFRAGE – auszuführende ABFRAGE (erforderlich) -W, --WARNUNGSANZAHL – Warnungsschwellenwert für Anzahl der von der Abfrage zurückgegebenen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
			Elemente (erforderlich) -S, --Socket UNIX-Socket, mit dem eine Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) **Verwendungsbeispiel** `Check-mysql-query-result-count.rb -h 127.0.0.1 -P 3306 -d mysql -q „Select * from user“ -W 5 -c 8`	
Ereignis	app.mysql.check-mysql-threads	Überprüft die MySQL DB-Anzahl der ausgeführten Threads und weist je nach Eingabewerten den Status OK/WARNUNG/ KRITISCH zu.	Check-mysql-Threads.rb (Optionen) -H, --hostname HOST Hostname, bei dem Sie sich anmelden möchten -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“ (erforderlich, wenn .ini-Pfad angegeben wird). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren,	CheckMySQLHealth OK/Kritisch/ Warnung und Anzahl der ausgeführten Threads

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
			geben Sie die Werte für die Eigenschaften „Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -C, --critnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -W, --warnnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -P, --Port MySQL-Port, mit dem eine Verbindung hergestellt werden soll -S, --Socket UNIX-Socket, mit dem eine Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) **Verwendungsbeispiel** `Check-mysql-Threads.rb -h 127.0.0.1 -P 3306`	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
			-l 0 -m 1 -c 25 -W 20	
Ereignis	util.check-mysql-query	Überprüft, ob MySQL DB ausgeführt wird.	Check-mysql-Threads.rb (Optionen) -H, --hostname HOST Hostname, bei dem Sie sich anmelden möchten -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“ (erforderlich, wenn der .ini-Pfad angegeben wird). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -C, --critnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -W, --warnnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung	CheckMySQLHealth OK/Kritisch/ Warnung und Anzahl der ausgeführten Threads

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Beispiel für Verwendung und Nutzung	Ausgabe
			ausgegeben wird -L, --critlow ANZAHL ANZAHL der laufenden Threads, unter denen eine Warnung ausgegeben wird -M, --warnlow ANZAHL der laufenden Threads, unter denen eine Warnung ausgegeben wird -P, --Port MySQL-Port, mit dem eine Verbindung hergestellt werden soll -S, --Socket UNIX-Socket, mit dem eine Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) **Verwendungsbeispiel** `Check-mysql-Threads.rb -h 127.0.0.1 -P 3306 -l 0 -m 1 -c 25 -W 20`	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	app.mysql.metrics-mysql	Gibt Metriken für die MySQL-DB zurück.	/Usr/local/bin/metrics-mysql-graphite.rb (Optionen) -H, --Host-MySQL-Host, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“ (erforderlich, wenn der .ini-Pfad angegeben wird). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -P, --Port MySQL-Port, mit dem eine Verbindung hergestellt werden soll. -S, --SCHEMASCHEMA Metrikbenennungsschema, Text, der an die Metrik angehängt werden soll -S, --Socket UNIX-Socket, mit dem eine	MysqlQueryCountCheck OK/KRITISCH/WARNUNG: Meldung zum Verhältnis zwischen Abfragelänge und Schwellenwerten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) -V, --ausführlich Fehler anzeigen (falls generiert) in Bezug auf sekundäre Statuskopien. Fügen Sie dem zu aktivierenden Befehl -V hinzu. **Verwendungsbeispiel** `Check-mysql-Threads.rb -h 127.0.0.1 -P 3306 -l 0 -m 1 -c 25 -W 20`	
Metrik	app.mysql.check-mysql-threads	Überprüft die MySQL DB-Anzahl der ausgeführten Threads und weist je nach Eingabewerten den Status OK/WARNUNG/ KRITISCH zu.	/Usr/local/bin/ metrics-mysql-graphite.rb (Optionen) -H, --hostname HOST Hostname, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“ (erforderlich, wenn der .ini-Pfad angegeben wird). Um die	Hostname.mysql.General.aborted 7600 1649630975 Hostname.mysql.General.aborted 247 1649630975 Hostname.mysql.General.txBytes 752733902 1649630975 hostname.mysql.commands.admi 1631 1649630975 hostname.mysql.commands.alter 0 1649630975

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -C, --critnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -W, --warnnum-NUMMER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -L, --critlow ANZAHL ANZAHL der laufenden Threads, unter denen eine Warnung ausgegeben wird -M, --warnlow ANZAHL der laufenden Threads, unter denen eine Warnung ausgegeben wird -P, --Port MySQL-Port, mit dem eine Verbindung	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			hergestellt werden soll -S, --Socket UNIX-Socket, mit dem eine Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) **Verwendungsbeispiel** `Metriken-mysql-Graphit.rb -h 127.0.0.1 -P 3306`	
Metrik	app.mysql.metrics-mysql-processes	Gibt verschiedene Metriken zu MySQL DB-Prozessen zurück	/Usr/local/bin/metrics-mysql-processes.rb (Optionen) -H, --Host MySQL-Host, mit dem eine Verbindung hergestellt werden soll -i, --ini WERT my.cnf ini-Datei WERTABSCHNITT „-ini-section“ in Datei „my.cnf ini“ (erforderlich, wenn der .ini-Pfad angegeben wird). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften	Prozesse, Befehle, die sie ausführen, und die Datenbanken, in denen sie die Befehle ausführen **Beispiel:** • Hostname.mysql.database.mys 1 1649631113 • hostname.mysql.command.Dae 1 1649631113 • hostname.mysql.command.Slee 4 1649631113 • hostname.mysql.command.Que 1 1649631113

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			„Anwender“ und „Passwort“ in an **Client** Abschnitt in der INI-Datei. -P, --Port MySQL-Port, mit dem eine Verbindung hergestellt werden soll -S --SCHEMASCHEMA Metrikbenennungsschema, Text, der an die Metrik angehängt werden soll -S, --Socket UNIX-Socket, mit dem eine Verbindung hergestellt werden soll (erforderlich, wenn der angegebene Host auf UNIX-ähnlichen Systemen „localhost“ ist) **Verwendungsbeispiel** `Metriken-mysql-processes.rb -h 127.0.0.1 -P 3306`	

Netzwerk-Ping-Standardprüfungen und -Richtlinien

Agent Client Collector Stellt die folgenden Standardprüfungen und -Richtlinien für die Netzwerk-Ping-Überwachung bereit. Richtlinien und Prüfungen sind für beide verfügbar Windows Und Linux.

Richtlinie für Netzwerk-Ping-Metriken

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
Util.metrics-ping	Wird für die in erkannte ip-Adresse ausgeführt	Metriken-Ping.rb (Optionen)		`c7inc0047383.ping.packets_tra`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Netzwerk-Ping-Metriken (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	ServiceNow Instanz. Pingt den Host an und sammelt Metriken. Der überwachte CI-Typ ist *cmdb_ci_hardware*Und ist an den entsprechenden Server gebunden. Ein Proxy-Agent ist erforderlich.	c – Anzahl Ping-Anzahl -H Host für Ping -T --Timeout ZEITÜBERSCHREITUNG Beispiel: ./metrics-ping.rb -h 10.196.121.11		nsmitted 5 1675923886 c7inc0047383.ping.packets_received 5 1675923886 c7inc0047383.ping.packet_loss 0 1675923886 c7inc0047383.ping.time 3999 1675923886 c7inc0047383.ping.min 0.253 1675923886 c7inc0047383.ping.avg 0.292 1675923886 c7inc0047383.ping.max 0.318 1675923886 c7inc0047383.ping.mdev 0.032 1675923886 **Hinweis:** Windows Unterstützt nicht *ping.time*Und *ping.mdev*Metriken.

Netzwerk-Ping-Metriken

In der folgenden Tabelle sind die Metriken aufgeführt, die als Ausgabe von Netzwerk-Ping-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk-Ping-Metriken

Metriktyp	Einheiten	Beschreibung des Metriktyps
Ping.Packets_Transported	count	Anzahl der Datenpakete, die während des Ping-Tests an den Zielhost gesendet wurden.
Ping.Packets_received	count	Anzahl der Datenpakete, die erfolgreich vom Zielhost empfangen wurden.
Ping.Paket_Verlust	percentage	Prozentsatz der Datenpakete, die den Zielhost nicht erreicht haben.
Ping.Zeit	ms	Zeit, die die Datenpakete zum Ziel und zurück senden.
Ping.Min	ms	Kürzeste Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.
Ping.Durchschn	ms	Durchschnittliche Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.
ping.max	ms	Längste Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.
Ping.mdev	ms	Mittlere Abweichung (Maß für die Variabilität oder Dispersion) der Roundtrip-Zeit (RTT) der während des Ping-Tests gesendeten Pakete.

Verfügbarkeitsprüfung des Netzwerkhosts

Agent Client Collector Stellt die folgende Standardprüfung für die Netzwerk-Ping-Überwachung bereit. Die Prüfung ist sowohl für Windows als auch für Linux verfügbar.

util.check-ping Scheck

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
util.check-ping	Überprüft die Verfügbarkeit des Netzwerkhosts über ICMP-Anforderungen (Ping). Generiert ein OK-Ereignis, wenn das Ping-Erfolgsverhältnis den Warnungsschwellenwert (-W, Standard	Check-ping.rb –h <ip-address> (Optionen) -H Host : Host für Ping (erforderlich). Standard=<localhost> -C-Anzahl : Anzahl der an den Host gesendeten Ping-Anforderungen. Standard=1		ICMP ping unsuccessful for host: 192.168.1.1 (successful: 0/5)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

util.check-ping Scheck (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	50 %) überschreitet. Generiert ein Warnungsereignis, wenn das Ping-Erfolgsverhältnis zwischen dem Warnungsschwellenwert (-W, Standard 50 %) und dem kritischen Schwellenwert (-C, Standard 20 %) liegt. Generiert ein kritisches Ereignis, wenn das Ping-Erfolgsverhältnis unter den kritischen Schwellenwert (-C, Standard 20 %) fällt. Ein Proxy-Agent ist erforderlich.	`-T-Zeitüberschreitung` : Die Zeitüberschreitung (in Sekunden) für jede Ping-Anforderung. Wenn die Zeitüberschreitung abläuft, bevor eine Antwort empfangen wird, gilt der Ping als fehlgeschlagen. Standard=5 `-6 ipv6` : Aktiviert IPv6-Pinging. Ping verwendet IPv4, wenn diese Kennzeichnung nicht verwendet wird. Standard = False `-i-Intervall` : Intervall (in Sekunden) zwischen jeder Ping-Anforderung. Standard=1 `-W-Verhältnis` : Der Schwellenwert für das Erfolgsverhältnis für einen Warnungsstatus. Wenn die erfolgreichen Ping-Antworten unter diesem Verhältnis und über dem Verhältnis „-C“ liegen, gibt das Skript eine Warnung zurück. Standard=0,5		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

util.check-ping Scheck (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
		-C-Verhältnis : Der Schwellenwert für das Erfolgsverhältnis für einen kritischen Status. Wenn die erfolgreichen Ping-Antworten unter diesem Verhältnis liegen, gibt das Skript einen kritischen Fehler zurück. Standard=0,2 -R-Bericht : Kennzeichnung, die an die Fehlermeldung eines MTR-Berichts (meine Ablaufverfolgungsroute) angehängt werden soll, wenn der Ping fehlschlägt. Wenn MTR ausgeführt wird, wird ein Netzwerkdiagnosebericht generiert. Standard=falsch		

Nginx – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Nginx-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für Windows und Linux verfügbar.

Nginx-Ereignisrichtlinie

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
nginx.check-nginx-alive	Überprüft, ob der Nginx-Server aktiv ist.	check-nginx-status.rb **-h, --host** Nginx-Hostname		Erfolgreich CheckNginxStatus OK: Nginx is Alive and healthy

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nginx-Ereignisrichtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	Hinweis: Verwenden Sie für Ereignisse die Standardauthentif	**-P, --Port** Nginx-Port **Hinweis:** Verwenden Sie für Ereignisse die Standardauthentifizierung.		(CheckNginxStatus OK: Nginx ist aktiv und fehlerfrei) Fehler CheckNginxStatus CRITICAL: Nginx is Down (CheckNginxStatus KRITISCH: Nginx ist ausgefallen)

Nginx-Metrikrichtlinie

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
nginx.metrics-nginx-server	Ruft die folgenden Informationen ab: **nginx.active_connections** Gesamtanzahl der aktiven Verbindungen auf dem Server. **nginx.accepts** Die akzeptierten Verbindungen. **nginx.handled** Behandelte Verbindungen, die normalerweise der Anzahl der akzeptierten Verbindungen entsprechen. **nginx.requests** Gesamtanzahl der vom Server	metrics-nginx.rb Optionen: -u --url Vollständige URL zur Serverstatusseite. Beispiel: https://yoursite.com/nginx_status		ws19-INC0047517.nginx.active_connections 1 1640135552 ws19-INC0047517.nginx.accepts 5746 1640135552 ws19-INC0047517.nginx.handled 5746 1640135552 ws19-INC0047517.nginx.requests 9603 1640135552 ws19-INC0047517.nginx.reading 0 1640135552 ws19-INC0047517.nginx.writing 1 1640135552 ws19-INC0047517.nginx.waiting 0 1640135552

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nginx-Metrikrichtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	verarbeiteten Anforderungen. **nginx.read** Zeigt an, ob vom Server Anforderungen gelesen werden. **nginx.writing** Zeigt an, ob vom Server Antworten an den Client geschrieben werden. **nginx.waiting** Inaktive Verbindungen, die auf eine Anforderung warten. **Hinweis:** Verwenden Sie für Metriken die Standardauthentifizierung.			

Automatische Übersetzung

Nginx-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Nginx-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-nginx – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
nginx.active_connections (empfohlene Metrik)	admin	count	Gesamtanzahl der auf dem Server geöffneten Verbindungen, einschließlich wartender Verbindungen (*`nginx.waiting`*-Wert). Sie gibt die Anzahl der aktuellen Benutzer auf der Website wieder. Für einen einzelnen Benutzer können mehrere Verbindungen geöffnet sein.
nginx.accepts (empfohlene Metrik)	admin	count	Stellt die Gesamtanzahl der hergestellten Verbindungen dar, wenn `https://yoursite.com/nginx_status` ausgelöst wird.
nginx.handled (empfohlene Metrik)	admin	count	Gesamtanzahl der vom Nginx-Server verarbeiteten Verbindungen.
nginx.requests (empfohlene Metrik)	admin	count	Gesamtanzahl der vom Nginx-Server verarbeiteten Anforderungen.
nginx.reading (empfohlene Metrik)	admin	count	Aktuelle Anzahl der Verbindungen, bei denen vom Nginx-Server der Anforderungsheader gelesen wird.
nginx.writing (empfohlene Metrik)	admin	count	Stellt die aktuelle Anzahl der Verbindungen dar, bei denen vom Nginx-Server die Antwort an den Client zurückgeschrieben wird.
nginx.waiting (empfohlene Metrik)	admin	count	Anzahl der im Leerlauf befindlichen Clientverbindungen, die auf eine Anforderung warten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für PostgreSQL-Systemüberwachung.

PostgreSQL-Prüfungen

Typ	Prüfung	Beschreibung	Befehl
Event	postgresql.check-alive	Löst eine Warnung zum Status der PostgreSQL-Datenbank aus	commonchecks check-postgres-alive -d {{.labels.params_database}} -p {{.labels.params_port}} -H {{.labels.params_host}}
Event	postgresql.check-connections	Löst basierend auf dem konfigurierten Schwellenwert eine Warnung über die gesamte Verbindungslast in der PostgreSQL-Datenbank aus	commonchecks check-postgres-connections -d {{.labels.params_database}} -c {{.labels.params_critical}} -p {{.labels.params_port}} -H {{.labels.params_host}} -w {{.labels.params_warning}} -a {{.labels.params_use_percentage}}
Metrik	postgresql.metric-active-connections	Stellt Metriken für die gesamte aktive Verbindung in der PostgreSQL-Datenbank bereit	commonchecks metric-postgres-connections -p {{.labels.params_port}} -d {{.labels.params_database}} -H {{.labels.params_host}}
Metrik	postgresql.metric-dbsize	Stellt Metriken zur Gesamtgröße für jede PostgreSQL-Datenbank des Servers bereit	commonchecks metric-postgres-dbsize -d {{.labels.params_database}} -H {{.labels.params_host}} -p {{.labels.params_port}}
Metrik	postgresql.metric-locks	Stellt Metriken für die Sperren für die PostgreSQL-Datenbank/Tabellen bereit	commonchecks metric-postgres-locks -p {{.labels.params_port}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL-Prüfungen (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			-d {{.labels.params_database}} -H {{.labels.params_host}}
Metrik	postgresql.metric-relation-size	Stellt Metriken zur Größe der Datenbanktabelle auf dem Server bereit	commonchecks metric-postgres-relation-size -p {{.labels.params_port}} -l {{.labels.params_limit}} -H {{.labels.params_host}} -d {{.labels.params_database}}
Metrik	postgresql.metric-statsbgwriter	Stellt Metriken im Zusammenhang mit Pufferzuordnungen bereit	commonchecks metric-postgres-statsbgwriter -p {{.labels.params_port}} -d {{.labels.params_database}} -H {{.labels.params_host}}
Metrik	postgresql.metric-statsdb	Stellt Metriken bereit, die sich auf Commits/ Rollbacks/Tupel-Transaktionen/Deadlocks/ Abfragekonflikte beziehen	commonchecks metric-postgres-statsdb -d {{.labels.params_database}} -H {{.labels.params_host}} -p {{.labels.params_port}}
Metrik	postgresql.metric-statsio	Stellt tabellenbasierte Metriken hinsichtlich Indexlesevorgängen/ Gesamttreffer für einen Tabellenindex bereit	commonchecks metric-postgres-statsio -s {{.labels.params_scope}} -H {{.labels.params_host}} -p {{.labels.params_port}} -d {{.labels.params_database}}
Metrik	postgresql.metric-statstable	Stellt Metriken im Zusammenhang mit CRUD-Vorgängen bereit	commonchecks metric-postgres-statstable -d {{.labels.params_database}} -H {{.labels.params_host}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL-Prüfungen (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			-s {{.labels.params_scope}} -p {{.labels.params_port}}

PostgreSQL-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von den angegebenen PostgreSQL-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

postgresql.check-connections-Metriken

Metrik	Beschreibung
pgsql.connections.active (Empfohlene Metrik)	Stellt Metriken für die gesamten aktiven Verbindungen in der PostgreSQL-Datenbank bereit
pgsql.connections.idle (Empfohlene Metrik)	Stellt Metriken für die gesamten inaktiven Verbindungen in der PostgreSQL-Datenbank bereit

postgresql.metric-dbsize-Metriken

Metrik	Beschreibung
pgsql.db.size (Empfohlene Metrik)	Stellt Metriken zur Gesamtauslastung der Laufwerksgröße für jede PostgreSQL-Datenbank auf dem Server bereit

postgresql.metric-locks-Metriken

Metrik	Beschreibung
pgsql.locks.AccessShareLock	Stellt Metriken für den Lesesperrmodus bereit, die automatisch aus abgefragten Tabellen abgerufen werden
pgsql.locks.ExclusiveLock	Stellt Metriken für den Lesesperrmodus bereit, die von der Tabelle LOCK TABLE für IN EXCLUSIVE MODE-Anweisungen abgerufen werden

postgresql.metric-relation-size-Metriken

Metrik	Beschreibung
pgsql.tables_size (Empfohlene Metrik)	Stellt Metriken zur Größe der Datenbanktabelle auf dem Server bereit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsbgwriter-Metriken

Metrik	Beschreibung
pgsql.statsbgwriter.buffers_alloc	Stellt Metriken im Zusammenhang mit der Anzahl zugeordneter Puffer bereit
pgsql.statsbgwriter.buffers_backend	Stellt Metriken bereit, die sich auf die Anzahl der direkt von einem Back-End geschriebenen Puffer beziehen
pgsql.statsbgwriter.buffers_backend_fsync	Stellt Metriken bereit, die sich auf die Häufigkeit beziehen, mit der ein Back-End seinen eigenen fsync-Aufruf ausführen muss (normalerweise verarbeitet der Hintergrund-Writer diese, auch wenn das Back-End seinen eigenen Schreibvorgang durchführt)
pgsql.statsbgwriter.buffers_checkpoint	Stellt Metriken bereit, die sich auf die Anzahl der während Prüfpunkten geschriebenen Puffer beziehen
pgsql.statsbgwriter.buffers_clean	Stellt Metriken bereit, die sich auf die Anzahl der vom Hintergrund-Writer geschriebenen Puffer beziehen
pgsql.statsbgwriter.checkpoint_sync_time	Stellt Metriken bereit, die sich auf die Gesamtzeit in Millisekunden beziehen, die für den Teil der Prüfpunktverarbeitung aufgewendet wurde, bei dem Dateien mit dem Laufwerk synchronisiert werden
pgsql.statsbgwriter.checkpoint_write_time	Stellt Metriken bereit, die sich auf die Gesamtzeit in Millisekunden beziehen, die für den Teil der Prüfpunktverarbeitung aufgewendet wurde, bei dem Dateien auf das Laufwerk geschrieben werden
pgsql.statsbgwriter.checkpoints_req (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der durchgeführten angeforderten Prüfpunkte beziehen
pgsql.statsbgwriter.checkpoints_timed (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der durchgeführten geplanten Prüfpunkte beziehen
pgsql.statsbgwriter.maxwritten_clean	Stellt Metriken bereit, die sich darauf beziehen, wie oft der Hintergrund-Writer einen Reinigungsscan angehalten hat, weil zu viele Puffer geschrieben wurden

postgresql.metric-statsdb-Metriken

Metrik	Beschreibung
pgsql.statsdb.blk_read_time (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Zeit in Millisekunden beziehen, die für das Lesen von Datendateiblöcken durch Back-Ends in dieser Datenbank aufgewendet wurde
pgsql.statsdb.blk_write_time (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Zeit in Millisekunden beziehen, die für das Schreiben von Datendateiblöcken durch Back-Ends in dieser Datenbank aufgewendet wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsdb-Metriken (Fortsetzung)

Metrik	Beschreibung
pgsql.statsdb.blks_hit (Empfohlene Metrik)	Stellt Metriken bereit, die sich darauf beziehen, wie oft Datenträgerblöcke im Puffer-Cache gefunden wurden, sodass kein Lesen erforderlich war. Dies umfasst nur Treffer im PostgreSQL-Puffer-Cache, nicht den Dateisystem-Cache des Betriebssystems.
pgsql.statsdb.blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank gelesenen Datenträgerblöcke beziehen
pgsql.statsdb.checksum_failures	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank (oder in einem gemeinsam genutzten Objekt) erkannten Prüfsummenfehler für Datenseiten beziehen, oder 0, wenn Datenprüfsummen nicht aktiviert sind
pgsql.statsdb.conflicts	Stellt Metriken bereit, die sich auf die Anzahl der Abfragen beziehen, die aufgrund von Konflikten mit der Wiederherstellung in dieser Datenbank abgebrochen wurden. Konflikte treten nur auf Standby-Servern auf.
pgsql.statsdb.deadlocks (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank erkannten Deadlocks beziehen
pgsql.statsdb.numbackends	Stellt Metriken bereit, die sich auf die Anzahl der aktuell mit dieser Datenbank verbundenen Back-Ends beziehen. Dies ist die einzige Spalte in dieser Ansicht, die einen Wert zurückgibt, der den aktuellen Status widerspiegelt. Alle anderen Spalten geben die kumulierten Werte seit dem letzten Zurücksetzen zurück.
pgsql.statsdb.temp_bytes	Stellt Metriken bereit, die sich auf die Gesamtmenge der Daten beziehen, die durch Abfragen in dieser Datenbank in temporäre Dateien geschrieben wurden. Alle temporären Dateien werden gezählt, unabhängig davon, warum die temporäre Datei erstellt wurde, und unabhängig von der Einstellung `log_temp_files`.
pgsql.statsdb.temp_files	Stellt Metriken bereit, die sich auf die Anzahl der temporären Dateien beziehen, die durch Abfragen in dieser Datenbank erstellt wurden. Alle temporären Dateien werden gezählt, unabhängig davon, warum die temporäre Datei erstellt wurde (wie zum Sortieren oder zur Hash-Generierung), und unabhängig von der Einstellung `log_temp_files`.
pgsql.statsdb.tup_deleted	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank gelöscht wurden
pgsql.statsdb.tup_fetched	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank abgerufen wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsdb-Metriken (Fortsetzung)

Metrik	Beschreibung
pgsql.statsdb.tup_inserted	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank eingefügt wurden
pgsql.statsdb.tup_returned	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank zurückgegeben wurden
pgsql.statsdb.tup_updated	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank aktualisiert wurden
pgsql.statsdb.xact_commit	Stellt Metriken bereit, die sich auf die Anzahl der Transaktionen in dieser Datenbank beziehen, für die ein Commit ausgeführt wurde
pgsql.statsdb.xact_rollback	Stellt Metriken bereit, die sich auf die Anzahl der Transaktionen in dieser Datenbank beziehen, für die ein Rollback ausgeführt wurde.

postgresql.metric-statsio-Metriken

Metrik	Beschreibung
pgsql.statsio.heap_blks_hit (Empfohlene Metrik)	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in dieser Tabelle bereit
pgsql.statsio.heap_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.idx_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in allen Indizes dieser Tabelle bereit
pgsql.statsio.idx_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in allen Indizes dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.tidx_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern im TOAST-Tabellenindex (sofern vorhanden) dieser Tabelle bereit
pgsql.statsio.tidx_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der im TOAST-Tabellenindex dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.toast_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in der TOAST-Tabelle (sofern vorhanden) dieser Tabelle bereit
pgsql.statsio.toast_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in der TOAST-Tabelle (falls vorhanden) dieser Tabelle gelesenen Datenträgerblöcke beziehen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsio-Metriken

Metrik	Beschreibung
pgsql.statstable.idx_scan	Stellt Metriken im Zusammenhang mit der Anzahl von Index-Scans bereit, die für diese Tabelle initiiert wurden
pgsql.statstable.idx_tup_fetch	Stellt Metriken bereit, die sich auf die Anzahl der aktiven Zeilen beziehen, die durch Index-Scans abgerufen wurden
pgsql.statstable.n_dead_tup	Stellt Metriken im Zusammenhang mit der geschätzten Anzahl inaktiver Zeilen bereit
pgsql.statstable.n_live_tup	Stellt Metriken im Zusammenhang mit der geschätzten Anzahl aktiver Zeilen bereit
pgsql.statstable.n_tup_del	Stellt Metriken im Zusammenhang mit der Anzahl gelöschter Zeilen bereit
pgsql.statstable.n_tup_hot_upd	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die im laufenden Betrieb aktualisiert wurden (wobei keine separate Indexaktualisierung erforderlich war)
pgsql.statstable.n_tup_ins	Stellt Metriken im Zusammenhang mit der Anzahl eingefügter Zeilen bereit
pgsql.statstable.n_tup_upd	Stellt Metriken im Zusammenhang mit der Anzahl aktualisierter Zeilen bereit
pgsql.statstable.seq_scan	Stellt Metriken im Zusammenhang mit der Anzahl von sequenziellen Scans bereit, die für diese Tabelle initiiert wurden
pgsql.statstable.seq_tup_read	Stellt Metriken bereit, die sich auf die Anzahl der aktiven Zeilen beziehen, die durch sequenzielle Scans abgerufen wurden

RabbitMQ – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die RabbitMQ-Systemüberwachung. Sie müssen die RabbitMQ-Erkennung durchführen, bevor Sie die Prüfungen ausführen. RabbitMQ-Prüfungen sind nur in einer Windows-Umgebung verfügbar.

Richtlinie für RabbitMQ-Ereignisse

Typ	Prüfung	Beschreibung	Befehl
Event	check-rabbitmq-alive	Überprüft mithilfe der REST-API, ob der RabbitMQ-Server aktiv ist. Wenn der Server inaktiv ist, wird eine Warnung ausgelöst.	`check-rabbitmq-alive.rb --host {{.labels.params_host}} --port {{.labels.params_port}} -v {{.labels.params_vhost}}`
Event	check-rabbitmq-cluster-health	Überprüft, ob die Clusterknoten des	`check-rabbitmq-cluster-`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
		RabbitMQ-Servers ausgeführt werden. Wenn die Knoten inaktiv sind, wird eine Warnung ausgelöst.	health.rb --host {{.labels.params_host}} --port {{.labels.params_port}}
Event	check-rabbitmq-consumers	Überprüft die Anzahl der Verbraucher auf dem RabbitMQ-Server und löst eine Warnung basierend auf dem konfigurierten Schwellenwert aus.	check-rabbitmq-consumers.rb {{if .labels.params_warn}} --warn {{.labels.params_warn}} {{end}} {{if .labels.params_critical}} --critical {{.labels.params_critical}} {{end}} --host {{.labels.params_host}} --port {{.labels.params_port}}
Event	check-rabbitmq-messages	Überprüft die Gesamtanzahl der Nachrichten in der Warteschlange auf dem RabbitMQ-Server und löst eine Warnung basierend auf dem Schwellenwert aus.	check-rabbitmq-messages.rb --critical {{.labels.params_critical}} --port {{.labels.params_port}} --warn {{.labels.params_warn}} --host {{.labels.params_host}}
Event	check-rabbitmq-network-partitions	Überprüft, ob die RabbitMQ-Netzwerkpartitionierung aufgetreten ist, und löst eine Warnung basierend auf dem Schwellenwert aus.	check-rabbitmq-network-partitions.rb --host {{.labels.params_host}} --port {{.labels.params_port}}
Event	check-rabbitmq-node-health	Überprüft, ob der RabbitMQ-Serverknoten den Status der Ausführung aufweist.	check-rabbitmq-node-health.rb --host {{.labels.params_host}} {{if .labels.params_watchalarms}} --alarms {{.labels.params_watchalarms}} {{end}} {{if .labels.params_socketwarn}} --swarn {{.labels.params_socketwarn}} {{end}}

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			{{if .labels.params_memcrit}} --mcrit {{.labels.params_memcrit}} {{end}} {{if .labels.params_fdcrit}} --fcrit {{.labels.params_fdcrit}} {{end}} {{if .labels.params_socketcrit}} --scrit {{.labels.params_socketcrit}} {{end}} --port {{.labels.params_port}} {{if .labels.params_memwarn}} --mwarn {{.labels.params_memwarn}} {{end}} {{if .labels.params_fdwarn}} --fwarn {{.labels.params_fdwarn}} {{end}}
Event	check-rabbitmq-node-usage	Überprüft die Nutzung des RabbitMQ-Serverknotens und zeigt sie an.	check-rabbitmq-node-usage.rb {{if .labels.params_procwarn}} --pwarn {{.labels.params_procwarn}} {{end}} --port {{.labels.params_port}} {{if .labels.params_socketwarn}} --swarn {{.labels.params_socketwarn}} {{end}} --type {{.labels.params_type}} {{if .labels.params_diskcrit}} --dcrit {{.labels.params_diskcrit}} {{end}} {{if .labels.params_fdcrit}} --fcrit {{.labels.params_fdcrit}} {{end}} {{if .labels.params_proccrit}} --pcrit {{.labels.params_pr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			occrit}} {{end}} {{if .labels.params_diskwarn}} --dwarn {{.labels.params_diskwarn}} {{end}} {{if .labels.params_socketcrit}} --scrit {{.labels.params_socketcrit}} {{end}} --host {{.labels.params_host}} {{if .labels.params_memcrit}} --mcrit {{.labels.params_memcrit}} {{end}} {{if .labels.params_fdwarn}} --fwarn {{.labels.params_fdwarn}} {{end}} {{if .labels.params_memwarn}} mwarn {{.labels.params_memwarn}} {{end}}
Event	check-rabbitmq-queue-drain-time	Überprüft die Zeit, die jede Warteschlange auf dem RabbitMQ-Server zum Leeren benötigt, basierend auf der aktuellen Nachrichtenausgangsrate. Wenn eine Warteschlange beispielsweise 1.000 Nachrichten enthält, aber nur 1 Nachricht pro Sekunde die Warteschlange verlässt, wird eine Warnung generiert, da die standardmäßig auf 360 Sekunden festgelegte Warnstufe „kritisch“ überschritten wurde.	check-rabbitmq-queue-drain-time.rb --host {{.labels.params_host}} --port {{.labels.params_port}} --warn {{.labels.params_warn}} --critical {{.labels.params_critical}}
Event	check-rabbitmq-queues-synchronised	Überprüft, ob alle gespiegelten Warteschlangen	check-rabbitmq-queues-synchronised.rb --host

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
		mit sekundären Warteschlangen synchronisiert sind.	{{.labels.params_host}} --port {{.labels.params_port}}
Event	check-rabbitmq-stomp-alive	Überprüft, ob der RabbitMQ-Server aktiv ist und auf STOMP reagiert.	check-rabbitmq-stomp-alive.rb --host {{.labels.params_host}} --queue {{.labels.params_queue}} --port {{.labels.params_port}}

Richtlinie für RabbitMQ-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	metrics-rabbitmq-overview	Stellt RabbitMQ-Übersichtsstatistiken bereit.	metrics-rabbitmq-overview.rb --port {{.labels.params_port}} --host {{.labels.params_host}}
Metrik	metrics-rabbitmq-queue	Stellt RabbitMQ-Metriken pro Warteschlange bereit.	metrics-rabbitmq-queue.rb --port {{.labels.params_port}} --host {{.labels.params_host}} {{if .labels.params_vhost}} --vhost {{.labels.params_vhost}} {{end}}

RabbitMQ-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von RabbitMQ-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

metrics-rabbitmq-overview – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.queue_totals.messages.count		count	Stellt Metriken zur Gesamtanzahl der Nachrichten bereit (bereit und nicht bestätigt).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-overview – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.queue_totals.messages.rate (empfohlene Metrik)		Rate/Sek.	Stellt Metriken zur Gesamtanzahl der Nachrichten bereit (bereit und nicht bestätigt)
rabbitmq.queue_totals.messages_ready.count		count	Stellt Metriken zur Anzahl der zur Zustellung bereiten Nachrichten bereit.
rabbitmq.queue_totals.messages_ready.rate		Rate/Sek.	Stellt Metriken zur Anzahl der zur Zustellung bereiten Nachrichten bereit.
rabbitmq.queue_totals.messages_unacknowledged.count		count	Stellt Metriken zur Anzahl der nicht bestätigten Nachrichten bereit.
rabbitmq.queue_totals.messages_unacknowledged.rate		Rate/Sek.	Stellt Metriken zur Anzahl der nicht bestätigten Nachrichten bereit.
rabbitmq.message_stats.deliver_get.count		count	Stellt Metriken zu Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_get.rate (empfohlene Metrik)		Rate/Sek.	Stellt Metriken zu Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_no_ack.count		count	Stellt Metriken zu nicht bestätigten Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_no_ack.rate		Rate/Sek.	Stellt Metriken zu nicht bestätigten Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.publish.count		count	Stellt Metriken zu kürzlich veröffentlichten Nachrichten bereit.
rabbitmq.message_stats.publish.rate		Rate/Sek.	Stellt Metriken zu den kürzlich veröffentlichten Nachrichten bereit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-overview – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.object_totals.channels.count		count	Stellt Metriken zur Gesamtanzahl der Kanäle bereit.
rabbitmq.object_totals.connections.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Verbindungen bereit.
rabbitmq.object_totals.consumers.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Verbraucher bereit.
rabbitmq.object_totals.exchanges.count		count	Stellt Metriken zur Gesamtanzahl der Austauschvorgänge bereit.
rabbitmq.object_totals.queues.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Warteschlangen bereit.

metrics-rabbitmq-queue – Metriken

rabbitmq.queue.{{QueueName}}.avg_egress_rate (empfohlene Metrik)	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Rate bereit, mit der nicht bestätigte Nachrichtendatensätze in den Arbeitsspeicher für die angegebene Warteschlange gelangen.
rabbitmq.queue.{{QueueName}}.consumers	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Gesamtanzahl der Verbraucher für die angegebene Warteschlange bereit.
rabbitmq.queue.{{QueueName}}.messages	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Gesamtanzahl der Nachrichten in der angegebenen Warteschlange bereit.
rabbitmq.queue.{{QueueName}}.drain_time	Abfragename	count	Stellt warteschlangenspezifische Metriken zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-queue – Metriken (Fortsetzung)

			Nachrichtenabflusszeit für die angegebene Warteschlange bereit.

Standardprüfungen und -Richtlinien der URL-Überwachung

Agent Client Collector Stellt Richtlinien für die URL-Überwachung bereit. Richtlinien enthalten eingebettete Prüfungen.

Die URL-Überwachung verwendet die Standardrichtlinien für HTTP-Einstiegspunkt. Details finden Sie unter HTTP – Standardprüfungen und Richtlinien.

Varnish – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die Varnish-Systemüberwachung.

Richtlinie für Varnish-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	app.varnish.metrics-varnish	Sammelt Varnish-Metriken vom Host.	linuxchecks metrics-varnish (Optionen) wobei: • -t = fields – Liste der erforderlichen Metriken, durch Kommas getrennt, zwischen "" • -v = varnishname – Die Varnish-Instanz, aus der Daten abgerufen werden sollen.	hostname.MAIN_sess_conn 175 1649420020 hostname.MAIN_sess_drop 0 1649420020 hostname.MAIN_client_req 173 1649420020 hostname.MAIN_cache_hit 0 1649420020 hostname.MAIN_cache_hitpass 0 1649420020 hostname.MAIN_cache_miss 167 1649420020 hostname.MAIN_backend_conn 0 1649420020 hostname.MAIN_backend_unhealthy 0 1649420020 hostname.MAIN_backend_b

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Varnish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
				usy 0 1649420020 hostname.MAIN_backend_fail 171 1649420020 hostname.MAIN_backend_reuse 0 1649420020 hostname.MAIN_backend_recycle 0 1649420020 hostname.MAIN_threads 200 1649420020 hostname.MAIN_threads_limited 0 1649420020 hostname.MAIN_threads_created 200 1649420020 hostname.MAIN_threads_failed 0 1649420020 hostname.MAIN_thread_queue_len 0 1649420020 hostname.MAIN_sess_queued 0 1649420020 hostname.MAIN_n_expired 167 1649420020 hostname.MAIN_n_lru_nuked 0 1649420020 hostname.MAIN_backend_req 0 1649420020

Automatische Übersetzung

Varnish-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Varnish-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Varnish-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
MAIN_sess_conn (empfohlene Metrik)		count	Kumulative Anzahl der akzeptierten Clientverbindungen nach Varnish-Cache.
MAIN_sess_drop (empfohlene Metrik)		count	Anzahl der Verbindungen, die aufgrund einer vollen Warteschlange getrennt wurden.
MAIN_client_req (empfohlene Metrik)		count	Kumulative Anzahl der empfangenen Clientanforderungen. Wird schrittweise erhöht, nachdem eine Anforderung empfangen wurde, aber bevor eine Antwort von Varnish erfolgt.
MAIN_cache_hit		count	Kumulative Anzahl, die angibt, wie oft eine Datei aus dem Cache von Varnish bereitgestellt wurde.
MAIN_cache_hitpass		count	Kumulative Anzahl von Treffern für eine Datei vom Typ „pass“.
MAIN_cache_miss		count	Kumulative Anzahl, die angibt, wie oft eine Datei angefordert wurde, sich aber nicht im Cache befand und daher vom Back-End angefordert wurde.
MAIN_backend_conn		count	Kumulative Anzahl erfolgreicher TCP-Verbindungen mit dem Back-End.
MAIN_backend_unhealthy (empfohlene Metrik)		count	Kumulative Anzahl der Back-End-Verbindungen, bei denen nicht versucht wurde, sie herzustellen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			da das Back-End als fehlerhaft markiert wurde.
MAIN_backend_busy		count	Kumulative Anzahl der Fälle, in denen die maximale Anzahl von Verbindungen mit dem Back-End erreicht wurde.
MAIN_backend_fail (empfohlene Metrik)		count	Kumulative Anzahl der fehlgeschlagenen Verbindungen mit dem Back-End.
MAIN_backend_reuse (empfohlene Metrik)		count	Kumulative Anzahl der Verbindungen, die aus dem Keep Alive-Pool wiederverwendet wurden.
MAIN_backend_recycle		count	Kumulative Anzahl der aktuellen Back-End-Verbindungen, die in einen Pool von Keep Alive-Verbindungen zurückversetzt und noch nicht verwendet wurden.
MAIN_threads (empfohlene Metrik)		count	Anzahl der Threads in allen Pools.
MAIN_threads_limited		count	Anzahl, die angibt, wie oft ein Thread erstellt werden musste, aber nicht konnte, weil die für varnishd konfigurierte Kapazität für neue Threads ausgeschöpft wurde.
MAIN_threads_created		count	Anzahl der Erstellungen eines Threads.
MAIN_threads_failed (empfohlene Metrik)		count	Anzahl der erfolglosen Versuche von Varnish, einen Thread zu erstellen.
MAIN_thread_queue_len		count	Aktuelle Warteschlangenlänge: Anzahl der Anforderungen, die im Worker Thread darauf warten, verfügbar zu werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
MAIN_sess_queued		count	Anzahl, die angibt, wie oft in Varnish keine Threads mehr vorhanden waren und eine Anforderung in die Warteschlange gestellt werden musste.
MAIN_n_expired (empfohlene Metrik)		count	Kumulative Anzahl abgelaufener Objekte, z. B. aufgrund von TTL.
MAIN_n_lru_nuked (empfohlene Metrik)		count	Least Recently Used Nuked Objects (Am längsten nicht verwendete entfernte Objekte): Kumulative Anzahl der zwischengespeicherten Objekte, die von Varnish aufgrund von Platzmangel aus dem Cache entfernt wurden.
MAIN_backend_req (empfohlene Metrik)		count	Anzahl der Anforderungen an das Back-End.

vSphere – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die vSphere-Systemüberwachung.

Richtlinie für Metriken für virtuelle vSphere-Maschinen

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vsphere.metric-VirtualMachine	Ruft Metriken für eine virtuelle vSphere-Maschine ab. Muss einen Proxy-Agent verwenden.	commonchecks metric-vsphere -H hostname -R VirtualMachine -v vm_id -r true -i 20 wobei: • -H = hostname – Instanz-Hostname • -i = intervalld – 20 für	vsphere.VirtualMachine.disk.usage 8 1654755994

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Metriken für virtuelle vSphere-Maschinen (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
			Echtzeitmetriken; 300 für 5 Minuten ältere zusammengefasste Metriken (Standardwert: 300) • -r = resourceLevelMetric – Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	

Richtlinie für vSphere-Datastore-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vSphere.metric-Datastore	Ruft Metriken für vSphere-Datastore ab. Muss einen Proxy-Agent verwenden.	commonchecks metric-vsphere -H hostname -R Datastore -v vm_id -r wobei: • -H = hostname – Instanz-Hostname • -r = resourceLevelMetric – Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	vsphere.Datastore.disk.capacity.lat 21474836480 1655182836

Richtlinie für vSphere-Datencenter-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vsphere.metric-Datacenter	Ruft Metriken für das vSphere-Datencenter ab.	commonchecks metric-vsphere -H hostname -R Datacenter -v vm_id -r	vsphere.Datacenter.vmop.numChangeDS.latest.total 217 1655194924

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für vSphere-Datencenter-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
			wobei: • -H = hostname – Instanz-Hostname • -r = resourceLevelMe Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	vsphere.Datacenter.vmop.numChangeHost.latest.total 1373 1655194924 vsphere.Datacenter.vmop.numChangeHostDS.latest.total 9 1655194924 vsphere.Datacenter.vmop.numClone.latest.total 192 1655194924

Richtlinie für vSphere ESX-Server-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vsphere.metric-ESX_Server	Ruft Metriken für vSphere ESX-Server oder -Hostsystem ab. Muss einen Proxy-Agent verwenden.	commonchecks metric-vsphere -H hostname -R HostSystem -v vm_id -r wobei: • -H = hostname – Instanz-Hostname • -r = resourceLevelMe Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	vsphere.HostSystem.net.broadcastRx.summation.total 63885 1655198166 vsphere.HostSystem.net.broadcastTx.summation.total 196 1655198166 vsphere.HostSystem.net.bytesRx.average.total 5924 1655198166

vSphere-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von vSphere-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
net.broadcastRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Broadcast-Pakete.
net.broadcastTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Broadcast-Pakete.
net.bytesRx.average	Netzwerkadapter	KiB	Durchschnittliche Menge der pro Sekunde empfangenen Daten.
net.bytesTx.average	Netzwerkadapter	KiB	Durchschnittliche Menge der pro Sekunde übertragenen Daten.
net.droppedRx.summation	Netzwerkadapter	Pakete	Anzahl der verworfenen empfangenen Pakete.
net.droppedTx.summation	Netzwerkadapter	Pakete	Anzahl der verworfenen übertragenen Pakete.
net.multicastRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Multicast-Pakete.
net.multicastTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Multicast-Pakete.
net.packetsRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Pakete.
net.packetsTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Pakete.
net.received.average	Netzwerkadapter	KiB	Durchschnittliche Rate, mit der Daten während des Intervalls empfangen wurden. Dies stellt die Bandbreite des Netzwerks dar.
net.transmitted.average	Netzwerkadapter	KiB	Durchschnittliche Rate, mit der Daten während des Intervalls übertragen wurden. Dies stellt die Bandbreite des Netzwerks dar.
net.usage.average (empfohlene Metrik)	Netzwerkadapter	KiB	Netzwerkauslastung (kombinierte Übertragungs- und Empfangsraten).
disk.maxTotalLatency.latest (empfohlene Metrik)	Laufwerk	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Festplatten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.read.average	Laufwerk	KiB	Durchschnittliche Anzahl der pro Sekunde von der Festplatte gelesenen Kilobytes.
disk.usage.average (empfohlene Metrik)	Laufwerk	KiB	Aggregierte Festplatten-E/A-Rate.
disk.usage.maximum	Laufwerk	KiB	Maximale Festplatten-E/A-Rate.
disk.usage.minimum	Laufwerk	KiB	Minimale Festplatten-E/A-Rate.
disk.write.average	Laufwerk	KiB	Durchschnittliche Anzahl der pro Sekunde auf die Festplatte geschriebenen Kilobytes.
cpu.costop.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine zur Ausführung bereit ist, aber aufgrund von Co-Scheduling-Einschränkungen nicht ausgeführt werden kann.
cpu.demand.average	cpu-core	Megahertz	Menge der CPU-Ressourcen, die von einer virtuellen Maschine verwendet würde, wenn es keinen CPU-Konflikt oder kein CPU-Limit gäbe.
cpu.demandEntitlementRatio.latest	cpu-core	Prozent	Verhältnis von CPU-Ressourcenberechtigung zu CPU-Bedarf.
cpu.entitlement.latest	cpu-core	Megahertz	Vom ESXi-Planer bereitgestellte CPU-Ressourcen.
cpu.idle.summation	cpu-core	Millisekunde	Gesamtzeit, die die CPU im Leerlauf verbracht hat.
cpu.latency.average	cpu-core	Prozent	Prozentsatz der Zeit, während der die virtuelle Maschine nicht ausgeführt werden kann, da sie um Zugriff auf die physische(n) CPU(s) konkurriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.maxlimited.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine zur Ausführung bereit ist, aber nicht ausgeführt wird, da der festgelegte Höchstwert des CPU-Limits erreicht ist.
cpu.overlap.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine unterbrochen wurde, damit von ihr Systemservices für sich selbst oder für andere virtuelle Maschinen ausgeführt werden konnten.
cpu.readiness.average	cpu-core	Prozent	Prozentsatz der Zeit, während der die virtuelle Maschine bereit war, die Ausführung auf der physischen CPU jedoch nicht geplant werden konnte.
cpu.ready.summation	cpu-core	Millisekunde	CPU-Zeit (in Millisekunden) im Status „Bereit“.
cpu.run.summation	cpu-core	Millisekunde	Zeit, zu der die Ausführung der virtuellen Maschine geplant ist.
cpu.swapwait.summation	cpu-core	Millisekunde	CPU-Zeit, während der darauf gewartet wird, dass auf die Festplatte ausgelagerte Prozesse zur Ausführung in den Arbeitsspeicher abgerufen werden (Swap-in).
cpu.system.summation	cpu-core	Millisekunde	Zeit, die für Systemprozesse auf jeder virtuellen CPU in der virtuellen Maschine aufgewendet wird.
cpu.usage.average (empfohlene Metrik)	cpu-core	Prozent	Prozentsatz der verwendeten CPU-Kapazität.
cpu.usagemhz.average	cpu-core	Megahertz	CPU-Auslastung, gemessen in Megahertz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.used.summation	cpu-core	Millisekunde	Zeit, die der virtuellen Maschine zugerechnet wird. Wenn ein Systemservice für diese virtuelle Maschine ausgeführt wird, sollte die von diesem Service aufgewendete Zeit (abgebildet durch cpu.system) dieser virtuellen Maschine in Rechnung gestellt werden. Wenn nicht, sollte die aufgewendete Zeit (abgebildet durch cpu.overlap) nicht dieser virtuellen Maschine berechnet werden.
cpu.wait.summation (empfohlene Metrik)	cpu-core	Millisekunde	Gesamte CPU-Zeit im Wartestatus. Die Gesamtwartezeit umfasst die Zeit, die in den Status „CPU-Leerlauf“, „CPU-Swap-Wartezeit“ und „CPU-E/A-Wartezeit“ verbracht wurde.
cpu.usage.vcpus.average	cpu-core	Prozent	Prozentsatz der verwendeten Kapazität virtueller CPUs.
cpu.utilization.average	cpu-core	Prozent	Prozentsatz der verwendeten CPU-Kapazität.
mem.active.average	memory	KiB	Aktiv genutzte Arbeitsspeichermenge, die von VMkernel basierend auf kürzlich bearbeiteten Arbeitsspeicherseiten geschätzt wird.
mem.activewrite.average	memory	KiB	Geschätzte Menge des Arbeitsspeichers, in den von der virtuellen Maschine aktiv geschrieben wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.compressed.average	memory	KiB	Arbeitsspeichermenge (in Kilobyte), die komprimiert wurde.
mem.compressionRate.average	memory	KiB	Rate der Arbeitsspeicherkomprimierung für die virtuelle Maschine.
mem.consumed.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, der von einer virtuellen Maschine, einem Host oder einem Cluster verbraucht wird.
mem.decompressionRate.average	memory	KiB	Rate der Arbeitsspeicherdekomprimierung für die virtuelle Maschine.
mem.entitlement.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, die die virtuelle Maschine beanspruchen kann, wie vom ESX Scheduler festgelegt.
mem.granted.average	memory	KiB	Menge des physischen Hostarbeitsspeichers oder des physischen Arbeitsspeichers, die einer virtuellen Maschine oder einem Host zugeordnet ist.
mem.latency.average	memory	KiB	Prozentsatz der Zeit, während der die virtuelle Maschine auf den Zugriff auf den ausgelagerten oder komprimierten Arbeitsspeicher wartet.
mem.llSwapInRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom Host-Cache in den aktiven Arbeitsspeicher ausgelagert wird.
mem.llSwapOutRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom aktiven Arbeitsspeicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			in den Host-Cache ausgelagert wird.
mem.llSwapUsed.average	memory	KiB	Platz, der zum Zwischenspeichern ausgelagerter Seiten im Host-Cache verwendet wird.
mem.overhead.average	memory	KiB	Physischer Hostarbeitsspeicher, der von der Virtualisierungsinfrastruktur für die Ausführung der virtuellen Maschine verbraucht wird.
mem.overheadMax.average	memory	KiB	Physischer Hostarbeitsspeicher, der für die Verwendung als Virtualisierungs-Overhead für die virtuelle Maschine reserviert ist.
mem.overheadTouched.average	memory	KiB	Aktiv belegter Overhead des physischen Hostarbeitsspeichers (KB), der für die Verwendung als Virtualisierungs-Overhead für die virtuelle Maschine reserviert ist.
mem.shared.average	memory	KiB	Menge des physischen Gastarbeitsspeichers, der mit anderen virtuellen Maschinen gemeinsam genutzt wird, bezogen auf eine einzelne virtuelle Maschine oder auf alle eingeschalteten virtuellen Maschinen auf einem Host.
mem.usage.average (empfohlene Metrik)	memory	Prozent	Arbeitsspeichernutzung als Prozentsatz des insgesamt konfigurierten oder verfügbaren Arbeitsspeichers.
mem.vmmemctl.average	memory	KiB	Menge des Arbeitsspeichers, die vom Treiber für die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Arbeitsspeichersteuerung der virtuellen Maschine zugeordnet wird.
mem.vmmemctltarget.average	memory	KiB	Von VMkernel festgelegter Zielwert für die Arbeitsspeicher-Balloon-Größe der virtuellen Maschine. In Verbindung mit der Metrik vmmemctl wird diese Metrik von VMkernel dazu verwendet, die Balloon-Größe für eine virtuelle Maschine zu erhöhen oder zu verringern.
mem.zero.average	memory	KiB	Arbeitsspeicher, der nur Nullen enthält. In der gemeinsamen Menge enthalten. Durch die transparente gemeinsame Seitennutzung (Transparent Page Sharing, TPS) können Speicherseiten, die nur Nullen enthalten, von virtuellen Maschinen, auf denen dasselbe Betriebssystem ausgeführt wird, gemeinsam genutzt werden.
power.energy.summation	Strom	Joule	Gesamte Energie (in Joule), die seit dem letzten Zurücksetzen der Statistik verbraucht wurde.
power.power.average	Strom	Watt	Aktueller Stromverbrauch.
sys.heartbeat.latest	System	Nummer	Anzahl der pro virtueller Maschine ausgegebenen Taktsignale (Heartbeats).
sys.osUptime.latest	System	seconds	Gesamtzeit (in Sekunden) seit dem letzten Start des Betriebssystems.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
sys.uptime.latest	System	seconds	Insgesamt verstrichene Zeit seit dem letzten Systemstart.
virtualDisk.read.average	virtuelle Festplatte	KiB	Durchschnittliche Anzahl der pro Sekunde von der virtuellen Festplatte gelesenen Kilobytes.
virtualDisk.write.average	virtuelle Festplatte	KiB	Durchschnittliche Anzahl der pro Sekunde auf die virtuelle Festplatte geschriebenen Kilobytes.
rescpu.actav1.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 1 Minute.
rescpu.actav15.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 15 Minuten.
rescpu.actav5.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 5 Minuten.
escpu.actpk1.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 1 Minute.
rescpu.actpk15.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 15 Minuten.
rescpu.actpk5.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 5 Minuten.
rescpu.runav1.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 1 Minute.
rescpu.runav15.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 15 Minuten.
rescpu.runav5.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 5 Minuten.
rescpu.runpk1.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 1 Minute.
rescpu.runpk15.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 15 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rescpu.runpk5.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 5 Minuten.
rescpu.sampleCount.latest	rescpu	Millisekunde	CPU-Abtastrate für Gruppe.
rescpu.samplePeriod.latest	rescpu	Millisekunde	CPU-Abtastzeitraum für Gruppe.

vsphere.metric-Datacenter – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmop.numChangeDS.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Datenspeicher-Änderungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numChangeHost.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Hoständerungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numChangeHostDS.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Host- und Datenspeicher-Änderungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numClone.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Klonvorgänge für die virtuelle Maschine.
vmop.numCreate.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Erstellungsvorgänge für die virtuelle Maschine.
vmop.numDeploy.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorlagenbereitstellungsvorgänge für die virtuelle Maschine.
vmop.numDestroy.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Löschvorgänge für die virtuelle Maschine.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datacenter – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmop.numPoweroff.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Ausschaltvorgänge für die virtuelle Maschine.
vmop.numPoweron.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Einschaltvorgänge für die virtuelle Maschine.
vmop.numRebootGuest.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Neustartvorgänge für den VM-Gast.
vmop.numReconfigure.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Neukonfigurationsvorgänge für die virtuelle Maschine.
vmop.numRegister.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Registrierungsvorgänge für die virtuelle Maschine.
vmop.numReset.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Zurücksetzen für die virtuelle Maschine.
vmop.numSVMotion.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Migrationen mit Storage vMotion (Datenspeicher-Änderungsvorgänge für eingeschaltete virtuelle Maschinen).
vmop.numShutdownGuest.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Herunterfahren für den VM-Gast.
vmop.numStandbyGuest.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Standby-Vorgänge für den VM-Gast.
vmop.numSuspend.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Anhalten für die virtuelle Maschine.
vmop.numUnregister.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zur Aufhebung der Registrierung für die virtuelle Maschine.
vmop.numVMotion.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Migrationen mit vMotion (Hosständerungsvorgänge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datacenter – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			für eingeschaltete virtuelle Maschinen).
vmop.numXVMotion.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Host- und Datenspeicher-Änderungsvorgänge für eingeschaltete und angehaltene virtuelle Maschinen.

vsphere.metric-Datastore – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.busResets.summation	Datenspeicher	Nummer	Anzahl der ausgegebenen Befehle zum Zurücksetzen des SCSI-Busses.
datastore.commandsAborted.summation	Datenspeicher	Nummer	Anzahl der abgebrochenen SCSI-Befehle.
datastore.datastoreIops.average	Datenspeicher	Nummer	Aggregierte IOPS für Datenspeicher-E/A-Ressourcenverwaltung (Storage I/O Control).
datastore.datastoreMaxQueueDepth.latest	Datenspeicher	Nummer	Maximale Datenspeicher-Warteschlangentiefe für Datenspeicher-E/A-Ressourcenverwaltung.
datastore.datastoreNormalReadLatency.latest	Datenspeicher	Millisekunde	Normalisierte Leselatenz des Storage DRS-Datenspeichers.
datastore.datastoreNormalWriteLatency.latest	Datenspeicher	Millisekunde	Normalisierte Schreiblatenz des Storage DRS-Datenspeichers.
datastore.datastoreReadBytes.latest	Datenspeicher	Millisekunde	Gelesene Bytes des Storage DRS-Datenspeichers.
datastore.datastoreReadIops.latest	Datenspeicher	Nummer	Rate gelesener E/A-Vorgänge des Storage DRS-Datenspeichers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.datastoreReadLoadMetric.latest	Datenspeicher	Nummer	Storage DRS-Datenspeichermetrik für das Lese-Workload-Modell.
datastore.datastoreReadOIO.latest	Datenspeicher	Nummer	Ausstehende Leseanforderungen des Storage DRS-Datenspeichers.
datastore.datastoreVMObservedLatency.latest	Datenspeicher	Mikrosekunden	Die durchschnittliche Latenz des Datenspeichers aus der Sicht von virtuellen Maschinen.
datastore.datastoreWriteBytes.latest	Datenspeicher	Millisekunde	Geschriebene Bytes des Storage DRS-Datenspeichers.
datastore.datastoreWriteIops.latest	Datenspeicher	Nummer	Rate geschriebener E/A-Vorgänge des Storage DRS-Datenspeichers.
datastore.datastoreWriteLoadMetric.latest	Datenspeicher	Nummer	Storage DRS-Datenspeichermetrik für das Schreib-Workload-Modell.
datastore.datastoreWriteOIO.latest	Datenspeicher	Nummer	Ausstehende Schreibanforderungen des Storage DRS-Datenspeichers.
datastore.maxTotalLatency.latest	Datenspeicher	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Datenspeicher.
datastore.numberReadAveraged.average	Datenspeicher	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Lesebefehle.
datastore.numberWriteAveraged.average	Datenspeicher	Nummer	Durchschnittliche Anzahl der während des Erfassungsintervalls pro Sekunde an den Datenspeicher ausgegebenen Schreibbefehle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.read.average (empfohlene Metrik)	Datenspeicher	KiB	Rate des Lesens von Daten aus dem Datenspeicher.
datastore.siocActiveTimePercentage.average (empfohlene Metrik)	Datenspeicher	Prozent	Prozentsatz der Zeit, während der die Latenz des Datenspeichers aktiv von der Datenspeicher-E/A-Ressourcenverwaltung gesteuert wurde.
datastore.sizeNormalizedDatastoreLatency.average	Datenspeicher	Mikrosekunden	Größennormalisierte E/A-Latenz der Datenspeicher-E/A-Ressourcenverwaltung.
datastore.throughput.contention.average	Datenspeicher	Millisekunde	Durchschnittliche Zeit für einen E/A-Vorgang für den Datenspeicher oder die LUN für alle ESX-Hosts, die darauf zugreifen.
datastore.throughput.usage.average	Datenspeicher	KiB	Aktuelle Bandbreitennutzung für den Datenspeicher oder die LUN.
datastore.totalReadLatency.average	Datenspeicher	Millisekunde	Durchschnittliche Zeitdauer für einen Lesevorgang aus dem Datenspeicher.
datastore.totalWriteLatency.average	Datenspeicher	Millisekunde	Durchschnittliche Zeitdauer für einen Schreibvorgang aus dem Datenspeicher.
datastore.unmapIOs.summation	Datenspeicher	Nummer	Anzahl der Vorgänge zum Aufheben von Zuordnungen.
datastore.unmapSize.summation	Datenspeicher	Nummer	Gesamtgröße des Aufhebens der Zuordnung.
datastore.write.average (empfohlene Metrik)	Datenspeicher	KiB	Rate des Schreibens von Daten in den Datenspeicher.
disk.busResets.summation	disk	Nummer	Anzahl der ausgegebenen Befehle zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Zurücksetzen des SCSI-Busses.
disk.capacity.latest	disk	KiB	Konfigurierte Größe des Datenspeichers.
disk.capacity.contention.average	disk	KiB	Ausmaß der Überbelegung der Speicherkapazität für die Entität, gemessen in Prozent.
disk.capacity.provisioned.average	disk	KiB	Bereitgestellte Größe der Entität.
disk.capacity.usage.average	disk	KiB	Menge der Speicherkapazität, die derzeit von oder in der Entität verbraucht wird.
disk.commands.summation	disk	Nummer	Anzahl der ausgegebenen SCSI-Befehle.
disk.commandsAborted.summation	disk	Nummer	Anzahl der abgebrochenen SCSI-Befehle.
disk.commandsAveraged.average	disk	Nummer	Durchschnittliche Anzahl der pro Sekunde ausgegebenen SCSI-Befehle.
disk.deltaused.latest	disk	KiB	Speicher-Overhead einer virtuellen Maschine oder eines Datenspeichers aufgrund von Delta-Festplattensicherungen.
disk.deviceLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die zum vollständigen Ausführen eines SCSI-Befehls von einem physischen Gerät benötigt wird.
disk.deviceReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die es dauert, bis der Vorgang des Lesens von einem physischen Gerät abgeschlossen ist.
disk.deviceWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die es dauert, bis der Vorgang des Schreibens

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			von einem physischen Gerät abgeschlossen ist.
disk.kernelLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes SCSI-Befehls aufgewendet wird.
disk.kernelReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes SCSI-Lesebefehls aufgewendet wird.
disk.kernelWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes SCSI-Schreibbefehls aufgewendet wird.
disk.maxQueueDepth.average (empfohlene Metrik)	disk	Nummer	Maximale Warteschlangentiefe.
disk.maxTotalLatency.latest	disk	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Festplatten.
disk.numberRead.summation	disk	Nummer	Anzahl der Festplatten-Lesevorgänge während des Erfassungsintervalls.
disk.numberReadAveraged.average	disk	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Lesebefehle.
disk.numberWrite.summation	disk	Nummer	Anzahl der Festplatten-Schreibvorgänge während der Erfassung.
disk.numberWriteAveraged.average	disk	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Schreibbefehle.
disk.provisioned.latest	disk	KiB	Speichermenge, die für die Verwendung durch einen Datenspeicher oder eine virtuelle Maschine reserviert ist. Dateien im Datenspeicher und auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			der virtuellen Maschine können auf diese Größe erweitert werden, jedoch nicht darüber hinaus.
disk.queueLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-Warteschlange (pro SCSI-Befehl) verbracht wird.
disk.queueReadLatency.average (empfohlene Metrik)	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-Warteschlange (pro SCSI-Lesebefehl) verbracht wird.
disk.queueWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-Warteschlange (pro SCSI-Schreibbefehl) verbracht wird.
disk.read.average	disk	KiB	Durchschnittliche Anzahl der pro Sekunde von der Festplatte gelesenen Kilobytes.
disk.scsiReservationCnflctsPct.average	Disk	Nummer	Anzahl der SCSI-Reservierungskonflikte für die LUN als Prozentsatz der gesamten Befehle während des Erfassungsintervalls.
disk.scsiReservationConflicts.summation	disk	Nummer	Anzahl der SCSI-Reservierungskonflikte für die LUN während des Erfassungsintervalls.
disk.throughput.contention.average	disk	Millisekunde	Durchschnittliche Zeit für einen E/A-Vorgang für den Datenspeicher oder die LUN für alle ESX-Hosts, die darauf zugreifen.
disk.throughput.usage.average	disk	KiB	Aktuelle Bandbreitennutzung für den Datenspeicher oder die LUN.
disk.totalLatency.average (empfohlene Metrik)	disk	Millisekunde	Durchschnittliche Zeit, die während des Erfassungsintervalls dafür

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Befehl zu verarbeiten.
disk.totalReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die dafür benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Lesebefehl zu verarbeiten.
disk.totalWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die dafür benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Schreibbefehl zu verarbeiten.
disk.unshared.latest	disk	KiB	Größe des Speicherplatzes, der ausschließlich einer virtuellen Maschine zugeordnet ist.
disk.usage.average (empfohlene Metrik)	disk	KiB	Aggregierte Festplatten-E/A-Rate.
disk.used.latest	disk	KiB	Tatsächlich von der virtuellen Maschine oder dem Datenspeicher verwendeter Speicherplatz. Kann kleiner sein als die zu einem bestimmten Zeitpunkt bereitgestellte Menge, je nachdem, ob die virtuelle Maschine ausgeschaltet ist, ob Snapshots erstellt wurden oder nicht, sowie in Abhängigkeit von anderen derartigen Faktoren.
disk.write.average	disk	KiB	Durchschnittliche Anzahl der pro Sekunde auf die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Festplatte geschriebenen Kilobytes.

vsphere.metric-ESX_Server – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.coreUtilization.average (empfohlene Metrik)	cpu-core	Prozent	CPU-Auslastung des entsprechenden Kerns (wenn Hyper-Threading aktiviert ist) als Prozentsatz.
cpu.reservedCapacity.average	cpu-core	Megahertz	CPU-Gesamtkapazität, die von virtuellen Maschinen reserviert wurde.
cpu.totalCapacity.average	cpu-core	Megahertz	CPU-Gesamtkapazität, die von virtuellen Maschinen reserviert wurde und für diese verfügbar ist.
datastore.maxTotalLatency.latest	datastore	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Datenspeicher.
hbr.hbrDiskReadLatency.average	hostbasierte Replikation	Millisekunde	Durchschnittliche Festplatten-Leselatenz.
hbr.hbrDiskStallLatency.average	hostbasierte Replikation	Millisekunde	Durchschnittliche Verzögerungslatenz der Festplatte.
hbr.hbrNetRx.average	hostbasierte Replikation	KiB	Durchschnittliche Menge der pro Sekunde empfangenen Daten.
hbr.hbrNetTx.average	hostbasierte Replikation	KiB	Durchschnittliche Menge der pro Sekunde übertragenen Daten.
hbr.hbrNumVms.average	hostbasierte Replikation	Nummer	Anzahl der eingeschalteten virtuellen Maschinen, die auf diesem Host ausgeführt werden und für die derzeit der hostbasierte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Replikationsschutz aktiviert ist.
mem.heap.average	memory	KiB	Virtueller VMkernel-Adressraum für den VMkernel-Haupt-Heap und zugehörige Daten.
mem.heapfree.average	memory	KiB	Freier Adressraum im VMkernel-Haupt-Heap. Variiert je nach Anzahl der physischen Geräte und Konfigurationsoptionen.
mem.llSwapIn.average	memory	KiB	Menge des per Swap-in geladenen Arbeitsspeichers aus dem Host-Cache.
mem.llSwapOut.average	memory	KiB	Menge des per Swap-out in den Host-Cache ausgelagerten Arbeitsspeichers.
mem.lowfreethreshold.average	memory	KiB	Schwellenwert für den freien physischen Hostarbeitsspeicher. Unterhalb dieses Schwellenwerts wird von ESX/ESXi mittels Ballooning (Zurückgewinnung und Wiederverwendung von ungenutztem Arbeitsspeicher) und Swapping (Auslagerung von Arbeitsspeicher) damit begonnen, Arbeitsspeicher von virtuellen Maschinen zurückzugewinnen.
mem.reservedCapacity.average	memory	MiB	Gesamtmenge der Arbeitsspeicherreservierung, die von eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host verwendet wird.
mem.sharedcommon.average	memory	KiB	Menge des VM-Arbeitsspeichers, der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			von allen eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host gemeinsam genutzt wird.
mem.state.latest	memory	KiB	Eine von vier Schwellenwertstufen, die den Prozentsatz des freien Arbeitsspeichers auf dem Host darstellen.
mem.swapin.average	memory	KiB	Menge des per Swap-in von der Festplatte geladenen Arbeitsspeichers.
mem.swapinRate.average	memory	KiB	Rate, mit der Arbeitsspeicher von der Festplatte in den aktiven Arbeitsspeicher geladen wird.
mem.swapout.average	memory	KiB	Menge des per Swap-out auf die Festplatte ausgelagerten Arbeitsspeichers.
mem.swapoutRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom aktiven Arbeitsspeicher auf die Festplatte ausgelagert wird.
mem.swapused.average	memory	KiB	Für den Auslagerungsvorgang verwendete Arbeitsspeichermenge. Summe des ausgelagerten Arbeitsspeichers aller eingeschalteten virtuellen Maschinen und vSphere-Dienste auf dem Host.
mem.sysUsage.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, der von VMkernel für Kernfunktionen verwendet wird, z. B. für Gerätetreiber und andere interne Zwecke. Enthält keinen Arbeitsspeicher, der von virtuellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Maschinen oder vSphere-Diensten verwendet wird.
mem.totalCapacity.average	memory	KiB	Gesamtmenge der Arbeitsspeicherreservierung, die von eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host verwendet wird und für diese verfügbar ist.
mem.unreserved.average	memory	KiB	Menge des nicht reservierten Arbeitsspeichers. Arbeitsspeicherreservierung, die nicht von der Servicekonsole, von VMkernel, vSphere-Diensten und anderen eingeschalteten virtuellen Maschinen verwendet wird, benutzerdefinierte Arbeitsspeicherreservierungen und Overhead-Arbeitsspeicher.
mem.vmfs.pbc.capMissRatio.latest (empfohlene Metrik)	memory	Prozent	Nachfolgender Durchschnitt des Verhältnisses von „Capacity Misses“ zu „Compulsory Misses“ für den VMFS-PB-Cache.
mem.vmfs.pbc.overhead.latest	memory	KiB	Menge des VMFS-Heaps, der vom VMFS-PB-Cache verwendet wird.
mem.vmfs.pbc.size.latest	memory	MiB	Platz, der zum Halten von VMFS-Zeigerblöcken im Arbeitsspeicher verwendet wird.
mem.vmfs.pbc.sizeMax.latest	memory	MiB	Maximale Größe, auf die der VMFS-Zeigerblock-Cache anwachsen kann.
mem.vmfs.pbc.workingSet.latest	memory	TiB	Anzahl der Dateiblöcke, deren Adressen im VMFS-PB-Cache zwischengespeichert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.vmfs.pbc.workingSetMax.latest	Maschine	TiB	Maximale Anzahl der Dateiblöcke, deren Adressen im VMFS-PB-Cache zwischengespeichert werden.
net.errorsRx.summation (empfohlene Metrik)	Netzwerkadapter	Nummer	Anzahl der empfangenen Pakete mit Fehlern.
net.errorsTx.summation (empfohlene Metrik)	Netzwerkadapter	Nummer	Anzahl der übertragenen Pakete mit Fehlern.
net.unknownProtos.summation	Netzwerkadapter	KiB	Anzahl der empfangenen Frames mit unbekanntem Protokoll.
power.powerCap.average	Strom	Watt	Maximal zulässiger Stromverbrauch.
rescpu.maxLimited1.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 1 Minute.
rescpu.maxLimited15.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 15 Minuten.
rescpu.maxLimited5.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 5 Minuten.
storageAdapter.maxTotalLatency.latest (empfohlene Metrik)	Speicheradapter	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Speicheradapter.
storagePath.maxTotalLatency.latest (empfohlene Metrik)	Speicheradapter	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Speicherpfade.

Windows – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für Windows-Systemüberwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Ereignisüberwachungsprüfungen

Richtlinie für Windows-Betriebssystemereignisse

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-event-log	Misst Windows Ereignisprotokoll für Parameterschwellenwerte und gibt ein zurück *CRITICAL**WARNING**OK*Ereignis.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die Ereignisprotokollanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn die Ereignisprotokollanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. • -E Ereignisebene: Gibt den Schweregrad des Ereignisses an. Mögliche Werte: Information, ausführlich, Kritisch, Warnung, Fehler. • -i: Eindeutige Ereignis-ID • -D: Die Dauer in Stunden, in der Ereignisse aus abgerufen werden sollen Windows Ereignisprotokoll. Anwendungsbeispiel: Winchecks Check-	Ereignisprotokoll überprüfen OK: Das Ereignisprotokoll, das dem Muster entspricht, ist <matched count>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Windows-event-log -W 5 -c 10 -e „Informationen“ -l „Anwendung“ -d 24	
os.windows.check-event-log-count	Misst Windows Ereignisprotokoll für Parameterschwellenwerte und gibt ein KRITISCHES \WARNENDES\OK-Ereignis zurück. Stellt Informationen zur Anzahl der Ereignisse bereit, die innerhalb einer angegebenen Dauer für eine einzelne Protokolldatei und eine einzelne ID aufgetreten sind. Gibt auch die Filter an, die zum Abrufen von Ereignissen für eine bestimmte einwertige Windows-Ereignisebene und den Anbieternamen angewendet werden sollen. Das Abrufen von Ereignissen aus mehreren Protokolldateien wird nicht unterstützt. Die Anzahl der Ereignisse wird angegeben, ohne Details zu jedem Ereignis.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die Ereignisprotokollanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn die Ereignisprotokollanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. • -L log_file: Die zu überwachende Protokolldatei. Der Name der Datei wird in doppelte Anführungszeichen geschrieben. • -R regex_pattern: Das Muster des regulären Ausdrucks, das die Beschreibung im Ereignisprotokoll herausfiltert. In doppelte Anführungszeichen geschrieben.	Ereignisprotokoll überprüfen OK: Das Ereignisprotokoll, das dem Muster entspricht, ist <matched count>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		• -E Ereignisebene: Gibt den Schweregrad des Ereignisses an. Mögliche Werte: Information, ausführlich, Kritisch, Warnung, Fehler. • -i-ID: Eindeutige Ereignis-ID • -D duration_Hour: Die Dauer in Stunden, in der Ereignisse aus abgerufen werden sollen Windows Ereignisprotokoll. Dezimalstellen können verwendet werden, z. B. 30 Minuten bis 0,5. • -P Provider_Name: Quelle des Ereignisses, in doppelte Anführungszeichen geschrieben. Anwendungsbeispiel: `Winchecks Check-Windows-event-log -W 5 -c 10 -e „Informationen“ -l „Anwendung“ -d 24`	
os.windows.check-event-log-details	Erfasst und filtert Windows-Ereignisprotokolle basierend auf `Duration_Hour`, `Event_log_level` Und `Log_file` Werte. Ruft Windows-Ereignisprotokolle gemäß den angegebenen Parametern ab	Verwendung: • -D duration_Hour: Dauer (in Stunden) ab der aktuellen Zeit zum Filtern von Ereignissen (Standard: 24). • -E event_log_level: Filtert die Ereignisse basierend auf der Ereignisebene.	WARNUNG zum Überprüfen der Ereignisprotokolldetails: Typ: Informationen, Kategorie: Anwendung, Computer: Ws19-inc0061393.LOCAL.LAB, Ereignis_ID: 1704, Nachricht: Sicherheitsrichtlinie in den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	und filtert sie. Gibt Details zu den Ereignissen mit dem Status „KRITISCH“, „WARNUNG“ oder „OK“ basierend auf dem angegebenen Schweregrad zurück.	Mögliche Werte sind: Information, ausführlich, Kritisch, Warnung, Fehler. Mehrere Werte sind kommagetrennt (Standard: Informationen). Beispiel: Informationen, Warnung • -i-ID: Filtert Ereignisse basierend auf den angegebenen Ereignis-IDs. Bei mehreren IDs sind Werte durch Kommas getrennt und in doppelte Anführungszeichen eingeschlossen. Beispiel: „1257, 1001“ • -L log_file: Gibt den Namen der Protokolldatei zum Filtern von Ereignissen an. Der Name der Datei wird in doppelte Anführungszeichen geschrieben. Unterstützt die Erstellung anwenderdefinierter Dateien, und mehrere Werte sind kommagetrennt. (Standard: Anwendung). Beispiel: „Anwendung, System“ • -P Provider_Name: Der Name des Ereignisanbieters, eingeschlossen	Gruppenrichtlinienobjekten wurde erfolgreich angewendet., timeCreated: 10/14/2024 12:09:35 UHR. Typ: Informationen, Kategorie: Anwendung, Computer: Ws19-inc0061393.LOCAL.LAB, Ereignis_ID: 16384, Nachricht: Erfolgreich geplanter Softwareschutzservice für Neustart um 2124-09-20T06:25:44Z. Grund: Regeln-Engine, Zeiterstellung: 10/13/2024 11:25:44 PM. Typ: Informationen, Kategorie: Anwendung, Computer: Ws19-inc0061393.LOCAL.LAB, Ereignis_ID: 16394, Nachricht: Offline-Migration auf Downlevel erfolgreich., timeCreated: 10/13/2024 11:24:19 PM. Typ: Informationen, Kategorie: Anwendung, Computer: Ws19-inc0061393.LOCAL.LAB, Ereignis_ID: 8224, Nachricht: Der VSS-Service wird aufgrund einer Leerlaufzeitüberschreitung heruntergefahren., timeCreated: 10/13/2024 11:51:36 AM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		in doppelte Anführungszeichen. • -R regex_pattern: Filtert Ereignisse, indem die Ereignisnachricht mit dem angegebenen Muster abgeglichen wird. Wert muss in doppelte Anführungszeichen eingeschlossen werden. • -S servicenow_event_severity – erstellt ein servicenow-Ereignis Mit dem in diesem Parameter angegebenen Wert. Mögliche Werte sind: Kritisch, Warnung und OK. Anwendungsbeispiel: `Winchecks Check-Windows-event-log-Details -d 24 -l Anwendung -e Warnung -r „*“ -s Warnung`	
os.windows.check-disk-name	Verwendet den Namen des Speicherlaufwerks als Eingabe und überprüft, ob das Laufwerk vorhanden ist. Gibt einen zurück *CRITICAL**WARNING**OK*Wert basierend auf dem angegebenen Parameter.	Winchecks Check-Windows-Disk-Name <options> -D: Datenträgername (Standard = C) Anwendungsbeispiel: `Winchecks Check-Windows-Disk-Name -d C`	Windows-Prüfungen OK: Festplattenspeicher C ist vorhanden.
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange anhand von	Verwendung:	Processor Queue Length OK: The Processor Queue length is 0.00 (Länge der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	• -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die Längenanzahl der Prozessorwarteschlange, die dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn die Längenanzahl der Prozessorwarteschlange, die dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Verwendungsbeispiel: `winchecks check-windows-processor-queue-length -w 5 -c 10`	Prozessorwarteschlange OK: Die Länge der Prozessorwarteschlange beträgt 0,00.)
os.windows.check-system-cpu-load	Überprüft die CPU-Last mithilfe von „typeperf“. Misst die CPU-Last anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die CPU-Lastanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES	CPU Load OK: The total CPU utilization is 26.92% (CPU-Last OK: Die CPU-Gesamtlast beträgt 26,92 %.)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Ereignis aus, wenn die CPU-Auslastungsanzahl, die dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Verwendungsbeispiel: `winchecks check-windows-cpu-load -w 85 -c 95`	
os.windows.check-system-disk	Misst den freien physischen Arbeitsspeicher anhand von Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn der Prozentsatz des Ereignisprotokolls, der dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn der Prozentsatz des Ereignisprotokolls, der dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Verwendungsbeispiel: `winchecks check-`	Disk Usage Check OK: The disk usage is % (Datenträgerverwendungsprüfung OK: Die Datenträgerverwendung beträgt %.)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		`windows-disk -w 85 -c 95`	
os.windows.check-system-memory-percent	Erfasst die RAM-Auslastung. Misst die Arbeitsspeicherauslastung anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn der Prozentsatz der Arbeitsspeichernutzung, der dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn der Prozentsatz der Arbeitsspeichernutzung, der dem Muster entspricht, über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Verwendungsbeispiel: `winchecks check-windows-ram -w 85 -c 95`	RAM Usage OK: The total memory utilization is 84% (RAM-Auslastung OK: Die Arbeitsspeicherauslastung insgesamt beträgt 84 %.)
os.windows.check-system-process	Laufende Prozesse werden zur Ermittlung laufender Prozesse abgefragt, die den angegebenen Argumenten entsprechen. (Muster, Name, Muster und Name. Mindestens ein Argument muss angegeben werden.)	Verwendung: • -n name – Name der ausführbaren Prozessdatei zur Überprüfung der Prozessausführung. • -P-Muster: Muster (Teilzeichenfolge), nach dem im Befehl gesucht werden soll, der	Check Process OK (Prozess überprüfen OK): OK Found 1 matching running processes named explorer (OK 1 übereinstimmender laufender Prozess mit Namen explorer gefunden)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	Misst die laufenden Prozesse anhand von konfigurierten Schwellenwerten und Filtern und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	den Prozess aufgerufen hat. Erzeugt nur dann gültige Ergebnisse, wenn der Benutzer, der den Agent ausführt, der Besitzer des abgefragten Prozesses ist und über Anzeigeberechtigungen für den abgefragten Prozess verfügt. • -w warnover – Löst einen Status vom Typ WARNUNG aus, wenn von der Abfrage mehr Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -W warnunder – Löst einen Status vom Typ WARNUNG aus, wenn von der Abfrage weniger Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -c critover – Löst ein Ereignis vom Typ KRITISCH aus, wenn von der Abfrage mehr Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -C critunder – Löst ein Ereignis vom Typ KRITISCH aus, wenn von	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		der Abfrage weniger Prozesse zurückgegeben werden, als vom Argument angegeben sind. Verwendungsbeispiel: `winchecks check-windows-processes -n explorer`	
os.windows.check-directory	Überprüft, ob ein Windows-Verzeichnis vorhanden ist.	Verwendung: -d --directory – Pfad zum entsprechenden Verzeichnis; verwenden Sie „\“ für die Trennung. Verwendungsbeispiel: `winchecks check-windows-directory -d dir_path`	Check Directory OK: The directory 'C:/Users/Public' exists (Verzeichnis überprüfen OK: Das Verzeichnis 'C:/Users/Public' ist vorhanden.)
os.windows.check-pagefile	Erfasst die *`Pagefile`*-Belegung und vergleicht sie mit den Schwellenwerten für WARNUNG und KRITISCH.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn der *`Pagefile`*Die Nutzung liegt über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn der *`Pagefile`*Die Nutzung liegt über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert. Verwendungsbeispiel: `winchecks check-`	Check Windows Page File OK: Page file usage at 31.63% (Windows-Auslagerungsdateien überprüfen OK: Belegung der Auslagerungsdateien bei 31,63 %)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		`windows-pagefile -w 75 -c 85`	
os.windows.check-free-physical-memory	Misst den freien physischen Arbeitsspeicher anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn der freie physische Speicher unter dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn sich der freie physische Speicher unter dem im Prüfparameter angegebenen KRITISCHEN Parameterwert befindet. Verwendungsbeispiel: `winchecks check-windows-free-physical-memory -w 10 -c 5`	Freier physischer Arbeitsspeicher OK: Der freie physische Arbeitsspeicher beträgt 20,25 %
os.windows.check-free-virtual-memory	Misst den freien virtuellen Arbeitsspeicher anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn der freie virtuelle Arbeitsspeicher über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn der freie virtuelle	Freier virtueller Arbeitsspeicher OK: Der freie virtuelle Arbeitsspeicher beträgt 66 %

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Arbeitsspeicher über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Anwendungsbeispiel: `Winchecks Check-Windows-free-Virtual-Memory -W 10 -c 5`	
os.windows.check-process-cpu	Misst „CPU-Auslastung Prozess“ anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -p processname – Prozessname zum Erfassen der CPU-Auslastung. • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die CPU-Auslastung über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn die CPU-Auslastung über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Anwendungsbeispiel: `Winchecks Check-Windows-Process-cpu-p gemäß -c 95 -W 85`	Check Process CPU OK: Process CPU usage is 0.0000% (Prozess-CPU überprüfen OK: CPU-Auslastung Prozess beträgt 0,0000 %.)
os.windows.check-process-memory	Misst die Prozessspeicherauslastung anhand von	Verwendung:	Check Process Memory OK: Process Memory usage is 0.0149% (Prozessspeicher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	• -p processname – Prozessname zum Erfassen der Speicherauslastung. • -W Warnung: Löst ein WARNUNGSEREIGNIS aus, wenn die Prozessspeichernutzung über dem im Prüfparameter angegebenen WARNUNGSPARAMETERWERT liegt. • -C Kritisch: Löst ein KRITISCHES Ereignis aus, wenn die Prozessspeichernutzung über dem im Prüfparameter angegebenen KRITISCHEN Parameterwert liegt. Anwendungsbeispiel: `Winchecks Check-Windows-Process-Memory-p gemäß -c 95 -W 85`	überprüfen OK: Die Prozessspeicherauslastung beträgt 0,0149 %.)
os.windows.check-user-account	Verwendet die Liste der Anwendernamen als Eingabe und überprüft, ob der Anwenderaccount aktiv ist. Gibt einen Wert „KRITISCH \WARNUNG\OK“ zurück.	Winchecks-Prüfung-Windows-user-disabled (Optionen) -U: Kommagetrennte Liste von Anwendernamen Anwendungsbeispiel: `Winchecks Check-Windows-user-disabled- u Administrator,Gast`	Anwendername und -Status

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Metriküberwachungsprüfungen

Richtlinie für Windows-Betriebssystem-Metriken

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-processor-queue-length --scheme hostname.proc`	win2019-dc-64bit.cpu.queuelength 0.00 1645371109
os.windows.check-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu-load -scheme hostname.proc`	win2019-dc-64bit.cpu.loadavgsec 15.07 1645371561
os.windows.check-system-cpu	Erfasst die CPU-Kern-Metrik.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu -scheme hostname.proc`	win2019-dc-64bit.cpu.cpu0.cores 2 1645371681

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-system-disk-usage	Erfasst die folgenden Metriken für die Datenträgerverwendung: • Summe in GB • Nutzung in GB • Verfügbarkeit in GB • verwendeter Prozentsatz	Verwendung: • -i, ignore_mnt – Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.disk_usage.disk_C.total(GB) 99.40 1645371774 win2019-dc-64bit.disk_usage.disk_C.used(GB) 50.72 1645371774 win2019-dc-64bit.disk_usage.disk_C.avail(GB) 48.68 1645371774 win2019-dc-64bit.disk_usage.disk_C.used_perc 51.02 1645371774
os.windows.check-system-memory-percent	Erfasst die prozentuale RAM-Auslastung, den Prozentsatz des freien physischen Arbeitsspeichers und den Prozentsatz des freien virtuellen Arbeitsspeichers.	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.mem.free_physical_percenta 13.30 1645371856 win2019-dc-64bit.mem.free_virtual_percentage 13.93 1645371856 win2019-dc-64bit.ram.usage_percentage 86.07 1645371856
os.windows.check-system-network	Erfasst die folgenden Metriken zu aktiven Netzwerkadaptern: • Gesamtanzahl Bytes/s • Pakete/s	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen	win2019-dc-64bit.system.network.Network_Int name> <metric value>Bytes_Total/sec 98742,67 1645372042

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	• Empfangene Pakete/s • Gesendete Pakete/s • Aktuelle Bandbreite • Empfangene Bytes/s • Unicastpakete empfangen/s • Nicht-Unicastpakete empfangen/s • Empfangene Pakete, verworfen • Empfangene Pakete, Fehler • Empfangene Pakete, unbekannt • Gesendete Bytes/s • Unicastpakete gesendet/s • Nicht-Unicastpakete gesendet/s • Ausgehende Pakete, verworfen • Ausgehende Pakete, Fehler • Ausgabewarteschlangenlänge • Abgeladene Verbindungen • Aktive TCP-Verbindungen für RSC • TCP-RSC: zusammengefügte Pakete/Sek.	Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-network --scheme hostname.proc`	Beispiel: win2019-dc-64bit.system.network.Network_Int sec 98742,67 1645372042

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	• TCP-RSC: Ausnahmen/Sek. • TCP RSC: durchschnittliche Paketgröße		
os.windows.check-system-uptime	Erfasst die Systemverfügbarkeit	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-uptime --scheme hostname.proc`	win2019-dc-64bit.system.uptime(sec) 4614142.06 1645372124
os.windows.check-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite • DiskReadBytesPerSec • DiskWriteBytesPerSec	Verwendung: • -i, ignore_mnt: Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte • – Schema – ersetzt Hostname und Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk`	win2019-dc-64bit.disk._total.AvgDisksec/Read 0.000000 1645372198 win2019-dc-64bit.disk._total.AvgDisksec/Write 0.000608 1645372198 win2019-dc-64bit.disk._total.DiskReadBytes/sec 0.000000 1645372198 win2019-dc-64bit.disk._total.DiskWriteBytes/sec 34941.692255 1645372198 win2019-dc-64bit.disk.C.AvgDisksec/Read 0.000000 1645372200 win2019-dc-64bit.disk.C.AvgDisksec/

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
			Write 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskReadBytes/sec 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskWriteBytes/sec 0.000000 1645372200
os.windows.check-system-memory	Erfasst die folgenden Datenträgermetriken: • FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory • TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemorySize	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-memory --scheme hostname.proc`	win2019-dc-64bit.mem.free_physical(KB) 1175440.00 1645372274 win2019-dc-64bit.mem.total_physical(KB) 8588898304.00 1645372274 win2019-dc-64bit.mem.free_virtual(KB) 1747636.00 1645372274 win2019-dc-64bit.mem.total_virtual(KB) 12263156.00 1645372274 win2019-dc-64bit.mem.available(KB) 1202032640.00 1645372274 win2019-dc-64bit.mem.total_visible(KB) 8387596.00 1645372274
os.windows.check-process-status	Erfasst den Windows-Prozessstatus mit CPU- und Arbeitsspeicherdaten, die vom Prozess verwendet werden.	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • – Schema – ersetzt Hostname und	win2019-dc-64bit.Process.Status 67 1645372421 win2019-dc-64bit.Process.CpuPercent 0 1645372421

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process).	win2019-dc-64bit.Process.Memory(KB) 1226444 1645372421
os.windows.metrics-process-status	Ruft die Anzahl der ausgeführten Instanzen, den Prozentsatz der CPU-Auslastung und die Arbeitsspeichernutzung (in Kilobyte) des angegebenen ab Windows Prozess.	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • – Schema – ersetzt Hostname und Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Anwendungsbeispiel: Befehl: Winchecks metric-Windows-Process-Status -n Svchost -s hostname.proc	WIN-R493MKFE75G.Prozess.Status 1 1625478491 WIN-R493MKFE75G.Prozess.KpiPercent 0 1625478491 WIN-R493MKFE75G.Prozess.Arbeitsspeic 276 162547849

Windows BS-Ereignisprüfungen – Erweitert

Wird Ausgeführt Windows Erweiterte Prüfungen der Betriebsfähigkeit Windows Server. Um diese Richtlinie auszuführen, aktivieren Sie eine der Prüfungen, und stellen Sie auf der Registerkarte „überwachte CIs“ der Richtlinie einen CI-Filter bereit, um diese Prüfungen für ausgewählte CIs auszuführen.

Windows BS-Ereignisse: Erweiterte Richtlinie

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process)	win2019-dc-64bit.cpu.queuelength 0.00 1645371109

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
		Verwendungsbeispiel: `command: winchecks metric-windows-processor-queue-length --scheme hostname.proc`	
os.windows.check-system-cpu	Erfasst die CPU-Kern-Metrik.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu -scheme hostname.proc`	win2019-dc-64bit.cpu.cpu0.cores 2 1645371681
os.windows.check-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu-load -scheme hostname.proc`	win2019-dc-64bit.cpu.loadavgsec 15.07 1645371561
os.windows.check-system-disk-usage	Erfasst die folgenden Metriken für die Datenträgerverwendung: • Summe in GB • Nutzung in GB • Verfügbarkeit in GB • verwendeter Prozentsatz	Verwendung: • -i, ignore_mnt – Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte.	win2019-dc-64bit.disk_usage.disk_C.total(GB) 99.40 1645371774 win2019-dc-64bit.disk_usage.disk_C.used(GB) 50.72 1645371774 win2019-dc-64bit.disk_usage.disk_C.avail(GB) 48.68 1645371774

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
		• --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.disk_usage.disk_C.used_perc 51.02 1645371774
os.windows.check-system-memory-percent	Erfasst die prozentuale RAM-Auslastung, den Prozentsatz des freien physischen Arbeitsspeichers und den Prozentsatz des freien virtuellen Arbeitsspeichers.	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.mem.free_physical_percenta 13.30 1645371856 win2019-dc-64bit.mem.free_virtual_percentage 13.93 1645371856 win2019-dc-64bit.ram.usage_percentage 86.07 1645371856
os.windows.check-system-network	Erfasst die folgenden Metriken zu aktiven Netzwerkadaptern: • Gesamtanzahl Bytes/s • Pakete/s • Empfangene Pakete/s • Gesendete Pakete/s • Aktuelle Bandbreite • Empfangene Bytes/s • Unicastpakete empfangen/s	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-network --scheme hostname.proc`	win2019-dc-64bit.system.network.Network_Int name> <metric value>Bytes_Total/sec 98742,67 1645372042 Beispiel: win2019-dc-64bit.system.network.Network_Int sec 98742,67 1645372042

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
	• Nicht-Unicastpakete empfangen/s • Empfangene Pakete, verworfen • Empfangene Pakete, Fehler • Empfangene Pakete, unbekannt • Gesendete Bytes/s • Unicastpakete gesendet/s • Nicht-Unicastpakete gesendet/s • Ausgehende Pakete, verworfen • Ausgehende Pakete, Fehler • Ausgabewarteschlangenlänge • Abgeladene Verbindungen • Aktive TCP-Verbindungen für RSC • TCP-RSC: zusammengefügte Pakete/Sek. • TCP-RSC: Ausnahmen/Sek. • TCP RSC: durchschnittliche Paketgröße		
os.windows.check-system-uptime	Erfasst die Systemverfügbarkeit	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process)	win2019-dc-64bit.system.uptime(sec) 4614142.06 1645372124

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
		Verwendungsbeispiel: `command: winchecks metric-windows-uptime --scheme hostname.proc`	
os.windows.check-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite • DiskReadBytesPerSec • DiskWriteBytesPerSec	Verwendung: • -i, ignore_mnt: Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk`	win2019-dc-64bit.disk._total.AvgDisksec/Read 0.000000 1645372198 win2019-dc-64bit.disk._total.AvgDisksec/Write 0.000608 1645372198 win2019-dc-64bit.disk._total.DiskReadBytes/sec 0.000000 1645372198 win2019-dc-64bit.disk._total.DiskWriteBytes/sec 34941.692255 1645372198 win2019-dc-64bit.disk.C.AvgDisksec/Read 0.000000 1645372200 win2019-dc-64bit.disk.C.AvgDisksec/Write 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskReadBytes/sec 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskWriteBytes/sec 0.000000 1645372200
os.windows.check-system-memory	Erfasst die folgenden Datenträgermetriken: • FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen	win2019-dc-64bit.mem.free_physical(KB) 1175440.00 1645372274

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
	• TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemoryS:	Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-memory --scheme hostname.proc`	win2019-dc-64bit.mem.total_physical(KB) 8588898304.00 1645372274 win2019-dc-64bit.mem.free_virtual(KB) 1747636.00 1645372274 win2019-dc-64bit.mem.total_virtual(KB) 12263156.00 1645372274 win2019-dc-64bit.mem.available(KB) 1202032640.00 1645372274 win2019-dc-64bit.mem.total_visible(KB) 8387596.00 1645372274
os.windows.check-process-status	Erfasst den Windows-Prozessstatus mit CPU- und Arbeitsspeicherdaten, die vom Prozess verwendet werden.	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process).	win2019-dc-64bit.Process.Status 67 1645372421 win2019-dc-64bit.Process.CpuPercent 0 1645372421 win2019-dc-64bit.Process.Memory(KB) 1226444 1645372421

Windows-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Windows-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Process.Status			Windows-Prozessstatus einschließlich CPU- und Speicherdaten.
Process.CpuPercent			Prozentsatz der vom Prozess verwendeten CPU.
Process.Memory(KB)		KB	Vom angegebenen Prozess verwendeter Arbeitsspeicher.
cpu.queuelength (empfohlene Metrik)			Länge der Prozessorwarteschlange.
cpu.loadavgsec (empfohlene Metrik)			Durchschnittliche CPU-Last pro Sekunde.
disk.AvgDisksec/Read		seconds	Durchschnittliche Zeit eines Lesevorgangs vom Datenträger.
disk.AvgDisksec/Write		seconds	Durchschnittliche Zeit eines Schreibvorgangs auf dem Datenträger.
disk.DiskReadBytes/sec		Byte/s	Rate, mit der Bytes während Lesevorgängen vom Datenträger übertragen werden.
disk.DiskWriteBytes/sec		Byte/s	Rate, mit der Bytes während Schreibvorgängen auf den Datenträger übertragen werden.
disk_usage.avail(GB)		GB	Verfügbarer Datenträger.
disk_usage.used(GB)		GB	Verwendeter Datenträger.
disk_usage.total(GB)		GB	Datenträger insgesamt.
disk_usage.used_percentage (empfohlene Metrik)			Verwendeter Datenträger in Prozent.
mem.free_physical_percentage			Freier physischer Arbeitsspeicher in Prozent.
mem.free_virtual_percentage			Freier virtueller Arbeitsspeicher in Prozent.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
ram.usage_percentage (empfohlene Metrik)			Verwendeter Arbeitsspeicher in Prozent.
mem.free_physical(KB)		KB	Menge des freien physischen Arbeitsspeichers.
mem.total_physical(KB)		KB	Physischer Arbeitsspeicher insgesamt.
mem.free_virtual(KB)		KB	Menge des freien virtuellen Arbeitsspeichers.
mem.total_virtual (KB)		KB	Virtueller Arbeitsspeicher gesamt.
mem.available(KB)		KB	Gesamtmenge des verfügbaren virtuellen Arbeitsspeichers.
mem.total_visible(KB)		KB	Gesamtmenge des physischen Arbeitsspeichers, auf den vom Betriebssystem zugegriffen werden kann.
system.uptime(Sec)		seconds	Dauer der Betriebsbereitschaft des Systems.
system.network.Bytes_Received/ sec (empfohlene Metrik)		Byte/s	Für aktive Netzwerkadapter empfangene Bytes pro Sekunde.
system.network.Bytes_Sent/ sec (empfohlene Metrik)		Byte/s	Für aktive Netzwerkadapter gesendete Bytes pro Sekunde.
system.network.Bytes_Total/ sec (empfohlene Metrik)		Byte/s	Summe der pro Sekunde empfangenen und gesendeten Bytes.
system.network.Current_Bandwidth		Bit/s	Geschätzte Bandbreite der Netzwerkschnittstelle.
system.network.Offloaded_Connections			Anzahl der IPv4- und IPv6-TCP-Verbindungen, die derzeit vom Netzwerkadapter verarbeitet werden, der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			TCP-Chimney-Abladung unterstützt.
system.network.Output_Queue_Length			Länge der Ausgabepaketwarteschlange.
system.network.Packets/sec			Rate, mit der Pakete im Netzwerk gesendet und empfangen werden.
system.network.Packets_Outbound_Discarded			Anzahl der ausgehenden Pakete, die verworfen wurden.
system.network.Packets_Outbound_Errors			Anzahl der ausgehenden Pakete, die aufgrund von Fehlern nicht gesendet werden konnten.
system.network.Packets_Received/sec			Rate, mit der Pakete empfangen werden.
system.network.Packets_Received_Discarded			Anzahl der eingehenden Pakete, die verworfen wurden.
system.network.Packets_Received_Errors			Anzahl der eingehenden Pakete, die aufgrund von Fehlern nicht gesendet werden konnten.
system.network.Packets_Received_Non-Unicast/sec			Die Rate, mit der Nicht-Unicastpakete (Subnetz-Broadcast oder Subnetz-Multicast) an ein übergeordnetes Protokoll übergeben werden.
system.network.Packets_Received_Unicast/sec			Rate, mit der Unicastpakete (Subnetz) an ein übergeordnetes Protokoll übergeben werden.
system.network.Packets_Received_Unknown			Anzahl der empfangenen, aber aufgrund eines unbekannten oder nicht unterstützten Protokolls verworfenen Pakete.
system.network.Packets_Sent/sec			Rate, mit der Pakete gesendet werden.
system.network.Packets_Sent_Non-Unicast/sec			Rate, mit der Pakete von übergeordneten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Protokollen an Nicht-Unicastadressen (Subnetz-Broadcast oder Subnetz-Multicast) übertragen werden sollen. Enthält Pakete, die verworfen oder nicht gesendet wurden.
system.network.Packets_Sent_Unicast/sec			Rate, mit der Pakete von übergeordneten Protokollen an Subnetz-Unicastadressen übertragen werden sollen. Enthält Pakete, die verworfen oder nicht gesendet wurden.
system.network.TCP_Active_RSC_Connections			Anzahl der IPv4- und IPv6-TCP-Verbindungen, über die momentan große Pakete vom RSC-fähigen Netzwerkadapter empfangen werden.
system.network.TCP_RSC_Average_Packet_Size		Byte	Durchschnittliche Größe der empfangenen Pakete über alle TCP-Verbindungen hinweg.
system.network.TCP_RSC_Coalesced_Packets/sec			Die Empfangsrate für große Pakete über alle TCP-Verbindungen hinweg.
system.network.TCP_RSC_Exceptions/sec			Die Rate für RSC-Ausnahmen für empfangene Pakete über alle TCP-Verbindungen hinweg.

Windows-Protokollüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgende Richtlinie für die Windows-Protokollüberwachung.

Richtlinie für die Windows-Protokollüberwachung

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	os.windows.check-log	Aktiviert die Überwachung von	Verwendung:	Windows-Protokoll KRITISCH: 4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für die Windows-Protokollüberwachung (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Protokolldateien auf einem Windows-Server.	• -c crit N – Kritische Stufe, wenn das Muster eine Gruppe aufweist. • -f -log-file FILE – Pfad zur Protokolldatei. • -o --warn-only – Bei Übereinstimmung warnen statt kritisch. • -q pattern PAT – Muster, nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in Anführungszeichen. Beispiel: "SEVERE|404" • -w warn N – Warnstufe, wenn das Muster eine Gruppe aufweist.	kritische Punkte gefunden, 0 Warnungen für Muster „SCHWERWIEGEND“| Ausnahme|404| Fehler in Datei C:\ProgramData \ServiceNow\Agent-Client-Collector\log \acc.log

Linux-Protokollüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgende Richtlinie für die Linux-Protokollüberwachung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-logs	Aktiviert die Überwachung von Protokolldateien, die einem normalen Benutzer gehören.	Verwendung: • -i --icase – Führt einen Abgleich aus, bei dem nicht nach Groß-/Kleinschreibung unterschieden wird. • -c, --crit N – Kritische Stufe (wenn das Muster eine Gruppe aufweist). • --encode-utf16u – Zeile vor dem Abgleich mit utf16 codieren. • -e, --encoding ENCODING-PAGE – Spezifische Codierungsseite zum Lesen der Protokolldatei. • -E, --exclude PAT – Muster, das vom Abgleich ausgeschlossen werden soll. • -F, --filepattern FILE – Überprüft ein Muster von Dateien anstelle einer einzigen Datei. Testen Sie das Muster bei regulären Ausdrücken (REGEX) zuerst auf https://	CheckLog CRITICAL: 0 warnings, 8 criticals for pattern SEVERE|Exception in log file /var/log/servicenow/agent-client-collector/acc.log (CheckLog KRITISCH: 0 Warnungen, 8 kritische Elemente für Muster SEVERE|Exception in Protokolldatei / var/log/servicenow/agent-client-collector/acc.log)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			rubular.com/, um die erwarteten Ergebnisse zu erhalten, und übergeben Sie es dann in Anführungszeichen als Parameter. Um beispielsweise alle Dateien mit der Erweiterung `.log` abzurufen, übergeben Sie "(.)*\.log$" als regulären Ausdruck (REGEX). • -f, --log-file FILE – Pfad zur Protokolldatei. • -l, --log-pattern PAT – Protokollformat der einzelnen Protokolleinträge: • -o, --warn-only – Bei Übereinstimmung warnen statt kritisch. • -q, --pattern PAT – Muster, nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Anführungszeichen (Beispiel: "SEVERE| 404"). • -r, --return – Gibt übereinstimmende Zeile zurück. • -L, --return-length N – Übereinstimmende Zeilenlänge. • -M, --return-error-limit N – Max. Anzahl der zurückgegebenen übereinstimmenden Zeilen (Protokolleinträge). • -n, --name NAME – Legt das Statusdateiverzeichnis automatisch mit dem Namen fest. • -s, --state_dir DIR – Verzeichnis, unter dem die Statusdateien aufbewahrt werden sollen. • -w, --warn N – Warnstufe, wenn das Muster eine Gruppe aufweist. Verwendungsbeispiel: `command: check-log.rb -c 2 -w 1 -q "SEVERE| Exception" -s /tmp/cache/ check-log -f /var/log/servicenow/agent-client-collector/acc.log`	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-logs-sudo	Aktiviert die Überwachung von Protokolldateien, die einem Root-Benutzer gehören.	Verwendung: • -i --icase – Führt einen Abgleich aus, bei dem nicht nach Groß-/Kleinschreibung unterschieden wird • -c, --crit N – Kritische Stufe (wenn das Muster eine Gruppe aufweist) • --encode-utf16u – Zeile vor dem Abgleich mit utf16 codieren • -e, --encoding ENCODING-PAGE – Spezifische Codierungsseite zum Lesen der Protokolldatei. • -E, --exclude PAT – Muster, das vom Abgleich ausgeschlossen werden soll • -F, --filepattern FILE – Überprüft ein Muster von Dateien anstelle einer einzigen Datei. Testen Sie das Muster bei regulären Ausdrücken (REGEX) zuerst auf https://rubular.com/, um die	CheckLog CRITICAL: 0 warnings, 8 criticals for pattern SEVERE|Exception in log file /var/log/servicenow/agent-client-collector/acc.log (CheckLog KRITISCH: 0 Warnungen, 8 kritische Elemente für Muster SEVERE|Exception in Protokolldatei / var/log/servicenow/agent-client-collector/acc.log)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			erwarteten Ergebnisse zu erhalten, und übergeben Sie es dann in Anführungszeichen als Parameter. Um beispielsweise alle Dateien mit der Erweiterung `.log` abzurufen, übergeben Sie "(.)*\.log$" als regulären Ausdruck (REGEX). • -f, --log-file FILE – Pfad zur Protokolldatei. • -l, --log-pattern PAT – Protokollformat der einzelnen Protokolleinträge: • -o, --warn-only – Bei Übereinstimmung warnen statt kritisch • -q, --pattern PAT – Muster, nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in Anführungszeichen (Beispiel:	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			"SEVERE| 404"). • -r, --return – Gibt übereinstimmende Zeile zurück. • -L, --return-length N – Übereinstimmende Zeilenlänge. • -M, --return-error-limit N – Max. Anzahl der zurückgegebenen übereinstimmenden Zeilen (Protokolleinträge). • -n, --name NAME – Legt das Statusdateiverzeichnis automatisch mit dem Namen fest. • -s, --state_dir DIR – Verzeichnis, unter dem die Statusdateien aufbewahrt werden sollen • -w, --warn N – Warnstufe, wenn das Muster eine Gruppe aufweist. Verwendungsbeispiel: `command: check-log.rb -c 2 -w 1 -q "SEVERE| Exception" -s /tmp/cache/ check-log -f /var/log/servicenow/agent-client-collector/acc.log`	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Metrikskript

Beim Erstellen einer neuen Richtlinie für Azure Cloud-Metriken erstellen Sie ein JSON-Skript, um die zu überwachenden Metriken zu bestimmen. Das Format für das Skript wird unten angezeigt, gefolgt von einer Tabelle, die den Skriptinhalt erklärt.

```
{
 "namespace": "Microsoft.Network/loadBalancers",
 "metrics": [
        "AllocatedSnatPorts",
        "ByteCount",
        "DipAvailability",
        "PacketCount",
        "SnatConnectionCount",
        "SYNCount",
        "UsedSnatPorts",
        "VipAvailability"
 ],
 "time_grain": "PT1M"
}
```

Ressourcen und ihre Metriken können aus abgerufen werden Unterstützte Metriken für Azure-Ressourcen Seite.

Header	Beschreibung
namespace	Der Name der überwachten Ressource.
Metriken	Die Metriken, die von der überwachten Ressource abgerufen werden.
Time_Grain	Die Granularität der Häufigkeit, mit der Metriken erfasst werden sollen. Mögliche Werte: • PT1M: Metrikwerte werden jede Minute erfasst. • PT5M: Metrikwerte werden alle 5 Minuten erfasst. • PT15M: Metrikwerte werden alle 15 Minuten erfasst. • PT30M: Metrikwerte werden alle 30 Minuten erfasst. • PT1H: Metrikwerte werden stündlich erfasst. • PT1D: Metrikwerte werden täglich erfasst.

Windows Filterparameter für Ereignisprotokoll

Die konfigurierbaren Werte auf der Registerkarte Prüfparameter der Prüfung os.windows.check-event-log.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Werte der Registerkarte „Parameter“

Parameter	Typ	Beschreibung
Provider_Name	Zeichenfolge	Name des Anbieters, der das Ereignis generiert hat. **Hinweis:** Wenn Sie keinen angeben `log_file`Wert zusammen mit `provider_name`, Durchsucht das System alle verfügbaren Protokolldateien, was die Zeit erhöht, die zum Empfangen von Ergebnissen benötigt wird.
Log_file	Zeichenfolge	Der Name des Windows Ereignisprotokolldatei, aus der Sie Ereignisse abrufen. Mögliche Werte: • Anwendung • System **Hinweis:** Wenn Sie keinen angeben `provider_name`Wert zusammen mit `log_file`, Durchsucht das System alle Ereignisse aus der Protokolldatei, was die Anzahl der abgerufenen Ereignisse erhöht.
id	Ganzzahl	Die numerische ID des Ereignisses. Mögliche Werte sind 0–65535.
Warnung	Ganzzahl	Jeder Wert über dem angegebenen Parameter generiert ein Warnungsereignis.
Event_level	Zeichenfolge	Der Schweregrad des Ereignisses. Mögliche Werte: • Kritisch • Fehler • Warnung • Informationen • Ausführlich
Regulärer Ausdruck_Muster	Zeichenfolge	Das Muster des regulären Ausdrucks, das beim Durchsuchen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die Werte der Registerkarte „Parameter“ (Fortsetzung)

Parameter	Typ	Beschreibung
		der Ereignisprotokolle verwendet werden soll. Der Wert muss in doppelte Anführungszeichen eingeschlossen werden. Beispiel: „Fehler“.
Duration_Hour	Ganzzahl	Der Zeitraum, für den Sie Ereignisse aus abrufen möchten Windows Ereignisprotokoll. Der Wert wird in Stunden angegeben. Bruchzahlen von Stunden werden mit Dezimalstellen angegeben.
kritisch	Ganzzahl	Ein beliebiger Wert, der dem angegebenen Parameter entspricht oder darüber liegt, generiert ein kritisches Ereignis.

Parameter eines verteilten MID Server-Clusters

Die folgenden MID Server-Parameter unterstützen den MID-Server-Clustertyp „Verteilt“.

Sie können auf diese Parameter in der zugehörigen Liste **Konfigurationsparameter** eines MID Servers zugreifen. Informationen zum Hinzufügen und Festlegen eines dieser Parameter finden Sie unter Fügen Sie einen MID-Server-Parameter hinzu .

Parameter	Beschreibung
mid.distributed.cluster.striped.threadpool.size	Größe des Striped-Thread-Pools im verteilten MID Server-Cluster. • **Typ**: Ganzzahl • **Standardwert**: Anzahl der Kerne des virtuellen Computers oder des Servers
mid.distributed.cluster.log.level	Protokollierungsebene für den verteilten MID Server-Cluster zur Unterstützung der Problembehandlung. Die Protokollierung wirkt sich jedoch auf die Leistung von Metric Intelligence aus. Bei einem leeren Wert erfolgt keine Protokollierung. • **Typ**: Ganzzahl • **Standardwert**: keiner • **Andere mögliche Werte**: info, debug, trace

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung

mid.distributed.cluster.global.timeout	Globale Zeitüberschreitung in Sekunden für verteilte MID Server-Cluster.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 180
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 60 (nicht erzwungen)
	  ○ **Maximalwert**: 300 (nicht erzwungen)

mid.distributed.cluster.node.max.off.heap.memory	Größe des Off-Heap-Speichers, der von Metric Intelligence zur Verarbeitung von Datenreihen pro Minute verwendet wird. Der Standardspeicherplatz von 4 GB entspricht der Menge an Off-Heap-Speicher, die für die Verarbeitung von 800.000 Datenreihen pro Minute erforderlich ist. Passen Sie diesen Wert proportional zur Menge der tatsächlichen Datenreihen an. Um beispielsweise 400.000 Datenreihen pro Minute zu verarbeiten, können Sie den Wert auf 2048 ändern. • **Typ**: Ganzzahl • **Standardwert**: 4096

Regelmäßige Aufgaben im verteilten MID Server-Cluster

Die folgende regelmäßige MID Server-Aufgabe ist im MID-Server-Clustertyp „Verteilt“ enthalten.

Name	Beschreibung
Verteilten MID Server-Cluster validieren	Validiert den Status des Clusterknotens für jeden MID Server im Cluster. Für einen MID Server, der inaktiv ist und dessen Status nicht „Gestoppt“ ist, wird der Knotenstatus auf „Gestoppt“ aktualisiert. Validiert auch den Gesamtstatus des Clusters. Während dieser Validierung wird der Cluster von der Aufgabe angehalten, wenn mehrere Untercluster in einem Cluster vorhanden sind.

Mit Metric Intelligence installierte Komponenten

Bei Aktivierung des Plugins „Metrikdaten“ (com.snc.sa.metric) werden mehrere Arten von Komponenten installiert, z. B. Tabellen, regelmäßige Aufgaben und Eigenschaften.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Regelmäßige Aufgaben installiert

Name	Beschreibung
Metric Intelligence – Aufgabe zum Lernen von Metriken	Wird täglich ausgeführt und erstellt die statistischen Modelle für die Anomalie-Erkennung
Metric Intelligence – Alte Metrikschemas und Anomaliepunktzahlen löschen	Bereinigt die Tabellen *sa_metric_anomaly_score* und *sa_metric_schema_definition*
Metric Intelligence – Metrikschema mit MID synchronisieren	Synchronisiert Daten aus der Instanz mit dem MID Server in der Metrikschematabelle *sa_metric_schema_definition*
Metric Intelligence – Tabellen mit MID synchronisieren	Synchronisiert Tabellendaten aus der Instanz mit dem MID Server
Metric Intelligence – Tabelle bereinigen	Bereinigt Tabellen im Zusammenhang mit verschiedenen Löschvorgängen
Metric Intelligence – Aufgabe zum Lernen des Beobachtungsintervalls	Berechnet das Beobachtungsintervall anhand gesammelter Datenpunkte für alle Datenreihen
Metric Intelligence – Anomaliepunktzahl für Prozessalterung – Täglich	Täglicher Job, der veraltete Anomaliepunktzahlen für ein bestimmtes Zeitfenster in der Tabelle „Anomaliepunktzahl der Metrik“ [sa_metric_anomaly_score] bereinigt. Verwendet die Eigenschaften *sa_metric.anomaly_score_stale_interval_in_days* und *sa_metric.anomaly_score_next_stale_interval_in_days*, um das Zeitfenster für die Bereinigung zu berechnen
Metric Intelligence – CI-Anomaliepunktzahlen synchronisieren	Hält Anomaliepunktzahlen beim Löschen von Metriken aktuell
Metric Intelligence – Konfigurationsaufgabe für Metriken	Synchronisiert Metrikkonfigurationen von der Instanz zu allen Metrikdaten-MID Servern
Metric Intelligence – Aufgabe zum Lernen des Kalman-Filtermodells auf lokaler Ebene	Erstellt Kalman-Filtermodelle auf lokaler Ebene, auf denen die Change-Erkennung ausgeführt wird
Metric Intelligence – Anomaliemodelltest	Regelmäßige Aufgabe, die bei Bedarf ausgeführt wird, wenn der Benutzer auf **Anomalietest ausführen** klickt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Metric Intelligence – Verteiltes MID-Cluster validieren	**1.** Überprüft den Status des Clusterknotens. Wenn der Status **Gestartet** lautet und der Status der Metrikdaten-Erweiterung nicht **Gestartet**/**Wird gestartet**/**Warnung** [Warnung mit bestimmten Fehlern] ist, ändert der Job den Status des Clusterknotens in **Gestoppt**. Dies passiert, wenn der MID Server unerwartet beendet wird, ohne dass die Instanz darüber benachrichtigt wird. **2.** Überprüft den Status aller Clusterknoten auf allen MID Servern im Cluster. ○ Wenn der Status aller Knoten **Gestoppt** und der Status des Clusters **Gestartet** lautet, ändert die Aufgabe den Status des Clusters in **Gestoppt**. ○ Wenn der Status des Clusters **Gestoppt** lautet, aber MID Server mit einem Clusterknoten vorhanden sind, der ausgeführt wird, wird der Status des Clusters in **Gestartet** geändert. **3.** Überprüft die Anzahl der Clusterleiter: Wenn zwei erkannt werden, stoppt der Auftrag den gesamten Cluster. Dies passiert, wenn MID Server keine Verbindung mit anderen Mitgliedern des Clusters herstellen und mehrere Subcluster bilden können.
Event Management – Metrikbindungsevents verarbeiten [1000 – 1020]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1000 – 1020).
Event Management – Metrikbindungsevents verarbeiten [1020 – 1040]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1020 – 1040).
Event Management – Metrikbindungsevents verarbeiten [1040 – 1060]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1040 – 1060).
Event Management – Metrikbindungsevents verarbeiten [1060 – 1080]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1060 – 1080).
Event Management – Metrikbindungsevents verarbeiten [1080 – 1100]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1080 – 1100).
Metric Intelligence – Aufgabe zum Lernen des stationären nichtparametrischen Modells	Lernt das stationäre nicht-parametrische Modell
Metric Intelligence – Aufgabe zum Lernen des kombinierten Modells	Konstruiert alle Informationen, die für die Durchführung der Anomalie-Erkennung in Echtzeit (Berechnen der Datenhäufigkeit und Erstellen statistischer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Modelle) erforderlich sind, für eine Teilmenge aller Reihen, für die Daten gesammelt werden.

Installierte Tabellen

Tabelle	Beschreibung
Metrikzeitreihenmodell [sa_time_series]	Für Metrikdaten erstellte statistische Modelle
Alarm-Anomalie [em_alert_anomaly]	Anomaliewarnungen, die aus Anomalie-Events erstellt wurden, die von Metric Intelligence gesendet wurden, damit Benutzer sie überprüfen können. Anomaliewarnungen werden von regulären Systemwarnungen getrennt gehalten.
Anomaliepunktzahl der Metrik [sa_metric_anomaly_score]	Speichert Anomaliepunktzahlen für die Metrik
Metrik-Zuordnung an CI # Gelöschte SysIds [sa_metric_map_deleted]	SysIds gelöschter Datensätze für Metrik-an-CI-Zuordnungen
Metrik-Zuordnung an CI [sa_metric_map]	Derzeit gültige Zuordnungen von Metriktypen zu CIs
Registrierung des SA-Metriktyps [sa_metric_registration]	Details zur Metriktypregistrierung
Metriktypregistrierung # Gelöschte SysIds [sa_metric_registration_deleted]	SysIds von Datensätzen, die aus der Tabelle „Registrierung des SA-Metriktyps“ [sa_metric_registration] gelöscht wurden
Metrikschemadefinition [sa_metric_schema_definition]	Zuordnung der empfangenen Metriken basierend auf der CI-Klasse. Sie wird verwendet, um die Metrikdaten-Nutzlast zu optimieren, die vom MID Server an die Instanz gesendet wird.
Metriktyp [sa_metric_type]	Quellmetriktyp
Typ der Überwachungssystemmetrik # Gelöschte SysIds [sa_source_metric_type_deleted]	SysIds der gelöschten Überwachungssystemmetriken
Typ der Überwachungssystemmetrik [sa_source_metric_type]	Metriktypen pro CI-Klasse, Aktivitätsstatus und Metrikquelle
Metrikeinstellungen [sa_metric_config_setting]	Standardkonfigurationseinstellungen für Metric Intelligence-MID Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Metrikkonfigurationsregeln [sa_metric_config_rule]	Regeln zum Überschreiben von Konfigurationseinstellungen für MID Server
Überschriebene Konfigurationen der Metrik [sa_metric_config_rule_setting]	Ordnet überschriebene Konfigurationen benutzerdefinierten Regeln zu
Bereitgestellte Konfigurationen der Metrik [sa_metric_config_staging]	Gespeicherte codierte Konfigurationen für die MID Server
Gelernte Parameter der Metrik [sa_metric_learned_param]	Parameter, die für CI/Metrik-Kombinationen gelernt wurden und mit den MID Servern synchronisiert werden
Metrik-Zuordnung an CI # Gelöschte Details [sa_metric_map_deleted_detail]	Details zu aus der Metrik-an-CI-Zuordnungstabelle gelöschten Einträgen. Schließt CI, Metrik und SysId des gelöschten Eintrags in der Tabelle „Metrik-Zuordnungen an CIs“ [sa_metric_map] ein.
In Metrikzuordnung erstellte eindeutige CIs nachverfolgen [sa_metric_ci_tracker]	Alle eindeutigen CIs, für die ein Metrikzuordnungseintrag erstellt wurde
Metrikklasse [sa_metric_class]	Metrikklassen, die bestimmten Metriken zugeordnet werden können, um gelernte Werte für Grenzen und Breiten zu überschreiben
Change-Punktzahl der Metrik [sa_metric_change_score]	Change Event-Informationen
Anomalietestregeln [sa_metric_anomaly_test_rule]	Anomalietestregeln, die für Anomaliemodelltests verwendet werden
Anomalietestergebnisse [sa_metric_anomaly_test_result]	Ergebnisse aus Anomaliemodelltests, z. B. Grenzen und Anomaliepunktzahlen
Konfiguration des Metrikanomalietests # angepasste Parameter [sa_metric_anomaly_test_config_custom_param]	Angepasste Parameter für ausgewählte Reihen in Anomaliemodelltests
Eigenschaften von Metric Intelligence [sa_metric_property]	Eigenschaften von Metric Intelligence nach Domäne.
Hostname mit Metrik-CI nachverfolgen [sa_metric_ci_host]	CIs, die mit dem Knotennamen aus dem Bindungsevent verbunden sind
Von der Metrikausdruckssprache unterstützte Funktionen [sa_metric_expr_funktion]	Von der Metrikausdruckssprache unterstützte Funktionen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Argumenttypen für Funktionen, die von der Metrikausdruckssprache unterstützt werden [sa_metric_expr_func_arg]	Argumenttypen für Funktionen, die von der Metrikausdruckssprache unterstützt werden
CI-Typen zu Metrikeinträgen nachverfolgen, die für verschiedene Quellen gültig sind [sa_metric_ci_type_map]	CI-Typen zu Metrikeinträgen nachverfolgen, die für verschiedene Quellen gültig sind
CI-Typ zu Ressourcenklasse [sa_ci_type_to_resource_class]	Enthält Zuordnungen des CI-Typs zur Ressourcenklasse. Wird für die Ressourcenbindung während der Ressourcensuche verwendet, wenn ein CI und ein `resource_path` im Event angegeben sind. Die Tabelle [sa_ci_type_to_resource_class] enthält einige Datensätze für Standardzuordnungen, und die Rolle evt_mgmt_admin ist zum Verwalten dieser Tabelle erforderlich.
CI-Ressource [ci_resource]	Übergeordnete Tabelle für Ressourcenbindungen
CI-Ressource – Hardware [ci_resource_hardware]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Anwendung [ci_resource_appl]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Service [ci_resource_service]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – virtueller Computer [ci_resource_vm_object]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Datenbank [ci_resource_database]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
Event-Verlauf der Serie [sa_series_event_history]	Informationen zum Starten und Beenden des Wartungsmodus von CIs. Metrikdaten speichert Verlaufsinformationen über die Zeiten, zu denen CIs in den Wartungsmodus treten und ihn wieder verlassen, wenn die Systemeigenschaft „sa.model_learner.maint_event_record_history_enabled“ auf „true“ (Standard) festgelegt ist. Wenn dann auch die Systemeigenschaft „sa_metric.maint_exclusion“ auf „true“ (Standard) festgelegt ist, werden Metriken von CIs im Wartungsmodus vom Modelllernen ausgeschlossen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Metadaten des Messgrößen-Dashboards [sa_metric_dashboard_metadata]	Diagrammkonfigurationen in Agent Workspace pro CI-Klasse für die Metriken, die für ein einer Warnung zugeordnetes CI angezeigt werden
Messgrößenkonfiguration – Bereitstellung der Anomalie-Erkennung [sa_metric_config_anomaly_detection_staging]	Interne Tabelle, die zur Berechnung der Aktionsebene für jeden Eintrag in der Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map] verwendet wird

Installierte Eigenschaften

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list` ein. Zum Öffnen der Tabelle „Metrikeinstellungen“ [sa_metric_config_setting] geben Sie im Navigationsfilter `sa_metric_config_setting.list` ein.

Eigenschaft	Verwendung
sa.metric.map.with.ci.expiration.sec	Dauer (in Sekunden), die Datensätze für die Zuordnung von Rohdaten zu CIs in Kraft bleiben, wenn die Zuordnung zum CI gefunden wird • **Typ**: Numerisch • **Standardwert**: 432000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten
sa.metric.map.without.ci.expiration.sec	Dauer (in Sekunden), die Datensätze für die Zuordnung von Rohdaten zu CIs in Kraft bleiben, wenn die Zuordnung zum CI nicht gefunden wird • **Typ**: Numerisch • **Standardwert**: 86400 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten
sa_metric.anomaly_score_stale_interval_in_days	Der Starttag des Zeitfensters, das die regelmäßige Aufgabe *`Operational Metrics - Process Stale Anomaly Score - Daily`* beim Überprüfen des Alterungsstatus der Anomaliepunktzahl verwendet. Das Zeitfenster reicht von heute so viele Tage zurück, wie in dieser Eigenschaft angegeben sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	• **Typ**: Numerisch • **Standardwert**: 3 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa_metric.anomaly_score_next_stale_interval_in_days	Anzahl der Tage, um die das von der regelmäßigen Aufgabe *`Operational Metrics - Process Stale Anomaly Score - Daily`* verwendete Zeitfenster erweitert wird. Gilt, wenn der Auftrag ausgeführt wird, aber unter der Verwendung des in der Eigenschaft *`sa_metric.anomaly_score_stale_interval_in_days`* angegebenen Zeitfensters keine Daten zurückgegeben werden. • **Typ**: Numerisch • **Standardwert**: 7 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

max_records_per_rest_request	Maximale Anzahl von Datensätzen, die in jedem Synchronisierungszyklus von der Instanz auf den MID Server heruntergeladen werden.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 10.000
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 1000
	  ○ **Maximalwert**: 20000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

normalized_metric_max_queue_size	Größe der Metrikwarteschlange. Der Anomaliedetektor liest diese Warteschlange und bestimmt für jede Metrik, ob sie anomal ist.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 3000000
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 1000000
	  ○ **Maximalwert**: 5000000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung

normalized_metric_queue_consumer_count	Anzahl der Threads, die die Anomalie-Erkennung gleichzeitig durchführen.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 12
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 8
	  ○ **Maximalwert**: 16
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

ignite_data_streamer_thread_count	Anzahl der Threads, die Datenstreamer zum Schreiben von Daten in den Cache verwenden.
	
	Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache hinzu.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 8
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 8
	  ○ **Maximalwert**: 32
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

ignite_data_streamer_flush_frequency	Häufigkeit der automatischen Löschung von Datenstreamern.
	
	Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache hinzu.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 1.000
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 0
	  ○ **Maximalwert**: 30000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

ignite_data_streamer_buffer_size	Puffergröße von Datenstreamern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung

	Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache hinzu.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 102400
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 1024
	  ○ **Maximalwert**: 1024000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

ignite_data_streamer_batch_size	Größe des Stapels, der einem Datenstreamer hinzugefügt wird.
	
	Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache hinzu.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 5.000
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 1
	  ○ **Maximalwert**: 10000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

ignite_data_streamer_batch_flush_frequency	Häufigkeit der automatischen Löschung der internen Stapelverarbeitung, bevor Daten zu Datenstreamern hinzugefügt werden.
	
	Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache hinzu.
	
	Diese Eigenschaft ist für die interne Verwendung bestimmt.
	
	• **Typ**: Ganzzahl
	• **Standardwert**: 5.000
	• **Andere mögliche Werte**:
	  ○ **Mindestwert**: 1000
	  ○ **Maximalwert**: 30000
	• **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
sa.metric.use.resource.binding	Ermöglicht Ressourcenbindung • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikbindung an Ressourcen
sa.metric.display.mid.setup.action	Zeigt den zugehörigen Link **Metric Intelligence einrichten** im MID Server-Formular für einen MID Server an, der validiert wurde und ausgeführt wird. • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: MID Server und verteilter MID Server-Cluster für Metric Intelligence
sa.model_learner.maint_event_record_history_enabled	Speichert Verlaufsinformationen zu Start und Ende des Wartungsmodus von CIs in der Tabelle „Event-Verlauf der Serie“ [sa_series_event_history]. • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa_metric.maint_exclusion	Schließt Metriken für CIs, die sich im Wartungsmodus befinden, vom Modelllernen aus • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa.model_learner.maint_history_batch_size	Ermittelt beim Speichern von Verlaufsinformationen zu Start und Ende des Wartungsmodus von CIs in der Tabelle „Event-Verlauf der Serie“ [sa_series_event_history] die Anzahl von Datenreihen pro Stapel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	Passen Sie die Einstellung dieser Eigenschaft an, wenn in diesem Zusammenhang Leistungsprobleme auftreten. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa_metric.scheduled_jobs_to_monitor_sys_id_list	Enthält die sys_ids der 3 regelmäßigen Aufgaben, die von der Eigensystemüberwachung für Metric Intelligence überwacht werden: • Metric Intelligence – Konfigurationsaufgabe für Metriken • Metric Intelligence – Tabellen mit MID synchronisieren • Metric Intelligence – Verteiltes MID-Cluster validieren

Schnellstarttests für Metrikdaten

Überprüfen Sie, ob Metrikdaten immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese zu bestehenden Schnellstarttests und konfigurieren Sie sie mit Ihren instanzspezifischen Daten.

Metrikdaten-Schnellstarttests erfordern die Aktivierung des Metrikdaten-Plugins (com.snc.sa.metric).

Metrikdaten-Schnellstarttests

Test	Beschreibung	Release-Version
OI: Sammlung von Integritätsmetriken	Ein einzelner Test, der Folgendes überprüft: • Mindestens eine Metrikdaten Metriken-Erweiterung wird ausgeführt. • Die Tabelle „Metrik an CI“ enthält Einträge für die „Integritätsmetriken“. • Für jede der derzeit ausgeführten Metrikdaten Metriken-Erweiterungen sind Daten in MetricBase gespeichert. Wenn der Test anfänglich fehlschlägt, warten Sie, bis die Metrikdaten Metriken-Erweiterung mindestens	Madrid

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdaten-Schnellstarttests (Fortsetzung)

Test	Beschreibung	Release-Version
	10-15 Minuten lang ausgeführt wird. Versuchen Sie es dann erneut.	

Zugehörige Informationen

Schnellstarttests

Ereignisschweregrade

Die Ereignisschweregradzahlen entsprechen den tatsächlichen Schweregraden auf der Seite „Zuordnungen der Metrik-Anomaliepunktzahl zu Ereignis-Schweregradzuordnungen“.

Ereignisschweregradzuordnung

Ereignisschweregradnummer	Ereignis-Schweregrad
0	Löschen (OK)
1	Kritisch
2	Schwerwiegend
3	Kleiner
4	Warnung

Agent Client Collector Visibility – Inhalt

Agent Client Collector Visibility – Inhalt(ACC-VC) ist ein ServiceNow Agent auf installiert Windows, Linux, Oder macOS Server zum Sammeln von Hostdaten.

Agent Client Collector Visibility – Inhalt – Übersicht

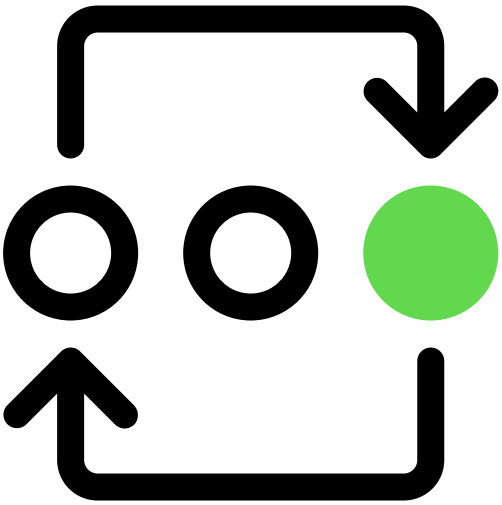
ACC-VC stellt Ruby-Skripts bereit, die BS-Abfragebefehle und BS-spezifische Befehle ausführen, um Informationen zu zu zu sammeln Windows, Linux, Oder macOS Server. Sie können Daten aus verschiedenen Dateisystemen und Speichergeräten, TCP-Verbindungen, laufenden Prozessen und anderen Informationen über Zielhosts erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

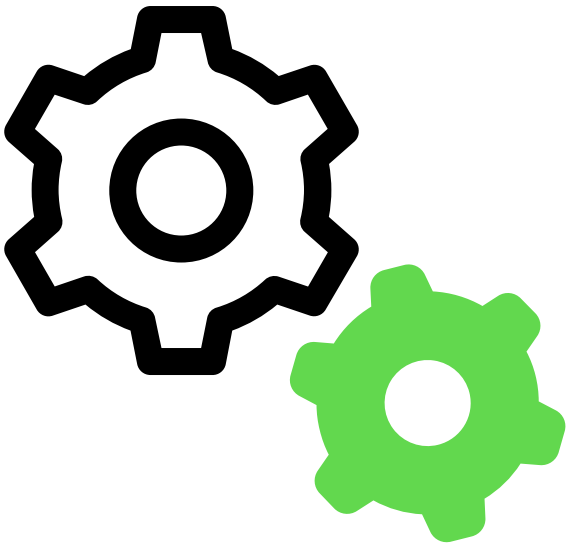
Automatische Übersetzung

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen kennen, die der bietet Agent Client Collector Visibility – Inhalt Anwendungsangebote.

Konfigurieren

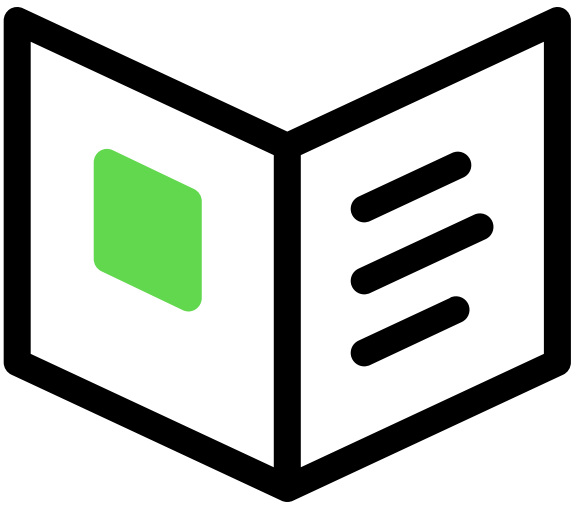


Konfigurieren Sie die zu aktivierenden Funktionen und Komponenten Agent Client Collector Visibility – Inhalt.

Verwenden

Anweisungen zur Verwendung Agent Client Collector Visibility – Inhalt.

Referenz



Rufen Sie zusätzliche Details zu ab Agent Client Collector Visibility – Inhalt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeiten

Für eine Liste von Agent Client Collector Visibility – Inhalt Plugin-Abhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Transparenz Und Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum für Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Agent Client Collector Visibility – Inhalt erkunden

Erfahren Sie, wie Sie verwenden können Agent Client Collector Visibility – Inhalt(ACC-VC), um Daten auf Ihren Zielhosts zu erkennen.

Agent Client Collector Visibility – Inhalt – Übersicht

ACC-VC ist ein zusätzlicher auszuführender Mechanismus Discovery. Dies ist eine Alternative zu horizontalen IP-basierten Discovery Für BS-bezogene Attribute, einschließlich Systeminformationen, Netzwerkschnittstellen, laufendem Prozess usw. ACC-VC eignet sich für lokale Server und Cloud-Instanzen. ACC-VC erkennt Software aus verschiedenen Installationsquellen, z. B. Chocolatey, Click-to-Run und winget, zusätzlich zu herkömmlichen MSI-basierten Installationen.

Agent Client Collector Visibility – Inhalt Unterstützt die folgenden Module:

- Datensammlung
- Erweiterter Bestand
- Seriennummern
- Speichergeräte
- Dateisysteme
- Netzwerkadapter
- TCP-Verbindungen
- Laufende Prozesse
- Installierte Software
- Lokaler Benutzer
- Intel vPro® Plattform

Hinweis:

- Derzeit Agent Client Collector Visibility – Inhalt Unterstützt keine mehrsprachigen Sprachen. Wenn die zurückgegebenen Werte nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Erkennung schlägt fehl.
- PowerShell wird in keinem der ACC-VC-Module auf verwendet Microsoft Windows Betriebssysteme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Ihre Zielsysteme in registrieren und verwalten ServiceNow Configuration Management Database (CMDB) Mit dem Pushbasierten ACC-VC-Modell. Es ist nicht erforderlich, Anmeldeinformationen anzugeben, Zeitpläne zu konfigurieren oder IP-Bereiche zu scannen.

Agent Client Collector Visibility – Inhalt – Workflow

Die folgende Abbildung beschreibt die allgemeine Architektur von Agent Client Collector Visibility – Inhalt.

ACC-VC-Architektur

ACC-VC funktioniert mit den folgenden Komponenten:

- ServiceNow Instanz
- ServiceNow MID-Server
- Zielhostcomputer
- ServiceNow Agent Client Collector Wird auf den Zielhostcomputern ausgeführt

Unterstützte Betriebssysteme

ACC-VC Version 1.0.3 erfasst die Systemattribute und zugehörigen Listen, die normalerweise vom BS-Muster erfasst werden. ACC-VC unterstützt derzeit die folgenden Betriebssysteme in der x86_64-Architektur:

- Linux
  - Red Hat Enterprise Linux (RHEL) und Oracle Linux (OL) 7, 8, 9
  - Centos 7, 8, 9

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- SLES 12, 15
- Ubuntu 18, 20
- Amazon Linux 2
- Debian 9 und 10

- Microsoft Windows
  - Windows Server 2012, 2012r2, 2016, 2019, 2022
  - Windows 10 Enterprise Edition
  - Windows 11 Enterprise und Professional Edition
- macOS (Ab ACC-VC Version 1,3.0)
  - 10.15 - Catalina
  - 11 - Big Sur
  - Monterey (x86)
  - 13: Ventura
  - macOS Ventura auf ARM64: Apple Silicon M1/M2
  - Sonoma

Zugehörige Informationen

Funktionsweise von Agent Client Collector Visibility – Inhalt

Funktionsweise von Agent Client Collector Visibility – Inhalt

Agent Client Collector Visibility – Inhalt(ACC-VC) erfordert die Installation von ServiceNow Agent Client Collector(ACC) auf dem Zielhost. ACC ist ein Derivat von Sensu-Go, einer Open-Source-Software.

ACC-VC-Anwendungsfälle

ACC-VC wendet Prüfungen und Richtlinien an, um Hostdaten zu planen und zu erfassen. ACC-VC wird in den folgenden Fällen ausgelöst:

- Regelmäßige Planung: Ein richtlinienbasierter Ansatz, bei dem Discovery Wird regelmäßig ausgelöst.
- Bei CI-Löschen: Wenn der Computer- oder Server-CI-Datensatz gelöscht wird.
- MID-Server Zyklus: Wenn MID-Server Geht runter und kommt wieder hoch.
- Zielhostzyklus: Wenn der Zielhost ausfällt und wieder hochfährt.
- Netzwerkunterbrechung: Wenn der Netzwerklink zum Ziel unterbrochen wird.

Hinweis: Discovery wird für die Agents ausgelöst, deren Hosts bereits vorhanden sind. Agents, deren Hosts nicht vorhanden sind, werden über ACC-F erkannt

ACC-VC Prüfungen und Richtlinien

Die ACC-VC-Assets werden als Agent-Plugins mit dem Haupteinstiegspunkt [ACC_Visibility_Main] und anderen Modulen für BS-Familien gespeichert. Es gibt ein Hauptsystem Discovery Prüfungsdefinition, aufgerufen *`Enhanced Discovery`*, Die von verwendet wird *`Enhanced Discovery Policy`*. Diese ACC-VC-Richtlinie wird nach einem Zeitplan ausgeführt, der standardmäßig auf 24 Stunden (86.400 Sekunden) festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Richtlinienkonfiguration wird mit allen Service Desk-Mitarbeitern synchronisiert, wie in der ACC-VC-Richtlinie definiert.

Wenn die Nutzlast von zurückgegeben wird MID-Server Für die Instanz den ACC-VC-Prüftyp, `EnhancedDiscovery`, Delegiert Aufgaben an die von ACC-VC bereitgestellte Skripteinbindung EnhancedDiscoveryHandler. Das Skript enthält Logik zur Verarbeitung der Daten aus der Prüfung und verarbeitet Aufgaben wie:

- Datentransformation in eine IRE-kompatible Nutzlast (Identification and Reconciliation Engine)
- Abgleich von Nicht-CI-Daten (cmdb_running_processes, cmdb_tcp_connections usw.)

Die ACC-VC-Prüfungsdefinition, `Enhanced Discovery`, Wird von initiiert ServiceNow Instanz. Dann wird in der Ausgabewarteschlange ein ECC-Warteschlangendatensatz mit dem Thema MonitoringProbe mit relevanten Prüfungsinformationen erstellt. Die MID-Server Verarbeitet dann die Prüfung, indem eine Nachricht über WebSocket über TLS an den ACC gesendet wird.

Während dieser Zeit bedient der MID-Server auch alle relevanten Assets oder Plugins, die vom ACC angefordert werden, um sicherzustellen, dass sie für das jeweilige Betriebssystem, die Plattform, die Betriebssystemversion und die Architektur relevant sind, auf der ACC ausgeführt wird.

Sie können alle Teile der ACC-VC-Anwendung bearbeiten und ändern, einschließlich Prüfungstyp, Richtlinie und Prüfungsdefinition. Weitere Informationen finden Sie unter Prüfungen und Richtlinien.

Virtuelle Maschinen (VM) und Cloud-Instanzen

ACC-VC ordnet ein Ziel zu, das über erkannt wurde Discovery, Mit bereits vorhandenen VM-Instanz-CIs. ACC-VC ordnet den erkannten CI-Datensatz einem bereits vorhandenen VM-Instanzdatensatz oder einem Cloud-Server-Instanzdatensatz mit entsprechenden CMDB-Beziehungen zu.

Die folgenden Varianten von Virtualisierungs- und Cloud-Server-Lieferanten werden für ACC-VC unterstützt:

- vCenter
- Amazon AWS Cloud
- Google (GCP)
- Microsoft Azure

Agent Client Collector Visibility – Inhalt konfigurieren

Planen und konfigurieren Sie Ihren Agent Client Collector Visibility – Inhalt(ACC-VC) Implementierung.

Konfiguration – Übersicht

ACC-VC erfordert die Installation von ServiceNow Agent Client Collector(ACC) auf dem Zielhost. ACC ist ein Derivat von Sensu-Go, einer Open-Source-Software.

Wird Konfiguriert Agent Client Collector Visibility – Inhalt Erfordert Folgendes:

- Das Plugin „Discovery“ (com.snc.discovery) muss installiert und aktiviert sein.
- Agent Client Collector Framework(ACC-F) muss auf installiert sein ServiceNow Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Agent muss auf dem Zielhost installiert sein.
- Stellen Sie sicher, dass Sie ein Upgrade auf durchgeführt haben Quebec Patch 3 oder höher.
- In einem Linux Oder macOS Umgebung: Stellen Sie sicher, dass Sie als servicenow-Anwender angemeldet sind.

  In einem Windows Umgebung: Stellen Sie sicher, dass Sie als lokaler Systemanwender angemeldet sind.
- ITOM Discovery Oder ITOM-Transparenz SKUs (SU-basierte Lizenzierung) sind erforderlich.

Sie können dann herunterladen und installieren Agent Client Collector Visibility – Inhalt(ACC-VC) Anwendung aus dem ServiceNow Store Oder aus der Instanz [sn_ACC_Visibility]. Siehe Agent Client Collector-Installation Für Details.

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow Store erstellten Anwendungen veröffentlicht. Wenn Sie die Anwendung bereits haben, können Sie die neueste Version herunterladen, um Ihre derzeitige Experience weiter zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert werden, werden die verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Agent Client Collector Visibility – Inhalt verwenden

Wenn Agent Client Collector Visibility – Inhalt(ACC-VC) ist auf Ihrem installiert Windows, Linux, Oder macOS Server werden verschiedene Informationen erfasst, je nachdem, welche anderen Funktionen oder Produkte Sie installiert haben.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Push-basierte Discovery und horizontale IP-basierte Discovery zusammen verwenden

Discovery Durchgeführt von Agent Client Collector Visibility – Inhalt(ACC-VC) ist kompatibel und kann mit horizontalen IP-basiert koexistieren Discovery. Möglicherweise ist ACC auf einem bestimmten Zielhost installiert, und dieser Host ist weiterhin Teil einer horizontalen IP-basierten Discovery Planen Sie auch.

Um Konflikte zu vermeiden, wird ACC-VC nicht ausgeführt Discovery Wenn die IP des Zielhosts bereits über ein CI verfügt, das von horizontaler IP-basiert erkannt wurde Discovery(Discovery_Source ist ServiceNow). Um dieses Verhalten außer Kraft zu setzen, setzen Sie die Systemeigenschaft [*sn_agent.disco_disable_ci_clobber_of_agentless_disco*] auf false. Diese Einstellung wird ignoriert, wenn horizontal IP-basiert Discovery Wurde über eine bestimmte Zeit nicht ausgeführt. Aktualisieren Sie gegebenenfalls die Systemeigenschaft [*sn_agent.disco_ci_clobber_of_agentless_disco_threshold_days*]. Der Standardwert ist 14 Tage. Siehe Systemeigenschaften Für weitere Details.

Zum Aktivieren Discovery Verwenden Agent Client Collector, Aktivieren Sie Folgendes Discovery Eigenschaften auf der Seite „Discovery-Eigenschaften“ (**Alle** > **Discovery-Definition** > **Eigenschaften**):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Eigenschaften von Agent Client Collector

Feld	Beschreibung
glide.discovery.domain.name.nbt	Legen Sie den BS-Domänennamen über NBT oder WMI fest. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird der Windows-Domänenname von NBT festgelegt. Andernfalls wird es von WMI festgelegt. • **Typ**: true | false • **Standardwert**: true
glide.discovery.enable.software_simplify	Aktiviert die Bereinigung für den Namen und die Version der Software. Bei Festlegung auf **true** werden alle angehängten Versionen oder häufig gefundenen Ausdrücke aus dem Namen sowie führende Nullen in der Version entfernt. Wenn auf festgelegt **Falsch** , Rohdaten werden in der Tabelle beibehalten. Verwenden Sie mit **Glide.Discovery.enable.Software_Simplify_sccm** Eigenschaft zur Vermeidung von Diskrepanzen zwischen Softwaredaten zwischen Discovery und SCCM. • **Typ**: true | false • **Standardwert**: true **Hinweis:** Sobald die Eigenschaft auf festgelegt ist **Falsch** , Um die Bereinigung zu deaktivieren, werden für eine bestimmte Software doppelte Datensätze generiert. Name und Version sind die primären Bezeichner.

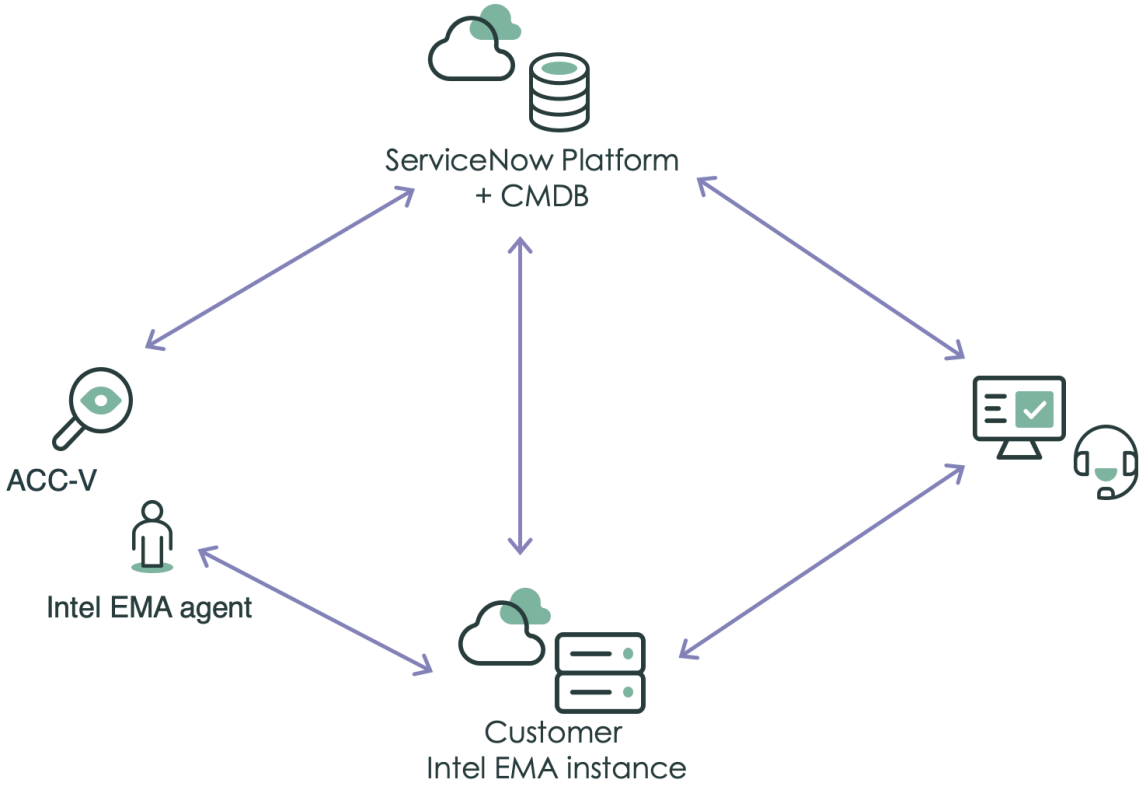
Pushbasierte Erkennung und Intel Endpoint Management Assistant (EMA) zusammen verwenden

Agent Client Collector Visibility – Inhalt(ACC-VC) kann Daten für Anwendungsfälle mit erfassen Intel VPro ®Plattform, wenn Intel ® EMA-Anwendung ist auf installiert Windows Endpunkte. Sie können die Anwendung Intel EMA aus dem ServiceNow Store installieren. Attribute werden in der CMDB gespeichert, wenn diese aktiviert ist. Derzeit können Daten für Intel EMA nur für Windows-Endpunkte abgerufen werden.

Mit der Anwendung Intel EMA können Kunden den Zugriff auf die Intel-Instanz über ihre ServiceNow-Instanz konfigurieren. Beispielsweise können IT-Supportgruppen eine Remote-Konsole öffnen und Aktionen wie das Aus- und Wiedereinschalten ausgehend von einem ServiceNow-Incident ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Intel + ServiceNow Platform



Automatische Übersetzung

Pushbasierte Erkennung und SAM zusammen verwenden

Agent Client Collector Visibility – Inhalt(ACC-VC) erfasst installierte Softwaredaten für Anwendungsfälle für Software Asset Management(SAM), wenn das SAM-Plugin installiert ist. Mit Push-basiert Discovery Und SAM zusammen kann die Softwaredatenerfassung mit SAM-Basismetriken und SAM-Gesamtnutzungsmetriken optimieren.

ACC-VC kann über Push-basierte Discovery die Zeit des letzten Zugriffs für die Software oder Anwendungen erfassen, die auf dem Ziel installiert sind. Diese Informationen werden zusammen mit der Ziel-CI-Referenz der Tabelle „Software-Update“ [samp_sw_usage] hinzugefügt.

SAM-Standardmetering und SAM-Gesamtnutzungsmetriken werden für beide unterstützt Windows Und macOS.

Die Softwarenutzungsdatensätze sind domänengetrennt. Die Datensätze werden mit der Domäne des ausgefüllt MID-Server Wird für den Agent-basierten verwendet Discovery Für das Ziel.

Hinweis: Um bei Softwareinstallationen (cmdb_sam_SW_install) das Einfügen doppelter Datensätze zu vermeiden, wird dieselbe Discovery-Quelle „ ServiceNow„ Wird für beide Push-basiert verwendet Discovery Und horizontal IP-basiert Discovery.

Anforderungen

SAM-Basismessung und SAM-Metriken zur Gesamtnutzung

Für die Metriken für die SAM-Standardmessung und die SAM-Gesamtnutzung muss der nicht privilegierte servicenow-Anwender (für den sich der Service Desk-Mitarbeiter als anmeldet) mit SCHREIBGESCHÜTZTEM Zugriff in der Registrierung konfiguriert werden. Dieser Zugriff ermöglicht die erfolgreiche Ausführung der OSQuery für die Tabelle „UserAssist“. Wechseln Sie zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

regulären Auswerten, und erlauben Sie dem servicenow-Anwender, UserAssist für alle anderen Anwenderaccounts zu lesen (z. B.: HKEY_USERS\SID... \Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UserAssist Für jeden Anwender in HKEY_USERS).

Hinweis: Die *UserAssist*Schlüssel erbt keine Berechtigungen von *HKEY_USERS\SID...*Übergeordneter Schlüssel. Daher müssen Sie zu navigieren *UserAssist*Schlüssel und Berechtigung direkt für den Schlüssel hinzufügen.

Voraussetzungen für die Anwendung der SAM-Basismessung oder der SAM-Metriken zur Gesamtnutzung:

- Das SAM-Plugin ist (com.snc.samp) aktiviert.
- Die Systemeigenschaft *sn_acc_vis_content.persist_sam_usage_metrics* ist auf „true“ gesetzt. Siehe Systemeigenschaften Für weitere Details.

Für Details zum Setup der SAM-Messung mit Agent Client Collector, Siehe Knowledge Base-artikel KB1642676 .

Informationen zur Software-Edition

Zum Abrufen von Informationen über die Software-Edition muss das SAM-Plugin (com.snc.samp) aktiviert sein.

SAM-Basismessung

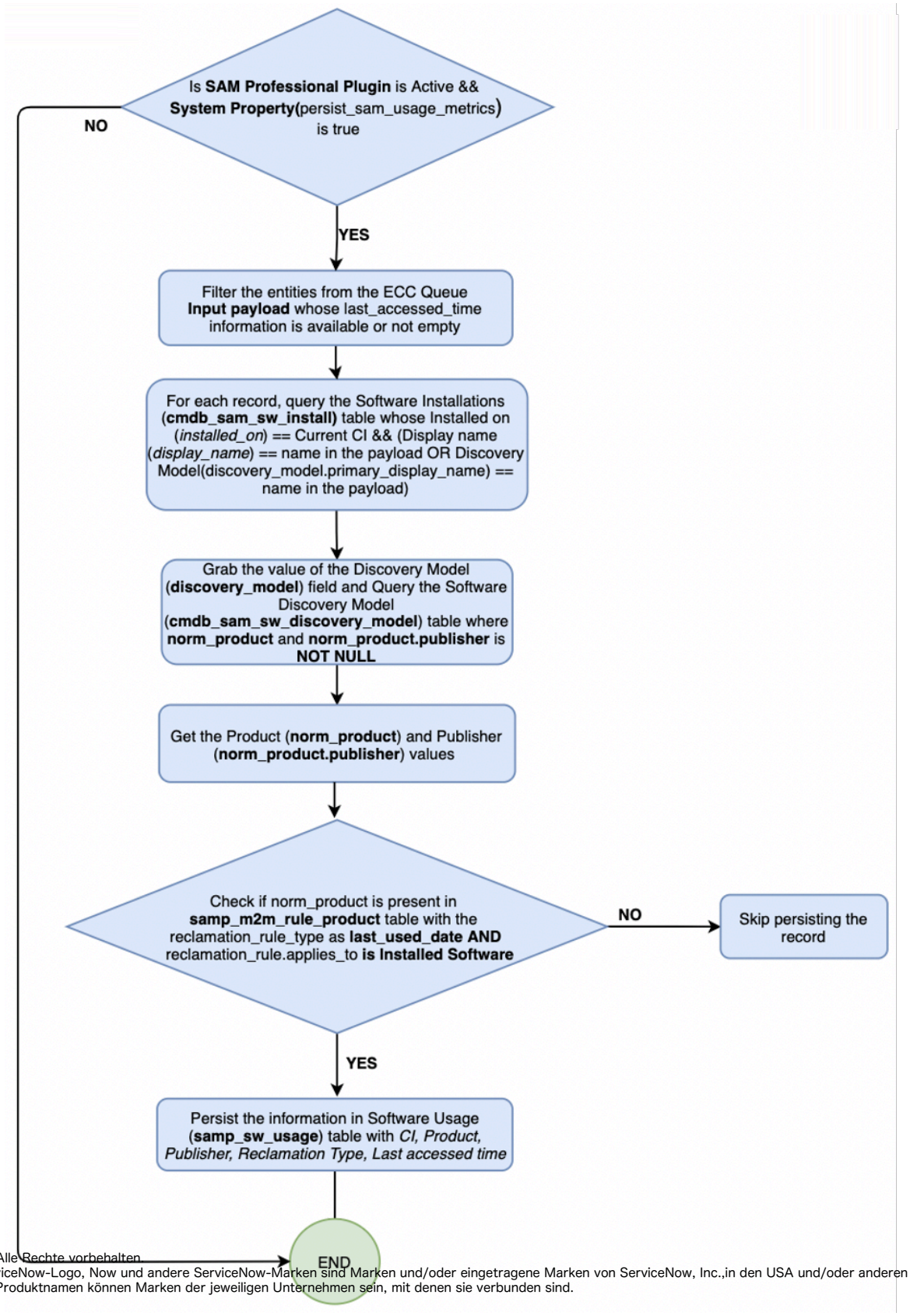
Hinweis: Es gibt eine Konfiguration in Windows Betriebssystemebene, die die korrekte Erkennung der Daten nicht zulässt. Aktualisieren Sie die Konfiguration, damit die Daten erfolgreich vom ACC-VC-Service Desk-Mitarbeiter erfasst und in die übertragen werden können ServiceNow Plattform richtig. Erstellen Sie im Registrierungs-Editor die folgenden Schlüssel im Pfad: *HKEY_CURRENT_USER \SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced.*

- Name: Start_TrackProgs
  - Basis: Hexadezimal
  - Wert: 1
- Name: Start_TrackProgsBase
  - Basis: Hexadezimal
  - Wert: 1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flussdiagramm zur SAM-Basismessung

Fragen Sie zum Beziehen einer Liste der Software in der Nutzlast die Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model] ab, um das entsprechende Produkt und seinen Herausgeber abzurufen. Sobald das Produkt abgerufen wurde, überprüfen Sie, ob die Rückforderungsregel aktiviert ist, damit in der Tabelle „Softwarenutzung“ [samp_sw_usage] die Informationen über die letzte Nutzung dieses Produkts erhalten bleiben. Einzelheiten können Sie dem Flussdiagramm entnehmen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Fragen Sie mithilfe der OSQuery aus der Tabelle „UserAssist“ den Zeitpunkt des letzten Zugriffs für das Ziel ab. Verwenden Sie dabei den Anwendungs- oder Softwarenamen als Eingabe für die Abfrage.

Verwenden Sie *sn_acc_vis_content.disable_sam_reclamation_rules_for_licensable_softwares*Eigenschaft zum Definieren von Reklamationsregeln für lizenzierbare Software wie folgt:

- **Wahr** : Aufruf von Reklamationsregeln für lizenzierbare Software deaktivieren. SAM nutzt weiterhin für alle lizenzierbaren Software und für nicht lizenzierbare Software mit definierten Reklamationsregeln.
- **Falsch** : SAM-Nutzung gemäß definierten Reklamationsregeln speichern.

Folgende häufig genutzte Anwendungen werden unterstützt:

- WinZip
- Google Chrome
- Sublime Text
- Notepad++
- Autodesk
- Microsoft Office 365
- Tableau

SAM-Metriken zur Gesamtnutzung

Mit SAM-Metriken zur Gesamtnutzung können Sie die Gesamtnutzungszeit und die Gesamtnutzungsanzahl für jede Anwendung messen, für die eine Rückforderungsregel für Software aktiviert ist.

Osquery stellt eine ausführbare Daemon-Datei bereit, die als Service ausgeführt werden kann, genannt Osqueryd. Osqueryd muss manuell bereitgestellt werden, damit die SAM-Metriken zur Gesamtnutzung ordnungsgemäß funktionieren. Jede Osqueryd-Bereitstellung erfordert die Datei osquery.conf, optional externe Pakete und Initialisierungskennzeichnungen (konfiguriert in der Datei osquery.flags), die beim Starten des Service bereitgestellt werden. Im Gegenzug führt der Daemon-Service geplante Abfragen auf dem Host aus und protokolliert ihn in einem lokalen Dateisystem.

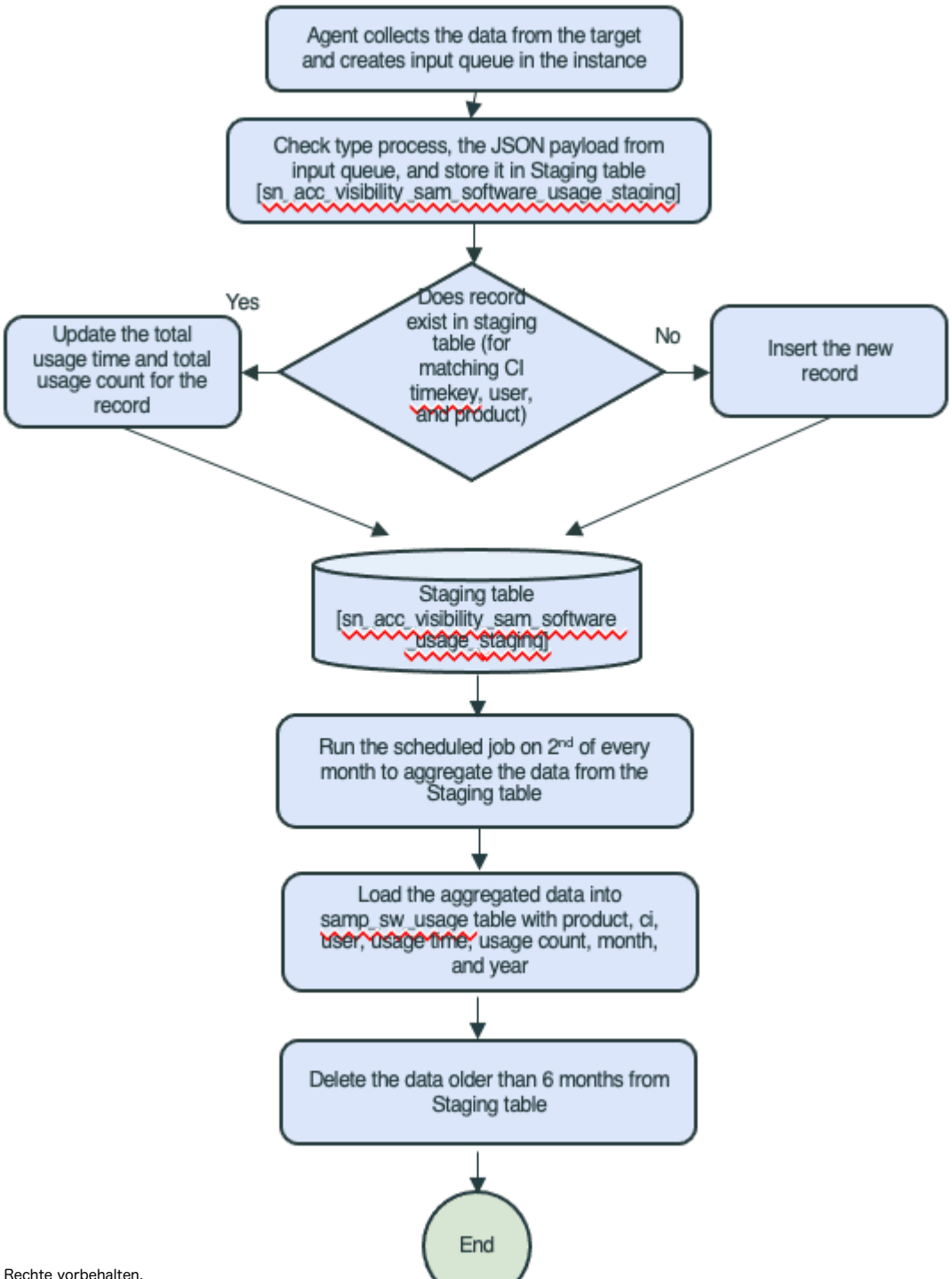
Hinweis: Osquery bietet standardmäßig Unterstützung für die dateisystembasierte Protokollierung. Diese Konfiguration wird bei jeder Neuinstallation von Osquery in der Datei osquery.conf bereitgestellt.

Domäneninformationen können während der Datensammlung erfasst werden. Dies kann großen Organisationen mit mehreren Mitarbeiterverzeichnissen helfen, Software dem richtigen Anwender zuzuordnen. Derzeit wird dies für unterstützt Windows Nur. Um die Softwarenutzung/assigned_to dem richtigen Anwender in einer domänengetrennten Umgebung zuzuordnen, verwenden Sie die Systemeigenschaft [sn_ACC_VIS_content.column_Name_for_user_Mapping] mit einem gültigen Feldnamen. Standardmäßig ist der Wert dieser Systemeigenschaft leer, d. h., sie validiert nur den Anwendernamen und nicht die Domäne. Sie können eines der folgenden Formate verwenden, um Anwendername und Domäne zu validieren: Anwendername@Domäne oder Domäne\Anwendername.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flussdiagramm für SAM-Metriken zur Gesamtnutzung

Mithilfe der Liste der Prozesse können Sie eine SAM-Normalisierung durchführen, um die Prozesse für die relevanten installierten Softwaredatensätze zuzuordnen. Dies bietet Flexibilität, da Namen und Prozesse installierter Software normalerweise nicht identisch sind. Fragen Sie zum Beziehen einer Liste der Prozesse in der Nutzlast die Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model] und die Tabelle „Softwareprodukt“ [samp_sw_product] ab, um das entsprechende Produkt und seinen Herausgeber abzurufen. Sobald das Produkt abgerufen wurde, überprüfen Sie, ob die Rückforderungsregel aktiviert ist, damit in der Tabelle „Softwarenutzung“ [samp_sw_usage] die Informationen über die gesamte Nutzungszeit dieses Produkts erhalten bleiben. Einzelheiten können Sie dem Flussdiagramm entnehmen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie Osqueryd für Windows Mit dem folgenden Skript.

```
# Install latest osquery

$msi = "osquery-5.7.0.msi"
$url = "https://pkg.osquery.io/windows/$msi"
$dst = "$PSScriptRoot\$msi"
Invoke-WebRequest -Uri $url -OutFile $dst
# msiexec /i "$dst" /quiet /qn /norestart
Start-Process msiexec.exe -Wait "/i $dst /quiet /qn /norestart"

# Configure osqueryd service

$flags = "--logger_rotate=true
--logger_rotate_size=26214400
--logger_rotate_max_files=1
--watchdog_level=-1
--config_path=C:\Program Files\osquery\osquery-sam.conf"
Set-Content -Path 'C:\Program Files\osquery\osquery.flags.default' -Value "$flags"

$conf = @'
{
  "options": {
    "config_plugin": "filesystem",
    "logger_plugin": "filesystem",
    "utc": "true"
  },
  "schedule": {
    "sam_process_info": {
      "query": "SELECT name, pid, elapsed_time, start_time, user_time, system_time, username
 FROM processes p JOIN users u ON u.uid = p.uid WHERE p.elapsed_time != -1 AND u.type !=
 'special';",
      "snapshot" : true,
      "interval": 300
    },
    "system_info": {
      "query": "SELECT hostname, cpu_brand, physical_memory FROM system_info;",
      "interval": 3600
    }
  },
  "decorators": {
    "load": [
      "SELECT uuid AS host_uuid FROM system_info;",
      "SELECT user AS username FROM logged_in_users ORDER BY time DESC LIMIT 1;"
    ]
  },
  "packs": {
  }
}
'@
Set-Content -Path 'C:\Program Files\osquery\osquery-sam.conf' -Value "$conf"

cd 'C:\Program Files\osquery'
.\manage-osqueryd.ps1 -uninstall
.\manage-osqueryd.ps1 -install
Restart-Service osqueryd
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Details zu Windows Und macOS Siehe Osqueryd-Zeitplan für SAM-Metriken zur Gesamtnutzung konfigurieren Und Osqueryd-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren.

SAM-Metriken ohne osqueryd werden erfasst

Optional können Sie die Effizienz verbessern, indem Sie bei Verwendung von Push-basiert nicht-osqueryd-Datensammlung verwenden Discovery Und Software Asset Management(SAM) zusammen. Wenn nicht-osqueryd-Datensammlung aufgerufen wird, wird die Datensammlung automatisch für alle verfügbaren Service Desk-Mitarbeiter durchgeführt, anstatt osqueryd für jeden Service Desk-Mitarbeiter einzeln aufzurufen.

So führen Sie eine nicht-osqueryd-Datensammlung durch:

1. Stellen Sie sicher, dass die folgenden Berechtigungen für das relevante Betriebssystem konfiguriert sind:
   - Windows: Entweder NT AUTHORITY\SYSTEM oder admin
   - Linux Und macOS: Stamm
2. Auf der Seite „Systemeigenschaften“ (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**), legen Sie fest *sn_acc_vis_content.enable_sam_collection_without_osqueryd*Eigenschaft bis **Wahr** .

Hinweis: Aktivieren Sie diese Eigenschaft nur, wenn alle Agents Version 4.1.0 oder höher haben.

Informationen zur Software-Edition

Ab ACC-VC Version 2,3 werden Editionsinformationen für Adobe Acrobat und MS SQL Server unterstützt. In zukünftigen Releases wird zusätzliche Software unterstützt. Mit dieser Funktion können SAM-Administratoren die Editionen der installierten Software transparent nachvollziehen. Osquery-Befehle werden dazu verwendet, Informationen über Editionen abzurufen, die dann in der Softwareinstallationstabelle [cmdb_sam_sw_install] in der Spalte „Editionsüberschreibung“ angezeigt werden. Weitere Informationen finden Sie im Support-KB-Artikel https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0721360 .

Zugehörige Informationen

Osqueryd-Zeitplan für SAM-Metriken zur Gesamtnutzung konfigurieren

Osqueryd-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren

Osqueryd-Zeitplan für SAM-Metriken zur Gesamtnutzung konfigurieren

SAM-Gesamtnutzungsmetriken sind abhängig davon, dass auf dem Zielhost der Osqueryd-Service ausgeführt wird. Konfigurieren Sie den Osqueryd-Service, um den erforderlichen Zeitplan für Osquery auf dem Host auszuführen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Osqueryd-Installationsordner**an.
2. Suchen Sie nach der Datei osquery.conf und bearbeiten Sie sie.
3. Fügen Sie das folgende Osquery-Paket unter dem Stichwort „Pakete“ hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Windows:

```
"packs": {
    "sam-metering":
 "C:\\ProgramData\\ServiceNow\\agent-client-collector\\cache\\acc-visibility-modules\
\bin\\sam-metering.conf"
 }
```

Für macOS:

```
"packs": {
   "sam-metering": "/Library/Application\
 Support/servicenow/agent-client-collector/cache/acc-visibility-modules/bin/sam-metering.
conf"
 }
```

Ergebnis

Sie können jetzt Osquery-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren.

Osqueryd-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren

Standardmäßig unterstützt Osquery die Protokollrotation basierend auf der Größe. Um sie für die SAM-Metriken zur Gesamtnutzung zu aktivieren und die Protokollgröße und -rotation zu konfigurieren, müssen Sie bestimmte Kennzeichnungen für den Osqueryd-Service hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: SAM mit Osqueryd verbraucht Arbeitsspeicher und CPU-Zyklen. Beispiel: Wenn der Agent auf einem Windows-Computer mit 2 CPU-Kernen, 8 GB RAM, 1.000 Softwareinstallationen und 500 laufenden Prozessen installiert ist, wurde Folgendes beobachtet:

- Die durchschnittliche CPU-Auslastung für Agent und Osqueryd betrug weniger als 10 % CPU-Auslastung und maximal 30 % CPU-Auslastung. Dies tritt nur auf, wenn die SAM-Hintergrundrichtlinie ausgelöst wird. Standardmäßig erfolgt der Auslöser alle 480 Sekunden.
- Die durchschnittliche Arbeitsspeichernutzung für Agent und Osqueryd war kleiner als 10 MB und es wurden maximal 26 MB verbraucht.

Um die Daten für einen einzelnen laufenden Prozess für zwei Tage zu speichern, sollte die Protokolldateigröße im Durchschnitt 52.429 Byte betragen. Die Protokolldateigröße muss erhöht werden, wenn die Anzahl der laufenden Prozesse auf dem Computer höher ist. Bei 500 laufenden Prozessen würde die Protokollgröße beispielsweise durchschnittlich 25 MB betragen, was 26.214.400 Byte entspricht.

Prozedur

1. Navigieren zu **Osqueryd-Installationsordner**an.
2. Suchen Sie nach der Datei osquery.flags und bearbeiten Sie sie.
3. Fügen Sie die folgenden Kennzeichnungen mit diesen Größenrichtlinien hinzu:

Hinweis: Die Änderung der Protokolldateigröße sollte gemäß den Richtlinien für die Osqueryd-Protokolldateigröße erfolgen.

Für Windows:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- --Logger_Rotation=wahr
- --Logger_Rotation_size=26214400
- --Logger_Rotation_max_files=1
- --Watchdog_level=1

Für macOS:

- --Logger_Rotation=wahr
- --Logger_Rotation_size=26214400
- --Logger_Rotation_max_files=1
- --Watchdog_level=1
- --Logger_Mode=0644

4. Speichern Sie die Datei.

Ergebnis
Sobald der Osqueryd-Zeitplan und die Osqueryd-Protokolle konfiguriert sind, kann der Osqueryd-Service gestartet werden.

Der Zeitplan führt die Osquery aus: Name, PID, verstrichene Zeit, Start_time, user_time, System_time, Anwendername aus Prozessen p JOIN-Anwender u AUF u.uid = p.uid, wobei p.elapsed_time != -1 UND u.type !='special';" alle 5 Minuten (300 Sekunden) auf dem Zielcomputer ausgeführt wird. Dadurch werden die Ergebnisse in der Protokolldatei protokolliert. Die Protokolldatei enthält Snapshot-Einträge aller Abfragen, die für die Ausführung durch Osqueryd konfiguriert sind. Diese Abfrage enthält alle Prozessattribute.

Hinweis:

Eine temporäre Datei *`Marker.JSON`* Wird in einem temporären lokalen Ordner auf Ihrem Computer im folgenden Verzeichnis erstellt:

Für Windows : `<userprofile>\\AppData\\local\\AgentClientCollector\\SAM` .

Für macOS: /Library/Application\ Support/servicenow/Agent-Client-Collector .

Diese Datei verfügt über Lese-/Schreibberechtigungen und enthält die Markerdaten: *`Data and Last Read Unix Time stamp`*.

Osqueryd kann auch so konfiguriert werden, dass die zugehörigen Protokolle in einen benutzerdefinierten Verzeichnispfad anstatt in das Standardverzeichnis geschrieben werden. Wenn Sie ein benutzerdefiniertes Verzeichnis auswählen, ändern Sie die Prüfungsdefinition [samadvanced-background-log-check].

Anwendungsmuster für Agent Client Collector

Anwendungsmuster erfassen Details zu den Anwendungen, die auf ausgeführt werden Agent Client Collector(ACC)-Host. Anwendungsmuster werden nur für Server unterstützt und nach ausgelöst Agent Client Collector Host Discovery Ist abgeschlossen.

Voraussetzungen für die Verwendung von Anwendungsmustern

Zum Aktivieren von Anwendungsmustern auf dem Agent Client Collector, Installieren Sie Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Agent Client Collector Framework
- Agent Client Collector Visibility – Inhalt
- Discovery

Legen Sie fest *sn_agent.appl_classification_behavior*Eigenschaft bis **Voll** , Und starten Sie jeden neu MID Servers Mit dem Service Desk-Mitarbeiter verbunden.

Bei der Arbeit in Windows Umgebung: Stellen Sie sicher, dass Sie mit Powershell 3,0 oder höher arbeiten.

Erforderliche Rolle (auf dem Hostgerät):

- In einem Linux Oder macOS Umgebung: servicenow-Anwender mit untergeordneten Elementen; nopasswd aktiviert mit „Normal“ Discovery Befehle.
- In einem Windows Umgebung: Lokaler Systemanwender, SYSTEM oder ein lokaler Anwenderaccount, in dem der lokale Anwenderaccount eine der folgenden Elemente verwendet:
  - Melden Sie sich als Service an
  - Sicherung (SeBackupPrivilege)
  - Berechtigungen für Debuggen von Programmen

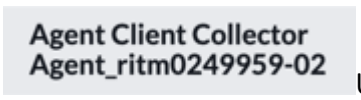
Verwendung der Zulässigkeitsfunktion für die Musterausführung

Legen Sie fest *enable-patterns-on-agent*Parameter bis **Wahr** In acc.yml Datei. Weitere Informationen finden Sie unter KB1585764 Knowledge Base-artikel.

Unterstützte Anwendungsmuster anzeigen

Um die Liste der für unterstützten Muster anzuzeigen Agent Client Collector, Navigieren Sie zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an. Anwendungsmuster sind die einzigen Mustertypen, die für die Verwendung mit unterstützt werden Agent Client Collector.

Sie können die Anwendungsmuster anzeigen, die für einen bestimmten Agent ausgeführt wurden.

1. Navigieren zu **Alle** > **Agent Client Collector** > **Service Desk-Mitarbeiter**an.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. Wählen Sie den Namen des Service Desk-Mitarbeiters aus, und halten Sie ihn gedrückt 

Und wählen Sie aus **Ansicht** > **Discovery**an.
4. Wählen Sie aus **Anwendungsmusterprotokolle** Registerkarte unten auf der Seite.

   Die Liste der für den Agent ausgeführten Muster wird angezeigt. Ausgeführte Muster werden mit dem Wert angezeigt **Wahr** In der Spalte ausgeführt für Agent.

Nicht unterstützte Anwendungsmustervorgänge

Anwendungsmuster werden in den folgenden Mustervorgängen nicht unterstützt:

- Auslösen der WMI-Methode
- Ändern/Ändern des Anwenders aufheben

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alle anwenderdefinierten Vorgänge
- SNMP-Abfrage
- Datei einfügen

Agent Client Collector Eigenschaften der Musterausführung

Konfigurieren Sie die folgenden Eigenschaften (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**), um die Verwendung von Anwendungsmustern mit zu maximieren Agent Client Collector:

Eigenschaften des Anwendungsmusters

Eigenschaft	Beschreibung
sn_Agent.appl_classification_Behavior	Legen Sie den Wert auf fest **Voll** Ermöglicht die Arbeit mit Anwendungsmustern und den Zugriff auf Musterbefehle in der Allow-Liste. Standard: Einfach **Hinweis:** Um die Ausführung von Anwendungsmustern mit der Allow-Liste zu aktivieren, verwenden Sie die Vorlage Allow-list für Anwendungsmuster. Weitere Informationen finden Sie unter Musterausführung für ACC: Beispiel-Allowlist für Musterinhalt artikel in Now Support Knowledge Base.

MID-Server Konfigurationsparametereigenschaften

mid.discovery.agent.command.mid.timeout	Die maximale Dauer in Sekunden, die der hat MID-Server Wartet auf eine Antwort des Service Desk-Mitarbeiters, bevor eine Zeitüberschreitung eintritt. Standard: 60 Sekunden
mid.discovery.agent.command.timeout	Die maximale Zeit in Sekunden, die der Befehl für die Ausführung auf dem Agent-Host gewährt wird. Standard: 60 Sekunden

Verwenden des Musterdesigner-Debugging im ACC-Modus

Sie können Anwendungsmuster debuggen, die im ACC-Modus konfiguriert sind.

1. Legen Sie fest *`sn_agent.appl_classification_behavior`*Eigenschaft bis **Voll** .
2. Aktivieren Sie im Musterdesigner die Debug-Option, und wählen Sie aus **Verwenden Sie die ACC-Verbindung** Im Abschnitt Debug-Identifizierung.

Das Musterprotokoll gibt an, ob das Muster erfolgreich auf dem Agent ausgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Musterdetails auch in den folgenden Protokollen erhalten:

- MID-Server Protokolle: Festgelegt `mid.log.level`Dient zum DEBUGGEN für das MID-Agent-Protokoll, um Details zum Musterschritt, zur ACC-Prüfung und zur Musterantwort anzuzeigen.
- ACC-Protokolle: Suchen Sie nach der Zeichenfolge `PatternOnTheFlyCheck`Für Details zu Musterprüfungen.

Oracle Globale GLAS-Datensammlung (Global License Advisory Services)

Oracle Java Process Discovery funktioniert entweder mit Mustern (bei Verwendung eines MID-Server Oder Agent Client Collector), oder mit dateibasierter Discovery (mit Agent Client Collector Mit dateibasierter Discovery). Wenn sowohl die Muster- als auch die dateibasierte Discovery dieselbe Java-Installation ausführen, haben die mustererfassten Daten Vorrang.

Beim Ausführen Discovery Mit Agent Client Collector, Stellen Sie sicher, dass Sie über die folgenden Einstellungen verfügen:

- Alle Anwender müssen über verfügen Oracle GLAS-Store-App, ab Version 1,8.4.
- Agent Client Collector Anwender:
  - Muss haben Agent Client Collector Framework Plugin speichern.
  - Kann haben Agent Client Collector Visibility – Inhalt Speichern Sie das Plugin für zusätzliche Daten.

  Informationen zum privilegierten Anwenderzugriff finden Sie unter KB1705845 .

  Hinweis: Oracle Java-Discovery mit ACC gilt in allen Serverumgebungen. Derzeit wird sie jedoch teilweise für verschiedene Desktop-Umgebungen unterstützt. Für ein Windows Desktop-Update-Satz siehe KB-artikel KB1705845 .

Für Informationen zur Java-Installation Discovery Verwenden Agent Client Collector Visibility – Inhalt, Siehe Erkennen Sie Java-Installationsdaten mit Agent Client Collector Visibility – Inhalt Dateibasierte Discovery.

Informationen zu den erfassten Daten finden Sie unter Daten, die während erfasst wurden Agent Client Collector Visibility – Inhalt Dateibasiert Discovery.

Unterstützung von Anwendungsmustern Oracle GLAS-Datensammlung in einem Linux Umgebung. Weitere Informationen zur Verwendung von Mustern finden Sie unter Oracle Global License Advisory Services (GLAS) – Datenerfassung anhand von Mustern.

Obwohl Oracle GLAS unterstützt PUT-Dateivorgänge, die zugehörigen Dateien werden mit bereitgestellt Agent Client Collector Plugins anstelle von SSH oder WMI.

Zugehörige Informationen

Von ITOM-Transparenz verwendete Erkennungsmuster

Erkennen Sie Java-Installationsdaten mit Agent Client Collector Visibility – Inhalt Dateibasierte Discovery

Java-Installationsdaten werden mit erkannt Agent Client Collector Visibility – Inhalt Mit der dateibasierten Discovery können Sie Dateiinformationen in Ihrem System erkennen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Installieren Sie die neueste Version von Agent Client Collector Visibility – Inhalt.
- Installieren Sie die dateibasierte Discovery.
- Aktivieren Sie Oracle Global License Advisory Services (GLAS) – Hardwaredatenerfassungsrichtlinie.

Erforderliche Rolle: discovery_admin

Prozedur

1. Aktivieren Sie die dateibasierte Discovery.
   a. Navigieren zu **Alle** > **Discovery-Definition** > **Konfigurationskonsole**an.
   b. Aktivieren Sie **Datei-Discovery** Eintrag.
2. Aktivieren Sie die Java Discovery-Eigenschaft.
   a. Suchen Sie nach *sn_acc_vis_content.file_discovery.enable_java_discovery*Eigenschaft auf der Seite „Systemeigenschaften“ (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an.
   b. Legen Sie den Eigenschaftswert mit **wahr** fest.
3. Gewähren Sie dem erhöhte Berechtigungen acc Anwender, der Zugriff auf Ihre Java-Installationsverzeichnisse aktiviert, z. B.:
   - /Usr/lib/jvm/*/bin/Java
   - /Usr/lib/jvm/*/*/bin/Java

   Sie können während der Java-Installation nach Bedarf zusätzliche Java-Verzeichnisse hinzufügen.
   - In einem Linux Umgebung, gewähren Sie erhöhte Berechtigungen in /Etc/sudoers Datei zum Aktivieren des Zugriffs auf die Java-Installationsverzeichnisse.
   - In einem Windows Umgebung: Gewähren Sie über den Systemadministrator erhöhte Berechtigungen (Lesen und Ausführen), um Zugriff auf die Java-Installationsverzeichnisse zu ermöglichen.

Ergebnis

Bei Ausführung Discovery Bei der Java-Installation werden Daten durch dateibasierte Discovery erkannt und in gespeichert Ora_Java_Audit Tabelle. Details zu den in dieser Tabelle gespeicherten Daten finden Sie unter Daten, die während erfasst wurden Agent Client Collector Visibility – Inhalt Dateibasiert Discovery.

DNS-Namen mithilfe pushbasierter Erkennung erkennen

CMDB-Verantwortliche sind darauf angewiesen, dass CIs alle Domänensystemnamen (DNS) enthalten, die dem System zugeordnet sind. Beginnt in Agent Client Collector Visibility – Inhalt(ACC-VC) Version 2,3.0, ACC-VC kann DNS-Namenslisten für erkennen Windows Und Linux CIs.

Bei der Erkennung von DNS-Namen, die Systemen zugeordnet sind, geschieht Folgendes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- network_adapters.rb wird dazu verwendet, den DNS-Namen für alle IP-Adressen mithilfe von Osquery auszufüllen. (Es gibt keine Begrenzung.)
- Nslookupcommand wird dazu verwendet, den DNS-Namen für alle IP-Adressen abzurufen.

Hinweis: Nslookup muss auf dem Zielsystem konfiguriert sein.

Dadurch wird eine Beziehung von erstellt *Owns::Owned by*Zwischen dem CI und den DNS-Namen.

Diese Informationen werden dann in die Tabelle [cmdb_ci_dns_name] eingetragen.

Portable Anwendungen mit pushbasierter Erkennung ermitteln

Portable Anwendungen sind Anwendungen, die nicht auf dem Zielsystem installiert werden müssen. Ab ACC-VC Version 2,3.0, Push-basiert Discovery Kann tragbare Anwendungen erkennen, z. B. Firefox, VLC, Notepad++ usw., für Windows Nur.

Hinweis: Nur portable Anwendungen, die unter https://portableapps.com/ aufgeführt sind, werden unterstützt.

Wenn die portable Anwendung ausgeführt wird, wird ein laufender Prozess erstellt. Von der Anwendung wird ein Pfad ähnlich dem folgenden für die Konfigurationsdatei appinfo.ini erstellt:

```
-\ <--- Directory with FirefoxPortable.exe
 +\App
 +\firefox
 +\Data
 +\profile
 +\settings
 +\plugins\ (optional)
```

Hinweis: Benutzer von ServiceNow-Systemen müssen auf das lokale Konto zugreifen können, um die Daten abzurufen und die Datei appinfo.ini zu lesen.

Die Attribute Name, Version und Lieferant werden aus der portablen Software abgerufen und befinden sich in den appinfo.ini-Dateien. Die Datei appinfo.ini ist die zum Ausführen einer portablen Anwendung zwingend notwendige Datei. Wenn SAM installiert ist, werden die Informationen in der Softwareinstallationstabelle [cmdb_sam_sw_install] angezeigt. Wenn SAM nicht installiert ist, werden die Informationen in der Softwareinstanzentabelle [cmdb_software_instance] angezeigt.

Ausschlusslisten für IP-Adressen und NIC festlegen

Agent Client Collector Visibility – Inhalt (ACC-VC) Version 1.3.0 unterstützt Ausschlusslisten für IPs und Netzwerkschnittstellen-Controller (NICs) mit einem flexiblen Mechanismus zum Herausfiltern von Werten für IPs und/oder NICs beim Erstellen oder Aktualisieren des Host-CI und der zugehörigen Elemente.

Die Eigenschaft [*sn_acc_visibility.network_adapter_exclusion_list*] enthält die Liste der regulären Ausdrücke für die Namen und IP-Adressen, die in den Tabellen „Netzwerkadapter“ und „IP-Adresse“ ausgeschlossen sind. Der Wert dieser Eigenschaft sind durch Kommata getrennte reguläre Ausdrücke. Stellen Sie sicher, dass der reguläre Ausdruck kein Komma enthält. nic und ip_addr sollten in verschiedenen Zeilen stehen.

Beispielformat für den Wert sollte folgendes sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- nic = nameRegex1, nameRegex2, nameRegex3
- ip_addr = IPRegex1, IPRegex2

Attribut „Zugewiesen an“ in Computer-CI für wird ausgefüllt Agent Client Collector Visibility – Inhalt

Um das Attribut Zugewiesen an des Computer-CI zu aktualisieren, müssen Sie Informationen vom angemeldeten Anwender erfassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie können Zugewiesen an für automatisch ausfüllen Windows Endpunktgeräte und macOS Geräte wie Workstations oder Mitarbeiter-Laptops als Teil der Agent-basierten Discovery mit ACC-VC mit diesen beiden Systemeigenschaften. Siehe Verfügbare Systemeigenschaften Weitere Informationen finden Sie unter .

- **sn_acc_vis_content.set_assigned_to**
- **sn_ACC_VIS_content.assigned_to_user_order**
- **sn_ACC_VIS.column_Name_for_user_Mapping**

Prozedur

1. Erstellen Sie höhere Anwenderberechtigungen, um die Details des angemeldeten Anwenders abzurufen. Verwenden Sie Anmelden als lokalen Systemanwender anstelle des Standardwerts ServiceNowAnwender zum Ausführen von Agent Client Collector.

   Diese Befehle werden auf ausgeführt Windows Computer:

   - WMIC COMPUTERSYSTEM – ANWENDERNAMEN ABRUFEN
   - Aus osquery: WÄHLEN SIE „l.user“ AUS „log_in_users“ AUS. L JOIN users u ON l.sid = u.uuid, WOBEI „u.type != „special“ ist.

   Dieser Befehl wird auf ausgeführt macOS Computer: WÄHLEN SIE DISTINCT(l.user) AUS „log_in_users“ AUS. L JOIN users u ON l.user = u.username

2. Die Übereinstimmung der Anwendernamen wird für die Anwenderdatensätze in der Tabelle „sys_user“ durchgeführt.
   Das Attribut Zugewiesen an wird ausgefüllt und erstellt dann einen Verweis auf den Anwender. Systemprotokolle zeigen eine Warnung an, wenn in sys_user kein Anwender gefunden werden kann. Die Anwendernamen, die für das Attribut „Zugewiesen an“ bezogen werden, basieren auf der Systemeigenschaft: **sn_ACC_VIS_content.assigned_to_user_order** .

3. Das Attribut „Assigned_to“ wird basierend auf Prioritäten festgelegt.
   Wenn „assigned_to“ bereits vorhanden ist, behalten Sie es standardmäßig unverändert bei. Sie können jedoch aktualisieren **sn_acc_vis_content.set_assigned_to** Systemeigenschaft zum Überschreiben. Wenn Abgleichsregeln definiert sind, füllt die IRE das Feld entsprechend aus.

Ergebnis

In der Tabelle „sys_user“ wird kein neuer Anwenderaccount erstellt. Stattdessen wird der vorhandene Anwender abgefragt, und derselbe wird als „Zugewiesen an Anwender“ für ein CI referenziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender werden basierend auf dem Typ für ausgefüllt Agent Client Collector Visibility – Inhalt

Sie können den Typ der Anwender beibehalten, die die CMDB ausfüllen, je nach Ihren Interessen. Derzeit werden lokale und System für unterstützt Windows, Linux, Und macOS.

Sie können die Anwendertypen mithilfe der Systemeigenschaft filtern: **sn_ACC_Visibility.persist_os_user_type** . Siehe Verfügbare Systemeigenschaften Weitere Informationen finden Sie unter .

Für Windows

Sie müssen identifizieren, ob ein Server Domänencontroller ist oder nicht. Da Domänencontroller-Computer keine lokalen Accounts haben, bleiben lokale Anwenderinformationen für diese Computer nicht erhalten und werden nicht ausgefüllt.

Verwenden Sie für Windows-Computer ohne Domänen-Controller OSquery-Befehle, um Anwenderinformationen über ACC-VC abzurufen: Auswählen *`uid`* , *`Anwendername`* , *`Verzeichnis`* , *`Typ`* Von Anwendern, wo **Typ=lokal** Oder **Typ=Spezial** .

Für Linux

Die userID definiert, ob ein Anwender ein lokaler Account oder ein Systemaccount ist. Dies wird durch definiert *`UID_MIN`*Und *`UID_MAX`*.

Verwenden Sie diesen Befehl, um Anwenderinformationen über ACC-VC abzurufen, um sie abzurufen *`UID_MIN`*Und *`UID_MAX`*Wert: *`Grep -E „^UID_MIN|^UID_MAX“ /etc/login.defs`* .

Verwenden Sie diesen Befehl, um Anwendernamen abzurufen: *`Cat /etc/passwd | awk -F“: „{print $1,$3,$6`* .

Für macOS

Verwenden Sie OSquery-Befehle, um Anwenderinformationen über ACC-VC: Select abzurufen *`uid`* , *`Anwendername`* , *`Verzeichnis`* Von Anwendern. Anwendernamen, denen „_“ vorangestellt ist, werden als Systemaccounts behandelt. Andere sind lokale Accounts.

Führen Sie die Zertifikat-Discovery über aus Agent Client Collector Visibility – Inhalt

Erkennen Sie TLS-/SSL-Zertifikate, die von Ports verwendet werden, die auf dem Server des Service Desk-Mitarbeiters ausgeführt werden. Die Zertifikatsbestand-Management Die Anwendung verwendet diese Informationen, um TLS-/SSL-Zertifikate zu verwalten.

Vorbereitungen

Überprüfen Sie, ob die neueste Version von ist Agent Client Collector Visibility – Inhalt(ACC-VC) ist installiert.

Überprüfen Sie, ob die neueste Version von ist Zertifikatsbestand-Management Ist installiert.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**an.
2. Aktivieren Sie *`TLS SSL Certificate Capture`*Richtlinie.
3. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
4. Suchen Sie nach der Eigenschaft *`sn_acc_vis_content.tls_ssl_scanner_ports`*, und wählen Sie sie aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie eine kommagetrennte Liste von Portnummern ein, für die im nach Zertifikaten gescannt werden soll **Auswahlmöglichkeiten** Feld.
   Standardmäßig sind die Werte mit den für konfigurierten Werten identisch `tls_ssl_certs`Eigenschaft.
6. **Wahlweise:** Um das Originalzertifikat in der Instanz zu speichern, legen Sie fest `sn_acc_vis_content.tls_ssl_keep_original`Eigenschaft bis **Wahr** .

Ergebnis

Die Agent Client Collector Erfasst die Daten und erkennt die TLS/SSL-Zertifikate. Diese Daten sind mit den Daten identisch, die vom IP-basierten erfasst werden `tls_ssl_probe`Eigenschaft.

Die TLS/SSL-Zertifikate werden in den folgenden Tabellen ausgefüllt:

- Erkannte Zertifikate [sn_Disco_certmgmt_certificate_history]
- Eindeutige Zertifikate [cmdb_ci_certificate]
- Installierte Zertifikate [sn_Disco_certmgmt_cmdb_installed_certificate]

Zwischen den erkannten Zertifikaten und dem entsprechenden Host-CI (in diesem Fall der Server des Service Desk-Mitarbeiters) wird eine CI-Beziehung erstellt.

Zugehörige Informationen

Zertifikatsbestand-Management

Wenn über Port-Scans ausführen

Cloud Native Operations für Transparenz

Cloud Native Operations für Transparenz(CNO für Transparenz) Wurde in Agent Client Collector für Kubernetes – Transparenz umbenannt. Die Bedingung Cloud Native Operations für Transparenz Wurde veraltet.

Für Agent Client Collector für Kubernetes – Transparenz Dokumentation, siehe Kubernetes Discovery mit Agent Client Collector für Kubernetes – Transparenz.

Agent Client Collector Visibility – Inhalt – Referenz

Die folgenden Informationen enthalten Details zu Abfrageskripts des Betriebssystems, zu erfassten Daten und zur Definition von Begriffen.

BS-Modulskripts für Agent Client Collector Visibility – Inhalt(ACC-VC)

Diese plattformspezifischen Plugins rufen plattformspezifische Modulskripts auf. Jedes Skript gibt an eine JSON-Standardnutzlast unabhängig von der Plattform aus.

Betriebssystemfamilie/Plugin	Name des Modulskripts
Linux: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	data_collection.rb
	running_processes.rb
	tcp_connections.rb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystemfamilie/Plugin	Name des Modulskripts
Windows: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	data_collection.rb
	running_processes.rb
	tcp_connections.rb
macOS-Betriebssysteme: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	running_processes.rb
	tcp_connections.rb
Linux: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb
	cloud.rb
Windows: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb
	cloud.rb
	sam_advanced.rb
	sam_processor.rb
	intel_ema.rb
macOS-Betriebssysteme: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystemfamilie/Plugin	Name des Modulskripts
	cloud.rb

Hinweis:

running_processes.rb und tcp_connections.rb sind voneinander abhängig. Daher sollten Sie für eine effiziente Discovery sowohl tcp_connection.rb als auch running_processes.rb beibehalten. Beide Dateien werden benötigt, um vollständige Daten zu erhalten. Wenn eine nicht vorhanden ist, sind die entsprechenden Daten nicht verfügbar.

Um Informationen zu allen running_processes auf dem macOS abzurufen, müssen Sie sudo-Zugriff für osquery bereitstellen. Wenn diese Konfiguration nicht vorgenommen wird, wird von running_processes.rb nur das abgerufen, was vom _servicenow-Benutzer ausgelöst wird. Für tcp_connections.rb müssen Sie in der Datei „sudoers“ den Befehl „sudo lsof“ hinzufügen. Wenn diese Konfiguration nicht vorgenommen wird, wird von tcp_connections.rb nur das abgerufen, was vom _servicenow-Benutzer ausgelöst wird.

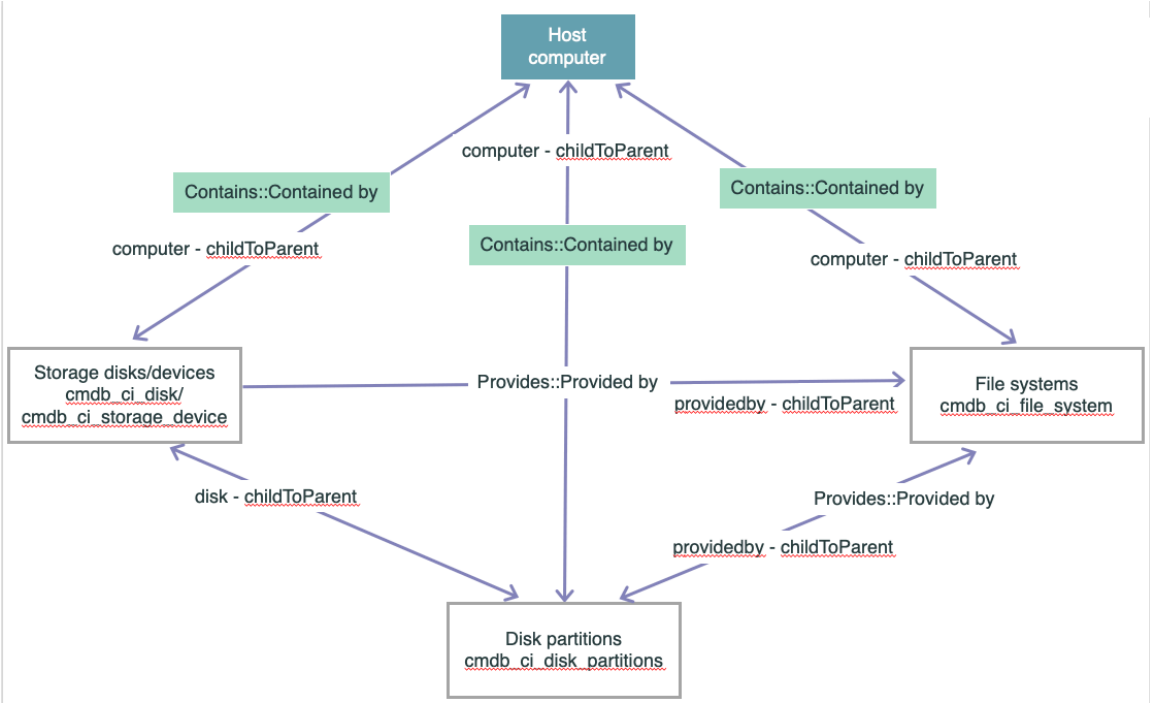
Erfasste Daten

ACC-VC verwendet dieselben Klassifizierungskriterien wie IP-basiert Discovery Zur Klassifizierung als Computer oder Server. Die Teilmenge der erfassten Daten umfasst die folgenden Kategorien:

- Basisbestand – Ab ACC-F Version 2.10.1 wird diese Kategorie nicht mehr verwendet.
- Datensammlung – Sammelt die erforderlichen Daten für die Klassifizierung und Identifizierung eines Host-CI. Dazu gehören Hostname, Seriennummern und Betriebssysteminformationen.
- Installierte Software – cmdb_sam_sw_install (wenn SAM aktiviert ist) und cmdb_software_instance (wenn SAM nicht aktiviert ist)
- Dateisystem – cmdb_ci_file_system
- Speichergeräte – cmdb_ci_disk und cmdb_ci_storage_device
- Seriennummern – cmdb_serial_number
- Netzwerkadapter – cmdb_ci_network_adapter und cmdb_ci_ip_address
- TCP-Verbindungen – cmdb_tcp
- Laufende Prozesse – cmdb_running_Process (ACC-VC klassifiziert auch die laufenden Prozesse und erstellt Anwendungs-CIs in cmdb_ci_appl, wenn möglich)
- Lokaler Anwender – cmdb_os_user (füllt die lokalen Anwender für alle von ACC-VC unterstützten Betriebssysteme aus, indem ein neues Modul namens local_user hinzugefügt wird)
- Erweiterter Bestand – Sammelt erweiterte Daten (z. B. CPU-Informationen, start_date, object_id), die zum Identifizieren eines eindeutigen Hosts nicht erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen zwischen Hostcomputer, Dateisystemen und Speichergeräten



Agent Client Collector Begriffe

Agent Client Collector (ACC)

Die auf Zielhosts installierte Softwarekomponente, die mit dem MID-Server kommuniziert. Wird manchmal auch als Agent bezeichnet. Diese Komponente ist ein ServiceNow-Derivat von Sensu-Go.

Agent Client Collector Framework (ACC–F)

A ServiceNow Bereichsbezogene Basisanwendung, die ACC nutzt und Kernfunktionen (einschließlich Prüftypen, Prüfungsdefinitionen, Richtlinien usw.) bereitstellt, die andere bereichsbezogene ACC-Anwendungen ermöglicht, einschließlich ACC-M und ACC-VC.

Agent Client Collector-Überwachung Überwachung (ACC-M)

Eine bereichsbezogene ServiceNow-Anwendung, die die Überwachung von Anwendungsfällen ermöglicht.

Agent Client Collector Visibility – Inhalt (ACC-VC)

Eine bereichsbezogene ServiceNow-Anwendung, die pushbasierte Discovery mit ACC und ACC-F implementiert.

Horizontal IP-basiert Discovery

Traditionell Discovery Verfügbar für Kunden vor ACC-VC. Dabei werden Daten über Probes und Muster durch den MID-Server erkannt. Hierzu ist das Plugin „Discovery“ erforderlich.

Module

Teilmenge der erkannten Daten, die im Rahmen der Discovery gefüllt werden. Beispiele für Module: Datensammlung, Installierte Prozesse, Seriennummern, Dateisysteme, Speichergeräte, Netzwerkadapter, Laufende Prozesse und TCP-Verbindungen.

Pushbasierte Discovery

Erkennen Sie Daten über ACC, ACC-F, ACC-VC und MID-Server Mit einem direkten Push von Daten vom Zielhost. Discovery Erfordert keine spezifische IP-Bereichskonfiguration auf einem Discovery Zeitplan oder Bereitstellung Discovery Anmeldeinformationen für Zielhost.

Sensu-Go-Agent

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das kostenlose Open Source-Projekt, aus dem ACC abgeleitet ist.

VM-Instanz

Ein virtueller Zielhost, der innerhalb eines Hypervisor ausgeführt wird, entweder lokal oder innerhalb eines Cloud Service Providers wie AWS, GCP oder Microsoft Azure.

VM-Abbild

In einem Dateisystem oder Cloud-Speicher abgelegter Snapshot der Live-Instanz einer virtuellen Maschine (VM).

Agent Client Collector Visibility – Inhalt – Standardprüfungen und Richtlinien

Agent Client Collector Visibility – Inhalt (ACC-VC) stellt verschiedene Prüfungen und Richtlinien sowie eine Business-Regel bereit.

Richtlinien

Hinweis: ACC-VC-Richtlinien werden mit einer Häufigkeit von einmal pro Tag ausgeführt. Die insgesamt erfasste Datenmenge beträgt etwa 572 KB. Dabei werden durchschnittlich etwa 1.500 installierte Softwareanwendungen und etwa 500 laufende Prozesse (mit Ausnahme von CI-Daten) pro Computer berücksichtigt.

ACC-VC-Richtlinien

Name	Beschreibung	Überprüft Definitionen
Erweiterte Erkennung	Wird standardmäßig alle 24 Stunden (86400 Sekunden) nach einem Zeitplan ausgeführt. Das Richtlinienintervall kann angepasst werden, z. B. so, dass es alle 4 Stunden ausgeführt wird (setzen Sie das Intervall auf 14.400). Die ACC-VC-Richtlinienkonfiguration wird basierend auf dem von ACC-VC definierten Richtlinienfilter mit allen Service Desk-Mitarbeitern synchronisiert. Aktualisieren Sie bei Bedarf die folgenden ACC-F-Systemeigenschaften: • *sn_agent.disco_minimum_threshold_for_rediscovery_minutes*: Um zu vermeiden, dass das System zu häufig erkannt wird. • *sn_agent.disco_disable_ci_clobber_of_agentless_disco*: Zu vermeiden Discovery Konflikte. • *sn_agent.disco_ci_clobber_of_agentless_disco_threshold_days*: Zu vermeiden Discovery Konflikte.	Erweiterte Erkennung
SAM-Discovery	Verantwortlich für die Erfassung der auf einem Endpunktgerät installierten Software, z. B.	Softwareinstallationen und Nutzungsmetriken

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Richtlinien (Fortsetzung)

Name	Beschreibung	Überprüft Definitionen
	Windows Desktops oder macOS Server.	
SAM-Hintergrund	Aktiviert einen Hintergrundauftrag zur Verarbeitung der Osqueryd-Protokolle für SAM in Windows Und macOS Endpunktgeräte.	SAM-Hintergrundprotokollprüfung
SAM-Hintergrund (nicht OsqueryD)	Ermöglicht einem Hintergrundauftrag, SAM-Informationen mit osqueryi anstelle von osqueryd zu erfassen.	SAM-Hintergrundrichtlinie (nicht OsqueryD)
Software installiert	Verantwortlich für die Erfassung der auf allen Geräten mit Ausnahme von installierten Software Windows Endpunktgeräte. Die erfassten Daten werden in der Tabelle [cmdb_sam_sw_install] gespeichert. Geplant für die Ausführung alle 24 Stunden.	Installierte Software
Dateibasierte Discovery-Hintergrundrichtlinie	Verwendet die Konfigurationsdatei als Eingabe aus der Instanz an einen Service Desk-Mitarbeiter. Scannt das System mithilfe von Konfigurationsdateiparametern und speichert die Ausgabe auf dem Agent. Wird auf dem Agent ausgeführt, wenn die dateibasierte Discovery aufgerufen wird. Details finden Sie unter File-based Discovery.	Dateibasierter Discovery-Hintergrund
Dateibasierte Discovery-Richtlinie	Sammelt die Ausgabedatei vom Service Desk-Mitarbeiter. Sendet die gesammelten Informationen an die Konfigurationstabellen. Wird auf dem Agent ausgeführt, wenn die dateibasierte Discovery aufgerufen wird. Details finden Sie unter File-based Discovery.	Dateibasierte Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Richtlinien (Fortsetzung)

Name	Beschreibung	Überprüft Definitionen
	Hinweis: • Während der dateibasierten Discovery auf einem Windows System, verfügt der servicenow-Anwender nicht über die erforderlichen Berechtigungen. Gewähren Sie daher dem Ordner, den Sie scannen möchten, manuell die Berechtigung Ordnerinhalte auflisten. • Um sicherzustellen, dass die Dateiversion erfolgreich abgerufen wird, führen Sie den Service Desk-Mitarbeiter als lokalen Systemaccount-Anwender anstelle von aus *servicenow*Anwender.	

Hinweis: Windows Endpunktgeräte umfassen Geräte, die über einen verfügen Windows Betriebssystem und gehören zur CI-Klasse: Computer.

Siehe Systemeigenschaften Für weitere Details. Weitere Informationen zu Richtlinien finden Sie unter Prüfungen und Richtlinien.

Überprüfungstyp

ACC-VC hat die folgenden Prüftypen: *EnhancedDiscovery*, *SAM Advanced Discovery*, Und *Installed Software*.

EnhancedDiscovery

Dieser Überprüfungstyp ist für den Aufruf der Skripteinbindung EnhancedDiscoveryHandler verantwortlich, die die von endpoint_discovery.rb generierte Nutzlast verarbeitet, wie sie von ACC ausgeführt wird.

SAM Advanced Discovery

Dieser Prüftyp gilt für die SAM-Discovery-Richtlinie, die die Skripteinbindung EnhancedDiscoveryHandler für die Verarbeitung der SAM-Daten aufruft, die von der Datei „sam_Advanced.rb“ erzeugt werden.

Installed Software

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Überprüfungstyp ist für die *`Software installed policy`* vorgesehen, nach der die Skripteinbindung EnhancedDiscoveryHandler zur Verarbeitung der Daten über die installierte Software aufgerufen wird, die von der Datei installed_software.rb erzeugt werden.

Prüfungsdefinitionen

ACC-VC-Prüfungsdefinitionen

Name	Beschreibung

Erweiterte Erkennung	Wird basierend auf dem von ACC-VC definierten Richtlinienfilter mit allen Service Desk-Mitarbeitern synchronisiert. Die Prüfungsdefinition ist für die Ausführung mit bestimmten Assets konfiguriert und bestimmt, was zwischen dem Service Desk-Mitarbeiter und dem synchronisiert wird MID-Server. Weitere Informationen zu Richtlinien finden Sie unter Prüfungen und Richtlinien.
	Hinweis:
	Damit der Service Desk-Mitarbeiter die BS-Seriennummern und TCP-Verbindungen zusammen mit zugehörigen laufenden Prozessen abrufen kann, ist sudo-Zugriff für „dmidecode“ und „ss“ für erforderlich Linux Systeme. Zum Beispiel kann dies zu /etc/sudoers oder zu einer einzelnen Datei in /etc/sudoers.d/ hinzugefügt werden:
	`Cmnd_Alias AGENT_ACC_V = /usr/sbin/dmidecode -s baseboard-serial-number,/usr/sbin/dmidecode -s chassis-serial-number,/usr/sbin/dmidecode -s system-serial-number,/usr/sbin/dmidecode -s system-uuid,/usr/sbin/ss -tanp`
	`servicenow ALL=(root) NOPASSWD:AGENT_ACC_V`

SAM-Hintergrundprotokollprüfung	Wird alle 8 Minuten ausgeführt und führt eine Inline-Zusammenfassung der Daten durch, die aus Osqueryd-Protokollen generiert wurden. Nach dem Sammeln der Daten werden alle Zwischendatenergebnisse in eine temporäre Markierungsdatei geschrieben, die bei der nächsten Ausführung wiederverwendet wird. Diese Wiederverwendung begrenzt die Anzahl der Protokolldateien und den erforderlichen Speicherplatz auf den Zielsystemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Prüfungsdefinitionen (Fortsetzung)

Name	Beschreibung
	Hinweis: Möglicherweise bemerken Sie einen Anstieg des Verbrauchs von Systemressourcen, da die Hintergrundzusammenfassungsprüfung jedes Intervall ausgeführt wird.
Softwareinstallationen und Nutzungsmetriken	Erfasst alle 24 Stunden Daten.
Installierte Software	Ruft installierte Softwaredaten für alle Geräte außer ab Windows Und macOS Endpunktgeräte.
Dateibasierter Discovery-Hintergrund	Führt einen Hintergrundauftrag zum Scannen von Dateien für den Service Desk-Mitarbeiter aus.
Dateibasierte Discovery	Ruft die Dateidaten vom Service Desk-Mitarbeiter ab.

Business-Regel

Die Geschäftsregel *Enhanced Discovery - On CI Delete* löst die Endpunkterkennungsprüfung aus, wobei das einem bestimmten CI zugeordnete CI aus sn_agent_cmdb_ci_agent gelöscht wird.

Agent Client Collector Parameter für Installationsbefehl ohne MID

Beschreibung der Befehlszeilenparameter, die während der MID-Phase ohne verwendet werden Agent Client Collector Installation.

Befehlszeilenparameter für Installation

Parameter	Beschreibung
CONNECT_WITHOUT_MID	Geben Sie An **Wahr** Zum Aktivieren von MID-less Agent Client Collector Installation. Wenn Sie keinen Wert angeben, der reguläre MID-Server websocket-Installation wird aufgerufen.
ACC_CNC	Geben Sie einen öffentlichen Gateway-Endpunkt für an Agent Client Collector.
REGISTRIERUNGSSCHLÜSSEL	Aktiver und gültiger Registrierungsschlüssel, mit dem der Service Desk-Mitarbeiter kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der der Service Desk-Mitarbeiter registriert ist.
ACC_ALLOW_LIST	Optionale Zeichenfolge; um die Allow-Liste zu deaktivieren, legen Sie fest *ACC_ALLOW_LIST=0*. Die Allow-Liste ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlszeilenparameter für Installation (Fortsetzung)

Parameter	Beschreibung
	Hinweis: Das Deaktivieren der Allow-Liste gefährdet die Sicherheit Ihres Systems und ist als temporäre Maßnahme während der Aktualisierung der Allow-Liste gedacht. Aktivieren Sie nach Abschluss des Updates die Einstellung Allow List by (Liste zulassen nach) **ACC_ALLOW_LIST=1** .
ACC_VALIDATE_SIG	Optionale Zeichenfolge; um die Verifizierung der Zertifizierungsvalidierung des Installationsprogramms zu deaktivieren, legen Sie fest *`ACC_VALIDATE_SIG=0`*Die Sie hinzufügen können, um die Verifizierung der Zertifizierungsvalidierung des Installationsprogramms zu deaktivieren. Die Validierung ist standardmäßig aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Zugehörige Informationen

Websocket-Server auf MID-Server installieren

Daten, die während erfasst wurden Agent Client Collector Visibility – Inhalt Dateibasiert Discovery

Die folgenden Tabellen beschreiben die während erfassten Daten Agent Client Collector Visibility – Inhalt Dateibasiert Discovery.

Java-Audit [ora_Java_Audit]

Feld	Beschreibung
Name	Name des Datensatzes. Beispiel: Java@Hostname
Name Des Physischen Computers	Name des Host-CI
Rechnertyp	Entweder Server(S) oder Desktop(D)
Java-Herausgeber/Runtime-Lieferant	Java-Lieferantenname
Betriebssystem	Betriebssystem, in dem die Java ausgeführt wird
Umgebungstyp	Produktions- oder Entwicklungs- oder QA-Umgebung
Java-Release/Version/Build	Java-Version
Installationspfad	Absoluter Installationspfad der Java-Binärdatei
Installationsdatum (Datum/Uhrzeit)	Datum und Uhrzeit der im Dateisystem erstellten Java-Binärdatei
Release-Datei (J/N)	Gibt an, ob A *`Release.md`* Datei ist in der Installation vorhanden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Java-Audit [ora_Java_Audit] (Fortsetzung)

Feld	Beschreibung
Prozessormarke/Modell	Name des Prozessormodells
Sockets (Ganzzahl)	Anzahl der CPU-Sockets
Kerne (Ganzzahl)	Anzahl der CPU-Kerne
V6 und früher	Gibt an, ob Sie haben eine Java-Version 6 oder früher
Open Source	Gibt an, ob Sie haben eine Open Source-Java-Installation
Schalten Sie kommerzielle Funktionen frei	Gibt an, ob Sie haben die kommerziellen Funktionen (z. B. JFR) aktiviert. Wird während der dateibasierten ACC-VC-Discovery (FBD) nicht erfasst.
Missionssteuerung	Gibt an, ob Das Plugin „Missionssteuerung“ ist aktiviert
AMC-Service Desk-Mitarbeiter	Gibt an, ob Das AMC Agent-Plugin ist aktiviert. Wird während der dateibasierten ACC-VC-Discovery (FBD) nicht erfasst.
Nutzungs-Tracker	Gibt an, ob Die Nutzungstracker-Funktion ist aktiviert
VM-Objekt-ID	Objekt-ID der VM-Instanz
PID	PID des laufenden Prozesses
IP-Adresse	IP-Adresse des Hosts/der VM
Zuerst erkannt	Das Datum der ersten Discovery
Neuester Discovery-Scan	Das Datum der letzten Discovery
Discovery-Quelle	Die Discovery-Methode
Anwendung	Verweis auf die Tabelle [cmdb_ci_appl]
Softwareinstallation	Verweis auf die Tabelle [cmdb_sam_SW_install]
Java-Nachweis	Verweis auf die Tabelle [cmdb_ora_Java_evidence]
Host	Verweis auf die Tabelle [cmdb_ci]

Java-Nachweis [ora_Java_evidence]

Feld	Beschreibung
Laufender Prozess	Verweis auf die Tabelle [cmdb_running_Process]
Host-CI	Verweis auf die Tabelle [cmdb_ci_Computer]
Datei-Informationen	Stellt einen Verweis auf die Tabelle [cmdb_file_Information] bereit. Relevant nur für dateibasierte Discovery (FBD); in der musterbasierten Discovery bleibt dieses Feld leer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erkennen Sie Java-Installationsdaten mit Agent Client Collector Visibility – Inhalt Dateibasierte Discovery

Agent Client Collector Log Analytics

Agent Client Collector Log Analytics (ACC-L) ermöglicht es Ihnen, Protokolldaten von Linux- und Windows-Hosts mit Agent Client Collector an eine ServiceNow-Instanz zu streamen.

Wie bei Agent Client Collector Framework (ACC-F) wird von Agent Client Collector eine Verbindung zu einem MID-Server hergestellt. Ein einzelner MID-Server kann mehrere Agents unterstützen. Im Rahmen des Failover-Schutzes funktioniert ein einzelner Agent jeweils mit einem MID-Server und wechselt bei Bedarf auf einen anderen MID-Server.

Verwenden Sie Agent Client Collector, um Protokolldaten mithilfe eines Protokollversenders an Ihre ServiceNow®-Instanz zu streamen. Die Protokolldaten werden in der Anwendung ServiceNow® Health Log Analytics zugeordnet und strukturiert. Weitere Informationen finden Sie unter Health Log Analytics Produktdokumentation.

Agent Client Collector Log Analytics Hat eine Abhängigkeit von Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store . Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

Die Anwendung Agent Client Collector Log Analytics (ACC-L), Version 3.2.0, August 2022, ist abhängig von der Anwendung Agent Client Collector Framework (ACC-F), Version 2.10.1, August 2022.

Um Agent Client Collector Log Analytics zu aktivieren, aktivieren Sie Protokollanalysen in Agent Client Collector, wie in Einrichten Agent Client Collector Log Analytics Ohne geführtes Setup beschrieben.

Abhängigkeiten

Für eine Liste von Agent Client Collector Log Analytics-Plugin-Abhängigkeiten, siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Setup von Agent Client Collector Log Analytics

Konfigurieren Agent Client Collector Log Analytics Auf Ihrem ServiceNow Instanz entweder mit oder ohne Verwendung des geführten Setups.

Einrichtung von Agent Client Collector Log Analytics mit Guided Setup

Das Guided Setup für Agent Client Collector Log Analytics stellt eine Reihe von Aufgaben bereit, die Sie bei der Konfiguration von Agent Client Collector Log Analytics für Ihre Instanz unterstützen. Durch die Verwendung des geführten Setups wird sichergestellt, dass Sie über das erforderliche Minimum für die Verwendung der Anwendung verfügen. Weitere Informationen finden Sie unter Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten.

Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Einrichtung von Agent Client Collector Log Analytics ohne Guided Setup

Wenn Sie kein geführtes Setup verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen. Weitere Informationen finden Sie unter Einrichten Agent Client Collector Log Analytics Ohne geführtes Setup.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten

Konfigurieren Agent Client Collector Log Analytics Auf Ihrem ServiceNow Instanz mit geführtem Setup.

Vorbereitungen

- Agent Client Collector Log Analytics Hat eine Abhängigkeit von ServiceNow® Ereignismanagement Anwendung. Einrichten Ereignismanagement Bevor Sie konfigurieren Agent Client Collector Log Analytics. Weitere Informationen finden Sie unter Setup von Ereignismanagement.
- ServiceNow Service Operations-Arbeitsbereich ITOM-Apps müssen installiert sein. Wenn sie nicht bereits installiert ist, installieren Sie sie manuell. Weitere Informationen finden Sie unter Installieren Service Operations-Arbeitsbereich Für ITOM Anwendung.

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. MTLs werden nicht unterstützt.

Erforderliche Rolle: agent_client_collector_admin

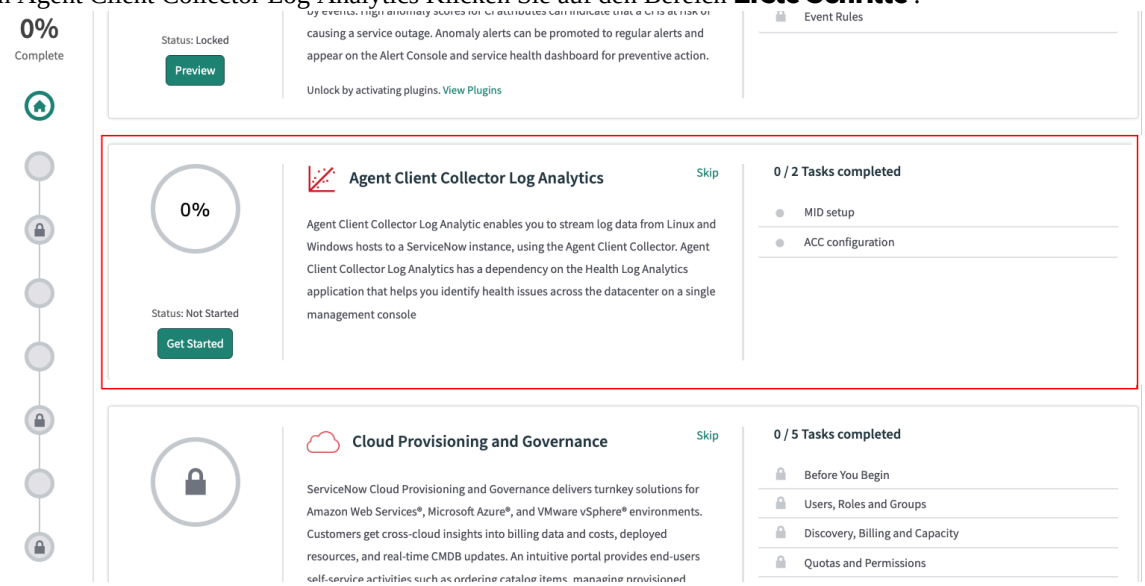
Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector Log Analytics Das geführte Setup bietet eine Reihe von Aufgaben, die Ihnen bei der Konfiguration helfen Agent Client Collector Log Analytics. Durch die Verwendung des geführten Setups wird sichergestellt, dass Sie über das erforderliche Minimum für die Verwendung der Anwendung verfügen.

Hinweis: Wenn Sie kein geführtes Setup verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen. Weitere Informationen finden Sie unter Einrichten Agent Client Collector Log Analytics Ohne geführtes Setup.

Prozedur

1. Navigieren zu **Alle** > **Geführtes Setup** > **Geführtes Setup für ITOM**an.
   Die IT Operations Management Der Willkommensbildschirm des geführten Setups wird angezeigt.
2. Wählen Sie Aus **Erste Schritte** .
3. In Agent Client Collector Log Analytics Klicken Sie auf den Bereich **Erste Schritte** .



4. In **MID-Setup** Führen Sie die entsprechende Aktion aus:

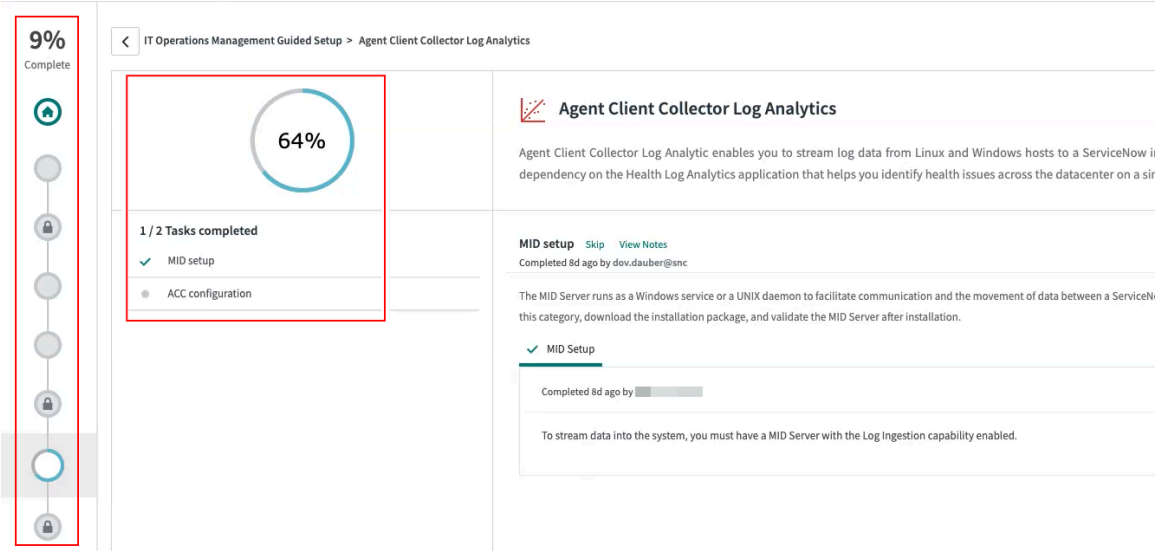
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie bereits konfiguriert haben MID-Server, Wählen Sie aus **Als abgeschlossen markieren** .
- Wenn Sie keinen konfiguriert haben MID-Server, Wählen Sie aus **Konfigurieren** Und richten Sie ein MID-Server, Und wählen Sie dann aus **Als abgeschlossen markieren** . Weitere Informationen finden Sie unter geführtes Setup für MID-Server verwenden.

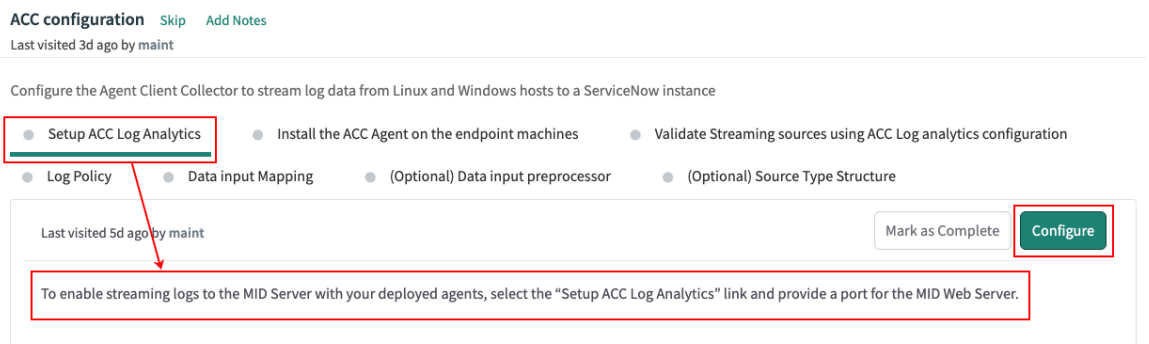
> **Hinweis:** Um Daten in das System zu streamen, benötigen Sie einen MID-Server Mit aktivierter Protokollerfassungsfunktion.

Wenn MID-Server Ist konfiguriert, der Statusindikator für Agent Client Collector Log Analytics Das geführte Setup zeigt, dass 64 % der Konfiguration abgeschlossen sind. Der Fortschrittsindikator zeigt den Fertigstellungsprozentsatz für alle an IT Operations Management Aufgaben.



5. Konfigurieren Sie Agent Client Collector Log Analytics.

a. In **ACC-Konfiguration** Wählen Sie eine Setup-Aufgabe aus, und lesen Sie die Anweisungen im Hilfebereich.



b. Wählen Sie Aus **Konfigurieren** Und schließen Sie die Aufgabe ab.
Detaillierte Informationen zu den einzelnen Setup-Aufgaben finden Sie im Agent Client Collector Log Analytics Produktdokumentation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Schließen Sie alle erforderlichen Setup-Aufgaben in der Aufgabenliste ab.

d. Wählen Sie Aus **Als abgeschlossen markieren** Um abzuschließen Agent Client Collector Log Analytics Konfiguration.

Einrichten Agent Client Collector Log Analytics Ohne geführtes Setup

Konfigurieren Sie Agent Client Collector Dient zum Streamen von Protokolldaten aus Linux Und Windows Hosts zu ServiceNow Instanz ohne geführtes Setup.

Vorbereitungen

Hinweis: Sie können konfigurieren Agent Client Collector Log Analytics Mit geführtem Setup. Das geführte Setup stellt sicher, dass Sie über das erforderliche Minimum für die Verwendung der Anwendung verfügen. Weitere Informationen finden Sie unter Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten.

- Das Plugin „Agent Client Collector Log Analytics“ (ACC-L) muss installiert sein. Das Plugin wird mit den Plugins „Agent Client Collector Framework“ (ACC-F) und „Agent Client Collector Monitoring“ (ACC-M) bereitgestellt. Weitere Informationen finden Sie unter Agent Client Collector Installationan.
- ServiceNow Service Operations-Arbeitsbereich ITOM-Apps müssen installiert sein. Wenn sie nicht bereits installiert ist, installieren Sie sie manuell. Weitere Informationen finden Sie unter Installieren Service Operations-Arbeitsbereich Für ITOM Anwendung.
- Agent Client Collector Log Analytics Hat eine Abhängigkeit von Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store . Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Agent Client Collector wird mit dem standardmäßigen `servicenow`-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector `servicenow`-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu /var/log/ unter Linux und des Pfads zu C:\Windows\System32 unter Windows. Informationen zum Konfigurieren von Berechtigungen für den `servicenow`-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. MTLs werden nicht unterstützt.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**an.
2. Auf der MID-Server Seite auswählen MID-Server Die validiert ist und einen Statuswert von hat **Aktiv** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Abschnitt „Zugehörige Links“ der MID-Server-Seite für den ausgewählten Server **Setup ACC Log Analytics** (ACC Log Analytics einrichten) aus.
   Das Setup von Agent Client Collector Log Analytics beginnt.

   Ferner wird vom System automatisch eine ACC-Dateneingabe erstellt. Nach der Erstellung wird der Dateneingabe-Datensatz der ACC-Dateneingabetabelle hinzugefügt, und die Dateneingabe ist zum Streamen von Protokollen bereit.

   Hinweis: Es ist wichtig, dass Sie eine ACC-Dateneingabe für jeden MID-Server konfigurieren, mit dem eine Verbindung von Agent Client Collector-Systemen hergestellt werden kann. Weitere Informationen finden Sie unter Zusätzliche ACC-Dateneingaben einrichten.

   Außerdem werden Sie vom System aufgefordert, den MID-Webserver einzurichten. Weitere Informationen finden Sie unter MID-Webserver.

4. Konfigurieren Sie im Dialogfeld „ACC Log Analytics Setup“ (ACC Log Analytics einrichten) die Ports.

   a. Geben Sie in den Feldern **Port des MID Web Server** und **ACC data input Port** (ACC-Dateneingabe-Port) die entsprechenden Port-Nummern ein.

   b. Wählen Sie **OK** aus.
      Die URL mit dem konfigurierten Endpunkt wird im Dialogfeld angezeigt.

   c. Kopieren und speichern Sie die Endpunkt-URL, um sie bei der Installation des ACC-Agent auf dem Endpunkt-Computer zu verwenden.

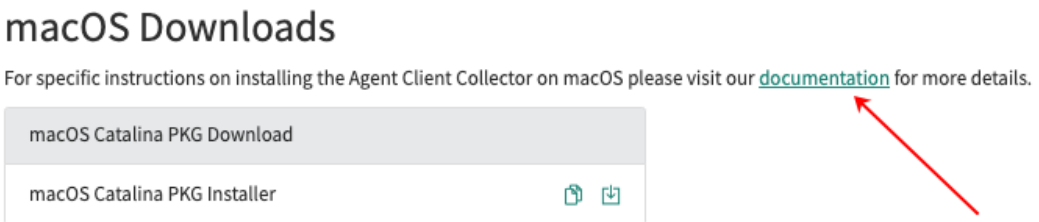
5. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Webserver API-Schlüssel** Kopieren und speichern Sie den MID-Webserver-API-Schlüssel, der bei der Installation des ACC-Agents auf dem Endpunktcomputer verwendet werden soll.

6. Installieren Sie den ACC-Agent auf dem Endpunkt-Computer.

   Hinweis: Wenn Sie den ACC-Agent bereits installiert haben, fahren Sie mit den Agent Client Collector-Protokollrichtlinien fort.

   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agenten-Downloads**an.

   b. Laden Sie den ACC-Agent für das entsprechende Betriebssystem herunter.
      Um detaillierte Anweisungen zu erhalten, klicken Sie auf den Dokumentationslink für das Betriebssystem. Beispiel:



Ergebnis

Agent Client Collector Log Analytics und der ACC-Agent sind installiert. Sie können die Anwendung nun verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Siehe Agent Client Collector-Protokollrichtlinien.

Zusätzliche ACC-Dateneingaben einrichten

Dateneingaben für das Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz mit Agent Client Collector werden automatisch als Teil des Agent Client Collector-Setups erstellt. Richten Sie zusätzliche ACC-Dateneingaben nach Bedarf manuell ein, indem Sie den Setup-Flow für Health Log Analytics-Dateneingaben verwenden.

Vorbereitungen

- Die Anwendung Agent Client Collector Log Analytics hat eine Abhängigkeit von den folgenden ServiceNow-Anwendungen, die im ServiceNow Store verfügbar sind:
  - Health Log Analytics, Version 22.0.12 - Dezember 2021 und spätere Releases.
  - Agent Client Collector Framework, Version 2.7.0 – Dezember 2021 und spätere Releases.
- Überprüfen Sie, ob ein MID-Server Ist installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .
- MID-Server muss für die Verwendung mit Agent Client Collector konfiguriert sein. Weitere Informationen finden Sie unter Agent Client Collector Monitoring auf dem MID-Server aktivieren.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Es ist wichtig, dass Sie eine ACC-Dateneingabe für jeden MID-Server konfigurieren, mit dem eine Verbindung von Agent Client Collector-Systemen hergestellt werden kann, auch wenn derzeit keine Verbindung mit einem Agent besteht. Ein Agent ist jeweils nur mit einem MID-Server verbunden, wird jedoch bei Bedarf mit einem anderen MID-Server verbunden, wenn dies zur Failover-Absicherung notwendig ist.

Wichtig: Als Teil des standardmäßigen Setups von Health Log Analytics-Dateneingaben können Sie JavaScript-Funktionen für die Zuordnung und Vorverarbeitung von nicht aufbereiteten Protokolldaten definieren. Die JavaScript-Funktion muss für alle ACC-Dateneingaben identisch sein, da Agents zu einer anderen ACC-Dateneingabe wechseln, wenn sie zum Zweck der Failover-Absicherung vom System mit einem anderen MID-Server verbunden werden. Die zuletzt veröffentlichte JavaScript-Funktion wird für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt und ersetzt die vorherige Funktion. Diese Funktion wird in unterstützt Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar über ServiceNow Store .

Prozedur

1. Richten Sie zusätzliche ACC-Dateneingaben manuell mit ein Health Log Analytics Setup-Flow für Dateneingabe.
   Weitere Informationen finden Sie unter ACC-Dateneingaben manuell konfigurieren.
2. Identifizieren und beheben Sie Probleme beim Protokoll-Streaming, um sicherzustellen, dass Ihre Dateneingaben ordnungsgemäß Daten streamen.
   Weitere Informationen finden Sie unter Stellen Sie sicher, dass die Dateneingabe Daten streamt .
3. Bestimmen Sie, wie Health Log Analytics Verarbeitet Rohprotokolldaten, die in Ihre Instanz gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig wird jede eingehende Protokollzeile automatisch dem richtigen Tag zugeordnet. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren. Weitere Informationen finden Sie unter Ordnen Sie die Rohdaten zu .

4. **Wahlweise:** Ändern Sie Rohprotokolldaten, und legen Sie Protokollnachrichten ab, bevor Sie verarbeitet werden.
   Definieren Sie eine JavaScript-Funktion, die Ihre Protokolldaten im Rohzustand ändert, bevor Health Log Analytics sie zuordnet und strukturiert. Weitere Informationen finden Sie unter Bearbeiten Sie Ihre Rohprotokolldaten vor der Verarbeitung .
5. **Wahlweise:** Verfeinern Sie die Quelltypstruktur, um dies sicherzustellen Health Log Analytics Extrahiert und klassifiziert alle Eigenschaften korrekt.
   Weitere Informationen finden Sie unter Verfeinern Sie die Quelltypstruktur in Health Log Analytics.

ACC-Dateneingaben manuell konfigurieren

Beim Setup von Agent Client Collector wird automatisch eine ACC-Dateneingabe zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz erstellt. Sie können zusätzliche ACC-Dateneingaben nach Bedarf manuell einrichten.

Vorbereitungen

- Die Anwendung Agent Client Collector Log Analytics hat eine Abhängigkeit von den folgenden ServiceNow-Anwendungen, die im ServiceNow Store verfügbar sind:
  - Health Log Analytics, Version 22.0.12 - Dezember 2021 und spätere Releases.
  - Agent Client Collector Framework, Version 2.7.0 – Dezember 2021 und spätere Releases.
- Überprüfen Sie, ob ein MID-Server Ist installiert und konfiguriert. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .
- MID-Server muss für die Verwendung mit Agent Client Collector konfiguriert sein. Weitere Informationen finden Sie unter Agent Client Collector Monitoring auf dem MID-Server aktivieren.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. MTLs werden nicht unterstützt.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Dateneingaben**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter ACC-Dateneingabe – Konfigurationsfelder.
4. **Wahlweise:** Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
5. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
6. Stellen Sie sicher, dass die Dateneingabe korrekt konfiguriert ist, indem Sie auswählen **Verbindung testen** .

   Health Log Analytics Versucht, eine Verbindung mit herzustellen MID-Server Zum Daten-Repository.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Verbindung hergestellt wurde, wird **Verbindung testen** Die Schaltfläche ist deaktiviert, und die **Veröffentlichen** Schaltfläche ist aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler in angezeigt **Fehlermeldung** Feld. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

  Beheben Sie das Problem, wählen Sie aus **Speichern** Wenn Sie die Konfiguration geändert haben, und wählen Sie dann aus **Verbindung testen** Um die Verbindung erneut zu testen.

  Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie auswählen **Änderungen Rückgängig Machen** . Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte Konfiguration ändern.

7. Wählen Sie Aus **Veröffentlichen** Um die Dateneingabe in zu veröffentlichen MID-Server.

Ergebnis

Die neue Dateneingabe ist bereit für das Streamen von Protokollen.

Hinweis: Der Datensatz einer Dateneingabe enthält die folgenden zugehörigen Listen:

- Agents – Listet alle aktiven Agents auf, die mit dem MID-Server für diese Dateneingabe verbunden sind.
- Streaming-Quellen: Listet alle Quellen für diese Dateneingabe und den MID-Server auf, der Protokolle davon empfängt.

Nächste Maßnahme

Vergewissern Sie sich, ob von der Dateneingabe Daten gestreamt werden.

ACC-Dateneingabe – Konfigurationsfelder

Beschreibung der Felder im Konfigurationsformular für ACC-Dateneingaben.

Basiskonfiguration

Feld	Beschreibung
MID	Der MID-Server, an den die Protokolle gestreamt werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Pro MID-Server kann nur eine ACC-Dateneingabe definiert werden. Sie können nur MID Servers mit AgentClientCollector-Funktionalität auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, werden nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID-Server-Eigenschaften ändern. Wenn jedoch 10 Dateneingaben, die keine ACC-Dateneingaben sind, für einen MID-Server definiert wurden, kann dennoch eine ACC-Dateneingabe für ihn definiert werden, sodass insgesamt 11 Dateneingaben für diesen MID-Server definiert sind. • Wenn Sie das Formular absenden, wird dieses Feld schreibgeschützt. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Der Port muss konfiguriert und aktiv sein. Er darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den Port öffnet, bevor Sie ihn zuweisen. **Hinweis:** Wenn Sie den Port aktualisieren, aktualisiert das System Agent Client Collector mit der neuen Port-Konfiguration. Das Protokollstreaming wird nach 1 bis 3 Minuten ohne Protokollverlust fortgesetzt. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Der Name der Dateneingabe: Agent Log Analytics. **Hinweis:** Alle ACC-Dateneingaben haben denselben Namen. Sie können eine ACC-Dateneingabe anhand des Namens des MID-Server s identifizieren, der für ihn definiert ist.
Status	Status der Dateneingabe.
Übertragung	Protokoll zum Senden der Protokolldaten. Die ACC-Dateneingabe sendet Daten mit einem ServiceNow-Agent.
Quellenanzahl	Die Gesamtzahl der Protokollquellen, die zusammen aus allen ACC-Dateneingaben stammen. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store .
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
SSL verwenden	Option für die Verwendung von SSL.	Wahr
Client inactivity timeout (sec) (Zeitüberschreitung bei Client-Inaktivität (Sek.))	Die Zeitüberschreitung in Sekunden, nach der ein inaktiver Kanal geschlossen wird	15
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Default time zone (Standardzeitzone)	Standardzeitzone von Events. Das System verwendet diesen Standard,	GMT

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration (Fortsetzung)

Feld	Beschreibung	Standardwert
	wenn im Protokoll keine Zeitzone angegeben ist.	
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	false

Agent Client Collector-Protokollrichtlinien

Von Agent Client Collector-Dateneingaben werden Protokollnachrichten mit ServiceNow Agent Client Collector in Ihre ServiceNow-Instanz gestreamt. Die Anwendung Agent Client Collector Log Analytics (ACC-L) bietet vordefinierte Protokollrichtlinien zum Sammeln von Protokolldaten aus den von ACC überwachten CIs.

Mit Agent Client Collector-Protokollrichtlinien können Sie auf folgende Weise arbeiten:

- Verwenden Sie die vordefinierten Protokollrichtlinien des Systems.

  Die Standardprotokollrichtlinien von ACC-L bestehen aus den überwachten CIs und der Prüfung, die für diese CIs ausgeführt wird. Eine vollständige Liste der vordefinierten Protokollrichtlinien und überwachten CI-Typen finden Sie unter Agent Client Collector Log Analytics Standardrichtlinien und -Prüfungen.

- Bearbeiten Sie eine vordefinierte Protokollrichtlinie.

  Sie können beispielsweise eine Standardrichtlinie ändern, wenn Ihre Organisation immer einen bestimmten nicht standardmäßigen Protokollpfad verwendet. Weitere Informationen finden Sie unter Protokollrichtlinie bearbeiten.

- Passen Sie eine veröffentlichte Protokollrichtlinie an, indem Sie daraus eine untergeordnete Richtlinie erstellen.

  Sie können eine vorhandene Protokollrichtlinie (die übergeordnete Richtlinie) als Vorlage verwenden, um eine neue Protokollrichtlinie (die untergeordnete Richtlinie) zu erstellen. Anschließend passen Sie die Parameter an, die die untergeordnete Richtlinie von der übergeordneten Richtlinie zum Zweck der Konzentration auf eine Untergruppe ihrer CIs oder Services übernimmt. Erstellen Sie beispielsweise eine untergeordnete Richtlinie, wenn Ihre Organisation eine Teilmenge der IIS-Serverprotokolle an einem anderen Ort speichert. Weitere Informationen finden Sie unter Untergeordnete Protokollrichtlinie erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die untergeordnete Richtlinie ist von Natur aus spezifischer als die übergeordnete Richtlinie. Wenn von Agent Client Collector eine Übereinstimmung mit einer in der untergeordneten Richtlinie definierten Bedingung festgestellt wird, erfolgt kein Abgleich mit der übergeordneten Richtlinie.

- Definieren Sie eine neue Protokollrichtlinie, wenn für das CI, das von Agent Client Collector überwacht werden soll, keine Richtlinie vorhanden ist.

  Weitere Informationen finden Sie unter Agent Client Collector-Protokollrichtlinie erstellen. Eine allgemeine Erklärung der Agent Client Collector-Richtlinien finden Sie unter Prüfungen und Richtlinien.

Agent Client Collector Log Analytics Standardrichtlinien und -Prüfungen

Agent Client Collector Log Analytics Stellt verschiedene Standardrichtlinien und -Prüfungen bereit.

Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

ACC-L-Standardrichtlinien

Name	BS	Beschreibung	Prüfung
Protokolle Apache unter Linux	Linux	Sammelt Protokolle von Apache-Servern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Apache unter Windows	Windows	Sammelt Protokolle von Apache-Servern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle IIS	Windows	Sammelt Protokolle von Microsoft IIS-Webservern und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle JBoss/WildFly-Anwendungsserver unter Linux	Linux	Sammelt Protokolle von JBoss/WildFly-Anwendungsservern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle JBoss/WildFly-	Windows	Sammelt Protokolle von JBoss/WildFly-	Protokollversender

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Anwendungsserver unter Windows		Anwendungsservern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	
Protokolle Linux-BS	Linux	Sammelt Protokolle vom Linux-Betriebssystem und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle MSSQL unter Linux	Linux	Sammelt Protokolle von MSSQL-DBs, die unter Linux ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	log_shipper
Protokolle MSSQL unter Windows	Windows	Sammelt Protokolle von MSSQL-Datenbanken, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle MySQL-DB unter Linux	Linux	Sammelt Protokolle von MySQL-DBs, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle MySQL-DB unter Windows	Windows	Sammelt Protokolle von MySQL-DBs, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Nginx aktiviert Linux Protokolle	Linux	Sammelt Protokolle von Nginx-Servern, die auf einem ausgeführt werden Linux Betriebssystem und sendet sie an MID-Server Zur weiteren Analyse.	Protokollversender
Protokolle Tomcat unter Linux	Linux	Sammelt Protokolle von Tomcat-Servern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Protokolle Tomcat unter Windows	Windows	Sammelt Protokolle von Tomcat-Servern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Oracle WebLogic	Windows und Linux	Sammelt Protokolle von Oracle WebLogic-Server und sendet sie an MID-Server Zur weiteren Analyse.	Protokollversender

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
		Hinweis: • Der Protokollpfad, den WebLogic verwendet, hat zwei Umgebungsvariablen, wie in der WebLogic-Dokumentation beschrieben. Weitere Informationen finden Sie unter Umgebungsvariablen. • Auf beiden Windows Und Linux, Agent Client Collector Log Analytics Fügt dem Protokollpfad eine Standardumgebungsvariable aus der WebLogic-Dokumentation hinzu. Sie können diese Standardumgebungsvariable entweder verwenden, um das vollständige Verzeichnis abzurufen, oder sie manuell ändern, wenn Sie ein bekanntes Direktverzeichnis verwenden möchten. Informationen zum Anpassen der Umgebungsvariablen finden Sie unter Protokollpfadkonfigurationen bearbeiten.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Protokolle WebSphere-Anwendungsserver unter Linux	Linux	Sammelt Protokolle von WebSphere-Anwendungsservern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Windows-Betriebssystemereignisse	Windows	Sammelt Windows-Ereignisprotokolle von Windows-Servern und sendet sie zur weiteren Analyse an den MID-Server	log shipper for win events

Umgebungsvariablen

Der Protokollpfad, der zum Sammeln von Protokollen von bestimmten Servern verwendet wird, kann Umgebungsvariablen enthalten. Es ist wichtig, dies auf zu beachten Linux-Systeme kann der ACC-Agent nur auf Umgebungsvariablen zugreifen, die sich im befinden /Etc/Environment Datei. Fügen Sie die Umgebungsvariablen hinzu, auf die der Service Desk-Mitarbeiter zugreifen muss /Etc/Environment Datei im Format *<NAME>='<VALUE>'*. Ein Windows Systeme können Sie Umgebungsvariablen auf die übliche Weise erstellen.

Standardmäßige ACC-L-Prüfungen

Agent Client Collector Log Analytics(ACC-L) stellt den folgenden Standard bereit **Typ=Protokoll** Prüfungen.

- Von der *log shipper*-Prüfung wird ein Hintergrundprozess gestartet, über den entsprechend dem konfigurierten Protokollpfad der Prüfung Protokolle an eine Agent-Dateneingabe gesendet werden. Wenn Zugriffsberechtigungen fehlen oder der Protokollpfad falsch konfiguriert ist, wird vom System eine Warnung an die Instanz gesendet. Vergewissern Sie sich für eine ordnungsgemäße Protokollkonfiguration, dass der *servicenow*-Benutzer über Berechtigungen für den Zugriff auf den konfigurierten Protokollpfad auf dem Computer verfügt, auf dem der Agent gehostet wird, und dass der Protokollpfad richtig konfiguriert ist.
- Die Prüfung *log shipper for win events* ähnelt der Prüfung *log shipper*, aber es werden Ereignisprotokolle von Windows-Servern an die Agent-Dateneingabe gesendet.

> **Hinweis:** Zum Erfassen von Windows-Sicherheitsereignisprotokollen müssen *servicenow*-Benutzer auf einem Computer, auf dem der Agent gehostet wird, über Administratorrechte verfügen.

Agent Client Collector-Protokollrichtlinie erstellen

Erstellen Sie eine neue ACC-Protokollrichtlinie, wenn für das CI, das von Agent Client Collector überwacht werden soll, keine Standardrichtlinie vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Die im ServiceNow Store verfügbare Anwendung Agent Client Collector Log Analytics (ACC-L) muss installiert sein. Weitere Informationen finden Sie unter Installation von Agent Client Collector.
- Agent Client Collector wird mit dem standardmäßigen *servicenow*-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector *servicenow*-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu /var/log/ unter Linux und des Pfads zu C:\Windows\System32 unter Windows. Informationen zum Konfigurieren von Berechtigungen für den *servicenow*-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollrichtlinien**an.
   Auf der Seite **Richtlinien** werden alle Log Analytics-Richtlinien angezeigt. Eine Liste der Richtlinien, die mit dem Basissystem bereitgestellt werden, finden Sie unter Agent Client Collector Log Analytics Standardrichtlinien und -Prüfungen.
2. Klicken Sie auf **Neu**.

   Hinweis: Allgemeine Informationen zum Erstellen einer ACC-Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

3. Füllen Sie die Felder des Formulars aus.

Formular „Policy Definition“ (Richtliniendefinition)

Feld	Beschreibung
Name	Beschreibender Name für die Richtlinie
Beschreibung	Beschreibung der Richtlinie
Veröffentlichungsstatus	Hartcodiert als **Draft** (Entwurf), was bedeutet, dass die Richtlinie noch nicht veröffentlicht wurde. Dieses Feld können Sie nicht bearbeiten.
Hierarchie	Hartcodiert als **Keine**. Wenn der Richtlinie eine untergeordnete Richtlinie hinzugefügt wird, ändert sich der Wert in **Übergeordnet**. Untergeordnete Richtlinien haben den Wert **Untergeordnetes Element**.

4. Verknüpfen Sie auf der Registerkarte **Überprüfungen** die Protokollrichtlinie mit der entsprechenden Protokollversender-Überprüfung.
   - Wählen Sie für Linux und Windows (mit Ausnahme von Windows-Ereignisprotokollen) die Prüfungsdefinition *log shipper* aus.
   - Wählen Sie für Windows-Ereignisprotokolle die Prüfungsdefinition *log shipper for win events* aus.
5. Geben Sie auf der Registerkarte **Überwachte CIs** die CIs an, für die die Richtlinie gilt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie den zu überwachenden CI-Typ aus.

- **Überwachter CI-Typ nach Filter**: Wählen Sie den überwachten CI-Typ aus. Sie können die zu überwachenden CIs mithilfe von Filterbedingungen eingrenzen.
- **Überwachter CI-Typ nach Skript**: Geben Sie die überwachten CIs mithilfe eines Skripts an.
- **Überwachter CI-Typ nach CMDB-Gruppe**: Geben Sie die überwachten CIs mithilfe von CMDB-Gruppenabfragen an.

Weitere Informationen zur Auswahl überwachter CI-Typen finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

b. **Wahlweise:** Wenn Sie ausschließlich CIs überwachen möchten, die einem Anwendungsservice zugeordnet sind, wählen Sie **Überwachte CIs nach Anwendungsservice filtern** aus.
Sie können die zu überwachenden Anwendungsservices mithilfe von Filterbedingungen angeben. Von Agent Client Collector werden dann ausschließlich die Protokolle von CIs abgerufen, die diesen Anwendungsservices zugeordnet sind.

6. Speichern Sie die Protokollrichtlinie.
In der zugehörigen Liste „Instanzen überprüfen“ wird ein Datensatz für die Überprüfungsinstanz angelegt.

7. Öffnen Sie den entsprechenden Datensatz für die Überprüfungsinstanz, und wählen Sie dann **In Sandbox bearbeiten** aus.

8. Wählen Sie die zugehörige Liste „Log path configuration“ (Protokollpfadkonfigurationen) aus.

9. Fügen Sie einen Protokollpfad für die Überprüfungsinstanz hinzu.

Hinweis: Für eine Prüfung muss mindestens ein Protokollpfad konfiguriert sein, damit Protokoll-Streaming aktiviert werden kann. Weitere Informationen zu Prüfungen finden Sie unter Prüfungen und Richtlinien.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder des Formulars aus.

Formular für neue Pfadkonfiguration

Feld	Beschreibung
Pfad	Vollständiger Pfad, aus dem die Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. Dies ist ein Pflichtfeld.
Komponente	Gerätetypen oder Stapelebenen, die Kontext für die Protokolle bieten, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat.
Quelltyp	Definiert, wie von Health Log Analytics bestimmte Protokolltypen verarbeitet und die Protokolldaten analysiert werden sollen. Beispiel: Tomcat Catalina.

c. **Wahlweise:** Konfigurieren Sie für den Versand von mehrzeiligen Protokollen mit Filebeat die folgenden Eigenschaften.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Mit diesen Parametern wird gesteuert, wie von Agent Client Collector Log Analytics (ACC-L) Nachrichten verarbeitet werden, die sich über mehrere Textzeilen erstrecken.

Weitere Informationen finden Sie unter Verwalten Sie mehrzeilige Nachrichten In der Elastic-Dokumentation.

Feld	Beschreibung
multiline.pattern (regex)	Der entsprechende reguläre Ausdruck **Hinweis:** Sie müssen diese Eigenschaft definieren, bevor Sie die Eigenschaften multiline.match und multiline.negate konfigurieren können.
multiline.match	Wie ACC-L übereinstimmende Zeilen zu einer einzigen Protokollzeile kombiniert. (Optional) Die verfügbaren Optionen sind Keine, Vorher und Nachher. Standard ist Keine.
multiline.negate	Option, um zu bestimmen, ob das in den Protokollzeilen identifizierte Muster negiert wird. (Optional) Die verfügbaren Optionen sind Keine, Wahr und Falsch. Standard ist Keine.

d. Wahlweise: Definieren Sie die folgenden Eigenschaften, mit denen die Filebeat-YML-Konfiguration gesteuert wird.

Feld	Beschreibung
Felder	Feld, mit dem Sie Informationen in die Ausgabe einbeziehen und aus der Ausgabe ausschließen können. Sie können beispielsweise ein Feld zum Filtern der Protokolldaten hinzufügen. (Optional) Mit dem Plus-Symbol neben dem Wertfeld fügen Sie weitere Feldzeilen hinzu: ⊕. Mit dem Minus-Symbol entfernen Sie eine Feldzeile: ⊖. Weitere Informationen finden Sie in der Beschreibung der Felder der Protokolleingabe in der Elastic-Dokumentation.
Konfigurationsoptionen	Feld, mit dem Sie den Protokollzeilen Konfigurationsoptionen hinzufügen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können beispielsweise die zu verwendende Codierung hinzufügen. **Hinweis:** Legen Sie nur Konfigurationsoptionen fest, die von Filebeat unterstützt werden. Weitere Informationen finden Sie in der Elastic-Dokumentation bei der Beschreibung der Konfigurationsoptionen der Protokolleingabe.

e. Wählen Sie **OK** aus.
Der Protokollpfad wird erstellt.

10. Wählen Sie **Zurück zur Richtlinie** aus.
11. Wählen Sie im Richtlinienformular die Option **Veröffentlichen** aus.
Der Veröffentlichungsstatus der Richtlinie ändert sich in **Veröffentlicht**.
12. **Wahlweise:** Aktivieren Sie die Richtlinie, indem Sie **Aktivieren** auswählen.

Nächste Maßnahme
Vergewissern Sie sich, ob von der Dateneingabe Daten gestreamt werden.

Untergeordnete Protokollrichtlinie erstellen

Verfeinern Sie eine vorhandene Protokollrichtlinie, um sich auf eine Teilmenge von CIs oder Services zu konzentrieren, indem Sie eine untergeordnete Richtlinie erstellen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Eine veröffentlichte Protokollrichtlinie (die übergeordnete Richtlinie) kann als Vorlage zum Erstellen einer neuen Protokollrichtlinie (der untergeordneten Richtlinie) verwendet werden. Sie können die Parameter anpassen, die die untergeordnete Richtlinie von der übergeordneten Richtlinie zum Zweck der Konzentration auf eine Untergruppe ihrer CIs oder Services übernimmt.

Die untergeordnete Richtlinie erbt Parameter von der übergeordneten Richtlinie, die nach der Erstellung der untergeordneten Richtlinie geändert werden, es sei denn, Sie deaktivieren diese Option in der untergeordneten Richtlinie. Sie können diese geänderten Parameter im Entwurfsmodus in jeder untergeordneten Richtlinie überprüfen, bevor Sie sie akzeptieren.

Hinweis: Die untergeordnete Richtlinie ist von Natur aus spezifischer als die übergeordnete Richtlinie. Wenn von Agent Client Collector eine Übereinstimmung mit einer in der untergeordneten Richtlinie definierten Bedingung festgestellt wird, erfolgt kein Abgleich mit der übergeordneten Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollrichtlinien**an.
2. Wählen Sie auf der Seite **Policies** (Richtlinien) eine veröffentlichte Richtlinie mit dem Hierarchiewert **None** (Keine) oder **Parent** (Übergeordnet) aus.
3. Wählen Sie **Untergeordnetes Element erstellen** aus.
   Es wird eine neue Richtlinie geöffnet, die dieselben Parameter aufweist, wie die veröffentlichte Richtlinie. Der Name der neuen Richtlinie lautet *<Policy name><date and time created>*.

   Beispiel: MySQL DB on Linux Logs 2022-02-13 04:44:12.

   Die folgenden Felder sind schreibgeschützt:

   Felder für untergeordnete Richtlinie

Feld	Wert
Veröffentlichungsstatus	Entwurf
Hierarchie	Untergeordnetes Element
Übergeordnet	<Name der übergeordneten Richtlinie>

   Der Wert im Feld **Reihenfolge** gibt die Priorität an, mit der der Agent im Verhältnis zu den gleichgeordneten Richtlinien an die untergeordnete Richtlinie angehängt wird. Eine niedrigere Zahl zeigt eine im Verhältnis höhere Priorität für die betreffende untergeordnete Richtlinie an. Standardmäßig nimmt jede neue untergeordnete Richtlinie einen höheren Wert (und daher eine niedrigere Priorität) an als die vorherige. Den Reihenfolgenwert können Sie bei Bedarf ändern.
4. Passen Sie die Parameter der untergeordneten Richtlinie an.
   Eine Beschreibung der Parameter finden Sie unter Agent Client Collector-Protokollrichtlinie erstellen.
5. Wählen Sie **Speichern** aus, um die untergeordnete Richtlinie zu erstellen.
6. **Wahlweise:** Wählen Sie **Vererbungsoption deaktivieren** aus, um die Option zu deaktivieren, dass geänderte Parameter automatisch von der übergeordneten Richtlinie geerbt werden.
7. Wählen Sie **Veröffentlichen** aus, um die untergeordnete Richtlinie zu veröffentlichen.

Ergebnis
Die untergeordnete Richtlinie wird veröffentlicht und auf der Registerkarte **Untergeordnete Richtlinien** der übergeordneten Richtlinie angezeigt.

Protokollrichtlinie bearbeiten

Sie können veröffentlichte Agent Client Collector-Protokollrichtlinien bearbeiten. Ändern Sie beispielsweise eine Standardprotokollrichtlinie, wenn Ihre Organisation immer einen bestimmten nicht standardmäßigen Protokollpfad verwendet.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollrichtlinien**an.
2. Wählen Sie eine Richtlinie aus, für die der **Veröffentlichungsstatus** auf **Veröffentlicht** festgelegt ist.
3. Wählen Sie **In Sandbox bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daraufhin wird die Richtlinie in der **Draft view** (Entwurfsansicht) angezeigt, und Sie können ihre Felder und Prüfungsinstanzen bearbeiten.

Hinweis: Auch in der **Draft view** (Entwurfsansicht) bleibt der Veröffentlichungsstatus der Richtlinie **Veröffentlicht**.

4. Bearbeiten Sie auf der Registerkarte **Überwachte CIs** die CIs, für die die Richtlinie gilt, je nach Bedarf.

   a. Wählen Sie den zu überwachenden CI-Typ aus.

   - **Überwachter CI-Typ nach Filter**: Wählen Sie den überwachten CI-Typ aus. Sie können die zu überwachenden CIs mithilfe von Filterbedingungen eingrenzen.
   - **Überwachter CI-Typ nach Skript**: Geben Sie die überwachten CIs mithilfe eines Skripts an.
   - **Überwachter CI-Typ nach CMDB-Gruppe**: Geben Sie die überwachten CIs mithilfe von CMDB-Gruppenabfragen an.

   Weitere Informationen zur Auswahl überwachter CI-Typen finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

   b. **Wahlweise:** Wenn Sie ausschließlich CIs überwachen möchten, die einem Anwendungsservice zugeordnet sind, wählen Sie **Überwachte CIs nach Anwendungsservice filtern** aus.
   Sie können die zu überwachenden Anwendungsservices mithilfe von Filterbedingungen angeben. Von Agent Client Collector werden dann ausschließlich die Protokolle von CIs abgerufen, die diesen Anwendungsservices zugeordnet sind.

5. **Wahlweise:** Wählen Sie in der Tabelle **Instanzen überprüfen** den Datensatz der Prüfungsinstanz des Protokollversenders aus, und bearbeiten Sie ihn.
   Weitere Informationen finden Sie unter Protokollpfadkonfigurationen bearbeiten.
6. Wählen Sie **Speichern** aus, um die Änderungen zu speichern, die Sie in den Richtlinienfeldern in der Sandbox eingegeben haben.
   Die Richtlinie bleibt in der **Draft view** (Entwurfsansicht), der **Publish status** (Veröffentlichungsstatus) lautet **Published*** (Veröffentlicht*). Das Sternchen (*) zeigt an, dass die aktuell veröffentlichte Version nicht die aktuellste ist, da sie gespeicherte Änderungen enthält, die noch nicht veröffentlicht wurden.
7. Wählen Sie **Erneut veröffentlichen** aus, um die Updates zu veröffentlichen.
   Die Richtlinie wird in den Status **Veröffentlicht** zurückversetzt und als veröffentlichte Richtlinie geöffnet.

   Hinweis: Diese Option wird nur nach der Bearbeitung von Richtlinienfeldern einer Richtlinie angezeigt, deren **Veröffentlichungsstatus** auf **Veröffentlicht*** festgelegt ist.

8. Bestimmen Sie den aktiven Status der Richtlinie, indem Sie entweder **Aktivieren** oder **Deaktivieren** auswählen.
9. **Wahlweise:** Wählen Sie **Löschen** aus, um sowohl die veröffentlichten Richtlinien als auch die Entwurfsrichtlinien zu löschen.

Protokollpfadkonfigurationen bearbeiten

Ändern Sie eine Protokollpfadkonfiguration in der Prüfungsinstanz des Protokollversenders.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollrichtlinien**an.
2. Wählen Sie einen Richtliniendatensatz aus.
3. Wählen Sie in der zugehörigen Liste „Instanzen überprüfen“ den Datensatz der Prüfungsinstanz des Protokollversenders aus.
4. Wählen Sie **In Sandbox bearbeiten** aus, um die Bearbeitung des Datensatzes zu aktivieren.
5. Bearbeiten Sie in der zugehörigen Liste Protokollpfadkonfiguration eine Protokollpfadkonfiguration.

   a. Wählen Sie die Protokollpfadkonfiguration aus, die Sie bearbeiten möchten.

   b. Bearbeiten Sie die Konfiguration.

   - Sie können anwenderdefinierte Felder hinzufügen, sodass Sie zusätzliche Informationen in die Ausgabe aufnehmen können.
   - Sie können zusätzliche Konfigurationsoptionen hinzufügen, z. B. `Codierung` , `Include_lines` , Und `EXCLUDE_Lines` , Um Ihre Protokolldaten zu filtern. Informationen zum Erkennen der Dateicodierung finden Sie unter So erkennen Sie Dateicodierung unter Windows, Linux und Mac [KB1702770] artikel in Now Support Knowledge Base.

     Diese Konfigurationsoptionen wirken sich auf alle Dateien aus, die die Dateneingabe an Ihre Instanz streamt.

     Hinweis: Legen Sie nur Konfigurationsoptionen fest, die von Filebeat unterstützt werden. Weitere Informationen finden Sie in der Elastic-Dokumentation bei der Beschreibung der Konfigurationsoptionen der Protokolleingabe.

   c. Wählen Sie Aus **Aktualisieren** Um Ihre Änderungen zu speichern.

6. **Wahlweise:** Fügen Sie eine Umgebungsvariable hinzu, oder bearbeiten Sie eine vorhandene in **Pfad** Feld. Verwenden Sie das entsprechende Format für den Namen:
   - Ein Linux, Großbuchstaben Sie den Namen, und stellen Sie ihm ein Dollarzeichen voran: $. Beispiel: `$HOME` . Beim Namen wird zwischen Groß- und Kleinschreibung unterschieden.
   - Ein Windows, Umgeben Sie den Namen mit Prozentzeichen: %. Beispiel: `%HOMEPATH%` . Beim Namen wird die Groß-/Kleinschreibung nicht beachtet.

   Wichtig: Der servicenow-Anwender und der ACC-Agent müssen Zugriff auf die Umgebungsvariable haben. Ein Linux Systeme, nur Umgebungsvariablen, die sich in befinden `/Etc/Environment` Datei ist zugänglich. Fügen Sie dieser Datei die Umgebungsvariable im Format hinzu *`<NAME>='<VALUE>'`*.

7. **Wahlweise:** Löschen Sie einen Protokollpfad.

   a. Aktivieren Sie das Kontrollkästchen neben der Protokollpfadkonfiguration, die Sie löschen möchten.

   Hinweis: Sie können mehrere Protokollpfadkonfigurationen auswählen, aber für eine Prüfung muss mindestens ein Protokollpfad konfiguriert sein, damit Protokoll-Streaming aktiviert werden kann. Weitere Informationen zu Prüfungen finden Sie unter Prüfungen und Richtlinien.

   b. Wählen Sie **Löschen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Zurück zur Richtlinie** aus, um zum Datensatz der Protokollrichtlinie zurückzukehren.
9. Wählen Sie **Erneut veröffentlichen** aus, und bestätigen Sie dann den Vorgang, um die Richtlinie mit den aktualisierten Protokollpfadkonfigurationen erneut zu veröffentlichen.
   Die Änderungen werden in wenigen Minuten wirksam.

Probleme beim Protokoll-Streaming identifizieren und beheben

Vergewissern Sie sich, ob von den ACC-Dateneingaben Daten ordnungsgemäß gestreamt werden, indem Sie Probleme beim Protokoll-Streaming identifizieren und beheben.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Datensatz der ACC-Dateneingabe werden in der zugehörigen Liste „Streamingquellen“ die Streaming-Daten der Quellen der betreffenden Dateneingabe angezeigt. Anhand dieser Daten können Sie Streaming-Probleme und deren mögliche Ursache identifizieren.

Wenn beispielsweise der letzte Zeitpunkt des Ereignisses für den Endpunktserver einer Dateneingabe gestern war, ist dieser Server möglicherweise ausgefallen oder falsch konfiguriert. Ein Streaming-Problem kann auch dadurch verursacht werden, dass die Dateneingabe-Konfigurationsdatei nicht auf dem Endpunkt installiert ist.

Hinweis: Sie können die Streaming-Daten aller Dateneingaben und die MID Servers, die Protokolle von ihnen empfangen, auf der Seite „Streamingquellen“ anzeigen. Weitere Informationen finden Sie in der Dokumentation der Anwendung ServiceNow Health Log Analytics unter Identifizieren und beheben Sie ein Protokoll-Streaming-Problem in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **ACC-Dateneingaben** Und wählen Sie einen Dateneingabedatensatz aus.
2. Wählen Sie im Dateneingabeformular die zugehörige Liste „Streamingquellen“ aus.
3. Überprüfen Sie die Streaming-Daten der Quellen dieser Dateneingabe.
   Eine Beschreibung der Filter finden Sie unter Streaming-Quellen für ACC-Dateneingaben.
4. Beheben Sie etwaig vorhandene Probleme beim Daten-Streaming.
   a. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollwarnungen**an.
   b. Öffnen Sie Warnungen, und beheben Sie die angegebenen Probleme.

Nächste Maßnahme

Fahren Sie mit dem nächsten Schritt im Setup-Flow für Health Log Analytics-Dateneingaben fort. Weitere Informationen finden Sie unter Zusätzliche ACC-Dateneingaben einrichten.

Streaming-Quellen für ACC-Dateneingaben

Im Datensatz der ACC-Dateneingabe werden in der zugehörigen Liste „Streamingquellen“ die Streaming-Daten der Quellen der betreffenden Dateneingabe angezeigt.

Zugehörige Liste „Streamingquellen“

Filter	Beschreibung
Status	Status der Quelle. Ein rotes Aufzählungszeichen zeigt an, dass diese Quelle in der letzten Stunde keine Daten gestreamt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste „Streamingquellen“ (Fortsetzung)

Filter	Beschreibung
Last event time (Zeit des letzten Events)	Die letzte aufgezeichnete Zeit, zu der auf dem MID-Server ein Event im letzten Ein-Minuten-Intervall eingetroffen ist. Health Log Analytics aktualisiert kontinuierlich die Zeit des letzten Events. Wenn die Zeit des letzten Events nicht aktuell ist, werden keine Daten gestreamt.
Raw log lines/sec (Protokollzeilen im Rohzutand/Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Protokollzeilen im Rohzutand vor der Vorverarbeitung dar.
Preprocessed log lines/sec (Vorverarbeitete Protokollzeilen/Sek.)	Die durchschnittliche Anzahl der vorbearbeiteten Protokollzeilen, die im letzten Ein-Minuten-Intervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass Protokolle während der Vorverarbeitung gelöscht wurden.

Protokollversenderwarnungen anzeigen

Zeigen Sie alle Protokollversender-Überprüfungswarnungen für Agents von Agent Client Collector Log Analytics (ACC-L) an.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

In der ACC-Warnungsliste können Sie auf einen Blick sehen, ob Probleme den Protokollversender daran hindern, Daten zu erfassen. In der Liste werden alle Warnungen im Zusammenhang mit dem Protokollversender an einem Ort angezeigt und Informationen zur Lösung der betreffenden Probleme bereitgestellt.

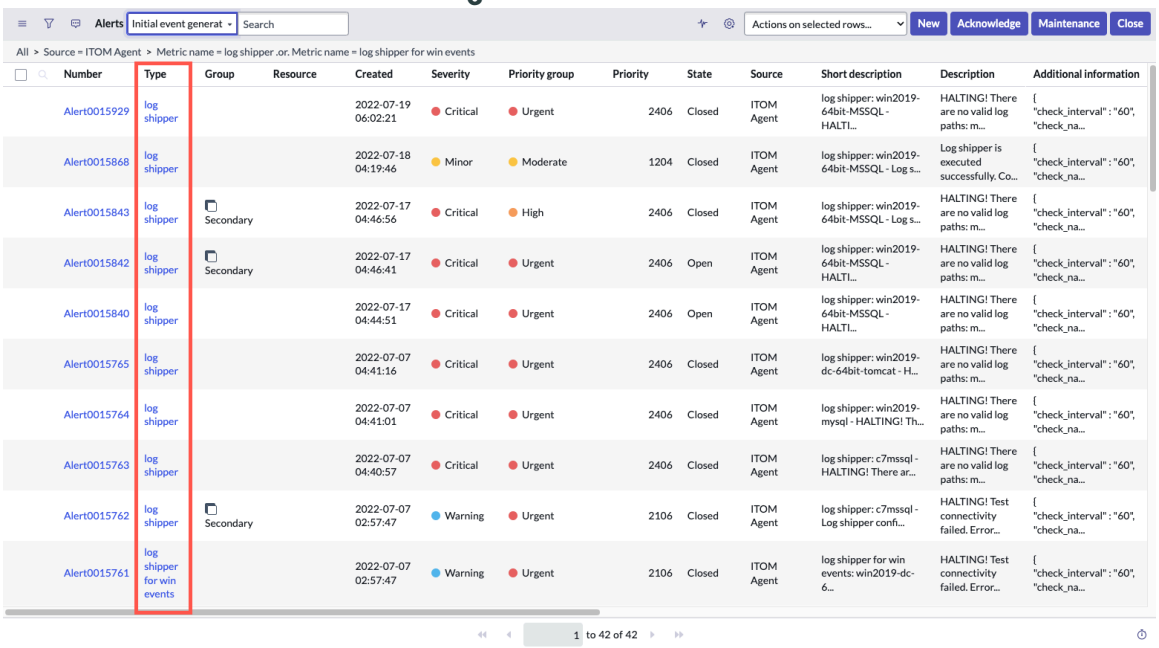
Die ACC-Warnungsliste enthält ausschließlich Warnungen über den Erfolg oder Misserfolg der Ausführung des Protokollversenders für ein CI für einen bestimmten Agent. Diese Warnungen sind eine Teilmenge der Warnungen, die in der Ereignismanagement-Warnungsliste angezeigt werden, die Warnungen aller Typen enthält. Weitere Informationen zur Ereignismanagement-Warnungsliste finden Sie unter Warnungsinformationen anzeigen.

Protokollversenderwarnungen werden aus Protokollversenderereignissen mit dem Schweregrad „Schwerwiegend“ oder „Kritisch“ generiert. Diese Warnungen beziehen sich normalerweise auf Protokollpfadprobleme oder fehlende Berechtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn ein Ereignis mit Status **OK** für den Protokollversender für ein CI empfangen wird, für das eine offene Protokollversenderwarnung vorhanden ist, wird die offene Protokollversenderwarnung für dieses CI geschlossen.

Liste der Protokollversenderwarnungen



Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollwarnungen**an.
2. Überprüfen Sie die Informationen in der Warnungsliste.
   Details und eine Beschreibung der Spalten finden Sie unter Eingehende Warnungen überwachen.

Zugehörige Informationen

Protokollversenderereignisse anzeigen

Protokollversenderereignisse anzeigen

Zeigen Sie alle Protokollversenderereignisse mit allen Schweregraden für Agents von Agent Client Collector Log Analytics (ACC-L) an.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

In der ACC-Ereignisliste werden alle Ereignisse im Zusammenhang mit dem Protokollversender an einem zentralen Ort angezeigt. Die Liste enthält ausschließlich Ereignisse über den Erfolg oder Misserfolg der Ausführung des Protokollversenders für ein CI für einen bestimmten Agent. Diese Ereignisse sind eine Teilmenge der Ereignisse, die in der Ereignismanagement-Ereignisliste angezeigt werden, die Ereignisse aller Arten enthält.

Prozedur

1. Navigieren zu **Alle** > **ACC-Protokoll-Analytics** > **ACC-Protokollereignisse**an.
2. Überprüfen Sie die Informationen in der Ereignisliste.
   Details und eine Beschreibung der Spalten finden Sie unter Events anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Protokollversenderwarnungen anzeigen

CI-Zuordnung zu einer dynamischen CI-Gruppe in Agent Client Collector Log Analytics

Wenn die Anwendung Agent Client Collector Log Analytics (ACC-L) ein CI erkennt, das keinem Anwendungsservice zugeordnet ist, erstellt die Anwendung eine dynamische CI-Gruppe und ordnet ihr das CI zu.

Eine dynamische CI-Gruppe ist eine Gruppe von CIs, die nach Attributen organisiert sind, z. B. dem CI-Typ. Standardmäßig werden mit Protokollrichtlinienprüfungen von Agent Client Collector nur CIs überwacht, die einem Anwendungsservice zugeordnet sind. Die Anwendung Agent Client Collector Log Analytics überprüft die CIs, die von Agent Client Collector erkannt werden. Wenn sie ein CI erkennt, das keinem Anwendungsservice zugeordnet ist, erstellt die Anwendung eine dynamische CI-Gruppe und ordnet ihr das CI zu.

Wenn das CI später einem tatsächlichen Anwendungsservice zugeordnet wird, wird seine Zuordnung zur dynamischen CI-Gruppe automatisch gelöscht. Die Baseline für das CI geht in diesem Prozess verloren. Während das System die neue Baseline einrichtet, gibt es keine Warnungen für den Anwendungsservice aus, dem das CI jetzt zugeordnet ist.

Sie können die Zuordnung nicht zugeordneter CIs zu einer dynamischen CI-Gruppe deaktivieren, indem Sie die Standardeinstellung der entsprechenden Systemeigenschaft *sn_accl.dynamic_service.creation.enabled* zu „false“ ändern. Die Anwendung Agent Client Collector Log Analytics verknüpft dann nicht zugeordnete CIs nicht mit dynamischen CI-Gruppen. In diesem Fall werden keine Protokolle für CIs gestreamt, die keinem Anwendungsservice zugeordnet sind.

Agent Client Collector Security Incident Response

Mit Agent Client Collector Security Incident Response (ACC-SIR) können Sie die Datenerfassungs- und Antwortaktionen für die Erweiterung von Security Incidents mit Agent Client Collector automatisieren. Diese Funktionalität wird durch Security Operations Security Incident Response (SIR) gemessen.

Hinweis: Agent Client Collector Security Incident Response Wird nicht mehr unterstützt. Weitere Informationen zu Ersatzoptionen finden Sie unter Leitfaden zur Einstellung für Agent Client Collector Security Incident Response [KB2249776] artikel In Now Support Knowledge Base.

Wählen Sie aus einer Liste von Aktionen (Fähigkeiten), die mit dem Basissystem bereitgestellt werden, damit sie für Security Incidents ausgeführt werden können. Von der Agent Client Collector Security Incident Response-Funktionalität werden die Prüfungsdefinitionen util.command.agent und util.osquery.agent (ausgeführt von der Agent Client Collector-Spoke) dazu verwendet, Befehle und Betriebssystemabfragen für Security Incidents auszuführen. Fähigkeiten sind Teil vorhandener System-Subflows in der Agent Client Collector Security Incident Response-Integrations-App. Sie können auch benutzerdefinierte Befehle und OSquery-SQL-Abfragen hinzufügen, die für die Security Incidents ausgeführt werden.

Für Details zu den mit installierten Plugins Security Incident Response, Siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Agent Client Collector Security Incident Response-Fähigkeiten

Agent Client Collector Security Incident Response Fähigkeiten, die im Basissystem enthalten sind, werden auf der Seite „ACC-Fähigkeiten“ (**Agent Client Collector-SIR-Integration** > **ACC-**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration – Fähigkeiten) an. Diese Fähigkeiten werden für Security Incidents ausgeführt, um Informationen über den Incident zu sammeln.

Wählen Sie im Abschnitt „Zugehörige Links“ des Security Incident eine Fähigkeit aus der Option **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus. Fähigkeiten sind Teil vorhandener System-Flows, auf die auf der Seite der ACC-Fähigkeiten verwiesen wird.

Agent Client Collector Security Incident Response-Fähigkeiten

Fähigkeitsname	Beschreibung	Flow
Angemeldete Anwender abrufen	Sammelt Daten zu angemeldeten Benutzern und bezieht sie auf den Security Incident	ACC SIR – Angemeldete Anwender abrufen
Netzwerkstatistiken abrufen	Sammelt Netzwerkstatistiken für das CI, das dem Security Incident zugeordnet ist	ACC SIR – Netzwerkstatistiken abrufen
Prozesse abrufen	Sammelt Prozessdaten und bezieht sie auf den Security Incident	ACC SIR – Prozesse abrufen
Get Services (Services abrufen)	Sammelt Servicedaten und bezieht sie auf den Security Incident	ACC SIR – Get Services (Services abrufen)
Systemdetails abrufen	Sammelt Systemdetails für das CI, das dem Security Incident zugeordnet ist	ACC SIR – Systemdetails
Befehl auf Agent ausführen	Führt einen benutzerdefinierten Befehl für Agent Client Collector aus und sendet Ergebnisse an den Security Incident	ACC SIR – Befehl aus Security Incident ausführen
OSQuery auf Agent ausführen	Führt eine benutzerdefinierte OSQuery für Agent Client Collector aus und sendet Ergebnisse an den Security Incident	ACC SIR – OSQuery aus Security Incident ausführen

Aktion für einen Security Incident ausführen

Führen Sie eine Agent Client Collector Security Incident Response-Aktion aus, um weitere Informationen zu einem Security Incident zu sammeln. Aktionen werden im System als **Fähigkeiten** bezeichnet und mit dem Basissystem konfiguriert.

Vorbereitungen

Fügen Sie das folgende JSON-Skript Ihrer Allow-Liste von Agent Client Collector hinzu, um die Ausführung der im Basissystem enthaltenen Aktionen zu ermöglichen.

```
{
 "args": [
  "--logger_min_status 1",
  "--json",
  "SELECT p.name, p.state, p.pid, p.parent as ppid, p.path, p.total_size, p.start_time,
 p.elapsed_time as run_time, p.cmdline, p.uid, p.username, u.type as owner_domain, u.uuid
 FROM processes as p LEFT JOIN users as u ON u.uid = p.uid",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "select name, process_open_sockets.pid, parent as ppid, processes.path,
process_open_sockets.state, total_size, process_open_sockets.protocol, local_address,
local_port, remote_address, remote_port from process_open_sockets, processes where
process_open_sockets.pid = processes.pid",
  "select * from services order by service_type",
  "select computer_name, hardware_serial, hostname, name as os, build, version, mac, address
from system_info, os_version, interface_details, interface_addresses where address like '%:%'
and interface_addresses.type='manual' or interface_addresses.type ='dhcp' limit 1",
  "select * from logged_in_users order by time"
 ],
 "exec": "osqueryi",
 "skip_arguments": false
}
```

Erforderliche Rolle: sn_si.admin oder sn_si.basic

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu den Fähigkeiten, die mit dem Basissystem bereitgestellt werden, finden Sie unter Agent Client Collector Security Incident Response-Fähigkeiten.

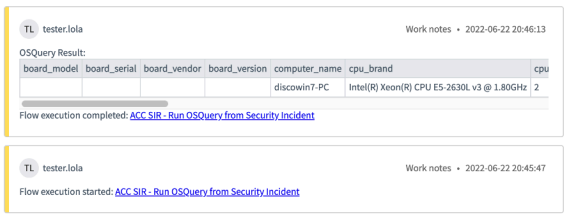
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie einen Incident aus.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus.
   Das Dialogfeld **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) wird geöffnet.
4. Wählen Sie die Fähigkeit aus, die Sie ausführen möchten.

Agent Client Collector-Fähigkeiten

Feld	Beschreibung
ACC Integration Capabilities (ACC-Integrationsfähigkeiten)	Die ACC-Integrationsfähigkeiten. Wenn die Fähigkeit „Osquery auf Agent ausführen“ ausgewählt ist, werden die Daten in den Arbeitsnotizen tabellarisch formatiert.
ACC Integration OSQuery (OSQuery-Abfrage der ACC-Integration)	Die Osquery-Abfrage der ACC-Integration. Beispiel: ausgewählte Systeminformationsspalten.
Kontrollkästchen „Transpose Data“ (Daten transponieren)	Transponieren Sie die Daten. Bei Auswahl werden die Informationen mit vertikalen Spalten angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	 Wenn diese Option deaktiviert ist, werden die Informationen horizontal angezeigt. 

5. Wählen Sie **Absenden** aus.
   Die ausgewählte Fähigkeit wird für das CI des Security Incident ausgeführt.

Zugehörige Informationen

Agent Client Collector-Zulassungsliste generieren

Agent Client Collector Security Incident Response-Befehl erstellen

Definieren Sie einen Befehl oder eine Befehlszeichenfolge, der/die auf einem Computer ausgeführt werden soll, auf den ein Security Incident verweist. Befehle werden nach Betriebssystem aufgelistet. Beispielsweise wird mit einem *ps*-Befehl unter einem Windows-Betriebssystem der Status aktiver Windows-Betriebssystemprozesse auf dem System abgerufen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector-SIR-Integration** > **ACC-Integration – Befehle**an.
2. Wählen Sie **Neu**.
   Die Seite **ACC Integration Commands – New Record** (ACC-Integrationsbefehle – Neuer Datensatz) wird angezeigt.
3. Konfigurieren Sie die Felder auf der Seite.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC Integration Commands (ACC-Integrationsbefehle)

Feld	Beschreibung
Name	Ein beschreibender Name für den Befehl
Betriebssystem	Das von Agent Client Collector unterstützte Betriebssystem des CI
Befehl	Der tatsächlich auszuführende Befehl oder die tatsächlich auszuführende Befehlszeichenfolge

4. Um zu überprüfen, ob der von Ihnen geschriebene Befehl funktioniert, wählen Sie **Test Command**(Befehl testen) aus.
   Die Seite **Test Command** (Befehl testen) wird angezeigt.

Test Command (Befehl testen)

Feld	Beschreibung
Mitarbeiter	Der spezifische Endpunkt, an dem der Befehl ausgeführt wird.

5. Geben Sie den spezifischen Endpunkt-Agent ein, auf dem das Ergebnis des Tests angezeigt wird.
   - – im Erfolgsfall
   - – Ausgabe zu groß
   - – oder es ist ein Fehler mit der Fehlermeldung aufgetreten, die für den sn_si.admin angezeigt wird.
6. Wählen Sie **Absenden** aus.

Agent Client Collector Security Incident Response-Befehl ausführen

Führen Sie einen angegebenen Befehl auf einem Computer aus, auf den ein Incident verweist, um Informationen zum CI des Incidents abzurufen. Wenn Sie beispielsweise einen *ps*-Befehl für einen Incident ausführen, wird mit dem Befehl der Status aktiver Prozesse auf dem System abgerufen. Befehle werden entsprechend dem CI-Betriebssystem aufgelistet, das dem Security Incident zugeordnet ist.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie einen Incident aus.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus.
   Das Dialogfeld **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) wird geöffnet.
4. Wählen Sie **Befehl auf Agent ausführen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Feld **ACC Integration Capabilities** (ACC-Integrationsfähigkeiten) die Option **Befehl auf Agent ausführen** aus.
   Das Feld**ACC Integration Command** (ACC-Integrationsbefehl) wird angezeigt.
6. Wählen Sie den Befehl aus, den Sie ausführen möchten.
   Die verfügbaren Befehle sind diejenigen, die auf der Seite „ACC Integration Commands“ (ACC-Integrationsbefehle) konfiguriert sind, wie in Agent Client Collector Security Incident Response-Befehl erstellen beschrieben.
7. Wählen Sie **Absenden** aus.
   Der Befehl wird gemäß dem im Befehl angegebenen Betriebssystem für das CI des Security Incident ausgeführt.

Agent Client Collector Security Incident Response-OSQuery erstellen

Definieren Sie eine OSQuery, um Informationen zum CI eines Security Incident zu sammeln. OSQuery bietet eine SQL-Ebene zusätzlich zu BS-Tabellen und wird zusammen mit Agent Client Collector als Teil des Basissystems gebündelt.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector-SIR-Integration** > **ACC-Integration – OSQuery**an.
2. Wählen Sie **Neu**.
   Die Seite **ACC Integration OSQuery – New Record** (ACC-Integrations-OSQuery – Neuer Datensatz) wird angezeigt.
3. Konfigurieren Sie die Felder auf der Seite.

ACC Integration OSQuery (OSQuery-Abfrage der ACC-Integration)

Feld	Beschreibung
Name	Ein beschreibender Name für die Abfrage
Abfrage	Abfragezeichenfolge.

4. Um zu überprüfen, ob die von Ihnen geschriebene Abfrage funktioniert, wählen Sie **Test Osquery**(Osquery testen) aus.
   Die Seite **Test Osquery** (Osquery testen) wird angezeigt.

Test Osquery (Osquery testen)

Feld	Beschreibung
Mitarbeiter	Der spezifische Endpunkt, an dem die Abfrage ausgeführt wird.

5. Geben Sie den spezifischen Endpunkt-Agent ein, auf dem das Ergebnis des Tests angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- – im Erfolgsfall
- – Ausgabe zu groß
- – oder es ist ein Fehler mit der Fehlermeldung aufgetreten, die für den sn_si.admin angezeigt wird.

6. Wählen Sie **Absenden** aus.
   Von OSQueries werden Informationen auf dem Zielcomputer erfasst, wobei die Incident-Befehle nach Betriebssystem aufgelistet sind. Beispielsweise werden von einer Abfrage, die als `select * from system_info` definiert ist, alle Informationen aus der OSQuery-Tabelle `system_info` abgerufen.

Agent Client Collector Security Incident Response-OSQuery ausführen

Führen Sie eine Osquery auf einem Computer aus, auf den ein Incident verweist, um Informationen zum CI des jeweiligen Incidents abzurufen. Wenn Sie beispielsweise die Abfrage `select * from system_info` ausführen, werden mit der Abfrage alle Informationen aus der OSQuery-Tabelle `system_info` abgerufen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie einen Incident aus.
3. Wechseln Sie im Abschnitt „Zugehörige Links“ zur Liste der **Konfigurationselemente**, und wählen Sie die CIs der einzelnen Incidents aus, für die Sie die Informationen abrufen möchten.
4. Wählen Sie im Kontextmenü die Option **Run ACC Osquery** (ACC-Osquery ausführen) aus.
   Das Dialogfeld **Osquery to run** (Auszuführende Osquery) wird geöffnet.
5. Wählen Sie den Namen der Abfrage aus, die Sie ausführen möchten.
   Die verfügbaren Abfragen sind diejenigen, die auf der Seite „ACC Integration Osquery“ (Osquery-Abfrage der ACC-Integration) konfiguriert sind, wie in Agent Client Collector Security Incident Response-OSQuery erstellen beschrieben. Optionen können entsprechend ihrem Wert für „Name“ ausgewählt werden.
6. Wählen Sie **Absenden** aus.
   Die Abfrage wird für die CIs der jeweils ausgewählten Security Incidents ausgeführt.

Live-CI-Daten mit Agent Client Collector anzeigen

Zeigen Sie Live-Daten für incident-bezogene CIs über an Agent Client Collector Für Informationen, die zur Lösung der Incidents beitragen können.

Vorbereitungen

- Laufende Prozesse für werden erfasst macOS System erfordert Sudo Berechtigungen. Wenn Sudo Berechtigungen werden nicht gewährt, nur Prozesse, die von ausgeführt werden Agent Client Collector Werden erfasst.

  Zum Aktivieren Sudo Berechtigungen für osqueryi: Fügen Sie entweder die folgenden Zeichenfolgen hinzu /Etc/sudoers Datei oder in eine einzelne Datei im /Etc/sudoers.d Verzeichnis:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cmnd_Alias LIVE_CI_VIEW = /Library/Application\ Support/servicenow/Agent-Client-Collector/osquery/bin/osqueryi
- _SERVICENOW ALLE=(ALLE) NOPASSWD:LIVE_CI_VIEW

- Damit die ausführbare OSQuery-Datei Informationen zu angemeldeten Anwendern in einer Windows-Umgebung abrufen kann, muss der Agent als lokaler SYSTEMACCOUNT ausgeführt werden.

Stellen Sie sicher, dass Sie installiert haben Agent Client Collector Framework Und Service Operations-Arbeitsbereich In Ihrer Instanz.

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol ( ).
3. Auswahlvorgang **Incidents** > **Alle**an.
4. Wählen Sie einen Incident aus der Liste aus.
5. Wählen Sie im Formular <Name des Incident> die Option aus **Live-CI-Daten** Registerkarte.
   Die CI-Daten werden auf den in der folgenden Tabelle beschriebenen Karten angezeigt.

Karten der Registerkarte „Live CI Data“ (Live-CI-Daten)

Karte	Beschreibung
Gerätedetails	Allgemeine Details zum CI
Speicherauslastung	Vom CI verwendeter Arbeitsspeicher
Top 5 running processes by CPU usage (Top 5 der laufenden Prozesse nach CPU-Auslastung)	Die fünf CI-Prozesse mit der meisten CPU.
Top 5 der laufenden Prozesse nach Arbeitsspeichernutzung	Die fünf CI-Prozesse, die den meisten Arbeitsspeicher verwenden.
Festplattenauslastung in %	Prozentsatz des vom CI verwendeten Speicherplatzes
Angemeldete Benutzer	Benutzer, die beim CI angemeldet sind. Ob diese Daten sichtbar sind, hängt von Ihren BS-Berechtigungen ab. ○ MacOS: Erfordert sudo-Berechtigungen ○ Windows-System: Erfordert Administratorrechte ○ Linux: Es sind keine besonderen Berechtigungen erforderlich

Zugehörige Informationen

Zeigen Sie Live-CI-Datenprotokolle an

Weisen Sie seinem Incident ein problematisches CI zu, um Live-CI-Daten anzuzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Live-CI-Datenprotokolle an

Zeigen Sie CI-Protokolle an, um beim Anzeigen von Live-CI-Daten zusätzliche Details zu einem Incident zu erhalten. Zum Beispiel kann das Anzeigen von Protokollinformationen für einen Prozess mit hoher CPU-Auslastung Ihnen helfen, herauszufinden, wann die Auslastung gestiegen ist, und Ihnen dabei helfen, die Ursache des Problems zu bestimmen.

Vorbereitungen

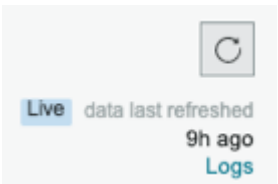
Stellen Sie sicher, dass Sie installiert haben Agent Client Collector Framework Und Service Operations-Arbeitsbereich In Ihrer Instanz.

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol ( ).
3. Auswahlvorgang **Incidents** > **Alle**an.
4. Wählen Sie einen Incident aus der Liste aus.
5. Wählen Sie die Registerkarte **Live CI Data** (Live-CI-Daten) aus.
6. Wählen Sie aus **Protokolle** Link auf der rechten Seite des Bereichs.

Link „Protokolle“



Hinweis: Der Wert **data last refreshed** (letzte Aktualisierung der Daten) folgt der Zeitzone der Instanz und nicht der Zeitzone Ihres lokalen Systems. Stellen Sie daher sicher, dass Ihre lokale Systemzeitzone mit der Instanzzeitzone übereinstimmt.

Die Protokolle werden im angezeigt **Protokoll** Seite.

Weisen Sie seinem Incident ein problematisches CI zu, um Live-CI-Daten anzuzeigen

Rufen Sie Live-CI-Daten ab, um die Probleme zu beheben, die einen Incident verursacht haben, indem Sie das problematische CI seinem Incident zuweisen. Ein Incident ist normalerweise dem CI zugeordnet, das den Incident verursacht hat. Wenn dies jedoch während der Incident-Erstellung ausgelassen wurde, können Sie das CI manuell zuweisen.

Vorbereitungen

Stellen Sie sicher, dass Sie installiert haben Agent Client Collector Framework Und Service Operations-Arbeitsbereich In Ihrer Instanz.

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol ( )-Symbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

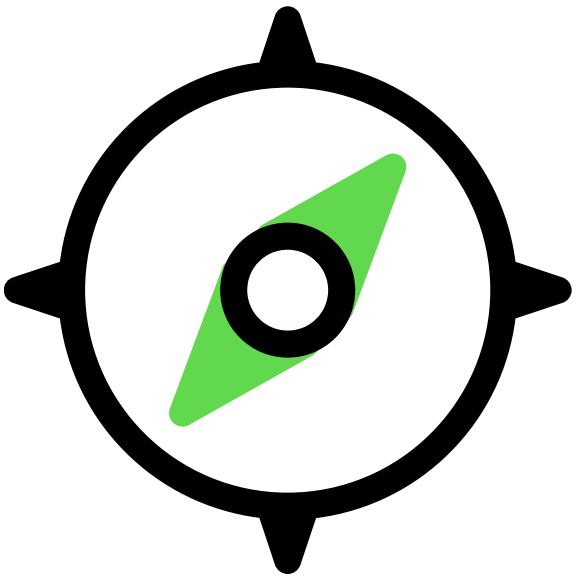
3. Auswahlvorgang **Incidents** > **Alle**an.
4. Wählen Sie einen Incident mit einem Wert von aus **Konfigurationselement = (leer)** .
5. Wählen Sie die Registerkarte **Live CI Data** (Live-CI-Daten) aus.
6. Geben Sie die ersten Zeichen des CI ein, das den Incident verursacht hat **Primäres Konfigurationselement** Feld.
   Eine Liste der CIs, die der Zeichenfolge entsprechen, wird angezeigt.
7. Wählen Sie das relevante CI aus der Liste aus.
   Der Name des CI wird in angezeigt **Primäres Konfigurationselement** Und die Live-Daten des CI werden im angezeigt **Live-CI-Daten** Registerkarte.

Metrikdaten

ServiceNow® Metrikdaten Bietet die Möglichkeit, operative Metrikdaten zu erfassen, zu untersuchen und zu analysieren und Anomalien zu identifizieren und anzuzeigen. Metrikdaten Generiert Anomaliewarnungen, die zu IT-Warnungen heraufgestuft werden können und im Service Operations-Arbeitsbereich und im Dashboard für die Serviceintegrität angezeigt werden. Sie können diese Analyse nutzen, um potenzielle Serviceausfälle zu vermeiden.

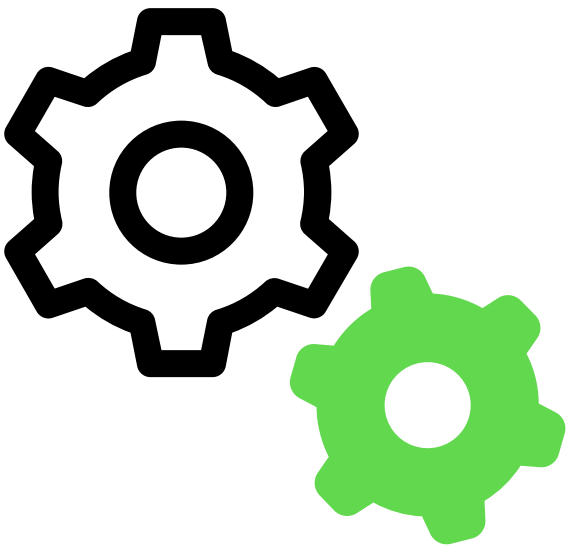
Erste Schritte

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen kennen, die der bietet Metrikdaten Anwendungsangebote.

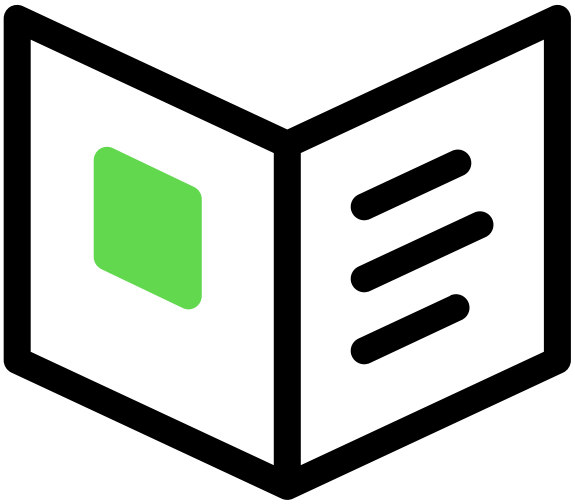
Konfigurieren



Konfigurieren Sie die zu aktivierenden Funktionen und Komponenten Metrikdaten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optimieren	Referenz
	
Verwalten Sie Metriken, Ereignisse, Warnungen und Anomalien, um Ihre Metrikdaten optimal zu nutzen.	Rufen Sie zusätzliche Informationen zu ab Metrikdaten Einstellungen und Eigenschaften.

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow-Universität

Jetzt erstellen

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://ServiceNow.com

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Store

http://ServiceNow.com

Support

- https://support.servicenow.com/now
- Known Error-Portal

Metrikdaten erkunden

Erfahren Sie mehr über die Verwendung von Metrikdaten Zum Analysieren von Metrikdaten und Identifizieren von Anomalien.

Metrikdaten – Übersicht

Metrikdaten Hilft, potenzielle Serviceausfälle zu identifizieren und zu verhindern. Basierend auf historischen Metrikdaten, Metrikdaten Gibt das anomale Verhalten von CIs an, die Ereignisse möglicherweise nicht erfassen.

Metrikdaten – Anwender

Anwender

Anwender	Beschreibung
Ereignismanagement-Anwender [evt_mgmt_user]	Kann Warnungen und ihre zugrunde liegenden Metriken anzeigen.
Ereignismanagement-Administrator [evt_mgmt_admin]	Kann alle Metrikdefinitionen und Connector-Einstellungen konfigurieren.
Operator [evt_mgmt_operator]	Kann alle Metrikdefinitionen und Connector-Einstellungen anzeigen.

Metrikdaten – Workflow

Die folgende Abbildung beschreibt das Layout und den Daten-Flow in Metrikdaten Anwendung.

Metrikdaten – Vorteile

Vorteil	Funktion	Anwender
Überwachen Sie die Integrität, Leistung und Verfügbarkeit Ihres Systems durch die automatisierte Erfassung von Ereignissen und Metriken, wobei automatisierte Konfigurationen genutzt werden.	Agent Client Collector-Überwachung	NOC-Operator, Ereignismanagement Administrator
Reduzieren Sie das Rauschen, indem Sie nur die aussagekräftigsten Anomalien heraufstufen.	Zeigen Sie Anomaliewarnungen an	Ereignismanagement-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteil	Funktion	Anwender
	Metrikregeln erstellen	
Erkennen Sie Anomalien mit der KI-basierten Anomalieerkennung, entweder mit der Erkennung abnormaler Muster für nicht überwachtes maschinelles Lernen (kein Anwendereingriff) oder durch das Festlegen deterministischer Warnungsregeln (manuelles Festlegen eines statischen Schwellenwerts).	Wie Health Log Analytics Warnungen generiert	Ereignismanagement-Administrator
Verbessern Sie die Lösungszeit für offene Warnungen und Incidents mit der Visualisierung von Rohmetrikdaten.	Metric Explorer	NOC-Operator, Ereignismanagement Administrator

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Metrikdaten finden Sie unter:

- Metrikdaten konfigurieren
- Wird Optimiert Metrikdaten
- Metrikdaten – Referenz

Metrikdaten verstehen

Verwenden Sie Metrikdaten, um potentielle Serviceausfälle zu erkennen und zu verhindern. Metrikdaten, das auf historischen Metrikdaten basiert, weist auf anomales Verhalten von CIs hin, das von Events möglicherweise nicht erfasst wird. Anomaliewarnungen können zu regelmäßigen IT-Warnungen heraufgestuft werden und im Service Operations-Arbeitsbereich und im ServiceintegritätsDashboard für vorbeugende Aktionen angezeigt werden.

Anomalie-Erkennung

Metrikdaten werden von verschiedenen Datenquellen wie SCOM, dem SolarWinds-Überwachungssystem oder dem Nagios XI-Server (einige sind teilweise standardmäßig für die Metriksammlung konfiguriert) gesammelt. Diese Überwachungssysteme sammeln regelmäßig Metrikdaten aus der Quellumgebung. Metrikdaten erfasst die Rohdaten aus diesen Überwachungssystemen und verwendet Ereignisregeln und die CMDB-Identifizierungs-Engine, um Daten zu bestehenden CIs und deren Ressourcen zuzuordnen. Die Daten werden dann analysiert, um Anomalien zu erkennen und andere statistische Punktzahlen bereitzustellen.

Metrikdaten verwendet historische Metrikdaten, um statistische Modelle zu erstellen. Diese Modelle erleichtern die Projektion der erwarteten Metrikwerte zusammen mit der oberen und der unteren Grenze. Metrikdaten verwendet dann diese Projektionen, um statistische Ausreißer zu erkennen und Anomaliepunktzahlen zu berechnen. Anomalien werden in einem Bereich von 0 bis 10 bewertet. Hohe Anomaliepunktzahlen für CI-Metriken können darauf hinweisen, dass bei einem CI das Risiko eines Serviceausfalls besteht.

Nach der Verarbeitung zeigt der Explorer für Einblicke Metrikstatistiken und Diagramme an, und die Anomaliezuordnung zeigt über eine Zeitleiste korrelierte Punktzahlen für die CIs mit den höchsten Anomaliepunktzahlen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gegebenenfalls empfiehlt es sich, die Anomalie-Erkennung während der Systemwartung zu deaktivieren, da Anomalien irrelevant sein können, wenn sie während der Wartung erkannt werden. Legen Sie dazu die Eigenschaft `mid.mi.anomaly_detection.disable` auf **true** fest.

Um die Anzeige von Anomalien für Metriken anzupassen, die als nahezu konstant klassifiziert sind, wenden Sie sich an den Kundensupport.

Metrikdaten ist verfügbar, wenn Sie das Plugin Metrikdaten (com.snc.sa.metric) aktivieren.

Mit Metrikdaten verwendete Begriffe

Quellmetriktyp

Eine Metrik wie „% freier Speicherplatz“ oder „Aktuelle Bandbreite“, die von einer Datenquelle für ein CI gemessen werden kann. Für jede Datenquelle können Sie auswählen, welcher der möglichen Quellmetriktypen verarbeitet wird. Beispielsweise sind etwa 380 Quellmetriktypen für die SCOM-Datenquelle standardmäßig aktiv.

Abweichung

Daten, die außerhalb der Kontrollgrenzen liegen, werden als statistische Ausreißer betrachtet. Diese Ausreißer werden zur Berechnung einer Anomaliepunktzahl verwendet, die einem Wert zwischen 0 und 10 entspricht und den Grad angibt, zu dem die Metrik unwahrscheinlich erscheint. Wenn eine Anomaliepunktzahl über einem Schwellenwert liegt, wird eine Anomaliewarnung generiert. Anomaliewarnungen werden getrennt von regulären IT-Warnungen gemeldet.

Ressource

Eine Komponente eines CI, die aus mehreren einzelnen Komponenten ähnlichen Typs besteht, wobei jede Unterkomponente separat überwacht werden kann. Beispielsweise einzelne Webseiten oder bestimmte Datenträger wie „Datenträger C:“ und „Datenträger D:“.

Zeitreihen

Eine Reihe von Werten (z. B. Metrikwerte) über einen Zeitbereich, die einem CI und einem Metriktyp zugeordnet sind. Da für jede Metrik eine Anomaliepunktzahl ausgewertet wird, entspricht die Reihe der Anomaliepunktzahlen über einen Zeitraum auch einer Zeitreihe. Zeitreihen werden vom statistischen Modell berechnet, das für eine Metrikdatenreihe erstellt wurde, und werden mit Metrikdatenwerten, Anomaliepunktzahlen sowie der oberen und der unteren Kontrollgrenze verwendet.

Statistische Modelle

Metric Intelligence-Aufträge lernen aus vergangenen Metrikdaten (bis zu 32 Tage alt). Ein Modelltrainingsprozess analysiert historische Daten, um ein Modell zu erstellen, das zukünftige Werte projiziert. In der Regel sind Modelle bis zur nächsten Ausführung des Modelllernprozesses gültig. Diese Modelle werden zur Berechnung der oberen und der unteren Grenze verwendet. Eingehende Werte, die diese Grenzen überschreiten und deren statistische Signifikanz von den erwarteten Werten abweicht, generieren Anomalien. Jedes Modell weist ein eindeutiges Muster auf und ist mit einem Klassifizierer versehen, der das allgemeine Verhalten des Modells veranschaulicht. Diese Klassifizierung bestimmt, ob eine Anomalie-Erkennung angewendet werden kann. Die meisten Modelle können projizieren, welche zukünftigen Werte von den erwarteten Werten abweichen. Derartige Modelle sind Kontrollgrenzen zugeordnet und die Anomalie-Erkennung kann angewendet werden (falls aktiviert).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einige Modelle sind jedoch nicht genügend Daten vorhanden, um zu bestimmen, welche Werte anomal sind. In diesem Fall kann die Anomalie-Erkennung nicht ohne zusätzliche Informationen angewendet werden (selbst wenn die Anomalie-Erkennung aktiviert ist).

Die gelernten Datenmodelle werden in der Tabelle „Metrikzeitreihenmodell“ [sa_time_series] gespeichert.

Die folgenden statistischen Modelle und Klassifizierer werden bei der Anomalie-Erkennung verwendet:

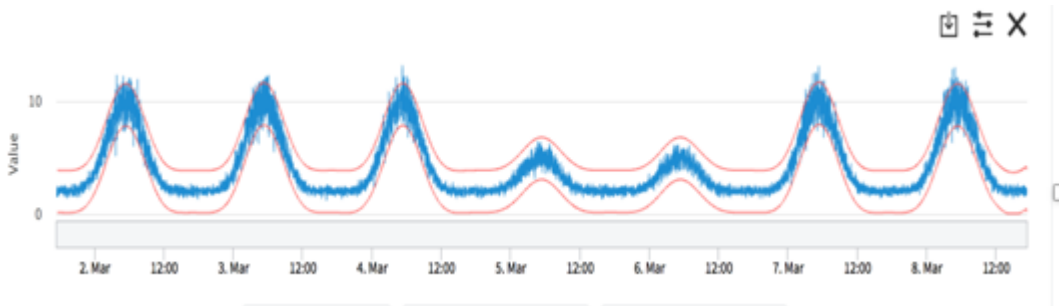
Statistisches Zeitreihenmodell

Nach der Einrichtung passt sich ein Zeitreihenmodell nicht an Änderungen in den eingehenden Metrikdaten an. Wenn sich daher das Muster eingehender Daten ändert, werden diese Änderungen wahrscheinlich als anomal eingestuft. Die obere und die untere Kontrollgrenze bleiben, nachdem sie erlernt wurden, bis zur nächsten Ausführung des Lernprozesses bestehen (Daten werden jeden Tag gelernt).

Wöchentlich

Daten mit einem Muster, das sich über wöchentliche Intervalle wiederholt (saisonales Modell).

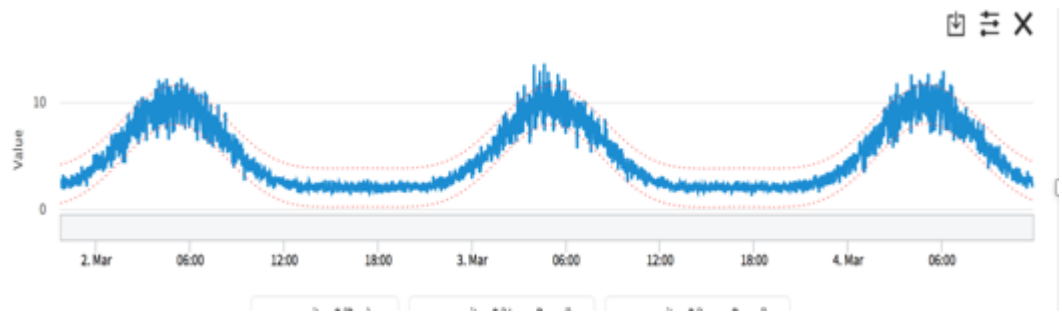
Erfordert Daten von mindestens 15 Tagen in der Reihe, wie in der Konfigurationseinstellung week_model_min_days festgelegt.



Täglich

Daten mit einem Muster, das sich über tägliche Intervalle wiederholt (saisonales Modell).

Erfordert Daten von mindestens 3 Tagen in der Reihe, wie in der Konfigurationseinstellung daily_model_min_days festgelegt.



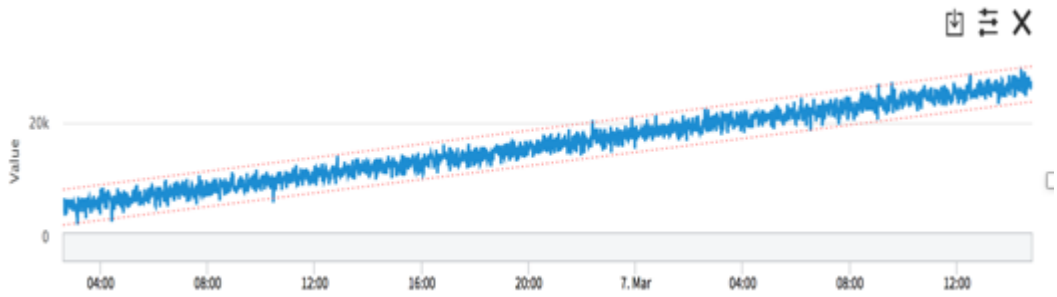
Mit Trend

Daten mit einem linearen Trend mit einer gewissen Steigung und mit einigem Rauschen.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.

Automatische Übersetzung

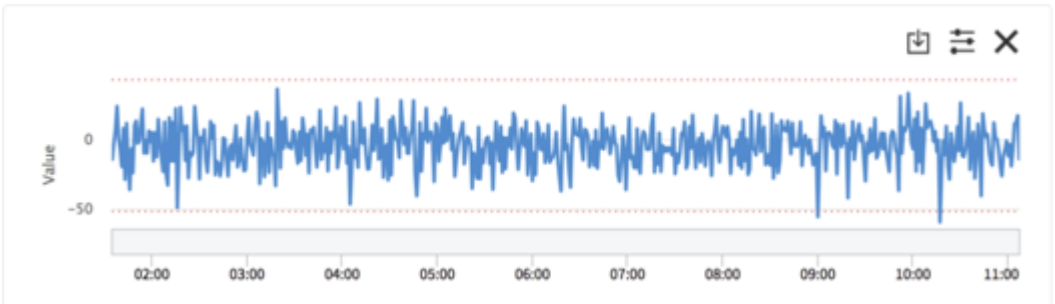
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verrauscht

Typische verrauschte Daten, die eine grundlegende Musterklassifizierung in einem Datenmodell darstellen. Das Muster lässt sich nicht mit einem bestimmten Trend oder einer bestimmten Saisonabhängigkeit identifizieren.

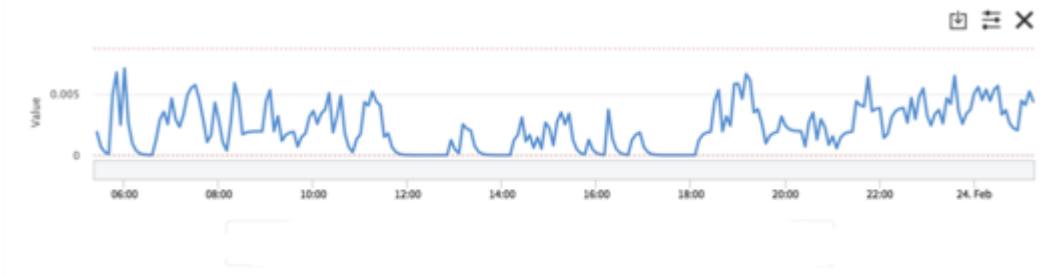
Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Positiv abgeschnitten verrauscht

Ähnlich dem verrauschten Klassifizierer mit Ausnahme der unteren Grenze, die auf 0 festgelegt ist.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Zentriert verrauscht

Verrauschte Daten, die sich typischerweise symmetrisch zwischen der benutzerdefinierten oberen und unteren Grenze ausbreiten. Die Formel, die zum Festlegen von Begrenzungen und Breitenwerten verwendet wird, ignoriert die statistischen Daten, und die untere und die obere Breite haben einen identischen Wert.

Erfordert, dass die Anzahl der Datenpunkte in der Reihe gleich Null ist.

Weitere Informationen finden Sie unter Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen.

Automatische Übersetzung

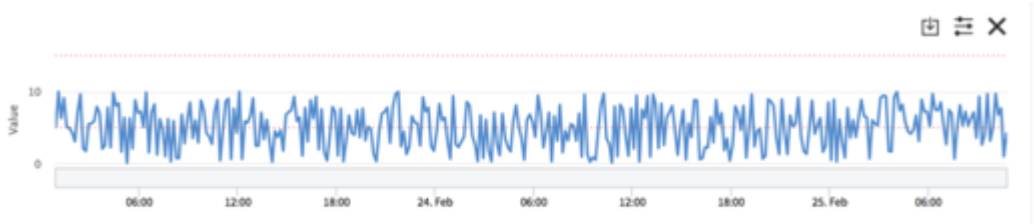
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verzerrt verrauscht

Verrauschte Daten, die nicht gleichmäßig zwischen der benutzerdefinierten oberen und unteren Grenze verteilt sind, sondern sich stattdessen tendenziell näher an einer der Grenzen konzentrieren. Der Median der Daten wird verwendet, um eine obere und eine untere Breite getrennt zu berechnen.

Erfordert mindestens einen Datenpunkt in der Reihe.

Weitere Informationen finden Sie unter Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen.



Verzerrtes Rauschen – Allgemeine Extremwertverteilung (Genaralized Extreme Value, GEV)

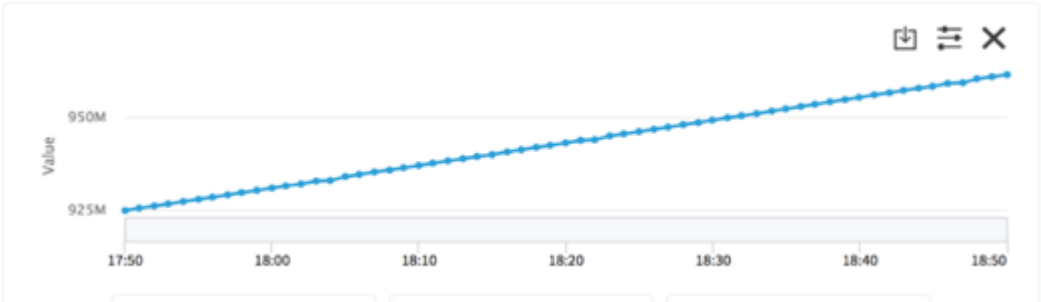
Verrauschte Daten, die nicht gleichmäßig zwischen der benutzerdefinierten oberen und unteren Grenze verteilt sind, sondern sich stattdessen tendenziell näher an einer der Grenzen konzentrieren. Außerdem weist die Datenverteilung ein langes Verteilungsende oder einen schweren Rand auf. Der vom Rand/Ende der Verteilung abgeleitete Median der Daten wird dazu verwendet, gesondert eine obere und eine untere Breite zu berechnen. Die Serie muss mindestens einen Datenpunkt enthalten.

Akkumulator

Datenmuster ähnlich dem Trend-Klassifizierer, aber mit monotonem Anstieg und ohne Rauschen. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.

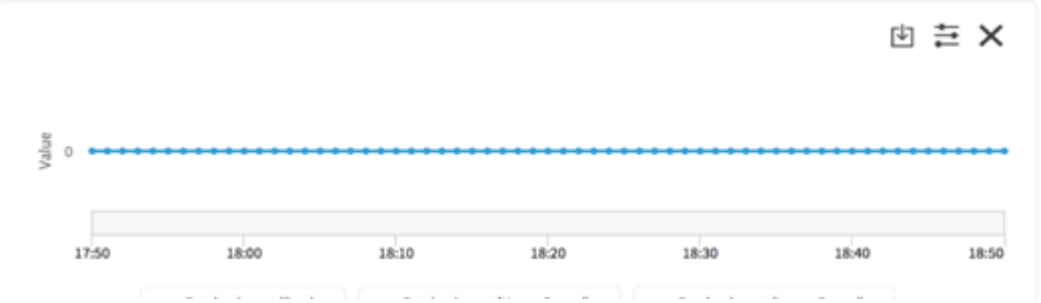
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nahezu konstant

Nahezu konstante Daten, bei denen die meisten Werte einem spezifisch konstanten Wert entsprechen. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Erkannte Konstante

Aktiviert die Überprüfung nahezu konstanter Metriken auf Anomalien. Dazu müssen Sie die Metriken über ein Systemtoken in das Modell „erkannte Konstante“ verschieben. Wenden Sie sich an den Kundensupport, um der Tokenliste Token hinzuzufügen und zu ermöglichen, dass weitere Metriken auf Anomalien gemessen werden können.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.

Aktiviert, wenn Metrik_Name_Analysis.add_detected_konstante_Candidate Systemeigenschaft ist auf festgelegt **Wahr** . Um den Wert dieser Eigenschaft für einen bestimmten Metriktyp zu überschreiben, aktualisieren Sie **Erkannter Konstanter Kandidat** Feld in der Tabelle „Metriktypen“, indem Sie wie folgt vorgehen:

1. Geben Sie Ein sa_metric_type.list Im Instanznavigationsfeld.
2. In **Erkannter Konstanter Kandidat** Wählen Sie den relevanten Wert für den Eintrag aus, den Sie aktualisieren möchten.

Erkannte konstante Kandidatenwerte

Wert	Beschreibung
<empty>	Ein Algorithmus hat automatisch entschieden, ob die Metrik für das erkannte Konstantenmodell berücksichtigt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
	Dies ist der Standardwert.
Ja	Die Metrik wird für das erkannte Konstantenmodell berücksichtigt.
Nein	Die Metrik wird für das erkannte Konstantenmodell nicht berücksichtigt.

Multinomial

Datenmuster, in dem alle Werte zu einer relativ kleinen Anzahl von Werten gehören. Beispielsweise lauten die Werte immer 100 oder 99,9. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 400 Datenpunkte in der Reihe, berechnet als 10-facher Wert der Konfigurationseinstellung multinomial_count_threshold.

Beschädigt

Die Daten haben nicht genügend Datenpunkte, um ein Muster zu identifizieren. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert, dass die Anzahl der Datenpunkte in der Reihe kleiner als der Wert der Konfigurationseinstellung corrupt_data_count_threshold (standardmäßig 30) ist.

Kalman-Filter – statistisches Modell

Add-on zum statistischen Zeitreihenmodell, das nur auf den verrauschten und positiv verrauschten Klassifizierer anwendbar ist. Dieses Modell ist eine allgemeine Methode zum Schätzen von Modellparametern aus einem Datenstrom, bei dem das Level der einzige Parameter im Modell ist. Das Kalman-Filtermodell kann an neue Werte in eingehenden Metrikdaten angepasst werden. Wenn das Rauschen keine eindeutigen Muster aufweist oder zu viel Rauschen vorhanden ist, wird das Kalman-Filtermodell nicht verwendet.

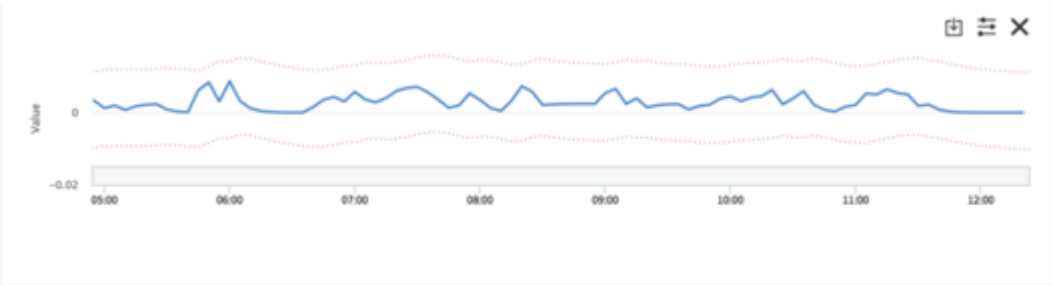
Lokales Level

Wenn eingehende Daten entsprechend den aktuellen Kontrollgrenzen um einen neuen Wert herum gruppiert werden, passt der Lernende das Datenmodell an, um einer permanenten Änderung Rechnung zu tragen. Dieses Clustering wird als neuer Wert im Datenmodell erkannt, sodass die meisten eingehenden Daten wieder innerhalb der Kontrollgrenzen liegen und nicht anomal sind. Eine solche Change-Erkennung ist nützlich, wenn z. B. einem Server Kerne oder Arbeitsspeicher hinzugefügt werden, die sich auf die Baselines auswirkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Nicht erkannt

Wenn Daten nicht zum Klassifizierer auf lokalem Level passen, werden Klassifizierer für Zeitreihen verwendet. Dies geschieht, wenn es nicht möglich ist, das Abweichungsverhältnis in einem erlernten Modell auf lokalem Level auf angemessene Werte anzupassen.

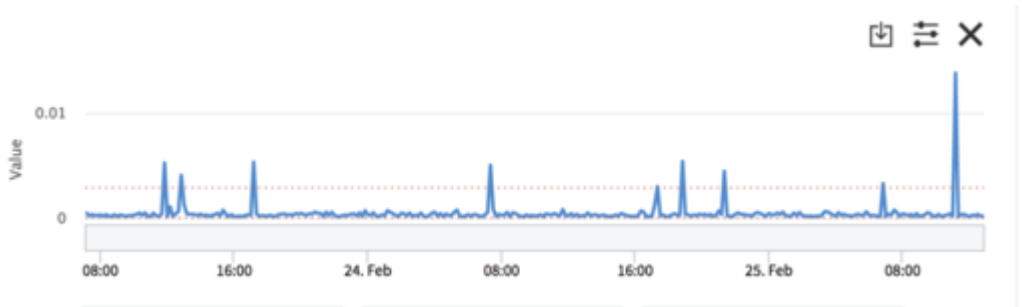
Nicht-parametrisches statistisches Modell

Add-on zum positiven verrauschten Klassifizierer. Im nicht-parametrischen Modell ist die Rauschverteilung nicht symmetrisch und entspricht keinem saisonalen Muster. Das nicht-parametrische Modell erstellt Kontrollgrenzen, die besser zu den tatsächlichen Daten passen, und die einmal gelernten Kontrollgrenzen bleiben bis zum nächsten Lernzyklus erhalten. Dieses Modell passt sich nicht an Änderungen in den Daten an, und es dauert länger, bis eine Abweichung als Anomalie erkannt wird.

Stationär, nicht parametrisch

Daten, die nicht zeitabhängig sind, was bedeutet, dass es bei der zeitlichen Verschiebung von Daten zu keiner signifikanten Verschiebung von Parametern wie Mittelwert und Abweichung kommt.

Erfordert mindestens 5.000 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung snpm_minimum_data_count festgelegt.



Nicht erkannt

Wenn Daten nicht zum stationären Klassifizierer passen, werden Klassifizierer für Zeitreihen verwendet.

Statistisches Modell der mittleren absoluten Abweichung vom Median (Median Absolute Deviation, MAD)

Ein Add-on zum verzerrten verrauschten Klassifizierer. Bei diesem Datentyp ist die Rauschverteilung nicht symmetrisch und entspricht keinem saisonalen Muster. Darüber hinaus entsprechen die Daten einer Verteilung mit langem Verteilungsende oder schwerem Rand. Im statistischen Modell der mittleren absoluten Abweichung vom Median werden Kontrollgrenzen erstellt, die besser zu den tatsächlichen Daten passen; die einmal gelernten Kontrollgrenzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bleiben dabei bis zum nächsten Lernzyklus erhalten. Durch Verwendung dieses Modells fällt die Entschlüsselung der Datenerfassung etwa 30 % effizienter aus.

MID Server und verteilter MID Server-Cluster für Metric Intelligence

Zur Nutzung von Metrikdaten muss mindestens ein verteiltes MID-Server-Cluster vorhanden sein, das einen einzelnen MID-Server enthält, der für Metrikdaten konfiguriert ist.

Wenn Sie einen einzelnen Metrikdaten MID-Server verwenden, muss dieser Server einem verteilten MID-Server-Cluster hinzugefügt werden.

Um den angegebenen Durchsatz zu unterstützen, erstellen Sie ein verteiltes Cluster mit einem einzelnen MID-Server, der die Metrikdaten MID-Server-Anforderungen erfüllt. Bei Verwendung eines virtuellen Computers (Virtual Machine, VM) kann nur ein einzelner MID-Server ausgeführt werden, der Metrikdaten unterstützt. Bei der Arbeit mit Agent Client Collector kann ein MID-Server auch mit mehreren Agents (ACC-M und ACC-L) verbunden werden.

Ein MID-Server, der Discovery unterstützt, kann auch mit anderen Anwendungen verwendet werden.

Weitere Informationen zum Einrichten von Metrikdaten finden Sie unter Erste Schritte mit Metrikdaten.

Verteilte MID Server-Cluster

Wird Aktiviert Metrikdaten(Com.snc.sa.metric), wird automatisch aktiviert MID-Server Verteilter Cluster (com.snc.Agent.Distributed.Cluster). A MID-Server Verteilter Cluster unterstützt verteilte MID-Server Clustertyp, der ausschließlich mit verwendet wird Metrikdaten.

Wenn die automatische Erstellung von MID-Server Verteilter Cluster schlägt fehl. Sie können den Cluster manuell konfigurieren. Weitere Informationen erhalten Sie vom Kundensupport.

Metrikdaten MID-Server

Der Metrikdaten MID-Server unterstützt die Metrikdaten-Funktion, indem Daten verarbeitet und Anomalien erkannt werden. Vom MID-Server werden Stapel verarbeiteter Daten an die Instanz übermittelt. Wenn eine Anomalie erkannt wird, werden Informationen über die Anomalie zusammen mit den Rohdaten sofort an die Instanz gesendet.

Jeder Metrikdaten MID-Server muss mit den folgenden Einstellungen konfiguriert werden:

- Metrikdaten als unterstützte Anwendung
- Die Fähigkeit „Metriken“
- Wird ausgeführt Metrikdaten Metrikerweiterung

Hinweis: Die Metrikdaten MID-Server Unterstützt IPv6 nicht.

Die Metrikdaten Anwendung, die Metrikdaten MID-Server Ist mit konfiguriert, können Sie zusätzliche unterstützte Anwendungen hinzufügen MID-Server. Standardmäßig Metrikdaten Ist in der Definition von enthalten MID-Server Option „ALLE“. Informationen zum Ändern des Verhaltens der Option ALLE bei der Auswahl unterstützter Anwendungen finden Sie unter Konfigurieren Sie Anwendungen, die in ALLEN Anwendungen enthalten sind .

Wenn das Installationsprogramm für Domänenunterstützung – Domänenerweiterungen aktiviert ist, können Sie einen konfigurieren MID-Server Mit der Metrikfunktion pro Domäne. In diesem Fall werden Metriken für einen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Business-Service in verarbeitet MID-Server Der sich in derselben Domäne wie der Business-Service befindet. Andernfalls wird A MID-Server Aus der globalen Domäne wird verwendet.

Stellen Sie sicher, dass MID-Server Die Sie für konfigurieren möchten Metrikdaten:

- Er ist validiert. Weitere Informationen finden Sie unter Validiert einen MID-Server
- Er wird ausgeführt.
- Er erfüllt alle Software-, Hardware- und Konfigurationsanforderungen.

Hardwareanforderungen für den virtuellen Computer/Host, auf dem der MID Server ausgeführt wird (skaliert für 5.000 CIs mit 100 Metriken pro CI)

Anforderung	
Eins MID-Server Mit: • Arbeitsspeicher: 12 GB • Prozessor: 4 Kerne	Unterstützt bis zu ca. 1,2 Millionen Metriken (12.000 CIs mit 100 Metriken pro CI).
Eins MID-Server Mit: • Arbeitsspeicher: 24 GB • Prozessor: 8 Kerne	Unterstützt bis zu ca. 1,7 Millionen Metriken (17.000 CIs mit 100 Metriken pro CI).

Software-Anforderungen

Software	Unterstützte Versionen	Zusätzliche Anforderungen
Windows	32-Bit- und 64-Bit-Versionen: • Windows 2008 R2 • Windows Server 2012 R2 • Windows Server 2019	32-Bit- oder 64-Bit-Version des MID-Servers
Linux	• Red Hat Enterprise Edition Linux 6.6 oder höher • CentOS Linux 6.6 oder höher	32-Bit- oder 64-Bit-Version des MID-Servers

Konfigurationsanforderungen

Konfiguration	Anforderung
MID-Server-Serviceanmeldeanwender (nur zum Abrufen erforderlich)	Muss auf einen Benutzer mit Lesezugriff auf die SCOM-Datenbank (OperationsManagerDW) festgelegt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsanforderungen (Fortsetzung)

Konfiguration	Anforderung
	1. Öffnen Sie auf dem MID Server das MID Server-Dialogfeld **Eigenschaften**. 2. Klicken Sie auf die Registerkarte **Anmeldung**. 3. Wählen Sie **Dieser Account** aus, und geben Sie die Anmeldeinformationen für einen Benutzer mit dem erforderlichen Zugriff ein. 4. Klicken Sie auf **Übernehmen**.

MID-Server-Drosselungsmechanismus

Der MID-Server-Drosselungsmechanismus schützt vor Daten-Bursts in der Instanz. Der Daten-Burst-Schutz verhindert eine Überlastung der Instanz und stellt gleichzeitig sicher, dass keine Daten verloren gehen.

Der MID-Server-Drosselungsmechanismus ist standardmäßig aktiviert. Es empfiehlt sich, diesen Mechanismus bei der Problembehandlung zu deaktivieren, damit gewährleistet ist, dass der Mechanismus keine Systemfehlfunktionen verursacht.

- Um diese Funktion für Metriken zu deaktivieren, legen Sie den Parameter mid.oi.metric_token_bucket_enabled auf **false** fest.
- Um diese Funktion für Anomalien zu deaktivieren, legen Sie den Parameter mid.oi.anomaly_token_bucket_enabled auf **false** fest.

Konfigurationsüberschreibung

Aktualisieren Sie die Datei wrapper-override.conf im Ordner ../agent/conf:

- Fügen Sie den folgenden Code am Ende der Datei hinzu:

```
# GC
wrapper.java.additional.5=-XX:+AlwaysPreTouch
wrapper.java.additional.6=-XX:+UseG1GC
wrapper.java.additional.7=-XX:+ScavengeBeforeFullGC
wrapper.java.additional.8=-XX:+DisableExplicitGC

# IP4
wrapper.java.additional.9=-DpreferIPv4Stack=true
```

- Vergewissern Sie sich, dass `wrapper.java.initmemory=1024` (oder höher) und `wrapper.java.maxmemory=4096` (oder höher) festgelegt sind, damit Metrikdaten ordnungsgemäß funktioniert.
- Optional können Sie, wenn auf einem Server zusätzlicher Arbeitsspeicher verfügbar ist, z. B. 16 GB RAM, in `wrapper.java.maxmemory=4096` den Wert 4096 durch 8192 ersetzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikkonfigurationsregeln

Mit Metrikkonfigurationsregeln können Sie bestimmen, wie eingehende Metriken aus Agent Client Collector verarbeitet werden sollen.

Wenn eine neue Metrik von Agent Client Collector eintrifft, wird in der Tabelle „Metrik-Zuordnung an CIs“ ein neuer Datensatz mit dem Wert **Aktionsebene der Anomalie-Erkennung = Grenzen** erstellt.

Um die Ausführung einer Metrikkonfigurationsregel auszulösen, navigieren Sie zur Tabelle Metrikkonfigurationsregeln (**Ereignismanagement** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**) Und wählen Sie aus **Mit MID synchronisieren** Schaltfläche oben auf der Seite. Damit werden auch alle mit der Instanz verbundenen MID Server synchronisiert.

Beim Ausführen der Regel überschreibt die in der Regel definierte Aktionsebene der Anomalie-Erkennung (durch den Parameter `anomaly_detection_action_level` festgelegt) rückwirkend die Aktionsebene der Anomalie-Erkennung, die für die Metrik in der Tabelle „Metrik-Zuordnung an CIs“ konfiguriert ist.

Wenn Sie die Regelausführung nicht auslösen, wird während der Ausführung der stündlich geplanten Aufgabe **Metric Intelligence – Metrikkonfiguration** der Parameter `Anomaly detection action level` rückwirkend überschrieben.

Beim Konfigurieren einer Metrikkonfigurationsregel werden Regeln mit einem Filter vor Regeln ohne Filter ausgeführt. Wenn mehrere Regeln dieselbe Priorität aufweisen, wird die zuletzt konfigurierte Regel zuerst ausgeführt.

Weitere Informationen zum Erstellen von Konfigurationseinstellungsregeln finden Sie unter Regel für Konfigurationseinstellungen erstellen.

Details zu den verfügbaren Aktionsebenen der Anomalieerkennung finden Sie unter Konfigurieren Sie die Aktionsebene für die Anomalieerkennung.

Empfindlichkeit der Metrikgrenzen

Beim Messen von Metriken im Explorer für Einblicke können Metrikgrenzen zu sensibel sein, was zu einer ungewöhnlich großen Anzahl von Anomalien führt. In diesem Fall passt sich das System selbst an, um sicherzustellen, dass weniger Anomalien erzeugt werden.

Wenn 95 % der Metrikwerte eines CI innerhalb von 2 Standardabweichungen (STDs) der mittleren Metrikwerte liegen, werden diese als `sensitive bounds` betrachtet. Mit sensiblen Grenzen wird eine große Anzahl von Anomalien generiert, von denen einige möglicherweise nicht relevant sind. Wenn sensible Grenzen erkannt werden, passt sich das System an und misst Metrikwerte innerhalb von 5 STDs, um weniger Anomalien zu generieren. Wenn keine sensiblen Grenzen erkannt werden (d. h. 95 % der Metriken liegen nicht innerhalb von 2 STDs des mittleren Metrikwerts), misst das System Metrikwerte innerhalb von 3 STDs. Alle Metrikwerte, die außerhalb der konfigurierten Grenzen liegen, werden zu Anomalien.

Die vorherigen Werte sind standardmäßig festgelegt. Details zum Anpassen dieser Werte finden Sie unter Eigenschaften der Empfindlichkeitsgrenzen für Metriken im Explorer für Einblicke.

Metriksammlungsquellen

Beim Einrichten Metrikdaten, Sie müssen eine Quelle für die Metriksammlung konfigurieren. Die Metriksammlung kann entweder von durchgeführt werden Agent Client Collector, Oder durch Metrik-Connectors.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Metriksammlungsquelle bestimmt, wo Metrikdaten Erfasst Metriken von. Um Details zum Erfassen von Metriken mit zu erhalten Agent Client Collector, Siehe Agent Client Collector-Überwachung konfigurieren.

Verwenden Sie beim Sammeln von Metriken mit Connectors entweder SCOM oder Dynatrace Connector. Details zum Verbinden von Metriken mit einem SCOM-Connector finden Sie unter SCOM-Connector-Instanz konfigurieren.

Für Details zum Verbinden von Metriken mit Dynatrace Connector, siehe Konfigurieren Sie Dynatrace Metriken-Connector-Instanz.

Metrikbindung

Nachdem Metrikdaten gesammelt wurden, identifiziert Metric Intelligence die CIs und die Ressourcen, an die die Daten gebunden werden sollen.

Die auf dem MID Server erfassten Daten sind Rohdaten, die sich nicht auf ein bestimmtes CI oder eine bestimmte Ressource in der CMDB beziehen. Um nützlich zu sein, durchlaufen die Daten einen **Normalisierungsprozess**, der CMDB-Identifizierungsregeln und Ereignisregeln verwendet, um CIs eindeutig zu identifizieren und sie den Rohdaten zuzuordnen und an diese zu binden. Rohdaten können auch Ressourcen zugeordnet und an diese gebunden werden, wenn die Bindung an ein CI erfolgreich und die Ressourcenbindung konfiguriert ist.

Datensätze für die Zuordnung von Rohdaten zu CIs werden automatisch generiert und bleiben für eine bestimmte, durch die Eigenschaften festgelegte Zeitspanne wirksam:

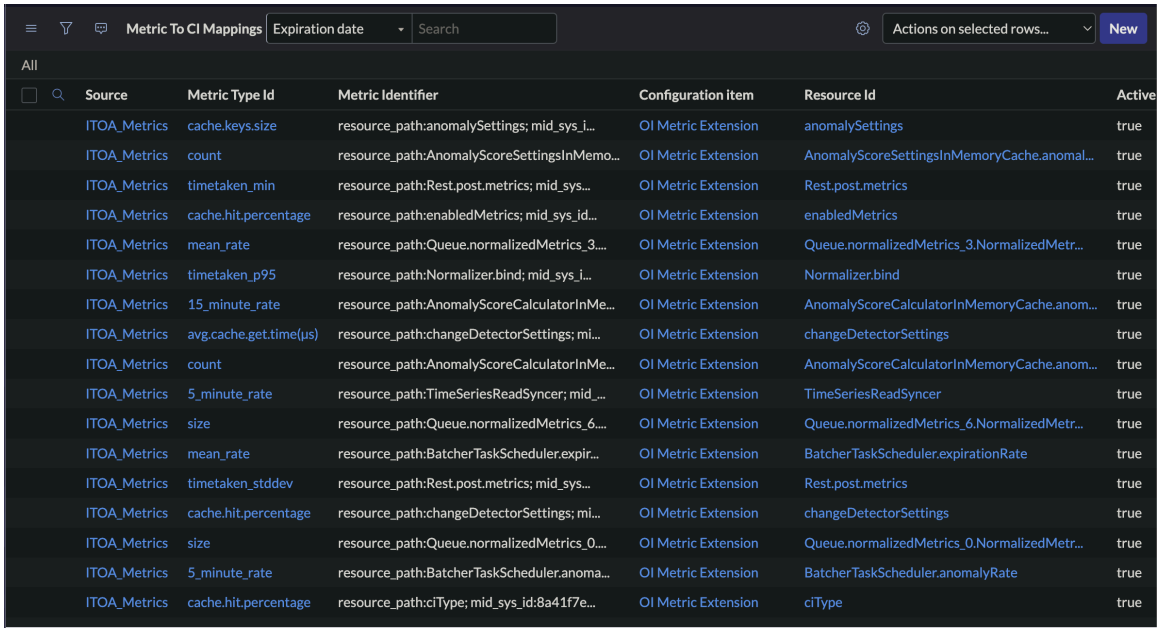
- `sa.metric.map.with.ci.expiration.sec`: Wenn die Zuordnung zum CI gefunden wurde. Standardmäßig auf eine Gültigkeitsdauer von fünf Tagen eingestellt.
- `sa.metric.map.without.ci.expiration.sec`: Wenn die Zuordnung zum CI nicht gefunden wurde. Standardmäßig auf eine Gültigkeitsdauer von 24 Stunden eingestellt.

Wenn ähnliche Metrikdaten innerhalb dieses Zeitraums eingehen, wird die vorhandene Zuordnung verwendet, um die Daten den CIs zuzuordnen. Am Ende des Zeitraums laufen Metrik-zu-CI-Datensätze ab. Außerdem führt eine Änderung der Ereignisregeln zum sofortigen Ablaufen der entsprechenden Metrik-zu-CI-Datensätze. Wenn Metrikrohdaten das nächste Mal eingehen, werden sie erneut normalisiert. Wenn Discovery CIs hinzufügt oder entfernt, werden die Zuordnungen so angepasst, dass diese Änderungen im nächsten Zyklus berücksichtigt werden.

Alle Informationen zur kürzlich vorhandenen Zuordnung werden in der Tabelle sa_metric_map in „Metrik zu CI“-Datensätzen gespeichert (siehe unten). Sie können auf die Tabelle „Metrik zu CI“ zugreifen, indem Sie zu **Alle > Event Management > Metriken > Metrik zu CI** navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Metrik zu CI“



Source	Metric Type Id	Metric Identifier	Configuration item	Resource Id	Active
ITOA_Metrics	cache.keys.size	resource_path:anomalySettings; mid_sys_i...	OI Metric Extension	anomalySettings	true
ITOA_Metrics	count	resource_path:AnomalyScoreSettingsInMemo...	OI Metric Extension	AnomalyScoreSettingsInMemoryCache.anomal...	true
ITOA_Metrics	timetaken_min	resource_path:Rest.post.metrics; mid_sys...	OI Metric Extension	Rest.post.metrics	true
ITOA_Metrics	cache.hit.percentage	resource_path:enabledMetrics; mid_sys_id...	OI Metric Extension	enabledMetrics	true
ITOA_Metrics	mean_rate	resource_path:Queue.normalizedMetrics_3....	OI Metric Extension	Queue.normalizedMetrics_3.NormalizedMetr...	true
ITOA_Metrics	timetaken_p95	resource_path:Normalizer.bind; mid_sys_i...	OI Metric Extension	Normalizer.bind	true
ITOA_Metrics	15_minute_rate	resource_path:AnomalyScoreCalculatorInMe...	OI Metric Extension	AnomalyScoreCalculatorInMemoryCache.anom...	true
ITOA_Metrics	avg.cache.get.time(µs)	resource_path:changeDetectorSettings; mi...	OI Metric Extension	changeDetectorSettings	true
ITOA_Metrics	count	resource_path:AnomalyScoreCalculatorInMe...	OI Metric Extension	AnomalyScoreCalculatorInMemoryCache.anom...	true
ITOA_Metrics	5_minute_rate	resource_path:TimeSeriesReadSyncer; mid_...	OI Metric Extension	TimeSeriesReadSyncer	true
ITOA_Metrics	size	resource_path:Queue.normalizedMetrics_6....	OI Metric Extension	Queue.normalizedMetrics_6.NormalizedMetr...	true
ITOA_Metrics	mean_rate	resource_path:BatcherTaskScheduler.expir...	OI Metric Extension	BatcherTaskScheduler.expirationRate	true
ITOA_Metrics	timetaken_stddev	resource_path:Rest.post.metrics; mid_sys...	OI Metric Extension	Rest.post.metrics	true
ITOA_Metrics	cache.hit.percentage	resource_path:changeDetectorSettings; mi...	OI Metric Extension	changeDetectorSettings	true
ITOA_Metrics	size	resource_path:Queue.normalizedMetrics_0....	OI Metric Extension	Queue.normalizedMetrics_0.NormalizedMetr...	true
ITOA_Metrics	5_minute_rate	resource_path:BatcherTaskScheduler.anoma...	OI Metric Extension	BatcherTaskScheduler.anomalyRate	true
ITOA_Metrics	cache.hit.percentage	resource_path:ciType; mid_sys_id:8a41f7e...	OI Metric Extension	ciType	true

Metrikbindung an Ressourcen

Binden Sie Metriken an Ressourcen, um die Bindung von Metrikereignissen zu vereinfachen, indem Sie zusätzlich zu CIs die Bindung an Ressourcen wie bestimmte Datenträger oder Webseiten aktivieren.

Metric Intelligence modelliert Metrikreihen mit einer der folgenden Methoden:

- Bindung einer Metrikreihe an ein CI und an die für dieses CI überwachte Metrik im Format „CI/Metrik“. Beispiel: „win_server_001/response_time_mean“.
- Bindung einer Metrikreihe an ein CI, eine Ressource innerhalb dieses CI und die für diese Ressource überwachte Metrik im Format „CI/Resource/Metrik“. Beispiel: „win_server_001/Disk — C/disk_usage“. Diese Methode wird als *`resource binding`* bezeichnet.

Die erste Methode ermöglicht das Modellieren, Speichern, Aggregieren und Abfragen von Daten auf CI-Level. Die Ressourcenbindung erstellt jedoch Ressourcendatensätze für bestimmte überwachte Entitäten wie einzelne Webseiten oder Datenträger. Daher ist die Ressourcenbindung effizienter, wenn mehrere Ressourcen ähnlichen Typs in einem CI vorhanden sind und Metriken, die für eine Kategorie dieser Ressourcen gelten, diesen Ressourcen zugeordnet werden.

Anwendungsfälle:

- Häufige Beispiele sind Laufwerke, Prozessoren und Netzwerkschnittstellen. In Fällen, in denen diese Entitäten überwacht werden, aber in der CMDB nicht vorhanden sind, ist die Verwendung von Ressourcen für die Metrikbindung hilfreich.
- Einige Überwachungslösungen erfassen Metrikdaten in Services wie KPIs für einzelne Webseiten in einer Anwendung. In solchen Fällen, in denen die überwachte Entität kein Konfigurationselement ist, kann die Metrikbindung an Ressourcen hilfreich sein.

In diesen Situationen führt die Verwendung der Ressourcenbindung zu aussagekräftigeren Zusammenfassungen für ähnliche Metriken (z. B. „avg disk_usage“ für einen Host auf allen Datenträgern).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenbindungsprozess

Der MID Server generiert Metrikbindungsereignisse, die von der Instanz verarbeitet werden. Bei der Verarbeitung eines Metrikbindungsereignisses wird versucht, das CI zu identifizieren, zu dem dieses Metrikbindungsereignis gehört. Wenn dieser Versuch erfolgreich ist, wird das Metrikbindungsereignis an das identifizierte CI gebunden und eine Bindung an eine Ressource wird versucht. Die folgenden Schritte beschreiben den Versuch, ein Metrikbindungsereignis an eine Ressource zu binden:

1. Identifizieren Sie die CI-Klasse des CI, das an das Metrikbindungsereignis gebunden wurde.
2. Ermitteln Sie die Ressourcenklasse, die dieser CI-Klasse zugeordnet ist (mithilfe der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class]).
3. Lesen Sie den Attributwert *resource_path* im Feld **additional_information** im Metrikbindungsereignis.
4. Überprüfen Sie, ob in der Ressourcenklassentabelle ein Ressourcendatensatz vorhanden ist, in dem *name* gleich *resource_path* und *cmdb_ci* gleich dem CI ist, das an das Metrikbindungsereignis gebunden wurde.
5. Wenn ein solcher Ressourcendatensatz vorhanden ist, wird das Metrikbindungsereignis an diese Ressource gebunden. Andernfalls wird ein neuer Ressourcendatensatz mit den vorherigen Werten erstellt und das Metrikbindungsereignis wird an die neu erstellte Ressource gebunden.

Ressourcenbindungen konfigurieren

- Stellen Sie sicher, dass sa.metric.use.resource.binding Systemeigenschaft ist auf „wahr“ festgelegt (Standard).
- Stellen Sie für Reihen, die an Ressourcen gebunden werden sollen, sicher, dass das Attribut *resource_path* ausgefüllt wird, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie eine Ereignisregel, um das Attribut *resource_path* dem Feld **Zusätzliche Informationen** in Ereignissen hinzuzufügen. Weitere Informationen finden Sie unter Erstellen einer Ereignisregel, um Metriken bestimmten CIs zuzuordnen.
  - Füllen Sie das Attribut *resource_path* als Teil des jeweiligen CI-Bezeichners aus, wenn Daten zur Verarbeitung an den MID Server gesendet werden.
- Überprüfen Sie die Standardzuordnungen in der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class], und passen Sie sie nach Bedarf an. Es ist wichtig, dass Zuordnungen vor der Datenverarbeitung wie gewünscht festgelegt werden.

  Zum Verwalten der Tabelle „CI-Typ zu Ressourcenklasse“ ist die Rolle „evt_mgmt_admin“ erforderlich.

Ressourcentabellen

Die Ressourcenbindung verwendet eine zugrunde liegende Hierarchiestruktur von Ressourcen, die eine Teilmenge der [cmdb_ci]-Hierarchie ist. Metric Intelligence installiert die folgenden Ressourcentabellen:

- CI-Ressource [ci_resource] (übergeordnete Tabelle):
- Tabellen, die die CI-Ressource [ci_resource] erweitern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ci_resource_hardware
- ci_resource_appl
- ci_resource_service
- ci_resource_vm_object
- ci_resource_database

CIs zu Ressourcen zuordnen

Zuordnungen von CI-Klassen zu Ressourcenklassen werden in der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class] gespeichert. Diese Tabelle wird mit Metric Intelligence installiert und während der Metrikbindung an Ressourcen verwendet.

Zuordnungen in der Tabelle „CI-Typ zu Ressourcenklasse“ (Standard)

CI-Klasse	Ressourcenklasse
cmdb_ci_hardware	ci_resource_hardware
cmdb_ci_appl	ci_resource_appl
cmdb_ci_service	ci_resource_service
cmdb_ci_database	ci_resource_database
cmdb_ci_vm_object	ci_resource_vm_object

Erstellen einer Ereignisregel, um Metriken bestimmten CIs zuzuordnen

Erstellen Sie Ereignisregeln, um eingehende Metrikrohdaten bestimmten CIs zuzuordnen, Metriknamen optional zu ändern und das Attribut `resource_path` für die Ressourcenbindung auszufüllen.

Das System generiert Ereignisse für alle neuen Metrikdaten, für die keine CI-Bindungsspezifikationen vorhanden sind. Sie können Ereignisregeln erstellen, die diese Ereignisse filtern, um die eingehenden Metrikdaten bestimmten CIs zuzuordnen. In solchen Ereignisregeln haben Sie z. B. die Möglichkeit zum Definieren eines Filters, der auf dem Überwachungsobjekt (z. B. SCOM) basiert.

Zur Verwendung der Ressourcenbindung muss das Attribut `resource_path` von Ereignissen ausgefüllt werden. Sie können eine Ereignisregel konfigurieren, um sicherzustellen, dass das Attribut `resource_path` dem Feld **Zusätzliche Informationen** in Ereignissen hinzugefügt wird. Weitere Informationen zum Konfigurieren und Verwenden der Ressourcenbindung finden Sie unter Ressourcenbindung.

Beispielsweise können Sie im Designer für Ereignisregeln die Ereignisregel **SCOM-IIS-Webserver** wie folgt aktualisieren:

- Definieren Sie auf der Registerkarte **Ereignisfilter** einen Filter, sodass nur IIS-Webserver zugeordnet werden.
- Legen Sie auf der Registerkarte **Bindung** für **Klasse** den Wert Microsoft IIS-Webserver fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Event-Regeln

Zuordnung zwischen Metriken und CI sowie Ressourcenbindung anzeigen

Erste Schritte mit Metrikdaten

CIs im Wartungsmodus

Konfigurieren Sie die Anomalie-Erkennung, um Metriken für CIs, die sich im Wartungsmodus befinden, vom Modelllernen auszuschließen.

Sie können die Einstellungen der Systemeigenschaften ändern, um Metrikdaten für CIs im Wartungsmodus ein- oder auszuschließen.

Wenn die Systemeigenschaft sa.model_learner.maint_event_record_history_enabled auf „true“ festgelegt ist (Standard), speichert Metric Intelligence Verlaufsinformationen über die Zeiten, zu denen CIs in den Wartungsmodus wechseln bzw. diesen verlassen. Wenn die Systemeigenschaft sa_metric.maint_exclusion auf „true“ festgelegt ist (Standard), werden Metriken von CIs, die sich im Wartungsmodus befinden, vom Modelllernen ausgeschlossen.

Anomaliemodelltests

Verwenden Sie Anomaliemodelltests zum Anwenden und Auswerten der Anomalie-Erkennung für einen kleinen Satz von CIs und Metriken unter Verwendung tatsächlicher Metrikdaten. Vergleichen Sie die Testergebnisse mit den erwarteten Ergebnissen, und optimieren Sie dann das Anomalie-Erkennungsmodell, bevor Sie die Anomalie-Erkennung für die getesteten CIs und Metriken in der Produktionsumgebung aktivieren.

Beispiel: Bevor Sie die Anomalie-Erkennung für Linux-Server aktivieren, können Sie Anomaliemodelltests mit tatsächlichen Metrikdaten verwenden, die für diese Linux-Server gesammelt wurden. Vorhandene Warnungen weisen möglicherweise auf eine Anomalie für eine bestimmte Metrik und ein bestimmtes CI hin. Sie können eine Anomalietestregel erstellen, um die Anomalie-Erkennung für diese CIs und Metriken zu testen und dann zu überprüfen, ob die erwartete Anomalie erkannt wird. Sie können auch die durch das Anomaliemodell berechneten Grenzen überprüfen, um festzustellen, ob sie den erwarteten Grenzen entsprechen. Nach der Feinabstimmung des Testmodells können Sie die Anomalie-Erkennung für Linux-Server aktivieren.

Anomaliemodelltests unterstützen bis zu 20 Zeitreihen, die 20 Metriktypen für dasselbe CI, denselben Metriktyp für 20 verschiedene CIs oder eine beliebige Kombination dieser Optionen enthalten können.

Testergebnisse im Explorer für Einblicke anzeigen

Nach Abschluss einer Testausführung wird eine URL für einen Explorer für Einblicke verfügbar. Die Testergebnisse des Anomaliemodells werden in dieser eingeschränkten Version des Explorers für Einblicke angezeigt. In diesem Explorer für Einblicke werden die Diagramme und Punktzahlen der in der Anomalietestregel angegebenen Metrikserien im Voraus geladen. Sie können diesem Explorer für Einblicke keine CMDB-Gruppen und Anwendungsservices hinzufügen.

Alle Diagramme im Explorer für Einblicke enthalten in den **Diagrammeinstellungen** den Abschnitt „Anomalieteststatistiken“. Dieser Abschnitt bezieht sich speziell auf Anomaliemodelltests und bietet die folgenden Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Grenzen anzeigen**: Zeigt die berechnete obere und untere Grenze für die Metrik in einem Anomaliemodelltest an, die auf dem Lernen vergangener Metrikwerte basiert. Die obere und die untere Grenze werden immer zusammen angezeigt.
- **Abweichende Punktzahlen anzeigen**: Zeigt abweichende Punktzahlen auf einer virtuellen Achse von 0–10 für einen Anomaliemodelltest an. Dabei basiert der Farbcode auf den Punktzahlschwellenwerten, die in der Tabelle der Zuordnung der Anomaliepunktzahl zum Event-Schweregrad [sa_metric_anomaly_score_to_event_severity_map] definiert sind.

Testergebnisse zum Optimieren der Anomalie-Erkennung verwenden

Beim Anomaliemodelltest werden die obere und die untere Grenze verwendet, die für die ausgewählte Serie in der Anomalietestregel konfiguriert sind. Die Ergebnisse des Anomaliemodelltests zeigen, wie viele Anomaliewarnungen basierend auf den angegebenen Einstellungen generiert worden wären, wenn die Anomalie-Erkennung für die getesteten CIs und Metriken aktiviert wäre. Anschließend können Sie entscheiden, ob dieses Ergebnis akzeptabel ist. Optimieren Sie die Grenzen so, dass die Anzahl der generierten Anomaliewarnungen nicht übermäßig, aber ausreichend ist, um eine Punktzahl außerhalb der Grenzen genau anzugeben.

Advanced Promotion Engine

Sie können eine Definition für erstellen Advanced Promotion Engine Damit Sie die Bedingungen für die Heraufstufung der Anomaliewarnungen in die Tabelle „alle Warnungen“ definieren können. Durch Heraufstufen der Warnungen, die die Bedingungen erfüllen, werden nur die relevantesten Anomaliewarnungen in die Tabelle verschoben.

Die Advanced Promotion Engine Verschiebt die relevantesten Warnungen aus der Liste der Anomaliewarnungen in die Tabelle alle Warnungen. Wenn eine Gruppe von Anomaliewarnungen für ein Konfigurationselement (Configuration Item, CI) die Bedingungen erfüllt, die Sie in der Definition festgelegt haben, die Sie für erstellt haben Advanced Promotion Engine, Der Gruppierungsmechanismus gruppiert die heraufgestuften Warnungen in der Tabelle „alle Warnungen“. Sie können beispielsweise eine Bedingung erstellen, die angibt, dass nur die Anomaliewarnungen, die zu einer bestimmten CI-Klasse mit dem Mindestschweregrad „schwerwiegend“ gehören, in die Tabelle „alle Warnungen“ heraufgestuft werden sollen.

Die Tabelle „alle Warnungen“ ist die Tabelle, die die Probleme enthält, die Ihre sofortige Aufmerksamkeit erfordern. Die Anomaliewarnungen für die verschiedenen Metriken innerhalb eines CI in einem bestimmten Zeitraum zeigen ein Problem an, das in die Tabelle „alle Warnungen“ hochgestuft werden muss.

Anomaliewarnungen weisen auf eine Abweichung von prognostizierten Metrikwerten für überwachte CIs hin. Details finden Sie unter Zeigen Sie Anomaliewarnungen an.

Die Advanced Promotion Engine Wird automatisch als Teil von aktiviert Metrikdaten Anwendung.

Sie können verwenden Advanced Promotion Engine Definitionen, die im Basissystem enthalten sind (für Linux Server und für Windows Server), oder Sie können Definitionen für die verschiedenen CI-Klassen erstellen. Die Basissystemdefinitionen geben an, dass die CIs auf der angegeben sind Linux Und Windows Server sind betriebsbereit, und die CIs mit dem Mindestschweregrad „schwerwiegend“ werden in die Tabelle „alle Warnungen“ heraufgestuft.

Alle Advanced Promotion Engine Aufgaben erfordern die Rolle evt_mgmt_admin. Mit der Rolle „evt_mgmt_user“ können Sie nur Definitionen und Eigenschaften anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metric Explorer

Metric Explorer bietet eine einfach zu bedienende Benutzeroberfläche, auf der Servicemitarbeiter die Integrität eines CI anzeigen können, das einer Warnung zugeordnet ist. Integritätsdetails für ein CI umfassen verschiedene Metrikdiagramme mit Kontrollgrenzen und Zusammenfassungen in einem Zeitraum.

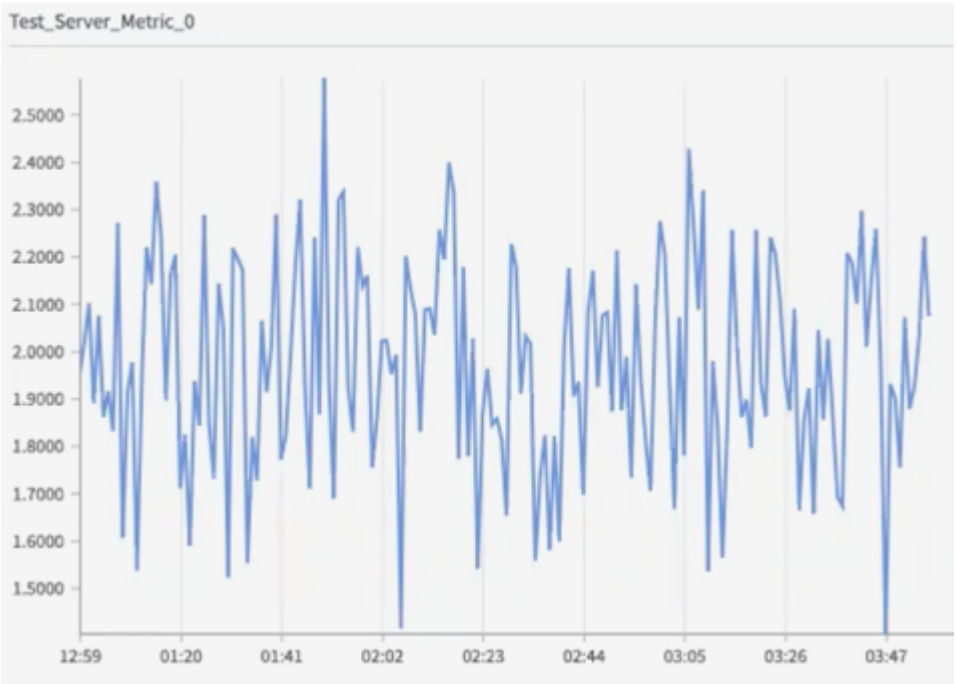
Der Satz von Metrikdiagrammen, die für eine CI-Klasse in angezeigt werden Metric Explorer Wird durch Metrikdiagrammkonfigurationen in der Tabelle „Metrik-Dashboard-Metadaten“ [sa_metric_Dashboard_metadata] bestimmt. Die Tabelle „Metadaten des Messgrößen-Dashboards“ wird anfänglich mit Konfigurationen für allgemeine Klassen und wichtigen Metriken für diese Klassen ausgefüllt. Ein Benutzer mit der Rolle admin oder evt_mgmt_admin kann die Standardkonfigurationen des Metrikdiagramms in der Tabelle „Metadaten des Messgrößen-Dashboards“ aktualisieren.

Es können jeweils bis zu 10 aktive Metrikdiagramme für eine Klasse konfiguriert werden.

Diagrammtypen

Ein Metrikdiagramm, das im Formular „Metrikdiagramme“ in Metric Explorer angezeigt wird, kann ein Diagramm vom Typ **Zeitreihe** oder **Einzelne Punktzahl** sein.

Zeitreihendiagramm



Der Zeitreihendiagrammtyp ist ein Diagramm aller Datenpunkte im angegebenen Zeitbereich für die Metriken des dem Diagramm zugeordneten CI. Zeitreihendiagramme ähneln Diagrammen im Explorer für Einblicke und enthalten je nach den Einstellungen eine obere oder untere Grenze.

Diagramm für einzelne Punktzahl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Diagrammtyp für einzelne Punktzahl zeigt eine einzelne Zahl an, die einer Zusammenfassung der Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms entspricht. Die Zusammenfassung ist ein Durchschnitt der Datenpunkte oder des Höchst-, Mindest- oder letzten Datenpunkts in der Zeitreihe.

Vorlagen

Die ITOM Service Operations-Arbeitsbereich Metric Explorer Die Vorlage ermöglicht das Drilldown von Metrikdiagrammen aus Dashboards für Digital Analytics (da) zum Metrik-Explorer. Weitere Informationen finden Sie unter Express-Listenübersicht Auf der ServiceNow® Entwicklerportal.

Eigensystemüberwachung für Metric Intelligence

Verwenden Sie Eigensystemüberwachungen von Ereignismanagement, um den allgemeinen Betriebszustand von Komponenten und Prozessen der Metric Intelligence-Infrastruktur zu überwachen und auf potenzielle Probleme aufmerksam zu machen. Die Selbstintegritätsüberwachung ermöglicht Ihnen, Probleme proaktiv zu beheben und Datenverluste zu minimieren.

Metric Intelligence ist für die Verwendung der Eigensystemüberwachung von Ereignismanagement vorkonfiguriert, um sicherzustellen, dass wichtige Komponenten und Prozesse ordnungsgemäß funktionieren. Wenn ein Monitor einen Fehler erkennt, erstellt die Selbstintegritätsüberwachung von Ereignismanagement ein Ereignis für das Problem. Diese Ereignisse werden dann in einen Ereignismanagement-Alarm umgewandelt oder an einen vorherigen Alarm angehängt. Die Eigensystemüberwachung von Metric Intelligence wird alle 60 Sekunden ausgeführt.

Wenn beispielsweise in einem verteilten Cluster mit einem Metric Intelligence-MID Server ein Problem auftritt, wird ein Event mit dem Status **Schwerwiegend** generiert. Anschließend wird dieses Ereignis in einen Alarm umgewandelt. Später, wenn das Problem gelöst wurde, wird ein neues Ereignis mit dem Status **Info** generiert, und die ursprüngliche Warnung wird geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachte Komponenten und Prozesse

Komponenten-/Prozessprüfung	Fehlerbedingung
Metric Intelligence-Erweiterung wird ordnungsgemäß ausgeführt	Der Monitor überprüft das *status*-Feld der *ecc_agent_ext_context_metric*-Tabelle, um einen **Fehler**- oder **Warnung**-Status zu erkennen.
Verteilter Cluster von Metric Intelligence-MID Servern wird ordnungsgemäß ausgeführt	Überwachung überprüft *status*Feld von *ecc_agent_cluster*Tabelle zum Erkennen eines Status **Fehler** , **Segmentiert** , Oder **Angehalten** . **Hinweis:** Für den Status **Gestoppt** wird nur dann ein Ereignis erstellt, wenn das Feld *error_message* nicht leer ist.
Metriken werden von aktiven Connectors erfasst, die für die Metriksammlung konfiguriert sind	Für jeden Connector, für den die Kennzeichnung *Metrics collection* auf **true** festgelegt ist: Der Monitor überprüft den Status des *last_kpi_status*-Felds der *em_connector_instance*-Tabelle, um einen **Fehler**-Status zu erkennen.
Wichtige regelmäßige Metric Intelligence-Aufgaben sind aktiv	Der Monitor überprüft die folgenden wesentlichen geplanten Aufträge, um festzustellen, ob einer davon inaktiv ist: • Metric Intelligence – Konfigurationsaufgabe für Metriken • Metric Intelligence – Tabellen mit MID synchronisieren • Metric Intelligence – Verteiltes MID-Cluster validieren

Weitere Informationen zum Aktivieren oder Deaktivieren einer Metric Intelligence-Eigensystemüberwachung finden Sie unter Eigensystemüberwachung konfigurieren.

Zugehörige Informationen

Eigensystemüberwachung für Ereignismanagement

Mit Metric Intelligence installierte regelmäßige Aufgaben

Domänentrennung und Metric Intelligence

Die Domänentrennung wird in Metrikdaten unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domänentrennung in Metrikdaten

Wenn Domänen in Metrikdaten getrennt sind, können Benutzer Warnungen und Ereignisse nur in ihrer eigenen (Mandanten-)Domäne anzeigen und verwalten. Nach Abschluss des Bindungsprozesses wird die Domäne des Configuration Item (CI) verwendet, damit Benutzer in dieser Domäne Metrikdaten untersuchen können. Es gibt eine Domänenspalte in Metrikdaten-Tabellen, die im Basissystem bereitgestellt werden. Die Domänenspalte zeigt den Namen der Domäne an, zu der das CI gehört.

Hinweis: Wenn die Domänenspalte nicht in der Liste angezeigt wird, klicken Sie auf (Liste personalisieren), und fügen Sie die erforderliche Spalte hinzu. Darüber hinaus können Sie eine Spalte hinzufügen, die den Domänenpfad anzeigt.

Die folgenden Funktionen von Metrikdaten unterstützen die Domain Separation nur eingeschränkt.

Funktion	Support
Metriktypen	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metriktypen für alle Domänen steuern.
Registrierung des Metriktyps	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metriktypregistrierung für alle Domänen steuern.
Metrikklasse	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metrikklassen, die für alle Domänen genutzt werden, steuern.
Regeln für Konfigurationseinstellungen	Auf globaler Ebene unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Support
	Der Instanzbesitzer kann die Regeln für die Konfigurationseinstellungen für alle Domänen steuern

Zugehörige Informationen

Domänentrennung für Service Provider

Metrikdaten konfigurieren

Planen und konfigurieren Sie Ihre Metrikdaten-Implementierung.

Konfiguration – Übersicht

Metrikdaten Die Konfiguration folgt normalerweise den folgenden Schritten:

1. Installieren Sie AIOps-Experience Plugin [sn_SOW_aiops].
2. MID-Server für Metrikdaten manuell konfigurieren.
3. Aktivieren Sie Metric Intelligence .
4. Streamen Sie Metriken über die relevante Datenquelle oder den entsprechenden Connector an die Instanz .
5. Zu überwachende Metriken auswählen und konfigurieren.
6. Stellen Sie sicher, dass Metriken ordnungsgemäß an CIs gebunden sind .
7. Konfigurieren Sie die Aktionsebene für die Anomalieerkennung.
8. Definieren Sie eine erweiterte Heraufstufungsregel, um die Bedingungen für die Heraufstufung einer Anomaliewarnung zu einer IT-Warnung zu bestimmen .

Erste Schritte mit Metrikdaten

Führen Sie die folgenden Setup- und ersten Konfigurationsschritte aus, um mit der Verwendung zu beginnen Metrikdaten.

Vorbereitungen

Aktivieren Sie Metrikdaten Plugin (com.snc.sa.metric).

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Metriken haben ein Ablaufdatum. Sie können weiterhin Daten ohne Unterbrechung empfangen, wenn das Ablaufdatum einer Metrik ansteht, indem Sie das Ablaufdatum entsprechend verschieben. Wenden Sie sich an den Kundensupport, um Einzelheiten zu erfahren.

Metrikdaten Das geführte Setup bietet eine Reihe von Aufgaben, mit denen Sie Metrik Intelligence in Ihrer ServiceNow-Instanz konfigurieren können. Zum Öffnen Metrikdaten Geführtes Setup, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**, Und klicken Sie auf **Fahren Sie Fort** . Scrollen Sie dann zu **Metric Intelligence**, und klicken Sie auf **Fortsetzen**. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Alternativ können Sie folgende Vorgehensweise verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Konfigurieren Sie ein MID-Server Für Metrikdaten.
   Weitere Informationen finden Sie unter MID-Server und verteilter MID-Server-Cluster für Metric Intelligence .
2. Verwenden Sie das Automatisiertes Setup von Metrikdaten.
3. Wählen Sie eine Quelle zum Sammeln von Metriken aus .
4. Zu überwachende Metriken auswählen und konfigurieren.
5. Erstellen Sie Ereignisregeln, um Rohmetrikdaten bestimmten CIs zuzuordnen Und Ereignisregel zum Binden von Metrikereignissen an Host-CIs erstellen.
6. Ungefähr 10 Minuten nach dem Start der Erweiterung „Metric Intelligence Metrics“ führen Sie die Schnellstarttests für Metric Intelligence durch, um die Funktionalität zu überprüfen.

Metrikdaten aktivieren

Metrikdaten Ermöglicht Ihnen das Erfassen, Erkunden und Analysieren von Betriebsmetrikdaten, Identifizieren und Anzeigen von Anomalien. Diese Analyse kann potenzielle Serviceausfälle verhindern.

Zeigen Sie an, und arbeiten Sie mit Metrikdaten Daten in Insight Explorer, Mitarbeiterbereich und Service Operations-Arbeitsbereich Schnittstellen.

Für Details zu den mit aktivierten Plugins Metrikdaten, Siehe Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Automatisiertes Setup von Metrikdaten

Beim ersten Setup von Metrikdaten können Sie viele Setupschritte automatisieren. Beispielsweise konfiguriert das automatisierte Setup einen MID-Server für Metrikdaten und erstellt einen verteilten MID-Server-Cluster, der diesen MID-Server enthält.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die folgenden Bedingungen erfüllt sind, wird im MID-Server-Formular der zugehörige Link **Metric Intelligence einrichten** angezeigt, um das automatisierte Setup zu ermöglichen:

- Der MID-Server wurde validiert.
- Der MID-Server wird ausgeführt.
- Die Eigenschaft *`sa.metric.display.mid.setup.action`* ist auf „true“ festgelegt (Standardwert).

Das automatisierte Setup für Metrikdaten führt die folgenden Setupaufgaben aus:

1. Es konfiguriert den MID-Server mit der Anwendung *`Operation Intelligence`*.
2. Es fügt dem MID Server die *`Metrics`*-Fähigkeit hinzu.
3. Es erstellt einen neuen MID-Server-Cluster vom Typ „Verteilt“ mit dem Standardport 47100 für Apache Ignite.
4. Es fügt den MID-Server dem neuen verteilten MID-Server-Cluster hinzu.
5. Es erstellt eine Erweiterung „Metrikdaten Metrics“ und startet sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Es öffnet das Formular „Metrikdaten Metrics Context“ (Metric Intelligence Metrics-Kontext). In diesem Formular können Sie auf die UI-Aktion **REST-Listener einrichten** klicken, um die MID Web Server-Erweiterung zu erstellen, die mit der Option „REST-Listener aktivieren“ und dem Standardport 8097 konfiguriert ist.

Wenn das automatische Setup fehlschlägt, können Sie einen erstellen MID-Server Cluster manuell verteilt, wie unter Verwenden von beschrieben **Richten Sie Metrik Intelligence Ein** Nur zum Erstellen des ersten verknüpfen MID-Server Verteilter Cluster, der eine einzelne enthält MID-Server, Mit Standardwerten. Nach Abschluss des automatisierten Setups müssen Sie zusätzliche manuell erstellen MID-Server Verteilte Cluster oder hinzufügen Metrikdaten MID Servers.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**an.
2. Wählen Sie aus MID-Server Die Sie als konfigurieren möchten Metrikdaten MID-Server.
3. Wählen Sie im MID-Server-Formular aus **Richten Sie Metrik Intelligence Ein** Im Abschnitt zugehörige Links.
4. In neu erstellt Metrikdaten Formular „Metrikerweiterung“:
   a. Warten Sie, bis der Statuswert ist **Gestartet** .
   b. Wenn konfiguriert wird MID-Server Wählen Sie zum Verschieben die UI-Aktion aus **Richten Sie DEN REST-Listener ein** .
   Es wird eine Benachrichtigung angezeigt, dass die MID-Server-Erweiterung erstellt wird. Das Feld **MID-Webservererweiterung** wird mit der ausgewählten Option **REST-Listener aktivieren** angezeigt. Sie können eine Vorschau von anzeigen MID-Server Erweiterungsdatensatz, um zu überprüfen, ob der Statuswert ist **Gestartet** .

Zugehörige Informationen

MID Server und verteilter MID Server-Cluster für Metric Intelligence

MID-Server für Metrikdaten manuell konfigurieren

Konfigurieren Sie zur Verwendung von Metrikdaten mindestens einen MID Server mit Metrikdaten als unterstützter Anwendung mit Metrikfunktionalität, der zudem die Erweiterung „Metrikdaten Metrics“ ausführt. Fügen Sie dann Metrikdaten MID-Server als Mitglied zu einem verteilten MID-Server-Cluster hinzu.

Vorbereitungen

Stellen Sie sicher, dass der MID-Server alle Software-, Hardware- und Konfigurationsanforderungen erfüllt, die für Metric Intelligence konfiguriert werden sollen.

Erforderliche Rolle: Für den Zugriff auf den MID-Server ist die Rolle mid_server erforderlich. Informationen zum Konfigurieren eines MID-Server in einer Instanz (z. B. zum Hinzufügen einer unterstützten Anwendung) finden Sie in der MID-Server-Dokumentation.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**an.
2. Klicken Sie auf den MID Server, den Sie für Metrikdaten konfigurieren möchten.
3. Fügen Sie die Anwendung Metrikdaten hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Mitte des MID-Serverformulars auf **Unterstützte Anwendungen**.

b. Klicken Sie im Abschnitt **Unterstützte Anwendungen** auf **Bearbeiten**.

c. Wählen Sie im Slushbucket das Element **OperationalIntelligence** aus, und klicken Sie auf die Hinzufügen-Schaltfläche **>**.

d. Klicken Sie auf **Speichern**.

4. Fügen Sie die Metrics-Fähigkeit hinzu:

a. Klicken Sie in der Mitte des MID-Server-Formulars auf **Funktionen**.

b. Klicken Sie im Abschnitt **Fähigkeiten** auf **Bearbeiten**.

c. Wählen Sie im Slushbucket **Metrics** aus, und klicken Sie auf die Hinzufügen-Schaltfläche „>“.

d. Klicken Sie auf **Speichern**.

5. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Erstellen Sie einen verteilten MID-Server-Cluster, und fügen Sie diesem Cluster den Metrikdaten MID-Server als Mitglied hinzu.

Konfigurieren Sie manuell Metrikdaten Erweiterung

Konfigurieren Sie MID-Server Metrikdaten Erweiterung zum Aktivieren von MID-Server Zum Abrufen von Rohmetriken aus externen Systemen, zum Erkennen von Anomalien und Melden von Anomalien zusammen mit Rohdaten an die Instanz. Dies MID-Server Metrikdaten Erweiterung ist erforderlich und muss ausgeführt werden, damit Ihr System erfassen kann Metrikdaten Daten.

Vorbereitungen

Unter Erste Schritte mit Metrikdaten finden Sie allgemeine Schritte zum Setup von Metrikdaten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die MID-Server Metrikdaten Die Erweiterung normalisiert die Rohdaten und überträgt die Daten dann an die Instanz. Wenn die Erweiterung Anomalien über einem angegebenen Schwellenwert erkannt hat, werden sie an die Instanz gesendet. Die Erweiterung wird ausgeführt, solange sie aktiviert ist. Dies stellt eine persistente Verbindung mit bereit MID-Server Um ständig auf Rohdaten zu hören Metrikdaten Daten aus externen Systemen.

Die MID-Server Metrikdaten Erweiterung:

- Empfängt Metrikrohdaten, fasst sie zu Stapeln zusammen und sendet sie in festgelegten Intervallen an die Instanz.
- Erkennt Anomalien und sendet einen Bericht an die Instanz.
- Die Informationen, die an die ServiceNow-Instanz gesendet werden, sind für relevant Metrikdaten, Damit die Datenverarbeitung effizient ist.

Die MID-Server Metrikdaten Die Erweiterung enthält keine API-Aufrufe. Wenn jedoch die Option **REST-Listener aktivieren** ausgewählt ist, fügt die Erweiterung einen Handler für die unterstützten REST APIs hinzu.

Hinweis:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nur bei der Konfiguration von Metrikdaten Erweiterung, die Metrikdaten MID Servers Treten Sie dem verteilten Cluster für tatsächlich bei Metrikdaten.
- Nach der Erstkonfiguration wird die erste Metrik nicht in die Metrikdaten aufgenommen.
- Beim Empfang von Metrikinformationen von der Synchronisierung der Instanz mit kommt es zu einer Verzögerung von einer Minute MID-Server.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Profile und Bereitstellungen** > **Metrikdaten**an.
2. In Metrikdaten Liste der Metrikkontexte klicken Sie auf **Neu** .
3. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Name	Ein eindeutiger Name für diese Erweiterung zur einfachen Identifizierung
Kurzbeschreibung	Eine Beschreibung dieser Erweiterung
Status	Dieses Feld wird automatisch mit dem Status der Erweiterung ausgefüllt. Das Feld ist leer, bis die Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die Erweiterung wird einer der folgenden Werte angezeigt: ○ **Gestartet**: Die Erweiterung wird ausgeführt. ○ **Gestoppt**: Die Erweiterung wird nicht ausgeführt. ○ **Offline**: Der MID-Server ist nicht erreichbar. ○ **Fehler**: Die Erweiterung ist mit einem Fehler fehlgeschlagen (die Fehlermeldung wird im Feld **Fehlermeldung**angezeigt). ○ **Warnung**: Eine Laufzeitausnahme ist aufgetreten. Die Erweiterung funktioniert weiterhin.
Fehlermeldung	Nachricht, die Fehler beschreibt, die dazu führen, dass Befehle wie **Starten** oder **Stoppen**fehlschlagen. Dieses Feld wird angezeigt, wenn das Feld **Status** den Wert **Fehler** hat oder wenn das Feld **Status** den Wert **Warnung** hat.
Ausführen auf	Ausführungsort dieser Erweiterung. Wenn Sie diese Option für die Verwendung mit konfigurieren Metrikdaten, Auf festgelegt **Bestimmter MID-Server** . Geben Sie dann an MID-Server Mit *`Operationalintelligence`*Als unterstützte Anwendung und *`Metrics`*Fähigkeit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Der Name des angegebenen MID-Server, Der mit konfiguriert ist `Operationalintelligence`Als unterstützte Anwendung und `Metrics`Fähigkeit.
Ausführung auf	[Schreibgeschützt] der Name des MID-Server Auf dem die Erweiterung ausgeführt wird. Dieses Feld zeigt den Namen des MID-Server an, auch wenn der MID-Server nicht erreichbar ist. Wenn der Benutzer die Erweiterung stoppt, ist dieses Feld leer.

4. Bei Verwendung der Push-Methode zum Sammeln Metrikdaten Daten, die MID-Server Metrikdaten Erweiterung muss mit konfiguriert werden **Aktivieren Sie DEN REST-Listener** Aktiviert. Diese Option aktiviert einen Listener, damit ein REST-Endpunkt Metrikrohdaten empfangen kann. Die Metrikrohdaten werden dann im regulären Datenfluss platziert, wo die Daten an die Instanz gesendet werden und der Anomaliedetektor nach Anomalien sucht. Wenn diese Option ausgewählt ist, wird dem Webserver ein Handler hinzugefügt, um nach Metriken zu hören, die an übertragen werden MID-Server. Wenn diese Option ausgewählt ist, die Webservererweiterung, die einen Webserver auf dem startet MID-Server, Muss ebenfalls konfiguriert werden. Weitere Informationen finden Sie unter MID-Webserver erweiterung konfigurieren.
5. Rechtsklicken Sie auf die Formularüberschrift, und wählen Sie **Speichern** aus.
6. Unter **Zugehörige Links** Klicken Sie auf **Starten** Um zu speichern Metrikdaten Daten in dieser Erweiterung, und starten Sie die Erweiterung.

In der Erweiterung „MID Server Metric Intelligence“ verfügbare Befehle

Zugehöriger Link	Beschreibung
Start	Startet die Erweiterung auf dem konfigurierten MID-Server Wenn es derzeit nicht ausgeführt wird.
Stoppen	Stoppt die ausgeführte Erweiterung auf dem konfigurierten MID-Server. Wenn die Erweiterung nicht läuft, wird keine Aktion ausgeführt.
Neu starten	Stoppt und startet dann die Erweiterung auf dem konfigurierten MID-Server.
Test	Der Test ist für nicht relevant Metrikdaten. Parameter werden bei Ausführung des **Tests** nicht getestet oder validiert.
Parameter aktualisieren	Sendet die zuletzt gespeicherten Parameter an die Erweiterung

Advanced Promotion Engine aktivieren

Bevor Sie verwenden können Advanced Promotion Engine Funktion, müssen Sie sie aus der Liste der Plugins aktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Aktivieren von `Var.Adv-promo-eng` , Sie müssen auch ein Plugin für ACC-M installieren, das das Metric Intelligence-Plugin enthält, wie in beschrieben Agent Client Collector-Überwachung erkunden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie ACC-M nicht verwenden möchten, installieren Sie nur das Plugin „Metrics Intelligence“, wie in beschrieben Erste Schritte mit Metrikdaten.

Prozedur

1. Navigieren zu **Systemdefinition** > **Plugins**an.
2. Suchen **Erweiterte Heraufstufungs-Engine** (id: sn_metric_Promote).
3. Wählen Sie den Eintrag aus, und überprüfen Sie die App-Details auf der **Engine Für Erweiterte Heraufstufung Der Store-Anwendung** Formular.
4. Wählen Sie Aus **Aktivieren/Upgrade Durchführen** Im Abschnitt zugehörige Links.
5. Wählen Sie **Aktivieren**.

Domänentrennung für Metric Intelligence konfigurieren

Konfigurieren Metrikdaten Für Domänentrennung zum Erstellen logisch definierter Domänen, die den nicht autorisierten Zugriff auf Daten einschränken.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

Prozedur

1. Aktivieren Sie das Plugin „Domain Support – Domain Extension Installer“.
2. Konfigurieren Sie den MID Server für Operational Intelligence als Benutzer, der zur gewünschten Domäne gehört, und dem die Rolle mid_server zugewiesen ist.
3. Konfigurieren Sie einen verteilten MID Server-Cluster in der gewünschten Domäne, und fügen Sie Operational Intelligence MID Server hinzu, die zur gleichen Domäne gehören.
   Weitere Informationen zum Einrichten von MID-Servern für Metrikdaten , Siehe MID Server und verteilter MID Server-Cluster für Metric Intelligence.

   Hinweis: Die Bindungsereignisse von Event Management werden mithilfe der Domäne des angemeldeten MID Server-Benutzers konfiguriert. Sobald der Prozess abgeschlossen ist, wird die Domäne des Datensatzes aktualisiert, um die Domäne aus dem CI zu verwenden, sodass jeder Benutzer in dieser Domäne die Metrikdaten sehen kann.

Wird Optimiert Metrikdaten

Sie können eine Vielzahl von Aufgaben ausführen, um Ihre Verwendung von zu optimieren Metrikdaten.

Anomalietestregel erstellen

Zur Verwendung von Anomaliemodelltests erstellen Sie eine Anomalietestregel, in der Sie bis zu 20 Metrikserien angeben, für die die Anomalie-Erkennung getestet werden soll. Führen Sie den Anomalietest aus, und verwenden Sie nach Abschluss die bereitgestellte URL, um den Explorer für Einblicke mit den Modelltestergebnissen zu laden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Anomaliemodelltests**an.
2. Wählen Sie eine vorhandene Anomalietestregel aus, die Sie bearbeiten und erneut ausführen möchten, oder klicken Sie auf **Neu**, und füllen Sie das Formular „Anomalietestregeln“ aus.

Feld	Beschreibung
Name	Name für die Modelltestregel
Betrifft	Die Tabelle, aus der CI/Metrik-Paare für die Modelltestregel ausgewählt werden. Hierfür wird die Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map] verwendet.
Regel	Filterbedingungen, um CI/Metrik-Paare für Anomaliemodelltests anzugeben. Ergibt die Regel mehr als 20 CI/Metrik-Paare, wird die Liste auf 20 Einträge beschränkt.
Startdatum/Enddaten	Der Zeitraum, für den die Anomalie-Erkennungstests angewendet werden sollen. Der Zeitraum muss innerhalb der letzten 7 Tage liegen.
Status	Der Status des Tests. Wird während der Ausführung von Testläufen automatisch vom System aktualisiert. Der Status lautet anfänglich „Geplant“ und wird schließlich in „Abgeschlossen“ geändert.
URL	URL zum Explorer für Einblicke, in dem die Ergebnisse des Anomaliemodelltests vorab geladen werden
Hinweise	Protokollierungszusammenfassung, die automatisch vom System mit Details zu jeder Testausführung der Anomalietestregel aktualisiert wird.

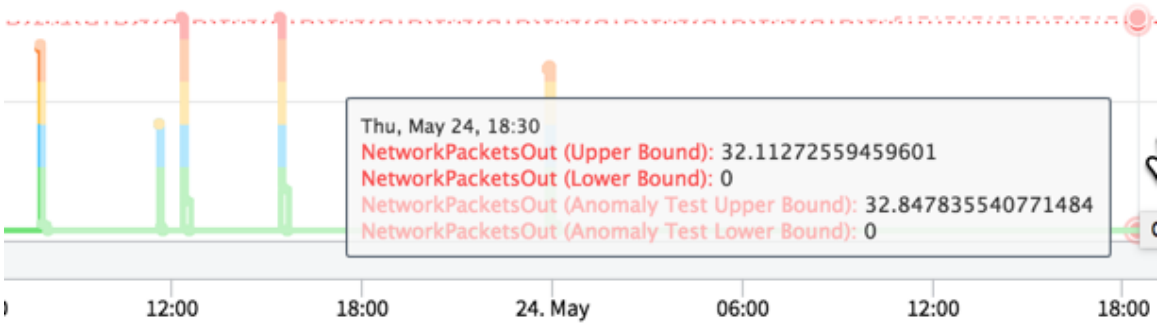
3. Klicken Sie auf **Anomalietest ausführen**.
   Während der Testausführung werden die Felder **Status**, **URL** und **Hinweise** automatisch aktualisiert, um den Fortschritt des Auftrags widerzuspiegeln.
4. Nachdem **Status** zu „Abgeschlossen“ geändert wurde, klicken Sie auf den **URL**-Link, um den Explorer für Einblicke mit den Testergebnissen zu öffnen.

Ergebnis

Die Grenzen und das Diagramm für den Anomaliemodelltest werden im Explorer für Einblicke in blassen Farben angezeigt. Außerdem wird für die obere und die untere Grenze, die durch den Test berechnet werden, ein Linienmuster verwendet, das sich von dem Linienmuster unterscheidet, das für tatsächliche Anomalie-Erkennungsergebnisse verwendet wird. Anhand dieser Unterschiede können Sie zwischen den Ergebnissen der tatsächlichen Anomalie-Erkennung und von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anomaliemodelltests unterscheiden, wenn beide in den Diagrammeinstellungen ausgewählt sind.



Nächste Maßnahme

- Ändern Sie den Datumsbereich für den Test, oder wählen Sie eine andere Zeitreihe aus, und klicken Sie erneut auf **Anomalietest ausführen**, um fortzufahren und das Modell zu optimieren.
- Klicken Sie auf das Symbol **Diagrammeinstellungen** für ein Diagramm, um zwischen der Anzeige von Statistiken und Zusammenfassungen im Diagramm umzuschalten. Wählen Sie in den Abschnitten mit den Anomalieteststatistiken und den Anomaliestatistiken die Optionen **Grenzen anzeigen** und **Abweichende Punktzahlen anzeigen** aus, um Testergebnisse neben den Ergebnissen der tatsächlichen Anomalie-Erkennung anzuzeigen.

  Hinweis: Die Ergebnisse von Anomaliemodelltests können den Ergebnissen der tatsächlichen Anomalie-Erkennung sehr ähnlich sein. Wenn Sie das Diagramm so konfigurieren, dass beide gleichzeitig angezeigt werden, ist es möglicherweise schwierig, Unterschiede zu erkennen, wenn Sie mit der Maus über das Diagramm fahren.

- Wenn Sie mit den Anomalietestergebnissen zufrieden sind, aktivieren Sie die Anomalie-Erkennung in der Produktionsumgebung für die im Test angegebenen Metriken und CIs. Unter Zu überwachende Metriken auswählen und konfigurieren finden Sie weitere Details.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen

Mit dem Assistenten für Grenzeneinstellungen können Sie gelernte Kontrollgrenzen außer Kraft setzen, indem Sie benutzerdefinierte Ober- und Untergrenzen für eine Metric Intelligence-Metrik festlegen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Metric Intelligence berechnet obere und untere **Kontrollgrenzen** für Metriken mithilfe von statistischen Modellen, die aus historischen Metrikdaten gelernt wurden. Die Ober- und Untergrenzen werden dann in der Analyse verwendet, um auffällige CIs oder Ressourcen zu erkennen, die sich auf die Anomaliepunktzahlen auswirken. Basierend auf historischen Daten können einige CIs, Ressourcen oder Metriken Werte aufweisen, über die Sie trotz der berechneten Bereiche ausdrücklich informiert werden möchten oder nicht. Beispielsweise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Versuch, eine SLA zu erfüllen, ohne dass eine Metrik einen bestimmten Wert zu lange über- oder unterschreiten darf, ohne darüber benachrichtigt zu werden. Wenn konkrete obere oder untere Grenzwerte für eine Metrik bekannt sind, können Sie diese Metrik mit benutzerdefinierten Grenzen konfigurieren, um die berechneten Grenzwerte außer Kraft zu setzen. Beispielsweise eine CPU-Metrik, die 85 % nicht überschreitet.

Mit dem Assistenten für Grenzeneinstellungen können Sie benutzerdefinierte statische Grenzen oder Grenzwertbereiche festlegen und eine Vorschau der Anomalieanalyse der tatsächlichen Daten basierend auf den benutzerdefinierten Einstellungen anzeigen. Der Assistent für Grenzeneinstellungen generiert automatisch die Metrikklasse und die Regel für die Konfigurationseinstellungen, mit denen benutzerdefinierte Grenzen verknüpft werden müssen.

Im Assistenten für Grenzeneinstellungen können Sie eine der folgenden Optionen für benutzerdefinierte Kontrollgrenzen auswählen:

Statische Ober- und Untergrenzen

Benutzerdefinierte statische Grenzwerte für die Ober- und Untergrenze werden als effektive Kontrollgrenzen verwendet, wobei die gelernten Werte für die Ober- und Untergrenze für die Metrik vollständig außer Kraft gesetzt werden. Der Mittelwert der Metrikdaten muss innerhalb des angegebenen Wertebereichs der statischen Grenzen liegen, andernfalls werden die statischen Grenzen nicht angewendet.

Wertebereiche für Unter- und Obergrenzen

Benutzerdefinierte Ober- und Untergrenzen, jeweils ausgedrückt als ein Wertebereich. Die geltenden Grenzen sind eine Kombination aus den benutzerdefinierten Minimal- und Maximalwerten, die den Grenzwertbereich definieren, und den erlernten oberen und unteren Grenzen:

- Wenn ein gelernter Grenzwert für einen Zeitpunkt innerhalb des benutzerdefinierten Wertebereichs der Ober- bzw. Untergrenze liegt, ist der gelernte Grenzwert wirksam.
- Wenn ein erlernter Grenzwert für einen Zeitpunkt außerhalb des benutzerdefinierten Wertebereichs liegt, gelten die **Max.**- bzw. **Min.**-Werte des benutzerdefinierten Bereichs. Wenn der erlernte Wert den benutzerdefinierten Bereich überschreitet, gilt der benutzerdefinierte **Max.**-Wert, und wenn er darunter liegt, gilt der benutzerdefinierte **Min.**-Wert.

Wenn ein metrischer Wert außerhalb einer Kontrollgrenze liegt, wird die Abweichung von der Kontrollgrenze durch einen **Breitenwert** normalisiert, den das System aus Daten berechnet. Die unteren und oberen Breitenwerte bestimmen, um wie viel ein Metrikwert die Kontrollgrenzen überschreiten muss, damit eine Anomalie vorliegt. Die Änderung einer Breite für die Kontrollgrenzen beeinflusst die Geschwindigkeit, mit der eine hohe Anomaliepunktzahl erreicht und über die Anomalie informiert wird. Neben der Einstellung benutzerdefinierter Kontrollgrenzen können Sie Breitenwerte außer Kraft setzen, indem Sie benutzerdefinierte Abweichungs- und Zeitwerte angeben, mit denen das System benutzerdefinierte Breitenwerte berechnet.

Das System speichert benutzerdefinierte Kontrollgrenzen und benutzerdefinierte Breiten für eine Metrik in einer **Metrikklasse**. Benutzerdefinierte Werte in einer Metrikklasse haben Vorrang vor den gelernten Grenzen und Breiten für die Metrik und werden dann in der nachfolgenden Anomalieanalyse verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Grenzwerteinstellungen**an.
2. Klicken Sie in der Listenansicht „Grenzeneinstellungen“ auf **Hinzufügen**, um den Assistenten für Grenzeneinstellungen zu öffnen.
3. Konfigurieren Sie auf der Registerkarte **Umfang auswählen** die folgenden Einstellungen, und klicken Sie dann auf **Weiter**.

Feld	Beschreibung
Quellmetriktypen	Quellmetriktyp, für den diese Grenzeneinstellung gilt. Wählen Sie ein Element aus der Dropdown-Liste und klicken Sie dann auf das Symbol „Quellenmetriktyp hinzufügen“ (**+**), um das ausgewählte Element zu **Ausgewählte Quellmetriktypen** hinzuzufügen.
Bereich	Umfang der CIs oder Ressourcen, für die diese Grenzeneinstellung gilt. Sie können für den Umfang **Alle CIs**, **Spezifisches CI oder spezifische Klasse**, **Bestimmte Ressourcen oder Ressourcenklassen**festlegen. Je nach Einstellung können Sie den Umfang dann weiter filtern.

4. Konfigurieren Sie auf der Registerkarte **Grenzeneinstellungen anwenden** die folgenden Einstellungen, und klicken Sie dann auf **Weiter**.

Feld	Beschreibung
Name der Grenzeneinstellungen	Eindeutiger Name für diese Grenzeneinstellung
Grenzentyp	Methode zur Angabe der benutzerdefinierten statischen Grenzen: ○ Statische Unter- und Obergrenzen festlegen ○ Wertebereiche für Ober- und Untergrenzen festlegen
Erweiterte Einstellungen anzeigen	Die folgenden Felder werden angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Wenn die untere Grenze** und **Der Metrikwert ist niedriger als die Untergrenze von** ○ **Wenn die obere Grenze** und **Der Metrikwert ist höher als die Obergrenze von** ○ **Kritischen Alarm nach der Dauer (Min.) senden** Geben Sie die Abweichung für ungewöhnliche Werte (in absoluten Werten) und die Dauer für das Senden einer Anomaliewarnung an. Diese Werte werden intern verwendet, um den Breitenwert für die Metrik zu berechnen. **Hinweis:** ○ Wenn die für die Grenzwerteinstellung angegebene Metrikklasse mit Werten für das Überschreiben der Breite aus einer aktualisierten Version konfiguriert ist, können Sie keine erweiterten Einstellungen festlegen. Um erweiterte Einstellungen festzulegen, akzeptieren Sie die angezeigten Benachrichtigung und erklären Sie sich damit einverstanden, dass diese Werte für das Überschreiben der Breite gelöscht werden. ○ Alle Felder müssen Werte enthalten. Wenn Sie keinen Metrikwert festlegen möchten, müssen Sie `0` entweder im Feld **Der Metrikwert ist niedriger als die Untergrenze von** oder im Feld **Und der Metrikwert liegt über der oberen Grenze von** eingeben. ○ Für die Mindestanzahl an Minuten können Sie den Wert `2` eingeben.
Untere Grenze	Statischer Wert der Untergrenze, der die gelernte Untergrenze für die Metrik ersetzt. Gilt für die Einstellung `Statische Ober- und Untergrenzen`.
Obere Grenze	Statischer Wert der Obergrenze, der die gelernte Obergrenze für die Metrik ersetzt. Gilt für die Einstellung `Statische Ober- und Untergrenzen`. Der Wert muss größer als der Wert für die **Untergrenze** sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wertebereich für die Untergrenze	**Min.** und **Max.** des benutzerdefinierten Wertebereichs der Untergrenze. Gilt für die Einstellung Wertebereiche für Ober- und Untergrenzen festlegen.
Wertebereich für die Obergrenze	**Min.** und **Max.** des benutzerdefinierten Wertebereichs der Obergrenze. Gilt für die Einstellung Wertebereiche für Ober- und Untergrenzen festlegen.

5. Auf der Registerkarte **Vorschau anzeigen und bestätigen**:

   a. Wählen Sie ein aus **Quellmetriktyp** .

   b. **Wahlweise:** Wählen Sie ein aus **Metriktyp** Für die Vorschau.

   c. **Wahlweise:** Geben Sie einen **CI-Namen** und einen **Ressourcennamen** ein, die Sie in die Vorschau aufnehmen möchten.
   Wenn Sie ein CI oder eine Ressource angeben, müssen sich diese innerhalb des zuvor angegebenen Umfangs befinden.

   d. Klicken Sie auf **Vorschau**, um eine Anomalie-Erkennung für die angegebene Metrik und das angegebene CI mithilfe der neu angegebenen benutzerdefinierten Grenzen durchzuführen.

   e. Überprüfen Sie die Vorschauergebnisse, und klicken Sie auf **Fertig stellen**, wenn die Ergebnisse den Erwartungen entsprechen.
   Andernfalls kehren Sie zur vorherigen Registerkarte **Grenzeneinstellungen anwenden** zurück, passen Sie die Einstellungen an, und führen Sie dann die Vorschau erneut aus. Die Vorschauergebnisse sind eine abgespeckte Version des Anomaliemodelltests. Weitere Informationen zu den Ergebnissen und zum Ändern von Diagrammeinstellungen finden Sie unter Anomaliemodelltests.

Zugehörige Informationen

Regel für Konfigurationseinstellungen erstellen

Zuordnung zwischen Metriken und CI sowie Ressourcenbindung anzeigen

Sie können die Ergebnisse der Bindungen zwischen Metriken und CIs bzw. Ressourcen anzeigen, einschließlich Details zu fehlgeschlagenen Bindungen, die Sie zur Eindämmung des Fehlers verwenden können. Wenn Metric Intelligence eine Metrik nicht zuordnen und nicht an ein CI oder eine Ressource binden kann, wird das CI bzw. die Ressource erst dann in der Anomalie-Erkennung berücksichtigt, wenn es bzw. sie ordnungsgemäß zugeordnet wurde.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Wenn die Ressourcenbindung nicht aktiviert ist, werden keine Ergebnisse zur Ressourcenbindung angezeigt.

Warum und wann dieser Vorgang ausgeführt wird

Metric Intelligence verwendet Event-Regeln, um Metrikdaten einem spezifischen CI oder einer Ressource zuzuordnen, das bzw. die mit dem Metrik-Event verbunden ist. Die Ergebnisse dieser Zuordnungen werden in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] gespeichert. Wenn die Zuordnung fehlschlägt, gibt der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bindungsstatus für die Metrik den allgemeinen Grund für den Fehler an, und weitere Details zum Fehler werden bereitgestellt. Untersuchen Sie die Details eines Zuordnungsfehlers und mindern Sie das Problem, um die genaue und effektive Verarbeitung der Metrikdaten zu verbessern.

- Wenn die Zuordnung zu einem CI erfolgreich ist, wird das zugeordnete CI in der Spalte **Configuration Item** angezeigt. Wenn die Ressourcenbindung versucht wurde, aber fehlgeschlagen ist, wird das zugeordnete CI nicht angezeigt, selbst wenn die Zuordnung zu einem CI erfolgreich war. Fehlende oder doppelte CIs können zum Fehlschlagen der CI-Zuordnung führen.
- Bei erfolgreicher Zuordnung zu einer Ressource wird die zugeordnete Ressource in der Spalte **Ressource** angezeigt. Fehlt eine Ressourcentabelle, die dem CI-Typ zugeordnet ist, an den das Event gebunden ist, oder fehlt ein *resource_path*-Attribut im Event, schlägt die Ressourcenbindung fehl.

Datensätze in der Tabelle „CI-Zuordnungen“ [sa_metric_map] bleiben 24 Stunden (standardmäßig, wenn die Zuordnung zum CI nicht erfolgreich ist) oder 5 Tage (standardmäßig, wenn die Zuordnung zum CI erfolgreich ist) gültig. Später, wenn innerhalb dieses Zeitraums Rohdaten für ein Metrik-CI-Paar ankommen, das bereits einen Datensatz hat, wird die vorhandene Zuordnung verwendet, um die Daten einem vorhandenen CI zuzuordnen. Nach dem Ablauf der Datensätze der Metrik-CI-Zuordnungen müssen die neu eingehenden Rohdaten neu zugeordnet werden. Diese Datensätze laufen ab, wenn:

- Der 24-Stunden- oder 5-Tage-Zyklus endet
- Sich eine Event-Regel geändert hat – dies löst ein sofortiges Ablaufen des jeweiligen Zuordnungsdatensatzes aus.

Das Anpassen von Zuordnungen an das Hinzufügen oder Entfernen von CIs durch Discovery wirkt sich erst ab dem Beginn des nächsten Zyklus aus.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**an.
   Die Seite **Metrik-Zuordnung an CIs** wird angezeigt.

Spalte	Beschreibung
Quelle	Datenquelle für die Metrik
Metriktyp-ID	Metrik, die für das CI gemessen wird, z. B. Datenträger% und CPU%
Metrik-Identifier	Eine Zeichenfolge in Form von CI/Ressource/Metrik, durch die ein CI und eine Metrik eindeutig identifiziert werden
Configuration Item	Das einer Metrik zugeordnete CI in der CMDB. Ein fehlender Wert bedeutet Folgendes: ○ Die Zuordnung der Metrik zu einem CI war nicht erfolgreich. ○ Die Ressourcenbindung ist aktiviert, jedoch fehlgeschlagen. **Configuration Item** fehlt, obwohl die Bindung an ein CI erfolgreich war.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Ressource	Die einer Metrik zugeordnete Ressource. Wenn die Ressourcenbindung aktiviert ist, deutet ein fehlender Wert darauf hin, dass die Zuordnung der Metrik zu einer Ressource nicht erfolgreich war.
Ablaufdatum	Ablaufdatum des Datensatzes
Aktionsebene der Anomalie-Erkennung	Die Ebene der Verarbeitung und Analyse der Erkennung von Anomalien, die auf CIs und Metriken angewendet wird. Verfügbare Optionen: ○ **Nur Metriken**: Die Metriken aus der Datenquelle werden nur erfasst, ohne sie weiter zu verarbeiten. ○ **Grenzen**: Beinhaltet die Verarbeitungsebene „Nur Metriken“. Zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt. ○ **Anomaliepunktzahlen**: Beinhaltet die Verarbeitungsebene „Grenzen“. Zusätzlich werden Anomaliepunktzahlen berechnet und angezeigt. ○ **Anomaliewarnungen**: Beinhaltet die Verarbeitungsebene „Anomaliepunktzahlen“. Zusätzlich werden gegebenenfalls Anomaliewarnungen erzeugt. ○ **IT-Warnungen**: Beinhaltet die Verarbeitungsebene „Anomaliewarnungen“. Zusätzlich werden gegebenenfalls IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.
Bindungsstatus	Status der Zuordnung der Metrik zu einem CI oder einer Ressource. Der Status **CI gefunden** gibt an, dass die Zuordnung erfolgreich war. In diesem Fall wird das zugeordnete CI in der Spalte **Configuration Item** angezeigt. Jeder andere Status gibt an, dass die Zuordnung fehlgeschlagen ist, und es wird ein allgemeiner Grund für den Fehler angegeben. Weitere Details zum Fehler finden Sie in der Spalte **Grund für Bindungsfehler**.
Grund für Bindungsfehler	Spezifische Details zur fehlgeschlagenen Zuordnung, z. B. Klassen- und Hostnamen und die verwendeten Abfragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Klicken Sie auf den entsprechenden **Event**-Link, um weitere Details im Feld **Verarbeitungsnotizen** anzuzeigen.

2. Überprüfen Sie ggf. den **Bindungsstatus** und den **Grund für den Bindungsfehler**.
   Lösen Sie das Problem anhand der angegebenen Details:

Bindungsstatus	Fehlerkorrektur
Host-CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden Host-CI aus.
Nicht-Host-CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden Nicht-Host-CI aus.
Nicht-Host-CI-Duplikat	Verwenden Sie Duplikat-CI-Nachbesserung Um die Duplizierung zu korrigieren.
Abhängiges CI-Duplikat	Verwenden Sie Duplikat-CI-Nachbesserung Um die Duplizierung zu korrigieren.
Abhängiges CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden abhängigen CI aus.
Doppelter Metrikzuordnungseintrag ist vorhanden	Überprüfen Sie **Grund für Bindungsfehler**, und vergleichen Sie die Metrikbezeichner, die den doppelten Metrikzuordnungseinträgen zugeordnet sind. Wenn sich Metrik-IDs geändert haben (z. B. wurde ein Bezeichner hinzugefügt), legen Sie den Eintrag für diese Reihe in der Tabelle „CI-Zuordnungen“ [sa_metric_map] so fest, dass sie ablaufen, oder löschen Sie den Eintrag. Überprüfen Sie auch die zugehörige Event-Regel und vergewissern Sie sich, dass sie die Attribute korrekt extrahiert und nicht die gleiche CI für zwei verschiedene Metrikbezeichner extrahiert. Dieser Fehler kann auftreten, wenn zwei verschiedene Metrik-IDs derselben CI/Metrik zugeordnet sind.
Ressourcen-ID nicht gefunden	Verifizieren Sie, dass die Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class] einen Zuordnungsdatensatz für den jeweiligen CI-Typ oder für einen seiner übergeordneten Typen enthält. Vergewissern Sie sich dann, dass es eine Tabelle mit dem Namen der Ressourcenklasse für diesen Datensatz gibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Gruppieren Sie den **Grund für den Bindungsfehler** nach dem **Bindungsstatus**, um eine Zusammenfassung mit der Anzahl der Datensätze pro Fehlerkategorie zu erstellen. Mit diesem Bericht können Sie die Probleme effizient beheben.

Zugehörige Informationen

Erstellen einer Ereignisregel, um Metriken bestimmten CIs zuzuordnen

Metrik für ein CI deaktivieren

Metric Intelligence kann so konfiguriert werden, dass erhebliche Datenmengen erfasst werden, von denen einige möglicherweise nicht erforderlich sind. Zur Optimierung der Leistung können Sie eine bestimmte Metrik für ein bestimmtes CI deaktivieren, um die Verarbeitung von Daten im Zusammenhang mit der angegebenen Metrik und dem CI zu beenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Die Einstellung `Active` („true“ oder „false“) für eine Quellenmetrik in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] hat Vorrang vor der Einstellung für die entsprechende Metrik in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map]. Wenn ein Quellmetriktyp in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] deaktiviert ist, werden alle Datensätze, die sich auf die entsprechenden Metriken beziehen, aus der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] entfernt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**an.
2. Suchen Sie den Datensatz für die Metrik bzw. das CI, die bzw. das Sie deaktivieren möchten, und legen Sie für die Spalte **Aktiv false** fest.

Event-Sammlung deaktivieren

Aus leistungstechnischen Gründen ist es vielleicht sinnvoll, die Erfassung von Ereignissen aus einer Datenquelle, aus der auch metrische Daten erfasst werden, zu deaktivieren. Sie können die Event-Sammlung für Datenquellen wie Nagios XI-Server, SolarWinds-Überwachungssystem und Zabbix-Server deaktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Um die Event-Sammlung nach der Deaktivierung wieder zu starten, müssen Sie das Originalskript des Connector wiederherstellen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**an.
2. Wählen Sie eine Connector-Instanz für die Datenquelle aus, für die die Event-Sammlung deaktiviert werden soll.
   Wählen Sie beispielsweise eine Connector-Instanz für Nagios, SolarWinds oder Zabbix aus.
3. Legen Sie einen hohen Wert für **Zeitplan für Eventsammlung (Sekunden)** fest, z. B. 20.000.000.
   Diese Einstellung vermeidet unnötige eine Kommunikation mit MID Server und optimiert die Leistung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.
5. Navigieren zu **MID-Server** > **Skripteinbindungen** Und erweitern Sie das Skript des Connectors (z. B. *NagiosMetrics_JS*, *SolarWindsJS*, Oder *ZabbixJS*) Durch Überschreiben von *execute*Methode. Fügen Sie ein Code-Snippet wie das Folgende hinzu, und klicken Sie dann auf **Aktualisieren**:

Example: Snippet für Nagios

```
var NagiosJSCustom = Class.create();

// Extending Nagios default script
NagiosJSCustom.prototype = Object.extendsObject(NagiosJS, {

// Override execute method
                execute: function() {
      var retVal = {};
      retVal['status'] = SUCCESS.toString();
     retVal['error_message'] = "Disabled by custom Class, 'Last event collection status'
 will be 'error' and this is normal. To achieve success status, enable event pull in custom
 class(NagiosJSCustom)";

      return retVal;
  });
```

Für den SolarWinds-Connector verwenden Sie:

```
var SolarWindsJSCustom = Class.create();

// Extending solarwinds default script
SolarWindsJSCustom.prototype = Object.extendsObject(SolarWindsJS, {
```

Für den Zabbix-Connector verwenden Sie:

```
var ZabbixJSCustom = Class.create();

// Extending zabbix default script
ZabbixJSCustom.prototype = Object.extendsObject(ZabbixJS, {
```

Schwellenwerte für Anomaliepunktzahlen konfigurieren

Metric Intelligence ordnet Anomalien eine Punktzahl zwischen 0 und 10 zu. Dieser Bereich ist in die fünf Stufen des Schweregrades von Ereignissen unterteilt, die im Explorer für Einblicke und in der Anomaliezuordnung jeweils durch eine andere Farbe dargestellt werden. Sie können den Schwellenwert für die Anomaliepunktzahl für jede Schweregradstufe konfigurieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Schwellenwerte für die Anomaliepunktzahl sind in der Tabelle „Zuordnung der Anomaliepunktzahl an den Event-Schweregrad“ [sa_metric_anomaly_score_to_event_severity_map] definiert. Beispielsweise haben Anomaliepunktzahlen von 8 bis 9 standardmäßig den Schweregrad 2 (Schwerwiegend) und werden im Explorer für Einblicke und in der Anomaliezuordnung dunkelorange angezeigt.

Informationen zu den Ereignisschweregraden, denen jede Zahl entspricht, finden Sie unter Ereignisschweregrade.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Zuordnung der Anomaliepunktzahl zu Schweregrad**an.
2. Doppelklicken Sie in der Listenansicht **Zuordnung der Anomaliepunktzahl der Metrik an Event-Schweregrad** auf den Event-Schweregrad, den Sie ändern möchten.
3. Ändern Sie den Wertebereich der Anomaliepunktzahlen, die dem jeweiligen Event-Schweregrad zugeordnet sind.
4. Klicken Sie auf **Aktualisieren**.

Zeigen Sie Anomaliewarnungen an

Anomaliewarnungen weisen auf eine Abweichung von den projizierten Metrikwerten für überwachte CIs hin. Anomaliewarnungen sind von den regulären IT-Warnungen getrennt und werden nicht im Service Operations-Arbeitsbereich angezeigt. Sie können eine Heraufstufungsregel für Anomaliewarnungen definieren, um eine IT-Warnung zu generieren, die auf Anomaliewarnungen basiert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Das statistische Modell wird verwendet, um Standardabweichungen, die obere und die untere Grenze sowie statistische Ausreißer zu berechnen, die dann zum Erkennen von Anomalien verwendet werden. Eine Anomalie tritt auf, wenn Metrikwerte außerhalb der prognostizierten Werte gemäß dem statistischen Modell liegen. Das System überwacht die Häufigkeit und Beständigkeit von statistischen Ausreißern im Zeitverlauf, um eine Punktzahl zwischen 0 und 10 zu berechnen, die angibt, wie anomal eine Abweichung ist.

Metrikdaten Generiert ständig Anomaliewarnungen, wenn die Anomaliepunktzahl über null liegt. Wenn eine Punktzahl über vier vorhanden ist und sich gegenüber der vorherigen Punktzahl geändert hat, wird sie an die Instanz gesendet. Auf der Instanz kann dann die gesamte Sequenz von Anomaliepunktzahlen im Zeitverlauf im Explorer für Einblicke angezeigt werden.

MetrikdatenÜberwacht Verlaufsdaten, um sicherzustellen, dass Metrikgrenzen genau sind und dass die Warnungen geschlossen werden, wenn das anomale Verhalten beendet wird. Metrikdaten Ignoriert auch irrelevante Anomalien basierend auf den Bezeichnungen der Metrik. Wenn beispielsweise die verfügbare CPU von ihrem oberen Grenzwert von 50 % auf 60 % ansteigt, wird die verwendet `available`Die Bezeichnung wird als Indikator identifiziert, dass das Verhalten nicht als Anomalie registriert werden sollte. Dies liegt daran, dass die Erhöhung der verfügbaren CPU ein positives Ergebnis darstellt, auch wenn die Metrik von 60 % andernfalls eine Anomalie darstellen würde.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Anomaliewarnungen**an.
2. Doppelklicken Sie in der Listenansicht **Alarm-Anomalien** auf den Alarm, den Sie anzeigen möchten. Informationen zu einer Anomaliewarnung umfassen Details wie Metrikwert, Heraufstufungsparameter, für die Warnung relevante Ereignisse (die in den Arbeitsnotizen für die Warnung angezeigt werden) sowie die obere und die untere Grenze (Untergrenzen dürfen nicht kleiner als 0 sein). Die Beschreibung enthält Details dazu, warum die Anomaliewarnung generiert wurde, und andere Details wie den Metriknamen und die Anomaliepunktzahl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Erstellen Sie einen Advanced Promotion Engine Definition, um die Bedingungen zu definieren, die erfüllt sein müssen, um Anomaliewarnungen zu IT-Warnungen heraufzustufen. Details finden Sie unter Erstellen Sie eine Definition für Advanced Promotion Engine.

Metrikwerte im Explorer für Einblicke anzeigen

Metric Intelligence berechnet Statistiken für CI-Metrikdaten. Der Explorer für Einblicke zeigt diese Metrikwerte als Metrikdiagramme für die CIs in der CMDB an. Mit dem Explorer für Einblicke können Sie Metriken für beliebige CIs in einem einzelnen Diagramm überlappen, um eine mehrschichtige Ansicht von Metrikwerten über einen Zeitbereich zu erstellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

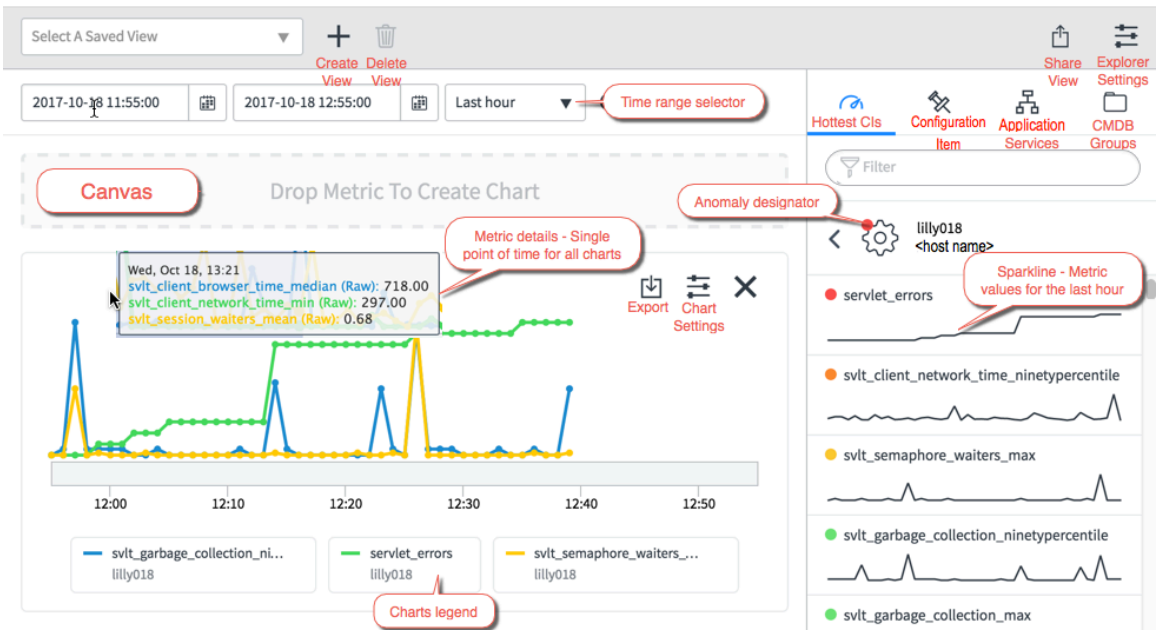
Der Explorer für Einblicke bietet eine Canvas, auf die Sie verschiedene Metriken für CIs ziehen und auf der Sie Diagramme erstellen können. Sie können eine einzelne Metrik auf der Canvas für eine einzelne Metrik für ein CI platzieren. Für ein umfassenderes Diagramm können Sie mehrere Metriken für ein einzelnes CI oder für verschiedene CIs übereinander legen, um ein Diagramm mit mehreren Metriken zu erstellen. In einem solchen Diagramm mit Ebenen wird jede Metrik durch eine eindeutige Farbe unterschieden, sodass Sie Metrikwerte über CIs innerhalb eines bestimmten Zeitbereichs vergleichen können.

Der Explorer für Einblicke zeigt Metrikgrenzen entsprechend dem zuletzt konfigurierten Modell an. Daher können Legacy-Anomalien aus einem vorherigen Build weiterhin als Anomalien angezeigt werden, auch wenn die Warnung gemäß den aktuellen Grenzen nicht als Anomalie qualifiziert ist.

Sie können den Explorer für Einblicke auch über die folgenden Zuordnungen aufrufen:

- Zeigen Sie Metriken in einer Abhängigkeitsansichtszuordnung an
- Zeigen Sie Metriken aus einer Business-Service-Zuordnung an

Explorer für Einblicke



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Hostname des CI verfügbar ist, wird er unter dem CI-Namen angezeigt. Der Hostname wird ausgefüllt, indem die Knoteninformationen aus dem generierten Bindungsereignis als Teil der Metrikbindung abgerufen werden.

So navigieren Sie zu einem CI, für das Metriken angezeigt werden sollen:

- Verwenden Sie „Heißeste Configuration Items“ ( ), um schnell auf die 10 anomalsten CIs zuzugreifen.
- Verwenden Sie „Configuration Items“ ( ), um eine separate benutzerdefinierte Liste aller CIs aus der CMDB zu erstellen und dann die Metriken für diese CIs der Canvas hinzuzufügen.
- Anwendungsservices verwenden ( ), um eine anwenderdefinierte Liste von Anwendungsservices zu erstellen, mit denen Sie Detailinformationen zu den CIs dieser Services anzeigen können. Anschließend können Sie der Canvas Metriken für diese CIs hinzufügen.
- Verwenden Sie „CMDB-Gruppen“ ( ), um eine benutzerdefinierte Liste von CMDB-Gruppen zu erstellen, mit der Sie Detailinformationen der CIs dieser Gruppen anzeigen können. Anschließend können Sie der Canvas Metriken für diese CIs hinzufügen.

Die folgenden Farben, die auf Farbeinstellungen für Warnungsschweregrade basieren, geben Anomalieschweregrade an:

Rot

Schweregrad „Kritisch“ (höchster Schweregrad)

Orange

Schweregrad „Schwerwiegend“

Gelb

Schweregrad „Gering“

Blau

Schweregrad „Warnung“ (niedrigster Schweregrad)

Grün

Informativ. Kein Schweregrad

Die Punkte oben links auf den CI-Symbolen zeigen den allgemeinen Nachverfolgungsstatus für Anomalien an:

- Grau: Metriken werden für das CI nachverfolgt, aber bei keiner dieser Metriken ist jemals eine Anomalie aufgetreten.
- Grün: Metrik für CI hatte mindestens eine Anomalie in der Vergangenheit, aber die Anomaliepunktzahl ist derzeit 0.
- Farbig: Entspricht dem zuletzt aufgezeichneten Schweregrad gemäß der Konfiguration der Farbbandbereiche.
- Kein Punkt: Es gibt keine Metriken für das CI und es sind keine Daten vorhanden, für die eine Anzeige der Detailinformationen ausgeführt werden kann.

Hinweis: **Configuration Items** und **Anwendungsservices** enthalten wahrscheinlich CIs, für die keine Metrikdaten vorhanden sind.

Metric Intelligence verfolgt keine Änderungen an einer Anomaliepunktzahl nach, wenn sie sich im grünen Bandbereich befindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beim Erstellen von Diagrammen wird automatisch eine Legende für jedes Seriendiagramm unter dem Diagramm angezeigt. Bei einem Diagramm mit einer Metrik enthält die Legende Einträge für die Zusammenfassungen im Diagramm. Bei einem Diagramm mit mehreren Metriken enthält die Legende Einträge für die Metriken in dem Diagramm.

Änderungen im Explorer für Einblicke bleiben während der Sitzung erhalten, sobald der Explorer für Einblicke aktualisiert wird, kehrt er jedoch in seinen Ausgangszustand zurück.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Explorer für Einblicke**an.
2. Klicken Sie auf ein CI, um Detailinformationen zur zugehörigen Liste von Metriken anzuzeigen, geordnet nach den neuesten Anomaliepunktzahlen.

   Für jede Metrik werden in einer Sparkline Metrikwerte für das CI für die letzte Stunde angezeigt. Zeigen Sie auf die Sparkline, um den Metrikwert zu jedem Zeitpunkt anzuzeigen.

   Wenn Ressourcenbindung aktiviert ist, enthält die Liste der für ein CI überwachten Reihen auch Reihen, die zu einer Ressource und Metrik gehören. Die Benennungskonvention für solche Reihen lautet „<Ressourcenname>/<Metrikname>“. Für eine Reihe, die nur an ein CI gebunden ist, lautet die Benennungskonvention „<Metrikname>“.
3. Ziehen Sie eine Metrik in die **Metrik Ablegen, Um Diagramm Zu Erstellen** Bereich auf der Canvas, und zeigen Sie auf das Diagramm, um den genauen Metrikwert zu jedem Zeitpunkt anzuzeigen.
   Das Metrikdiagramm zeigt Daten für den angegebenen Zeitraum gemäß den Diagrammeinstellungen an. Standardmäßig werden Rohdaten angezeigt. Wenn der Zeitraum länger als eine Woche ist oder vor der vergangenen Woche liegt, werden Durchschnittsdaten angezeigt. Ziehen Sie die nachfolgende Metrik wie folgt auf die Canvas:
   - In den Bereich **Metrik zum Erstellen von Diagramm ablegen**, damit sie einzeln in einem neuen Diagramm angezeigt wird.
   - Auf ein vorhandenes Diagramm im hervorgehobenen Block **Diagramm ersetzen**, um das vorhandene Diagramm zu überschreiben.
   - Auf ein vorhandenes Diagramm im hervorgehobenen Block **Metrik hinzufügen**, um sie mit den im Diagramm vorhandenen Metriken zu überlappen.

     Wenn Sie mehrere Metriken in einem einzelnen Diagramm anzeigen, gilt dieselbe Zusammenfassungsauswahl für alle Metriken und die Statistikeinstellungen sind nicht verfügbar. Wenn beispielsweise **Durchschnitt** in den **Diagrammeinstellungen** ausgewählt ist, werden Durchschnittswerte für alle Metriken im Diagramm angezeigt.
4. Verwenden Sie **Suchen** Feld zum Suchen und Filtern nach bestimmten Konfigurationselementen, Anwendungsservices oder CMDB-Gruppen, die standardmäßig nicht aufgeführt sind.
   Klicken Sie im Abschnitt SUCHERGEBNISSE auf das +-Symbol neben dem Element, das Sie dem Abschnitt HINZUGEFÜGTE ELEMENTE hinzufügen möchten. Oder verwenden Sie die erweiterte Suche:
   - Wählen Sie aus, und klicken Sie dann auf **Configuration Item hinzufügen**, um bestimmte CIs hinzuzufügen. Wählen Sie im Dialogfeld „Konfigurationselemente hinzufügen“ einen **CI-Klassentyp** wie „Linux-Server“ aus.
   - Wählen Sie Aus Und klicken Sie dann auf **Fügen Sie Anwendungsservice Hinzu** Zum Hinzufügen aller CIs, die in einem bestimmten Anwendungsservice enthalten sind. Wählen Sie im Dialogfeld Anwendungsservices hinzufügen die Option aus Erkannter Service Oder Manueller Service Als **CI-Klassentyp** Und geben Sie dann Filterbedingungen an, um die Suche einzugrenzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können Anwendungsservices nur hinzufügen, wenn dies der Fall ist `Operational Status`Ist „betriebsbereit“.

- Wählen Sie aus, und klicken Sie dann auf **CMDB-Gruppe hinzufügen**, um alle CIs hinzuzufügen, die in einer angegebenen CMDB-Gruppe enthalten sind. Geben Sie im Dialogfeld „CMDB-Gruppen“ Filterbedingungen wie **[Gruppenname] [beginnt mit] [d]** an, um die Suche einzugrenzen.

Nachdem Sie die Elemente ausgewählt haben, die Sie hinzufügen möchten, klicken Sie auf **Hinzufügen**.

5. Fügen Sie die zugehörigen CIs hinzu:

   a. Klicken Sie auf das Symbol **Zugehörige CIs hinzufügen** ( ) neben einem CI.
   Das Dialogfeld „Zugehörige Configuration Items hinzufügen“ wird mit allen Beziehungen angezeigt, in denen das ausgewählte CI ein übergeordnetes oder untergeordnetes Element ist.

   b. Um die Liste weiter zu filtern, können Sie bestimmte Bedingungen definieren, die erfüllt werden müssen.

   c. Wählen Sie die Beziehungen aus, aus denen Sie das übergeordnete oder untergeordnete CI hinzufügen möchten, je nachdem, welches nicht das ausgewählte CI ist.

   d. Klicken Sie auf **Hinzufügen**.

   Die CIs aus den ausgewählten Beziehungen, die nicht dem ausgewählten CI entsprechen, werden der Liste der CIs im Explorer für Einblicke hinzugefügt.

6. Zeigen Sie auf ein Legendenelement, und klicken Sie auf das **X**-Symbol, um die entsprechende Metrik aus dem Diagramm zu entfernen oder die entsprechende Zeile in den **Diagrammeinstellungen** zu deaktivieren.
7. Klicken Sie auf das Zahnradsymbol **Einstellungen**, um die Anwendungseinstellungen zu öffnen:
   - Aktivieren oder deaktivieren Sie die Aktualisierung von Anomaliedaten im Explorer für Einblicke bzw. legen Sie die Häufigkeit dafür fest.
   - Aktivieren oder deaktivieren Sie die Anzeige zugehöriger Listen wie „Alle Warnungen“, „Incidents“ und „Probleme“. Weitere Informationen finden Sie unter Kartenindikatoren erstellen oder ändern .
8. Klicken Sie auf das Symbol **Diagrammeinstellungen**, um zwischen der Anzeige von Statistiken und Zusammenfassungen im Diagramm umzuschalten.
   Durch Aktivieren oder Deaktivieren eines Elements zum Hinzufügen oder Entfernen von Metriken aus einem Diagramm wird auch die Legende des Diagramms aktualisiert, um die Änderung widerzuspiegeln.

Diagrammeinstellung	Beschreibung
Grenzen anzeigen	Zeigt die berechnete obere und untere Grenze für die Metrik an, die auf dem Lernen vergangener Metrikwerte basiert. Die obere und die untere Grenze werden immer zusammen angezeigt.
Abweichende Punktzahlen anzeigen	Zeigt Anomaliepunktzahlen auf einer virtuellen Achse von 0–10 an. Dabei basiert der Farbcode auf den Punktzahlschwellenwerten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammeinstellung	Beschreibung
	die in der Tabelle der Zuordnung der Anomaliepunktzahl zum Event-Schweregrad [sa_metric_anomaly_score_to_event_severity_map] definiert sind.
Durchschnitt	Zeigt zusammengefasste durchschnittliche Metrikwerte an, die in Intervallen von einer Stunde berechnet werden. Zusammengefasste Durchschnittswerte werden wie folgt angezeigt: ○ Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an. ○ Für Daten, die bis zu 94 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an. ○ Für ältere Daten: Zeigt Zusammenfassungsfenster von 1 Stunde an.
Minimum	Zeigt zusammengefasste minimale Metrikwerte an, die pro Stunde berechnet werden. Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an.
Maximum	Zeigt zusammengefasste maximale Metrikwerte an, die pro Stunde berechnet werden. Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an.
Roh	Zeigt die rohen, nicht zusammengefassten Metrikwerte an. Diese Werte werden nur für die letzten 8 Tage gespeichert.

Nächste Maßnahme

- Zeigen Sie auf das Symbol eines CI in der rechten Leiste, um den CI-Typ anzuzeigen.
- Vergrößern oder verkleinern Sie die Ansicht, indem Sie die Standardauswahl **Letzte Stunde** für den Zeitbereich ändern. Wählen Sie einen der voreingestellten Zeiträume aus, um beispielsweise Anomaliepunktzahlen für die letzten **6 Stunden** anzuzeigen, oder geben Sie einen benutzerdefinierten Zeitraum für die letzten maximal 90 Tage an.

  Um die Anzeige zu vergrößern, markieren Sie einen Diagrammbereich, indem Sie auf die linke obere Ecke des Abschnitts zeigen und die Maus in die rechte untere Ecke des Abschnitts ziehen. Der Zeitbereich des Diagramms wird entsprechend geändert. Wenn sich auf der Canvas weitere Diagramme befinden, werden alle automatisch synchronisiert, um Daten für denselben Zeitbereich anzuzeigen. Der Zeitbereich in der Titelleiste wird automatisch entsprechend dem neuen Zeitbereich aktualisiert.
- Klicken Sie mit der rechten Maustaste auf ein CI in der rechten Seitenleiste, und wählen Sie **Formular anzeigen** aus, um das zugehörige CI- Formular zu öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf das Kartensymbol neben einem Anwendungsservice, der auf der Registerkarte **Anwendungsservices** aufgeführt ist, um die zugehörige Anwendungsservicezuordnung zu öffnen.
- Klicken Sie neben einem CI auf „Entfernen“ ( ), um es aus dem Explorer für Einblicke zu entfernen.
- Klicken Sie auf das Exportsymbol in einem Diagramm, um es als PNG- oder SVG-Bild oder als PDF-Dokument herunterzuladen.

Zugehörige Informationen

Ansicht des Explorers für Einblicke erstellen

Ansicht des Explorers für Einblicke erstellen

Sie können eine benutzerdefinierte Ansicht im Explorer für Einblicke erstellen, in der alle der Canvas hinzugefügten Metrikdiagramme und alle hinzugefügten Konfigurationselemente gespeichert werden. Nachdem Sie eine Ansicht erstellt haben, können Sie einen Link zur Ansicht freigeben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Explorer für Einblicke**an.
2. Klicken Sie auf **Ansicht erstellen** ( ), und geben Sie im Dialogfeld „Neue Ansicht erstellen“ einen **Namen** ein.
   Wenn Sie bereits dabei sind, eine Ansicht zu erstellen, können Sie **Mit vorhandenen Elementen erstellen** auswählen, um eine vorhandene Ansicht zur Bearbeitung zu laden, anstatt mit einer leeren Canvas zu beginnen.
3. Klicken Sie auf **Erstellen**.
4. Fügen Sie Elemente hinzu, die in der Ansicht enthalten sein sollen:
   a. Ziehen Sie Metriken, und erstellen Sie Diagramme auf der Canvas.
   b. Fügen Sie Konfigurationselemente hinzu.
   Während Sie eine Ansicht ändern, wird sie bei jeder Aktualisierung automatisch gespeichert. Die Zeiteinstellungen werden nicht in Ansichten gespeichert, und wenn eine gespeicherte Ansicht geladen wird, wird ihr Zeitraum immer auf **Letzte Stunde** mit aktuellen Informationen festgelegt.

Nächste Maßnahme

- Freigeben einer Ansicht: Klicken Sie auf **Freigabeansicht** ( ), und klicken Sie dann im Dialogfeld „Freigeben“ auf **Link kopieren**. Senden Sie den Link, oder fügen Sie ihn ein, um ihn für alle Personen zugänglich zu machen, für die Sie die Ansicht freigeben möchten. Ein freigegebener Link erfasst den Zeitbereich der Ansicht, die der Canvas hinzugefügten Diagramme und alle hinzugefügten Konfigurationselemente.
- Gespeicherte Ansicht anzeigen: Öffnen Sie die Dropdown-Liste **Gespeicherte Ansicht auswählen**, und wählen Sie eine zuvor gespeicherte Ansicht aus, die Sie anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdiagramme in Agent Workspace anzeigen

Agent Workspace für Metric Intelligence bietet einfachen Zugriff auf Metrikdiagramme für ein CI. Auf einem Warnungsformular können Sie Detailinformationen zu wichtigen Metrikdiagrammen für das CI anzeigen, das der Warnung zugeordnet ist.

Vorbereitungen

- Das CI, für das Sie Metrikdiagramme anzeigen möchten, muss einer Warnung zugeordnet sein.
- Die Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] muss aktive Diagrammkonfigurationen für die CI-Klasse enthalten, für die Sie Metrikdiagramme anzeigen möchten.

Erforderliche Rolle: Workspace_user und itil

Warum und wann dieser Vorgang ausgeführt wird

Der Satz der Metrikdiagramme, Diagrammtypen und anderen Diagrammmerkmalen wird durch die Diagrammkonfigurationen in der Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] für die CI-Klasse bestimmt.

Prozedur

1. Navigieren Sie zu **Agent Workspace** und klicken Sie auf **Agent Workspace-Startseite**.
2. Klicken Sie in Agent Workspace auf **Liste**, und wählen Sie im Bereich **Listen** eine der kategorisierten Listen unter **Warnungen** wie **Alle Alarme** oder **Höchste Priorität** aus.
3. Öffnen Sie in der Warnungslistenansicht eine Warnung.
   Der Warnung muss ein **Configuration Item** zugeordnet sein.
4. Klicken Sie auf der Registerkarte **Details** des Warnungsformulars auf **Metriken**.

Ergebnis

Alle Metrikdiagramme, die für das der Warnung zugeordnete CI konfiguriert und aktiv sind, werden im Metrikdiagrammformular auf der Registerkarte **Metriken** angezeigt. Die Berechnung des Standardzeitbereichs für die Diagramme basiert auf den Zeiten, zu denen das erste und das letzte Ereignis aufgetreten sind, von denen die Warnung generiert wurde.

Nächste Maßnahme

- Ändern Sie den Zeitbereich für die Diagramme, indem Sie die **Startzeit** und **Endzeit** ändern. Wenn Sie den Zeitbereich ändern, werden alle Diagramme entsprechend dem neuen Zeitbereich aktualisiert.
- Klicken Sie auf das Zahnradsymbol **Einstellungen öffnen**, und ändern Sie die Einstellungen für alle Diagramme:
  - **Grenzen anzeigen**: Zum Anzeigen der Grenzen im Diagramm. Auch wenn diese Option aktiviert ist, sind in dem Diagramm keine Grenzen für zusammengefasste Ressourcen vorhanden.
  - **Legende anzeigen**: Zum Anzeigen der Diagrammlegende.
- Klicken Sie auf **Explorer für Einblicke**, um den Explorer für Einblicke in einer neuen Browserregisterkarte zu öffnen. Dieser Explorer für Einblicke wird mit dem aktuell vorausgewählten CI und den aktuellen Zeitbereichseinstellungen in Agent Workspace geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdiagramme für Agent Workspace konfigurieren

Konfigurieren Sie den Satz von Metric Intelligence-Metrikdiagrammen, Diagrammtypen und anderen Diagrammeigenschaften, die in Agent Workspace angezeigt werden.

Vorbereitungen

Erforderliche Rolle: admin oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Bis zu 10 Metrikdiagramme für eine Klasse können so konfiguriert werden, dass sie im Metrikdiagrammformular von Metrikdaten in Agent Workspace erscheinen. Die Metrikdiagrammkonfigurationen werden in der Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] gespeichert und bestimmen, welche Metrikdiagramme für ein CI angezeigt werden, das einer Warnung zugeordnet ist. Standardmäßig enthält die Tabelle „Metadaten des Messgrößen-Dashboards“ vorkonfigurierte Metrikdiagramme für mehrere Klassen.

Wenn die Ressourcenbindung aktiviert ist und Sie einen **Ressourcentyp** in der Metrikdiagrammkonfiguration angeben, werden alle Ressourcen für das CI in das Diagramm aufgenommen. Die von Ihnen angegebene Klassentabelle für die Ressourcenklasse (z. B. `ci_resource_metric_extension`) wird zum Abrufen aller Ressourcen für das CI verwendet. Dann werden die Werte der Ressourcen für jeden Zeitpunkt in der Datenreihe zu einem einzelnen Datenpunkt zusammengefasst, der den Durchschnitt der Metrikwerte aller Ressourcen für diesen Zeitpunkt darstellt.

Diagrammzusammenfassung

Die Zusammenfassung wird je nach Einstellung des* Diagrammtyps *und je nachdem, ob Ressourcen im Diagramm enthalten sind, unterschiedlich angewendet, wie durch die Einstellung des* Ressourcentyps *angegeben:

Diagrammtyp	Ressourcen	Zusammenfassung
Time_Series	Nein	Keine Zusammenfassung
Time_Series	Ja	Ressourcen werden pro Datenpunkt gemittelt.
Single_Score	Nein	Datenpunkte werden gemäß der Einstellung **Diagrammzusammenfassung** zusammengefasst.
Single_Score	Ja	Datenpunkte werden pro Datenpunkt gemittelt und die Datenpunkte werden dann gemäß der Einstellung **Diagrammzusammenfassung** zusammengefasst.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Konfiguration der Metrikansicht**an.
2. Wählen Sie in der Listenansicht „Metadaten des Messgrößen-Dashboards“ (Dashboard-Metadaten) eine vorhandene Konfiguration aus, oder klicken Sie auf **Neu**.
3. Füllen Sie das Formular „Metadaten des Messgrößen-Dashboards“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Fügen Sie das Diagramm in das Formular für Metric Intelligence-Diagramme in Agent Workspace ein.
Ressourcentyp	Ressourcenklasse, die dem CI zugeordnet ist und für die alle Ressourcen abgerufen und zusammengefasst werden sollen
Configuration Item-Typ	CI-Klasse, für die das Diagramm gilt, z. B. `cmdb_ci_metric_extension`
Diagrammzusammenfassung	Typ der Zusammenfassung, die auf Diagramme mit einer Punktzahl angewendet wird. Die Zusammenfassung kann dem Durchschnitt der Datenpunkte in der Zeitreihe entsprechen. Oder dem Mindest-, Höchst- oder letzten Datenpunkt in der Zeitreihe.
Quellmetriktyp	Metriken wie „% freier Speicherplatz“, die für den CI-Typ überwacht werden
Reihenfolge	Reihenfolge, in der das Metrikdiagramm in allen für die Klasse angegebenen Metrikdiagrammen angezeigt wird. Für eine ordnungsgemäße Darstellung und Ausrichtung werden alle Diagramm für einzelne Punktzahl unabhängig von den Reihenfolgeeinstellungen immer nach Zeitreihendiagrammen angezeigt.
Diagrammtyp	○ Time_Series: Stellt alle Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms dar. ○ Single_Score: Eine einzelne Zahl, die einer Zusammenfassung der Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms entspricht. Die Zusammenfassung wird durch die Einstellung von **Diagrammzusammenfassung** bestimmt.

Statistiken der Eigensystemüberwachung für Metric Intelligence anzeigen

Überwachen Sie den Status von Metric Intelligence-Komponenten und -Prozessen. Verwenden Sie die Seite „Xmlstats“, um Statistiken und Diagnosedetails anzuzeigen, die bei der Behebung von Problemen mit Metric Intelligence helfen können.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Öffnen Sie einen Browser, und geben Sie die URL der Instanz ein.
   Geben Sie ein: `http://<Instanzname>.service-now.com`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Hängen Sie den folgenden Text an die URL der Instanz an: xmlstats.do?include=XMLStatsOI. Das vollständige URL-Format ist: http://<Instanzname>.service-now.com/xmlstats.do?include=XMLStatsOI
3. Drücken Sie die Eingabetaste.

Ergebnis

Details werden zwischen zwei Abschnitten getrennt: Statistiken auf Instanzebene und Statistiken auf Knotenebene. Details im Knotenabschnitt beziehen sich auf den Knoten in der URL.

Knotenabschnitt

Eintrag	Beschreibung
batches_recieved	Die Anzahl der Metrikstapel, die der Knoten vom MID Server erhalten hat
batches_processed	Anzahl der auf dem Knoten verarbeiteten Metrikstapel

Details im Instanzabschnitt beziehen sich auf die gesamte Instanz und zeigen den Status der Selbstintegritätsüberwachung an.

Instanzabschnitt

Eintrag	Beschreibung
scheduled_jobs_monitor	Status der Eigensystemüberwachung, die überprüft, ob die wesentlichen regelmäßigen Metric Intelligence-Aufgaben aktiv sind.
distributed_cluster_monitor	Status der Eigensystemüberwachung, die überprüft, ob der verteilte Cluster von Metric Intelligence-MID Servern ordnungsgemäß ausgeführt wird.
oi_extension_monitor	Status der Eigensystemüberwachung, die überprüft, ob die Metric Intelligence-Erweiterung ordnungsgemäß ausgeführt wird.
metrics_collection_monitor	Status der Selbstintegritätsüberwachung, die überprüft, ob Metriken von aktiven Connectors erfasst werden, die für die Metriksammlung konfiguriert sind

Überprüfen Sie, ob die Definitionen für Advanced Promotion Engine Sind aktiv

Überprüfen Sie, ob Advanced Promotion Engine Definitionen, die im Basissystem enthalten sind, sind aktiv.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die aktiven Definitionen heben eine Gruppe von Anomaliewarnungen in die Tabelle „alle Warnungen“ herauf, wenn alle Bedingungen der Definition erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Bedingungen der Definitionen, die im Basissystem enthalten sind, nicht ändern. Informationen zum Erstellen anwenderdefinierter Definitionen finden Sie unter Erstellen Sie eine Definition für Advanced Promotion Engine.

Prozedur

1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Erweiterte Heraufstufungsdefinitionen**an.
2. Wählen Sie aus Advanced Promotion Engine Definition, die Sie aktiv sein möchten:
   - Windows-Server
   - Linux-Server
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.
4. Wählen Sie **Speichern**.

Erstellen Sie eine Definition für Advanced Promotion Engine

Erstellen Sie eine Definition für Advanced Promotion Engine Damit Sie die Bedingungen für die Heraufstufung der Anomaliewarnungen zu IT-Warnungen definieren können. Durch Heraufstufen der Warnungen, die die Bedingungen erfüllen, werden nur die relevantesten Warnungen in die Tabelle verschoben.

Warum und wann dieser Vorgang ausgeführt wird

IT-Warnungen werden in der Express-Liste angezeigt und von einem Operator bearbeitet.

Nur Metriken, die einer Metrikkonfigurationsregel zugeordnet sind, die hat **Anomaliepunktzahlebene = Anomaliewarnungen** Werden für die Heraufstufung zu IT-Warnungen berücksichtigt. Weitere Informationen zu Metrikkonfigurationsregeln finden Sie unter Metrikkonfigurationsregeln.

Vorbereitungen

Stellen Sie sicher, dass Metrikdaten Plugin (com.snc.sa.metric) ist installiert.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Erweiterte Heraufstufungsdefinitionen**an.
2. Wählen Sie **Neu**.
3. In **Name** Feld einen beschreibenden Namen für die Definition eingeben.
4. In **Reihenfolge** Feld die Ausführungsreihenfolge für die Definition festlegen.
   Die Definitionen mit einer niedrigeren Reihenfolge werden zuerst ausgeführt.
5. Aktivieren Sie die Definition, indem Sie auswählen **Aktiv** Kontrollkästchen.
6. Auf der **CIs** Füllen Sie die Felder für die CI-aIerts aus, die Sie für die Heraufstufung berücksichtigen möchten.

Felder der Registerkarte „CIs“

Feld	Beschreibung
CI-Klasse	CI-Klassenwarnungen, die in die Tabelle „alle Warnungen“ heraufgestuft werden sollen.
Filter	Filter, um einzuschränken, für welche CIs die Definition gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie Aus **Neue Kriterien** Dient zum Konfigurieren der Bedingungen, für die die Definition gilt. Sie können weitere Bedingungen hinzufügen, indem Sie eine der folgenden Optionen auswählen **ODER** Oder **UND** .
CIs überspringen, die vor weniger als dieser Anzahl von Tagen erstellt wurden	Anzahl der Tage in der Vergangenheit, in denen ein während dieser Zeit erstelltes CI ignoriert wird. Beispielsweise gibt der Wert 7 an, dass alle CIs, die vor weniger als 7 Tagen erstellt wurden, nicht für die Heraufstufung in die Tabelle „alle Warnungen“ berücksichtigt werden.

7. Auf der **Schweregrad** Geben Sie den Mindestschweregrad der Warnungen ein, die für die Heraufstufung berücksichtigt werden sollen.
   Warnungen mit dem angegebenen Schweregrad und höheren Stufen werden für die Heraufstufung berücksichtigt.
8. Auf der **Anzahl der Warnungen** Registerkarte im **Anzahl der Warnungen für CI** Geben Sie die Mindestanzahl der Warnungen eines CI mit identischem Schweregrad (oder höher) ein, die für die Heraufstufung berücksichtigt werden sollen.
   Beispielsweise gibt der Wert 3 an, dass mindestens drei Warnungen mit dem angegebenen Schweregrad (oder höher) in einem CI vorhanden sein müssen, damit die Warnung für die Heraufstufung berücksichtigt werden kann.
9. Auf der **Zeitfenster** Registerkarte:
   - In **Berücksichtigen Sie Warnungen, die vor mindestens dieser Anzahl von Minuten aktualisiert wurden** Geben Sie die Mindestanzahl von Minuten ein, bis eine Warnung für die Heraufstufung berücksichtigt werden soll.

     Wenn der Wert des Felds beispielsweise 5 ist, werden nur Warnungen für die Heraufstufung berücksichtigt, die vor mindestens fünf Minuten aktualisiert wurden.
   - Wählen Sie im blauen Feld den Link Anzahl der Minuten aus, um die Anzahl der Minuten zu ändern, während der Warnungen für die Heraufstufung berücksichtigt werden sollen.

     Die **Eigenschaften** Seite wird geöffnet, und Sie ändern den Wert in **Die Breite der Zeit...** Feld.

     Standard = 30.

   Zum Beispiel:
   - Die aktuelle Zeit ist 10:05 Uhr.
   - In **Die Breite der Zeit...** Feld haben Sie einen Wert von 30 eingegeben.
   - In **Berücksichtigen Sie Warnungen, die vor mindestens dieser Anzahl von Minuten aktualisiert wurden** Feld, haben Sie 5 eingegeben.

   Warnungen, die zwischen 9:30 und 10:00 auftreten, werden für die Heraufstufung berücksichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Stellen Sie sicher, dass eine Metrikkonfigurationsregel vorhanden ist, die Metriken enthält, die zu einer IT-Warnung heraufgestuft werden sollen, und dass die Anomaliepunktzahlstufe der Regel ist **Anomaliewarnungen** . Details zum Konfigurieren einer Metrikkonfigurationsregel finden Sie unter Regel für Konfigurationseinstellungen erstellen.

Zeigen Sie die heraufgestuften Ereignisse an

Zeigen Sie die Anomaliewarnungen an, die die Advanced Promotion Engine Zu IT-Ereignisse heraufgestuft. Durch das Anzeigen VON IT-Ereignissen können Sie die Quelle des Ereignisses nachverfolgen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Das System generiert ein IT-Ereignis, wenn eine Anomaliewarnung heraufgestuft wird. Diese Ereignisse werden dann zu IT-Warnungen. Details finden Sie unter Zeigen Sie die heraufgestuften Anomaliewarnungen an.

Prozedur
1. Navigieren zu **Alle** > **Erweiterte Heraufstufungs-Events**an.
2. Zeigen Sie auf der Seite „Ereignisse“ die IT-Ereignisse an, die aus den Anomaliewarnungen von erstellt werden Advanced Promotion Engine.

Zeigen Sie die heraufgestuften Anomaliewarnungen an

Zeigen Sie die Anomaliewarnungen an, die die Advanced Promotion Engine Zu Ereignissen heraufgestuft, die dann als Warnungen in der Tabelle „alle Warnungen“ verarbeitet werden. Durch das Anzeigen von Warnungen in der Tabelle „alle Warnungen“ können Sie die Quelle der Warnung nachverfolgen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Die Ereignismanagement Die Warnungsgruppierungsfunktion verwendet die Anomaliewarnungen, die zu den IT-Ereignissen heraufgestuft werden, und gruppiert sie in neue IT-Warnungen.

In der Tabelle Warnungen werden alle relevanten Probleme im System angezeigt.

Prozedur
1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Anomaliewarnungen**an.
2. Zeigen Sie im Spaltenheader ist erweitert die Warnungen mit dem Wert an **Wahr** .
   Die IT-Warnung, die aus der Anomaliewarnung erstellt wird, wird in der Spalte IT-Warnung angezeigt.
3. **Wahlweise:** Wählen Sie eine Warnung aus, um weitere Informationen zur Warnung zu erhalten.
   Weitere Informationen zu den angezeigten zusätzlichen Informationen finden Sie unter Warnungen in Service Operations-Arbeitsbereich.

Metrikregeln erstellen

Erstellen Sie eine Metrikregel, um die Metrik, die Schwellenwerte und -Bereiche und den Schweregrad generierter Ereignisse zu bestimmen. Sie können einen Filter hinzufügen, der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Konfigurationselemente (Configuration Items, CI)-Typen oder -Ressourcen bestimmt, für die Sie Warnungen erhalten. Sie können beispielsweise einen Filter so konfigurieren, dass er nur für Warnungen empfängt Windows Server.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn eine Metrik einen konfigurierten Schwellenwert überschreitet oder innerhalb des Bereichs liegt, erstellt das System ein einzelnes Ereignis, das schließlich in eine IT-Warnung verarbeitet wird. Der Schweregrad des Ereignisses (und der Warnung) wird durch einen definierten Schwellenwert bestimmt, und das Ereignis ist an ein CI gebunden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Metrikregeln**an.
2. Wählen Sie Aus **Neue Metrikregel** .
   Die **CI-Auswahl** Seite wird geöffnet.
3. Wählen Sie die CI-Klasse aus, für die die Regel in ausgeführt werden soll **CI-Klasse** Feld.
   Nur CIs mit Metriken können ausgewählt werden.
4. **Wahlweise:** Wenden Sie einen Filter innerhalb der ausgewählten CI-Klasse an.
   Beispiel: Wenn Sie eine CI-Klasse von ausgewählt haben **Linux-Server** , Sie können einen Filter anwenden, um anzugeben, dass die Regel nur für die Server gilt, deren Hostname mit einer angegebenen Zeichenfolge beginnt.
5. Wählen Sie **Weiter**.
   Die **Warnungskriterien** Seite wird geöffnet.
6. Wählen Sie die Metrik und die Kriterien aus, um eine Warnung zu erstellen.

   a. Wählen Sie den Warnungsschweregrad aus, den Sie in konfigurieren möchten **Warnungsschweregrad** Feld.
   Wählen Sie aus Folgendem:
   - Kritisch
   - Hoher
   - Geringer
   - Warnung

   b. Wählen Sie die Metrik aus, auf die der Warnungsschweregrad angewendet werden soll **Metrik** Feld.

   c. Wählen Sie den Vergleichsoperator (gleich, ist größer als, ist größer als, ist größer als oder gleich usw.) in aus **Vergleichsoperator** Feld.

   d. Geben Sie einen Wert in ein **Wert** Feld.

   Sie können beispielsweise Kriterien konfigurieren, um anzugeben, dass die Metrik bei der Metrik angegeben wird **Node_rx_Packets** Ist größer als 10, wird eine kritische Warnung generiert.

   Um zusätzliche Warnungsschweregrade zu definieren, wählen Sie aus **Fügen Sie einen weiteren Warnungsschweregrad hinzu** Und wiederholen Sie diesen Schritt.

7. Wählen Sie aus, wann die Warnung in generiert werden soll **Warnung, wenn** Abschnitt.
   Wählen Sie aus Folgendem:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Alle Stichprobenwerte müssen im folgenden Zeitraum gegen die Kriterien verstoßen** .

  Wählen Sie den Zeitraum in Minuten aus.

- **Der Durchschnitt der Stichprobenwerte im folgenden Zeitraum muss gegen die Kriterien verstoßen** .

  Wählen Sie den Zeitraum in Minuten aus.

- **Jedes Mal, wenn die als Stichprobe erfassten Werte die Kriterien verletzen** .

8. Wählen Sie **Weiter**.
   Die **Name und Aktivierung** Seite wird geöffnet.
9. Überprüfen Sie den Namen und die Details der Metrikregel.

   Um die Regel zu aktivieren, stellen Sie sicher, dass **Aktiv** Umschalter

   Ist aktiviert.
10. Wählen Sie **Fertigstellen** aus.

Ereignisregel zum Binden von Metrikereignissen an Host-CIs erstellen

Erstellen Sie Ereignisregeln, um die Bindung von Metrikereignissen an Host-CIs explizit zuzulassen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ab Release London stützt sich Metric Intelligence nicht mehr auf den standardmäßigen Ereignismanagement-Workflow, der Knoten an Host-CIs bindet. Ereignismanagement ist so konfiguriert, dass der standardmäßige Hostbindungsalgorithmus angewendet wird, wenn eine Event-Regel basierend auf Event-Daten keine CIs für die Bindung finden kann. In Metric Intelligence kann mit einer bestimmten Event-Regel und zwei verschiedenen Events eine Situation auftreten, in der ein Event an das richtige CI gebunden wird, ein anderes Event aber nicht. In diesem Fall wird für das ausgewählte CI und das CI auf Hostebene derselbe Metriktyp erstellt, was zu Verwirrung führt.

Beispiel: Mit einer Ereignisregel, die die Prozentsatzmetrik des Datenträgers an einen Speicherdatenträger bindet, kann ein Ereignis ein Datenträger-CI finden, ein anderes Ereignis jedoch nicht. Dies führt dazu, dass die Prozentsatzmetrik des Datenträgers für ein Datenträger-CI und ein Host-CI erstellt wird.

Um diese Verwirrung zu vermeiden, ist die standardmäßige Ereignismanagement-Hostbindung für Metrikereignisse im Basissystem deaktiviert. Um die Hostbindung für Metrikereignisse zuzulassen, erstellen Sie die folgende Ereignisregel explizit im Ereignismanagement Designer für Ereignisregeln. Die zugrunde liegende Bindungsfunktionalität des Designers für Ereignisregeln wird verwendet, um CIs Metriken zuzuordnen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Bedingungen** > **Ereignisregeln** Zum Öffnen des Ereignisregel-Designers.
2. Klicken Sie auf **Neu**, und stellen Sie sicher, dass der **Aktiv**-Umschalter nach rechts gesetzt ist (Aktiv).
3. Auf der Registerkarte **Ereignisregel-Informationen**:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Legen Sie **Quelle** auf die Datenquelle fest, für die diese Regel gilt.

b. **Wahlweise:** Geben Sie eine **Beschreibung** wie Metriken auf Hostebene binden ein.

4. Legen Sie auf der Registerkarte **Ereignisfilter** eine Filterbedingung fest, um anzugeben, dass **Klassifizierung** auf **Metrik** gesetzt ist.
5. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

Metrikdaten – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Metrikdaten Einstellungen und Eigenschaften.

Einstellungen des Insights-Explorers

Sie können die Einstellungen des Explorers für Einblicke konfigurieren, um z. B. die Aktualisierungshäufigkeit oder die Anzeige zugehöriger Datensätze zu steuern.

Klicken Sie auf das Zahnradsymbol **Einstellungen**, um das Dialogfeld „Anwendungseinstellungen“ zu öffnen.

Einstellung	Beschreibung
Aktualisierungsintervall	Aktivieren Sie die Aktualisierung von Metrikdaten im Explorer für Einblicke bzw. legen Sie die Häufigkeit dafür fest.
Indikatoren	Aktivieren Sie einen beliebigen Indikator, um zugehörige Datensätze wie Incidents oder Probleme für CIs anzuzeigen. Das entsprechende Symbol wird auf der Zeitleiste im Metrikdiagramm angezeigt und gibt die Anzahl der Datensätze für das CI an. Ein Umschalter ist nur verfügbar, wenn das Feld **In Metriken aktiv** im Formular „Kartenindikator“ für die entsprechende Tabelle ausgewählt ist. Beispiel: Der Umschalter **Incident** ist nur verfügbar, wenn **In Metriken aktiv** im Formular „Kartenindikator“ für die Incident-Tabelle [Incident] ausgewählt ist.

Zugehörige Informationen

Dependency Views-Kartenindikatoren

Eigenschaften der Empfindlichkeitsgrenzen für Metriken im Explorer für Einblicke

Die folgenden Eigenschaften können konfiguriert werden, um das Systemverhalten bei der Erkennung sensibler Grenzen für Metriken im Explorer für Einblicke anzupassen. Um Änderungen an den Standardwerten aufzurufen, navigieren Sie zu **Systemeigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Alle Eigenschaften** Und fügen Sie die angegebenen Eigenschaften hinzu (sie sind standardmäßig nicht sichtbar).

Eigenschaften von sensiblen Grenzen

Eigenschaftsname	Beschreibung
sa_metric.sensitive_bounds_calculation_enabled	Aktivieren/Deaktivieren Sie die Berechnung sensibler Grenzen. Standardwert: True
sa_metric.sensitive_bounds_percentile	Prozentwert der Berechnung der Empfindlichkeitsgrenzen. Wenn der konfigurierte Prozentsatz der Metrikwerte innerhalb der in der Eigenschaft *sa_metric.sensitive_bounds_sensitivity_factor* angegebenen Anzahl der Standardabweichungen (STDs) liegt, werden sensible Grenzen erkannt und die Empfindlichkeitsberechnung ändert sich auf den in der Eigenschaft *sa_metric.sensitive_bounds_control_factor* angegebenen Wert. Standard: 95 %
sa_metric.sensitive_bounds_control_factor	Anzahl der Standardabweichungen (STDs) vom mittleren Metrikwert, mit denen Metrikgrenzen gemessen werden, nachdem das System sensible Grenzen erkannt hat. Standard: 5,0
sa_metric.sensitive_bounds_sensitivity_factor	Anzahl der Standardabweichungen (STDs) vom mittleren Metrikwert, anhand denen das System auf sensible Grenzen testet. Standard: 2,0

Zugehörige Informationen

Empfindlichkeit der Metrikgrenzen

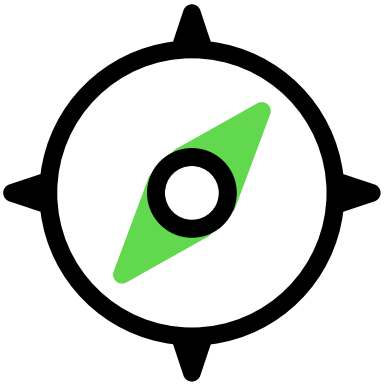
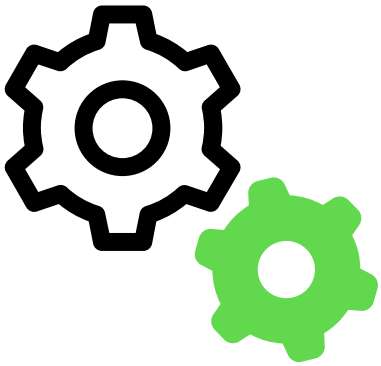
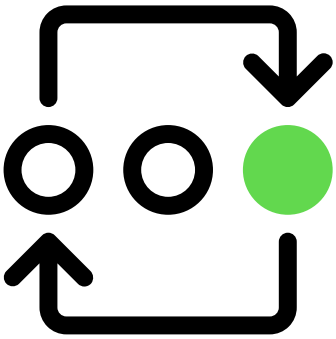
Automatische Übersetzung

Now Assist für IT Operations Management (ITOM)

Verwenden Sie ServiceNow® Now Assist für IT Operations Management (ITOM) Anwendung zum Analysieren von Warnungen in Ereignismanagement. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, damit Sie die Warnung effektiver untersuchen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über Now Assist für ITOM	Konfigurieren Sie die Anwendung Now Assist für ITOM, um zu beginnen	Verwenden Sie generative KI-Fähigkeiten, die von Now Assist für ITOM angeboten werden

Wichtig:

- Nicht alle Modellanbieter sind für Kunden mit landesinternen SKUs verfügbar, und einige Now Assist-Produkte/-Funktionen sind derzeit für Kunden im Land nicht verfügbar. Weitere Informationen finden Sie unter KB1584492 artikel in der Now Support Knowledge Base. Überprüfen Sie in zukünftigen Releases auf Updates der Modellanbieter-Verfügbarkeit.
- Einige Now Assist Produkte/Funktionen sind derzeit für Kunden in den mit FedRAMP, NSC DOD IL5 oder Australia IRAP geschützten Rechenzentren, selbst gehosteten Kunden oder anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.
- Einige Now Assist Produkte/Funktionen sind derzeit nur für Kunden in einigen Regionen verfügbar. Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.

Sie können verwenden Now LLM Service, Azure OpenAI, Google Gemini Oder Anthropic Claude auf AWS Als KI-Modellanbieter für alle Now Assist Kompetenzen und KI-Agenten. Verwenden Sie die Konfigurationssteuerungen in KI-Governance Um zu definieren, welche Optionen verfügbar sind, legen Sie dann die Einstellungen auf Kompetenzebene in fest Now Assist-Administrator Konsole an. Weitere Informationen finden Sie unter Große Sprachmodelle auf der ServiceNow AI Platform® .

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basierte, regelbasierte und Log Analytics-Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Abhängigkeiten

Für eine Liste von Now Assist für IT Operations Management (ITOM) Plugin-Abhängigkeiten, siehe Mit Now Assist für ITOM installierte Anwendungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- KI und Intelligenz in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus besteht keine Garantie dafür, dass diese Anwendung für Ihren Anwendungsfall vollständig trainiert oder getestet wurde. Um diese Probleme zu mindern, liegt es in Ihrer Verantwortung, Ihre Verwendung dieser Anwendung auf Richtigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, menschliche Aufsicht über die Ausgabe zu übernehmen und zu Entscheidungszwecken nicht ausschließlich KI-generierte Ausgaben zu verwenden. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung, Sicherheit und Infrastruktur einsetzen möchten. Sie stimmen zu, sich an zu halten Richtlinie zur zulässigen Nutzung von KI von ServiceNow , Die von ServiceNow aktualisiert werden kann.

Wichtig: Nicht verwenden Now Assist für ITOM Für kritische Sicherheitswarnungen.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now Assist Abwählseite beschrieben.

Weitere Informationen finden Sie unter Now Assist Dokumentation an.

Zugehörige Informationen

Now Assist für IT Operations Management (ITOM) erkunden

Now Assist für IT Operations Management (ITOM) erkunden

Die Now Assist für IT Operations Management (ITOM) Die Anwendung verwendet generative KI, um Warnungsanalysen bereitzustellen. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, damit Sie die Warnung effektiver untersuchen können.

Die Warnungsanalyse ist eine wichtige Funktion, die den Warnungsselektierungsprozess vollständig transformiert und zu einem schnelleren, nahtlosen Warnungsmanagement

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beitragen kann. Basierend auf generativer KI wird ein großes Sprachmodell (LLM) verwendet, um visuell lesbare Warnungstitel und detaillierte Beschreibungen basierend auf angereicherten und umsetzbaren Warnungsdaten zu generieren. Die KI-generierten Warnungsinformationen erleichtern die schnelle Selektierung von Warnungen und eine effektive Analyse für Ihr Team, was zu einer erheblichen Verkürzung der Lösungszeit führen kann.

Die Warnungsanalyse verbessert die Effizienz und Effektivität des Warnungsmanagements.

Zu den wichtigsten Funktionen gehören:

- Automatische Generierung klarer, leicht verständlicher Warnungsbeschreibungen.
- Verfügbarkeit der Analyse im Warnungsformular und in der Express-Liste.
- Möglichkeit, Daten mithilfe der Kartenaktualisierung zu aktualisieren und erneut zu generieren.

Hinweis: Warnungsanalysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basiert, CMDB, Log Analytics, Gemischte und auf Netzwerkdatenverkehr basierende Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Konfigurieren von Now Assist für IT Operations Management (ITOM)

Aktivieren Ereignismanagement Anwender zum Anzeigen von Warnungsanalysen, die angezeigt werden Now Assist für ITOM Erstellt mit generativer KI.

Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin

Installieren Sie ITOM Plugin in ServiceNow® Now Assist Funktion.

Vorbereitungen

Installieren Sie AIOps-Experience[sn_SOW_aiops] Anwendung aus dem ServiceNow Store. Weitere Informationen finden Sie unter Installieren Service Operations-Arbeitsbereich Für ITOM Anwendung.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Installieren Now Assist Plugins Zum Aktivieren von generativer KI und agentischer KI in Ihrer Instanz.

Prozedur

1. Wechseln Sie zu ServiceNow Store Website.
2. Geben Sie in der Suchleiste ein Now Assist für ITOM Und wählen Sie dann aus **Suchen** .
3. Wählen Sie aus Now Assist für ITOM Widget, und wählen Sie dann aus **Abrufen** Um diese Anwendung für die Installation in Ihren Instanzen verfügbar zu machen.
4. Installieren Sie die Anwendung Now Assist für ITOM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.

b. Suchen Sie nach Now Assist für IT Operations Management (ITOM).

c. Wählen Sie **Installieren** aus.

Zugehörige Informationen

Zeigen Sie eine Warnungsanalyse von an Now Assist In Express-Liste

Aktivieren Now Assist KI-Agents für IT Operations Management(ITOM)

Aktivieren Now Assist KI-Agents, die dem agentischen Workflow „Selektierung und Warnungsanalyse“ zugeordnet sind, um die agentische KI-Experience zu aktivieren.

Vorbereitungen

Bevor aktiviert wird Now Assist KI-Agents müssen Sie installieren Now Assist für IT Operations Management (ITOM) Plugin. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.

Um mit KI-Agents zu beginnen, müssen Sie Folgendes haben:

- Eine Instanz in Yokohama Patch 3 und höher.
- A ServiceNow Pro Plus- oder Enterprise Plus-Lizenz.
- KI-Suche In Ihrer Instanz aktiviert.

Erforderliche Rolle: Administrator

Prozedur

1. Aktivieren Sie den Workflow Selektierung und Analyse von Warnungen in KI-Agenten-Studio.
   a. Navigieren zu **Alle** > **KI-Agenten-Studio** > **Erstellen und verwalten**an.
   b. Wählen Sie in der Tabelle aus **Selektieren und analysieren Sie Warnungen** .

   Die Seite „Warnungen selektieren und analysieren“ in KI-Agenten-Studio Ermöglicht Ihnen die Verwaltung des agentischen Workflows, einschließlich Optionen für Beschreiben und Verbinden, Definieren des Auslösers und Anzeige „Auswählen“.

2. Machen Sie den agentischen Workflow „Selektierung und Warnungen analysieren“ in sichtbar Now Assist Bereich.
   a. Navigieren Sie zu **Wählen Sie Anzeige aus** .
   b. Neben **Now Assist-Bereich** Wählen Sie aus **Anzeige** Umschalten, um die Anzeige zu aktivieren.
   c. Wählen Sie Aus **Speichern und testen** .
   d. Navigieren zu **Alle** > **Virtual Agent** > **Designer**an.
   e. Von **Wählen Sie Assistent aus** Dropdown-Liste auswählen **Now Assist-Bereich – Plattform (Standard).**
   f. Suchen Sie nach **Selektieren und analysieren Sie Warnungen** .
   g. Wählen Sie das Symbol Zeilenaktionen (⋮), und wählen Sie aus **Heraufgestuft** .

Nächste Maßnahme

Um auf KI-Agents in zuzugreifen Now Assist Bereich müssen Sie den Bereich aktivieren. Weitere Informationen finden Sie unter Aktivieren Sie Now Assist Bereich .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Now Assist Kompetenzen in Now Assist für IT Operations Management (ITOM)

Sie können aktivieren Now Assist Kompetenzen zur Verwendung in Now Assist für IT Operations Management (ITOM).

Vorbereitungen

Bevor aktiviert wird Now Assist-Kompetenzen müssen Sie installieren Now Assist für IT Operations Management (ITOM) Plugin. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie Now Assist Kompetenzen in Now Assist für IT Operations Management (ITOM) Plugin zum Aktivieren der generativen KI in Ihrer Instanz.

Prozedur

1. Navigieren zu **Alle** > **Now Assist Admin** > **Kompetenzen**an.

   Wenn Sie sich bereits in befinden Now Assist-Administrator-Konsole auswählen **Now Assist-Kompetenzen** Registerkarte.

2. Wählen Sie im Navigationsbereich aus **Technologie** > **ITOM** Dient zum Überprüfen des Kompetenzsatzes.

   Schalten Sie zwischen Listen- und Rasterlayouts um, um eine optimale Anzeige zu erzielen.

3. Wählen Sie Aus **Kompetenz aktivieren** .

   Wählen Sie nach der Konfiguration eines Schritts aus **Speichern und fortfahren** Um zum nächsten Schritt zu wechseln. Kehren Sie zu einem vorherigen Schritt zurück, indem Sie auswählen **Zurück** .

4. Wählen Sie aus, wo angezeigt werden soll Now Assist Kompetenzen.

   Sie können auswählen, wo angezeigt werden soll Now Assist Kompetenzen. Es wird empfohlen, beides zu aktivieren **Produktinterner Desktop** Und **Now Assist-Bereich** . Für jede Anzeigeoption können Sie die Rollen auswählen, für die die verwendet werden soll Now Assist Kompetenzen werden angezeigt.

   a. Navigieren Sie zu **Wählen Sie Anzeige aus** .

   b. Wählen Sie aus, wo Sie die Kompetenz anzeigen möchten, indem Sie auswählen **Anzeige** Umschalten, um die Anzeige zu aktivieren.

   c. Wählen Sie Aus **Speichern und testen** .

KI-Agents für konfigurieren Now Assist für ITOM

Konfigurieren Sie KI-Agents für den agentischen Workflow „Warnungsauswirkung analysieren“. Nach der Konfiguration sammeln die KI-Agents Informationen, um Sie bei der Untersuchung von Warnungen zu unterstützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Dynatrace Analyse-KI-Agent

Verbinden Sie mit Dynatrace Analyse-KI-Agent für Ihren Dynatrace Instanz, die im agentischen Workflow „Warnungsauswirkung analysieren“ verwendet werden soll. Nach der Verbindung sammelt der KI-Agent Informationen, um Sie bei der Untersuchung von Warnungen zu unterstützen.

Vorbereitungen

Vor der Konfiguration von Dynatrace Analyse-KI-Agent müssen Sie Folgendes tun:

- Installieren Now Assist für IT Operations Management (ITOM) an.
- Integrieren Dynatrace Plattformereignisse mit Ereignismanagementan.
- Kopieren Sie Ihren Dynatrace Verbindungs-URL und Dynatrace Zugriffstoken oder persönliches Zugriffstoken.

  Die Dynatrace Zugriffstoken oder persönliches Zugriffstoken muss über verfügen `Probleme.Lesen` Umfang.

Erforderliche Rolle: Connection_admin und credential_admin

Prozedur

1. Navigieren zu **Alle** > **sys_alias.LIST**an.
2. Suchen und wählen Sie aus *`Dynatrace`***Analyse-KI-Agent** .
3. Wählen Sie Aus **Neue Verbindung Und Anmeldeinformationen Erstellen** .
4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Verbindungsname	Name von *`Dynatrace`*Verbindung. Dieser Name hilft Ihnen, ihn später zu identifizieren. Beispiel: *`Dynatrace`*Analyse der KI-Agent-Verbindung .
Verbindungs-URL	URL von *`Dynatrace`*Instanz. *`Dynatrace`*URLs folgen diesem Format: `https://<your-resource-name>.live.dynatrace.com` .
Zugriffstoken oder persönliches Zugriffstoken (muss „API-Token“ vorangestellt sein)	*`Dynatrace`* Zugriffstoken oder persönliches Zugriffstoken. Das Token muss mit beginnen `Api-Token` , Beispiel: `API-Token dt0s01.STABCDEF12345.G3HIJKLMNOP` .
Header-Name	Headername für *`Dynatrace`*Plattform-Token: `Autorisierung` . Ändern Sie diesen Wert, um den Header für verschiedene APIs anzupassen oder bestimmte Sicherheitsrichtlinien zu befolgen.

5. Wählen Sie **Erstellen** aus.
   Ihre Verbindung wird in angezeigt **Verbindungen** Registerkarte.

Nächste Maßnahme

Aktivieren Sie Dynatrace Analyse-KI-Agent, um ihn im agentischen Workflow „Warnungsauswirkung analysieren“ zu verwenden. In KI-Agenten-Studio, Navigieren Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen und verwalten , suchen Sie nach Dynatrace Analysieren Sie den KI-Agent, und aktivieren Sie den Agent in der Definieren Sie wichtige Anforderungen Bildschirm.

Hinweis: Während der Arbeit in KI-Agenten-Studio, Stellen Sie sicher, dass der KI-Agent für den Abruf von Warnungsinformationen aktiv ist. Sie ist auch für den agentischen Workflow „Warnungsauswirkung analysieren“ erforderlich.

Um mehr über die Verwendung von zu erfahren Dynatrace Analyse-KI-Agent im agentischen Workflow „Warnungsauswirkung analysieren“ finden Sie unter Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“.

Konfigurieren Sie Kentik Analyse-KI-Agent

Verbinden Sie mit Kentik Analyse-KI-Agent für Ihren Kentik Instanz, die im agentischen Workflow „Warnungsauswirkung analysieren“ verwendet werden soll. Nach der Verbindung sammelt der KI-Agent Informationen, um Sie bei der Untersuchung von Warnungen zu unterstützen.

Vorbereitungen

Vor der Konfiguration von Kentik Analyse-KI-Agent müssen Sie Folgendes tun:

- Installieren Now Assist für IT Operations Management (ITOM) an.
- Integrieren Kentik Warnungen mit Ereignismanagement an.
- Kopieren Sie Ihren Kentik Verbindungs-URL, API-Token und E-Mail-Adresse, die dem API-Token zugeordnet ist.

  Die Kentik API-Token erfordert diese Berechtigung: Kann Geräte anzeigen.

Erforderliche Rolle: Connection_admin und credential_admin

Prozedur

1. Navigieren zu **Alle** > **sys_alias.LIST**an.
2. Suchen und wählen Sie aus **KI-Agent für Kentik-Analyse** .
3. Wählen Sie Aus **Neue Verbindung Und Anmeldeinformationen Erstellen** .
4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Verbindungsname	Name von Kentik Verbindung. Dieser Name hilft Ihnen, ihn später zu identifizieren. Beispiel: Kentik Prod.
Verbindungs-URL	URL von Kentik Instanz. Kentik URLs folgen diesem Format: `https://<your-resource-name>.api.kentik.com` .
Anwender-E-Mail	E-Mail-Adresse, die dem zugeordnet ist Kentik API-Token.
API-Token	Kentik API-Token.

5. Wählen Sie **Erstellen** aus.
   Ihre Verbindung wird in angezeigt **Verbindungen** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Aktivieren Sie Kentik Analyse-KI-Agent, um ihn im agentischen Workflow „Warnungsauswirkung analysieren“ zu verwenden. In KI-Agenten-Studio, Navigieren Sie zu Erstellen und verwalten , suchen Sie nach Kentik Analysieren Sie den KI-Agent, und aktivieren Sie den Agent in der Definieren Sie wichtige Anforderungen Bildschirm.

Hinweis: Während der Arbeit in KI-Agenten-Studio, Stellen Sie sicher, dass der KI-Agent für den Abruf von Warnungsinformationen aktiv ist. Sie ist auch für den agentischen Workflow „Warnungsauswirkung analysieren“ erforderlich.

Um mehr über die Verwendung von zu erfahren Kentik Analyse-KI-Agent im agentischen Workflow „Warnungsauswirkung analysieren“ finden Sie unter Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“.

Konfigurieren Sie den KI-Agent „New Relic Analysis“

Verbinden Sie mit New Relic Analyse-KI-Agent für Ihren New Relic Instanz, die im agentischen Workflow „Warnungsauswirkung analysieren“ verwendet werden soll. Nach der Verbindung sammelt der KI-Agent Informationen, um Sie bei der Untersuchung von Warnungen zu unterstützen.

Vorbereitungen

Vor der Konfiguration von New Relic Analyse-KI-Agent müssen Sie Folgendes tun:

- Installieren Now Assist für IT Operations Management (ITOM) an.
- Integrieren Sie New Relic mit Ereignismanagementan.
- Kopieren Sie Ihren New Relic API-Schlüssel.

  Die New Relic API-Schlüssel muss ein Anwenderschlüssel sein, auch als persönlicher API-Schlüssel bezeichnet.

Erforderliche Rolle: Connection_admin und credential_admin

Prozedur

1. Navigieren zu **Alle** > **sys_alias.LIST**an.
2. Suchen und wählen Sie aus *New Relic***Analyse-KI-Agent** .
3. Wählen Sie Aus **Neue Verbindung Und Anmeldeinformationen Erstellen** .
4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Verbindungsname	Name von New Relic Verbindung. Dieser Name hilft Ihnen, ihn später zu identifizieren. Beispiel: New Relic Prod.
Verbindungs-URL	URL von New Relic KI-API: `https://nrai-streaming.service.newrelic.com` . Die Verbindungs-URL kann je nach Region oder Account variieren.
API-Schlüssel	New Relic API-Schlüssel.
Header-Name	Headername für New Relic API-Schlüssel: `X-API-Schlüssel` . Ändern Sie diesen Wert, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	den Header für verschiedene APIs anzu–passen oder bestimmte Sicherheitsrichtlini–en zu befolgen.

5. Wählen Sie **Erstellen** aus.
   Ihre Verbindung wird in angezeigt **Verbindungen** Registerkarte.

Nächste Maßnahme

Aktivieren Sie New Relic Analyse-KI-Agent, um ihn im agentischen Workflow „Warnungsauswirkung analysieren“ zu verwenden. In KI-Agenten-Studio, Navigieren Sie zu Erstellen und verwalten , suchen Sie nach New Relic Analysieren Sie den KI-Agent, und aktivieren Sie den Agent in der Definieren Sie wichtige Anforderungen Bildschirm.

Hinweis: Während der Arbeit in KI-Agenten-Studio, Stellen Sie sicher, dass der KI-Agent für den Abruf von Warnungsinformationen aktiv ist. Sie ist auch für den agentischen Workflow „Warnungsauswirkung analysieren“ erforderlich.

Um mehr über die Verwendung von zu erfahren New Relic Analyse-KI-Agent im agentischen Workflow „Warnungsauswirkung analysieren“ finden Sie unter Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“.

Verwenden von Now Assist für IT Operations Management (ITOM)

Sie können verwenden ServiceNow® Now Assist für ITOM Anwendung zum Anzeigen von Warnungsanalysen, die Now Assist Erstellt mit generativer KI.

Warnungsanalysen umfassen visuell lesbare Beschreibungen der Warnung und zusätzliche technische Informationen, damit Sie die Warnung effektiver untersuchen können. Die Analysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

Weitere Informationen zu finden ServiceNow® Now Assist für IT Operations Management (ITOM) Anwendung, siehe Now Assist für IT Operations Management (ITOM).

Zeigen Sie eine Warnungsanalyse von an Now Assist In Service Operations-Arbeitsbereich

Zeigen Sie eine Warnungsanalyse von an Now Assist Für eine Warnung auf der Registerkarte Übersicht der Warnung in Service Operations-Arbeitsbereich. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, damit Sie die Warnung effektiver untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basiert, CMDB, Log Analytics, Gemischt, Und auf Netzwerkdatenverkehr basierende Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_Operator

Prozedur

1. Navigieren zu **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol ( ).
3. Wählen Sie in der Liste Warnungen die Option aus **Alle Warnungen** .
4. Wählen Sie eine Warnung aus.
   Die Warnung wird auf einer separaten Registerkarte geöffnet, auf der die untergeordnete Registerkarte **Übersicht** angezeigt wird.
5. In **Analyse** Abschnitt auswählen **Warnung analysieren** .
6. Überprüfen Sie die in der Warnungsanalyse bereitgestellten Informationen.

Hinweis: Warnungsanalysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

Zeigen Sie eine Warnungsanalyse von an Now Assist In Express-Liste

Zeigen Sie eine von erstellte Warnungsanalyse an Now Assist Generative KI verwenden. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, damit Sie die Warnung effektiver untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Hinweis: Derzeit Now Assist für ITOM Analysiert nur Tag-basiert, CMDB, Log Analytics, Gemischt, Und auf Netzwerkdatenverkehr basierende Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste die aus Express-Liste Symbol ( ).
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Neben der Warnung.
4. Im Vorschaubereich **Info** Wählen Sie die Registerkarte aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

Hinweis: Warnungsanalysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

6. **Wahlweise:** Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsanalysesymbole

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Zeigen Sie eine Warnungsgruppenanalyse nach an Now Assist In Express-Liste

Zeigen Sie eine von erstellte Warnungsgruppenanalyse an ServiceNow® Now Assist Generative KI verwenden. Die Analyse bietet eine vereinfachte, visuell lesbare Beschreibung der Warnungsgruppe und technische Informationen, damit Sie sie effizienter untersuchen können.

Vorbereitungen

Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.

Zeigen Sie wichtige Informationen zu an ServiceNow® Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie aus Express-Liste Symbol ( ) In der linken Navigationsleiste.
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Links neben einer Warnungsgruppe, um den Vorschaubereich anzuzeigen.
4. Wählen Sie auf der Registerkarte Info des Vorschaubereichs die Option aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden unabhängig von der in den Warnungsbeschreibungen verwendeten Sprache in Englisch bereitgestellt.

6. **Wahlweise:** Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Warnungsanalysesymbole

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbol	Beschreibung
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Zugehörige Informationen

Anzeigen einer Warnungsgruppenanalyse nach Now Assist In Express-Liste

Speichern Sie die Zusammenfassung der Warnungsanalyse nach Now Assist Als Warnungsgruppenbeschreibung in Express-Liste

Speichern Sie die visuell lesbare Zusammenfassung, die von generiert wurde Now Assist In der Warnungsanalyse als Beschreibung einer Warnungsgruppe.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie aus Express-Liste Symbol ( ) In der linken Navigationsleiste.
3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol ( ) Links neben einer Warnung.
4. Wählen Sie auf der Registerkarte Info des Vorschaubereichs die Option aus **Analysieren** In Warnungsanalyse von Now Assist.
5. Überprüfen Sie die visuell lesbare, KI-generierte Zusammenfassung der Warnungsanalyse.

   Hinweis: Warnungsanalysen werden unabhängig von der in der Warnungsbeschreibung verwendeten Sprache in Englisch bereitgestellt.

6. **Wahlweise:** Bearbeiten Sie den Zusammenfassungsinhalt.
7. Wählen Sie Aus **Speichern Sie die Beschreibung** Dient zum Speichern des Zusammenfassungsinhalts als Beschreibung der Warnungsgruppe.
   Der KI-generierte Zusammenfassungsinhalt ersetzt die ursprüngliche Beschreibung der Warnungsgruppe.

Generieren Sie in eine Warnungsgruppenbeschreibung Express-Liste Verwenden Now Assist

Verwenden Now Assist Dient zum Generieren einer aussagekräftigen Beschreibung einer Warnungsgruppe in Express-Liste Das umfasst alle Warnungen innerhalb der Gruppe. Die generierte Beschreibung ersetzt die ursprüngliche Beschreibung der Gruppe.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie aus Express-Liste Symbol ( ) In der Navigationsleiste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie in der Liste aktive Warnungen das Informationssymbol (ⓘ) Für eine Warnung.
4. Wählen Sie unter der angezeigten Warnungsgruppenbeschreibung aus **Aktualisieren Sie die Beschreibung** .
   Now Assist Generiert eine umfassende neue Beschreibung der Warnungsgruppe, die alle Warnungen innerhalb der Gruppe umfasst. Wenn Sie auswählen **Aktualisieren** , Die generierte Beschreibung ersetzt die ursprüngliche Beschreibung der Warnungsgruppe aus der frühesten, schwersten sekundären Warnung in der Gruppe.
5. **Wahlweise:** Stellen Sie die ursprüngliche Warnungsgruppenbeschreibung wieder her, indem Sie auf das Symbol „Zurücksetzen“ (⟲) Neben **Aktualisieren Sie die Beschreibung** Und dann auswählen **Wiederherstellen** .

Starten Sie eine Warnungsanalyse aus dem Now Assist Bereich

Initiieren Sie eine Warnungsanalyse aus dem Now Assist Bereich. Die Warnungsanalyse wird direkt in angezeigt Now Assist Bereich für bequeme Überprüfung.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an ServiceNow® Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Für umfassende Informationen über Now Assist Bereich, siehe Now Assist-Bereich .

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol (☰) In der Navigationsleiste.
3. Auswahlvorgang **Listen** > **Alerts** > **Alle Warnungen**an.
4. Initiieren Sie eine Warnungsanalyse aus dem Now Assist Bereich mit einer der verfügbaren Methoden.

Starten Sie eine Warnungsanalyse	Prozedur
Aus der Liste	**a.** Wählen Sie aus Now Assist Bereichssym–bol (✦). Die Now Assist Bereich wird angezeigt. **b.** Geben Sie eine Warnungsanalyseanfor–derung einschließlich der Warnungsnum–mer in das Feld unten im Bereich ein. **Hinweis:** Wenn Sie unvollständige In-formationen angeben, Now Assist Fordert Sie zur Eingabe der fehlenden Details auf. Die Warnungsanalyse wird im Bereich angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Starten Sie eine Warnungsanalyse	Prozedur
Aus einem Warnungsformular	**a.** Öffnen Sie eine Warnung. **b.** Wählen Sie aus Now Assist Bereichssym–bol (✦). Die Now Assist Bereich wird angezeigt. **c.** Wählen Sie Aus **Führen Sie eine War nungsanalyse durch** . Die Warnungsanalyse wird im Bereich angezeigt.

5. **Wahlweise:** Geben Sie Folgefragen oder -Anforderungen ein.
   Beispiel: Fassen Sie die Analyse zusammen Oder Warnungsschweregrad anzeigen .

Erstellen Sie einen Incident aus einer Warnung mit Now Assist In Express-Liste

Erstellen Sie einen Incident mit einer visuell lesbaren, KI-generierten Beschreibung aus der Express-Liste Bereich mit Now Assist.

Vorbereitungen

Derzeit ist diese Funktion für verfügbar CMDB, Log Analytics, Tag-basierte und komponentenbasierte Warnungen.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie aus Express-Liste Symbol ( ) In der linken Navigationsleiste.
3. Erstellen Sie einen Incident aus einer ausgewählten Warnung.

   a. In Express-Liste Wählen Sie die Warnung aus.

   Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Chevron-Symbol (›) Am Anfang der Warnungsgruppenzeile.

   b. Von **Schließen** Wählen Sie in der Dropdown-Liste unter Korrekturaktionen die Option aus **Incident mit Now Assist erstellen** .

   Aus der ausgewählten Warnung wird ein Incident mit einer visuell lesbaren, KI-generierten Beschreibung erstellt, und eine Bestätigungsmeldung wird angezeigt.

4. **Wahlweise:** Zeigen Sie den erstellten Incident an, indem Sie auswählen **Incident anzeigen** In der Bestätigungsnachricht oder im Warnungsvorschaubereich.

Beschleunigen Sie die Warnungslösung mit Now Assist Analyse vergangener zugehöriger Incidents

Verwenden Now Assist Um relevante vergangene Incidents zu untersuchen und effektive Strategien zu ihrer Lösung zu präsentieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist Fragt Verlaufsdatensätze ab, um vergangene Incidents zu finden, und analysiert ihre Häufigkeit, Relevanz, Arbeitsnotizen und Lösung. Es wird eine Zusammenfassung der relevantesten zugehörigen Incidents in angezeigt Now Assist Bereich. Die Zusammenfassung enthält verwendete Lösungsstrategien sowie Kontaktdetails für Einzelpersonen oder Teams, die die Incidents gelöst haben und bei der aktuellen Warnung helfen könnten. Die bereitgestellten Informationen helfen Ihnen, den Kontext und die Bedeutung der aktuellen Warnung besser zu verstehen und effizienter an ihrer Lösung zu arbeiten.

Hinweis: Der KI-Suchfunktion wird eine zusätzliche Validierungsebene für großes Sprachmodell (LLM) hinzugefügt, um die Genauigkeit der Ergebnisse zu verbessern, die von KI-Kompetenzen zurückgegeben werden.

Generieren Sie einen Now Assist Zusammenfassung vergangener zugehöriger Incidents

Zeigen Sie ein an Now Assist Zusammenfassung vergangener Incidents für dieselben oder zugehörigen Konfigurationselemente (Configuration Items, CIs) und Strategien, die zu ihrer Lösung verwendet wurden.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in Now Assist Funktion. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Stellen Sie sicher, dass die Kompetenz „Warnungsuntersuchung“ aktiv ist. Weitere Informationen finden Sie unter Installieren Sie Now Assist Für IT Operations Management(ITOM)-Plugin.
- Zeigen Sie wichtige Informationen zu an ServiceNow® Now Assist für IT Operations Management (ITOM) Anwendung in Now Assist für IT Operations Management (ITOM).

Für umfassende Informationen über Now Assist Bereich, siehe Now Assist-Bereich .

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie das Listensymbol ( ) In der Navigationsleiste.
3. Auswahlvorgang **Listen** > **Alerts** > **Alle Warnungen**an.
4. Öffnen Sie eine Warnung.
5. Wählen Sie aus Now Assist Bereichssymbol ( ).
   Die Now Assist Bereich wird angezeigt.
6. Fordern Sie ein an Now Assist Untersuchung vergangener Incidents durch Auswahl **Analysieren Sie zugehörige Incidents** .
   Der KI-Suchfunktion wird eine zusätzliche Validierungsebene für großes Sprachmodell (LLM) hinzugefügt, um die Genauigkeit der Ergebnisse zu verbessern, die von KI-Kompetenzen zurückgegeben werden.
   Eine Zusammenfassung der relevantesten zugehörigen Incidents wird im Bereich angezeigt.
7. **Wahlweise:** Überprüfen Sie die Details eines zugehörigen Incidents, indem Sie den entsprechenden Link unter zugehörige Incidents auswählen.
   Die Incident-Seite wird geöffnet und zeigt die Registerkarte Übersicht an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit agentischen Workflows in Now Assist für IT Operations Management (ITOM)

Verwenden Sie IT Operations Management(ITOM) Agentische Workflows zum autonomen Abschließen von Aufgaben.

Verfügbare agentische Workflows für ITOM KI-Agent-Sammlung

Name des Agentischen Workflows	Beschreibung	Verfügbare KI-Agents
Warnungen selektieren und analysieren	Selektiert Warnungen, indem Zuweisungen aktualisiert, Warnungen analysiert, wiederkehrende Muster erkannt und zwischen Rauschen und echten Warnungen unterschieden wird.	• Umgang mit Warnungen – KI-Agent • KI-Agent für die Warnungsanalyse • KI-Agent zur Analyse des Warnungsverlaufs • KI-Agent für die Analyse zugehöriger Incidents • KI-Agent zur Warnungsverifizierung
Warnungsauswirkungen analysieren	Untersucht eine Warnung und gibt Ihnen den Kontext, den Sie benötigen, um effizient zu reagieren.	• KI-Agent für den Abruf von Warnungsinformationen • KI-Agent für die Überprüfung der Warnungsauswirkung • Business and Technology Management Service Impact Analysis KI-Agent • Dynatrace Analyse-KI-Agent • Kentik Analyse-KI-Agent • New Relic Analyse-KI-Agent • Auswirkungsanalyse der Serviceinstanz – KI-Agent • KI-Agent für Anwenderauswirkungsanalyse
Analysieren Sie potenzielle Auswirkungen	Analysiert die potenziellen Auswirkungen einer Change-Anforderung auf relevante Server und vorgeschlagene Services.	Analysieren Sie Potenzielle Auswirkungen
TLS-Zertifikatverlängerung	Zeigen Sie alle Zertifikate an, die ablaufen und verlängern sollen, und dann automatisch alle gleichzeitig.	

Wichtig: Standardmäßig sind alle agentischen Anwendungsfall-Workflows und KI-Agent-Datensätze schreibgeschützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KI-Modellanbieter

Sie können verwenden Now LLM Service, Azure OpenAI, Google Gemini Oder Anthropic Claude auf AWS Als KI-Modellanbieter für alle Now Assist Kompetenzen und KI-Agenten. Verwenden Sie die Konfigurationssteuerungen in KI-Governance Um zu definieren, welche Optionen verfügbar sind, legen Sie dann die Einstellungen auf Kompetenzebene in fest Now Assist-Administrator Konsole an. Weitere Informationen finden Sie unter Große Sprachmodelle auf der ServiceNow AI Platform® .

Sicherheit

Aktivieren Sie Sicherheitseinstellungen, um KI-Agents und agentische Workflows mithilfe von Zugriffssteuerungslisten (ACLs) und Anwenderidentitäten auszuführen. Sie können die ACLs in konfigurieren und verwalten KI-Agenten-Studio. Weitere Informationen finden Sie unter Implementieren Sie die Zugriffssteuerung für Sicherheit in KI-Agents .

Installierte Agents

Suchen Sie nach einem KI-Agenten?

- Möglicherweise sind KI-Agenten mit installiert Now Assist Anwendung, die nicht in Agenten-Workflows verwendet wird. Informationen zum Anzeigen aller in Ihrer Instanz verfügbaren Agenten finden Sie unter Suchen Sie KI-Agenten .
- Um Agenten zu finden, die möglicherweise nicht auf Ihrer Instanz installiert sind, besuchen Sie die KI-Agent-Marketplace Auf ServiceNow Store.

Besuchen Sie die folgenden Links, um mehr über zu erfahren Now Assist für ITOM Agentische Workflows.

Selektieren und analysieren Sie Warnungen – agentischer Workflow

Verwenden Sie den agentischen Workflow „Selektierung und Warnungen analysieren“, um vorläufige Warnungsaufgaben und Analysen abzuschließen Für Warnungen .

Selektierung und Analyse von Warnungen – Übersicht über den agentischen Workflow

Der agentische Workflow „Selektierung und Warnungen analysieren“ verwendet KI-Agents, um die Selektierung, Untersuchung und Analyse von Warnungen zu unterstützen. KI-Agents können die folgenden Funktionen ausführen:

- Warnungen bestätigen.
- Weisen Sie einzelnen Anwendern und Zuweisungsgruppen Warnungen zu.
- Fassen Sie Warnungs- und Warnungsgruppendaten zusammen, um eine visuell lesbare Beschreibung zu erstellen und technische Analysen hinzuzufügen.
- Untersuchen Sie relevante vergangene Incidents, um die Bedeutung der Warnung zu analysieren und Lösungsoptionen anzubieten.

Hinweis: Diese Funktionen können auch für die Ursprungswarnung eines Incident verwendet werden, wenn über das Incident-Formular oder auf den Workflow zugegriffen wird Express-Liste Mit Now Assist Bereich.

Verwenden Sie die Informationen auf dieser Seite, um mehr über die Service Desk-Mitarbeiter im Zusammenhang mit dem agentischen Workflow „Selektierung und Warnungen analysieren“ zu erfahren. Um den agentischen Workflow „Selektierung und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen analysieren“ zu ändern, müssen Sie ihn duplizieren und die Einstellungen entsprechend Ihren Anforderungen anpassen. Weitere Informationen finden Sie unter Duplizieren Sie einen agentischen Workflow .

Wichtig: Wenn Sie einen agentischen Workflow, einen KI-Agent oder ein Tool ändern, stellen Sie sicher, dass Sie alle Anweisungen entsprechend aktualisieren.

Selektieren und analysieren Sie Warnungen – agentischer Workflow

Bestätigen, weisen Sie aktuelle und vergangene Warnungen zu, und untersuchen Sie sie, um die Bedeutung und mögliche Lösungen zu bestimmen.

Um auf den agentischen Workflow zuzugreifen, verwenden Sie Now Assist Bereich. Weitere Informationen zur Verwendung des agentischen Workflows in finden Sie Now Assist Bereich, siehe Now Assist-Bereich .

KI-Agents, die im agentischen Workflow „Selektierung und Analyse von Warnungen“ verwendet werden

Der agentische Workflow „Selektierung und Warnungen analysieren“ verwendet ein Team von KI-Agents, um vorläufige Aufgaben auszuführen und die Lösung von Warnungen zu unterstützen.

KI-Agents, die im agentischen Workflow „Selektierung und Analyse von Warnungen“ verwendet werden

KI-Agent	KI-Agent-Rolle
KI-Agent für den Umgang mit Warnungen	Weisen Sie einen aktuellen Warnungsdatensatz zu, bestätigen Sie ihn, und verwalten Sie ihn.
KI-Agent für die Warnungsanalyse	Führen Sie eine Warnungsanalyse durch, und aktualisieren Sie gegebenenfalls die Warnungsbeschreibung.
KI-Agent zur Analyse des Warnungsverlaufs	Analysieren Sie frühere Vorkommen, bewerten Sie ihre Bedeutung, und schließen Sie die Warnung, falls zutreffend.
KI-Agent für die Analyse zugehöriger Incidents	Analysieren Sie vergangene Incidents, und geben Sie Einblicke in allgemeine Zuweisungen und zusammengefasste Lösungshinweise.
KI-Agent zur Warnungsverifizierung	Bewerten Sie die Vollständigkeit der Daten, und bestimmen Sie, ob die Warnung für die Analyse geeignet ist.

Analysieren Sie den agentischen Workflow für Warnungsauswirkungen

Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“, um eine Warnung zu untersuchen und den Kontext abzurufen, den Sie benötigen, um effizient zu reagieren.

Übersicht über den agentischen Workflow für Warnungsauswirkungen analysieren

Der agentische Workflow „Warnungsauswirkung analysieren“ verwendet KI-Agents, um mit Erkennbarkeitstools zu interagieren, z. B. Dynatrace, Kentik, Und New Relic. Sie enthält auch AIOps-KI-Agents, die Service, Anwender und Geschäftsauswirkungen analysieren. Zusammen zeigen die Service Desk-Mitarbeiter Informationen an, die Ihnen bei Folgendem helfen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Machen Sie sich mit dem Schweregrad und den Auswirkungen von Warnungen vertraut.
- Suchen Sie mithilfe von Einblicken potenzielle Ursachen, z. B. aktuelle Bereitstellungen.
- Identifizieren Sie den Besitz, indem Sie relevante Services und verantwortliche Teams aufzeigen.
- Unterstützen Sie die Kommunikation mit Stakeholdern mit klaren, umsetzbaren Informationen.

Verwenden Sie die Informationen auf dieser Seite, um mehr über die Service Desk-Mitarbeiter im Zusammenhang mit dem agentischen Workflow „Warnungsauswirkung analysieren“ zu erfahren. So ändern Sie den agentischen Workflow „Warnungsauswirkung analysieren“: Duplizieren Sie es Und passen Sie die Einstellungen an.

Wichtig: Wenn Sie einen agentischen Workflow, einen KI-Agent oder ein Tool ändern, stellen Sie sicher, dass Sie alle Anweisungen entsprechend aktualisieren.

Analysieren Sie den agentischen Workflow für Warnungsauswirkungen

Untersuchen Sie eine Warnung, und erhalten Sie Einblicke in ihren Schweregrad, Geschäft und Service Auswirkung, Besitz und Ursachen.

Um in auf den agentischen Workflow zuzugreifen KI-Agenten-Studio:

1. Navigieren zu **Alle** > **KI-Agenten-Studio** > **Erstellen und verwalten**an.
2. Wählen Sie Aus **Analysieren Sie die Auswirkung der Warnung** .

Auf der Seite „Auswirkung auf Warnungen analysieren“ können Sie den agentischen Workflow verwalten, einschließlich der Definition wichtiger Anforderungen, des Hinzufügen eines bevorzugten Auslösers und der Auswahl einer UI-Anzeige. Navigieren Sie zu Wählen Sie eine UI-Anzeige aus Dient zum Aktivieren des agentischen Workflows in Now Assist Bereich.

KI-Agents, die im agentischen Workflow „Warnungsauswirkung analysieren“ verwendet werden

Der agentische Workflow „Warnungsauswirkung analysieren“ verwendet AIOps und KI-Agents für Observability, um Informationen aus Warnungen zu sammeln und Einblicke anzufordern. Nur die AI-Agents für Observability erfordern eine zusätzliche Konfiguration. Weitere Informationen finden Sie unter KI-Agents für konfigurieren Now Assist für ITOM.

Wichtig: Aktivieren Sie die zugehörigen KI-Agents, bevor Sie den agentischen Workflow „Warnungsauswirkung analysieren“ verwenden. In KI-Agenten-Studio, Suchen Sie die KI-Agents in Erstellen und verwalten, und aktivieren Sie die KI-Agents in Bildschirm „wichtige Anforderungen definieren“ .

KI-Agents und ihre Rollen

KI-Agent	KI-Agent-Rolle
KI-Agent für die Überprüfung der Warnungsauswirkung	Validiert Ihre Frage und extrahiert eine einzelne Warnung zur Analyse.
KI-Agent für den Abruf von Warnungsinformationen	Sammelt wichtige Erkennbarkeitsdetails für eine bestimmte Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KI-Agents und ihre Rollen (Fortsetzung)

KI-Agent	KI-Agent-Rolle
Business and Technology Management Service Impact Analysis KI-Agent	Analysiert die Auswirkungen, indem Anwendungsservices mit geschäftlichen und technischen Services anhand von Service-Portfoliodaten zugeordnet werden.
Dynatrace Analyse-KI-Agent	Sammelt Einblicke von Dynatrace Informationen zu möglichen Ursachen, betroffenen Entitäten und betroffenen Umgebungen.
Kentik Analyse-KI-Agent	Sammelt Einblicke von Kentik Informationen zu Leistung, Konnektivität, DDOS-Angriffen und Anomalien des Servicenetzwerks.
New Relic Analyse-KI-Agent	Sammelt Einblicke von New Relic Informationen zu Warnungsauswirkungen, einschließlich Service- und Anwenderauswirkungen, Ursachentheorien und verantwortliche Teams.
Auswirkungsanalyse der Serviceinstanz – KI-Agent	Analysiert, wie sich die Warnung auf die zugehörige Serviceinstanz auswirkt.
KI-Agent für Anwenderauswirkungsanalyse	Identifiziert Probleme im Zusammenhang mit den betroffenen Services und bietet dem Anwender eine zusammengefasste Übersicht.

Warnungsanalyse wird generiert

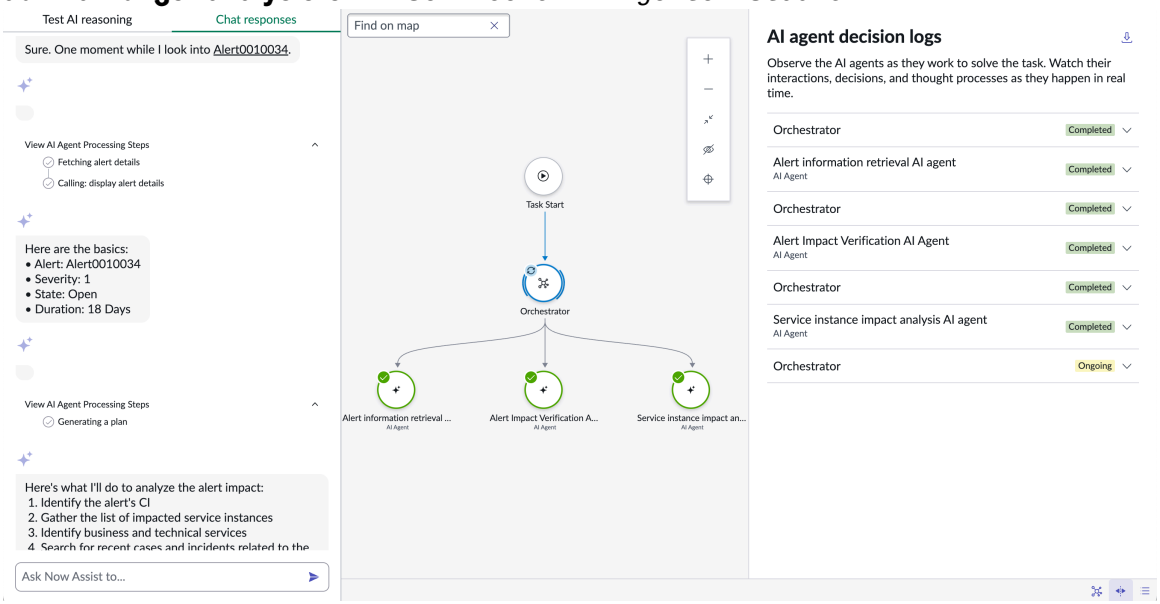
Im Datensatz des agentischen Workflows:

1. Überprüfen Sie die Informationen auf dem Bildschirm Schlüsselanforderungen beschreiben und einen bevorzugten Auslöser hinzufügen, nehmen Sie die erforderlichen Aktualisierungen vor, und wählen Sie dann aus **Fahren Sie Fort** .
2. Im Bildschirm UI auswählen:
   a. Aktivieren Sie die Anzeige des Now Assist-Bereichs.
   b. Wählen Sie Aus **Speichern und testen** .
3. Testen Sie den agentischen Workflow, indem Sie z. B. eine Frage stellen: `Welche Auswirkungen hat Alert0010007?`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie Aus **Test starten** .

Beispiel für die Ausgabe des agentischen Workflows „Auswirkung auf Warnungen analysieren“ in *ServiceNow KI-Agenten-Studio*



In *KI-Agenten-Studio*, Sie werden benachrichtigt, wenn die Analyse generiert wird. Sie können dann anhand der Informationen handeln oder weitere Fragen zur Warnung stellen. Weitere Informationen zur Verwendung des agentischen Workflows in finden Sie Now Assist Bereich, siehe Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“.

Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“

Erfahren Sie, wie Sie den agentischen Workflow „Warnungsauswirkung analysieren“ in verwenden Now Assist Bereich. Der agentische Workflow hilft Ihnen, eine Warnung zu untersuchen und den Kontext zu erhalten, den Sie benötigen, um effizient zu reagieren.

Vorbereitungen
Bevor Sie den agentischen Workflow „Warnungsauswirkung analysieren“ verwenden, müssen Sie haben Now Assist für IT Operations Management (ITOM) Auf Ihrer Instanz installiert. Weitere Informationen zur Installation von finden Sie Now Assist Plugins, siehe Now Assist-Plugins installieren .

Sie müssen auch Folgendes tun:

- Aktivieren Sie den agentischen Workflow „Warnungsauswirkung analysieren“ im Now Assist Bereich. Weitere Informationen finden Sie unter Analysieren Sie den agentischen Workflow für Warnungsauswirkungen.
- Konfigurieren und aktivieren Sie KI-Agents für die Observability-Tools, die Sie in integriert haben Ereignismanagement, Z. B. Dynatrace, Kentik, Oder New Relic. Weitere Informationen finden Sie unter KI-Agents für konfigurieren Now Assist für ITOM.

Hinweis: Das folgende Verfahren zeigt die Verwendung von Now Assist Bereich für den agentischen Workflow „Warnungsauswirkung analysieren“. Allgemeine Anleitungen zur Verwendung von Now Assist Bereich, siehe Now Assist-Bereich .

Erforderliche Rolle: evt_mgmt_operator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**an.
2. Wählen Sie in der Navigationsleiste das Express-Listensymbol aus: .
3. Wählen Sie eine Warnung aus.
4. Öffnen Sie den Bereich, indem Sie auswählen Now Assist Symbol ( ).
5. Fragen Sie Now Assist Eine Frage zur Warnung.

Option	Beschreibung
Fragen Sie nach Impact	Ruft eine Zusammenfassung der betroffenen Services und Anwender ab. Schließen Sie das Wort ein Auswirkung In Ihrer Frage. Beispiel: Welche Auswirkungen hat diese Warnung? Oder Wie hoch ist die Auswirkungsstufe dieser Warnung? . Wenn die Warnungsquelle ein Erkennbarkeitstool ist, z. B. Kentik, Now Assist Enthält auch relevante Informationen aus diesem Tool in die Antwort.
Stellen Sie eine toolspezifische Frage	Erhalten Sie detaillierte Einblicke in die Warnung vom relevanten Erkennbarkeitstool. Beispiel: Für New Relic Warnungen können Sie fragen Gab es letzte Bereitstellungen für diese Warnung? . Siehe Fragen für den agentischen Workflow „Warnungsauswirkung analysieren“ Für die Liste der verfügbaren Fragen.

Now Assist Verwendet die relevanten KI-Agents, um Ihre Frage zu analysieren und mit einer Zusammenfassung oder einem Einblick zu antworten. Die erste Antwort für eine Warnung kann einige Sekunden dauern, bis sie angezeigt wird.

Nächste Maßnahme

Verwenden Sie die Informationen, die Sie erhalten haben, um die Auswirkung der Warnung zu verstehen und entsprechend zu reagieren. Sie können auch weitere Fragen zur Warnung stellen.

Hinweis: Ihre Konversation in Now Assist Der Bereich ist spezifisch für die Warnung, die Sie in Schritt 2 ausgewählt haben. Um nach einer anderen Warnung zu fragen, öffnen Sie diese Warnung, und wählen Sie aus Now Assist Symbol ( ), um eine neue Konversation zu beginnen.

Analysieren Sie den agentischen Workflow für potenzielle Auswirkungen

Der agentische Workflow „potenzielle Auswirkung analysieren“ analysiert, wie sich eine Change-Anforderung auf Server und vorgeschlagene Services auswirken kann. Diese Analyse hilft Ihnen, fundierte Entscheidungen über die nächsten Schritte in Bezug auf die Change-Anforderung zu treffen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analysieren Sie die Übersicht über den agentischen Workflow für potenzielle Auswirkungen

Mithilfe des agentischen Workflows „potenzielle Auswirkungen analysieren“ erstellt der Agent „potenzielle Auswirkungen analysieren“ eine Analyse potenziell betroffener relevanter Server und vorgeschlagene Services.

Hinweis: Relevante Server beziehen sich auf die Server, die derzeit betriebsbereit und in Gebrauch sind, mit Ausnahme nicht funktionsfähiger oder stillgelegter Server.

KI-Agent, der im agentischen Workflow „potenzielle Auswirkungen analysieren“ verwendet wird

KI-Agent und seine Rolle

KI-Agent	KI-Agent-Rolle
Analysieren Sie Potenzielle Impact-Mitarbeiter	Verwendet die Change-Anforderung, um die potenziellen Auswirkungen des Change auf relevante Server und vorgeschlagene Services zu analysieren.

Auswirkungsanalyse wird generiert

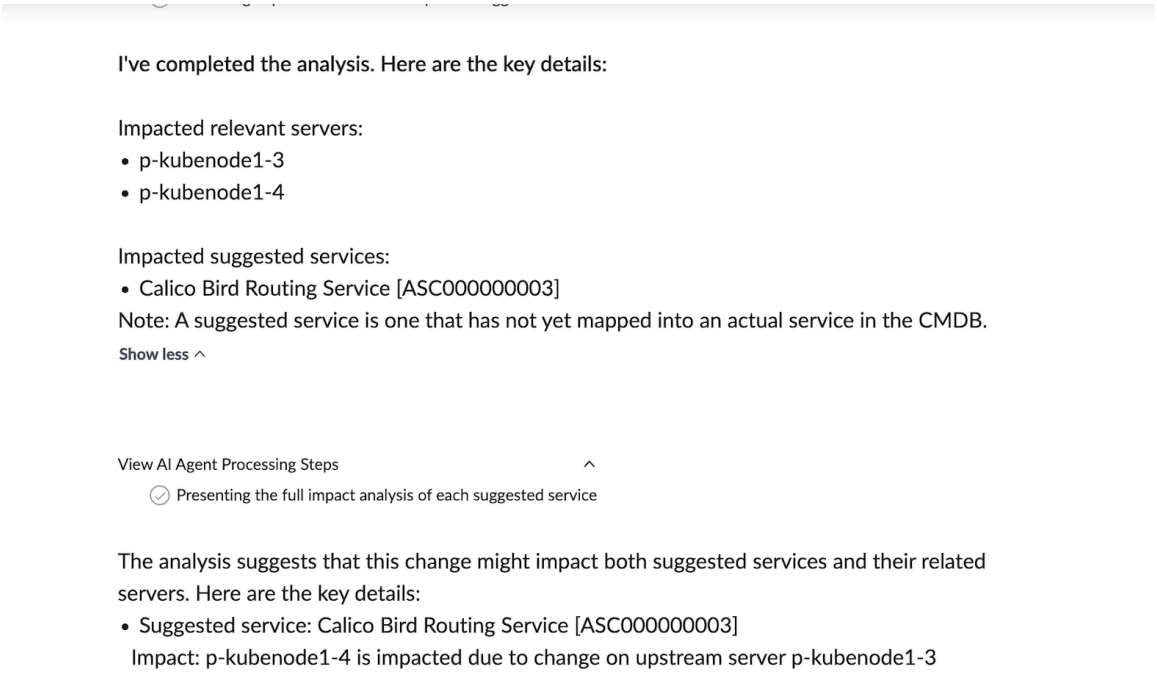
Der agentische Workflow „potenzielle Auswirkung analysieren“ in Now Assist Verwendet einen einzelnen Service Desk-Mitarbeiter, um die potenziellen Auswirkungen einer Change-Anforderung zu bewerten. Wenn Sie im den Agent potenzielle Auswirkung analysieren auswählen Now Assist Wird der Workflow wie folgt initiiert:

- **Erforderliche Verifizierung** – Der Service Desk-Mitarbeiter überprüft zuerst, ob alle Voraussetzungen erfüllt wurden.
- **Identifizierung der Change-Anforderung** – Wenn Sie eine Change-Anforderung geöffnet haben, ruft der Service Desk-Mitarbeiter die Nummer der Change-Anforderung von der aktuell aktiven Seite ab. Andernfalls werden Sie aufgefordert, die Nummer der Change-Anforderung anzugeben.
- **Serverauswahl** – Der Service Desk-Mitarbeiter wählt bis zu 10 betroffene Server aus den betroffenen Konfigurationselementen (CIs) in der Change-Anforderung aus.
- **Identifikation abgleichen** – Der Service Desk-Mitarbeiter identifiziert Übereinstimmungen zwischen Servern und vorgeschlagenen Services.
- **Auswirkungsanalyse** – Schließlich priorisiert und zeigt der Service Desk-Mitarbeiter bis zu 10 betroffene relevante Server an, wobei Server, die Teil der vorgeschlagenen Services sind, und bis zu 3 betroffene vorgeschlagene Services Priorität erhalten. Darüber hinaus bietet Ihnen der Service Desk-Mitarbeiter eine Zusammenfassung über jeden vorgeschlagenen Service und darüber, wie er von zugehörigen Servern betroffen sein könnte. Diese Informationen werden in angezeigt Now Assist Bereich.
- **Auswirkungsanalyse wird gespeichert** – Die vom agentischen Workflow „potenzielle Auswirkungen analysieren“ generierte Analyse wird in den Arbeitsnotizen der Change-Anforderung gespeichert.

Weitere Informationen zur Verwendung des Workflows finden Sie unter Verwenden Sie den agentischen Workflow potenzielle Auswirkungen analysieren, um eine Change-Anforderung zu bewerten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für die Analyse aus dem agentischen Workflow „potenzielle Auswirkung analysieren“



Domänentrennung

Derzeit unterstützt der agentische Workflow potenzielle Auswirkungen analysieren keine Instanzen mit Domänentrennung. Führen Sie alle Konversationen auf Englisch durch, um optimale Ergebnisse zu erzielen.

Verwenden Sie den agentischen Workflow potenzielle Auswirkungen analysieren, um eine Change-Anforderung zu bewerten

Verwenden Sie den agentischen Workflow potenzielle Auswirkungen analysieren, um die Auswirkungen einer Change-Anforderung zu bewerten. Dieser Workflow hebt die potenziell betroffenen Server und vorgeschlagenen Services hervor, damit Sie Risiken und Vorteile identifizieren und erforderliche Anpassungen vornehmen können.

Vorbereitungen
Die Verwendung des agentischen Workflows „potenzielle Auswirkungen analysieren“ erfordert die Installation von:

- Service-Mapping Plus Version 1.16.3.
- Now Assist für IT Operations Management (ITOM) Version 2,3.0.
- Now Assist für ITSM Version 11.1,3.

Erforderliche Rolle: sn_Change_write

Warum und wann dieser Vorgang ausgeführt wird
Der Service Desk-Mitarbeiter überprüft die Voraussetzungen zu Beginn des agentischen Workflows. Wenn Voraussetzungen nicht erfüllt sind, wird der Workflow beendet, und Sie werden informiert, damit Sie die Voraussetzungen erwerben können. Weitere Informationen zum agentischen Workflow finden Sie unter Analysieren Sie den agentischen Workflow für potenzielle Auswirkungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

Initiieren Sie entweder den agentischen Workflow potenzielle Auswirkungen analysieren mithilfe einer Change-Anforderungsnummer oder über eine offene Change-Anforderung.

Situation	Schritte
Nummer der Change-Anforderung ist bekannt	**a.** Wählen Sie im Header-Menü die Opti–on aus Now Assist Symbol Um zu öffnen Now Assist Bereich. **b.** Wählen Sie Aus **Analysieren Sie Potenziel le Auswirkungen** . **c.** Geben Sie bei Aufforderung die Nummer der Change-Anforderung ein.
Öffnen Sie die Change-Anforderung	**a.** Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** > **an.** **b.** Wählen Sie das Listensymbol aus . **c.** Navigieren zu **Changes** > **Alle**an. **d.** Wählen Sie die entsprechende Chan–ge-Anforderung aus der Liste aus. **e.** Wählen Sie im Header-Menü die Opti–on aus Now Assist Symbol Um zu öffnen Now Assist Bereich. **f.** Wählen Sie Aus **Analysieren Sie Potenziel le Auswirkungen** .

Der agentische Workflow potenzielle Auswirkungen analysieren wird initiiert, und der Service Desk-Mitarbeiter beginnt mit der Verifizierung der Voraussetzungen.

Ergebnis

In Now Assist Im Bereich generiert der agentische Workflow potenzielle Auswirkungen analysieren eine Analyse der potenziell betroffenen relevanten Server und vorgeschlagenen Services.

Now Assist KI-Agent für Zertifikatverlängerung

Mit Now Assist Zertifikatverlängerung KI-Agent, sehen Sie, welche Zertifikate bald ablaufen, und verlängern Sie sie. Wählen Sie ein bestimmtes Zertifikat aus, und verlängern Sie es vor Ort.

Verwenden Sie den KI-Agent für Now Assist-Zertifikatverlängerung, um Zertifikate automatisch zu verlängern, bevor sie ablaufen. Mit dem KI-Agent für die Now Assist-Zertifikatverlängerung können Sie Folgendes ausführen:

- Verlängern Sie ein einzelnes Zertifikat
- Suchen Sie nach allen Zertifikaten, die kurz vor dem Ablauf stehen
- Verlängern Sie alle Zertifikate, die kurz vor dem Ablauf stehen, in einem einzigen Prompt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie müssen zuerst Ihr System für die automatische Verlängerung konfigurieren. Die Konfiguration erfordert zwei Schritte:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server

Erkennen und verlängern Sie Zertifikate, die mit ablaufen sollen Now Assist

Verwenden Now Assist Um herauszufinden, welche Zertifikate an einem bestimmten Datum oder innerhalb eines bestimmten Datumsbereichs ablaufen. Now Assist Erstellt eine eindeutige Zertifikatliste dieser Zertifikate und fordert Sie auf, sie mit einem einzigen Klick zu verlängern.

Vorbereitungen

Führen Sie die folgenden Schritte aus, um Ihr System für zu konfigurieren Now Assist KI-Agent für Zertifikatverlängerung:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server

Erforderliche Rolle: sn_Disco_certmgmt.pki_admin

Prozedur

1. Navigieren zu **Alle** > **Eindeutige Zertifikate**an.
2. Wählen Sie aus Now Assist Symbol.
3. Geben Sie „Zertifikate abrufen, die zwischen dem 1. Mai 2026 und dem 1. August 2026 ablaufen“ ein. an.

   Hinweis: Sie können einen beliebigen Datumsbereich auswählen, den Sie benötigen.

4. Wählen Sie aus **Zertifikate** Link Now Assist Gibt zurück.

Ergebnis

Now Assist Leitet Sie zu einer Liste von Zertifikaten weiter, die zwischen dem 1. Mai 2026 und dem 1. August 2026 ablaufen. Now Assist Fragt Sie dann, ob Sie diese Zertifikate verlängern möchten. Verlängern Sie sie alle gleichzeitig, indem Sie „Ja“ auswählen.

Verlängern Sie automatisch ein Zertifikat mit Now Assist KI-Agent

Verlängern Sie automatisch ein einzelnes Zertifikat mit Now Assist KI-Agent für Zertifikatverlängerung.

Vorbereitungen

Führen Sie die folgenden Schritte aus, um Ihr System für zu konfigurieren Now Assist KI-Agent für Zertifikatverlängerung:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server

Erforderliche Rolle: sn_Disco_certmgmt.pki_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Navigieren Sie zu dem Zertifikat, das Sie verlängern möchten, und verwenden Sie Now Assist Zertifikatverlängerung – KI-Agent zum verlängern des Zertifikats.

Prozedur
1. Navigieren zu **Alle** > **Eindeutige Zertifikate**an.
2. Wählen Sie das Zertifikat aus, das Sie verlängern möchten.
3. Wählen Sie aus Now Assist Schaltfläche.

> ⚠ **Warnung:** Stellen Sie sicher, dass Sie sich im befinden **Eindeutiges Zertifikat** Seite des Zertifikats, das Sie verlängern möchten.

4. Geben Sie den Prompt „dieses Zertifikat verlängern“ ein.
5. Beantworten Sie die Fragen Now Assist Fragt Sie.

Ergebnis
Now Assist Informiert Sie über den Fortschritt bei der Verlängerung Ihres Zertifikats. Der KI-Agent für die Zertifikatverlängerung gibt Ihnen einen Link zum Anzeigen von **Aufgabendatensatz** Zeigt den Status des verlängerten Zertifikats an.

Verwenden Now Assist Um einen Zertifikatsatz zur manuellen Verlängerung zu verlängern

Einige Zertifikate sind so festgelegt, dass sie manuell verlängert werden. Verwenden Sie Now Assist Zertifikatverlängerung KI-Agent, um diese Zertifikate sofort zu verlängern.

Vorbereitungen
Führen Sie die folgenden Schritte aus, um Ihr System für zu konfigurieren Now Assist KI-Agent für Zertifikatverlängerung:

1. Konfigurieren Sie Ihren MID-Server Für automatische Zertifikatverlängerung
2. Fügen Sie die erforderlichen Anwendungen und Fähigkeiten zu hinzu MID-Server

Erforderliche Rolle: sn_Disco_certmgmt.pki_admin

Warum und wann dieser Vorgang ausgeführt wird
Suchen Sie nach Aufgaben, die erfordern, dass Sie Ihre Zertifikate manuell verlängern und sofort mit verlängern müssen Now Assist Agent für KI-Zertifikatverlängerung.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Zertifikatverwaltung**an.
2. Wählen Sie Aus **Aufgaben** .
3. Wählen Sie im aus **Verlängerungsaufgaben** Bereich, die Anzahl der Verlängerungsaufgaben.
4. Wählen Sie aus **Nummer** Der Verlängerungsaufgabe, die Sie automatisch verlängern möchten.
5. Wählen Sie aus Symbol in **Eindeutiges Zertifikat** Feld.

> **Hinweis:** Durch Auswahl des Symbols wird der Datensatz des Zertifikats geöffnet.

6. Wählen Sie Ihr aus Now Assist KI-Tool.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie „dieses Zertifikat verlängern“ in das Eingabeaufforderungsfeld von ein Now Assist.
8. Beantworten Sie die Fragen Now Assist Gibt Ihnen.

Ergebnis
Das Zertifikat wird von verlängert Now Assist Agent für KI-Zertifikatverlängerung.

Now Assist für IT Operations Management (ITOM) – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von Now Assist für ITOM Anwendung.

Mit Now Assist für ITOM installierte Anwendungen

Tabelle, in der Anwendungen aufgelistet werden, die mit installiert sind Now Assist für IT Operations Management (ITOM) Anwendung. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Mit installierte Anwendungen Now Assist für ITOM(sn_itom_gen_ai)

Anwendungsname	Beschreibung
Now Assist für Plattform (sn_genai_Platform)	Aktiviert Now Assist-Kompetenzen und -Funktionen in verschiedenen BU-Anwendungen.
KI-Agents für AIOps (sn_aiops_ai_Agents)	Ermöglicht IT-Vorgänge mit KI-Service Desk-Mitarbeitern, die helfen können, Warnungen autonom zu selektieren, geschäftliche und technische Auswirkungen zu bewerten, die Ursachen zu untersuchen und Korrekturschritte zu empfehlen oder auszuführen. Diese Service Desk-Mitarbeiter arbeiten innerhalb koordinierter agentischer Workflows.
KI-Agents für Observability (sn_obs_aia)	Hilft IT-Betreibern, die Auswirkungen auf Geschäfts- und Anwendungsservices zu bewerten und Theorien wahrscheinlicher Ursachen zu formulieren. Hilft bei der Priorisierung von Untersuchungen durch die Analyse von Daten aus ServiceNow und die Zusammenarbeit mit KI-Agents von Drittanbietern führender APM- und Erkennbarkeitsanbieter.
AIOps-LEAP (sn_itom_LEAP)	AIOps LEAP (Learning-Enhanced Automation Playbook) nutzt KI-gesteuerte Einblicke, um historische Incident-Daten zu extrahieren, Aufgaben dynamisch zu priorisieren und Playbooks für umsetzbare Lösungen zu generieren.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit aktivierte Plugins ITOM-Optimierung

Fragen für den agentischen Workflow „Warnungsauswirkung analysieren“

Fragen zu Warnungen in Now Assist für IT Operations Management (ITOM) Analysieren Sie den agentischen Workflow für Warnungsauswirkungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fragen, organisiert nach Warnungsquelle

Stellen Sie die folgenden Fragen zu Warnungen von bestimmten Erkennbarkeitstools in Now Assist Bereich. Weitere Informationen zur Verwendung des agentischen Workflows „Warnungsauswirkung analysieren“ finden Sie unter Verwenden Sie den agentischen Workflow „Warnungsauswirkung analysieren“.

Warnungsquelle	Was Sie fragen sollten
Dynatrace	• Welche Auswirkungen hat diese Warnung? • Was ist die Ursachenentität? • Was ist die Ursachentheorie? • Welche Entitäten sind von dieser Warnung betroffen? • Welche Umgebungen sind von dieser Warnung betroffen?
Kentik	• Gibt es Netzwerkanomalien zwischen den betroffenen Services für diese Warnung? • Wird derzeit ein DDOS-Angriff auf die betroffenen Services für diese Warnung ausgeführt? • Besteht eine Konnektivität zwischen den betroffenen Services für diese Warnung?
New Relic	• Gab es letzte Bereitstellungen für diese Warnung? • Was sind die Ursachentheorien für diese Warnung? • Was ist noch von dieser Warnung betroffen? • Welche Auswirkungen hat der Anwender auf diese Warnung? • Welche Engineering-Teams sollte ich anrufen, um diese Warnung zu untersuchen? • Wer besitzt die betroffene Entität für diese Warnung?

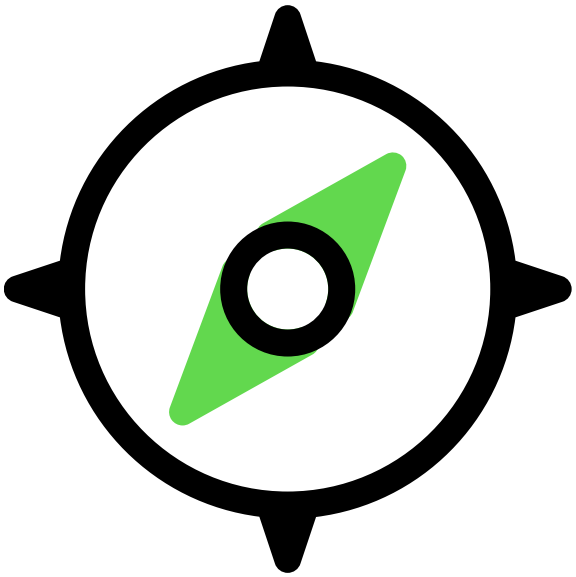
Playbook für verbesserte Automatisierung von AIOps-Lernen (LEAP)

AIOps LEAP Die Anwendung verwendet KI-gesteuerte Einblicke und Automatisierung, um IT-Vorgänge zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

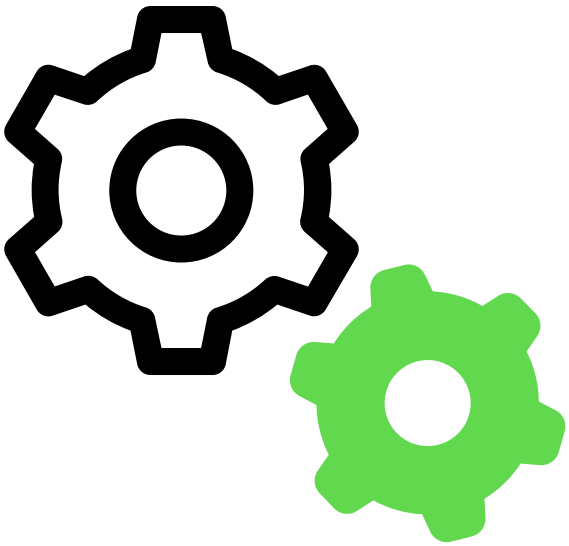
Erste Schritte

Untersuchen



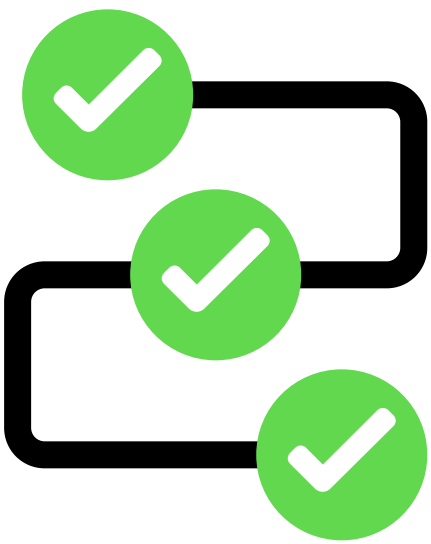
Erfahren Sie mehr über AIOps LEAP-Vorteile, -Funktionen und -Fähigkeiten.

Konfigurieren



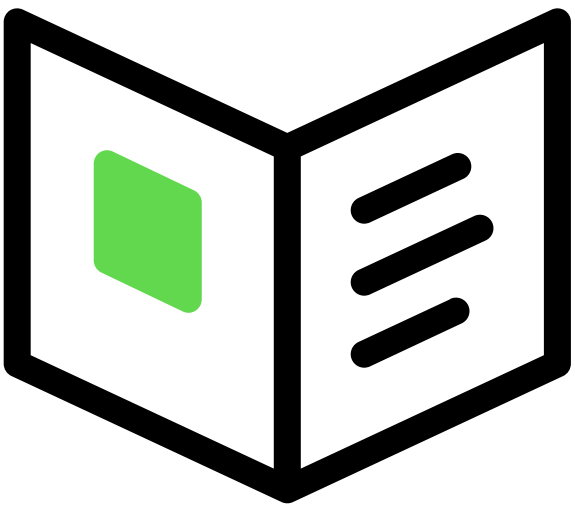
Installieren und konfigurieren Sie AIOps LEAP.

Verwenden



Erstellen Sie Problemdatensätze und Playbooks mit AIOps LEAP.

Referenz



Erhalten Sie detaillierte Informationen zur Konfiguration wichtiger Kompetenzen während der AIOps LEAP-Installation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Nicht alle Modellanbieter sind für Kunden mit landesinternen SKUs verfügbar, und einige Now Assist-Produkte/-Funktionen sind derzeit für Kunden im Land nicht verfügbar. Weitere Informationen finden Sie unter KB1584492 artikel in der Now Support Knowledge Base. Überprüfen Sie in zukünftigen Releases auf Updates der Modellanbieter-Verfügbarkeit.
- Einige Now Assist Produkte/Funktionen sind derzeit für Kunden in den mit FedRAMP, NSC DOD IL5 oder Australia IRAP geschützten Rechenzentren, selbst gehosteten Kunden oder anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.
- Einige Now Assist Produkte/Funktionen sind derzeit nur für Kunden in einigen Regionen verfügbar. Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.

Unterstützte LLMS für Now Assist für ITOM

Sie können verwenden Now LLM Service, Azure OpenAI, Google Gemini Oder Anthropic Claude auf AWS Als KI-Modellanbieter für Now Assist-Kompetenzen und KI-Agents. Sie können Einstellungen auf Kompetenzebene in festlegen Now Assist-Administrator Konsole an. Weitere Informationen finden Sie unter Große Sprachmodelle auf der ServiceNow AI Platform® .

Problembehandlung und Hilfe

- IT Operations Management-Produkt auf der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus besteht keine Garantie dafür, dass diese Anwendung für Ihren Anwendungsfall vollständig trainiert oder getestet wurde. Um diese Probleme zu mindern, liegt es in Ihrer Verantwortung, Ihre Verwendung dieser Anwendung auf Richtigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, menschliche Aufsicht über die Ausgabe zu übernehmen und zu Entscheidungszwecken nicht ausschließlich KI-generierte Ausgaben zu verwenden. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung, Sicherheit und Infrastruktur einsetzen möchten. Sie stimmen zu, sich an zu halten Richtlinie zur zulässigen Nutzung von KI von ServiceNow , Die von ServiceNow aktualisiert werden kann.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Darüber hinaus erfasst diese Anwendung Informationen zu Skripts (und zugehörigen Skriptdatensätzen) in denen Now Assist Für die Codegenerierung wird aufgerufen. Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now Assist Abwählseite beschrieben.

Weitere Informationen finden Sie unter Now Assist Dokumentation an.

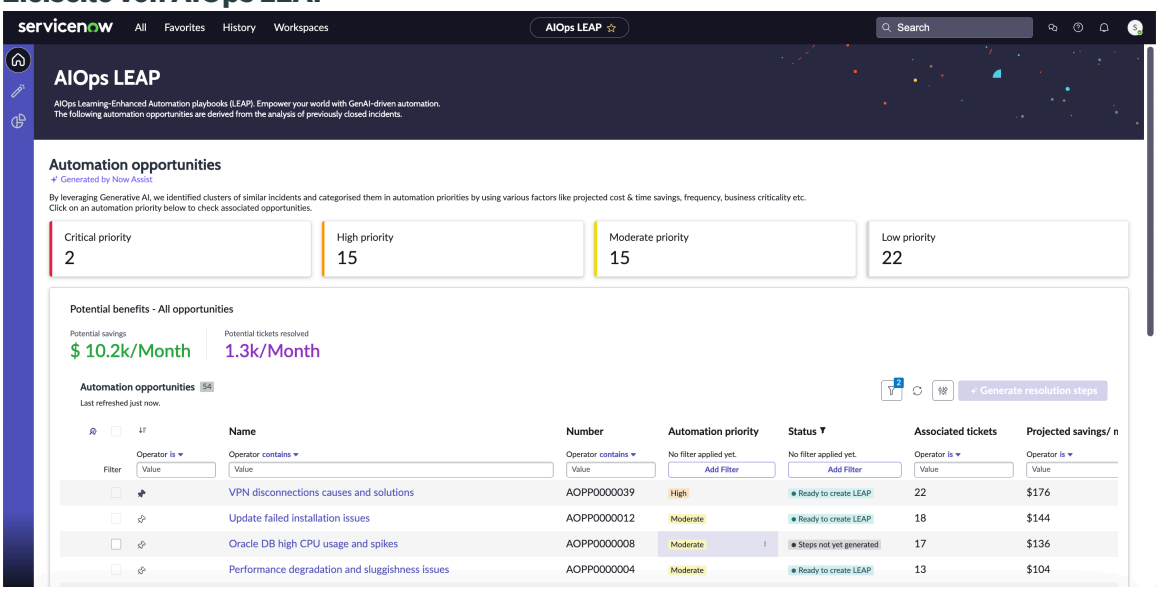
AIOps LEAP erkunden

AIOps LEAP Kategorisiert ähnliche Incidents in Gruppen, führt Incident-Analysen mithilfe von KI durch und erstellt Playbooks für dynamische Standardlösungen, um eine schnelle Incident-Lösung zu fördern.

AIOps LEAP – Übersicht

AIOps LEAP Hilft Ihnen, Incidents und operative Aufgaben effizient zu verwalten. Mithilfe von KI werden Informationen aus vorhandenen Incidents gesammelt und Lösungen generiert, die automatisiert werden können. Die AIOps LEAP Die Automatisierung bietet Tools, um Incidents frühzeitig zu verwalten, die Lösung zu beschleunigen und vor zu verwenden Hat Automatisierung erstellt, und befolgen Sie klare Schritte, um Probleme zu behandeln. Diese Tools helfen, reibungslose Vorgänge zu unterstützen.

Zielseite von AIOps LEAP



AIOps LEAP – Anwender

Anwenderrollen

Rolle	Beschreibung
AIOps LEAP-Administrator	Sie haben die volle Kontrolle über AIOps LEAP Fähigkeiten, einschließlich der folgenden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderrollen (Fortsetzung)

Rolle	Beschreibung
	• Aktivieren und deaktivieren Sie Funktionen • Führen Sie geplante Aufgaben aus • Verwalten AIOps LEAP Tabellen und AIOps LEAP Arbeitsbereich • Lösungsschritte generieren und aktualisieren • Erstellen und zeigen Sie Probleme und an AIOps LEAP Playbooks aus Automatisierungsmöglichkeiten (AO)
AIOps LEAP-Betrachter	Sie können auf Daten im Zusammenhang mit zugreifen und sie anzeigen AIOps LEAP, Einschließlich Tabellen, Arbeitsbereich und Problemen, die aus AOS stammen.
AIOps LEAP Service Desk-Mitarbeiter	Sie können auf zugreifen AIOps LEAP Menü aus dem Service Operations-Arbeitsbereich(SOW) Und Auslöser AIOps LEAP Ausführungen direkt von innerhalb SOW.

Diese Rollen arbeiten zusammen, um einen optimierten und sicheren Ansatz für die Verwaltung der Automatisierung, die Lösung von Incidents und die Weitergabe von Wissen über Teams hinweg zu erstellen.

AIOps LEAP – Vorteile

Fördert die Automatisierungskultur

Nutzt umfassende Einblicke aus Incidents, um Lücken bei der Einführung von Automatisierungen zu schließen und die Automatisierungsskalierung zu ermöglichen.

Steuert die Incident-Lösung

Bietet geführte Schritte für L1-Betreiber, um die Produktivität zu verbessern, häufige Probleme schnell zu lösen und die Gesamteffizienz zu verbessern.

Ziele für L1-Operatoren

Stattet L1-Operatoren mit strukturierten, datengesteuerten Fragen für wiederkehrende Incidents aus, die häufige Probleme lösen und Eskalationen an L2 minimieren

Verbessert MTTR

Reduziert die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR) durch optimierte Prozesse und reduzierte Verzögerungen.

Optimieren Sie die Ressourcenzuteilung

Erleichtert eine bessere Verteilung der Arbeitsauslastung und fördert eine bessere Ressourcennutzung.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von AIOps LEAP finden Sie unter:

- AIOps LEAP konfigurieren
- AIOps LEAP verwenden
- AIOps LEAP – Referenz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AIOps LEAP Funktionen

AIOps LEAP Enthält Funktionen wie das Gruppieren von Incidents, das Erstellen von Problemdatensätzen und das Generieren von Playbooks.

Identifizieren und priorisieren Sie Bereiche mit hoher Auswirkung

AIOps LEAP Verwendet datengesteuerte Analytics, um Anwendern zu helfen, kritische Probleme zu identifizieren und Automatisierungsmöglichkeiten mit hoher Auswirkung zu priorisieren. Dadurch wird sichergestellt, dass Ressourcen für die Bereiche priorisiert werden, die die höchste betriebliche Effizienz und den höchsten Geschäftsnutzen bieten.

Messen und verbessern Sie die Leistung

AIOps LEAP Trägt zur Verbesserung der durchschnittlichen Reparaturzeit (Mean Time to Repair, MTTR) und der betrieblichen Effizienz bei, indem erweiterte Analytics und KI-gestützte Einblicke zur kontinuierlichen Überwachung und Optimierung von IT-Prozessen verwendet werden.

Interpretieren Sie Daten, und automatisieren Sie Datensätze

AIOps LEAP Generiert automatisch Problemdatensätze und führt automatisierte Playbooks aus, indem Verlaufsdatenmuster analysiert werden, was eine schnellere Ursachenidentifizierung ermöglicht und manuelle Eingriffe in komplexen IT-Umgebungen reduziert.

Personas in AIOps LEAP

AIOps LEAP Unterstützt verschiedene Personas, denen verschiedene Rollen zugewiesen werden können, um sie zu verbessern IT Operations Management.

AIOps LEAP Personas

Persona	Beschreibung	Verantwortlichkeit
Automatisierungsarchitekt	Ein Automatisierungsarchitekt ist ein leitender technischer Experte, der Automatisierungslösungen entwirft und entwickelt und bei Bedarf skaliert. Sie sind eine Brücke zwischen IT-Betrieb, Geschäftsanforderungen und Automatisierungsstrategie. Der Automatisierungsarchitekt optimiert manuelle, sich wiederholende und fehleranfällige Aufgaben.	• Identifiziert Bereiche mit hoher Auswirkung für die Automatisierung • Entwickelt Automatisierungsskripts, integriert KI-gestützte Einblicke und pflegt skalierbare Automatisierungs-Frameworks • Extrahiert Muster aus historischen Ticketdaten, um zukünftige Lösungen zu optimieren • Verfeinert Automatisierungslösungen basierend auf Feedback und sich entwickelnden Geschäftsanforderungen. • Arbeitet mit verschiedenen Geschäftsbereichen zusammen, um die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AIOps LEAP Personas (Fortsetzung)

Persona	Beschreibung	Verantwortlichkeit
		Automatisierung an den Unternehmenszielen auszurichten.
IT-Betreiber	Ein IT-Betreiber umfasst alle L1- und L2-Incident-Handler, die den täglichen IT-Betrieb unterstützen.	• Verwendet KI-generierte Playbooks zur Lösung von Incidents • Greift auf zu Knowledge Base
Käufer, Geschäftszielbesitzer	Ein Käufer oder ein Geschäftszielbesitzer erhält strategische und operative Vorteile mit AIOps LEAP.	• Verwendet AIOps LEAP Um den IT-Betrieb zu verbessern • Optimiert die Ressourcenzuteilung • Automatisiert die Lösung wiederkehrender Probleme

Ein Automatisierungsarchitekt kann AIOps LEAP verwenden, um Feedback zu sammeln und Lösungen zu verfeinern. Auf ähnliche Weise verwenden IT-Betreiber AIOps LEAP, um wiederkehrende Probleme zu erkennen und Vorschläge für die vorbeugende Automatisierung anzuzeigen. Dies ermöglicht eine schnellere Lösung, und Betreiber können mehr Incidents unabhängig lösen, was zu einer verbesserten Effizienz und Servicequalität führt.

AIOps LEAP Priorisierungslogik und Berechnung von Kosteneinsparungen

AIOps LEAP Verwendet die integrierte Priorisierungslogik, um die Automatisierungsmöglichkeiten mit den höchsten Auswirkungen zu identifizieren. Diese Logik hilft Ihnen, sich auf die wertvollsten Automatisierungsaufgaben zu konzentrieren. Die Berechnungen liefern eine Schätzung der potenziellen Kosten- und Zeitersparnisse. Es ist am besten, diese Werte in einer nicht-Produktionsumgebung zu validieren, bevor sie in der Produktion implementiert werden.

Die Automatisierungspriorität wird durch die Kombination der folgenden Schlüsselfaktoren berechnet:

- Geschäftsauswirkung
- Prognostizierte Kosten-/Zeitersparnisse

Die Priorität für eine Automatisierungsmöglichkeit wird anhand des folgenden Diagramms bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Priorität der Automatisierungsmöglichkeit

Die Schlüsselfaktoren werden für jede Gruppe zugehöriger Incidents, sogenannte#Automatisierungsmöglichkeiten, bewertet, und die Ergebnisse helfen Teams, sich auf Bereiche mit hohem Wert zu konzentrieren.

Geschäftsauswirkung

Jede Automatisierungsmöglichkeit ist ein Cluster von Tickets. Jedes Ticket wird basierend auf den folgenden Faktoren bewertet:

- Business-Relevanz
- Status des schwerwiegenden Incidents
- Auswirkungsstufe

Diese Faktoren sind angegebene Werte. Beispielwerte für#Relevanz:

- Am Kritischsten = 100 %
- Etwas Kritisch = 75 %
- Weniger Kritisch = 50 %
- Nicht Kritisch = 25 %

Eigenschaftentabelle

Schlüssel	Standardwert	Beschreibung
ohf_p4	0,8	Overhead-Faktor für P4-Datensätze.
ohf_p5	0,4	Overhead-Faktor für P5-Datensätze.
ohf_p1	1,8	Overhead-Faktor für P1-Datensätze.
ohf_p2	1.4	Overhead-Faktor für P2-Datensätze.
Cost_per_entry	20	Kosten in Dollar, die dem Hinzufügen eines Arbeitsnotizeintrags zu einem Datensatz zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftentabelle (Fortsetzung)

Schlüssel	Standardwert	Beschreibung
ohf_p3	1.1	Overhead-Faktor für P3-Datensätze.
Time_per_entry	0,5	Zeit in Stunden, die dem Hinzufügen eines Arbeitsnotizeintrags zu einem Datensatz zugeordnet ist.
First_Run_Group_limit	0	Gesamtzahl der Gruppen, für die bei der ersten Ausführung Lösungsschritte generiert werden.
gaf_Mapping_min_threshold	0,2	Mindestverhältnis von Incidents, die auf eine aktive Gruppe verweisen, die für die Neuzuordnung nach dem Clustering berücksichtigt wird.
Group_Prioritization_Trigger_Delay	{"Minuten":10}	Verzögerung in Sekunden, bevor die Gruppenpriorisierungslogik ausgelöst wird.

Hinweis:

- Sie können die Werte in der Eigenschaftentabelle ändern. Wenn Sie die Werte jedoch ändern, unterscheiden sich die Berechnungen.
- Sie sollten die Werte in der Eigenschaftentabelle vor der Aktivierung ändern AIOps LEAP.
- Wenn Sie Werte in der Eigenschaftentabelle ändern, müssen Sie deaktivieren und erneut aktivieren AIOps LEAP Kompetenz

Jeder Faktor wird gewichtet. Nehmen Sie beispielsweise an, dass Relevanz = 0,8, schwerwiegender Incident = 0,2 und Auswirkung = 0,4 ist.

```
Ticket Score = (Criticality × 0.8 + Major Incident × 0.2 + Impact × 0.4) ÷ 3
```

Der#Durchschnitt aller Ticketpunktzahlen ☒ In der Gruppe wird zu ☒ Geschäftsauswirkungspunktzahl. Basierend auf dieser Punktzahl werden Automatisierungsmöglichkeiten als hohe Auswirkung (die Top 33 %)#, mittlere Auswirkung#(nächste 33 %) und geringe Auswirkung#(verbleibende 33 %) gekennzeichnet.

Prognostizierte Auswirkungen auf Kosten oder Zeitersparnisse

AIOps LEAP Schätzt, wie viel Zeit und Kosten durch die Automatisierung einer Gruppe von Incidents mit historischen Ticketdaten eingespart werden können.

Die wichtigsten Eingaben für Kosten- und Zeitersparnisse sind die folgenden:

- Häufigkeit der Incidents (FOI)#: Durchschnittliche Anzahl ähnlicher Incidents pro Monat
- Durchschnittliche Anzahl manueller Arbeitsnotizen (AWNC)
- Overhead-Faktor (OHF)#: Variiert je nach Incident-Priorität basierend auf der Prioritätstabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AIOps LEAP Verwendet die folgenden Formeln, um die prognostizierten Kosten- oder Zeitersparnisse zu berechnen:

- Prognostizierte Kosteneinsparungen = Σ (FOI x OHF) x AWNC x Kosten pro Arbeitsnotiz
- Voraussichtliche Zeitersparnisse = Σ (FOI x OHF) x AWNC x Mitarbeiterzeit pro Eintrag

Die prognostizierten Einsparungen jedes Tickets werden berechnet. Der#Durchschnitt für die Gruppe ☒ Wird zu ☒ Punktzahl für prognostizierte Kosten-/Zeitersparnisse, die auch als#hoch,#Mittel oder#Niedrig kategorisiert wird. Die Automatisierungsmöglichkeiten werden in absteigender Reihenfolge basierend auf den prognostizierten Kosten- oder Zeitersparnissen sortiert.

Bestimmung der Gesamtpriorität

Nach der Berechnung der Werte für das Unternehmen ich Mpact und die voraussichtlichen Kosten-/Zeitersparnisse, AIOps LEAP Weist jeder Automatisierungsmöglichkeit mithilfe dieser Matrix eine Prioritätsstufe zu:

Automatisierung p Rangfolge M atri X

Geschäft ich Mpact	Prognostizierte Kosten-/ Zeitersparnisse	Automatisierungspriorität
Hoch	Hoch	Sehr hoch
Mittel	Hoch	Hoch
Hoch	Mittel	Hoch
Mittel	Mittel	Mittel
Mittel	Niedrig	Niedrig
Niedrig	Mittel	Niedrig
Niedrig	Niedrig	Sehr niedrig

Diese priorisierten Automatisierungsmöglichkeiten werden im angezeigt AIOps LEAP Startseite Seite.

Verfolgen der tatsächlichen Kosten- und Zeitersparnisse

Nachdem die Automatisierung implementiert ist, AIOps LEAP Verfolgt die#tatsächlichen Kosten- und Zeitersparnisse und zeigt sie im#SCHALTWERT-Dashboard an, damit Sie die Auswirkungen messen und Entscheidungen treffen können.

Schlüsselmetriken:

- Zusätzliche Arbeitsnotizen (AWN)#: Manuelle Einträge nach der Playbook-Ausführung
- Overhead-Faktor (OHF) nach Priorität#: Beispiel: P1 = 1,8x

Formeln:

- Gespeicherte Arbeitsnotizen (SWNs) = AWNC – AWN
- AWN = SWN X OHF
- Tatsächliche Kosteneinsparungen = AWN x Kosten pro Arbeitsnotiz
- Tatsächliche Zeitersparnisse = AWN x Mitarbeiterzeit pro Eintrag

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Berechnungen der prognostizierten Kosten und Zeitersparnisse

Ein Cluster hat 20 AWNC und ist einem P2-Incident mit 6 AWN zugeordnet. Die c ost pro Arbeitsnotiz beträgt 20 USD, und die Zeit des Service Desk-Mitarbeiters pro Eintrag beträgt 0,5 Stunden.

Gemäß den Formeln beträgt die SWN-Anzahl `(20 - 6) = 14` . Gemäß den Eigenschaftentabellen ist der OHF = 1,4.

`SWN X OHF = AWN` Also `14 x 1,4 = 19,6`

Dieser Wert kann auf 20 AWN abgerundet werden. Jeder AWN-Eintrag stellt Einsparungen in Höhe von 20 USD dar.

Die tatsächlichen Kosteneinsparungen nach der Automatisierung = `AWN x Kosten pro Arbeitsnotiz = 20 x 20 = 400 USD` .

Wenn Sie also Automatisierung verwenden, können die prognostizierten Kosteneinsparungen bis zu 400 USD betragen. Daher bietet die Berechnung umsetzbare Einblicke für die laufende Prozessverbesserung und Ressourcenzuteilung.

AIOps LEAP konfigurieren

Sie können herunterladen und installieren AIOps LEAP Anwendung aus dem ServiceNow® Store Um Ihren IT-Betrieb effizient zu verwalten.

Konfiguration – Übersicht

1. AIOps LEAP installieren

   Installieren AIOps LEAP Wenn Sie die Administratorrolle innehaben.

2. AIOps LEAP aktivieren

   Aktivieren AIOps LEAP Um die Gruppierung von Incidents zu aktivieren, erstellen Sie Problemdatensätze, und generieren Sie Playbooks für Lösungen.

AIOps LEAP installieren

Sie können installieren AIOps LEAP Anwendung mit Now Assist für IT Operations Management (ITOM)(sn_itom_gen_ai), wenn Sie die Administratorrolle innehaben. Die zugehörigen Anwendungsinstallationen ServiceNow® Store Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Berechtigung für abrufen ServiceNow Produkt oder Anwendung an.
- Überprüfung des folgenden Elements: AIOps LEAP Anwendungsliste in ServiceNow Store Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: Systemadministrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit AIOps LEAP installiert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Rollen
- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter Mit AIOps LEAP installierte Komponenten.

Prozedur

1. Wechseln Sie zu ServiceNow Store Website.
2. Geben Sie in der Suchleiste ein Now Assist für ITOM Und wählen Sie dann aus **Suchen** .
3. Wählen Sie aus Now Assist für ITOM Widget, und wählen Sie dann aus **Abrufen** Um diese Anwendung für die Installation in Ihren Instanzen verfügbar zu machen.
4. Installieren Sie die Anwendung Now Assist für ITOM.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
   b. Suchen Sie nach Now Assist für IT Operations Management (ITOM).
   c. Wählen Sie **Installieren** aus.

AIOps LEAP aktivieren

Aktivieren Sie AIOps LEAP Kompetenz Nach der Installation der Anwendung zum Zusammenstellen und Kategorisieren von Incidents.

Vorbereitungen

Erforderliche Rolle: Systemadministrator oder AIOps LEAP Administrator

Prozedur

1. Aktivieren *AIOps LEAP*Mit einer der folgenden Optionen.

Optionen	Schritte
Arbeitsbereiche	a. Navigieren zu **Arbeitsbereiche** > **AIOps-LEAP**an. b. Wählen Sie Aus **Now Assist Admin-Arbeitsbereich** . c. Wählen Sie auf der LEAP-Installations–karte die Option aus **Kompetenz aktivieren** .
Now Assist-Administrator	a. Navigieren zu **Alle** > **Now Assist Admin** > **Now Assist-Kompetenzen** b. Wählen Sie in der Workflow-Liste unter Technologie die Option aus **ITOM** . c. Wählen Sie auf der LEAP-Installations–karte die Option aus **Kompetenz aktivieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Im Eingabeabschnitt DES LEAP-Installationsprogramms von *LEAP-Installationsprogramm* , Geben Sie die Details für ein AIOps LEAP Um Scans für vorhandene Datensätze auszuführen, und wählen Sie aus **Speichern und fortfahren** .
   Weitere Informationen zu Installationsfeldern finden Sie unter LEAP Felder des Installationsprogramms
3. Im Abschnitt Anzeige auswählen von *LEAP-Installationsprogramm* , Wählen Sie die gewünschte Anzeige aus, und wählen Sie aus **Speichern und fortfahren** .
4. Im Abschnitt Überprüfen und aktivieren von *LEAP-Installationsprogramm* , Überprüfen Sie die Auswahl, und wählen Sie aus **Aktivieren** .
5. Wählen Sie Aus **Zurück zu ITOM** In der Erfolgsmeldung.

AIOps LEAP verwenden

AIOps LEAP Sammelt Incidents oder Probleme und gruppiert sie in Elemente, die Automatisierungsmöglichkeiten (AOS) genannt werden.

AIOps LEAP-Aufgaben

AOS werden kategorisiert, je nachdem, wie kritisch die Services sind, Anzahl der Übergaben und Incident-Informationen:

- Kritisch
- Hoch
- Mittel
- Niedrig

Das Priorisieren von AOS hilft IT Operations Management Personas behandeln die kritischsten Probleme oder die Probleme, die die Leistung beeinträchtigen. AIOps LEAP Stellt Aufgaben bereit, die bei der Erforschung der Incidents helfen, um die Ursache zu analysieren und Lösungen abzuleiten. Playbooks helfen IT-Betreibern, auf Lösungsschritte zuzugreifen, um die Gesamtleistung des IT-Betriebs zu verbessern.

1. Erstellen AIOps LEAP Problemdatensätze

   Erstellen Sie einen Problemdatensatz mithilfe der Lösungsschritte eines AO. Der Problemdatensatz hilft Ihnen, eine eingehende Analyse durchzuführen, um die Ursache des Incident zu finden.

2. Generieren AIOps LEAP Playbooks

   Generieren Sie automatisierte Playbooks, die die Lösungsschritte verwenden, um ähnliche Incidents in der Zukunft effizient zu lösen.

Erstellen AIOps LEAP Problemdatensätze

Erstellen Sie Problemdatensätze für AIOps LEAP Aus verfügbaren Incident-Clustern, auch als Automatisierungsmöglichkeiten bezeichnet, für weitere Analysen.

Vorbereitungen
Erforderliche Rolle: AIOps LEAP Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Prozess zur Erstellung von Problemdatensätzen überträgt automatisch kritische Informationen aus Incidents in Problemdatensätze. Wenn ein Problemdatensatz erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird, AIOps LEAP Enthält alle relevanten Informationen, z. B. die Beschreibung der Incident-Gruppe, den Incident-Gruppenlink und Lösungsschritte. Die automatisierte Datenübertragung zeichnet sich aus durch:

Ursachendokumentation

AIOps LEAP Füllt aus Ursachennotizen Abschnitt des Problemdatensatzes mit denselben Details wie in vorhandenen Incident-Datensätzen verfügbar.

Incident-Anhang

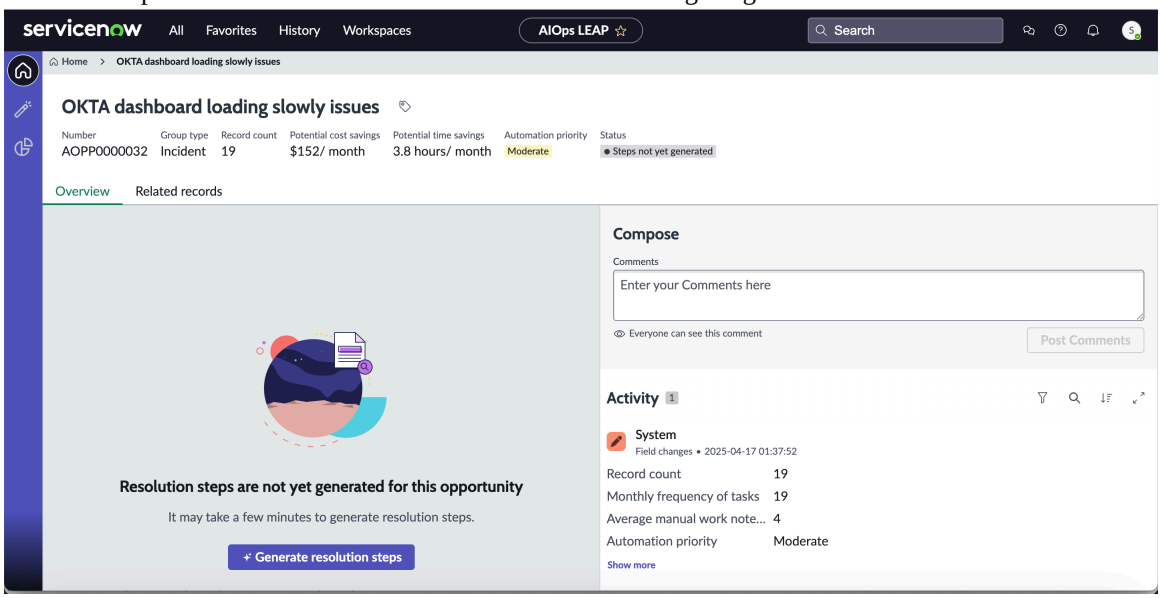
Alle der Gruppe zugeordneten Incidents werden automatisch mit dem Problemdatensatz verknüpft, um eine umfassende Nachverfolgung zu ermöglichen.

Asynchrone Verarbeitung

Problemdatensätze werden ohne manuelles Eingreifen auch in Szenarien mit hohem Volumen effizient generiert.

Prozedur

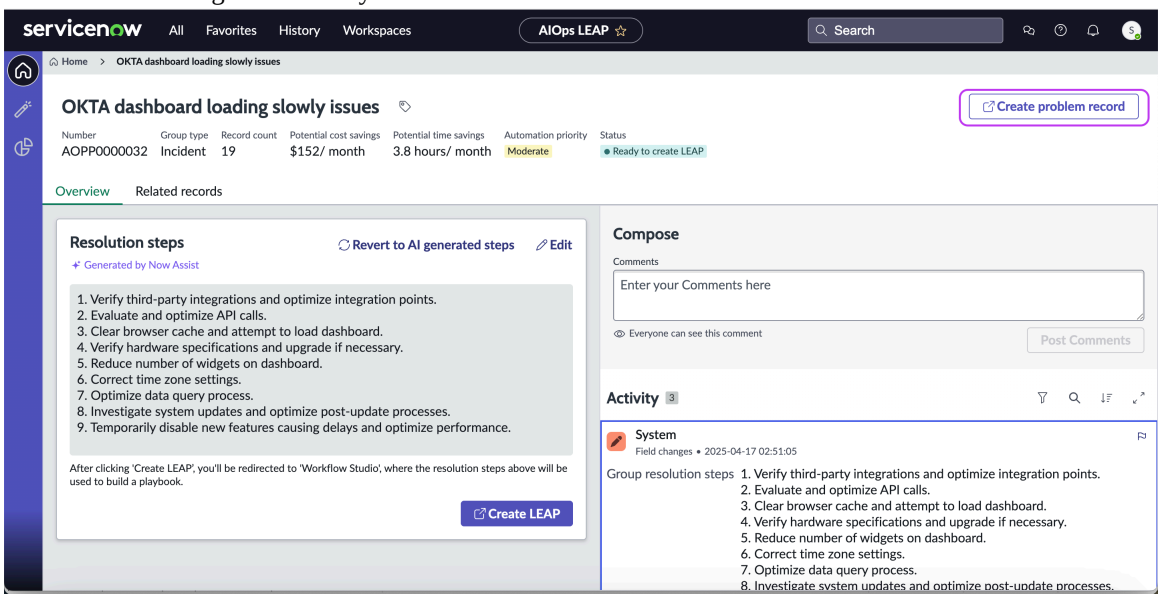
1. Auswahlvorgang **Arbeitsbereiche** > **AIOps-LEAP**an.
2. Auf der AIOps LEAP Zielseite wählen Sie eine Automatisierungsmöglichkeit aus.



3. Wenn eine Liste von Lösungsschritten nicht in der Übersicht angezeigt wird Registerkarte , Wählen Sie aus **Generieren Sie Lösungsschritte** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie aus **Erstellen Sie einen Problemdatensatz** Schaltfläche zum Erstellen eines Datensatzes für eine weitere eingehende Analyse.



Generieren AIOps LEAP Playbooks

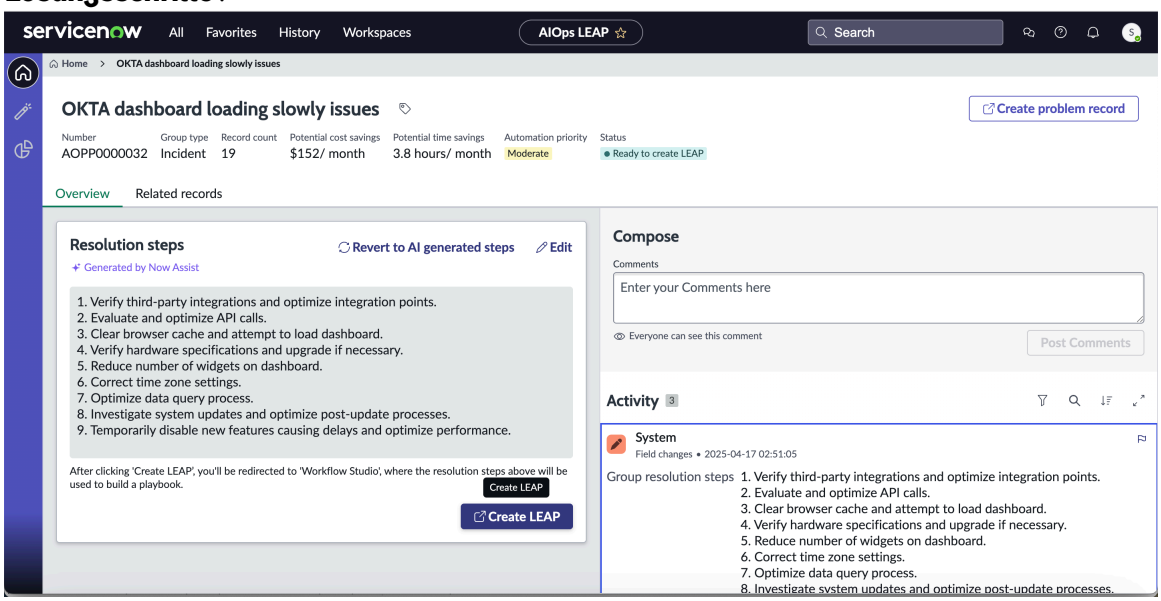
Erstellen Sie mit Standard-, dynamische und automatisierte Playbooks AIOps LEAP Zum Heraufstufen einer schnellen Incident-Lösung und der Antwortzeit.

Vorbereitungen

Erforderliche Rolle: AIOps LEAP Administrator

Prozedur

1. Auswahlvorgang **Arbeitsbereiche** > **AIOps-LEAP**an.
2. Auf der AIOps LEAP Zielseite wählen Sie die erforderliche Automatisierungsmöglichkeit aus.
3. Wenn die Liste der Lösungsschritte nicht in der Übersicht angezeigt wird, wählen Sie aus **Generieren Sie Lösungsschritte** .

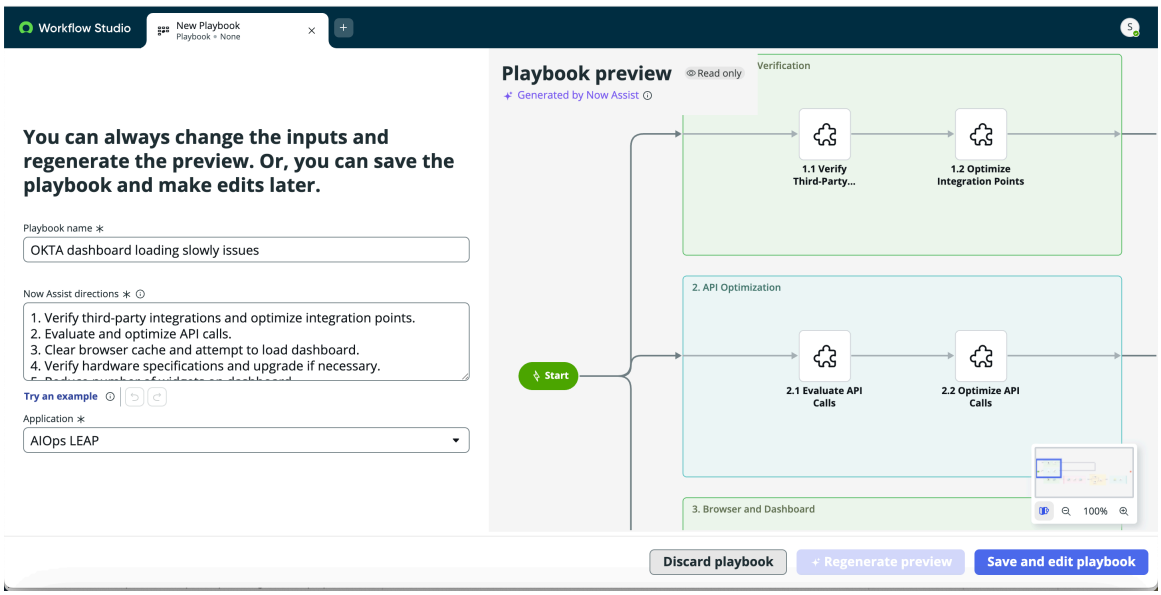


4. Wählen Sie Aus **Erstellen Sie LEAP** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Studio Wird geöffnet, und der Playbook-Generierungsprozess wird gestartet. Die **Playbook-Name** Und **Now Assist-Anweisungen** Felder sind mit dem Titel des Problemdatensatzes und den generierten Lösungsschritten vorab ausgefüllt.



AIOps LEAP – Referenz

Diese Themen enthalten detaillierte Feldbeschreibungsinformationen, die während erforderlich sind AIOps LEAP Installation.

LEAP Felder des Installationsprogramms

Beschreibung der Feldwerte, die Sie während der Installation konfigurieren AIOps LEAP.

AIOps LEAP Kompetenzen

Kompetenz	Beschreibung
Ausführungshäufigkeit	Häufigkeit der Ausführung AIOps LEAP In der erforderlichen Tabelle .
Gruppieren Sie Datensätze aus dieser Tabelle *	Auszuführender Tabellenname AIOps LEAP Abfrage zum Filtern von Datensätzen für die Gruppierung .
Verwenden Sie diese Spalte zum Gruppieren *	Spaltenname aus der obigen Tabelle, der zum Lesen von Datensätzen für die Gruppierung verwendet wird. Der Standardwert ist „short_description“.
Diesen Filter verwenden	Filterdetails, die zum Lesen von Datensätzen für die Gruppierung verwendet werden. **Hinweis:** Dieses Feld kann von Kunden geändert werden. Standardmäßig werden die Incidents für die letzten 6 Monate gruppiert und gefiltert.
Verwenden Sie diese Spalte für die Themengenerierung *	Datensatzspalten, die zum Erstellen der Titel für die erstellten Gruppen verwendet werden .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AIOps LEAP Kompetenzen (Fortsetzung)

Kompetenz	Beschreibung
	Hinweis: Dieses Feld kann von Kunden geändert werden.

Mit AIOps LEAP installierte Komponenten

Bei der Aktivierung des -Plugins werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und Scheduled Jobs.

Installierte Rollen

Rollentitel [Name]	Beschreibung
AIOps LEAP administrator [sn_itom_LEAP.LEAP_admin]	Sie haben die volle Kontrolle über AIOps LEAP Fähigkeiten, einschließlich der folgenden: • Aktivieren und deaktivieren Sie Funktionen • Führen Sie geplante Aufgaben aus • Verwalten AIOps LEAP Tabellen und AIOps LEAP Arbeitsbereich • Lösungsschritte generieren und aktualisieren • Erstellen Sie Probleme, zeigen Sie sie an, und generieren Sie AIOps LEAP Playbooks aus Automatisierungsmöglichkeiten (AO)
AIOps LEAP betrachter [sn_itom_LEAP.LEAP_Viewer]	Sie können auf Daten im Zusammenhang mit zugreifen und sie anzeigen AIOps LEAP, Einschließlich Tabellen, Arbeitsbereich und Problemen, die aus AOS stammen.
AIOps LEAP Service Desk-Mitarbeiter [sn_itom_LEAP.LEAP_Agent]	Sie können auf zugreifen AIOps LEAP Menü aus dem Service Operations-Arbeitsbereich(SOW) Und Auslöser AIOps LEAP Ausführungen direkt von innerhalb SOW.

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Datensatzmetriken Ausfüllen – Datensätze Zusammenfassen	Wird einmal pro Tag ausgeführt, um die Tabelle der SCHALTAGGREGIERUNGSMETRIKEN nach Zeiträumen auszufüllen.
Aktualisieren Sie die Datensatzmetriktabelle mit berechneten Metriken	Wird täglich ausgeführt, um die Datensätze in der Tabelle „LEAP-Datensatzmetriken“ für alle Datensätze zu berechnen und zu aktualisieren, für die die Metriken noch nicht berechnet wurden.
GAF: Offline-Flow ausführen	Wird monatlich ausgeführt, um die Aufgaben anhand der Aufgabendaten zu gruppieren, die in der Kompetenzkonfiguration bereitgestellt werden, während die LEAP-Kompetenz aktiviert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Tabellen

Tabelle	Beschreibung
Aggregierte LEAP-Metriken	Enthält Metriken wie Kosteneinsparungen, Zeitersparnisse und Datensatzanzahl für jeden Zeitraum. Diese Daten werden auf der LEAP-Berichtsseite im Arbeitsbereich verwendet.
LEAP-Feedback	Speichert das Feedback des Service Desk-Mitarbeiters für die Playbooks, die zur Behebung der Aufgaben ausgeführt werden.
LEAP-GAF-Zuordnung	Verwaltet eine Zuordnung zwischen den GAF-Gruppen und den veröffentlichten Schritten, um Informationen in den nachfolgenden GAF-Clustering-Ausführungen beizubehalten.
LEAP-Gruppe	Speichert die SCHALTGRUPPENDETAILS, z. B. Gruppenbeschreibung, Lösungsschritte und ob der SCHALTVORGANG automatisiert ist oder nicht.
LEAP-Gruppen-Rangliste	Verwaltet Daten wie Geschäftsauswirkung, prognostizierte Kosteneinsparungen, Problemdatensatz und Status, wird auf der Seite „Automatisierungsmöglichkeiten“ des Arbeitsbereichs verwendet.
LEAP-Eigenschaften	Legt anwenderdefinierte Werte für die Eigenschaften fest, die in verwendet werden AIOps LEAP.
LEAP-Datensatzmetriken	Verwaltet Daten, die auf der veröffentlichten LEAP-Seite im Arbeitsbereich verwendet werden. Enthält berechnete Daten wie Zeitersparnis, gelöste Tickets und Bewertungstrend.

Auf Cloud-Umgebungen für ITOM-Produkte zugreifen

Wenn Ihre Organisation IT-Assets in der Cloud bereitstellt, müssen ITOM-Produkte auf Ihre Cloud-Umgebung zugreifen, um Informationen über die IT-Infrastruktur zu sammeln.

Zugehörige Informationen

Cloud-Discovery erkunden

Referenzen zur Discovery von Cloud-Ressourcen

Installieren und konfigurieren MID Servers Um auf Cloud-Umgebungen zuzugreifen

Installieren und konfigurieren Sie MID Servers Richtig, um ITOM-Produkte den Zugriff auf die Cloud-Ressourcen zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: Discovery_admin oder sn_CMP.Cloud_admin (für Cloud Provisioning and Governance)

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Für IP-basierte Discovery MID-Server wird installiert Auf einem Server in der Cloud-Umgebung in einer Virtual Private Cloud (VPC).

   Example

   Wenn Sie beispielsweise den Zugriff auf AWS-Servicekonten mit IAM-Rollen konfigurieren, installieren Sie MID-Server in der Amazon-EC2-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Wenn Sie AWS-Anmeldeinformationen für ServiceNow AI Platform konfigurieren, spielt der Standort des MID-Server s keine Rolle.

Wenn Ihre Organisation mehrere VPC-Segmente hat, stellen Sie bereit MID Servers In einer Manage-Mentor-Transit-VPC.

2. Aktivieren Sie IP-basierte Erkennungsaufträge, um mit agentlosen Anmeldeinformationen auf die Rechenebene zuzugreifen.
3. Konfigurieren Sie MID-Server mit den Funktionen, die für die Cloud-Umgebung erforderlich sind, für die Sie eine Erkennung durchführen möchten.

   Sie können auswählen ALLE Fähigkeit oder Konfiguration bestimmter Fähigkeiten für eine höhere Sicherheit.

   Hinzufügen Cloud-Management In **Unterstützte Anwendung** In MID-Server Für Cloud Provisioning and Governance Anforderungen, die verarbeitet werden sollen.

Cloud-Umgebung	Von Cloud-Discovery benötigte MID-Server-Funktion	Von Cloud Provisioning and Governance benötigte MID-Server-Funktion
Amazon AWS Cloud	AWS Oder Cloud-Management Oder ALLE	AWS Oder Cloud-Management
Microsoft Azure Cloud	Azure Oder Cloud-Management Oder ALLE	Azure Oder Cloud-Management
Google Cloud	Google Oder Cloud-Management Oder ALLE	Google Oder Cloud-Management
IBM Cloud Platform	IBM Oder Cloud-Management Oder ALLE	N/V
Oracle Cloud-Infrastruktur (OCI)	OCI Oder Cloud-Management Oder ALLE	N/V
OpenStack	OpenStack Oder Cloud-Management Oder ALLE	N/V
Red hat-Virtualisierung (RHV)	RHV Oder Cloud-Management Oder ALLE	N/V

4. Wenn MID Servers Muss einen nicht authentifizierten Proxy-Server durchlaufen, um auf Cloud-Ressourcen zuzugreifen, ändern Sie den Agent\conf\Wrapper-override.conf Datei wie folgt:

```
wrapper.java.additional.1=-Dhttp.proxySet=true
wrapper.java.additional.2=-Dhttp.proxyHost=<proxyHost>
wrapper.java.additional.3=-Dhttp.proxyPort=<proxyPort>
wrapper.java.additional.4=-DuseProxy=true
```

5. Wenn Sie einen authentifizierten Proxy-Server verwenden, konfigurieren Sie MID-Server Parameter in config.xml Datei.

   Eine Beschreibung der Parameterwerte finden Sie unter **Proxy-Serverparameter** Abschnitt in MID-Server-Parameter .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden

Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden

Sie können den MID-Server für Cloud Provisioning and Governance für die Verwendung eines Proxy-Servers konfigurieren. Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten wie Ausführen von Discovery, Abrechnungsdownloads, Bereitstellen virtueller Computer und Ausführen von Lebenszyklusvorgängen auf virtuellen Computern unterstützt.

Einschränkungen für Proxy-Server

- VMware Cloud wird nicht unterstützt.
- Windows Oder Linux Nur Plattformen werden unterstützt.
- Die Integration mit Google Cloud Console bietet keine Unterstützung für das Herunterladen von Abrechnungsdaten.
- Remote-PowerShell-Skripts können nicht ausgeführt werden.
- Benutzerdefinierte APIs funktionieren möglicherweise nicht.

Hinweis:

SSH-Aufrufe sollten nicht über einen Proxy-Server weitergeleitet werden, wenn eine private Cloud-Umgebung verwendet wird, die sich auf derselben Seite des Proxys wie der befindet MID-Server.

Festlegen `mid.capi.skip_proxy_for_ssh`Auf „wahr“, um sie zu überspringen. Weitere Informationen finden Sie unter MID-Server-Eigenschaften, die von Service-Mapping verwendet werden.

`mid.capi.skip_proxy_for_ssh`:

- Bestimmt, ob MID-ServerÜberspringt den Proxy-Server bei der Weiterleitung von SSH-Aufrufen.
- Typ: Wahr | Falsch
- Standardwert: falsch

Unterstützte Proxy-Server-Authentifizierung für Cloud Provisioning and Governance

Typ des Proxy-Servers	Authentifizierungstyp
HTTP/HTTPS	Keine Authentifizierung
SOCKS5	Keine Authentifizierung
HTTP/HTTPS	Basic Authentication
SOCKS5	Basic Authentication
HTTP/HTTPS	NTLM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Proxy-Server-Konfigurationen für Cloud Provisioning and Governance

Unterstützte Konfigurationseinstellungen

Konfiguration	Betriebssystem	Proxy-Server	Authentifizierungsmodus
Konfiguration 1	Linux	Keine	Nicht zutreffend
Konfiguration 2	Windows	Squid (HTTPS)	Keine
Konfiguration 3	Linux	Squid (HTTPS)	Lokal
Konfiguration 4	Windows	Squid (HTTPS)	Active Directory

Unterstützte Konfigurationen

Cloud Provider	Funktionalität	Konfiguration 1	Konfiguration 2	Konfiguration 3	Konfiguration 4
Amazon AWS Cloud, Microsoft Azure Cloud und IBM Cloud Platform	Cloud-Discovery	Ja	Ja	Ja	Ja
	VM-Bereitstellung	Ja	Ja	Ja	Ja
	VM-Lebenszyklus	Ja	Ja	Ja	Ja
	CFT-Bereitstellung	Ja	Ja	Ja	Ja
	Abrechnungsdownload	Ja	Ja	Ja	Ja
	Skripts mit SSH	Ja	Ja	Ja	Ja
	Skripts mit PowerShell	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
	Cloud Events	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Google Cloud Platform	Cloud-Discovery	Ja	Ja	Ja	Ja
	VM-Bereitstellung	Ja	Ja	Ja	Ja
	VM-Lebenszyklus	Ja	Ja	Ja	Ja
	CFT-Bereitstellung	Ja	Ja	Ja	Ja
	Abrechnungsdownload	Nein	Nein	Nein	Nein
	Skripts mit SSH	Ja	Ja	Ja	Ja
	Skripts mit PowerShell	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
	Cloud Events	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
VMware Cloud	Nicht zutreffend				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

MID Server unter Windows installieren

MID Server unter Linux installieren

MID-Server-Parameter

Wiederholung von Cloud-Anforderungen konfigurieren

Wenn eine Anforderung während der Discovery von einem Cloud-Anbieter gedrosselt wird, bietet die Konfiguration der Wiederholung von Cloud-Anforderungen eine anpassbare Methode zum erneuten Versuch von Anforderungen. Muster für Discovery und Service-Mapping Enthält eine Wiederholungskonfiguration für AWS Und Azure. Sie können die enthaltene Konfiguration anpassen oder eine eigene erstellen.

Discovery-Administratoren und Cloud-Administratoren können unter auf die Konfiguration der Anforderungswiederholung zugreifen **Alle** > **Discovery** > **Wiederholung von Cloud-Anforderungen konfigurieren**an. Sie können eine Konfiguration für jeden Provider erstellen.

Wenn eine Anforderung eingeschränkt wird, wird vom Framework für Wiederholungen die für den Provider definierte Wiederholungskonfiguration dazu verwendet, Wiederholungen zu verarbeiten, bevor die endgültige Antwort an die ApiCommand-Klassen zurückgegeben wird:

- AwsApiCommand
- AzureApiCommand

Die Wiederholungskonfigurationen werden über die MID-Server-Eigenschaft `mid.cloud.discovery.retry.configuration` mit den MID Servers n synchronisiert.

Es gibt die folgenden Wiederholungsstrategien:

- Exponentielles Backoff
- Antwortheader – Backoff
- Anwenderdefiniertes Backoff

Exponentielles Backoff

Für die folgende Beispielkonfiguration …

Einstellung	Wert
Max. Wiederholungen	3
Antwortcodes	429
Basisverzögerung in ms	1.000
Max. Verzögerung in ms	10000
Additional delay window in ms (Fenster „Weitere Verzögerung“ in ms)	1500

… funktioniert die Wiederholungsstrategie „Exponentielles Backoff“ wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 1 ausgewählt. Der maximale Verzögerungswert beträgt 400 ms (400 * 1).
- 2. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 3 ausgewählt. Der maximale Verzögerungswert beträgt 1.200 ms (400 * 3).
- 3. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 7 ausgewählt. Der maximale Verzögerungswert beträgt 2.800 ms (400 * 7).

Wenn die Verzögerung bei nachfolgenden Wiederholungen 10.000 überschreitet (die maximale Verzögerung), wird der Wert 10.000 als anfängliche Verzögerung verwendet.

Sobald die anfängliche Verzögerung generiert wurde, wird der Verzögerung Jitter hinzugefügt. Das Fenster „Jitter“ wird durch das Feld **Additional delay window in ms** (Fenster „Weitere Verzögerung“ in ms) definiert. Vom System wird ein zufälliger Wert zwischen 0 und 1.500 ausgewählt und zur anfänglichen Verzögerung addiert.

Wenn die anfängliche Verzögerung 500 beträgt, kann die endgültige Verzögerung (mit Jitter) einen Wert zwischen 500 und 2.000 ms annehmen.

Antwortheader – Backoff

Für die folgende Beispielkonfiguration …

Einstellung	Wert
Max. Wiederholungen	3
Antwortcodes	429
Antwortheader	Retry-After (Wiederholen-nach)
Verzögerungseinheit für Antwortheader	Sekunden
Additional delay window in ms (Fenster „Weitere Verzögerung“ in ms)	1500

… funktioniert die Backoff-Strategie für Antwortheader wie folgt:

- Rufen Sie den Wert des Headers `Retry-After` aus der Serverantwort ab.
- Konvertieren Sie den Wert von `Retry-After` in Millisekunden, indem Sie ihn mit 1.000 multiplizieren.

Sobald die anfängliche Verzögerung generiert wurde, wird der Verzögerung Jitter hinzugefügt. Das Fenster „Jitter“ wird durch das Feld **Additional delay window in ms** (Fenster „Weitere Verzögerung“ in ms) definiert. Vom System wird ein zufälliger Wert zwischen 0 und 1.500 ausgewählt und zur anfänglichen Verzögerung addiert.

Wenn die anfängliche Verzögerung 2.000 beträgt, kann die endgültige Verzögerung (mit Jitter) einen Wert zwischen 2.000 und 3.500 ms annehmen.

Anwenderdefiniertes Backoff

Mit einer anwenderdefinierten Backoff-Wiederholungsstrategie definieren Sie **Max. Wiederholungen** Und **Antwortcodes** Und erstellen Sie eigene **Mid-Skripteinbindung** Das definiert, wie Anforderungen mit wiederholt werden `getDelay()`Funktion. Weitere Informationen finden Sie unter Skripteinbindungen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie einen Cloud-Service-Account ein

Erstellen und konfigurieren Sie ServiceNow-Cloud-Accounts unter ServiceNow AI Platform Für die entsprechenden Cloud-Lieferantenservice-Accounts.

Zugehörige Informationen

Cloud-Discovery Referenz des Service-Account-Formulars

Richten Sie Service-Accounts für Oracle Cloud Infrastructure (OCI) ein

Erstellen und konfigurieren Sie Cloud-Service-Accounts unter ServiceNow AI Platform Für den entsprechenden Oracle Cloud Infrastructure-Service-Accounts (OCI).

OCI-Servicekonto ist eine Art von Identität, die zum Authentifizieren und Autorisieren des Zugriffs auf OCI-Ressourcen und -Services verwendet wird. Sie bietet Anwendungen, Services und Anwendern die Möglichkeit, sicher mit OCI-Ressourcen zu interagieren. Service-Accounts werden häufig für automatisierte Prozesse, Anwendungen oder Services verwendet, die innerhalb von OCI ausgeführt werden, sodass sie gemäß den definierten Berechtigungen und Richtlinien auf Ressourcen zugreifen können.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

OCI-Zugriff und -Berechtigung mithilfe von Richtlinien

Oracle Zugriff und Berechtigungen für Cloud Infrastructure (OCI) mithilfe von Richtlinien bieten Berechtigungen für die sichere Nutzung und Verwaltung von Cloud-Ressourcen in OCI.

Informationen zu OCI-Berechtigungen finden Sie unter Oracle Help Center Und suchen Sie nach dem artikel „Verwalten des Zugriffs auf Ressourcen“.

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Erstellen Oracle API-Anmeldeinformationen

Erstellen Oracle API-Anmeldeinformationen auf dem ServiceNow AI Platform Um den Zugriff auf zu aktivieren Oracle Ressourcen während Oracle Discovery.

Vorbereitungen
Stellen Sie sicher, dass Ihr OCI-Anwender mindestens schreibgeschützten Zugriff auf alle hat Oracle Services. Informationen zu Zugriffsberechtigungen erhalten Sie von Ihrem Systemadministrator.

Rufen Sie die folgenden Eigenschaften aus dem ab Oracle Cloud-Konsole:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Oracle Cloud-Bezeichner des Mandanten (Mandanten-OCID)
- Anwender-OCID
- Schlüssel-Fingerabdruck
- Privater Schlüssel

Anweisungen zum Abrufen dieser Eigenschaften finden Sie unter Oracle Help Center Und suchen Sie nach dem artikel „erforderliche Schlüssel und OCIDs“.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie Aus **Oracle API-Anmeldeinformationen** .
4. Füllen Sie die Felder im Formular mit den abgerufenen Eigenschaftswerten aus.

Formular „Oracle API-Anmeldeinformationen“

Feld	Wert
Name	Eindeutiger und beschreibender Name für die Oracle-Anmeldeinformationen
Aktiv	Option zur Verwendung der Anmeldeinformationen.
Mandanten-ID	Oracle Cloud-Bezeichner (OCID) für Ihren Mandanten.
Anwender-ID	OCID des OCI-Anwenders.
Schlüssel-Fingerabdruck	Fingerabdruck des öffentlichen Schlüssels.
Privater Schlüssel	Privater RSA-Schlüssel, der für die API-Signaturauthentifizierung verwendet wird.

5. Wählen Sie **Absenden**.

Nächste Maßnahme

Erstellen Sie OCI-Service-Accounts. Weitere Informationen finden Sie unter Erstellen Sie OCI-Service-Accounts.

Erstellen Sie OCI-Service-Accounts

Erstellen Oracle Cloud Infrastructure-Service-Accounts (OCI) auf der ServiceNow AI Platform Um auf zuzugreifen Oracle Account während Oracle Discovery.

Vorbereitungen

Verifizieren Sie das Oracle API-Anmeldeinformationen wurden erstellt. Weitere Informationen finden Sie unter Erstellen Oracle API-Anmeldeinformationen.

Rufen Sie die Compartment-ID ab, die unter zu finden ist **Identität Und Sicherheit** > **Fächer** In Oracle Cloud-Konsole.

Erforderliche Rolle: discovery_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie im Navigationsfilter ein `cmdb_ci_Cloud_Service_Account.list` .
2. Wählen Sie **Neu**.
3. In **Feld „Discovery-Anmeldeinformationen“** , Beginnen Sie mit der Eingabe des Anmeldeinformationsnamens, und wählen Sie ihn aus der Liste aus.
4. Füllen Sie die verbleibenden Felder im Formular aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Ein eindeutiger Name für den OCI-Service-Account.
Account-ID	Compartment-ID, die ist Oracle Cloud-Bezeichner (OCID) des Compartments, das diesem Service-Account zugeordnet ist.
Rechenzentrums-URL	URL des Rechenzentrums. Beispiel: `https://service.ap-mumbai-1.oraclecloud.com` .
Datencenter-Typ	Typ des Rechenzentrums, in dem der Account gehostet wird, wobei es sich um das OCI-Rechenzentrum [cmdb_ci_oci_Datacenter] handeln muss.

5. Wählen Sie **Absenden**.

Nächste Maßnahme

Planen Sie eine OCI-Cloud-Discovery. Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

Wird eingerichtet AWS Service-Accounts

Erstellen und konfigurieren Sie Cloud-Servicekonten auf der ServiceNow AI Platform für die entsprechenden Amazon Web Services-Servicekonten (AWS).

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Sie müssen mit der Hierarchie der AWS-Servicekonten in Ihrer Umgebung vertraut sein. Wenn es beispielsweise AWS-Organisationen gibt, richten Sie in ServiceNow AI Platform Verwaltungs- und Mitgliedskonten ein, die diese Hierarchie abbilden. Sie können AWS-Servicekonten der folgenden Typen einrichten:

- **Diskretes Konto**: Eigenständiges Konto ohne Verwaltungskonto.
- **Verwaltungskonto**: Verwaltungskonto, das Mitgliedskonten (Unterkonten) enthalten kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In einigen UI-Bildschirmen in ServiceNow werden Verwaltungskonten als Master-Konten bezeichnet.

- **Mitgliedskonto**: Unterkonto, das zum (Verwaltungs-)Konto gehört.

Zugriff für AWS-Servicekonten einrichten

Cloud-Discovery und Cloud Provisioning and Governance benötigen Zugriff auf Ressourcen in den AWS-Servicekonten (Amazon Web Services). Informieren Sie sich über verschiedene Methoden zur Konfiguration dieses Zugriffs.

Cloud-Discovery und Cloud Provisioning and Governance greifen auf Ressourcen in den AWS-Servicekonten über MID Servers zu. Sie müssen eingehenden Datenverkehr an autorisieren Amazon EC2-Instanzen aus dem MID-Server Zum Einrichten der ersten Kommunikation. Weitere Informationen finden Sie unter Konfigurieren Sie eingehende Regeln für Sicherheitsgruppen mit der AWS-Verwaltungskonsole .

Typen von AWS-Anmeldeinformationen

Es gibt permanente und temporäre AWS-Anmeldeinformationen, die Sie zur Konfiguration des Zugriffs auf AWS-Servicekonten verwenden können.

Permanent

Die permanenten Anmeldeinformationen sind die eigentlichen AWS-Anmeldeinformationen für das Servicekonto, das Sie zum Modul Verbindungen und Anmeldeinformationen von ServiceNow AI Platform hinzufügen. Es kann zwar zeitaufwändig sein, Anmeldeinformationen für zu verwalten ServiceNow AI Platform, Vermeiden Sie die komplexen Konfigurationen, die bei der Verwendung temporärer Anmeldeinformationen erforderlich sind.

Temporär

Die temporären Anmeldeinformationen werden vom AWS-Sicherheitstoken-Service (AWS STS) für IAM-Rollen generiert. Nachdem Sie IAM-Rollen für konfiguriert haben AWS Accounts, die MID-Server Zugriffe AWS Ressourcen mit diesen temporären Anmeldeinformationen. Sie können die IAM-Standardrolle `OrganizationAccountAccessRole` verwenden oder benutzerdefinierte IAM-Rollen erstellen.

Die Annahme von IAM-Rollen in einer großen AWS-Organisation ist bequemer und bietet mehr Sicherheit als die Verwendung einer hohen Anzahl permanenter Anmeldeinformationen für alle AWS-Konten. Temporäre Anmeldeinformationen werden nur im Namen eines Service-Accounts erworben, wenn für diesen Service-Account keine permanenten Anmeldeinformationen in der Tabelle „Service-Accounts“ [cmdb_ci_Cloud_Service_Account] angegeben sind.

Die MID-ServerVerwendet AssumeRole Aktion in AWS-Sicherheits-Token-Service-API Um eine Mitgliedsaccount-Rolle zu übernehmen. An diese API übergebene Parameter bestimmen, welche zusätzlichen Sicherheitsbeschränkungen auf die Rolle beim Zugriff auf AWS-Ressourcen angewendet werden.

Standardmäßig ist der MID-Server so konfiguriert, dass er die Rolle `OrganizationAccountAccessRole` übernimmt, mit der allen Mitgliedern eines Primärkontos temporäre Anmeldeinformationen gewährt werden. Diese Aktion erfolgt automatisch, wenn keine permanenten Anmeldeinformationen für die Mitgliedskonten vorhanden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind. Durch diese Konfiguration werden keine zusätzlichen Sicherheitseinstellungen angewendet; der Zugriff auf Ressourcen in Mitgliedskonten wird nicht eingeschränkt.

Standardmäßig werden temporäre Anmeldeinformationen für Mitgliedskonten 60 Minuten lang im Cache der ServiceNow-Instanz gespeichert. Mit diesem Intervall kann der horizontale Discovery-Prozess mehrmals ausgeführt werden, ohne während jeder Discovery neue Anmeldeinformationen zu generieren. Sie können das Caching von Anmeldeinformationen vermeiden oder den Caching-Zeitraum mit ändern MID-Server-Eigenschaften .

IAM-Rollen und -Berechtigungen

Dient zur Verbesserung der standardmäßig bereitgestellten Sicherheit AWS OrganizationAccountAccessRole -Rolle können Sie anpassen AWS Rollen, die MID Servers Kann annehmen, dass temporäre Anmeldeinformationen für Mitgliedsaccounts erhalten werden. Sie können zusätzliche Berechtigungen konfigurieren, um die Sicherheit zu verbessern und um anzupassen, wie die Rolle des Mitgliedskontos angenommen wird, wenn Cloud-Ressourcen erkannt werden.

Methoden zum Gewähren von Zugriff

Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Normalerweise richten Sie den Zugriff auf die AWS-Konten in Ihrer Organisation mit den folgenden Methoden ein:

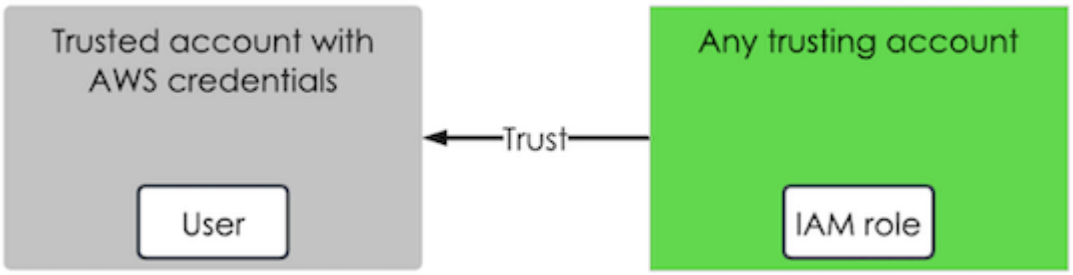
Konfigurieren des Zugriffs für einen einzelnen Account

- Konfigurieren AWS Anmeldeinformationen für ServiceNow AI Platform Um die Komplexität der Erstellung und Einrichtung von IAM-Rollen zu vermeiden. Weitere Informationen finden Sie unter Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren.
- Erstellen Sie einen AWS Service-Account auf der ServiceNow AI Platform. Weitere Informationen finden Sie unter Erstellen AWS Service-Accounts.

Konfigurieren des Zugriffs für einen Account, der einem Zugriffsberechtigungs-Account mit vertraut AWS Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Konten so einrichten, dass sie auf ein vertrauenswürdiges Konto mit AWS-Anmeldeinformationen zurückgreifen

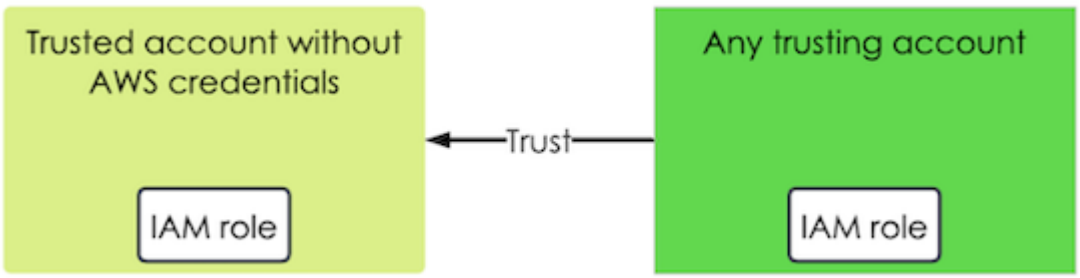


- Konfigurieren Sie jede Art von Account – diskret (unabhängig), Management oder Mitglied –, um sich auf einen vertrauenswürdigen Account mit zu verlassen AWS Anmeldeinformationen für den Zugriff.
- Wenn Sie eine IAM-Rolle konfigurieren, die zu den vertrauenden Accounts gehört, um dem Anwender des vertrauenswürdigen Accounts zu vertrauen, können Sie nur einen Satz von verwenden AWS Anmeldeinformationen für die Bereitstellung von Zugriff auf mehrere AWS Accounts.

Weitere Informationen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.

Konfigurieren des Zugriffs für einen Account, der einem Zugriffsberechtigungs-Account ohne vertraut AWS Anmeldeinformationen

AWS-Konten so einrichten, dass sie auf einem vertrauenswürdigen Konto ohne AWS-Anmeldeinformationen beruhen



- Konfigurieren Sie jede Art von Account – diskret (unabhängig), Management oder Mitglied – so, dass Sie sich ohne auf einen vertrauenswürdigen Account verlassen können AWS Anmeldeinformationen für den Zugriff.
- Konfigurieren Sie einen Account ohne AWS Anmeldeinformationen mit einer IAM-Rolle und Berechtigungen für den Zugriff auf den vertrauenden Service-Account.
- Richten Sie die IAM-Rolle des vertrauenden Accounts ein, um Zugriff auf die IAM-Rolle des vertrauenswürdigen Accounts zu gewähren.

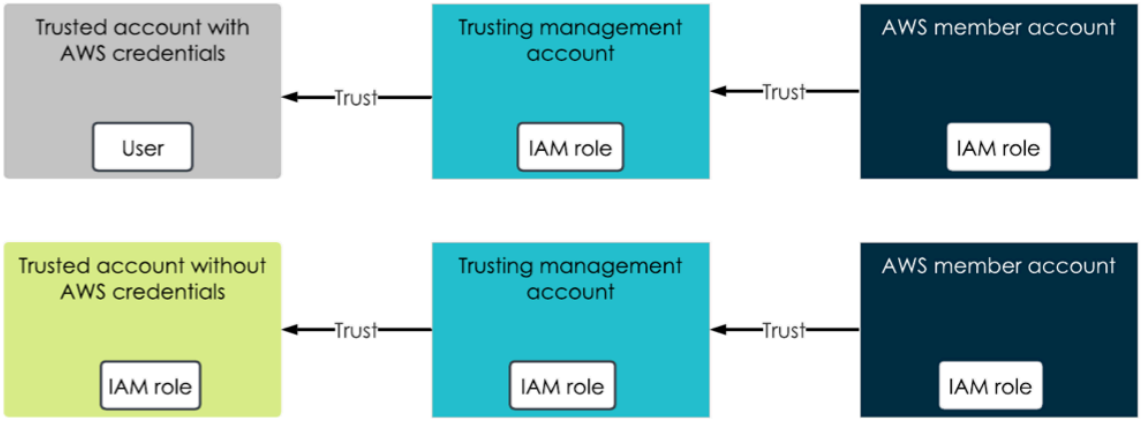
Weitere Informationen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren.

Konfigurieren des Zugriffs für AWS mitglieds-Accounts mithilfe einer Vertrauenskette vom Zugriffsberechtigten über den Verwaltungs-Account.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mitgliedskonten so konfigurieren, dass sie für den Zugriff das jeweilige Verwaltungskonto nutzen



- Konfigurieren Sie die IAM-Rollen der Mitglieds-Accounts so, dass sie der IAM-Rolle ihres Verwaltungs-Accounts vertrauen. Weitere Informationen finden Sie unter Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren.
- Konfigurieren Sie die Verwaltungsaccounts so, dass sie den Zugriffsberechtigte-Accounts mit oder ohne vertrauen AWS Anmeldeinformationen. Weitere Informationen finden Sie unter:
  - Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.
  - Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren.

Wie Cloud-Discovery die zu verwendenden Anmeldeinformationen bestimmt

Mitgliedsaccount vertraut dem Verwaltungsaccount

Cloud-Discovery Verwendet die folgende Logik, um zu bestimmen, welche Anmeldeinformationen für die Erkennung verwendet werden sollen AWS Cloud-Ressourcen in Mitgliedsaccounts:

1. Wenn für das Mitgliedskonto in der Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service_account] dauerhafte Anmeldeinformationen definiert sind, verwendet Discovery diese Anmeldeinformationen. Die Tabelle „Cloud-Servicekonten“ [cmdb_ci_cloud_service_account] enthält die Informationen zu den Servicekontotypen wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
2. Wenn für den Mitgliedsaccount keine permanenten Anmeldeinformationen definiert sind, DiscoveryÜberprüft die Tabelle „AWS-Org-Rollenübernahmeparameter für Cloud-Service-Account“ [Cloud_Service_Account_aws_org_take_role_params] auf spezielle Parameter, die dem Mitgliedsaccount zugeordnet sind. Wenn in dieser Tabelle Parameter vorhanden sind, verwendet Discovery die temporären Anmeldeinformationen, die durch Angabe einer Rolle und deren Parameter in der Aktion „AssumeRole“ der AWS-Sicherheits-Token-Service-API abgerufen wurden.
3. Wenn dem Mitgliedsaccount in der Tabelle [Cloud_Service_Account_aws_org_take_role_params] keine speziellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter zugeordnet sind, DiscoveryÜberprüft diese Tabelle auf Parameter, die dem Verwaltungs-Account zugeordnet sind. Wenn Parameter vorhanden sind, die eine Rolle für den Verwaltungsaccount definieren, Discovery Verwendet die von dieser Rolle bereitgestellten temporären Anmeldeinformationen.

4. Wenn in der Tabelle [cloud_service_account_aws_org_assume_role_params] keine speziellen Parameter für Verwaltungs- oder Mitgliedskonten vorhanden sind, verwendet Discovery die Standardeinstellungen, die für die Rolle OrganizationAccountAccessRole definiert sind.

Mitglieds- oder Verwaltungsaccount vertraut dem Account des Zugreifers

1. Wenn dauerhafte Anmeldeinformationen für das Mitglied oder den Verwaltungsaccount in der Tabelle „Cloud-Service-Account“ [cmdb_ci_Cloud_Service_Account] definiert sind, Discovery Verwendet diese Anmeldeinformationen. Die Tabelle „Cloud-Servicekonten“ [cmdb_ci_cloud_service_account] enthält die Informationen zu den Servicekontotypen wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
2. Wenn für den Account keine permanenten Anmeldeinformationen definiert sind, DiscoveryÜberprüft die Tabelle „AWS-übergreifende Rollenübernahmeparameter für Cloud-Service-Account“ [Cloud_Service_Account_aws_Cross_take_role_params] auf spezielle Parameter, die dem Account zugeordnet sind. Wenn in dieser Tabelle Parameter vorhanden sind, verwendet Discovery die temporären Anmeldeinformationen, die durch Angabe einer Rolle und deren Parameter in der Aktion „AssumeRole“ der AWS-Sicherheits-Token-Service-API abgerufen wurden.

Zugehörige Informationen

KB2184482: Schritt-für-Schritt-Anleitung zum Konfigurieren der AWS Cloud Discovery in ServiceNow mithilfe von Mustern

Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Damit die Anmeldeinformationen für Discovery und Cloud Provisioning and Governance verfügbar sind, müssen Sie in der AWS-Verwaltungskonsole zunächst einen Benutzer mit programmgesteuertem Zugriff erstellen. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in ServiceNow AI Platform.

Vorbereitungen

Erforderliche Rollen:

- AWS-Verwaltungskonsole-Administrator
- Für Cloud-Discovery: Discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. **Wahlweise:** Um einen Benutzer für Cloud Provisioning and Governance zu erstellen (für den Zugriff des Programms auf Ihre AWS-Ressource und Abrechnungsdaten), gehen Sie wie folgt vor:

   a. Auf der AWS-Verwaltungskonsole, Navigieren Sie zu **Identitäts- und Zugriffsmanagement (IAM)** > **Zugriffsverwaltung** > **Anwender**an.

   b. Klicken Sie im IAM-Ressourcenportal auf **Anwender**.

   c. Wählen Sie **Anwender hinzufügen** aus.

   d. Konfigurieren Sie auf der Seite „Details“ die Benutzereinstellungen, und klicken Sie dann auf **Weiter**.

   Detailseite

Feld	Beschreibung
Benutzername	Name des Benutzers in Form eines Programms. Beispiel: servicenowcloud.
Zugriffstyp	Wählen Sie **Programmatic access** (Programmgesteuerter Zugriff) aus.

   e. Auf der Seite für die Berechtigungen fügen Sie den Benutzer einer Richtlinie hinzu. Konfigurieren Sie die folgenden Einstellungen, und wählen Sie dann **Weiter** aus.

Feld	Beschreibung
Berechtigungen für <Benutzername> festlegen	Wählen Sie **Attach existing policies directly** (Vorhandene Richtlinien direkt anhängen) aus.
Attach one or more policies … (Mindestens eine Richtlinie anhängen …)	Wählen Sie die entsprechende Richtlinie aus. **Hinweis:** Die Richtlinie **AdministratorAccess** hat die umfassendste Berechtigungsstufe, einschließlich der Berechtigung zum Bereitstellen von Cloud-Ressourcen. Die Richtlinie ermöglicht den gleichen Zugriff, der der Instanz gewährt würde, wenn Sie nicht IAM, sondern die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres AWS-Kontos verwenden würden. Sie können stattdessen eine Richtlinie erstellen oder mehrere Richtlinien kombinieren, um die entsprechende Berechtigungsstufe zu gewähren. Weitere Detailinformationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.

   f. Überprüfen Sie auf der Seite „Prüfung“ Ihre Auswahl, und wählen Sie dann **Benutzer erstellen** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Kopieren Sie auf der Seite „Security Credentials“ (Sicherheitsanmeldeinformationen) den geheimen Zugriffsschlüssel und die Zugriffsschlüssel-ID.

> **Wichtig:** Verlassen Sie die Seite erst, wenn Sie beide Schritte abgeschlossen haben. Der Wert des **geheimen Zugriffsschlüssels** wird nicht erneut angezeigt. Die in diesen Schritten generierten Werte müssen Sie in ein Cloud Provisioning and Governance-Formular einfügen.

i. Klicken Sie auf **Anzeigen**, um den geheimen Zugriffsschlüssel anzuzeigen. Kopieren Sie den Wert.

ii. Wählen Sie **Download .csv** (.csv herunterladen) aus, um die Datei, die den Benutzernamen, die Zugriffsschlüssel-ID und den Wert des geheimen Zugriffsschlüssels enthält, im CSV-Format zu speichern. Erstellen Sie die Datei als Sicherung für den Fall, dass Sie die Werte verlieren. Stellen Sie sicher, dass die Datei erstellt wurde, und speichern Sie sie dann sicher.

2. In ServiceNow Instanz, navigieren Sie zu **Discovery** > **Anmeldeinformationen**an.
3. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein (z. B. Cloud-Bereitstellungskonto), und füllen Sie dann das Formular aus.

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

4. Wählen Sie **Aktualisieren** oder **Absenden**.

Nächste Maßnahme

Erstellen Sie einen AWS Service-Account auf der ServiceNow AI Platform. Weitere Informationen finden Sie unter Erstellen AWS Service-Accounts.

Erstellen AWS Service-Accounts

Erstellen AWS Service-Accounts auf der ServiceNow AI Platform Um auf zuzugreifen AWS Account während AWS Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Rufen Sie die Anwenderkontonummer ab, die sich im befindet AWS-VerwaltungskonsoleIndem Sie die Liste unter erweitern AWS Account-Name.
- Bestätigen Sie das Discovery-Administratorarbeitsbereich Verwendet mindestens Version 1.10.0. Die **Discovery** > **Cloud-Service-Accounts** Das Navigationsmodul ist mit früheren Versionen nicht verfügbar. Um auf zuzugreifen **Cloud-Service-Accounts** Geben Sie bei einer früheren Version im Navigationsfilter Folgendes ein: cmdb_ci_Cloud_Service_Account.list .

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Service-Account ist ein sicherer Datensatz in Ihrer Instanz, der die Anmeldeinformationen und Zugriffsinformationen für Ihren Provider-Account speichert. Discovery Verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen, um Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Account ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in der Cloud-Verwaltung. Ein Cloud-Account kann mehrere Service-Accounts enthalten, sogar Service-Accounts verschiedener Anbieter. Geben Sie für jeden Service-Account an, welches Rechenzentrum in den Cloud-Account aufgenommen werden soll.

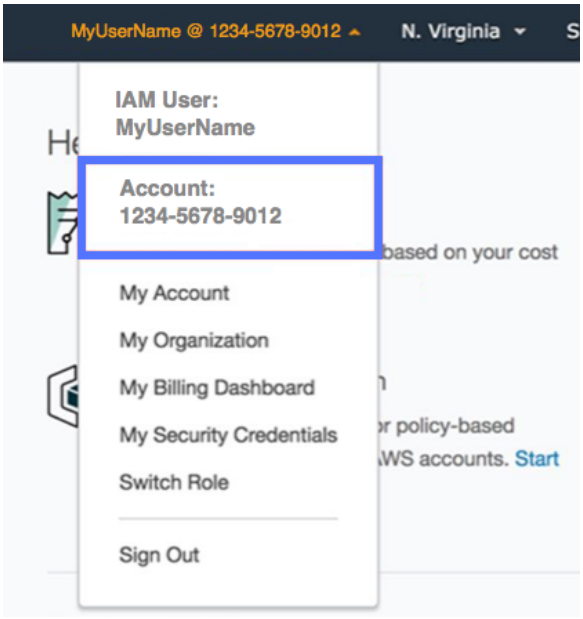
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nummer des IAM-Benutzerkontos 
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ○ Wenn Sie Konfigurierte AWS-Anmeldeinformationen unter ServiceNow AI Platform , Wählen Sie das Lupensymbol, und wählen Sie dann den Namen des entsprechenden aus AWS Anmeldeinformationen. ○ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für erforderlich AWS Region China und AWS GovCloud (USA)-Accounts. Zum Beispiel: ○ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ○ AWS GovCloud (USA): `https://ec2.us-gov-west-1.amazonaws.com`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen. **Hinweis:** Sie müssen die richtige Berechtigung in einrichten AWS Oder die Organisationsrolle für Standardanmeldeinformationen. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

4. Wählen Sie **Absenden**.

Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren

Konfigurieren Sie das vertrauende Konto, auf dessen Ressourcen zugegriffen werden muss, so, dass es über die Identity and Access Management (IAM)-Rolle auf das vertrauenswürdige Konto zurückgreift.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Entscheiden Sie, welches AWS-Konto das vertrauenswürdige Konto sein soll. Sie verwenden den vertrauenswürdigen Account, um temporäre Anmeldeinformationen für zu konfigurieren Cloud-Discovery Mit IAM-Rollen. Der vertrauenswürdige Account, den Sie für den Zugriff auf andere Accounts mit IAM-Rollen verwenden, wird als Account eines Zugriffsberechtigten bezeichnet.
- Wenn Sie eine Vertrauenskette einrichten, bei der ein Mitgliedsaccount einem Verwaltungs-Account vertraut und der Verwaltungsaccount einem Zugriffsberechtigungs-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Account vertraut, überprüfen Sie, ob Sie den Mitgliedsaccount so konfiguriert haben, dass er dem Verwaltungs-Account vertraut. Weitere Informationen finden Sie unter Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren.

- Bestätigen Sie das Discovery-Administratorarbeitsbereich Verwendet mindestens Version 1.10.0. Die **Discovery** > **Cloud-Service-Accounts** Das Navigationsmodul ist mit früheren Versionen nicht verfügbar. Um auf zuzugreifen **Cloud-Service-Accounts** Geben Sie bei einer früheren Version im Navigationsfilter Folgendes ein: cmdb_ci_Cloud_Service_Account.list .

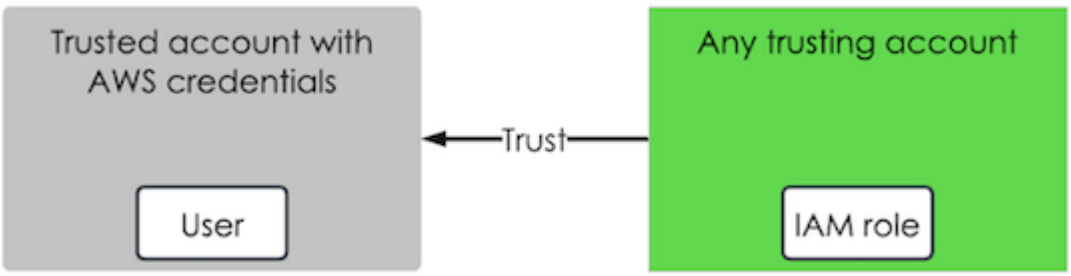
Erforderliche Rolle:

- Für Cloud-Discovery: Discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Während dieser Konfiguration erstellen Sie eine IAM-Rolle für das vertrauende Konto und konfigurieren dann das vertrauenswürdige Servicekonto für das vertrauende Konto in ServiceNow AI Platform. Schließlich ordnen Sie die IAM-Rolle, die Sie für das vertrauende Konto erstellt haben, dem vertrauenden Konto selbst zu.

AWS-Konten so einrichten, dass sie auf ein vertrauenswürdiges Konto mit AWS-Anmeldeinformationen zurückgreifen



Prozedur

1. Erstellen Sie eine IAM-Rolle für das vertrauende Konto, und konfigurieren Sie die Vertrauensstellung zwischen dem Benutzer, der diese Rolle übernimmt, und dem vertrauenswürdigen Konto (Account des Zugriffsberechtigten).

   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Account an.

   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des vertrauenswürdigen Kontos (des Accounts des Zugriffsberechtigten) angeben.
   Für Informationen zum Erstellen AWS-Rollen finden Sie unter Amazon Dokumentation an.

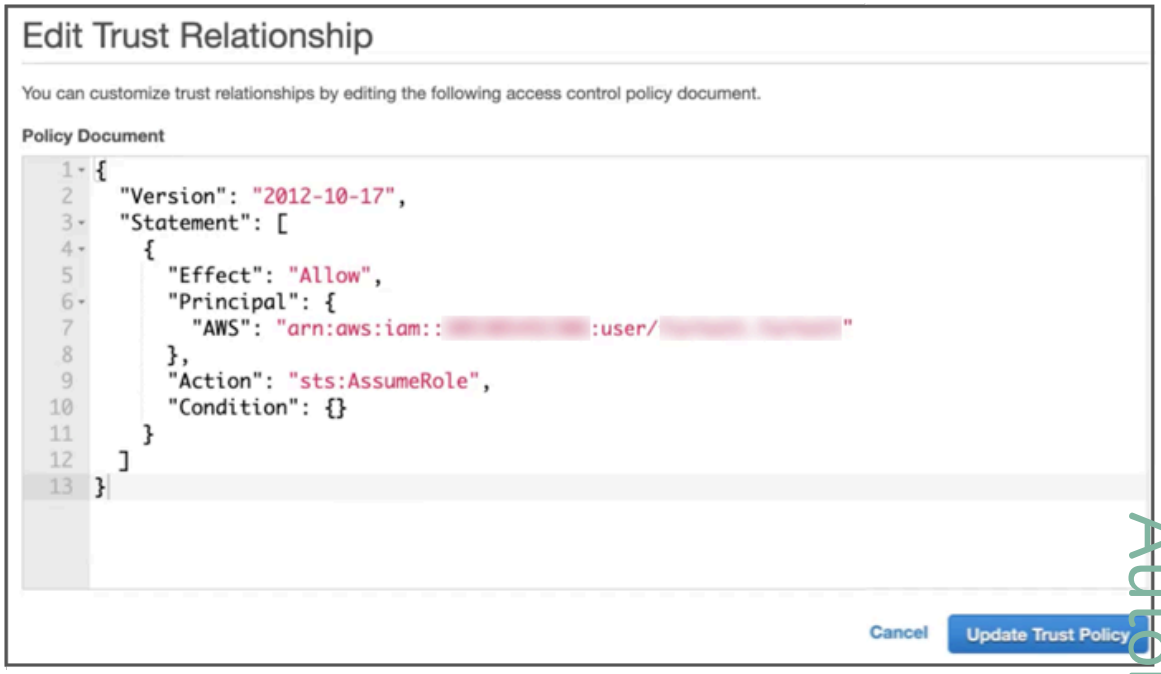
   c. Wählen Sie auf der Seite „Zusammenfassung“ für die IAM-Rolle die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten).
   Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

   e. Legen Sie den Parameter *AWS* auf den vollständigen Benutzer-ARN des vertrauenswürdigen Accounts (des Zugriffsberechtigten) fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

f. Verifizieren Sie, ob der *`Action`*-Wert auf *`sts:AssumeRole`* festgelegt ist.

g. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Auf der ServiceNow AI Platform, Konfigurieren Sie den vertrauenswürdigen Service-Account.

a. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.

b. Auswählen **Neu** .

c. Füllen Sie im Formular die Felder aus.
Eine Beschreibung der Feldwerte finden Sie unter Erstellen AWS Service-Accounts.

d. Wählen Sie **Absenden**.

3. Auf der ServiceNow AI Platform, Konfigurieren Sie den vertrauenden Service-Account.

a. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.

b. Wählen Sie **Neu**.

c. In **Zugriffsberechtigter-Account** Geben Sie den Namen des vertrauenswürdigen Accounts ein.

d. Füllen Sie die verbleibenden Felder im Formular aus.
Eine Beschreibung der Feldwerte finden Sie unter Erstellen AWS Service-Accounts.

e. Wählen Sie **Absenden**.

4. Auf der ServiceNow AI Platform, Weisen Sie zu AWS IAM-Rolle für den vertrauenden Account mithilfe des entsprechenden Formulars basierend auf der Beziehung zum vertrauenswürdigen Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vertrauenswürdiger Account-Typ	Schritte
Verwaltungsaccount	**a.** Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS-Org. – Parameter für Rollenübernahme**an. **b.** Wählen Sie **Neu**. **c.** Konfigurieren Sie im Formular nur die folgenden Felder für den Account des vertrauenden Mitglieds: **Formular „AWS-Organisation für Cloud-Service-Account – Rollenparameter über nehmen“** **Feld** / **Definition** Name der Zugriffsrolle Name der IAM-Rolle, die für den vertrauende Account erstellt wurde. ▪ Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den vollständigen ARN mit einem Sternchen (*) als Platzhalter für die Account-ID im folgenden Format ein: `arn:aws:iam::*:role/MemberRoleName`. Beispiel: `arn:aws:iam::*:role/SN_MEMBER_ACCOUNT_ROLE`. ▪ Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie den vollständigen ARN der spezifischen IAM-Rolle für jeden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

<table>
<tr><th>Vertrauenswürdiger Account-Typ</th><th>Schritte</th></tr>
<tr><td></td><td>
<table>
<tr><th>Feld</th><th>Definition</th></tr>
<tr><td></td><td>Mitgliedsaccount in einem separaten Eintrag ein.</td></tr>
<tr><td>Cloud-Servicekonto</td><td>Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen.
Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den Namen des Verwaltungsaccounts ein.
Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie jeden Mitgliedsaccount in einem separaten Eintrag ein.</td></tr>
</table>
d. Wählen Sie Absenden.
</td></tr>
<tr><td>Mitglieds- oder diskreter Account</td><td>a. Navigieren zu Alle > Cloud Provisioning and Governance > Zugriffsparameter der Organisation > AWS – Parameter für über greifende Rollenübernahmean.
b. Wählen Sie Neu.
c. Konfigurieren Sie im Formular nur die folgenden Felder für den vertrauenden Account:</td></tr>
</table>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vertrauenswürdiger Account-Typ	Schritte
	Formular „AWS-übergreifende Rollen übernahmeparameter für Cloud-Service-Account“ **Feld** / **Beschreibung** Name der Zugriffsrolle: Name der IAM-Rolle, die für den vertrauende Account erstellt wurde. Cloud-Servicekonto: Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen. **d.** Wählen Sie **Absenden**.

Nächste Maßnahme

Stellen Sie sicher, dass ServiceNow-Anwendungen mithilfe der IAM-Rolle auf das vertrauende Servicekonto zugreifen können:

1. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.
2. Wählen Sie das Vertrauen aus AWS Service-Account.
3. Unter **Zugehörige Links** , Wählen Sie aus **Erstellen Sie Einen Discovery-Zeitplan** .
4. Wählen Sie auf der Seite Discovery Manager Cloud Discovery die Option aus **Test-Account** .
   - Wenn die Verbindung erfolgreich ist, wird eine Meldung angezeigt, die angibt, dass die Accountvalidierung erfolgreich war.
   - Wenn die Verbindung nicht erfolgreich ist, wird eine Fehlermeldung angezeigt, die die Fehlerursache angibt.

Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren

Richten Sie ein vertrauenswürdiges Konto ohne Anmeldeinformationen ein, auf das andere AWS-Konten für den Zugriff zurückgreifen können.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Entscheiden Sie, welches AWS-Konto das vertrauenswürdige Konto sein soll. Sie verwenden den vertrauenswürdigen Account, um temporäre Anmeldeinformationen für zu konfigurieren Cloud-Discovery Mit IAM-Rollen. Der vertrauenswürdige Account, den Sie für den Zugriff auf andere Accounts mit IAM-Rollen verwenden, wird als Account eines Zugriffsberechtigten bezeichnet.
- Wenn Sie eine Vertrauenskette einrichten, bei der ein Mitgliedsaccount einem Verwaltungs-Account vertraut und der Verwaltungsaccount einem Zugriffsberechtigungs-Account vertraut, überprüfen Sie, ob Sie den Mitgliedsaccount so konfiguriert haben,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dass er dem Verwaltungs-Account vertraut. Weitere Informationen finden Sie unter Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren.

- Bestätigen Sie das Discovery-Administratorarbeitsbereich Verwendet mindestens Version 1.10.0. Die **Discovery** > **Cloud-Service-Accounts** Das Navigationsmodul ist mit früheren Versionen nicht verfügbar. Um auf zuzugreifen **Cloud-Service-Accounts** Geben Sie bei einer früheren Version im Navigationsfilter Folgendes ein: `cmdb_ci_Cloud_Service_Account.list` .

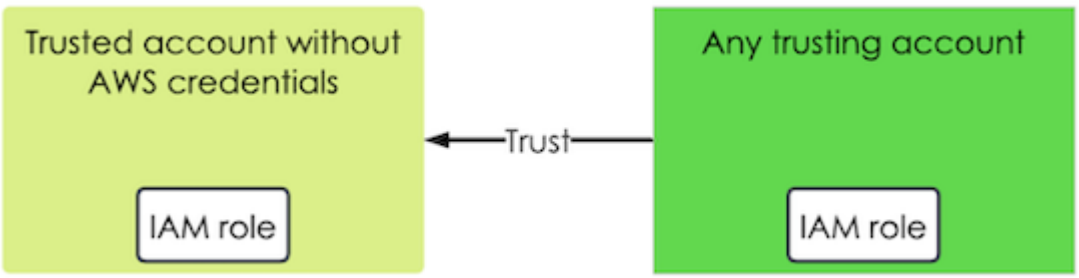
Erforderliche Rolle:

- Für Cloud-Discovery: Discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Dient zur Verwendung eines Accounts ohne AWS Anmeldeinformationen müssen Sie diesen Account zuerst mit einer IAM-Rolle und Berechtigungen für den Zugriff auf den vertrauenden Service-Account konfigurieren. Dann richten Sie die IAM-Rolle des vertrauenden Accounts ein, um Zugriff auf die IAM-Rolle des vertrauenswürdigen Accounts zu gewähren.

AWS-Konten so einrichten, dass sie auf einem vertrauenswürdigen Konto ohne AWS-Anmeldeinformationen beruhen

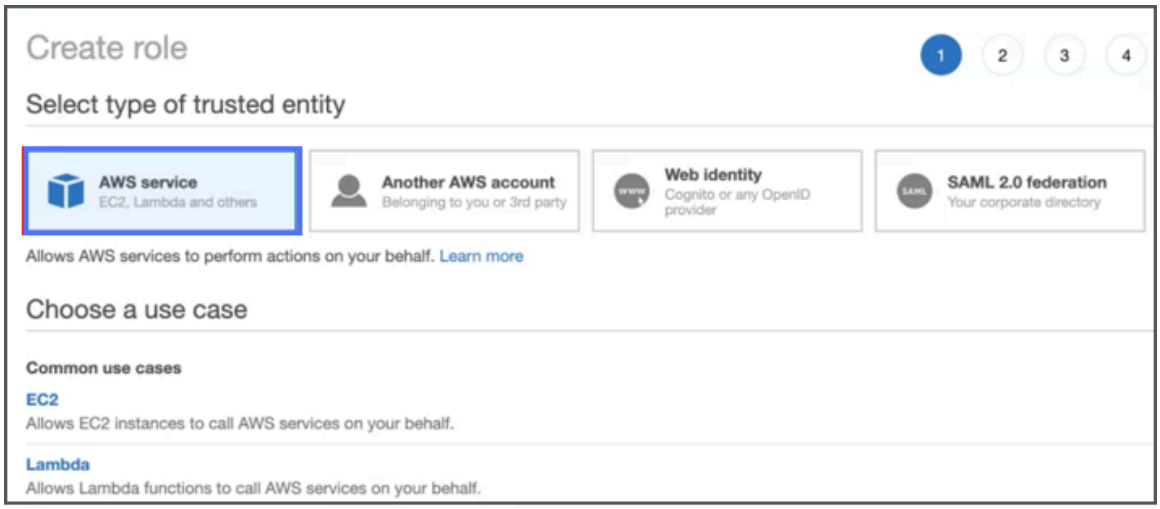


Prozedur

1. Konfigurieren Sie eine IAM-Rolle für das vertrauende Konto.
   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Konto an.
   b. Erstellen Sie eine IAM-Rolle für dieses Konto.
   Verwenden Sie beim Erstellen dieser IAM-Rolle die Konto-ID des vertrauenswürdigen Kontos.
   Bedienungsinformationen zum Arbeiten mit AWS-Rollen finden Sie in der Amazon-Dokumentation.
   c. Erstellen Sie eine ReadOnlyAccess-Richtlinie, und hängen Sie sie an die neu erstellte IAM-Rolle an.
2. Konfigurieren Sie die IAM-Rolle für das vertrauenswürdige Konto.
   a. Melden Sie sich bei der AWS-Managementkonsole mit den Anmeldeinformationen des Kontos an, das Sie als vertrauenswürdiges Konto einrichten möchten.
   b. Wählen Sie die Option **AWS service** aus, um eine IAM-Rolle zu erstellen.

Automatische Übersetzung

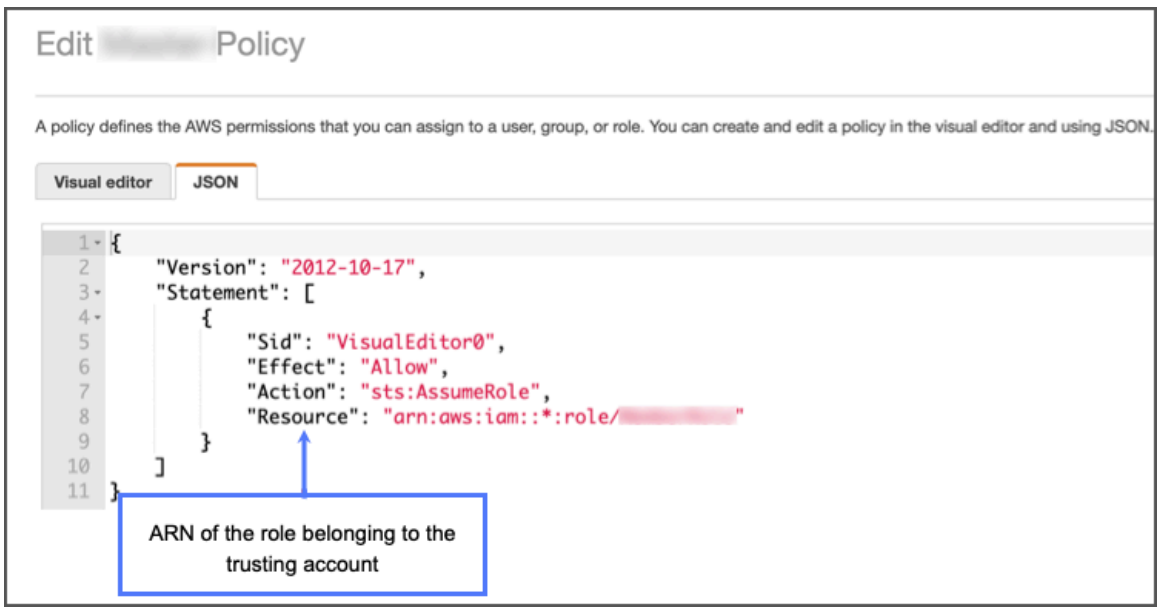
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Erstellen Sie eine ReadOnlyAccess-Richtlinie für die IAM-Rolle des vertrauenswürdigen Kontos.

d. Erstellen Sie eine zusätzliche Richtlinie, um dieser IAM-Rolle Zugriff auf Ressourcen in vertrauenden Konten zu gewähren:

- Legen Sie den Parameter *`Action`* auf `sts:AssumeRole` fest.
- Legen Sie den Parameter *`Resource`* auf den ARN der Rolle des vertrauenden Kontos fest, die Sie in 1.b erstellt haben.



e. Hängen Sie die neu erstellte Rolle an die relevante Amazon EC2-Instanz an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine IAM-Rolle an eine EC2-Instanz anhängen, wird standardmäßig eine Vertrauensstellung zwischen dieser Rolle und der EC2-Instanz erzeugt.

3. Konfigurieren Sie das vertrauende Servicekonto, um Zugriff auf die IAM-Rolle zu gewähren, die zum vertrauenswürdigen Konto gehört.

   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Konto an.

   b. Navigieren Sie zu der IAM-Rolle, die Sie für dieses Konto in 1.b erstellt haben.

   c. Bearbeiten Sie die Vertrauensstellung für diese IAM-Rolle wie folgt:

   - Legen Sie den Parameter *`Action`* auf `sts:AssumeRole` fest.
   - Legen Sie den Parameter *`AWS`* auf den ARN der Rolle des vertrauenswürdigen Kontos fest, die Sie in 2.b erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. MID-Server für AWS-IAM-Rollen konfigurieren.
5. Auf der ServiceNow AI Platform, Konfigurieren Sie den vertrauenswürdigen Service-Account.
   a. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.
   b. Auswählen **Neu** .
   c. Füllen Sie im Formular die Felder aus.
   Eine Beschreibung der Feldwerte finden Sie unter Erstellen AWS Service-Accounts.
   d. Wählen Sie **Absenden**.
6. Auf der ServiceNow AI Platform, Konfigurieren Sie den vertrauenden Service-Account.
   a. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.
   b. Wählen Sie **Neu**.
   c. In **Zugriffsberechtigter-Account** Geben Sie den Namen des vertrauenswürdigen Accounts ein.
   d. Füllen Sie die verbleibenden Felder im Formular aus.
   Eine Beschreibung der Feldwerte finden Sie unter Erstellen AWS Service-Accounts.
   e. Wählen Sie **Absenden**.
7. Auf der ServiceNow AI Platform, Weisen Sie zu AWS IAM-Rolle für den vertrauenden Account mithilfe des entsprechenden Formulars basierend auf der Beziehung zum vertrauenswürdigen Account.

Vertrauenswürdiger Account-Typ	Schritte
Verwaltungsaccount	a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS-Org. – Parameter für Rollenübernahme**an. b. Wählen Sie **Neu**. c. Konfigurieren Sie im Formular nur die folgenden Felder für den Account des vertrauenden Mitglieds: **Formular „AWS-Organisation für Cloud-Service-Account – Rollenparameter über nehmen“** **Feld** / **Definition** Name der Zugriffsrolle – Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vertrauenswürdiger Account-Typ	Schritte

Feld	Definition
	▪ Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den vollständigen ARN mit einem Sternchen (*) als Platzhalter für die Account-ID im folgenden Format ein: `arn:aws:iam::*:role/MemberRoleName`. Beispiel: `arn:aws:iam::*:role/SN_MEMBER_ACCOUNT_ROLE`. ▪ Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie den vollständigen ARN der spezifischen IAM-Rolle für jeden Mitgliedsaccount in einem separaten Eintrag ein.
Cloud-Servicekonto	Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen. ▪ Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den Namen des Verwaltungsaccounts ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

<table>
<tr><th>Vertrauenswürdiger Account-Typ</th><th>Schritte</th></tr>
<tr><td></td><td>
<table>
<tr><th>Feld</th><th>Definition</th></tr>
<tr><td></td><td>▪ Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie jeden Mitgliedsaccount in einem separaten Eintrag ein.</td></tr>
</table>
d. Wählen Sie Absenden.</td></tr>
<tr><td>Mitglieds- oder diskreter Account</td><td>a. Navigieren zu Alle > Cloud Provisioning and Governance > Zugriffsparameter der Organisation > AWS – Parameter für über greifende Rollenübernahmean.
b. Wählen Sie Neu.
c. Konfigurieren Sie im Formular nur die folgenden Felder für den vertrauenden Account:
Formular „AWS-übergreifende Rollen übernahmeparameter für Cloud-Service-Account“
<table>
<tr><th>Feld</th><th>Beschreibung</th></tr>
<tr><td>Name der Zugriffsrolle</td><td>Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.</td></tr>
<tr><td>Cloud-Servicekonto</td><td>Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen.</td></tr>
</table>
d. Wählen Sie Absenden.</td></tr>
</table>

Nächste Maßnahme

Stellen Sie sicher, dass ServiceNow-Anwendungen mithilfe der IAM-Rolle auf das vertrauende Servicekonto zugreifen können:

1. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.
2. Wählen Sie das Vertrauen aus AWS Service-Account.
3. Unter **Zugehörige Links** , Wählen Sie aus **Erstellen Sie Einen Discovery-Zeitplan** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie auf der Seite Discovery Manager Cloud Discovery die Option aus **Test-Account** .
   - Wenn die Verbindung erfolgreich ist, wird eine Meldung angezeigt, die angibt, dass die Accountvalidierung erfolgreich war.
   - Wenn die Verbindung nicht erfolgreich ist, wird eine Fehlermeldung angezeigt, die die Fehlerursache angibt.

Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren

Konfigurieren Sie den Zugriff für AWS mitglieds-Accounts mithilfe einer Vertrauenskette vom Zugriffsberechtigten über den Verwaltungs-Account.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Vergewissern Sie sich, dass Sie wissen, welche AWS-Mitgliedskonten demselben Verwaltungskonto zugewiesen sind. Sie verwenden das Verwaltungskonto zur Konfiguration temporärer Anmeldeinformationen für die Cloud-Erkennung mithilfe von IAM-Rollen.
- Bestätigen Sie das Discovery-Administratorarbeitsbereich Verwendet mindestens Version 1.10.0. Die **Discovery** > **Cloud-Service-Accounts** Das Navigationsmodul ist mit früheren Versionen nicht verfügbar. Um auf zuzugreifen **Cloud-Service-Accounts** Geben Sie bei einer früheren Version im Navigationsfilter Folgendes ein: `cmdb_ci_Cloud_Service_Account.list` .

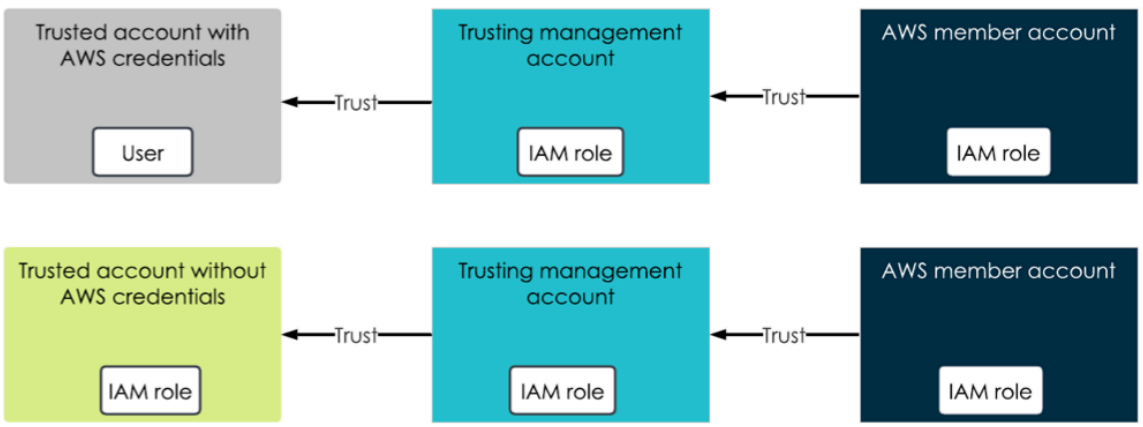
Erforderliche Rolle:

- Für Cloud-Discovery: Discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Zugriff für konfigurieren AWS mitglieds-Accounts mithilfe einer Vertrauenskette vom Zugriffsberechtigten über den Verwaltungs-Account. Der Account des Zugriffsberechtigten hat entweder AWS Anmeldeinformationen oder verwendet eine Methode ohne Anmeldeinformationen.

Mitgliedskonten so konfigurieren, dass sie für den Zugriff das jeweilige Verwaltungskonto nutzen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine IAM-Rolle für den Mitgliedsaccount, und konfigurieren Sie die Vertrauensbeziehung zwischen dem Anwender, der diese Rolle übernimmt, und dem vertrauenswürdigen Verwaltungs-Account.

   a. Melden Sie sich bei der AWS-Managementkonsole mit den Anmeldeinformationen des Mitgliedskontos an, für das Sie den Zugriff konfigurieren.

   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des Verwaltungskontos angeben.
   Bedienungsinformationen zum Erstellen von AWS-Rollen finden Sie in der Amazon-Dokumentation.

   c. Klicken Sie auf der Seite **Summary** (Zusammenfassung) für die IAM-Rolle auf die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten).
   Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

   e. Bearbeiten Sie die Vertrauensstellung wie folgt:

   - Legen Sie den Parameter *`Action`* auf `sts:AssumeRole` fest.
   - Legen Sie den Parameter `AWS` auf den vollständigen ARN der Rolle des Verwaltungskontos fest.

   f. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Auf der ServiceNow AI Platform, Konfigurieren Sie den Service-Account des vertrauenden Mitglieds.

   a. Navigieren zu **Alle** > **Discovery** > **Cloud-Service-Accounts**an.

   b. Wählen Sie **Neu**.

   c. In **Übergeordneter Account** Geben Sie den Namen des Verwaltungs-Accounts ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Füllen Sie die verbleibenden Felder im Formular aus.
Eine Beschreibung der Feldwerte finden Sie unter Erstellen AWS Service-Accounts.

e. Wählen Sie **Absenden**.

3. Auf der ServiceNow AI Platform, Weisen Sie zu AWS IAM-Rolle für den Mitgliedsaccount.

> **Wichtig:** Führen Sie diesen Schritt nur aus, wenn Sie anwenderdefinierte IAM-Rollen erstellt haben. Standardmäßig ist die Rolle OrganizationAccountAccessRole dem vertrauenden Verwaltungsaccount des Mitglieds zugewiesen, und Sie müssen die Rolle OrganizationAccountAccessRole keinem Service-Account zuweisen.

a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS-Org. – Parameter für Rollenübernahme**an.

b. Wählen Sie **Neu**.

c. Konfigurieren Sie im Formular nur die folgenden Felder für den Account des vertrauenden Mitglieds:

Formular „AWS-Organisation für Cloud-Service-Account – Rollenparameter übernehmen“

Feld	Definition
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde. ▪ Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den vollständigen ARN mit einem Sternchen (*) als Platzhalter für die Account-ID im folgenden Format ein: `arn:aws:iam::*:role/MemberRoleName` . Beispiel: `arn:aws:iam::*:role/SN_MEMBER_ACCOUNT_ROLE` . ▪ Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie den vollständigen ARN der spezifischen IAM-Rolle für jeden Mitgliedsaccount in einem separaten Eintrag ein.
Cloud-Servicekonto	Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen. ▪ Wenn IAM-Rollen für alle Mitgliedsaccounts identisch sind: Geben Sie den Namen des Verwaltungsaccounts ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Definition
	▪ Wenn sich die IAM-Rollen in den Mitgliedsaccounts unterscheiden: Geben Sie jeden Mitgliedsaccount in einem separaten Eintrag ein.

d. Wählen Sie **Absenden**.

Nächste Maßnahme

Konfigurieren Sie den vertrauenden Verwaltungsaccount und den vertrauenswürdigen Zugriffsberechtigungsaccount.

- Informationen zum Konfigurieren von Zugriffsberechtigungskonten mit AWS Anmeldeinformationen, siehe Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.
- Informationen zum Konfigurieren von Zugriffsberechtigungsaccounts ohne AWS Anmeldeinformationen, siehe Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren.

MID-Server für AWS-IAM-Rollen konfigurieren

Konfigurieren Sie den MID-Server, um die temporären Sicherheitsanmeldeinformationen abzurufen, die einer IAM-Rolle zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Discovery_admin oder sn_CMP.Cloud_admin (für Cloud Provisioning and Governance)

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **MID-Server**an.
2. Wählen Sie einen MID-Server aus, der auf einer Amazon EC2-Instanz innerhalb des betreffenden AWS-Servicekontos installiert ist.
3. Wählen Sie die zugehörige Liste **Konfigurationsparameter** aus.
4. Klicken Sie auf **Neu**.
5. Wählen Sie im Konfigurationsparameterformular `mid.aws.instance_profile_name` im Feld **Parametername** aus.
6. Geben Sie in das Feld **Wert** den Namen der IAM-Rolle ein, die mit der EC2-Instanz verbunden ist.

   Hinweis: AWS Cloud Discovery für „mid.aws.instance_profile_name" akzeptiert sowohl „Rollenname“ als auch „vollständiger ARN“ als gültige Parameterwerte. Beispielsweise sind beide der folgenden Werte zulässig:

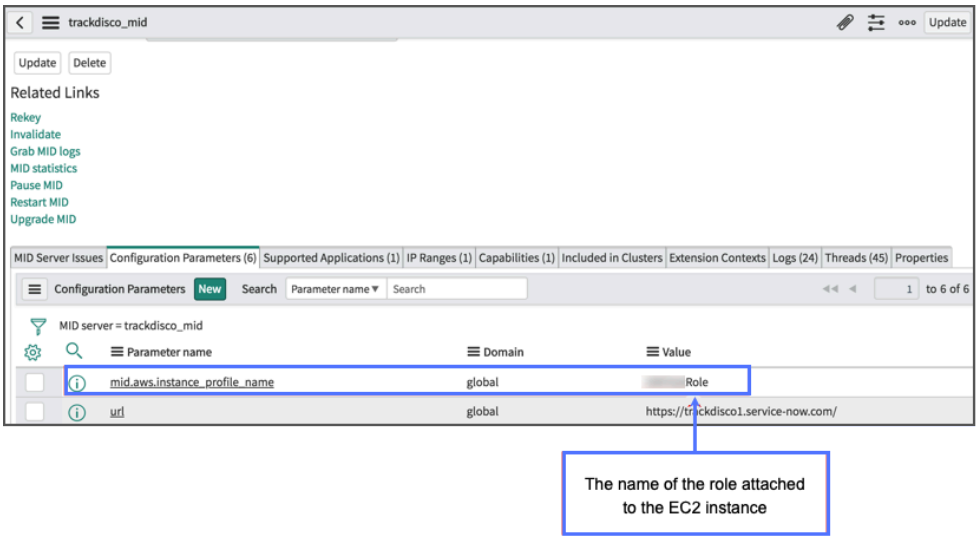
   - arn:Partition:Service:Region:Account-ID:resource-type/resource-ID
   - Ressourcen-ID

   Die MID-Server Verwendet dieselbe IAM-Rolle, die für den entsprechenden eingerichtet ist AWS Service-Account. Weitere Informationen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.

   Für operative Informationen zum Erstellen AWS Rollen finden Sie in der Amazon-Dokumentation unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Anwender .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Absenden**.
   Der neue Parameter wird im MID-Server-Datensatz aufgelistet.



AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern

Konfigurieren Sie Richtlinien mit der erforderlichen Berechtigungsstufe, um Zugriff auf die AWS-Ressourcen für Cloud-Discovery und Cloud Provisioning and Governance bereitzustellen.

Vorbereitungen

Machen Sie sich mit dem Erstellen von IAM-Benutzern und Benutzerrichtlinien vertraut. Konsultieren Sie dazu die AWS-Dokumentation .

Identifizieren Sie die Berechtigungsstufe, die zum Erkennen der Ressourcen mit Cloud-Discovery und zum Verwalten der Ressourcen mit Cloud Provisioning and Governance erforderlich ist. Zum Beispiel:

- Zusätzliche S3-Berechtigungen sind als erforderlich AWS Verwendet einen S3-Bucket, um die Cloud-Formationsvorlagen zu speichern und auszuführen, um Stapel mit CloudFormation bereitzustellen. Diese Berechtigungen sind auch dann erforderlich, wenn Sie dieselbe CloudFormation-Vorlage über die AWS-Konsole ausführen.
- Schreibgeschützter Zugriff ist erforderlich, um eine Muster-Discovery mit der anwenderdefinierten Richtlinie durchzuführen.

Mit AWS CloudFormation werden Ressourcen bereitgestellt und konfiguriert, indem die in der Vorlage beschriebenen AWS-Services aufgerufen werden. Weitere Informationen hierzu finden Sie unter Funktionsweise von AWS CloudFormation .

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Erforderliche Rollen:

- AWS-Verwaltungskonsole-Administrator
- Für Cloud-Discovery: Discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Mit der von Ihnen konfigurierten Richtlinie werden die AWS-Berechtigungen definiert, die Sie einem Benutzer, einer Gruppe oder einer Rolle zuweisen können. Geben Sie abhängig von den AWS-Services, die Sie verwenden, Aktionen für den Service an, um mit Cloud Provisioning and Governance Erkennungs-, Bereitstellungs- und Lebenszyklusaktionen auszuführen.

Prozedur

1. Melden Sie sich bei an AWS Verwaltungskonsole mit den Anmeldeinformationen des entsprechenden Service-Accounts.
   Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwendet haben, um Zugriff mit temporären Anmeldeinformationen bereitzustellen, melden Sie sich mit demselben IAM-Benutzer oder derselben IAM-Rolle an.
2. Öffnen Sie den Benutzerdatensatz in der Instanz für den entsprechenden Benutzer.
3. Definieren Sie eine Benutzerrichtlinie in der AWS-Managementkonsole mit einer der folgenden Methoden:
   - Gewähren Sie dem Administrator Zugriff auf die Instanz. Diese Methode bietet die gleiche Zugriffsebene wie die Verwendung der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels. Hängen Sie die Richtlinie `AdministratorAccess` an das Benutzerprofil an.

     Hinweis: Zum Erstellen einer Benutzerrichtlinie, die nur Cloud-Discovery und nicht die Bereitstellung von Cloud-Ressourcen unterstützt, hängen Sie stattdessen die Richtlinie `ReadOnlyAccess` an.

   - Erstellen Sie eine benutzerdefinierte Richtlinie mit einem beschreibenden Namen. Geben Sie im Feld für das Richtliniendokument den Code ein, der die APIs enthält, deren Ausführung durch diese Richtlinie erlaubt wird.

     Hinweis: Das folgende JSON-Beispiel ist ein Teilbeispiel mit Berechtigungen für Cloud-Discovery. Es handelt sich nicht um eine vollständige Liste aller erforderlichen Berechtigungen.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"PermissionsNeededForDiscovery",
      "Effect":"Allow",
      "Action":[
        "account:ListRegions",
        "apigateway:GET",
        "application-autoscaling:Describe*",
        "autoscaling-plans:Describe*",
        "autoscaling:Describe*",
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeLaunchConfigurations",
        "cloudformation:Describe*",
        "cloudformation:DescribeStack*",
        "cloudformation:List*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "config:ListDiscoveredResources",
        "dynamodb:Describe*",
        "dynamodb:DescribeTable",
        "dynamodb:ListGlobalTables",
        "dynamodb:ListTables",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "ec2:Describe*",
            "ec2:ReportInstanceStatus",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:Describe*",
            "lambda:Get*",
            "lambda:List*",
            "organizations:Describe*",
            "organizations:DescribeOrganization",
            "organizations:List*",
            "rds:Describe*",
            "redshift:Describe*",
            "route53:GetHostedZone",
            "route53:List*",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucket*",
            "s3:GetBucketLocation",
            "s3:List*",
            "sdb:GetAttributes",
            "sns:GetEndpointAttributes",
            "sns:GetSubscriptionAttributes",
            "sns:List*",
            "sns:ListPlatformApplications",
            "sns:ListSubscriptions",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics"
        ],
        "Resource":"*"
    }
  ]
}
```

- Das folgende JSON-Beispiel ist ein Teilbeispiel mit Berechtigungen für Cloud-Discovery Und Cloud Provisioning and Governance. Es handelt sich nicht um eine vollständige Liste aller erforderlichen Berechtigungen.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PermissionsNeededForCPG",
         "Effect": "Allow",
         "Action": [
            "account:ListRegions",
            "apigateway:GET",
            "application-autoscaling:Describe*",
            "autoscaling-plans:Describe*",
            "autoscaling:Describe*",
            "autoscaling:DescribeAutoScalingGroups",
            "autoscaling:DescribeLaunchConfigurations",
            "cloudformation:Describe*",
            "cloudformation:DescribeStack*",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "cloudwatch:Get*",
            "cloudwatch:List*",
            "config:ListDiscoveredResources"
            "dynamodb:Describe*",
            "dynamodb:DescribeTable",
            "dynamodb:ListGlobalTables",
            "dynamodb:ListTables",
            "ec2:Describe*",
            "ec2:ReportInstanceStatus",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:Describe*",
            "lambda:Get*",
            "lambda:List*",
            "organizations:Describe*",
            "organizations:DescribeOrganization",
            "organizations:List*",
            "rds:Describe*",
            "redshift:Describe*",
            "route53:GetHostedZone",
            "route53:List*",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucket*",
            "s3:GetBucketLocation",
            "s3:List*",
            "sdb:GetAttributes",
            "sns:GetEndpointAttributes",
            "sns:GetSubscriptionAttributes",
            "sns:List*",
            "sns:ListPlatformApplications",
            "sns:ListSubscriptions",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics"
        ],
        "Resource": "*"
    },
    {
        "Sid": "MinimalPermissionsNeededForEc2ProvisioningThroughCloudFormation",
        "Effect": "Allow",
        "Action": [
            "cloudformation:CreateStack",
            "cloudformation:CreateUploadBucket",
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStackEvents",
            "cloudformation:DescribeStackResources",
            "cloudformation:DescribeStacks",
            "cloudformation:GetTemplate",
            "cloudformation:GetTemplateSummary",
            "cloudformation:List*",
            "cloudformation:UpdateStack",
            "cloudformation:ValidateTemplate"
            "ec2:*",
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:PutObject"
        ],
        "Resource": "*"
    }
  ]
}
```

Zugehörige Informationen

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create-console.html#access_policies_create-start

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand-service-summary.html

Azure-Servicekonten einrichten

Erstellen und konfigurieren Sie Cloud-Service-Accounts unter ServiceNow AI Platform Für den entsprechenden Microsoft Azure Accounts.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Vorbereitungen

Stellen Sie die Konfiguration von sicher Azure Anmeldeinformationen

Weitere Informationen finden Sie unter Anmeldeinformationen für Azure-Cloud erstellen Und Konfigurationsschritte für Azure-Service-Prinzipalanwender und Anmeldeinformationen (KB2202765)

Stellen Sie sicher, dass Sie mit der Hierarchie von vertraut sind Azure Service-Accounts in Ihrer Umgebung.

Richten Sie die Service-Accounts unter ein ServiceNow AI Platform Um die Hierarchie Ihrer Umgebung widerzuspiegeln. Sie können einrichten Azure Service-Accounts Für Folgendes Azure Account Typen:

- Verwaltungsgruppe .
- Abonnement .

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Service-Account ist ein sicherer Datensatz in Ihrer Instanz, der die Anmeldeinformationen und Zugriffsinformationen für Ihren Provider-Account speichert. Discovery Verwendet die Informationen, um auf Ihren Provider-Account zuzugreifen, um Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Account ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infrastruktur in der Cloud-Verwaltung. Ein Cloud-Account kann mehrere Service-Accounts enthalten, sogar Service-Accounts verschiedener Anbieter. Geben Sie für jeden Service-Account an, welches Rechenzentrum in den Cloud-Account aufgenommen werden soll.

Prozedur

1. Geben Sie im Navigationsfilter ein `cmdb_ci_Cloud_Service_Account.list` .
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder in der folgenden Reihenfolge aus:
   a. Wählen Sie das Rechenzentrum aus.
   b. Aktivieren Sie das Kontrollkästchen von **Ist Verwaltungsaccount** Wenn Sie einen Service-Account für eine Verwaltungsgruppe erstellen.
   c. Wählen Sie Aus **Sollte Ereignisse abrufen** Um die ereignisbasierte Discovery vorzubereiten. Weitere Informationen finden Sie unter Über Microsoft Azure-Warnungen gesteuerte Erkennung

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	Wenn Sie einen Service-Account für eine Verwaltungsgruppe erstellen, füllen Sie aus Azure Verwaltungsgruppe ID, die zur Verwaltungsgruppe gehört. Wenn Sie einen Service-Account für ein Abonnement erstellen , Füllen Sie aus Azure Abonnement ID .
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind.
Rechenzentrums-URL	URL des Rechenzentrums. Die Konfiguration dieses Felds ist für erforderlich Azure Gov Cloud-Accounts (USA). Beispiel: https://management.usgovcloudapi.net/.
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie Aus **Azure-Rechenzentrum** .
Rechenzentrums-Discovery-Status	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung der Discovery im Rechenzentrum.
Übergeordneter Account	Beim Einrichten von Service Account Für einen Azure Abonnement , Füllen Sie die Verwaltung aus Gruppe ID. Wenn **Ist Verwaltungsaccount** Kontrollkästchen Ist ausgewählt, th E **Übergeordneter Account** Feld Ist nicht zutreffend
Account des Zugriffsberechtigten	Nicht zutreffend für Azure Service-Accounts.

4. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erkennung von Azure-Clouds

Richten Sie Google Cloud Platform-Service-Accounts ein

Erstellen und konfigurieren Sie Cloud-Service-Accounts unter ServiceNow AI Platform Für den entsprechenden Google Cloud Platform(GCP) Service-Accounts.

GCP Der Service-Account ist ein eindeutiger Account, der normalerweise von einer Anwendung oder einer Rechenarbeitsauslastung verwendet wird, z. B. einer Compute Engine-Instanz, und nicht von einem Anwender. Ein Service-Account wird anhand seiner E-Mail-Adresse identifiziert, die für den Account eindeutig ist. Es wird verwendet, um Interaktionen zwischen Ihrer Anwendung und verschiedenen GCP-Services zu authentifizieren und zu autorisieren.

Überprüfen Sie die REST API-Berechtigungen

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

Konfigurieren Sie Google API-Anmeldeinformationen für Cloud-Discovery

Erstellen Google API-Anmeldeinformationen, die zugelassen werden sollen Cloud-Discovery Um auf die Daten in zuzugreifen Google Account sicher.

Vorbereitungen

Stellen Sie sicher, dass die neuesten Versionen der folgenden Anwendungen installiert sind:

- Muster für Discovery und Service-Mapping
- Visibility Content
- CMDB CI-Klassenmodelle

Erforderliche Rolle: Discovery_ Administrator

Prozedur

Konfigurieren Sie GCP Anmeldeinformationen entweder durch Importieren einer JSON-Datei oder durch manuelles Einreichen des Datensatzes.

Option	Aktionen
Importieren Sie die JSON-Datei	**a.** Beim Erhalt der E-Mail von GCP, Laden Sie die JSON-Datei herunter. **b.** Navigieren zu **Discovery** > **Anmeldeinformationen**an. **c.** Wählen Sie Aus **Neu** Und wählen Sie dann aus **Google API-Anmeldeinformationen** . **d.** Wählen Sie Aus **JSON-Datei importieren**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktionen
	e. Wählen Sie Aus **Wählen Sie Datei** Und wählen Sie die heruntergeladene JSON-Datei aus. **f.** Wählen Sie Aus **Laden Sie Anmeldeinformationsdaten Hoch** .
Konfigurieren Sie die Anmeldeinformationen manuell	**a.** Navigieren zu **Discovery** > **Anmeldeinformationen**an. **b.** Wählen Sie Aus **Neu** Und wählen Sie dann aus **Google API-Anmeldeinformationen** . **c.** Wählen Sie **Neu**. **d.** Füllen Sie die Felder im Formular gemäß der Formularbeschreibung aus. Eine Beschreibung der Formularfelder finden Sie unter Google API-Anmeldeinformationsformular. **e.** Wählen Sie **Absenden**.

Google API-Anmeldeinformationsformular

Füllen Sie das Formular „Google API-Anmeldeinformationen“ aus, um die Anmeldeinformationen zu konfigurieren.

Feld	Beschreibung
Name	Legen Sie einen eindeutigen Namen für fest Google Cloud API-Anmeldeinformationen.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	MID-Server, auf den Sie die Anmeldeinformationen anwenden. Wählen Sie **Alle MID Server**.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen ausführt, wenn versucht wird, sich bei Geräten anzumelden. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
E-Mail	Ihr GCP E-Mail-Adresse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Schlüssel	Geheimer Schlüssel, den Sie auf der generiert haben Google Cloud Konsole.
Anmeldeinformationsalias	Ein Anmeldeinformationsalias, der von den Anmeldeinformationen zum Autorisieren von Aktionen verwendet wird.

Erstellen GCP Service-Accounts

Erstellen Google Cloud Platform (GCP) Service-Accounts auf der ServiceNow AI Platform Um auf zuzugreifen GCP Account während GCP Discovery.

Vorbereitungen

Überprüfen Sie, ob Google API-Anmeldeinformationen erstellt wurden. Weitere Informationen finden Sie unter Konfigurieren Sie Google API-Anmeldeinformationen für Cloud-Discovery.

Rufen Sie ab **Projekt_ID** Wert aus der JSON-Schlüsseldatei, die dem Service-Account zugeordnet ist.

Erforderliche Rolle: discovery_admin

Prozedur

1. Geben Sie im Navigationsfilter ein `cmdb_ci_Cloud_Service_Account.list` .
2. Wählen Sie **Neu**.
3. In **Feld „Discovery-Anmeldeinformationen“** , Beginnen Sie mit der Eingabe des Anmeldeinformationsnamens, und wählen Sie ihn aus der Liste aus.
4. Füllen Sie die verbleibenden Felder im Formular aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Ein eindeutiger Name für GCP Service-Account.
Konto-ID	GCP Projekt-ID.
Rechenzentrums-URL	URL des Rechenzentrums, die leer bleiben sollte.
Datencenter-Typ	Typ des Rechenzentrums, in dem der Account gehostet wird, wobei es sich um das Google-Rechenzentrum [cmdb_ci_google_Datacenter] handeln muss.

5. Wählen Sie **Absenden**.

Nächste Maßnahme

Planen Sie einen GCP Cloud-Discovery. Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Cloud Operations Workspace.

GCP-Zugriff und -Berechtigung mithilfe von Richtlinien

Google Cloud Platform(GCP) Zugriff und Berechtigungen mithilfe von Richtlinien bieten Berechtigungen für die sichere Nutzung und Verwaltung von Cloud-Ressourcen in GCP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laden Sie herunter Cloud-Discovery Mustertabelle Damit können Sie Anwenderberechtigungen gewähren, die für die Ausführung von erforderlich sind Discovery Muster. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, um sicherzustellen, dass Sie über die neueste Version der Tabelle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.